MICRO FOCUS

TeamWorks 18.2.1
Maintenance Guide

March 2020

Legal Notice

Contents

About This Guide

This guide is for TeamWorks administrators and covers various TeamWorks administrative tasks that come into play after your TeamWorks system is deployed and providing services to end users.

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 this guide and other documentation, visit the Micro Focus TeamWorks Documentation website (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).

1 Adding an Appliance to an Existing Deployment

You can add TeamWorks appliances to the TeamWorks system to accommodate additional load only if your original TeamWorks system was configured with shared storage (`/vashare`).

Do Not Mix Appliance Versions

It is critical to never allow mixed-version appliances to service user requests in the same deployment.

If mixed versions are allowed to service user requests, a full reindex of the system might be required to restore service stability.

Follow the instructions in this section exactly to avoid mixed-version problems.

Prerequisites

You can add TeamWorks and Search appliances to an existing TeamWorks deployment only if your TeamWorks deployment meets the following prerequisites:

- **It is not an all-in-one TeamWorks deployment:** All-in-one TeamWorks deployments cannot be expanded.
- **The NFS mount is accessible to all appliances:** All TeamWorks appliances in the cluster need to have access to the NFS mount.
- **(Recommended) A load balancing solution is in place:** If you want to provide a common access URL for all your TeamWorks users, you must provide a solution for load balancing between the TeamWorks appliances.

  Micro Focus does not provide a load balancing appliance; however, there are many software solutions available, such as Apache, HAProxy, and NGinx.

  There are also hardware solutions available, such as F5 Networks, Juniper, Riverbend, and A10 Networks.

  Searching the web for `Layer 4-7 switches` or `Application Delivery Controller` is a good place to start finding a solution that meets your requirements.

Adding 18.2 Search Appliances to an Existing Deployment

To add Search appliances to an exiting large TeamWorks deployment:

1. Ensure that your system meets the necessary prerequisites.
2. Assuming that you have planned the installation, downloaded the software, and so on, install the additional Search appliance, beginning with "Setting Up Subsequent Search Appliances" in the *GroupWise TeamWorks 18.2.1: Installation and Deployment Guide*.

   IMPORTANT: Choose the same configuration options (including the same NFS mount) that you chose when you installed the original Search appliance.
3. Run the installation wizard for a multiple-appliance deployment (at port 9443), as described in "Setting Up Subsequent Search Appliances" in the *GroupWise TeamWorks 18.2.1: Installation and Deployment Guide*.
4. Restart each TeamWorks appliance to ensure that the entire TeamkWorks system is synchronized.

Adding 18.2 TeamWorks Appliances to an Existing Deployment

To add a TeamWorks appliance to an exiting large TeamWorks deployment:

1. Ensure that your system meets the necessary prerequisites.
2. Assuming that you have planned the installation, downloaded the software, and so on, install the additional TeamWork appliance, beginning with "Creating the TeamWorks Virtual Machines" in the *GroupWise TeamWorks 18.2.1: Installation and Deployment Guide*.

   The process is the same as when you installed the original TeamWorks appliances.

   IMPORTANT: Choose the same configuration options (including the same NFS mount) that you chose when you installed the original TeamWorks appliances.
3. Run the installation wizard for a multiple-appliance deployment (at port 9443), as described in "Setting Up the TeamWorks Appliances" in the *GroupWise TeamWorks 18.2.1: Installation and Deployment Guide*.

2 Port 8443 Administrative Access

About Port 8443 Administrators

There are two types of Port 8443 Administrators

- **Built-in administrator (Admin):** This user, named Admin by default, has full rights to the Port 8443 console, including the right to add or remove Direct administrators.
- **Direct administrators:** Have rights to administer only
  - Users
  - Groups

Adding or Removing Administrative Rights for Users and Groups

See “Assigning and Managing Port 8443 Designated Administrators” in the *TeamWorks 18.2.1: Administrative UI Reference*.

Modifying Port 8443 Administrator Accounts

The modifications you can make depend on the type of user, as follows:

- **Built in administrator:** You can change this username and password by logging in as the user, clicking the ***Username*** (upper right), selecting **View Profile**, clicking **Edit**, and making the changes.

  Changing this affects
  - The name you enter to log in as the built-in administrator
  - The name that appears in the upper-right corner of the Port 8443 console
  - The name that appears in the administration console under **Administrators**
- **LDAP users (Direct administrators):** User names and passwords are controlled in the LDAP source.
- **Internal TeamWorks users:** User names cannot be changed; passwords can.

  Administrators click the user in the Users list, click the Profile button, and enter a new password.

  Internal users edit their profile to change their passwords.

Simplifying Management through Administrative Groups

You can simplify your management tasks by creating administrative groups and assigning group members with specific administrative tasks.

1. Create a group.
2. Add it to the **Administrators** list.

   See “Assigning and Managing Port 8443 Designated Administrators” in the *TeamWorks 18.2.1: Administrative UI Reference*
3. Assign users to the group.
4. Task group members with specific tasks that they have rights to perform.

3 Helping Micro Focus Improve TeamWorks

In order to improve the TeamWorks product, it is critical that the TeamWorks development team understands how organizations are deploying TeamWorks.

Organizational Privacy Is Protected

IMPORTANT: We do not collect information that can be used to identify specific organizations.

Rather we collect the following, depending on how you configure your system.

At a basic level (Tier 1), TeamWorks collects the following information:

- Product version
- License type
- Number of users

If you allow us to, we also collect basic information about the deployment size and configuration:

You can view the information collected after the system has been running for 24 hours, by using the View the information collected link in the Product Improvement dialog.

How Micro Focus Collects Product Improvement Data

The first time you log in to TeamWorks, after changing the admin user’s password, a dialog displays that explains the purpose of the TeamWorks data collection system and lets you change the configuration.

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

See “Product Improvement” in the *TeamWorks 18.2.1: Administrative UI Reference*.

How Micro Focus Receives Product Improvement Data

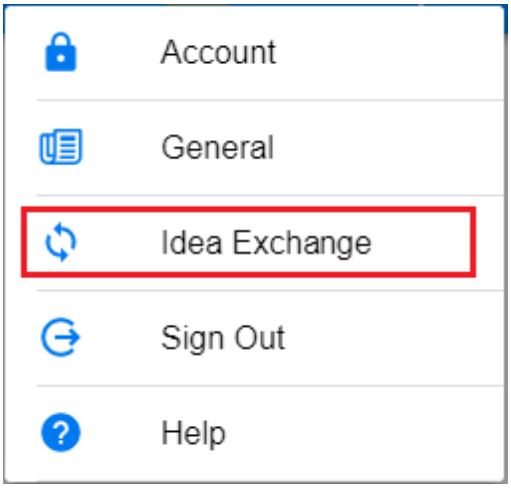
After the weekly data collection process concludes, the system creates a `.json` data file and sends it to `ftp://productfeedback.novell.com/stats/TeamWorks`.

If the FTP transfer is unsuccessful, the system attempts to send it again during the next weekly cycle. No send attempts are made outside of the weekly cycles.

Data files are sent through a regular non-secure FTP connection. File contents are not encrypted because no sensitive or identifying information is included.

Submitting Your Product Improvement Ideas

When you are logged in as an administrative user, you can access the Micro Focus TeamWorks Ideas Portal page from the Port 8443 TeamWorks Administration Console by clicking the Gear icon and selecting the **Idea Exchange** link.



You can also view the ideas that others have submitted, add comments, and vote for your favorite product-improvement ideas.

4 Language and Locale Settings

The following points summarize TeamWorks' language settings:

- **Administrative Interfaces:** These are English only.
- **User App Interfaces:** These reflect the language settings of the mobile device, web browser, or GroupWise client.
- **Email Notifications:** These reflect the Locale setting for individual users. Locale settings are assigned to users at the time they are created, as follows:
  - **LDAP Users:** When you import LDAP users, their Locale reflects the Default Locale at the time of the import.

    The Default Locale is set at install time.

    It can be changed in the Port 8443 Console: **LDAP > User Settings > Use the following when creating new users**.

    Changes to the Default Locale affect only those LDAP users that are imported subsequent to the change.
  - **Internal (Non-LDAP) Users:** When you create an internal user, the Locale drop-down list reflects the setting in **Port 8443 ConsoleManagementDefault User Settings**, by default. However, if desired, you can select another Locale as you create each user.
- **Changing Users' Profiles:** Port 8443 administrators can change the Locale for any users (LDAP or internal) by editing their profiles. See "Viewing and Managing User Properties" in the *TeamWorks 18.2.1: Administrative UI Reference*.

5 Monitoring

For information on all TeamWorks monitoring capabilities, see “Logging and Monitoring” in the *TeamWorks 18.2.1: Administrative UI Reference*.

Enabling Debug Logging

IMPORTANT: Do not adjust the settings described in this section unless you are instructed to do so by a TeamWorks support engineer.

Adjusting the settings without guidance from TeamWorks support can negatively impact the performance of your TeamWorks deployment.

1. In a text editor, open the `log4j.properties` file from both of the following directories:

   `/opt/novell/esncd esn/apache-tomcat/conf`
2. Uncomment each line for which you want to enable debug logging in the `log4j.properties` file.
3. Monitor the `/var/opt/novell/tomcat-esn/logs/appserver.log` file.

Monitoring the Indexing Process

1. On the TeamWorks appliance (or on any appliance in a TeamWorks cluster), append the following line to the `/opt/novell/esn/apache-tomcat/webapps/ssf/WEB-INF/log4j.properties` file:

   ```
   log4j.category.org.kablink.teaming.module.binder.impl.BinderModuleImpl=INFO
   ```
2. Restart the TeamWorks process with `rcTeamWorks restart`.
3. After re-indexing has started, watch the `ssf.log` file for the following statement:

   ```
   2013-06- INFO  [http-bio-8080-exec-1]
   [org.kablink.teaming.module.binder.impl.BinderModuleImpl] - indexTree took
   1480.470827 ms
   ```
4. Check the results using `grep indexTree /var/opt/novell/apache-tomcat/logs/ssf.log`.

   Look for the key words "indexTree took" as shown above.

   This shows that the re-indexing previously triggered has now completed.

   Please note that the indexing recommendations made elsewhere in this guide still apply, and a pair of TeamWorks Search appliances should be deployed as part of your system. Start both TeamWorks Search appliances as `read/write` and make them available to TeamWorks Clients. Change one of the appliances to be indexed to `Write` and use that server for the re-index process.

This forces all the TeamWorks clients to use the other indexing server.

After the re-indexing process is complete, as indicated by the log file discussed earlier, the appliance can be changed back to `Read/Write`. Any deferred updates should be applied, and the second server can then be re-indexed by using the same process.

6 PostgreSQL—Backup and Restore from the Command Prompt

IMPORTANT: If you deploy the Micro Focus PostgreSQL appliance, use the phpPgAdmin web front end to back up the TeamWorks database.

A “Hot Backup” process for PostgreSQL is available from Oracle as part of the paid-for version of PostgreSQL.

Backing Up PostgreSQL from the Command Line

If you need to back up or restore the TeamWorks database from the command line, do the following:

1. Shut down the PostgreSQL service.
2. Run the following command:

   ```
   PostgreSQLdump -u root -p TeamWorks >/backupdir/TeamWorksback.sql
   ```

   This creates a file named `TeamWorksback` that can be used to restore the database.
3. Restart PostgreSQL.

Restoring PostgreSQL from a Backup File

1. (Optional) If a `TeamWorks` table does not exist in the location where you want to restore the TeamWorks database, you must create it as follows:
   a. Log in to PostgreSQL using the following command:

      ```
      PostgreSQL -p
      ```

   b. Create the database using the following command:

      ```
      create database TeamWorks;
      ```
2. When a `TeamWorks` table exists on the location where you want to restore the database, do the following:
   a. Quit PostgreSQL
   b. Run the following command:

      ```
      PostgreSQL -p TeamWorks < /backupdir/TeamWorks-back.sql
      ```

   This completes the restore of the TeamWorks database and its associated tables.

7 Customizing Email Notifications

You can customize many of the TeamWorks-generated strings that appear in notifications sent to TeamWorks users.

About TeamWorks's Email Templates

TeamWorks generates email notifications using Apache Velocity version 1.5 templates.

You can customize the following templates:

Template Name	Purpose
footer.vm	Text or images applied at the end of each email
header.vm	Text or images applied at the beginning of each email
passwordChangedNotification.vm	Notification that user's password changed
publicLinkNotification.vm	Notifcation of a publicly available link to a file
selfRegistrationRequired.vm	Shared item notification to user who must register with TeamWorks in order to view it
sharedEntryInvite.vm	Shared file invitation to an existing TeamWorks user
sharedEntryNotification.vm	Shared file notification of change to existing TeamWorks user
sharedFolderInvite.vm	Shared folder invitation to existing TeamWorks user
sharedFolderNotification.vm	Shared folder notification of change to existing TeamWorks user
style.vm	CSS style sheet for email notifications
teaming.vm	Macros that get applied to all emails

Template Tips and Documentation

IMPORTANT: Micro Focus TeamWorks doesn't attempt to document third-party products, such as Apache Velocity.

For complete information and instructions for the Apache Velocity version 1.5 template language, visit the Apache Velocity Project website (https://velocity.apache.org/engine/releases/velocity-1.5/).

The following are tips about the template files in TeamWorks.

- Each template contains a brief explanation about what it affects and what you can customize in it.
- TeamWorks system-generated emails contain both text and HTML MIME parts.

  You can customize these independently.
- You can customize for specific languages to localize the emails your TeamWorks system generates.
- You can revert back to the default template by selecting a customized template in the list and then clicking the Delete button.
- Make sure you use the Velocity documentation (https://velocity.apache.org/engine/releases/velocity-1.5/user-guide.html).

  For example, one user assumed that the hash marks (#) indicated comments, when in fact they are part of the Velocity scripting language.

Modifying the Email Template Files

The default email templates that reside on the TeamWorks system cannot be changed or deleted, but you can create and deploy customized copies of them by doing the following:

1. Download a template to your local disk by clicking it in the Email Templates dialog.
2. Open the downloaded template in a text editor.
3. Customize the file as discussed in the Video Walkthrough below and documented on the Apache Velocity Project website (https://velocity.apache.org/engine/releases/velocity-1.5/).
4. Save the template on your local disk.
5. Upload the customized file by dragging and dropping it into the Email Templates dialog.

   The **Type** then changes to **Customized**.

Email Template Customization—A Video Walkthrough

To see a demonstration of the email template customization process, view the following video created for the Micro Focus Filr release:

http://www.youtube.com/watch?v=AA4A-nG3dlY

8 Search Appliance Maintenance

Best Practices

Best practices require that multi-appliance TeamWorks deployments have three active Search appliances.

- Never remove from service more than one Search appliance at a time.
- Always Make sure that the appliance is back in service as soon as possible.

  Allowing extended search-appliance downtime risks creating a split-brain situation wherein multiple appliances have taken on the primary-node role.

CAUTION: After the appliance is decommissioned and permanently removed from service, make sure that you replace it as soon as possible.

IMPORTANT: If running this process breaks your TeamWorks system, you must contact Micro Focus Support for help with repairing it.

Permanently Removing (Decommissioning) a Search Appliance

When using the **Decommission Server** option, make sure to complete all of the following steps in the order prescribed.

1. Access the Port 9443 Appliance Console on the Search appliance that you are planning to decommission.
2. Click the Configuration icon, then click **Services**.
3. Make sure that Search Cluster Health is Green (healthy).

   NOTE: If the status is Yellow, that means that the TeamWorks system is working to return to a healthy state. We recommend that you give it a few minutes and then check back.

   If the status is Red or if it has been Yellow for an extended period of time, you should contact Micro Focus Support for help resolving the issue.

   ---
4. Click **Decommission Appliance** and confirm that you want the process to proceed.
5. When a message displays indicating that the Search appliance has been removed from the deployment, you can shut down the appliance.

   All traces of the decomissioned appliance have been removed from the TeamWorks deployment. You can even reuse the IP address for another search appliance in the future if needed.

Shutting Down and Restarting All Search Appliances

If you need to shut down your TeamWorks Deployment, make sure to follow the instructions in Chapter 10, “Shutting Down and Restarting TeamWorks Appliances,” on page 37.

Best practices dictate that you run TeamWorks Messaging Services on two of your three Search appliances.

9 Security

Backup and Restore

- VMware lets you create virtual disks on remote storage, which can be backed up and restored independent of TeamWorks.

Certificate Maintenance

Micro Focus appliances ship with a self-signed digital certificate. However, you should use a trusted server certificate that is signed by a trusted certificate authority (CA) such as VeriSign or Equifax.

The certificate works for both the Micro Focus Appliance and the TeamWorks software (ports 9443 and 8443, respectively). You do not need to update your certificate when you update the TeamWorks software.

Complete the following sections to change the digital certificate for your Micro Focus Appliance. You can use the digital certificate tool to create your own certificate and then have it signed by a CA, or you can use an existing certificate and key pair if you have one that you want to use.

NOTE: If you are using a Godaddy SSL certificate with TeamWorks, follow the steps in "Godaddy SSL Certificates for TeamWorks" (https://www.novell.com/communities/coolsolutions/godaddy-ssl-certificates-for-filr/) at the Micro Focus Cool Solutions website (https://www.novell.com/communities/coolsolutions/).

Using the Digital Certificate Tool

Creating a New Self-Signed Certificate

Path: Port 9443 Appliance Console

1. Log in to the Micro Focus appliance at https://*server_url*:9443.
2. Click **Digital Certificates**.
3. In the **Key Store** drop-down list, ensure that **Web Application Certificates** is selected.
4. Click **File** > **New Certificate (Key Pair)**, then specify the following information:

   Alias: Specify a name that you want to use to identify and manage this certificate.

   Validity (days): Specify how long you want the certificate to remain valid.

   Key Algorithm: Select either **RSA** or **DSA**.

   Key Size: Select the desired key size.

   Signature Algorithm: Select the desired signature algorithm.

   Common Name (CN): This must match the server name in the URL in order for browsers to accept the certificate for SSL communication.

   Organizational Unit (OU): (Optional) Small organization name, such as a department or division. For example, Purchasing.

   Organization (O): (Optional) Large organization name. For example, Micro Focus

   City or Lacality (L): (Optional) City name. For example, Provo.

   State or Province (ST): (Optional) State or province name. For example, Utah.

   Two-letter Country Code (C): (Optional) Two-letter country code. For example, US.
5. Click **OK** to create the certificate.

   After the certificate is created, it is self-signed.
6. Make the certificate official, as described in "Getting Your Certificate Officially Signed" on page 27.

Getting Your Certificate Officially Signed

1. On the Digital Certificates page, select the certificate that you just created, then click **File** > **Certificate Requests** > **Generate CSR**.
2. Complete the process of emailing your digital certificate to a certificate authority (CA), such as Verisign.

   The CA takes your Certificate Signing Request (CSR) and generates an official certificate based on the information in the CSR. The CA then mails the new certificate and certificate chain back to you.
3. After you have received the official certificate and certificate chain from the CA:
   - **3a** Revisit the Digital Certificates page by clicking **Digital Certificates** from the Micro Focus Appliance.
   - **3b** Click **File** > **Import** > **Trusted Certificate**. Browse to the trusted certificate chain that you received from the CA, then click **OK**.
   - **3c** Select the self-signed certificate, then click **File** > **Certification Request** > **Import CA Reply**.
   - **3d** Browse to and upload the official certificate to be used to update the certificate information.

     On the Digital Certificates page, the name in the **Issuer** column for your certificate changes to the name of the CA that stamped your certificate.
4. Activate the certificate, as described in “Activating the Certificate” on page 27.

Using an Existing Certificate and Key Pair

When you use an existing certificate and key pair, use the .P12 key pair format.

1. Go to the Digital Certificates page by clicking **Digital Certificates** from the Micro Focus Appliance.
2. Click **File** > **Import** > **Trusted Certificate**. Browse to and select your existing certificate, then click **OK**.
3. Click **File** > **Import** > **Trusted Certificate**. Browse to your existing certificate chain for the certificate that you selected in Step 2, then click **OK**.
4. Click **File** > **Import** > **Key Pair**, then browse to and select your .P12 key pair file, specify your password if needed, then click OK.

   Because of a browser compatibility issue with HTML 5, the path to the certificate is sometimes shown as `c:\fakepath`. This does not adversely affect the import process.
5. Continue with “Activating the Certificate” on page 27.

Activating the Certificate

1. On the Digital Certificates page, select the certificate that you want to make active, click **Set as Active**, then click **Yes**.
2. Verify that the certificate and the certificate chain were created correctly by selecting the certificate and clicking **View Info**.

Managing Certificates

All certificates that are included with the OpenJDK Java package that is bundled with the version of SLES that TeamWorks ships with are installed when you install TeamWorks.

TeamWorks uses only the certificates that relate to LDAP and SMTP.

You can use the Digital Certificates tool on the TeamWorks appliance to remove certificates that are not used by your organization if you are concerned about keeping them.

Also, you can use the Digital Certificates tool on the TeamWorks appliance to maintain the certificate store by removing certificates that have expired and then installing new certificates as needed, according to your organization's security policies.

To access the Digital Certificates tool:

1 Click **Digital Certificates** from the Micro Focus Appliance.

Coverity

The TeamWorks development team runs all TeamWorks code through Coverity.

Coverity not only checks for memory leaks and possible bugs using stack code analysis techniques, but it also helps developers identify security vulnerabilities, such as buffer over-runs.

Database Communication Encryption

TeamWorks Administrators can enable or disable data encryption between the TeamWorks server and the database.

The Database Connection page on the Appliance Console now includes a new option **Encrypt Database Communication** that enables you to encrypt the data from the TeamWorks server. This option is disabled by default. Before selecting this option, you must ensure that the settings for your database are enabled to allow encryption of the data from the database server to the TeamWorks server.

- "Configuring the Database for Secure Communications" on page 28
- "Configuring TeamWorks for Secure Communications" on page 29

Configuring the Database for Secure Communications

To enable data encryption between the TeamWorks server and the database server, you must first configure your database server to support data encryption. Only then can you configure the settings on the TeamWorks server.

- "For the PostgreSQL Appliance" on page 29
- "For Other Database Servers" on page 29

For the PostgreSQL Appliance

If you are using the PostgreSQL appliance, perform the following steps to secure the database communication:

1. On the PostgreSQL database server, create a folder named `/vastorage/conf/ssl-certs-dir/`.
2. Download the `ssl_PostgreSQL.sh` script from the TeamWorks 1.0 download site (https://www.microfocus.com/products/filr/trial-download) to the folder you created in the previous step.

   Registration with Micro Focus is required. If you have already registered and received an email with a download link, the file is on the linked page.
3. Run the following command to install the files required for data encryption:

   ```
   # sh ssl_PostgreSQL.sh INSTALL
   ```
4. Run the following command to enable the SSL setting:

   ```
   # sh ssl_PostgreSQL.sh ENABLE <db-root-password>
   ```
5. Run the following command to check if SSL is enabled in the PostgreSQL database server. The value of **have_ssl** flag should have changed from **DISABLED** to **YES**.

   ```
   # PostgreSQL -uroot -p<db-root-password> -e "SHOW GLOBAL VARIABLES LIKE 'have_%ssl';"
   ```

NOTE: To disable the secure database communication, run the following command:

```
# sh ssl_PostgreSQL.sh DISABLE <db-root-password>
```

For Other Database Servers

If you using your existing database server instead of the PostgreSQL appliance, refer to the following database-specific documentation to enable the data encryption from the database server to the TeamWorks server:

- **MS SQL Server:** See *Enable Encrypted Connections to the Database Engine (SQL Server Configuration Manager)* on the Microsoft Website (https://msdn.microsoft.com/en-us/library/ms191192).
- **PostgreSQL Server:** See *Server-Side Configuration for Secure Connections* in the PostgreSQL Documentation (https://dev.mysql.com/doc/refman/5.7/en/using-secure-connections.html).
- **MariaDB Server:** See the following MariaDB Documentation pages:
  - Configuring MariaDB with my.cnf (https://mariadb.com/kb/en/mariadb/configuring-mariadb-with-mycnf/)
  - SSL/TLS System Variables (https://mariadb.com/kb/en/mariadb/ssltls-system-variables/)

Configuring TeamWorks for Secure Communications

IMPORTANT: Before you configure your TeamWorks appliance to support data encryption, you must first configure the database server to support it. See “Configuring the Database for Secure Communications” on page 28.

To configure the TeamWorks server to encrypt data:

1. Log in to the TeamWorks appliance at https://*server_url*:9443.
2. Click **Configuration** > **Database**.
3. Specify the configuration options that apply to your configuration.

   For information about the options, click the help icon.
4. A message reminds you that you must have encryption from the database server already enabled. Ensure that the encryption from the database server is enabled and then click **OK**.
5. Click **OK**, then click **Reconfigure TeamWorks Server** for your changes to take effect.

   This stops and restarts your TeamWorks server. Because this results in server downtime, you should restart the server at off-peak hours.

NOTE: To disable the data encryption between TeamWorks and the database server, you must first disable secure database communication and then deselect the **Encrypt Database Communication** option. For information about configuring the database settings, see "Configuring the Database for Secure Communications" on page 28.

Email Communications Security

When you install Micro Focus TeamWorks, you can choose whether the TeamWorks internal mail host uses TLS (Transport Layer Security) when it communicates with other SMTP mail hosts.

If your TeamWorks site needs to send email messages to an email system that requires secure SMTP (SMTPS), the TeamWorks site must have the same type of root certificate as is required for secure LDAP (LDAPS). If you have not already set up secure LDAP for your TeamWorks site, follow the instructions in "LDAP Synchronization Security" on page 33 to set up secure SMTP for communications with your email system.

Encryption

- TeamWorks encrypts all sensitive authentication credentials and all data on the wire between each TeamWorks appliance.
- Communication between the TeamWorks web application and the TeamWorks server is sent with SSL encryption.
- Communication between the TeamWorks mobile apps and the TeamWorks server is sent with SSL encryption.

TeamWorks Component Security

- **TeamWorks Software:** The TeamWorks software is a customized version of Apache Tomcat. The version of Apache used for the TeamWorks software contains all security fixes and patches that were available when TeamWorks was released.
- **PostgreSQL Database:** The TeamWorks database is a PostgreSQL database built with SuSE Studio, and contains all security fixes and patches that were available when TeamWorks was released.
- **Search:** The search index is an ElasticSearch index. It contains all security fixes and patches that were available when TeamWorks was released.

TeamWorks Data Security

Understanding Administrator Access to TeamWorks Data

The TeamWorks administrator can see all rooms, topics and comments:

This includes file attachments as well.

Limiting Physical Access to TeamWorks Servers

Servers where Micro Focus TeamWorks data resides should be kept physically secure so that unauthorized persons cannot gain access to the server consoles.

Protecting the TeamWorks Database

Depending on your local security guidelines, you might want to encrypt the database connections between the TeamWorks software and the TeamWorks database. SSL-encrypted data between the TeamWorks application and the database server imposes a performance penalty because of the increased overhead of encrypting and decrypting the retrieved data.

Support for this is highly dependent on the database client drivers and JDBC connector support, and on how you are configuring your database client and server certificates. You should check with your database vendor on how to set up SSL connections on both the client and server sides of the connection. You might need to modify the JDBC URL on an all-in-one TeamWorks deployment. For example, for PostgreSQL, you might add `useSSL=true&requireSSL=true` to the `options` part of the JDBC URL.

TeamWorks Security Defaults

- Client access is only allowed through REST over SSL (HTTPS), using unique self-signed certificates for each instance.
- By default, user provisioning is done via LDAP over SSL (LDAPS).
- TeamWorks supports replacing self-signed certificates with certificates that have been signed by a trusted certificate authority (CA).
- All security-related credentials and passwords are encrypted with unique 2048-bit keys.
- Communication between virtual machines is authenticated and encrypted.

TeamWorks Site Security

Configuring a Proxy Server

Your Micro Focus TeamWorks system should be located behind your firewall. If TeamWorks users want to access the TeamWorks site from outside your firewall, you should set up a proxy server outside your firewall to provide access.

Setting the TeamWorks Port 8443 Administrator Password

The TeamWorks site is initially installed to allow administrator access by using the user name `admin` and the password `admin`. You are prompted to change the TeamWorks administrator password the first time you log in to the Port 8443 TeamWorks Administration Console. Thereafter, you can change the password as described in “Modifying Port 8443 Administrator Accounts” on page 11.

XSS—TeamWorks Is Secure

Cross-site scripting (XSS) is a client-side computer attack that is aimed at web applications. Because XSS attacks can pose a major security threat, Micro Focus TeamWorks contains a built-in security filter that protects against XSS vulnerabilities. This security filter is enabled by default.

What Content Is Not Permitted

By default, the XSS security filter in TeamWorks is very strict, and does not allow users to add certain types of content. For example, the following content is not permitted:

- HTML that contains JavaScript
- Forms
- Frames
- Objects
- Applets

Where the Content Is Not Permitted

The type of content discussed in “What Content Is Not Permitted” on page 32 is filtered by TeamWorks in the following areas:

- Text and HTML fields in comments
- Uploaded HTML files

LDAP Synchronization Security

If your LDAP directory service requires a secure LDAP connection (LDAPS), you must configure Micro Focus TeamWorks with a root certificate. The root certificate identifies the root certificate authority (CA) for your TeamWorks site, which enables you to export a self-signed root certificate based on your eDirectory or Active Directory tree.

Exporting a Root Certificate

Exporting a Root Certificate for eDirectory

1. Launch and log in to iManager for your tree.
2. Click **Directory Administration**.
3. Click **Modify Object**.
4. Click the magnifying glass icon to browse to and select the "*Tree Name* CA" object in the Security container of the eDirectory tree.
5. Click **OK**.
6. Click the **Certificates** tab.
7. Select the check box for the root certificate (this is not the certificate titled **Self Signed Certificate**, but rather the root certificate), then click **Validate**.
8. Select the check box for the root certificate, then click **Export**.
9. Deselect **Export private key**, then click **Next**.
10. Click **Save the exported certificate**, then select **File in binary DER format**.
11. Save the file to a location where it can be accessed later and with a file name that you can remember, such as `SelfSignCert.der`.
12. Click **Close** > **OK**.
13. Continue with "Importing the Root Certificate into the Java Keystore" on page 34.

Exporting the Root Certificate for Active Directory

1. On the Windows server, click **Start > Run**, then enter `mmc`.
2. In MMC, type `Ctrl+M`.
3. If the **Internet Information Services (IIS) Manager** snap-in is not installed on your Windows server, install it.
4. With IIS selected, click **Add**, then click **OK**.
5. In the left frame, click **Internet Information Services**, then click a Windows server that TeamWorks can connect to for synchronizing users.
6. In the Filter list, scroll down to **Server Certificates** and double-click the icon.
7. In the **Actions** list, click **Create Self-Signed Certificate**.

8 Name the certificate with a name you can remember, such as the server name, then click **OK**.

9 Type Ctrl+M, select the **Certificates** plug-in, then click **Add**.

10 Select **Computer account**, then click **Next**.

11 Click **Finish**.

12 In the Snap-ins dialog, click **OK**.

13 In MMC, expand the **Certificates** plug-in, expand **Personal**, then click **Certificates**.

14 Right-click the certificate you created, select **All Tasks**, then click **Export...**.

15 In the Certificate Export wizard, click **Next**.

16 Ensure that **No, do not export the private key** is selected, then click **Next**.

17 Ensure that **DER encoded binary** is selected, then click **Next**.

18 Name the certificate, then click **Next**.

19 Click **Finish > OK**.

The certificate is saved in `C:\Users\Your-User-Name`.

20 Ensure that the certificate is accessible from your management browser.

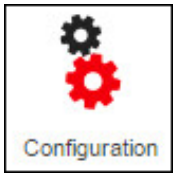
21 Continue with "Importing the Root Certificate into the Java Keystore" on page 34.

Importing the Root Certificate into the Java Keystore

1 Navigate to the management console of your Micro Focus Appliance:

`https://ip_address:9443`

2 Click the **Appliance System Configuration** icon.



The Micro Focus Appliance Configuration page is displayed.

3 Click **Digital Certificates**.

4 In the **Key Store** drop-down list, select **JVM Certificates**.

5 Click **File** > **Import** > **Trusted Certificate**.

A `.der` certificate is required for the import to be successful.

6 Browse to and select the trusted root certificate that you want to import.

If you want to import multiple certificates, ensure that the certificate names are different for each certificate.

7 Do not make any changes to the **Alias** field. It is populated by default.

8 Click **OK**.

The certificate should now be displayed in the list of JVM certificates.

9 Restart TeamWorks so that Tomcat rereads the updated Java keystore file.

You can restart the TeamWorks service as described in "Shutting Down and Restarting the Micro Focus Appliance" in the *TeamWorks 18.2.1: Administrative UI Reference*.

You are now ready to configure your TeamWorks site for secure LDAP synchronization, as described in see “LDAP Servers and Synchronization” in the *TeamWorks 18.2.1: Administrative UI Reference*.

NESSUS Scans

The TeamWorks development team runs NESSUS scans on all TeamWorks code and fixes all reported problems.

This means that no unexpected ports are open and all open ports are protected according to industry standards.

Proxy User Security

- TeamWorks uses administrator-created proxy users for communicating with LDAP providers.
- LDAP proxy users must have sufficient rights to read user and group objects from the desired contexts within LDAP providers.
- Proxy users’ identities and credentials are secured, encrypted, and protected in TeamWorks.

Security Scan Risk Reports

Running regular security scans on your network is critical to security administration. Security is a top priority for the TeamWorks development team.

Occasionally, reputable security scanning software reports risks that the TeamWorks team considers to be less significant than reported. The following are specific examples:

- **PHP as a Security Vulnerability:** Although in many cases the presence of PHP scripts is a legitimate concern, in the case of TeamWorks, there is no PHP access without first authenticating through port 9443. Since access through port 9443 is secure by definition, TeamWorks’s PHP implementation is secure.
- **Diffie-Hellman 1024 Keys:** If you run a Nessus or equivalent security scan, you might receive a report of “Medium Risk” associated with Diffie-Hellman 1024-bit keys.

  The TeamWorks team is aware of this and is considering increasing the key size in a future release. At this time, however, the team does not feel that this is a significant threat to TeamWorks installations; breaking 1024-bit keys requires computing resources that only a nation-state would have at its disposal.

  If you are concerned or feel that your organization might be vulnerable to nation-state attacks, you can specify a stronger key through the Java security policy.

SSH Access for the Root User

By default, the root user is able to SSH to each appliance in the TeamWorks system. When logged in as `root`, you can disable this access on each appliance so that only the vaadmin user can SSH to the system.

See “Changing Passwords and SSH Access for vaadmin and root” in the *TeamWorks 18.2.1: Administrative UI Reference*.

Universal Passwords (eDirectory) Security

If you use Universal Passwords and if eDirectory LDAP is not NMAS-aware, users are able to log in to TeamWorks with case-insensitive passwords even though the passwords are actually case sensitive. For example, they can log in with 'p@$wrd1!' when their password is 'P@$Wrd1!'

In addition to the security concern, when users log in with the incorrect case, they cannot upload any files.

To prevent users from logging in to TeamWorks with an incorrect password, set eDirectory LDAP to be NMAS-aware by following the instructions in this TID (https://www.novell.com/support/kb/doc.php?id=3307424).

Users and Security

- TeamWorks supports authentication using IDs and credentials that are validated with the LDAP identity source from which they were provisioned. The credentials from these LDAP providers are cached within TeamWorks, but they are never really synchronized from the LDAP provider.
- Local users that are not provisioned via LDAP have their local credentials stored in TeamWorks. These credentials are secured, encrypted, and protected.

XSS Security Filter

Cross-site scripting (XSS) is a client-side computer attack that is aimed at Web applications. Because XSS attacks can pose a major security threat, Micro Focus TeamWorks contains a built-in security filter that protects against XSS vulnerabilities.

The XSS security filter protects the TeamWorks site from XSS in two key areas:

- Text and HTML fields in entries and folders
- Uploaded HTML files

10 Shutting Down and Restarting TeamWorks Appliances

If you need to shut down and restart TeamWorks appliances, make sure to follow the guidelines and instructions in this section.

Use the Shutdown Button in the Appliance's Port 9443 Console

When you need to shut down a Micro Focus appliance, always use the Shutdown button to ensure that appliance processes are properly terminated.

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

Limit Shutdowns to One Appliance at a Time

As a best practice, you should try to only take one appliance out of service (shut it down) at a time. This not only prevents service interruption, but it also helps keep TeamWorks services in a healthy state.

For example, if you need to increase the memory assigned to each appliance, shut one appliance down, increase the memory, start the appliance back up, and then perform the same process with the next appliance.

Disable User Access Before Shutting Down TeamWorks Services

If you are shutting down multiple appliances and taking TeamWorks services offline, make sure to disable user access to TeamWorks before beginning the process.

NOTE: If you are shutting down only one appliance at a time for maintenance or other purposes, TeamWorks services should not be disrupted, so disabling user access is not required.

Shutdown Order Is Critical

Make sure to shut down the appliances in the following order:

1. **TeamWorks First:** Shut down the TeamWorks Appliances first.

   Order is not important for the TeamWorks appliances, but make sure they are all shut down before moving to the Search appliances.

2. **Search Second:** Shut down the Search appliances next and *make a record of the shutdown order*.

   WARNING: The Messaging services that run on the Search appliances require that the last service node to be shut down is the first service node to be started back up. Otherwise, the messaging service fails to restart and must be repaired.

3. **PostgreSQL Last:** Shut down the PostgreSQL appliance last.

Startup Order Is Also Critical

Make sure to start up the appliances in reverse shutdown order:

1. **PostgreSQL First:** Start up the PostgreSQL appliance first.

   Make sure that database services are running before starting the Search appliances.

2. **Search Second:** Referring to the shutdown-order record created in Step 2 on page 38, start up the last Search appliance that you shut down.

   2a If Messaging services were previously enabled on the first Search appliance that you restart, verify that the RabbitMQ service is running in **Port 9443 Console > System Services icon** > the list of appliance system services.

   If RabbitMQ should be running but is not, follow the instructions in “Fixing a Messaging Service That Won’t Start” on page 38.

   2b If Messaging services were not previously enabled on the first Search appliance that you restarted, best practices dictate that they must have been enabled on the second appliance. Therefore, follow the instructions in Step 2a on the second Search appliance that you start up.

   If Messaging services were enabled on the first Search appliance that you restarted and you have verified that RabbitMQ is running on it, then start up the second and third Search appliances.

3. **TeamWorks Last:** Start all of the TeamWorks appliances.

   The order doesn’t matter.

Fixing a Messaging Service That Won’t Start

IMPORTANT: The following procedures assume that you know which two of your three Search appliances were configured to provide Messaging services.

Referring to Table 10-1, find the cause of the Messaging service failure and complete the steps shown.

Table 10-1 *Fixing a Messaging Service That Won't Start*

Cause of Failure	Steps to Resolve

Power failure on both Messaging services nodes or other simultaneous shut down.
 	
When this happens, both Search appliances running Messaging services are set as the first node that shut down, meaning that neither Messaging service can start until the other is running.
	1. Make sure to start the database server or PostgreSQL appliance first.
	2. When the database is running, start one of the Search appliances that is registered to run Messaging services. It doesn't matter which of the two appliances you start first since they shut down at the same time.
	3. Access the appliance's console and log in as the `root` user.
	4. Set the messaging service to start without timing out by entering the following command:
	`rabbitmqctl force_boot`
	5. Start the messaging service by entering the following command:
	`systemctl start esn-rabbitmq-server`
	6. Enter `exit` to log out as `root`.
	7. Start the other Search appliances and then the TeamWorks appliances as outlined in "Startup Order Is Also Critical" on page 38.

You start the wrong Messaging node (Search appliance) first and when you check the RabbitMQ status as directed in Step 2 on page 38, service status is **Stopped**.	1. Click **Home**, then click the Configuration icon.
	2. On the Configuration Summary page, under **Messaging Service**, check to verify which two appliances are registered to run Messaging Services.
	The appliance currently running should be listed. The other appliance listed should be the last one shut down, and therefore the first one to start up.
	3. Click **Home > Shutdown**.
	4. When the Search appliance is completely shut down, start the other Search appliance that has Messaging services enabled.
	5. Check the RabbitMQ service status.
	If the status is **Running**, exit the Port 9443 console and continue wth appliance startup as outlined in "Startup Order Is Also Critical" on page 38.
	If the status is **Stopped**, do the following:
	a. Access the appliance's console and log in as the `root` user.
	b. Set the messaging service to start without timing out by entering the following command:
	`rabbitmqctl force_boot`
	c. Start the messaging service by entering the following command:
	`systemctl start esn-rabbitmq-server`
	d. Enter `exit` to log out as `root`.
	6. Continue with appliance startup as outlined in "Startup Order Is Also Critical" on page 38.

Cause of Failure	Steps to Resolve
You delete, recycle, etc. one of the Search appliances that was registered to run Messaging services and was not properly decommissioned. This causes the “Messaging cluster” configuration to become invalid and creates system problems. **NOTE:** The primary assumption here is that the deleted Search appliance was also the “last down” and this fact is preventing Messaging services from starting. However, the same steps should be completed if the “first down” Messaging node is deleted. This is because that would also cause the cluster configuration to become invalid and create system problems.	Repair the “Messaging cluster” configuration by removing the node that no longer exists. 1. Access the console of the remaining appliance that is registered to run Messaging services and log in as the `root` user. 2. Remove the appliance that no longer exists from the Messaging cluster by entering the following command: `rabbitmqctl forget_cluster_node -offline rabbit@`*`short_hostname_deleted_node`* Where **short_hostname_deleted_node** is the hostname of the appliance that was deleted but not decommissioned, for example `tw-search-2`. 3. Start the messaging service by entering the following command: `systemctl start esn-rabbitmq-server` 4. Enter `exit` to log out as `root`. 5. Make sure that you restore the TeamWorks deployment to best practice status as soon as possible. In other words, run three Search Appliances, two of which are running Messaging services.

11 Storage Management

Expanding the /var Partition

The Storage Expansion Option in the Port 9443 Appliance Console must temporarily unmount the disk target in order to complete a disk expansion. However, because the `/var` partition contains the system log volume, it is constantly being written to and cannot be unmounted while the system is running.

Therefore, expanding the /var partition requires a manual process, as follows:

1. Shut down the appliance and use the VMware management tools to increase the size of Disk 3. For example, edit the disk size in Settings and save the changes.
2. Start the appliance.
3. Using your management browser, access the Port 9443 Appliance Console > **Storage** icon.
4. Select the `/var` partition and click **Expand Partitions**.
5. At the appliance’s terminal prompt, log in as `root`.
6. Edit `/etc/fstab`, remove the line: `/dev/sdc1 /var ext3 rw 0 0` and save the change.
7. Shut down the appliance.
8. Start the appliance in failsafe mode by using the down arrow on the boot screen.
9. At the appliance’s terminal prompt, log in as `root`.
10. Edit `/etc/fstab` and insert the line: `/dev/sdc1 /var ext3 rw 0 0`, then save the change.
11. Enter the following command:

    ```
    /opt/novell/base_config/va_expand_partition
    ```
12. Restart the appliance.

    The appliance is now using the expanded `/var` partition.

Optimizing Disk Performance

Micro Focus recognizes that many pilot deployments and demo systems are deployed on VMware Workstation.

Therefore, since VMware Workstation only supports LSI Logic as the SCSI disk controller type, that setting is specified in the OVF files used to deploy all TeamWorks-related appliances.

On the other hand, VMware strongly recommends **VMware Paravirtual** as the SCSI disk controller type in all high-data-load installations.

For this reason, the installation instructions in "Edit settings" in the *GroupWise TeamWorks 18.2.1: Installation and Deployment Guide*, recommend changing the controller type to **VMware Paravirtual** during initial appliance configuration in ESX and ESXi environments.

If you didn't make this change during the initial deployment, you can change the controller type later by doing the following:

1. Power off the appliance you are changing.
2. Edit the appliance settings and change the **SCSI Disk Controller** type to **VMware Paravirtual**.
3. Power on the appliance and move to the next appliance you are configuring.

Backing Up TeamWorks Data

Reliable backups are critical to the stability of your Micro Focus TeamWorks site.

IMPORTANT: Do not use VMware snapshots as a backup method for TeamWorks. Doing so creates problems when managing the system disk and inhibits your ability to update TeamWorks in the future.

Locating TeamWorks Data to Back Up

In order to keep adequate backups of your Micro Focus TeamWorks data, you must back up the following types of data:

TeamWorks File Repository (/vastorage)

Back up the following location on the TeamWorks appliance. In a multiple-appliance deployment, back up this location on each TeamWorks appliance in the cluster.

```
/vastorage/esn/filerepository
```

TeamWorks Database

Back up the following location on the TeamWorks appliance (in an all-in-one deployment) or on the PostgreSQL database appliance (in a multiple-appliance deployment):

```
/vastorage/postgres
```

Specifically, you should back up the following databases: `TeamWorks`, `information_schema`, `PostgreSQL`

Refer to the Backup and Restore (https://www.postgresql.org/docs/9.6/static/backup.html) in the PostgreSQL documentation.

Search Index

You can back up the following location on the TeamWorks appliance (in an all-in-one deployment) or the Search index appliance (in a multiple-appliance deployment):

`/vastorage/conf`

The Search index does not need to be backed up because it can be rebuilt at any time.

Certificates

Back up the following location on the TeamWorks appliance. In a multiple-appliance deployment, back up this location on each TeamWorks appliance.

`/vastorage/conf/certs`

Scheduling and Performing Backups

You do not need to bring your Micro Focus TeamWorks site down in order to perform backups. You might want to back up the TeamWorks file repository and the TeamWorks database every night, perhaps doing a full backup once a week and incremental backups on other days. You can back up the Elasticsearch index whenever it is convenient. You can always reindex the TeamWorks site in order to re-create the Elasticsearch index, but being able to restore content from a backup can save time in case of an outage.

Restoring TeamWorks Data from Backup

If you need to restore your Micro Focus TeamWorks site from a backup, restoring the same backup version for both the file repository and the database creates a TeamWorks site that is consistent within itself but might be missing information that was added after the backups were created. If you lose the file repository but not the database, you can restore the backed-up file repository and keep the more current database, but some files are likely to be missing from the file repository.

Disk Usage Checks

Each hour, TeamWorks checks the amount of disk space that is being used on the system drive for a given appliance. If disk usage reaches 90% capacity or greater on the system drive for any appliance, the TeamWorks services are stopped.

Following are the scripts that are used to monitor disk usage for each type of appliance:

- **TeamWorks Appliance:** `/etc/cron.hourly/esn-diskcheck.sh`
- **Search Index Appliance:** `/etc/cron.hourly/lucene-diskcheck.sh`
- **Database Appliance:** `/etc/cron.hourly/postgresql-diskcheck.sh`

When the TeamWorks services are stopped because of low disk space, a message is logged to both the `/var/opt/novell/va_status` and `/var/log/messages` files.

After the services are stopped, you must clean up unneeded data or add additional disk space to the appliance before restarting the services.

12 Troubleshooting

eDirectory Users Can Log In But Cannot Upload Files

See ““Universal Passwords (eDirectory) Security” on page 36.”

Online Update Service Registration Fails With An Error Message

Problem: While registering the online update service, if you do not specify a value for the **Namespace** path when staging is enabled on the SMT server, the registration fails with a `"An error occurred while communicating with the server"` message. On refreshing the page, the update service registration with the SMT server message is displayed on the page. However, no patches are displayed on the page even if they are available. Clicking the **Deregister** option in the Registration Status dialog fails to deregister the online update service.

To correctly register the online update service, perform the following steps:

1. In the SSH terminal, run the following command to deregister the existing incorrect registration:

   ```
   zypper rs SMT-http_<HOSTNAME_OF_SMT_SERVER>
   ```

2. Log in to the TeamWorks Appliance Console and register the online update service again.

Unable to Connect to the TeamWorks Site (HTTP 500 Error)

Problem: Trying to connect to TeamWorks yields an HTTP 500 error.

To fix this problem, ensure that your DNS server is properly configured and that your TeamWorks server is directed at the proper DNS server.

For information about how to configure TeamWorks to point to your DNS server, see “Changing Network Settings” in the *TeamWorks 18.2.1: Administrative UI Reference*.

Using VACONFIG to Modify Network Information

The easiest way to update the configuration information for the appliance (such as the IP address, host name, and so forth) after TeamWorks is already installed, is to use the VACONFIG utility from the appliance command prompt:

1. In the vSphere client, select the TeamWorks appliance, then click the **Console** tab.
2. From the command prompt, log in to the appliance.
3. Type `vaconfig`, then press Enter.
4. In the VACONFIG utility, select **Configure**, then press Enter.
5. Press the Tab key until the IP address is selected, then modify the IP address as desired.
6. Select **Next**, then press Enter.

13 User and Group Maintenance

User accounts change over time and need periodic maintenance.

Adding and Creating TeamWorks Users and Groups

You can add new users to your TeamWorks site in any of the following ways:

- **LDAP:** Synchronize newly-added users from an LDAP directory, as described in “LDAP Servers and Synchronization” in the *TeamWorks 18.2.1: Administrative UI Reference*.
- **Local:** Add local users and groups, as described in Managing Users and Managing Groups in the TeamWorks 18.2.1: Administrative UI Reference.
- **Profile Files:** Import XML profile files to add and manage local users and groups, as described in “Import Profiles... button” in the *TeamWorks 18.2.1: Administrative UI Reference*.

Creating Groups of Users

This section describes how to create groups within TeamWorks. You can also synchronize groups of users from your LDAP directory to your Micro Focus TeamWorks site, as described in “LDAP Servers and Synchronization” in the *TeamWorks 18.2.1: Administrative UI Reference*.

You can create either static or dynamic groups.

Creating Static Groups

Path: Port 8443 TeamWorks Administration Console**Management > Groups > Add > Group Membership Is Static > Edit Group Membership**

For help specifying group membership, see “Static Membership for Group dialog” in the *TeamWorks 18.2.1: Administrative UI Reference*.

Static groups contain only the users and groups that you specifically select as group members.

Static groups exist only in TeamWorks and can contain any users and groups in TeamWorks, including LDAP-synchronized users and groups.

Creating Dynamic Groups

Groups based on LDAP queries are dynamic because they can be configured to have their membership updated when the information in the LDAP directory changes.

Creating groups based on LDAP queries is a quick way to create TeamWorks groups that consist of users who match specific criteria. You can create dynamic groups as described in the following sections:

Creating Dynamic Groups within LDAP

Depending on the LDAP directory that you are using, you might be able to create dynamic groups within your LDAP directory. For example, you can create dynamic group objects in eDirectory with NetIQ iManager (for more information, see the iManager Documentation (https://www.netiq.com/documentation/imanager27/)).

Dynamic groups created within LDAP are stored in your LDAP directory and can then be synchronized to TeamWorks, as described in "LDAP Servers and Synchronization" in the *TeamWorks 18.2.1: Administrative UI Reference*.

Creating Dynamic Groups within TeamWorks

Advantages of TeamWorks Dynamic Groups:

- Allows Port 8443 admins, including Direct administrators, to control group membership without having direct access to the group object in the LDAP user store.
- Provides dynamic group functionality whether or not your LDAP directory supports dynamic groups.
- TeamWorks-based dynamic groups don't synchronize to other applications that are leveraging the same LDAP directory as TeamWorks.

Path: Port 8443 TeamWorks Administration Console**Management > Groups > Add > Group Membership Is Dynamic > Edit Group Membership**

For help specifying group membership, see "Edit Dynamic Membership dialog" in the *TeamWorks 18.2.1: Administrative UI Reference*.

Deleting TeamWorks Users

When users no longer need access to your Micro Focus TeamWorks site, you have two options to revoke their access to the TeamWorks site: disabling or deleting their TeamWorks user accounts.

Consider Disabling User Accounts Instead of Deleting Them

Micro Focus recommends that you disable user accounts rather than deleting them, especially if there is a chance that users might need TeamWorks access in the future.

When you delete a user account, the account can never be re-activated.

For information on how to disable a user, see "Disabling TeamWorks User Accounts" on page 50.

Deleting User Objects and Workspaces

Path: Port 8443 TeamWorks Administration Console > **Management** > **Users** > ***select the users to delete*** > **Delete**

Important Terminology

- **User Object:** This represents the user in the TeamWorks system and contains:
  - The user's profile information, including the profile picture and other information the user has entered.
  - Individually assigned Quotas.

  If you delete a user object, the above information is permanently deleted from TeamWorks and the user can no longer access TeamWorks.
- **User Workspace:** This is a physical location in the TeamWorks system.

  If you move the user workspace to trash, the user account is disabled. In TeamWorks this cannot be undone because user workspaces cannot be recovered from trash.

  If you delete a user's workspace, the TeamWorks-based Storage associated with the users is permanently deleted and cannot be recovered. However, the User Object still exists, and the user still has access to TeamWorks, items shared with the user, comments, and so on.

Deleting an LDAP User

If you delete user accounts that were created by the LDAP synchronization process without following the instructions in this section, new users with the same name are created the next time the users log in or the next time the LDAP synchronization occurs.

User accounts can be synchronized to the TeamWorks site with an LDAP directory. Although you can delete TeamWorks user accounts, Micro Focus recommends that you disable them, as described in "User and Group Maintenance" on page 47.

If you decide to delete TeamWorks user accounts, it is safer to manually delete than to delete them through the LDAP synchronization process. Because user accounts that are deleted cannot be recovered, ensure that you know exactly which users you are deleting; the only way to be sure is to manually delete them.

Manually Deleting User Accounts That Are Being Synchronized through LDAP

The following method is preferred for deleting user accounts from the TeamWorks site if the accounts are being synchronized from an LDAP directory:

1. In your LDAP directory, modify the User objects that you want to delete from the TeamWorks site so that the User objects no longer match the LDAP synchronization criteria that you previously set.

   For information about setting LDAP synchronization criteria, see "LDAP Servers and Synchronization" in the *TeamWorks 18.2.1: Administrative UI Reference*.
2. In TeamWorks, manually delete the user accounts, as described in "Deleting User Objects and Workspaces" on page 49.

Having LDAP Automatically Delete User Accounts Is Not Recommended

---

CAUTION: Micro Focus recommends against having the LDAP synchronization process automatically delete TeamWorks users and workspaces because it might result in unwanted deletion of users!

For example, if the LDAP context is entered incorrectly and none of the users match the incorrect LDAP context, all of the users are permanently deleted.

For more information about configuring LDAP synchronization to automatically delete TeamWorks users and workspaces, see "For user accounts provisioned from LDAP that are no longer in LDAP sub-section" in the *TeamWorks 18.2.1: Administrative UI Reference*.

Disabling TeamWorks User Accounts

Path: Port 8443 TeamWorks Administration Console

Micro Focus recommends that you disable user accounts instead of deleting them. When you delete a user account, the account can never be re-activated. If there is the slightest possibility that the user might return to your TeamWorks site, disable the user account rather than deleting it.

Disabled accounts do not count as a licensed user.

The way to disable a user account differs depending on whether the user was created in TeamWorks or in an LDAP directory and then synchronized to TeamWorks.

Disabling or Re-enabling a Local User Account

Path: Port 8443 TeamWorks Administration Console**Management > Users > *select user accounts* > More > Disable or Enable**

Disabling an LDAP User Account

If users are being synchronized from an LDAP directory, you must disable the accounts directly from the LDAP directory. User accounts that are disabled in the LDAP directory are disabled in TeamWorks at the next LDAP synchronization.

For more information about LDAP synchronization in TeamWorks, see "LDAP Servers and Synchronization" in the *TeamWorks 18.2.1: Administrative UI Reference*.

Renaming a TeamWorks User

Micro Focus TeamWorks users are identified by

- **User Names:** Identify personal profiles—can be changed.
- **User IDs:** Used for logging in—cannot be changed.

The way you change a user's name depends on how the user was created.

Renaming a TeamWorks User from LDAP

1. In the LDAP directory, change the user's first, middle, and/or last name.

   The name changes with the next LDAP synchronization.

Renaming a Local TeamWorks User

Path: Port 8443 TeamWorks Administration Console **> Management > Users >** ***select a user name*** **>** **Profile >** ***Change the First Name and/or Last Name***