

MotionWorks Enterprise

RFID Reader Management



ZEBRA

Installation Guide

2023/06/15

ZEBRA and the stylized Zebra head are trademarks of Zebra Technologies Corporation, registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners. ©2023 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements.

For further information regarding legal and proprietary statements, please go to:

SOFTWARE: zebra.com/linkoslegal.

COPYRIGHTS: zebra.com/copyright.

PATENTS: ip.zebra.com.

WARRANTY: zebra.com/warranty.

END USER LICENSE AGREEMENT: zebra.com/eula.

Terms of Use

Proprietary Statement

This manual contains proprietary information of Zebra Technologies Corporation and its subsidiaries ("Zebra Technologies"). It is intended solely for the information and use of parties operating and maintaining the equipment described herein. Such proprietary information may not be used, reproduced, or disclosed to any other parties for any other purpose without the express, written permission of Zebra Technologies.

Product Improvements

Continuous improvement of products is a policy of Zebra Technologies. All specifications and designs are subject to change without notice.

Liability Disclaimer

Zebra Technologies takes steps to ensure that its published Engineering specifications and manuals are correct; however, errors do occur. Zebra Technologies reserves the right to correct any such errors and disclaims liability resulting therefrom.

Limitation of Liability

In no event shall Zebra Technologies or anyone else involved in the creation, production, or delivery of the accompanying product (including hardware and software) be liable for any damages whatsoever (including, without limitation, consequential damages including loss of business profits, business interruption, or loss of business information) arising out of the use of, the results of use of, or inability to use such product, even if Zebra Technologies has been advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Contents

About this Guide.....	4
Installing the Software.....	5
Accessing the Zebra Artifactory.....	5
Creating a Zebra Account.....	5
Creating an Identity Token.....	9
Verify System Requirements.....	12
Installing the Operating System.....	13
Installing the Reader Management Software.....	13
Preparing Reader Management Files.....	13
Running the Reader Management Script—Online Installation.....	13
Running the Reader Management Script—Offline Installation.....	15
Starting Reader Management.....	16
Validating the Reader Management Installation.....	16
Reader Management User Interface.....	17
Installing the Prerequisite Software.....	18
Docker.....	18
Utility Software.....	18
Configuring the Server.....	19
System Validation.....	21
Configuring Authentication Type.....	22
Upgrading the Software.....	26
Upgrading the Software Online.....	26
Upgrading the Software Offline.....	27

About this Guide

This guide provides information about preparing for and installing MotionWorks Enterprise (MWE) RFID Reader Management (RM) software.

To use the Reader Management software, you must:

1. Verify System Requirements—the installation includes a process that verifies the server meets the system requirements.
2. Install the Operating System with the specified partitions/volumes.
3. Install the Prerequisite Software as reported by the self-check tool.
4. Install Reader Management Software.

Installing the Software

This section describes how to install the MotionWorks Enterprise RFID Reader Management software.

Accessing the Zebra Artifactory

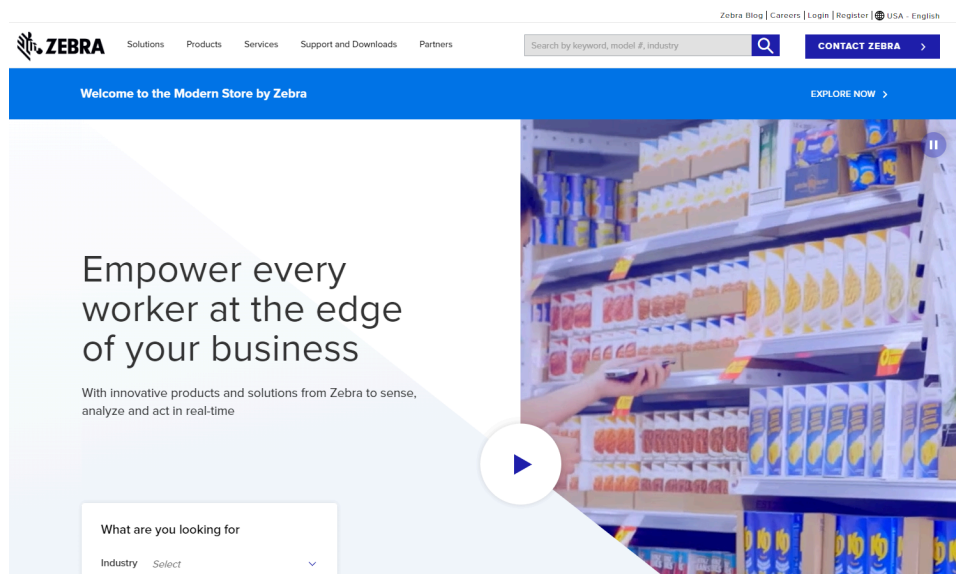
This section describes how to generate an Identity Token to log into the Zebra Artifactory, and how to download the MotionWorks Enterprise RFID Reader Management software package.

A Zebra SSO Account is required to access the artifactory.

An identity token is required to install MotionWorks Enterprise RFID Reader Management Software online package.

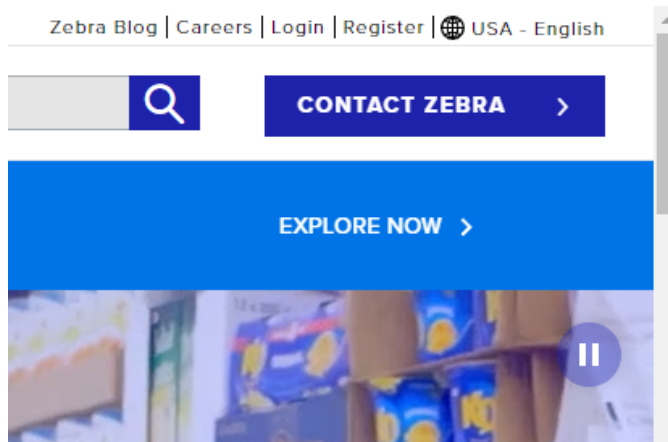
Creating a Zebra Account

1. Go to www.zebra.com.



Installing the Software

2. In the top right of the home page, click **Register**.



3. In the **Email** field, enter a valid email address.
4. Click **NEXT**.

A screenshot of the 'Zebra.com Account Registration' page. At the top, there's a navigation bar with the Zebra logo, links for 'Solutions', 'Products', 'Services', 'Support and Downloads', and 'Partners', a search bar, and a 'CONTACT ZEBRA' button. Below this is a progress indicator with four steps: 1. Enter User Email Address (active), 2. Verify User Email Address, 3. Enter User Information, and 4. Enter Application Information. The main content area is titled 'Register with email:' and features an 'Email' field with the placeholder text 'john.doe@gmail.com'. Below the field, it states 'Your email address will be your User ID'. There are two buttons: 'NEXT' (highlighted in blue) and 'CANCEL'. The footer is a dark grey bar containing the Zebra logo with the tagline 'CAPTURE YOUR EDGE', a list of links categorized under 'About Zebra', 'Discover', 'Support Resources', and 'Connect with our team', and a 'Register Now' button. Social media icons for LinkedIn, Twitter, Facebook, and YouTube are also present.

Installing the Software

5. A verification code is sent to the email address.



This e-mail has been sent in response to your request to create a user account. To complete this process, please use the below Verification Code

2UR8TP

Please note that this link will expire 10 minutes after it has been sent.

Best regards,
Zebra Technologies

Please note: This e-mail was sent from an auto-notification system that cannot accept incoming e-mail. Please do not reply to this message.

ZEBRA COMMUNICATIONS

6. In the **Enter Verification Code** field, enter the code from the email.

7. Click **SUBMIT**.

Zebra.com Email Verification

1 Enter User Email Address * 2 Verify User Email Address * 3 Enter User Information * 4 Enter Application Information *

Your request has been received. We have sent a verification code through your email to verify your account. Please enter your verification code below to finish registration. Can't find your email? Please check your junk mail or click this link: [Resend Verification Code](#).

Enter Verification Code *

2UR8TP

SUBMIT CANCEL

[Return to Previous Step](#)

ZEBRA CAPTURE YOUR EDGE

About Zebra
Careers
Events
Story Hub/Newsroom
Investors
Corporate Social Responsibility
Global Locations

Discover
Solutions
Products
Services
Success Stories
Resource Library

Connect with our team

Support Resources
Support and Downloads
Contact Support
Request a Repair
Product Warranty Information
Developer Portal
Report a Potential Security Vulnerability or Concern

Contact Zebra Find A Partner

Stay up to date with Zebra.
Sign up for our newsletter.

Register Now

Manage Contact Preferences

in t f y d

Privacy Policy

8. Enter the required information, and accept the terms and conditions.

Installing the Software

9. Click **SUBMIT AND CONTINUE**.

Zebra Blog | Careers | Login | Register | USA - ENGLISH

ZEBRA Solutions Products Services Support and Downloads Partners

Search by keyword

[CONTACT ZEBRA](#)

✓ Email verified successfully!

Zebra.com User Information and Account Security

1 Enter User Email Address * 2 Verify User Email Address * 3 Enter User Information * 4 Enter Application Information *

First Name *

Last Name *

Password *

Confirm Password *

Select Country *

*Mandatory fields

☒ I have read and agree to the [Terms and Conditions](#) *

[Privacy](#) [Terms](#)

You are returned to the home page.

Zebra Blog | Careers | | USA - English

ZEBRA Solutions Products Services Support and Downloads Partners

Search by keyword, model #, industry

[CONTACT ZEBRA](#)

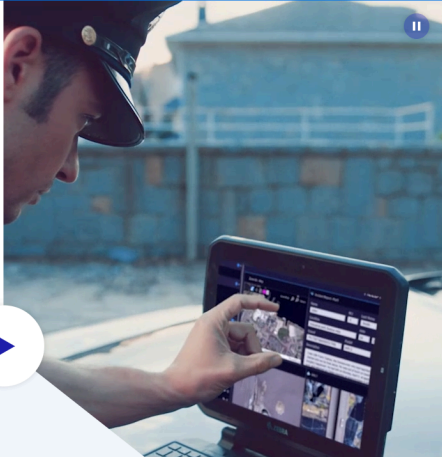
Welcome to the Modern Store by Zebra [EXPLORE NOW](#)

Empower every worker at the edge of your business

With innovative products and solutions from Zebra to sense, analyze and act in real-time

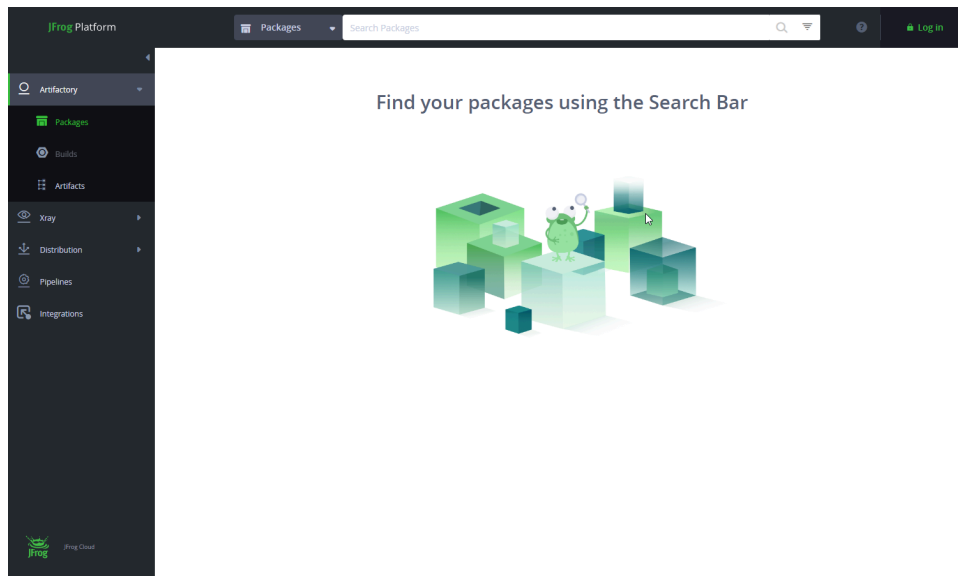
What are you looking for

Industry



Creating an Identity Token

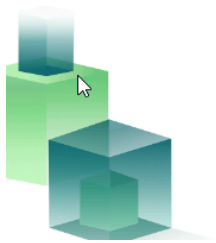
1. Go to zebratech.jfrog.io.



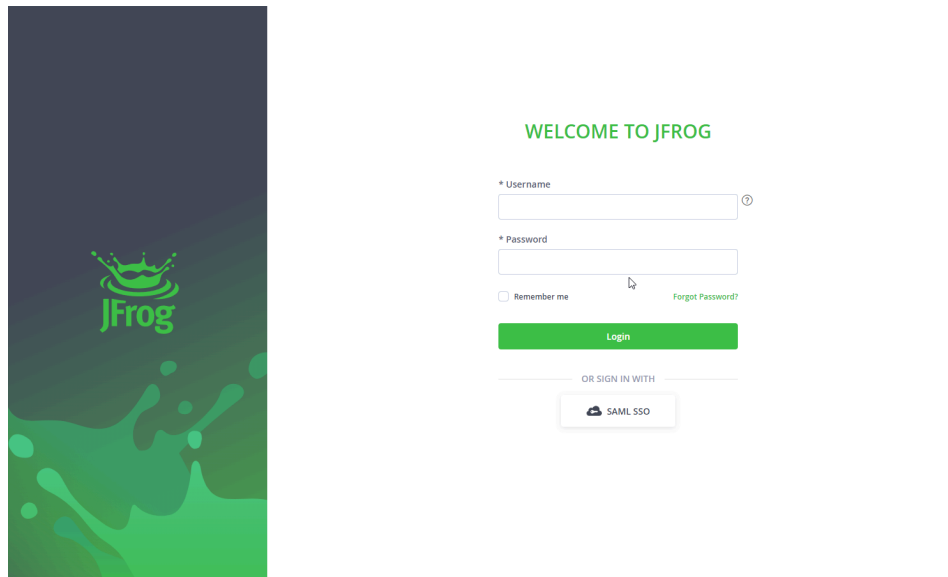
2. Click **Log In**.



the Search Bar

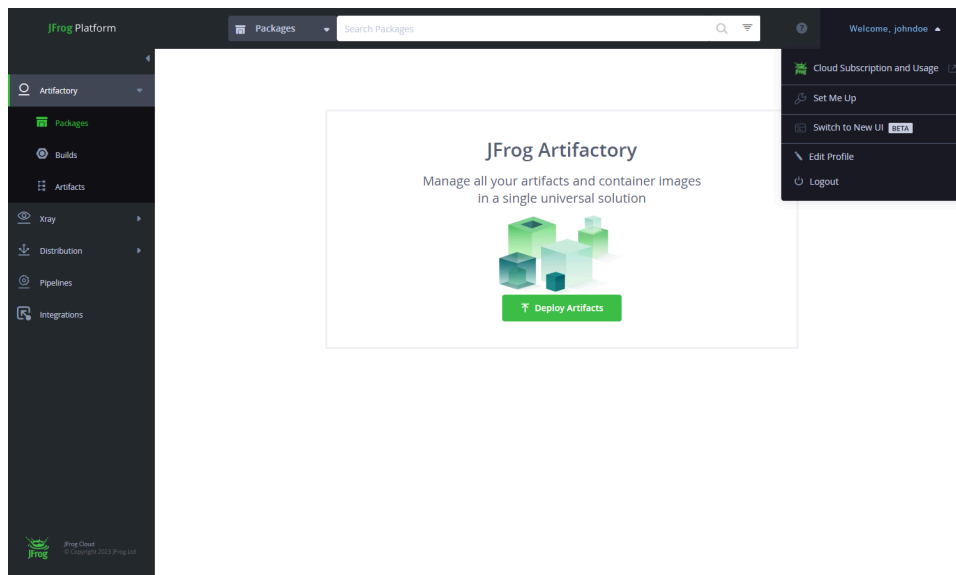


3. Click **SAML SSO**.

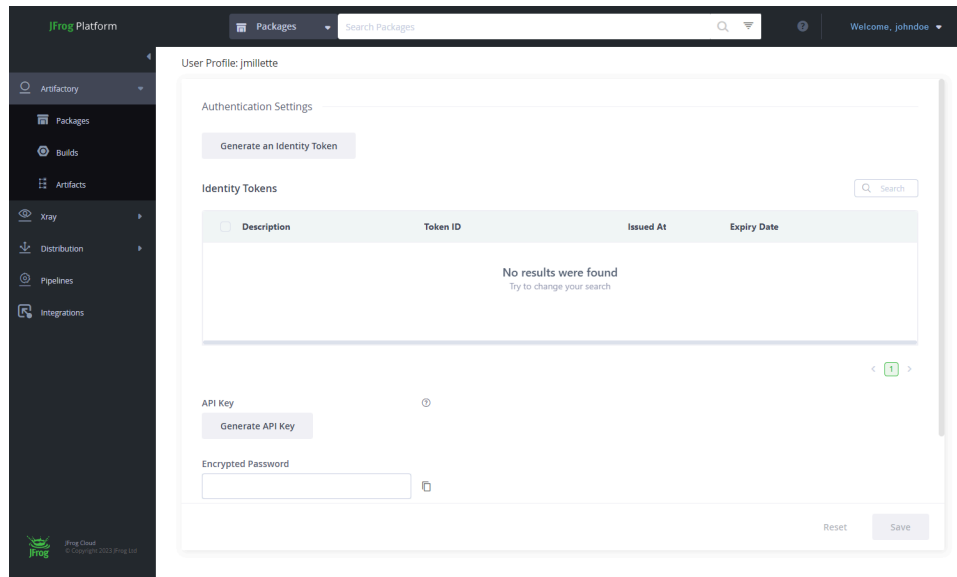


You are logged into the Zebra Artifactory.

4. Click the **Welcome, [user name]** drop-down menu, and then select **Edit Profile**.



5. Click **Generate an Identity Token**.




6. In the **Add Description** field, enter a description for the token.

7. Click **Next**.

Generate An Identity Token
×

Add Description

Zebra Artifactory Token


This will help you identify and manage the token. Example description "My Maven Client Token"

Cancel
Next

The information for the identity token is displayed.

Generate Identity Token
×

Username
johndoe


Scope
applied-permissions/user


Audience
@

Expires In
11 month(s) 30 day(s)


Token ID
7542391a-1c92-4d50-a78d-cf89b2b2766c

Reference Token

cmVmdGtuOjAxOjE3MTMwNTc5NTk6OW9QaE9RcERGN1FGY2FEOVIC...


 Important: Tokens generated here are not stored in the JFrog Platform for security reasons; therefore, make sure you copy the token before closing this window. Once closed the token will not be available.

Close
Copy

8. Click **Copy** at the bottom of the window, or click  next to the **Reference Token** to copy the Reference Token text to the clipboard. You can then paste it into a document for reference.

Verify System Requirements

MWE RFID Reader Management can be installed on a physical or virtual machine. In either case, the operating system must be dedicated to only MWE RFID Reader Management.

The table details the minimum system requirements for MWE RFID Reader Management. Verify the server meets or exceeds these requirements before proceeding.

VM	Mem	vCPU	OS Disk	Data Storage
MWE RFID Reader Management	32GB	Quad core CPU @ 2.4 GHz (or equivalent)	100GB or more	512GB



NOTE: If the server is to be used only for Reader Management, 16GB of memory is sufficient. The customer may have additional requirements for the server that are not specific to MWE RFID

Reader Management. If the customer has security software installed, some requirements may be adjusted for use with MWE RFID Reader Management.

Installing the Operating System

- Install one of the following operating systems with the latest updates:
 - CentOS 7.2009
 - RedHat Enterprise Linux 7.9

Table 1 Recommended Disk and Partition/Volume Sizes

Name	Partition/Volume	Size (GB)	Device Type	Volume Group	File System
sdbxx	/data	500	Logical Volume Manager (LVM)	centos	xfs



NOTE: The operating system partition can be system generated or per IT policies. The total disk size is rounded up to the nearest whole number. You can use standard partitions instead of LVMs. Larger disks and partitions are acceptable.

Installing the Reader Management Software

This section describes how to install the Reader Management software.

1. Download and extract the installation tarball files.
2. Run the set-up script with the `--setup` option.
3. Run the Reader Management install with the `--install` option.
4. Validate the installation.

Preparing Reader Management Files

1. Obtain the installation file from Zebra:
 - a) `trifecta-containers-setup-1.0.1.xx.tar.gz` (For online installation)
 - b) `trifecta-containers-setup-1.0.1.xx-offline.tar.gz` (For offline installation)
2. Copy this file to the Server: `/root/`

Running the Reader Management Script—Online Installation

1. Log in to the Trifecta VM as root or a user with sudo privileges.
2. Run the following command to extract the tarball: `tar -xzf trifecta-containers-setup-1.0.0.xx.tar.gz cd trifecta_setup/`
3. Run the following command: `bash ./trifecta_setup.sh --setup`

4. Select from one of the options:

```
-----  
  
Welcome to Trifecta Checklist Tool  
  
This tool runs a series of checks to ensure this application can be  
installed on this host.  
  
Once validated, this script is used to create the privileged tasks on  
this host.  
  
-----  
  
1) Production Deployment (4vCPU, 16GB RAM)  
2) Demo Deployment (2vCPU, 8GB RAM)  
3) Quit  
  
Please enter your install/upgrade mode:
```

5. Run the following command to begin the installation: `bash ./trifecta_setup.sh --install`
During the installation process, the following options are presented. Refer to [Accessing the Zebra Artifactory](#) to retrieve your credentials:

```
Please login to Zebra Artifactory:  
  
Username:  
  
Password:
```

6. Enter the fully qualified domain name of the Server in which MWE RFID is being installed.

```
Enter the FQDN of this Server (hit return if none):
```

7. Select a NTP Server from the list and select the Custom option if you are running a NTP Server.

```
NTP Servers: 0: 0.centos.pool.ntp.org1: 1.centos.pool.ntp.org2:  
2.centos.pool.ntp.org3: 3.centos.pool.ntp.org 4: Custom Please select an  
NTP server to be used on the readers:
```

8. Select the authentication type, that needs to be configured for authentication type.

```
Authentication types:  
1. database  
2. ldap  
3. adfs  
4. database,adfs  
5. oidc
```

```
6. database,oidc
0. Keep current value: database
```

9. If Reader Management is being installed on a cloud instance, select the Cloud configuration.

```
-----
Cloud configuration:
-----
Is the Trifecta installation on the cloud and Readers On-Prem? (y/n):
```

10. Once the above options are submitted, the installation will continue and will complete with the following message:

```
Trifecta has been installed successfully and is running at /data/trifecta
as user trif-user!
```

Running the Reader Management Script—Offline Installation

1. Log in to the Trifecta VM as root or a user with sudo privileges.
2. Run the following command to extract the tarball:

```
tar -xzvf trifecta-containers-setup-1.0.0.xx-offline.tar.gz
cd trifecta _setup/
```

3. Run the following command:

```
bash ./ trifecta_setup.sh --offline-setup
```

4. Then select from one of the options.

```
sudo ./ trifecta_setup.sh --offline-setup
-----
Welcome to Trifecta Checklist Tool
This tool runs a series of checks to ensure this application can be
installed on this host.
Once validated, this script is used to create the privileged tasks on this
host.
-----
1) Production Deployment (4vCPU, 16GB RAM)
2) Demo Deployment (2vCPU, 8GB RAM)
3) Quit
Please enter your install/upgrade mode:
```

5. Run the following command to begin the offline installation on the Reader Management software:

```
bash ./ trifecta _setup.sh --offline-install
```

6. Once the images are loaded, the following options will display:

```
Enter the FQDN of this Server (hit return if none): NTP Servers:
0: 0.centos.pool.ntp.org
1: 1.centos.pool.ntp.org
2: 2.centos.pool.ntp.org
3: 3.centos.pool.ntp.org
4: Custom
Please select an NTP server to be used on the readers:
Authentication types:
1. database
2. ldap
3. adfs
4. database,adfs
5. oidc
6. database,oidc
0. Keep current value: database
Choose an option:
-----
Cloud configuration:
-----
Is the Trifecta installation on the cloud and Readers On-Prem? (y/n):
Trifecta has been installed successfully and is running at /data/ as user
MWE RFID!
```

Starting Reader Management

When the Reader Management software is installed successfully, the system automatically starts all the services.

Validating the Reader Management Installation

1. Run the following command to switch the user to a trif account:

```
sudo su - trif-user
cd /data/trifecta
```


2. Verify all containers are running by executing the following command:

```
docker-compose ps
```



NOTE: The output displays the list of applications with a status of running.

Figure 1 Application Status

```
[trif-user@ip-172-20-3-106 trifecta]$ docker-compose ps
```

NAME	COMMAND	SERVICE	STATUS	PORTS
db-mongo	"docker-entrypoint.s..."	db-mongo	running (healthy)	27017/tcp
db-postgres	"docker-entrypoint.s..."	db-postgres	running (healthy)	5432/tcp
logging-logrotate	"/sbin/tini -- /usr/..."	logging-logrotate	running	
messaging-kafka	"/entrypoint.sh"	messaging-kafka	running	9092/tcp
messaging-mqtt	"/usr/bin/docker-ent..."	messaging-mqtt	running (healthy)	18083/tcp
messaging-zookeeper	"/etc/confluent/dock..."	messaging-zookeeper	running	3888/tcp
monitoring-alertmanager	"/bin/alertmanager -..."	monitoring-alertmanager	running (healthy)	9093/tcp
monitoring-cadvisor	"/usr/bin/cadvisor -..."	monitoring-cadvisor	running (healthy)	8080/tcp
monitoring-grafana	"/run.sh"	monitoring-grafana	running (healthy)	3000/tcp
monitoring-kafka-exporter	"/bin/kafka_exporter..."	monitoring-kafka-exporter	running (healthy)	9308/tcp
monitoring-mongodb-exporter	"/mongodb_exporter -..."	monitoring-mongodb-exporter	running	9216/tcp
monitoring-nginx-exporter	"/usr/bin/nginx-prom..."	monitoring-nginx-exporter	running	
monitoring-node-exporter	"/bin/node_exporter -..."	monitoring-node-exporter	running (healthy)	9100/tcp
monitoring-postgres-exporter	"/bin/postgres_expor..."	monitoring-postgres-exporter	running (healthy)	9187/tcp
monitoring-prometheus	"/start.sh --config..."	monitoring-prometheus	running (healthy)	9090/tcp
monitoring-push-gateway	"/bin/pushgateway"	monitoring-push-gateway	running (healthy)	9091/tcp
monitoring-uisvc-exporter	"/usr/bin/nginx-prom..."	monitoring-uisvc-exporter	running	
trifecta-alerting-sidecar	"/app/alertmanager"	trifecta-alerting-sidecar	running (healthy)	8080/tcp
trifecta-authsvc	"docker-entrypoint.s..."	trifecta-authsvc	running (healthy)	8083/tcp
trifecta-cert-signing-service	"docker-entrypoint.s..."	trifecta-cert-signing-service	running	8091/tcp
trifecta-device-initializer	"/bin/sh -c 'java -j..."	trifecta-device-initializer	running	8080/tcp
trifecta-device-prom-proxy	"python -m device_pr..."	trifecta-device-prom-proxy	running	
trifecta-device-registry	"/bin/sh -c 'java -j..."	trifecta-device-registry	running	8085/tcp
trifecta-device-task-manager	"/bin/sh -c 'java -j..."	trifecta-device-task-manager	running	8085/tcp
trifecta-dmsvc	"docker-entrypoint.s..."	trifecta-dmsvc	running	8086/tcp
trifecta-fileserver	"/bin/sh -c 'java -j..."	trifecta-fileserver	running	8090/tcp
trifecta-messagebridge	"/bin/sh -c 'java -j..."	trifecta-message-bridge	running	8080/tcp
trifecta-sitesvc	"docker-entrypoint.s..."	trifecta-sitesvc	running	8080/tcp
trifecta-tilesrver	"/usr/src/app/run.sh"	trifecta-tilesrver	running	8080/tcp
trifecta-uisvc	"/docker-entrypoint...."	trifecta-uisvc	running	8080/tcp
trifecta-user-service	"java -jar /root/use..."	trifecta-user-service	running	8099/tcp
web-api-gateway	"/docker-entrypoint...."	web-api-gateway	running	0.0.0:443->8443/tcp
web-nginx	"/opt/bitnami/script..."	web-nginx	running	8443/tcp

Reader Management User Interface

The Reader Management Web user interface (UI) can be accessed from a browser at: <https://<Fully Qualified Domain Name of RM Server>>

Figure 2 Reader Management Web UI



Contact Zebra support for help with accessing the Web UI.

Installing the Prerequisite Software

MWE RFID Reader Management software requires third-party utilities to verify the system prerequisites, perform the installation, and manage operations.

Docker

The installer is bundled with Docker Engine and Docker Compose, which are installed on the system as part of the setup.

The Docker root is set to:

```
/data/docker
```

Which is linked to:

```
/var/lib/docker
```

Utility Software

MWE RFID Reader Management requires third-party software for server administration.

Install the latest stable versions of curl, wget, vim, tar, bc, and firewallld.

```
sudo yum update
```

```
sudo yum install -y curl
```

```
sudo yum install -y wget
```

```
sudo yum install -y vim
```

```
sudo yum install -y tar
```

```
sudo yum install -y bc
```

```
sudo yum install -y firewalld
```

Configuring the Server

The MWE RFID Reader Management server requires access to installation files and communication with readers.

Configure the following:

- Host Setup: Configure the following before MWE RFID installation:
 - Hostname
 - Static IP address (Zebra recommends a static IP with valid FQDN)
 - Subnet mask
 - Default gateway
- Time synchronization
 - All systems require time synchronization to a central NTP (Network Time Protocol) server.
 - The Reader Management server requires an NTP client that syncs to the same NTP server as the readers. Install an NTP client if one is not already installed.
 - Set the time zone as appropriate for all local systems.
- DNS
 - Configure DNS to enable communication with other MWE RFID Reader Management components.
 - The Reader Management server must be resolvable by the DNS server(s).
 - DNS server(s) must forward to internet DNS to resolve public FQDNs such as repos required for installation.

Installing the Software

- Network (ports/protocols): For online installation, ensure the server has access to the destinations and ports shown in the following table:

Destination Host	Destination IP	Destination Port
trifecta-doc-rel.artifactory-us.zebra.com	35.201.100.70	443

- SSH
 - The Docker registry above serves all Reader Management Service container Images.
 - Reader Management installation requires direct SSH access to the server. See the service account details under User Accounts and Permissions.
- Groups: Reader Management installation requires the following groups:

Group	Command to Add
trif-user	This group is created during installation. Do not add manually.
docker	This group is created during Docker installation. Do not add manually.

- File/Folder permissions
 - The required file/folder permissions for **trif-user** are granted during installation.
 - Use the following group folder and file configuration:

Folder/File	Permission
/data/trifecta	drwxr-xr-x. (trif-user:trif-user)
/data/docker	drwx--x--x. (root:root)
/data/trifecta-conf	drwxrwsr-x. (trif-user:root)

- User Accounts and Permissions: Configure the system with a minimum of two accounts with permissions specified as follows:

User	Privilege	Group	Description
root	root	wheel/root	Configure and install all prerequisites.
trif-user	RM service account	trif-user docker	Service account used for installation, configuration, and operation of Reader Management.

System Validation

MWE RFID Reader Management requires validation of system components for proper functionality.

Server Configuration

Resource	Minimum Requirement	Validation Command
OS	CentOS7 with latest updates	<code>more /etc/centos-release</code>
Memory	32GB	<code>lsmem grep "Total online memory"</code>
vCPU	8	<code>lscpu grep "CPU(s)"</code>
Disk Layout & Sizing	256GB	<code>df -h -x overlay</code>
Swap	24GB	<code>swapon -s</code>
Hostname	Verify domain is appended	<code>hostname -f</code>
Trifecta user	tri-user user is in the docker groups	<code>groups <tri-user administrative user></code>

Network Configuration


Resource	Validation Command
DNS Name resolution for all systems	Run the nslookup command for each hostname and ensure that each resolves:
	<code>nslookup <hostname></code>
	<hostname> = Docker host
	<hostname> = NTP server
	<hostname> = All readers
Time is in sync with the NTP server	Verify time synchronization using:
	<code>date</code>
	or
	<code>chronyc sources</code>



NOTE: Commands and output may vary. If Chrony is not used as the NTP service, another command associated with the NTP service must be used to verify time is in sync with the NTP server.

Docker and Docker-Compose Configuration

Resource	Validation Command	Example Validation Result
Docker	<code>docker info</code>	<code>\$ docker info</code> Containers: 34 Running: 34 Paused: 0 Stopped: 0 Images: 34 Server Version: 18.09.2 Storage Driver: overlay2 Backing Filesystem:

Resource	Validation Command	Example Validation Result
		xfs ... <additional info may be included>
docker-compose is installed and executable from anywhere.	Run the following command and verify a version response: docker-compose -v	Docker Compose version v2.2.2  NOTE: Build versions may vary.

Configuring Authentication Type

MWE RFID Reader Management supports authentication modes for accounts logging into the Reader Management web client and configuration tools.

Database

In this mode, login accounts are created and authenticated locally in the MWE RFID Reader Management database. The default admin account created by the installation scripts is a local database account.

LDAP

When this mode is selected, login accounts are authenticated against an LDAP server on the network. Active directory authentication is supported under this authentication mode. When the LDAP mode is selected, it is still possible to specify an exception list of local database accounts authenticated against the local MWE RFID Reader Management database.

ADFS

In this mode, login accounts are authenticated against an ADFS server on the network. This mode does not allow login by any local database accounts.

Database, ADFS

This mode allows accounts authenticated against an ADFS server and local MWE RFID Reader Management database accounts.

OIDC

In this mode, login accounts are authenticated against an OIDC server on the network. This mode does not allow login by any local database accounts.

Database, OIDC

This mode allows accounts authenticated against an OIDC server and local MWE RFID Reader Management database accounts.

When installing Reader Management, select one of these authentication modes. Database is normally chosen at installation time, as the other options require entering several configuration parameters that may not be available.

At any time after installation, you can select and configure any of the authentication modes listed above. This is done by logging into the server as trif-user and cd to /data/trifecta/ directory and update the AUTH_TYPE environment variable in the .env file (file location /data/trifecta/.env).

LDAP

To configure LDAP authentication, edit the .env file and set: AUTH_TYPE=ldap

Provide values for the LDAP parameters in the .env file. Default values are provided as examples shown below:

```
LDAP_URL=ldap://192.168.30.52
LDAP_USER_BASE_DN=CN=Users,DC=CLUSTER,DC=ZEBRA,DC=COM
LDAP_SEARCH_BASE_DN=CN=Users,DC=CLUSTER,DC=ZEBRA,DC=COM
LDAP_EXCLUDE_USERS=admin,user1,user2
LDAP_DEFAULT_USERGROUP=defaultLdapUserGroup
LDAP_AD_DOMAIN=CLUSTER LDAP_VENDOR=ActiveDirectory
LDAP_SVC_ACCOUNT_NAME=uid=Ldap.Svc,ou=People,dc=cluster,dc=wherenet,dc=com
LDAP_SVC_ACCOUNT_PASSWORD=password
LDAP_GROUP_USER_LIST_FIELD=memberUid
LDAP_USER_GROUP_FIELD=uid LDAP_USER_ID_TYPE=uid
```

Here is a brief explanation of some of the parameters:

LDAP_URL

LDAP_USER_BASE_DN

LDAP_SEARCH_BASE_DN

LDAP_AD_DOMAIN

LDAP_VENDOR

This parameter can be set to ActiveDirectory or OpenLdap, depending on the LDAP version.

LDAP_EXCLUDE_USERS

This is a comma-separated list of local Reader Management login accounts (that is, accounts defined using the Reader Management web client and stored in the database) allowed to log in when LDAP is enabled.

LDAP_DEFAULT_USERGROUP

If Reader Management cannot obtain from the LDAP server the user group for a particular user, or if the obtained user group cannot be matched to an existing user group, then Reader Management will assign this user to the user group specified in LDAP_DEFAULT_USERGROUP. The default setting is LDAP_DEFAULT_USERGROUP=defaultLdapUserGroup. The user will therefore have the permissions or access level associated with this default user group.

LDAP_SVC_ACCOUNT_NAME

LDAP_SVC_ACCOUNT_PASSWORD

The above two parameters are needed only for OpenLDAP, which requires a service account to grant access for directory search of a user's DN (Distinguished Name). In OpenLDAP, DN is required for the user login.



NOTE: You will see the parameter LDAP_SVC_ACCOUNT_PASSWORD in the .env configuration file only before running the Reader Management installation scripts. These scripts will remove all passwords from the .env file and encrypt them into the vault service. Therefore, only enter the password in .env before performing a Reader Management installation.

The final step is to create Reader Management user groups that match the names of user groups on the LDAP server. For example, if the domain user accounts that will log into the web client belong to the LDAP user groups 'Managers' and 'Operators', then you should create the user groups 'Managers' and

'Operators' in Reader Management. To do so, log into the Reader Management web client using the admin account, click **Users** on the menu bar, and select the **USER GROUPS** tab. Add the groups and specify the permissions granted to each group.



NOTE: Do not forget to add the group defaultLdapUserGroup as mentioned above.

After updating .env, save the file and run the following commands to apply the changes:

```
cd /data/trifecta/  
docker-compose up -d trifecta-authsvc
```

ADFS

To configure ADFS authentication, Edit the .env file and set: AUTH_TYPE=adfs

Provide valid values for the ADFS parameters in the .env file. Default values in .env are provided only as examples and are shown below:

ADFS_CLIENT_ID=fce8beb4-3974-4d02-a3d4-a7233343fcd8

ADFS_CLIENT_SECRET=eb4QD9L5xwJOYWB9Y4-iBTli4YqkqBNOixVx_xm5

ADFS_DISCOVERY=https://WIN-C3V92OI2O7J.example.com/adfs/.well-known/openid-configuration/

ADFS_RELIVING_PARTY_TRUST_ID=mwe-adfs

ADFS_PARSER=IsMemberOf

ADFS_IDENTITY_KEY=mail

ADFS_GROUP_KEY=memberof

The values for these parameters should be provided by the customer's IT Department.

It should be noted that possible values for ADFS_PARSER are:

IsMemberOf (for example, [CN=MWE,...])

groupsOnly (for example, [MWE, ...])

tokenGroup (for example, [zebra\MWE, zebra.lan\MWE, ...])

The final step is to create user groups that match the names of user groups on the ADFS server. For example, if the domain user accounts that will log into the web client belong to the ADFS user groups 'Managers' and 'Operators', then you should create the user groups 'Managers' and 'Operators' in Reader Management. To do so, log into the Reader Management web client using the admin account, click **Users** on the menu bar, and select the **USER GROUPS** tab. Add the groups and specify the permissions granted to each group.

After updating .env, save the file and run the following commands to apply the changes:

```
cd /data/trifecta/  
docker-compose up -d trifecta-authsvc
```

Database, LDAP

To configure Database, LDAP authentication, Edit the .env file and set: AUTH_TYPE=database, ldap

Configure the ADFS parameters as explained in the ADFS previous section.

In the Reader Management web client, add as many local user accounts as desired (Refer to the Database section).

When launching the Reader Management web client, you will see the normal login screen for database accounts and an ADFS Login button for ADFS account login.

After updating .env, save the file and run the following commands to apply the changes:

```
cd /data/trifecta/  
docker-compose up -d trifecta-authsvc
```

Upgrading the Software

This section describes the steps required to upgrade the MWE RFID Reader Management software from version 1.0.1.24 to version 1.0.2.22.



NOTE:

If the current deployment was installed using the online package (trifecta-containers-setup-1.0.1.24.tar.gz), follow the steps for Upgrading the Software Online.

If the current deployment was done using the offline package (trifecta-containers-setup-1.0.1.24-offline.tar.gz), follow the steps for Upgrading the Software Offline.

Upgrading the Software Online

Make sure you have the required identity token from the Zebra Artifactory.

1. Go to <https://zebratech.jfrog.io/artifactory/trifecta-gen-ext/builds/>.
2. Download the upgrade package: trifecta-containers-setup-1.0.22.tar.gz.
3. Extract the package under the same location as the current version.
4. Change the directory to:

```
trifecta_setup
```

5. Run the following command:

```
./trifecta_setup.sh --upgrade
```

6. When the upgrade has finished, the following message is displayed:

```
Trifecta has been upgraded successfully and is running at /data/ as user  
trif-user!
```

7. Run the following commands to verify the upgrade:

```
sudo su - trif-user  
cd /data/trifecta_setup
```

```
docker-compose ps
```

```
[root@ip-172-20-3-244 trifecta_setup]# sudo su - trif-user
Last login: Thu Apr  6 14:44:15 UTC 2023 on pts/0
[trif-user@ip-172-20-3-244 ~]$ cd /data/trifecta
[trif-user@ip-172-20-3-244 trifecta]$ docker-compose ps
NAME                                COMMAND                                SERVICE    STATUS    PORTS
db-mongo                           "docker-entrypoint.s..." db-mongo   running   (healthy) 27017/tcp
db-postgres                         "docker-entrypoint.s..." db-postgres running   (healthy) 5432/tcp
logging-logrotate                  "/sbin/tini -- /usr/..." logging-logrotate running
messaging-kafka                    "/entrypoint.sh"           messaging-kafka running   (healthy) 9092/tcp
messaging-mqtt                     "/usr/bin/docker-ent..." messaging-mqtt running   (healthy) 18083/tcp
messaging-zookeeper                "/etc/confluent/dock..." messaging-zookeeper running   (healthy) 3888/tcp
monitoring-alertmanager            "/bin/alertmanager -..." monitoring-alertmanager running   (healthy) 9093/tcp
monitoring-cadvisor                "/usr/bin/cadvisor -..." monitoring-cadvisor running   (healthy) 8080/tcp
monitoring-grafana                 "/run.sh"                   monitoring-grafana running   (unhealthy) 3000/tcp
monitoring-kafka-exporter          "/bin/kafka_exporter..." monitoring-kafka-exporter running   (healthy) 9308/tcp
monitoring-mongodb-exporter        "/mongodb_exporter -..." monitoring-mongodb-exporter running   (healthy) 9216/tcp
monitoring-nginx-exporter          "/usr/bin/nginx-prom..." monitoring-nginx-exporter running
monitoring-node-exporter           "/bin/node_exporter ..." monitoring-node-exporter running   (healthy) 9100/tcp
monitoring-postgres-exporter       "/bin/postgres_expor..." monitoring-postgres-exporter running   (healthy) 9187/tcp
monitoring-prometheus              "/start.sh --config..." monitoring-prometheus running   (healthy) 9090/tcp
monitoring-pushgateway             "/bin/pushgateway"         monitoring-pushgateway running   (healthy) 9091/tcp
monitoring-uisvc-exporter          "/usr/bin/nginx-prom..." monitoring-uisvc-exporter running
trifecta-alerting-sidecar           "/app/alertmanager"         trifecta-alerting-sidecar running   (healthy) 8080/tcp
trifecta-authsvc                    "docker-entrypoint.s..." trifecta-authsvc running   (healthy) 8083/tcp
trifecta-cert-signing-service       "docker-entrypoint.s..." trifecta-cert-signing-service running
trifecta-container-monitor          "/app/container_moni..." trifecta-container-monitor running   (healthy) 8080/tcp
trifecta-device-initializer         "/bin/sh -c 'java -j..." trifecta-device-initializer running
trifecta-device-prom-proxy          "python -m device_pr..." trifecta-device-prom-proxy running
trifecta-device-registry            "/bin/sh -c 'java -j..." trifecta-device-registry running
trifecta-device-task-manager        "/bin/sh -c 'java -j..." trifecta-device-task-manager running
trifecta-dmsvc                      "docker-entrypoint.s..." trifecta-dmsvc running
trifecta-fileserver                 "/bin/sh -c 'java -j..." trifecta-fileserver running
trifecta-messagebridge              "/bin/sh -c 'java -j..." trifecta-message-bridge running
trifecta-sitesvc                    "docker-entrypoint.s..." trifecta-sitesvc running
trifecta-tilserver                  "/usr/src/app/run.sh"       trifecta-tilserver running
trifecta-uisvc                      "docker-entrypoint.s..." trifecta-uisvc running
trifecta-user-service               "java -jar /root/use..." trifecta-user-service running
web-api-gateway                    "/docker-entrypoint.s..." web-api-gateway running
web-nginx                          "/opt/bitnami/script..." web-nginx running
```

Upgrading the Software Offline

Ensure that you have the required identity token from the Zebra Artifacts.

1. Go to <https://zebratech.jfrog.io/artifactory/trifecta-gen-ext/builds/>.
2. Download the upgrade package: trifecta-containers-setup-1.0.2.22-offline.tar.gz.
3. Extract the package under the same location as the current version.
4. Change the directory to:

```
trifecta_setup
```

5. Run the following command:

```
./trifecta_setup.sh --offline-upgrade
```

6. When the upgrade has finished, the following message is displayed:

```
Trifecta has been upgraded successfully and is running at /data/ as user
trif-user!
```

7. Run the following commands to verify the upgrade:

```
sudo su - trif-user
cd /data/trifecta_setup
```

docker-compose ps

```
[trif-user@ip-172-20-3-244 trifecta]$ docker-compose ps
NAME                                COMMAND                                SERVICE    STATUS    PORTS
db-mongo                            "docker-entrypoint.s..."            db-mongo   running   27017/tcp
db-postgres                         "docker-entrypoint.s..."            db-postgres running   5432/tcp
logging-logrotate                   "/sbin/tini -- /usr/..."            logging-logrotate running
messaging-kafka                     "/entrypoint.sh"                      messaging-kafka running   9092/tcp
messaging-mqtt                      "/usr/bin/docker-ent..."            messaging-mqtt running (healthy) 18083/tcp
messaging-zookeeper                 "/etc/confluent/dock..."            messaging-zookeeper running   3888/tcp
monitoring-alertmanager              "/bin/alertmanager -..."            monitoring-alertmanager running (healthy) 9093/tcp
monitoring-cadvisor                  "/usr/bin/cadvisor -..."            monitoring-cadvisor running (healthy) 8080/tcp
monitoring-grafana                   "/run.sh"                              monitoring-grafana running (unhealthy) 3000/tcp
monitoring-kafka-exporter            "/bin/kafka_exporter..."            monitoring-kafka-exporter running (healthy) 9308/tcp
monitoring-mongodb-exporter          "/mongodb_exporter -..."            monitoring-mongodb-exporter running   9216/tcp
monitoring-nginx-exporter            "/usr/bin/nginx-prom..."            monitoring-nginx-exporter running
monitoring-node-exporter             "/bin/node_exporter -..."            monitoring-node-exporter running (healthy) 9100/tcp
monitoring-postgres-exporter         "/bin/postgres_expor..."            monitoring-postgres-exporter running (healthy) 9187/tcp
monitoring-prometheus                "/start.sh --config..."            monitoring-prometheus running (healthy) 9090/tcp
monitoring-push-gateway              "/bin/pushgateway"                  monitoring-push-gateway running (healthy) 9091/tcp
monitoring-uisvc-exporter            "/usr/bin/nginx-prom..."            monitoring-uisvc-exporter running
trifecta-alerting-sidecar             "/app/alertmanager"                  trifecta-alerting-sidecar running (healthy) 8080/tcp
trifecta-authsvc                      "docker-entrypoint.s..."            trifecta-authsvc running (healthy) 8083/tcp
trifecta-cert-signing-service         "docker-entrypoint.s..."            trifecta-cert-signing-service running   8091/tcp
trifecta-container-monitor            "/app/container_moni..."            trifecta-container-monitor running (healthy) 8080/tcp
trifecta-device-initializer           "/bin/sh -c 'java -j..."            trifecta-device-initializer running   8080/tcp
trifecta-device-prom-proxy            "python -m device_pr..."            trifecta-device-prom-proxy running
trifecta-device-registry              "/bin/sh -c 'java -j..."            trifecta-device-registry running   8085/tcp
trifecta-device-task-manager          "/bin/sh -c 'java -j..."            trifecta-device-task-manager running   8085/tcp
trifecta-dmsvc                        "docker-entrypoint.s..."            trifecta-dmsvc running   8086/tcp
trifecta-filserver                    "/bin/sh -c 'java -j..."            trifecta-filserver running   8090/tcp
trifecta-messagebridge                "/bin/sh -c 'java -j..."            trifecta-message-bridge running   8080/tcp
trifecta-sitesvc                      "docker-entrypoint.s..."            trifecta-sitesvc running   8080/tcp
trifecta-tilserver                    "/src/app/run.sh"                  trifecta-tilserver running   8080/tcp
trifecta-uisvc                        "docker-entrypoint..."              trifecta-uisvc running   8080/tcp
trifecta-user-service                 "java -jar /root/use..."            trifecta-user-service running   8099/tcp
web-api-gateway                      "docker-entrypoint..."              web-api-gateway running   0.0.0.0:443->8443/tcp
web-nginx                           "/opt/bitnami/script..."            web-nginx running   8443/tcp
[trif-user@ip-172-20-3-244 trifecta]$
```

