



Rocket MultiValue Experiences

Installation and User Guide

Version 1.3.0

July 2022
MVX-130-UG-01

Notices

Edition

Publication date: July 2022

Book number: MVX-130-UG-01

Product version: Version 1.3.0

Copyright

© Rocket Software, Inc. or its affiliates 1996–2022. All Rights Reserved.

Trademarks

Rocket is a registered trademark of Rocket Software, Inc. For a list of Rocket registered trademarks go to: www.rocketsoftware.com/about/legal. All other products or services mentioned in this document may be covered by the trademarks, service marks, or product names of their respective owners.

Examples

This information might contain examples of data and reports. The examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

License agreement

This software and the associated documentation are proprietary and confidential to Rocket Software, Inc. or its affiliates, are furnished under license, and may be used and copied only in accordance with the terms of such license.

Note: This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when exporting this product.

Corporate information

Rocket Software, Inc. develops enterprise infrastructure products in four key areas: storage, networks, and compliance; database servers and tools; business information and analytics; and application development, integration, and modernization.

Website: www.rocketsoftware.com

Rocket Global Headquarters
77 4th Avenue, Suite 100
Waltham, MA 02451-1468
USA

To contact Rocket Software by telephone for any reason, including obtaining pre-sales information and technical support, use one of the following telephone numbers.

Country	Toll-free telephone number
United States	1-855-577-4323
Australia	1-800-823-405
Belgium	0800-266-65
Canada	1-855-577-4323
China	400-120-9242
France	08-05-08-05-62
Germany	0800-180-0882
Italy	800-878-295
Japan	0800-170-5464
Netherlands	0-800-022-2961
New Zealand	0800-003210
South Africa	0-800-980-818
United Kingdom	0800-520-0439

Contacting Technical Support

The Rocket Community is the primary method of obtaining support. If you have current support and maintenance agreements with Rocket Software, you can access the Rocket Community and report a problem, download an update, or read answers to FAQs. To log in to the Rocket Community or to request a Rocket Community account, go to www.rocketsoftware.com/support.

In addition to using the Rocket Community to obtain support, you can use one of the telephone numbers that are listed above or send an email to support@rocketsoftware.com.

Contents

Notices.....	2
Corporate information.....	3
Chapter 1: MVX: Performance Overview.....	6
System Requirements.....	6
Chapter 2: Installing MVX.....	8
Installing MVX on Windows.....	8
Installing MVX on Linux.....	10
Upgrading MVX.....	13
Upgrading from MVX 1.1.1 or MVX 1.2.0 without Keycloak migration.....	13
Upgrading from MVX 1.2.0 and performing a Keycloak data migration.....	14
Uninstalling MVX.....	15
Chapter 3: Installing MVAdmin.....	17
Installing or upgrading MVAdmin on Windows.....	17
Installing or upgrading MVAdmin on Linux and AIX.....	19
Anti-CSRF protection in MVX UI/API.....	21
Uninstalling MVAdmin.....	22
Starting and stopping MVAdmin.....	23
Chapter 4: Configuring MVX.....	24
Logging in to Keycloak for the first time.....	24
Configuring MVX log files.....	25
Configuring MVAdmin log files.....	25
Keycloak log files.....	26
Configuring performance snapshot data storage.....	26
Updating the credentials for application server connections in MVAdmin.....	27
Changing your MVAdmin UI login credentials.....	27
Chapter 5: SuperAdmins and user account management.....	29
Logging in as SuperAdmin for the first time.....	29
Creating user accounts.....	30
Editing user accounts.....	32
Enabling and disabling user accounts.....	32
Deleting user accounts.....	32
Resetting user passwords.....	33
Resetting the SuperAdmin password.....	33
Changing the Keycloak client secret.....	34
Chapter 6: Managing your account.....	36
Managing your account profile.....	36
Entering your RBC credentials.....	36
Managing subscriptions.....	37
Chapter 7: MVX User Guide.....	39
Logging-in.....	39
Registering an existing MultiValue Application Server instance.....	40
Instance Details dashboard.....	41
MVX Performance Dashboard.....	42
Events.....	42
Reviewing events.....	43
Managing tasks.....	44
Event definition files.....	45
Editing event definition files.....	51
Configuring the accounts that are monitored.....	52

MV Sessions.....	53
Locks.....	54
Host CPU/Memory.....	55
Appendix A: mvx.bat and mvx.sh files.....	57
Appendix B: mvx.ini configuration file.....	59

Chapter 1: MVX: Performance Overview

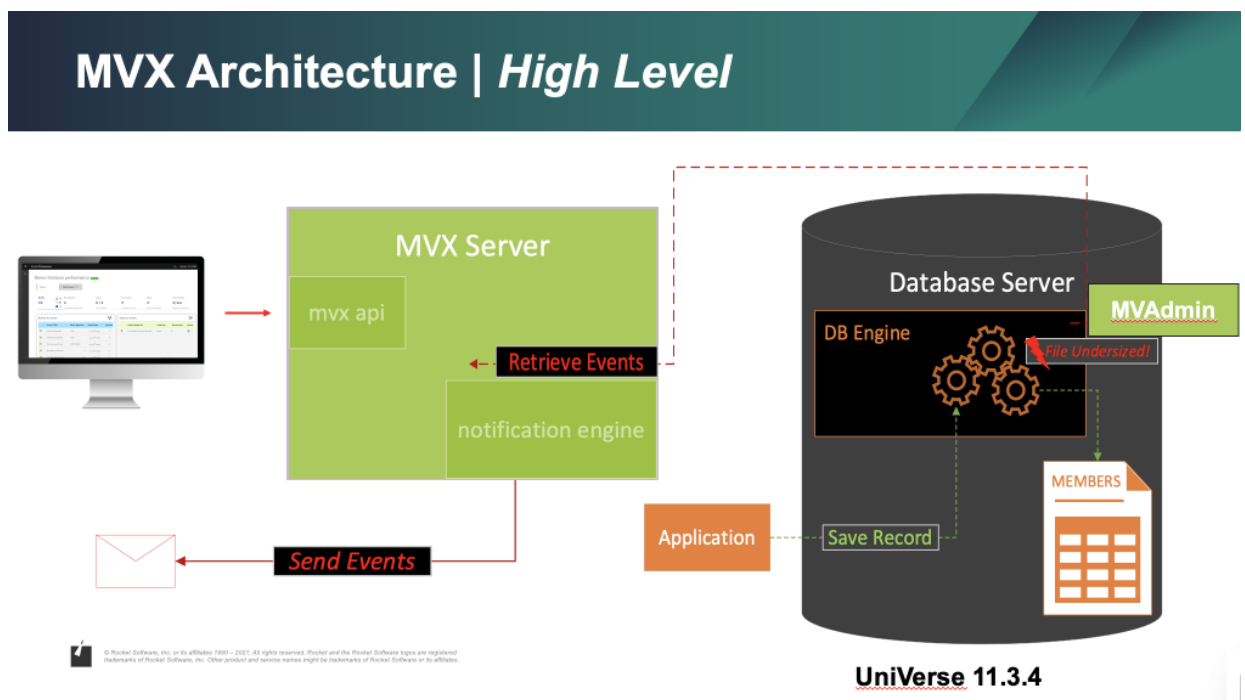
The Rocket MultiValue Performance Experience (MVX: Performance) is a system monitoring tool for your MultiValue Application Server (MVAS) enabling you to understand and enhance UniVerse performance.

MVX: Performance helps you identify and escalate performance-impacting events. Escalated events include possible resolutions, allowing you to easily track the source of the issue and address it to improve overall performance. In addition to the Events tile, MVX: Performance includes monitoring tiles that actively monitor issues with Sessions and Locks plus the ability to deep dive into specific Process IDs (PIDs).

The MVX architecture comprises three components:

- MVX Core: the browser accessible central portal with which you can register and manage your MVAS, access Rocket Business Connect (RBC) to enable entitlement services, and activate experiences such as MVX: Performance.
- MVAdmin: provides a set of MVAS specific services for MVX such as registration, experience activation, and communication between MVX and MVAS.
- MVX: Performance: provides a UI for registering your MVAS with MVX and a dashboard for identifying and escalating performance-impacting events and monitoring sessions and locks.

Figure 1: High-level architecture and example flow for a File Undersized event escalation



System Requirements

Before you install and configure MVX and MVAdmin, ensure that your environment meets the following minimum hardware and software requirements.

MVX Hardware Requirements

The hardware requirements for MVX are:

- At least 5 GB of available hard disk space
- At least 8 GB of RAM

MVX Software Requirements

The software requirements for MVX are:

- MVX v1.3.0 is delivered as a Docker image built on a Rocky Linux 8.6 base image. Both the Docker Community edition and the Docker Enterprise edition are supported.
- Supported platforms: Windows 10 using Docker Desktop for Windows, RedHat Linux 7.x and CentOS 7.x using Docker v1.13.1-161 or later, or Red Hat Linux 8.x and CentOS 8.x using Podman v1.6.4 and above.
- For Red Hat 7.x and CentOS 7.x, ensure that the Linux package `libseccomp` is up to date.

MVAdmin Software Requirements

Before you install and configure MVAdmin on an MultiValue Application Server, ensure that your environment meets the following software requirements:

- UniVerse v11.3.4 HotFix 4
- Supported platforms: Windows, Linux or AIX
- For Linux or AIX implementations, make sure the UNIX `sar` command is available for use on your system.

Browser Recommendation

When logging on to the Rocket MVX Experience console, it is recommended that you use the Google Chrome browser.

Other Considerations

MVX and MVAdmin log files are configured to roll-over on a daily basis or when they exceed 100 MB. When they roll-over, they are archived to the `logs/archived` folder in compressed format. These archived files are automatically purged after 30 days. It is recommended that you monitor `logs/archived` directory for both the MVX and MVAdmin servers. If the volume grows too large, you may need to manually remove older archives so that they do not consume large amounts of disk space on your server.

Chapter 2: Installing MVX

MVX can be installed on-premise on your local machine, or in the cloud.

The following topics provide instructions and information on installing and uninstalling MVX using a Docker container and setting up security for your MVX implementation.

Important: If you have a firewall configured on the server that will be hosting the MVX server, please make the required changes to your firewall to allow port 9243 (default port number supplied with MVX) as in inbound connection so other devices can communicate with the MVX Server. If you change the default port number in MVX, then make the appropriate change in your firewall configuration.

Note: MVX: Performance can only be installed on the VOU, VEU, DEU, ASP, U2 or HOST editions of UniVerse. It cannot be installed on the GOLD, EVAL, OEM STBY or EDU editions of UniVerse.

- [Installing MVX on Windows](#)
Complete these instructions to install MVX on Windows.
- [Installing MVX on Linux](#)
Complete these instructions to install MVX on Linux.
- [Upgrading MVX](#)
Complete these instructions to upgrade to the latest MVX version.
- [Uninstalling MVX](#)
Complete these instructions to uninstall MVX.

Installing MVX on Windows

Complete these instructions to install MVX on Windows.

Review the [System Requirements](#) before installing the image.

Note:

- Rocket recommends installing the MVX server on a different host machine than the machine where the MultiValue Application Server is installed.
 - We strongly recommend that
-

These instructions include steps for installing Docker - a container platform provider. Containers allow an application or its services and configurations to be packaged as a container image. This containerized application can then be tested as a unit and deployed as an image instance to the OS.

Note: Docker Desktop for Windows requires the use of the Hyper-V feature in Windows. This Windows feature must be installed before installing Docker Desktop. Depending upon your system, you may need to enable virtualization in your computer's BIOS to support running the Windows Hyper-V feature. Also, be aware that due to a conflict with Hyper-V, if a VMWare Workstation version previous to v14.5 is installed, then VMWare Workstation will fail to start a virtual machine after the installation of Hyper-V.

Procedure

1. Download the Docker Desktop for Windows installer from <https://www.docker.com/> and then run the downloaded file to install the Docker Desktop. When the installation completes, start the Docker Desktop.
2. Order MultiValue Experience (MVX) and the Rocket MultiValue Performance Experience add-on from [Rocket Business Connect](#) (RBC).
3. From the Product Availability feature in [Rocket Business Connect](#), download the MVX package (mvx_<version>.zip where <version> is the three-digit version and three-digit build number of the release (for example, 1.1.1.100)) file to a directory on your system (for example, c:\temp).
4. Extract the mvx_<version>.zip.

This will create a directory structure as illustrated below (assuming you used the c:\temp directory to hold the mvx_<version>.zip).

```
temp/
  mvxserver/
    mvx-docker-SB-<mm-dd-yy>.tar.gz (where <mm-dd-yy> is the date of the release)
    linux/
      license.txt
      notices.txt
      mvx.bat
      mvx.ini
    Windows/
      license.txt
      notices.txt
      mvx.bat
      mvx.ini
  mvadmin/
    MVAdminSetup.exe
    mvadmin-linux.tar
    mvadmin-aix.tar
```

5. Create a new directory for the installation on your server (for example, C:\mvx). Note that the path name cannot include any spaces.

```
c:\> mkdir mvx
```

6. Copy the mvx-docker-SB-<mm-dd-yy>.tar.gz (where <mm-dd-yy> is the date of the release) and the Windows versions of the mvx.bat and mvx.ini files into your new mvx directory.

```
c:\> copy c:\temp\mvxserver\mvx-docker-SB-<mm-dd-yy>.tar.gz c:\mvx\
c:\> copy c:\temp\mvxserver\Windows\mvx.bat c:\mvx\
c:\> copy c:\temp\mvxserver\Windows\mvx.ini c:\mvx\
```

7. Create a directory named data in the mvxserver directory.

```
c:\> mkdir c:\mvx\data
```

8. Open the mvx.ini file in a text editor and modify the *WebPort* and *DataDir* values appropriate for your system and either configure *DNS* values appropriate for your system (if using DNS for name resolution) or change *UseHostNetwork* value to yes (if using your local host file for name resolution). Save the edited file. See [mvx.ini configuration file](#) for more information on these settings.

(if using your local host file for name resolution)

(if using DNS for name resolution)

9. From the mvx directory, run the following command to load the MVX docker image:

```
c:\mvx> mvx.bat load <date>
```

where <date> is the date portion of the Docker image file name (for example, for a file named mvx-docker-SB-12-01-21.tar.gz, the date would be specified as 12-01-21).

MVX is installed and the container is started. A message displays indicating:

```
Container has been started
```

This message is followed by a message indicating:

```
It may take several minutes for MVX to fully start
```

Subsequent to this message, messages for the startup of the Kafka, Keycloak and MVX components are displayed. Finally, the last message displays indicating the MVX startup is complete:

```
MVX system has been fully started
```

Note: If you receive the error `docker: "Error response from daemon: user declined directory sharing"`, you may need to enable write permissions on the data directory you created.

- In Windows Explorer, right-click the data directory and select **Properties**.
- Select the **Security** tab and then enable Full access to the Windows principal running Docker Desktop for Windows (likely the logged in Windows user).
- Run the `mvx.bat load <date>` command again. As a result, Docker Desktop should display a dialog asking if you agree to share the data directory. Respond **Yes** to this prompt. As a result, the `mvx.bat load <date>` command should succeed without error.

Important: After installing MVX, users should take the appropriate actions to open the following ports to outside access:

- For MVX: 9243 - The Web UI for MVX should be reachable by a browser.
 - For Keycloak: 9543 - The Keycloak Authentication and Authorization server must be accessible to MVAdmin installations running on MVASs. Additionally, it should be accessible to a browser for occasionally accessing its administrative console.
 - For Kafka: 9643 - The Kafka server must be accessible to MVAdmin installations running on MVASs.
-

Parent topic: [Installing MVX](#)

Installing MVX on Linux

Complete these instructions to install MVX on Linux.

Review the [System Requirements](#) before installing the image.

Note: Rocket recommends installing the MVX server on a different host machine than the machine where the MultiValue Application Server is installed.

For more information on managing and configuring your Docker image after installation, see [MVX .bat and .sh files](#).

These instructions include steps for installing Docker (for Red Hat or Centos 7.x implementations) and Podman (for Red Hat Linux 8.x or Centos 8.x implementations), which are container platform providers. Containers allow an application or its services and configurations to be packaged as a

container image. This containerized application can then be tested as a unit and deployed as an image instance to the OS.

Important: Because Red Hat Linux 8.x and Centos 8.x implementations include the Security Enhanced Linux (SELinux) feature, if you are installing MVX on a Red Hat Linux 8.x or Centos 8.x implementation, before installing, we recommend running the following command from the command line to confirm whether or not SELinux is enabled.

```
sudo sestatus
```

If the `Current mode:` value indicates that SELinux is enabled, run the following command to temporarily disable SELinux. Note that this change is only valid for the current session and will not persist after a reboot.

```
sudo setenforce 0
```

To confirm that SELinux has been disabled for the current session, run `sudo sestatus` again and verify that the `Current mode:` value is set to `permissive`.

Procedure

1. Do one of the following to install the standard Linux Docker or Podman package:

Note: You must have root access to install Docker or Podman via yum.

For Red Hat Linux 7.x or Centos 7.x, run the following command:

```
yum install docker
```

For Red Hat Linux 8.x or Centos 8.x, run the following command:

```
yum install podman
```

2. Order MultiValue Experience (MVX) and the Rocket MultiValue Performance Experience add-on from [Rocket Business Connect](#) (RBC).
3. From the Product Availability feature in [Rocket Business Connect](#), download the MVX package (`mvx_<version>.zip` where `<version>` is the three-digit version and three-digit build number of the release (for example, 1.1.1.100)) file to a directory on your system (for example `/tmp`).
4. Extract the `mvx_<version>.zip`.

Note: If your Linux system does not have the unzip utility, you can install it via the `yum install unzip`:

```
# unzip mvx_<version>.zip
```

This will create a directory structure as illustrated below (assuming you used the `/tmp` directory to hold `mvx_<version>.zip`):

```
tmp/
  mvxserver/
    mvx-docker-SB-<mm-dd-yy>.tar.gz (where <mm-dd-yy> is the date of the release)
  linux/
    license.txt
    notices.txt
    mvx.bat
    mvx.ini
  Windows/
    license.txt
```

```
    notices.txt
    mvx.bat
    mvx.ini
mvadmin/
    MVAdminSetup.exe
    mvadmin-linux.tar
    mvadmin-aix.tar
```

5. Create a new directory to use for installing MVX (we recommend `/opt/rocketsoftware/mvx`, but note that creating a subdirectory in `/opt` requires root access). Note that the path name cannot include any spaces.

```
# mkdir -p /opt/rocketsoftware/mvx
```

6. Copy the `mvx-docker-SB-<mm-dd-yy>.tar.gz` (where *<mm-dd-yy>* is the date of the release) and the Linux versions of the `mvx.sh` and `mvx.ini` files into your new `mvx` directory.

```
# cp /tmp/mvxserver/mvx-docker-SB-<mm-dd-yy>.tar.gz /opt/rocketsoftware/mvx/
# cp /tmp/mvxserver/linux/mvx.sh /opt/rocketsoftware/mvx/
# cp /tmp/mvxserver/linux/mvx.ini /opt/rocketsoftware/mvx/
```

7. Create a directory named `data` in your `mvx` directory.

```
# mkdir /opt/rocketsoftware/mvx/data
```

8. Open the `mvx.ini` file in a text editor and modify the `WebPort` and `DataDir` values appropriate for your system and either configure `DNS` values appropriate for your system (if using `DNS` for name resolution) or change `UseHostNetwork` value to `yes` (if using your local host file for name resolution). Save the edited file. See [mvx.ini configuration file](#) for more information on these settings.

9. Run the following command to load the MVX docker image:

```
mvx.sh load <date>
```

where *<date>* is the date portion of the Docker image file name (for example, for a file named `mvx-docker-SB-12-01-21.tar.gz`, the date would be specified as `12-01-21`).

MVX is installed and the container is started. A message displays indicating:

```
Container has been started
```

This message is followed by a message indicating:

```
It may take several minutes for MVX to fully start
```

Subsequent to this message, messages for the startup of the Kafka, Keycloak and MVX components are displayed. Finally, the last message displays indicating the MVX startup is complete:

```
MVX system has been fully started
```

Note: Each time you run `mvx.sh load <date>` on Red Hat 8.x or CentOS 8.x using Podman, Podman creates a temporary file in `/var/tmp`. If you are running low on space for the file system used by `/var/tmp`, we recommend you delete these files.

Important: After installing MVX, users should take the appropriate actions to open the following ports to outside access:

- For MVX: 9243 - The Web UI for MVX should be reachable by a browser.
 - For Keycloak: 9543 - The Keycloak Authentication and Authorization server must be accessible to MVAdmin installations running on MVASs. Additionally, it should be accessible to a browser for occasionally accessing its administrative console.
 - For Kafka: 9643 - The Kafka server must be accessible to MVAdmin installations running on MVASs.
-

Parent topic: [Installing MVX](#)

Upgrading MVX

Complete these instructions to upgrade to the latest MVX version.

For more information on managing and configuring your Docker image, see [MVX .bat and .sh files](#).

Warning: Always backup your MVX data directory (located in the root directory of your MVX installation) prior to performing an upgrade.

At MVX version 1.3.0 there are different upgrade options depending on what version you are upgrading from, and if you want to skip the migration of Keycloak data files.

The options are summarized here and the detailed instructions for each option are detailed below.

1. Upgrading from MVX 1.1.1 or upgrading from MVX 1.2.0 and skipping the Keycloak migration.
 - Due to a problem with the Kafka configuration in MVX 1.1.1, if you are upgrading from MVX 1.1.x to MVX 1.2.0, you must rename your existing data directory and then create a new empty data directory before performing the upgrade.
 - If you are upgrading from MVX 1.2.0, but do not wish to perform the Keycloak migration, you will also have to rename your existing data directory and then create a new empty data directory before performing the upgrade.

Starting MVX with an empty data folder means that you will lose all previous registration information, UniVerse instance registrations and user information created in the previous version.
2. Upgrading from MVX 1.2.0 and performing the Keycloak data migration.
 - When upgrading to the latest version of MVX, you are installing MVX over data that is maintained by a previous version of MVX. Migration of Keycloak user account data is required if you want to maintain Keycloak user accounts that you have set up with your previous MVX installation.

Parent topic: [Installing MVX](#)

Upgrading from MVX 1.1.1 or MVX 1.2.0 without Keycloak migration

If you prefer to skip the Keycloak migration and lose previous Keycloak data, you can continue with these steps.

Note: In the following steps, `mvx.bat` or `mvx.sh` refer to the files from your new 1.3.0 package. Do not run the steps with `mvx.bat` or `mvx.sh` from your previously installed packages.

Complete these steps to migrate Keycloak-stored user accounts from previous MVX versions to the current release.

Procedure

1. Open a command window and navigate to the root directory of your MVX installation.
2. Run the following command to stop the MVX Docker container:
 - a. **For Windows:** `mvx.bat stop`
 - b. **For Linux:** `mvx.sh stop`
3. Run the following command to delete the MVX Docker container:
 - a. **For Windows:** `mvx.bat delete`
 - b. **For Linux:** `mvx.sh deleteimage`
4. Run the following command to delete the MVX Docker image:
 - a. **For Windows:** `mvx.bat deleteimage`
 - b. **For Linux:** `mvx.sh deleteimage`
5. Rename the current `data` directory in the root directory of your MVX installation, or in the same location as your `mvx.ini` setup, to `data.old`
6. Create a new directory named `data` in the root directory of your MVX installation.
7. Remove the existing `mvx.bat` or `mvx.sh` script file from your installation directory.
8. Extract the `mvx_<version>.zip` to a temporary location and copy the files.
9. Do one of the following:
 - a. **For Windows:** From the `\mvxserver\Windows` sub-directory, copy the `mvx.bat` into your existing installation directory.
 - b. **For Linux:** From the `\mvxserver\linux` sub-directory, copy the `mvx.sh` into your existing installation directory.
10. From the `\mvxserver` sub-directory, copy the `mvx-docker-SB-<date>.tar.gz` file to your existing installation directory.
You can remove any old `mvx-docker-SB-<date>.tar.gz` files.
11. Run the following command to load the MVX Docker image:
 - a. **For Windows:** `mvx.bat load <date>`
 - b. **For Linux:** `mvx.sh load <date>`

Where `<date>` is the date portion of the Docker image file name (for example, for the `mvx-docker-SB-12-01-21.tar.gz` file, the date would be specified as `12-01-21`)

Contact support@rocketsoftware.com if you need to restore your RBC registration, user accounts, and instances.

Upgrading from MVX 1.2.0 and performing a Keycloak data migration

When upgrading to the latest version of MVX, you are installing MVX over data that is maintained by a previous version of MVX. Migration of Keycloak user account data is required if you want to maintain Keycloak user accounts that you have set up with your previous MVX installation.

1. Open a command window and navigate to the root directory of your MVX installation.
2. Run the following command to stop the MVX Docker container:
 - a. **For Windows:** `mvx.bat stop`
 - b. **For Linux:** `mvx.sh stop`
3. Run the following command to delete the MVX Docker container:

- a. **For Windows:** `mvx.bat delete`
 - b. **For Linux:** `mvx.sh delete`
4. Run the following command to delete the MVX Docker image:
 - a. **For Windows:** `mvx.bat deleteimage`
 - b. **For Linux:** `mvx.sh deleteimage`
5. Remove the existing `mvx.bat` or `mvx.sh` script file from your installation directory.
6. Extract the `mvx_<version>.zip` to a temporary location and copy the files.
7. Do one of the following:
 - a. **For Windows:** From the `\mvxserver\Windows` sub-directory, copy the `mvx.bat` and `mvx-install-util.sh` into your existing installation directory.
 - b. **For Linux:** From the `\mvxserver\linux` sub-directory, copy the `mvx.sh` and `mvx-install-util.sh` into your existing installation directory.
8. To start your previously installed MVX version, open a command window and navigate to the root directory of that version.

If the Docker image is deleted, run:

- a. **For Windows:** `mvx.bat load 04-22-22 skip-migrate-kc`
- b. **For Linux:** `mvx.sh load 04-22-22 skip-migrate-kc`

If the Docker image is not deleted, run:

- a. **For Windows:** `mvx.bat start`, or `mvx.bat run 04-22-22`
- b. **For Linux:** `mvx.sh start`, or `mvx.sh run 04-22-22`

9. Generate Keycloak 12.0.4 migration data:

- a. **For Windows:** `mvx.bat migrate-kc`
- b. **For Linux:** `mvx.sh migrate-kc`

Once migration is complete, the 04-22-22 container will be stopped and the image will be deleted.

10. From the `\mvxserver` sub-directory, copy the `mvx-docker-SB-<date>.tar.gz` file to your existing installation directory.

You can remove any old `mvx-docker-SB-<date>.tar.gz` files.

11. Load and start the new Docker image:

- a. **For Windows:** `mvx.bat load mm-dd-yy`
- b. **For Linux:** `mvx.sh load mm-dd-yy`

Where `mm-dd-yy` is the timestamp of the new Docker image.

12. The message `Keycloak data migration is pending, continue` will display and you must press **Enter** to complete the Keycloak migration when the new container is run for the first time.

Uninstalling MVX

Complete these instructions to uninstall MVX.

For more information on managing and configuring your Docker image, see [mvx.bat and mvx.sh files](#).

Procedure

1. Open a command window and navigate to the root directory of your MVX installation.
2. Run the following command to stop the MVX docker container:
 - **For Windows:** `mvx.bat stop`
 - **For Linux:** `mvx.sh stop`

3. Run the following command to delete the MVX docker container:
 - **For Windows:** `mvx.bat delete`
 - **For Linux:** `mvx.sh delete`
4. Run the following command to delete the MVX docker image:
 - **For Windows:** `mvx.bat deleteimage`
 - **For Linux:** `mvx.sh deleteimage`

Note: If you want to completely remove all MVX artifacts, delete the entire directory structure where MVX was installed.

Parent topic: [Installing MVX](#)

Chapter 3: Installing MVAdmin

MVAdmin is a key component of the MVX infrastructure. It provides a set of MVAS specific services for MVX such as registration, experience activation, and communication between MVX and MVAS. The files for installing MVAdmin are included in the `.zip` file you downloaded when you installed MVX.

Note: As part of the MVAdmin installation, the following UniVerse file will be replaced on your system:

For Windows implementations, in the `<UV Home Directory>` directory, the `u2modulelist.exe` file is replaced.

Additionally, a new entry is added to the `unirpcservices` file for use by MVAdmin.

- [Installing or upgrading MVAdmin on Windows](#)
Complete these instructions to install or upgrade MVAdmin on Windows.
- [Installing or upgrading MVAdmin on Linux and AIX](#)
Complete these instructions to install or upgrade MVAdmin on Linux or AIX.
- [Anti-CSRF protection in MVX UI/API](#)
Cross-Site Request Forgery (CSRF, or XSRF) is an attack that allows a hacker to perform unauthorized operation by stealing/reusing a user's authenticated session. One of the most used measures to defeat these attacks is the use of anti-CSRF tokens. Beginning at version 1.3.0, MVX uses anti-CSRF tokens to defend against CSRF attacks.
- [Uninstalling MVAdmin](#)
Complete the instructions below for your platform to uninstall MVAdmin.
- [Starting and stopping MVAdmin](#)
You can start and stop MVAdmin from the command line using the `mvadmin.sh` (Linux/AIX) and `mvadmin.bat` (Windows) scripts.

Installing or upgrading MVAdmin on Windows

Complete these instructions to install or upgrade MVAdmin on Windows.

Review the [System Requirements](#) before installing MVAdmin.

Important: Before installing MVAdmin, we highly recommend making the following changes to your UniVerse `uvconfig` file. Note that if you are upgrading your version of MVAdmin, these changes can be skipped as you would have already performed them during your original installation.

- The `uvconfig` `PERF_MON_MODE` parameter must be set to 1 to enable performance monitoring and allow the Performance dashboard to collect and display performance data from MVAdmin. To update the `PERF_MON_MODE` parameter, open the `uvconfig` file and set the `PERF_MON_MODE` parameter to 1.
- After making these changes to the `uvconfig` file, save your changes and then perform the following tasks in this order:
 - Open an elevated command prompt (a command prompt run as administrator) and run the `uvregen` command from UV Home.
 - Stop and restart the UniVerse Resource Service.

Tip: After MVAdmin is installed, if you should ever need to edit the `uvconfig` file, for your changes to take effect, you will need to perform the following tasks in this order:

1. Run the `mvadmin` command to stop MVAdmin.
2. Stop and restart UniVerse.
3. Run the `mvadmin` command again to restart MVAdmin.

See [Starting and stopping MVAdmin, on page 23](#) for more information.

1. If you haven't already done so, obtain the MVX package from the Product Availability feature in Rocket Business Connect. The package is a `.zip` file with the name `mvx_<version>.zip`, where `<version>` is the version and build number of the release (for example, `1.1.1.1000`). Copy the zip file to a directory on your MVAS system (for example, `c:\temp`) and extract it.

This will create a directory structure as illustrated below (assuming you used the `c:\temp` directory to hold the `mvx_<version>.zip`).

```
temp\  
  mvxserver\  
  ...  
  mvadmin\  
    MVAdminSetup.exe  
    mvadmin-linux.tar  
    mvadmin-aix.tar
```

2. Navigate to the unzipped downloaded media file and open the `mvadmin` folder.
3. Double-click the `MVAdminSetup.exe` file.
The MVAdmin InstallShield Wizard displays.
4. Click **Next**.
5. Review the MVAdmin license agreement and select the `I accept the terms of the license agreement` option to agree to the terms of the license agreement. Click **Next**.
6. Select the destination folder where MVAdmin will be installed. The default is `C:\U2\MVAdmin`. Click **Browse ...** if you want to install MVAdmin to an alternate location.

Note:

- The default installation directory is according to the drive on your system where Windows is installed. For example, if Windows is installed on your D: drive, the MVAdmin install will default to D:\U2\MVAdmin.
 - If you are upgrading an existing MVAdmin installation, no changes are required to the destination folder because the system automatically recognizes where MVAdmin was installed previously and uses that folder.
-

Click **Next** when you are done selecting a location.

7. Enter your **Username** and **Password** for your MVAS account and then click **Next**.
-

Note: The **Username** and **Password** being requested is a valid username and password that you use in a UniVerse UniObject connection. These credentials will be used by MVAdmin to access the MVAS.

8. Click **Install** to start the MVAdmin installation process.

When the installation completes, the InstallShield Wizard Complete screen displays.

9. Click **Finish**.

MVAdmin is installed and the MVAdmin Service starts automatically. To confirm that the service has started, open the Windows Services app and find the MVAdmin Service in the Services list. If the service has started, the **Status** for the service will indicate **Running**.

Parent topic: [Installing MVAdmin](#)

Installing or upgrading MVAdmin on Linux and AIX

Complete these instructions to install or upgrade MVAdmin on Linux or AIX.

Review the [System Requirements](#) before installing MVAdmin.

Important: Before installing MVAdmin, we highly recommend making the following changes to your UniVerse `uvconfig` file. Note that if you are upgrading your version of MVAdmin, these changes can be skipped as you would have already performed them during your original installation.

- The `uvconfig` `PERF_MON_MODE` parameter must be set to 1 to enable performance monitoring and allow the Performance dashboard to collect and display performance data from MVAdmin. To update the `PERF_MON_MODE` parameter, open the `uvconfig` file and set the `PERF_MON_MODE` parameter to 1.
- After making these changes to the `uvconfig` file, save your changes and then perform the following tasks in this order:
 - Run the `uvregen` command from UV Home.
 - Stop and restart UniVerse.

Tip: After MVAdmin is installed, if you should ever need to edit the `uvconfig` file, for your changes to take effect, you will need to perform the following tasks in this order:

1. run the `mvadmin` command to stop MVAdmin.
2. Stop and restart UniVerse.
3. Run the `mvadmin` command again to restart MVAdmin.

See [Starting and stopping MVAdmin, on page 23](#) for more information.

1. If you haven't already done so, obtain the MVX package from the Product Availability feature in Rocket Business Connect. The package is a `.zip` file with the name `mvx_<version>.zip`, where `<version>` is the version and build number of the release (for example, 1.1.1.1000). Copy the zip file to a directory on your MVAS system (for example, `/tmp`) and extract it.

This will create a directory structure as illustrated below (assuming you used the `/tmp` directory to hold the `mvx_<version>.zip`).

```
/tmp
/mvxserver
...
/mvadmin
  MVAdminSetup.exe
  mvadmin-linux.tar
  mvadmin-aix.tar
```

2. Navigate to the unzipped downloaded media file and open the `mvadmin` directory.
3. Copy the appropriate `.tar` file (for Linux, `mvadmin-linux.tar`, for AIX, `mvadmin-aix.tar`).
4. Create a new directory to use for installing MVAdmin on the MVAS you want to monitor and then navigate to that new directory and paste the copied `.tar` file in that location.

Note: This directory is only for your temporary use and can be deleted after you complete the install process.

5. Run the `tar -xvf` command from that location to untar the files.
The `setup.sh` install file and `mvadmin_media` directory are added to the directory where you performed the `tar -xvf` command.
6. Update your permissions on the `setup.sh` install file by running the following command:
`chmod a+x setup.sh`

7. Run `./setup.sh` to install MVAdmin.

You will be prompted for the following information:

The license.txt and notices.txt files are located in the mvadmin_media/license directory and will be installed to the root of your installation directory. Please review these two files and accept here if you agree to the terms of these license agreements. Do you agree to the terms of these license agreements? (y/n)	Enter <code>y</code> to accept the terms of the license agreements.
Please input the installation path:	The installation path for MVAdmin. We recommend that you use <code>/usr/mvadmin</code> as the installation path.
MVAdmin is already installed on your system. Do you want to upgrade to the latest version of MVAdmin? (y/n)	This message displays only if an existing version of MVAdmin exists in the path you input above. Enter <code>y</code> to continue with the upgrade installation. Entering <code>n</code> will exit the upgrade process.
Please input user name:	The user name that will be used by MVAdmin to open a connection to your MVAS.
Please input password:	The password for the user name provided in the previous step.
Please confirm password:	Confirm the password provided in the previous step.

Press Enter after responding to each prompt. Upon completion, MVAdmin is installed to the specified path.

Note: After installation, MVAdmin starts automatically. To confirm that MVAdmin has started, run the following command:

- For Linux RHEL 7 or 8 implementations, run `systemctl status mvadmin`
- For Linux RHEL 6 or AIX implementations, run `ps -ef|grep mvadmin`

Parent topic: [Installing MVAdmin](#)

Anti-CSRF protection in MVX UI/API

Cross-Site Request Forgery (CSRF, or XSRF) is an attack that allows a hacker to perform unauthorized operation by stealing/reusing a user's authenticated session. One of the most used measures to defeat these attacks is the use of anti-CSRF tokens. Beginning at version 1.3.0, MVX uses anti-CSRF tokens to defend against CSRF attacks.

Anti-CSRF tokens

Beginning at version 1.3.0, all mutable requests (any method other than GET, HEAD, OPTIONS, and TRACE) will have the correct CSRF token in the X-CSRF-TOKEN header. The token is returned in the XSRF-TOKEN cookie in the response to the initial login request.

The CSRF token is associated with the login session; therefore, its lifetime is the same as that of the session. If a session expires, the token cannot be validated, so a logging in again to create a new session is needed.

Possible Errors related to CSRF handling

The following is a list of errors that may be returned from an anti-CSRF token:

When an anti-CSRF token is not found in a request that requires such tokens, a 403 error message with payload will display, similar to:

```
{ "errorCode": 403, "errorMessage": "Invalid CSRF Token 'null' was found on the request parameter '_csrf' or header 'X-CSRF-TOKEN'." }
```

When a token is invalid or otherwise does not match the one associated with the session, a 403 error message with payload will display, similar to:

```
{ "errorCode": 403, "errorMessage": "Invalid CSRF Token 'd68af793-cdf7-46f9-8a12-2f4a18b1aad9' was found on the request parameter '_csrf' or header 'X-CSRF-TOKEN'." }
```

When a session is invalid or a null session cookie is sent, the response will have a 403 status code, and the following payload:

```
{ "errorCode": 403, "errorMessage": "Could not verify the provided CSRF token because your session was not found." }
```

When a session is expired, you will receive a 403 status code and payload:

```
{ "errorCode": 403, "errorMessage": "Session is invalid or timed out, require re-login" }
```

Parent topic: [Installing MVAdmin](#)

Uninstalling MVAdmin

Complete the instructions below for your platform to uninstall MVAdmin.

Uninstalling MVAdmin on Windows

To uninstall MVAdmin on Windows, open the Control Panel and click **Programs and Features**. Select MVAdmin from the list of programs and click **Uninstall**.

Uninstalling MVAdmin on Linux or AIX

To uninstall MVAdmin on Linux or AIX, run the following commands (depending on the Linux or AIX version you have installed). Note that these commands assume you have MVAdmin installed to the /usr/mvadmin directory. If you installed MVAdmin to a different directory, adjust these commands accordingly.

For Linux 7.x and 8.x

```
systemctl stop mvadmin
systemctl disable mvadmin
rm /etc/systemd/system/mvadmin.service
```

```
rm -rf /usr/mvadmin
```

For AIX

```
rmitab mvadmin  
rm -rf /usr/mvadmin
```

Parent topic: [Installing MVAdmin](#)

Starting and stopping MVAdmin

You can start and stop MVAdmin from the command line using the `mvadmin.sh` (Linux/AIX) and `mvadmin.bat` (Windows) scripts.

Starting and stopping MVAdmin is performed using the `mvadmin` command, which also allows you to check whether MVAdmin is currently running and change your password if the password has expired. The syntax for this command is:

```
mvadmin.sh|mvadmin.bat start|stop|status|password
```

This command is run from the root directory of your MVAdmin installation.

Note: On Windows, when starting or stopping MVAdmin, the `mvadmin.bat` file must be run from an elevated command prompt (a command prompt run as administrator).

- To start MVAdmin, run the following command:
For Windows: `mvadmin.bat start`
For Linux/AIX: `mvadmin.sh start`
- To stop MVAdmin, run the following command:
For Windows: `mvadmin.bat stop`
For Linux/AIX: `mvadmin.sh stop`
- To check whether MVAdmin is currently running, run the following command:
For Windows: `mvadmin.bat status`
For Linux/AIX: `mvadmin.sh status`
- To change the MVAdmin password in cases where the password has expired, run the following command:
For Windows: `mvadmin.bat password`
For Linux/AIX: `mvadmin.sh password`

Note: You will be prompted to enter and confirm the new password.

Parent topic: [Installing MVAdmin](#)

Chapter 4: Configuring MVX

- [Logging in to Keycloak for the first time](#)
After MVX is installed, the system administrator in your organization responsible for MVX administrative functions should log into Keycloak and change the default Keycloak Administration Console password.
- [Configuring MVX log files](#)
The MVX installation creates two log files named `mvx.log` and `audit.log` in the `mvx/data/logs/` directory of your MVX installation.
- [Configuring MVAdmin log files](#)
The MVAdmin installation creates one log file named `mvadmin.log` in the `mvadmin/logs/` directory of your MVAdmin installation.
- [Keycloak log files](#)
Keycloak log files are stored in the `data/keycloak/log` directory of your MVX installation.
- [Configuring performance snapshot data storage](#)
You can configure the length of time the MVAdmin server will store performance metrics snapshot objects in the `PERFHIST` data file.
- [Updating the credentials for application server connections in MVAdmin](#)
If the username and password for your MultiValue Application Server account should change, you will need to update those credentials in MVAdmin.
- [Changing your MVAdmin UI login credentials](#)
The default username and password used to access the MVAdmin UI are `admin` and `admin`. Use this procedure to change these credentials to something more private and secure.

Logging in to Keycloak for the first time

After MVX is installed, the system administrator in your organization responsible for MVX administrative functions should log into Keycloak and change the default Keycloak Administration Console password.

The default Keycloak Administration Console username is *admin* and the default password is also *admin*. After installing MVX, your MVX system administrator should log in to Keycloak and change the Keycloak Administration Console password to something more private and secure.

Procedure

1. To access the Keycloak Administration Console, open a browser and go to the following URL:
`https://<your_host_name>:9543`
where *<your_host_name>* is your machine's host name and 9543 is the default port used by MVX to communicate with Keycloak.
2. Click **Administration Console** and then enter the default admin username and password (*admin* & *admin*) in the **Username or email** and **Password** text boxes of the **Sign in to your account** dialog box. Click **Sign In**.
The Keycloak Administration Console displays.
3. Select **Master** from the realm drop-down menu (top of the side menu panel).
4. Select **Users** from the **Manage** menu in the side menu panel.
The Users screen display.
5. From the **Lookup** tab of the Users screen, click the ID link for the Username *admin*.
The Admin screen displays.

6. Select the **Credentials** tab and then enter your new password in the **Password** and **Password Confirmation** text boxes.
7. Select **OFF** from the **Temporary ID** slider.
8. Click **Reset Password**.

The Keycloak Administration Console password is updated.

Parent topic: [Configuring MVX](#)

Configuring MVX log files

The MVX installation creates two log files named `mvx.log` and `audit.log` in the `mvx/data/logs/` directory of your MVX installation.

The `mvx.log` file receives and stores various messages from Spring and MVX. The `audit.log` file receives and stores MVX authentication and authorization messages.

The logging behavior for messages source, categories and levels are configured from the `[LOGGING]` properties section of the `mvx.properties` file (located in the `mvx/data/config/` directory of your MVX installation).

Log file archiving is configured from the `logback-spring.xml` file which is also located in the `mvx/data/config/` directory. This file contains two appender sections near the end of the document named `AUDIT-LOG` and `FULL-LOG` which control the archiving behavior with the following properties:

<code><maxFileSize></code>	Maximum file size in MB that the currently active log file can reach before being archived. The default value is 100 MB.
<code><maxHistory></code>	Maximum number of archive files to keep in the logs directory. If the number of archived files reaches or exceeds the specified maximum, the oldest files will be removed asynchronously. For example, if you specify a daily roll-over, and set <code><maxHistory></code> to 15, only the 15 newest daily logs will be kept. The default value is 30.
<code><totalSizeCap></code>	Maximum size of all archived log files. The oldest files will be removed asynchronously when the total size cap is exceeded. This value specified for this property only applies when <code><maxHistory></code> is set. <code><maxHistory></code> is always applied first. The default value is 5 GB.

By default, the `logback-spring.xml` file rolls-over daily or when the file reaches the size specified in the `<maxFileSize>` property, whichever comes first. If you want to set your logs to roll over weekly or monthly, you can change the `<fileNamePattern>` property as follows:

- **For weekly roll-overs:** `${logging.path}/archived/mvx.%d{yyyy-ww}.%i.log.gz`
- **For monthly roll-overs:** `${logging.path}/archived/mvx.%d{yyyy-MM}.%i.log.gz`

Note: Any changes you make to the `logback-spring.xml` file will take effect on the next MVX start.

Parent topic: [Configuring MVX](#)

Configuring MVAdmin log files

The MVAdmin installation creates one log file named `mvadmin.log` in the `mvadmin/logs/` directory of your MVAdmin installation.

The `mvadmin.log` file receives and stores various messages from Spring and MVAdmin.

The logging behavior for messages source, categories and levels are configured from the [LOGGING] properties section of the `mvadmin.properties` file (located in the root directory of your MVAdmin installation).

Log file archiving is controlled by the `logback-spring.xml` file. Note that this file is not exposed in this release and cannot be configured by the user. The `logback-spring.xml` file contains an appender section near the end of the document named `FULL-LOG` which controls general MVAdmin archiving behavior with the following properties:

<code><maxFileSize></code>	Maximum file size in MB that the currently active log file can reach before being archived. The default value is 100 MB.
<code><maxHistory></code>	Maximum number of archive files to keep in the logs directory. If the number of archived files reaches or exceeds the specified maximum, the oldest files will be removed asynchronously. For example, if you specify a daily roll-over, and set <code><maxHistory></code> to 15, only the 15 newest daily logs will be kept. The default value is 30.
<code><totalSizeCap></code>	Maximum size of all archived log files. The oldest files will be removed asynchronously when the total size cap is exceeded. This value specified for this property only applies when <code><maxHistory></code> is set. <code><maxHistory></code> is always applied first. The default value is 5 GB.

By default, the `logback-spring.xml` file rolls-over daily or when the file reaches the size specified in the `<maxFileSize>` property, whichever comes first.

Parent topic: [Configuring MVX](#)

Keycloak log files

Keycloak log files are stored in the `data/keycloak/log` directory of your MVX installation.

There are two Keycloak log files: `server.log` and `audit.log`. These files are compressed and archived daily. However, if you have to restart MVX at any time, each time you perform the restart a new compressed archive is created.

Archived logs are gzip compressed and named using the following format:

```
server.log.yyyy-xx-dd.gz
```

where `yyyy` indicates the year and `dd` indicates the day the log was created. Note that the `xx` is a random set of digits and does not represent the month. Archived logs more than 14 days old are automatically removed from the system.

Parent topic: [Configuring MVX](#)

Configuring performance snapshot data storage

You can configure the length of time the MVAdmin server will store performance metrics snapshot objects in the `PERFHIST` data file.

The `db.instance.snapshot.interval` and `db.instance.snapshot.history` properties in the `dbinst_1.properties` file allow you to configure the length of time the MVAdmin server will store performance metrics snapshot objects in the `PERFHIST` data file.

1. Navigate to the root folder of your MVAdmin installation and open the `dbinst_1.properties` file for editing.

2. Locate the *db.instance.snapshot.interval* and *db.instance.snapshot.history* properties and edit the values as appropriate for your implementation.

<i>db.instance.snapshot.interval</i>	Specifies how often (in seconds) the MVAdmin server takes a performance metrics snap shot and saves the object into the <code>PERFHIST</code> data file. The default is 900 (15 minutes).
<i>db.instance.snapshot.history</i>	Specifies the number of days the MVAdmin server will keep the historic snapshot objects to prevent the <code>PERFHIST</code> data file from growing too large. The default is 30 days.

3. Save the `dbinst_1.properties` file.
4. Restart MVAdmin for your changes to take effect.

Parent topic: [Configuring MVX](#)

Updating the credentials for application server connections in MVAdmin

If the username and password for your MultiValue Application Server account should change, you will need to update those credentials in MVAdmin.

Procedure

1. Open a browser and log into the MVAdmin UI using the following URL:
`https://<dataserver-hostname>:8383`
 where `<dataserver-hostname>` is the hostname for the dataserver and 8383 is the default port used by MVAdmin.
2. Enter the MVAdmin UI username and password. The default username and password are *admin* and *admin*.

Note: When logging into the MVAdmin UI, a security warning indicating that your connection is not private may display in your browser. This occurs because MVAdmin by default uses a self-signed certificate. If you want to install your own SSL certificate, the `mvx.bat` and `mvx.sh` scripts include the `(setuptls)` command for setting up certificates. For more information on using this command, contact support@rocketsoftware.com.

3. Click **Configuration** to open the MV Admin Server Configuration screen.
4. From the Accounts section, click the Edit account icon associated to the **dbservices** row.
5. From the Account Configuration dialog box, enter the new username and password for the application server account in the **Username** and **Password** text boxes and the click **Test Connection** to confirm the credentials are correct.
6. Click **Save** to save the new credentials.

Parent topic: [Configuring MVX](#)

Changing your MVAdmin UI login credentials

The default username and password used to access the MVAdmin UI are *admin* and *admin*. Use this procedure to change these credentials to something more private and secure.

Procedure

1. Navigate to the root directory of your MVAdmin installation and open the `mvadmin.properties` file.
2. From the *Auth* properties section of the file, change the *auth.user* property to the new username.
3. Save and close the `mvadmin.properties` file.
4. To change and encrypt your password, from the root directory of your MVAdmin installation, run the following command:
 - For Windows: `.\mvadmin password`
 - For Linux or AIX: `./mvadmin.sh password`
5. Enter and confirm the password when prompted. This will encrypt and save the new password into the *auth.password* property of the `mvadmin.properties` file.

Note: After saving the `mvadmin.properties` file, for the changes to take effect, you will need to perform the following tasks in this order:

- a. Run the `mvadmin` command to stop MVAdmin.
- b. Stop and restart UniVerse.
- c. Run the `mvadmin` command again to restart MVAdmin.

See [Starting and stopping MVAdmin, on page 23](#) for more information.

Parent topic: [Configuring MVX](#)

Chapter 5: SuperAdmins and user account management

The role of SuperAdmin owns the responsibility of setting-up and maintaining MVX user accounts and their roles.

After installing your MVX system, the first person to log into the system will be the individual that will act as the SuperAdmin. The SuperAdmin has the responsibility of setting-up user accounts for all MVX users in their organization.

Roles

User accounts are assigned by role which controls what the user can and cannot do in the MVX application. the three types of user roles are:

SuperAdmin:

- Configure MVX and MVAdmin
- Register MVX
- Register and deregister instances
- Ignore and re-activate events and change event thresholds from the event threshold YAML file
- View, accept as task, snooze, ignore events from the Events to review table and change event thresholds from the Events Manager
- Delete incomplete tasks from the Tasks to complete table and complete, delete and change event thresholds from the Tasks Manager
- Create and edit user accounts and edit their own account

Admin:

- Register and deregister instances
- View, accept as task, snooze, ignore events from the Events to review table and change event thresholds from the Events Manager
- Delete incomplete tasks from the Tasks to complete table and complete, delete and change event thresholds from the Tasks Manager
- Edit their own account

Viewer:

- View, accept as task, snooze, ignore events from the Events to review table and change event thresholds from the Events Manager
- Delete incomplete tasks from the Tasks to complete table and complete, delete and change event thresholds from the Tasks Manager
- Edit their own account

Logging in as SuperAdmin for the first time

The first time you log in as the SuperAdmin user, there are a number of important steps to take to begin setting-up your system.

MVX is shipped with Keycloak, which is configured with one existing user with the SuperAdmin role. This existing SuperAdmin user has the default username of *superadmin* and the default password of

superadmin. It also contains pseudo first and last names and emails. After logging in, the password should be changed to a password of your choosing, and the first and last names and email should be changed to your name and emails. Additionally, your RBC credentials should be added.

Note: Network access to <https://rbc.rocketsoftware.com:7171> is required to log in.

Procedure

1. Open a browser and type `https://localhost:nnnn` in the address bar where *nnnn* is the port number (the default port 9243, unless it has been changed in the `mvx.ini` file). This will open the MVX log on screen.
2. Log into MVX using the default username *superadmin* and the default password *superadmin*. The MVX Registration dialog box displays.
3. Enter your RBC ID, password and serial number in the **RBC ID**, **RBC Password** and **Serial Number** text boxes and then click Register.
If registration is successful, the Rocket MV Experience UI displays, and you will see a confirmation message:

```
Product registration complete. You have successfully registered MVX.
```
4. Click the Your Account icon  and select **My Account**.
The My Account Settings dialog box displays.
5. Select **Account** from the side panel menu.
6. Type your first and last name in the **First name** and **Last name** text boxes.
7. Type your primary email and optionally a secondary email in the **Primary email** and **Secondary email** text boxes.
8. Click the **Change Password** button.
9. Type your current password (*superadmin*) in the Current Password text box and then type your new password in the **New Password** and **Confirm Password** text boxes.
10. Click **Submit & Close**.
Your profile changes are saved.
11. Select **RBC Credentials** from the side panel menu.
12. Type your RBC ID and password in the **RBC ID** and **RBC Password** text boxes. If you are unsure of the RBC ID and password registered with RBC, contact your RBC Business Administrator: rbc@rocketsoftware.com.
13. Click **Submit & Close**.
Your account changes and RBC credentials are saved.

Important: It is also important that you change the Keycloak client secret after the initial MVX installation. See [Changing the Keycloak client secret, on page 34](#) for more information.

Creating user accounts

You can add new user accounts to the MVX system.

New MVX users must have an RBC account registered in RBC before you can add them in MVX. If you need information on users registered with RBC, contact your RBC Business Administrator: rbc@rocketsoftware.com.

Procedure

1. Select **User Accounts** from the **Administration** menu.
2. Select **Create User** from the **Action** drop-down.
The **Create User Account** dialog box displays.
3. Fill in the following fields:

Table 1:

First name	User's first name.
Last name	User's last name.
User role	Viewer, Admin or SuperAdmin. See SuperAdmins and user account management, on page 29 for more information.
Primary email	Primary email for the user.
Secondary email	Secondary email for the user.
RBC ID	RBC ID activated within RBC. You can either choose to provide the RBC ID and password, or allow the new user to provide when they log in to the system. If you need information on users registered with RBC, contact your RBC Business Administrator: rbc@rocketsoftware.com . Important: To function properly, MVX requires a persistent internet connection with Rocket Business Connect (RBC). MVX calls out to RBC to register the MVX serial number and to check whether the UniVerse server to be monitored is on Active Maintenance. If MVX is unable to establish and maintain an active connection with RBC, after several warning messages, MVX will cease to function.
RBC Password	User's RBC password.
Enable User	Select or deselect the Enable User check box to initially enable or disable the new user account in the MVX system.
Username	Username the user will use when logging on to MVX.
Temporary Password	Temporary password the user will use when logging on to MVX.
Confirm Temporary Password	Confirm the temporary password the user will use when logging on to MVX.

4. When you are done creating the new user account, click **Create New User & Close**. If you want to create another user account, click **Save and Create Another User** instead.

The new user account is created and added to the **User Accounts** table. If you clicked **Save and Create Another User**, a new Create User Account dialog box displays for you to add an additional new user account.

Editing user accounts

You can edit a user's name, role, primary email, secondary email and whether they are enabled or disabled on the MVX system.

Procedure

1. Select **User Accounts** from the **Administration** menu.
2. Select the user account you want to edit from the **User Accounts** table.
3. Select **Edit User** from the **Action** drop-down.
The Edit User Account dialog box displays.
4. Edit any of the following fields:
 - First name
 - Last name
 - User role
 - Primary email
 - Secondary email
5. Select or deselect the **Enable User** check box to enable or disable the user account in the MVX system.
6. When you are done making your edits to the user account, click **Submit & Close**.
The user account is updated in the MVX system.

Enabling and disabling user accounts

User access to the MVX system can be enabled or disabled. Note that disabling a user account is a temporary action and the user is not deleted from the MVX system.

Procedure

1. Select **User Accounts** from the **Administration** menu.
2. Select the user account you want to enable or disable from the **User Accounts** table.
3. Select **Enable/Disable User** from the **Action** drop-down.
The specified user account's status is toggled to either the enabled or disabled status. For example, selecting the **Enable/Disable User** option on a currently enabled user account will change its status to disabled. Conversely, selecting the **Enable/Disable User** option on a currently disabled user account will change its status to enabled.

Deleting user accounts

You can delete user accounts from the MVX system. Once a user is deleted, they will no longer have access to your MVX system.

Procedure

1. Select **User Accounts** from the **Administration** menu.
2. Select the user you want to delete from the **User Accounts** table.
The Delete User prompt displays.
3. Click **Delete**.

The user is deleted and will no longer have access to your MVX system.

Resetting user passwords

If a user forgets their password, you can reset their password on their behalf and they can subsequently change this new password to a password of their choosing.

Procedure

1. Select **User Accounts** from the **Administration** menu.
2. Select the user whose password you want to reset from the **User Accounts** table.
3. Select **Reset Password** from the **Action** drop-down.
4. Type and confirm a new password in the **New Password** and **Confirm New Password** text boxes.
5. Click **Reset Password**.

The user's password is reset.

Tip: It is recommended to inform the user that they can now change the new password to a password of their choosing from the **Account** option of their My Account Settings dialog.

Resetting the SuperAdmin password

If a SuperAdmin loses or forgets their password, they can reset the password from the Keycloak Administration Console.

Procedure

1. To access the Keycloak Administration Console, open a browser and go to the following URL:
`https://<your_host_name>:9543`
where `<your_host_name>` is your machine's host name and 9543 is the default port used by MVX to communicate with Keycloak.
2. Click **Administration Console** and then enter the default admin username and password (*admin* & *admin*, unless you reset these previously) in the **Username or email** and **Password** text boxes of the **Sign in to your account** dialog box. Click **Sign In**.
The Keycloak Administration Console displays.
3. Select **Users** from the **Manage** menu in the side menu panel.
The Users screen displays.
4. From the **Lookup** tab of the Users screen, click the **View all users** button to display the list of all users defined on the MVX system.
5. Click the ID link for the Username *superadmin*.
The Admin screen displays.
6. Select the **Credentials** tab and then enter your new password in the **Password** and **Password Confirmation** text boxes.
7. Select **OFF** from the **Temporary ID** slider.
8. Click **Reset Password**.
The SuperAdmin password is updated.

Changing the Keycloak client secret

The Keycloak application installed with MVX is configured with two pre-created admin clients: *mvxapp* and *mvadminapp*. These clients are used internally by MVX to perform various user management operations and are created with default client secrets, which function similar to user passwords. Both of these default client secrets should be changed after your initial MVX installation.

Changing the Keycloak client secret requires logging into the Keycloak Administration Console as well as using the `mvx.bat` or `mvx.sh` scripts provided with MVX. You must have the SuperAdmin role to perform this task.

Procedure

1. To access the Keycloak Administration Console, open a browser and go to the following URL:
`https://<your_host_name>:9543`
 where `<your_host_name>` is your machine's host name and 9543 is the default port used by MVX to communicate with Keycloak.
2. Click **Administration Console** and then enter the default admin username and password (*admin* & *admin*) in the **Username or email** and **Password** text boxes of the **Sign in to your account** dialog box. Click **Sign In**.
 The Keycloak Administration Console displays.
3. Select **Mvx** from the realm drop-down menu (top of the side menu panel).
4. Select **Clients** from the **Configure** menu in the side menu panel.
 The Clients screen displays.
5. Do one of the following:
 - If you are changing the mvxapp client secret, click **mvxapp** from the list of Client IDs to display the Mvxapp screen.
 - If you are changing the mvadminapp client secret, click **mvadminapp** to display the Mvadminapp screen.
6. Click the **Credentials** tab and then click the **Regenerate Secret** button to create a new client secret.
7. Copy the new client secret from the **Secret** text box.
8. Open a command prompt and navigate to the root directory of your MVX installation.
9. Run one of the following commands depending on your implementation:
 - For Windows: `mvx.bat config clientsecret`
 - For Linux: `mvx.sh config clientsecret`
10. Enter your username and password. The default user name and password for a user in the SuperAdmin role is *superadmin* and *superadmin*. However, if you have already changed these credentials, enter your new credentials instead.
 The following prompt displays:
 Input keycloak admin client name mvxapp(1) or mvadminapp(2): [1/2]
11. Enter 1 or 2, depending on whether you are changing the mvxapp or mvadminapp client secret.
 The following prompt displays:
 Input keycloak admin client secret
12. Paste the new client secret you copied earlier in this task and then press Enter.
 The following message displays:
 Client secret updated
 Please restart MVX for it to take effect

Caution: Once you have updated both the mvxapp or mvadminapp client secrets, you must restart MVX for your changes to take effect. Failure to do so will result in losing your client secret changes, which may result in subsequent login failures.

Chapter 6: Managing your account

Use the My Account Management feature to change your username or password, setup your RBC credentials and create event notifications.

To open the My Account Settings dialog box, click the Your Account icon  and select **My Account**.

Managing your account profile

You can make changes to your name, primary and secondary emails, and change the password to your account.

You cannot make changes to your MVX role or your username. If you need to change either of these, contact your SuperAdmin.

Tip: Click the **Save Progress** button at any time to save your settings. Once you've saved your progress, you can navigate to other side panel menu features if you like. However, to complete your work, you will need to click **Save & Close**. Any work you've saved using the **Save Progress** button will be lost if you close the My Account Settings dialog box before clicking **Save & Close**.

Procedure

1. Click the Your Account icon  and select **My Account**.
The My Account Settings dialog box displays.
2. Select **Account** from the side panel menu.
3. Make your desired changes to any of the following text boxes.
 - First name
 - Last name
 - Primary email
 - Secondary email
4. To change your password, click the **Change Password** button. Enter your current password and then enter and confirm your new password.
5. Click **Submit & Close**.
Your profile changes are saved.

Entering your RBC credentials

To activate your MVX system to access the Performance Experience, you'll need to provide your RBC credentials.

If you don't know your RBC credentials, contact your SuperAdmin.

Important:

- In some cases, your SuperAdmin may have entered your RBC credentials on your behalf when creating your account. If that is the case, there is no need to complete these steps as your system is already activated.
- To function properly, MVX requires a persistent internet connection with Rocket Business Connect (RBC). MVX calls out to RBC to register the MVX serial number and to check whether the UniVerse server to be monitored is on Active Maintenance. If MVX is unable to establish and maintain an active connection with RBC, after several warning messages, MVX will cease to function.

Tip: Click the **Save Progress** button at any time to save your settings. Once you've saved your progress, you can navigate to other side panel menu features if you like. However, to complete your work, you will need to click **Save & Close**. Any work you've saved using the **Save Progress** button will be lost if you close the My Account Settings dialog box before clicking **Save & Close**.

Procedure

1. Click the Your Account icon  and select **My Account**.
The My Account Settings dialog box displays.
2. Select **RBC Credentials** from the side panel menu.
3. Enter your RBC ID in the **RBC ID** text box.
4. Enter your RBC password in the **RBC Password** text box.
5. Click **Submit & Close**.
Your system is authorized to access the Performance Experience.

Managing subscriptions

You can subscribe to receive real-time notifications or daily, weekly or monthly reports for any performance events that occur on your system.

You can create as many event subscriptions as you like.

Tip: Click the **Save Progress** button at any time to save your settings. Once you've saved your progress, you can navigate to other side panel menu features if you like. However, to complete your work, you will need to click **Save & Close**. Any work you've saved using the **Save Progress** button will be lost if you close the My Account Settings dialog box before clicking **Save & Close**.

Procedure

1. Click the Your Account icon  and select **My Account**.
The My Account Settings dialog box displays.
2. Select **Subscriptions** from the side panel menu.
3. Click the plus button (+) to add a new row to the Event Subscriptions table and then click the edit icon (pencil).

Note: To save your new subscription, all fields must be completed.

4. Enter a name for the subscription in the **Report Name** text box.
 5. Select the email to send notifications to from the **Email** drop-down.
 6. Select the event severity to use from the **Event Severity** drop-down. Available severity options are `critical`, `medium`, `low` and `all`. If you select `critical`, `medium` or `low`, then you *only* receive notifications when events of those severities occur on your selected instance. If you select `all`, then you will receive notifications for all events on your selected instance, regardless of the severity.
 7. Select the notification frequency from the **Send Frequency** drop-down. Available frequency options are `immediate`, `daily`, `weekly` and `monthly`. If you select `immediate`, you will receive an email notification whenever a new event of your selected severity occurs on your selected instance.
 8. Select the instance whose events will trigger the notifications from the **Instance Scope** drop-down.
 9. Click **Submit & Close**.
- Your event subscription is started.

Note: If you should need to delete a subscription, click the delete icon corresponding to the subscription you want to delete from the **Event Subscription** table and then click **Submit & Close**.

Chapter 7: MVX User Guide

This user guide discusses all the information you need to provision a new instance of a MultiValue Application Server (MVAS).

Use this section to learn how to sign into the MVX Experience console, change your container's MVX password, register and deprovision an existing instance of a MVAS.

- [Logging-in](#)
Local operating system users can log into the Rocket MV Experiences console when running in a container using their defined MVX username and password.
- [Registering an existing MultiValue Application Server instance](#)
Registering a server identifies an existing MultiValue Application Server (MVAS) instance to the MVX system. Once a server has been registered, the MVX system will be able to communicate with the server and perform various tasks such as status checks and performance monitoring.
- [Instance Details dashboard](#)
The Instance Details dashboard provides an overview of a registered MV instance and includes a toggle for enabling reporting performance data to the MultiValue Performance Experience.
- [MVX Performance Dashboard](#)
The MVX Performance dashboard is accessed from the **Performance** tab on the Instance Details page of a registered MV instance. This dashboard provides a facility to monitor the system for various conditions, such as file size problems, excessive locks, peak license usage, and others.

Logging-in

Local operating system users can log into the Rocket MV Experiences console when running in a container using their defined MVX username and password.

Note: If you attempt to log into MVX before your SuperAdmin has performed the initial setup of the MVX system, your log in attempt will fail with an error message.

Procedure

1. Open a browser and type `https://localhost:nnnn` in the address bar where `nnnn` is the port number (the default port 9243, unless it has been changed in the `mvx.ini` file). This will open the MVX log on screen.

Note: The default port for MVX is 9243. If you choose not to use `https://localhost`, be sure to point to the machine where you're running MVX.

Note: When logging into the MV Experiences console, a security warning indicating that your connection is not private may display in your browser. This occurs because MVX by default uses a self-signed certificate. If you want to install your own SSL certificate, the `mvx.bat` and `mvx.sh` scripts include the `(setuptls)` command for setting up certificates. For more information on using this command, contact support@rocketsoftware.com.

2. Type your username and password that have been defined for MVX and click **Login**.

Note: The first time you log into MVX after installing, the interface may take 15 or 20 seconds to load. Load times in subsequent logins will be much quicker.

Parent topic: [MVX User Guide](#)

Registering an existing MultiValue Application Server instance

Registering a server identifies an existing MultiValue Application Server (MVAS) instance to the MVX system. Once a server has been registered, the MVX system will be able to communicate with the server and perform various tasks such as status checks and performance monitoring.

All servers that are to be used by MVX must be registered prior to use. Once a server has been registered, it will remain in the MVX system until unregistered.

Users with the role of Viewer are not allowed to register or de-register an existing MVAS instance. Only users with the roles of Admin and SuperAdmin can register or de-register an instance.

Prerequisites

- Confirm you are running the supported OS and UniVerse version. Without the proper versions, MVX will be unable to run. See [System Requirements](#) for information on the supported OS and UniVerse versions.
- From the installation media, download and install MVAdmin in the same environment as the MVAS and then start MVAdmin. See [Installing MV Admin](#) for more information.

Procedure

1. From the Instances dashboard, click **Register existing instance**.

The Register existing instance dialog box displays.

Tip: Click the How to register button to review and confirm you have met the operating system and UniVerse version minimum requirements and the MVAdmin requirements.

2. Enter a name to use for the MVAS instance you are registering and the host machine on which it resides in the **Instance Name** and **Host Machine Name** text boxes.

Note:

- Since MVX is running a Linux container, specifying localhost as the **Host Machine Name** will fail because this is resolved to the Linux installation in the Docker container. To access UniVerse on the same machine as the MVX server is running, you need to specify the machine name or its IP address.
- When specifying the MVAS name to register, the process will use the DNS server settings defined in your `mvx.ini` file. If you need the MVX Server to use the local hosts file, then you must set the `UseHostNetwork` parameter in your `mvx.ini` file to yes. Once this is done, you will need to create a new container for the change to be recognized. Run the following commands to create the new container (where `<date>` is the date of the image from which to create the container):

For Windows

```
mvx.bat stop
mvx.bat delete
mvx.bat run <date>
```

For Linux

```
mvx.sh stop
mvx.sh delete
mvx.sh run <date>
```

3. Select a purpose for registering this instance from the **Purpose** drop-down.

Note: The port numbers shown in the **Admin Port** and **UniVerse Port** text boxes are the default ports used to connect to MVAdmin and UniVerse. These should not be changed from the default values.

4. Click **Register**.
The MVAS instance is registered and the instance tile displays in the Instances screen.

Note: To deregister an instance, from the Instances dashboard, click the vertical ellipses menu button for the instance you want to deregister and select **Deregister**. Click **Deregister** to confirm.

Parent topic: [MVX User Guide](#)

Instance Details dashboard

The Instance Details dashboard provides an overview of a registered MV instance and includes a toggle for enabling reporting performance data to the MultiValue Performance Experience.

To view the Instance Details dashboard for a registered MV instance, from the Instances screen, click the **View** button for the Instance you want to display.

The following information is displayed in the Instance Details dashboard:

- the number of users licensed on the MultiValue server
- the version of the MultiValue server

- the platform on which the MultiValue server is running
- the enabled and disabled licensing packages on the MultiValue server

To enable reporting performance data to the MultiValue Performance Experience, from the MultiValue Experience Enablement section, click the **Performance** toggle **On**.

Note: Users assigned to the Viewer role cannot enable or disable the MultiValue Performance Experience. Only users assigned to the Admin or SuperAdmin roles can perform this action.

Parent topic: [MVX User Guide](#)

MVX Performance Dashboard

The MVX Performance dashboard is accessed from the **Performance** tab on the Instance Details page of a registered MV instance. This dashboard provides a facility to monitor the system for various conditions, such as file size problems, excessive locks, peak license usage, and others.

To view the Performance dashboard for a registered MV instance, from the Instances screen, click the **View** button for the instance you want to display and then select the Performance tab.

Note: To view performance data for your instance, you need to enable the MultiValue Performance Experience. To enable the MultiValue Performance Experience, from the MultiValue Experience Enablement section of the Details tab, click the **Performance** toggle **On**.

Use this section to learn how to review and manage performance impacting events that are occurring on the MVAS registered with MVX. You will also learn how to review information on the users and processes currently consuming resources on your system.

The Performance dashboard in version 1.1.1 includes three monitoring tiles:

- Events
- MV Sessions
- Locks
- Host CPU/Memory

Parent topic: [MVX User Guide](#)

Events

The Events monitoring tile lists all performance impacting events that are occurring on the MVAS registered with MVX.

The Events tile displays the current number of performance impacting events. Active performance impacting events are displayed in the **Events to review** table, which provides the event severity, title (type), specifics and date for each event in the table. The severity of each event is indicated with the following icons:

	Critical
	Medium
	Low

The **Events to review** table allows you to review all current events and then select whether to snooze, ignore or accept an event as a task. Events can be filtered by Type, Severity and their current Status.

Clicking an event from the **Events to review** table displays the **Event Manager** panel. The **Event Manager** panel provides the definition of the event, includes additional information that was captured at the time the event triggered, some suggested tasks to take to remedy the event, and the ability to configure the event threshold to a more appropriate level to avoid a recurring event. You can also select whether to snooze, ignore or accept an event as a task from the **Event Manager** panel.

Tip: Click the **Additional Details** button to display additional data on the event such as record lock held details and port status output.

Events that are accepted as tasks transition from the **Events to review** table to the **Tasks to complete** table. Events in the **Tasks to complete** table can be filtered by Severity or deleted using the **Actions** menu. Clicking an event from the **Tasks to complete** table displays the **Task Manager**, which provides additional information on that event type along with an editable checklist of suggested actions to take to remedy the event. The **Task Manager** also allows you to configure event thresholds to a more appropriate level to avoid recurring events.

Reviewing events

The **Events to review** table displays all performance impacting events that are occurring on the MVAS registered with MVX.

This topic describes how to review and manage events in the events list.

Procedure

1. From the **Performance** tab, select the **Events** tile.

The **Events to review** and **Tasks to complete** tables display.

Tip:

- Use the left and right arrows at the bottom of the **Events to review** table to page through the list of events.
 - Use the up/down arrows in the column headings to sort the **Events to review** table by Type, Title or Date.
 - Click the Filter button to filter displayed events by Severity, Status or Type.
 - Click an event from the **Events to review** table to display the **Event Manager** panel which provides additional information on that event type along with some suggested actions to take to remedy the event.
-

2. Review the events currently displayed in the **Events to review** table and decide what action to take. The quick actions you can perform are:
 - **Accept as Task:** Indicates that the event should be addressed and resolved (for example, when you need to resize a file for *file undersized events* or when correcting an application problem that caused a lock event). Selecting this option transitions the event from the **Events to review** table to the **Tasks to complete** table where you can take actions to remedy the event. See [Managing event tasks](#) for more information.
 - **Snooze:** Indicates that the event is not ready to be worked on (for example, when a file that needs to be resized, but can't be resized while the system is busy). Selecting this option removes the event from the **Events to review** table for a period of 24 hours. If after 24 hours this event were to occur again, the event will be redisplayed in the **Events to review** table.

Snoozed events can be reactivated by selecting the **Ignored** check box from the Events to review filter and then selecting the **Reactivate** option from the **Actions** menu associated to the snoozed event.

- **Ignore:** Indicates that the event doesn't pose a serious problem to the system and can safely be ignored for 48 hours (for example, during busy times of the day when many user sessions are active, a high license usage event may be raised - but it will subside later in the day as the number of active sessions drops). Selecting this option removes the event from the **Events to review** table for a period of 48 hours. If after 48 hours this event were to occur again, the event will be redisplayed in the **Events to review** table.

Note: A snapshot of contextually relevant data captured at the moment the specific event triggered is also available to help the user with troubleshooting. This snapshot can be accessed by selecting the **Additional Details** button from the **Event Manager**. The same data is carried forward when an event is converted to a task, and is available from the **Additional Details** button of the **Task Manager**.

3. When you've decided what quick action you want to take for an event, click the **Actions** drop-down menu for the specific event and select the action you want to perform.

Managing tasks

The **Tasks to complete** table displays the performance impacting events that you have accepted as a task. It includes the action required for the task, the numbers of days the task is past due (since you accepted the event as a task) and the number of times this particular event has recurred since you accepted the event as a task (events that recur multiple times should be addressed as they may affect system performance).

This topic describes how to review and manage tasks. It assumes that you have already committed to addressing the escalated issues from one or more events as a task from the **Events to review** table. See [Reviewing events](#) for more information.

Procedure

1. From the **Performance** tab, select the **Events** tile.
The **Events to review** and **Tasks to complete** tables display.

Tip:

- Use the left and right arrows at the bottom of the **Tasks to complete** table to page through the list of events.
 - Use the up/down arrows in the column headings to sort the **Tasks to complete** table by Type, Action Required or Past Due date.
 - Click the Filter button to filter displayed tasks by Severity.
 - If you decide you no longer need to complete a task, click the **Delete** button from the **Action** menu.
-

2. Click a task from the **Tasks to complete** table to display the **Task Manager** panel. Like the **Event Manager**, this panel provides the definition of the event, includes additional information that was captured when the event triggered, some suggested tasks to take to remedy the event and the ability to configure event thresholds to a more appropriate level to avoid recurring events.

3.

Tip: Click the **Additional Details** button to display additional data on the task such as file reads blocked details and port status output.

4. Review and perform the suggested tasks. As you complete each suggested task, select the task's check box to indicate that the task has been completed.

Tip: If you have performed another additional task (one that is not listed in the suggested tasks list), type a description of the task in the **Additional task done to solve Performance issue** text box and select the associated check box.

5. If you need to change the event threshold for this task, change the threshold to the appropriate value from the **Change event threshold** panel.

Note: If at any point you decide you want to discontinue this task, click the **Delete Incomplete Task** button to discontinue your work and delete the task.

6. To complete your task, click **Complete! Inform & Educate Engine**. This allows us to collect the necessary data and evaluate the actions you completed (as indicated by the check boxes selected). This collected data and its analysis will be incorporated into future versions of this product to inform and drive personalized recommendations.

Event definition files

Event definition files contain detailed information about an event including event threshold values.

Event definition files are formatted as YAML files and are located in the `MVAdmin/events` directory. These files can be manually edited if you need to update the threshold value for any event type.

Caution: Take great care when editing these files as introducing a syntax error could prevent MVX (the MVAdmin service) from reading the file.

Note: If you edit any of the event definitions, the MVAdmin service must be restarted for the changes to take effect.

Threshold properties, which include the threshold name, data type and value, are defined in the `eventParams` section of the file. For example, the `UniVerseFileUndersizedWarning` event definition is found in the `UniVerseFileUndersizedWarning.yaml` file and the `eventParams` section of that file contains the following threshold properties:

```
eventParams:
- name: undersizedBufferScanRatioTriggerThreshold
  type: percent
  value: 15%
```

MVX comes with the following default values for the following event types:

OSProcessCpuUsage

The Process CPU Usage event is generated when a process's CPU usage is higher than the `cpuUsageTriggerThreshold`. This event will auto-clear when a process's CPU usage drops below the `cpuUsageClearThreshold`.

```
eventParams:
```

- name: cpuUsageTriggerThreshold
type: percent
value: 80%
- name: cpuUsageClearThreshold
type: percent
value: 50%

OSProcessHandleUsage (Windows only)

The Process Handle Usage event is generated when process handle usage is higher than the handleUsageTriggerThreshold. This event will auto-clear when process handle usage drops below the handleUsageClearThreshold.

- ```
eventParams:
- name: handleUsageTriggerThreshold
 type: double
 value: 10000

- name: handleUsageClearThreshold
 type: double
 value: 10000
```

### OSProcessMemoryUsage

The Process Memory Usage event is generated when a process's memory usage is higher than the memoryUsageTriggerThreshold. This event will auto-clear when a process's memory usage drops below the memoryUsageClearThreshold.

- ```
eventParams:  
- name: memoryUsageTriggerThreshold  
  type: percent  
  value: 80%  
  
- name: memoryUsageClearThreshold  
  type: percent  
  value: 80%
```

OSSystemCacheFaults

The Cache Faults event is generated when system cache faults exceeds the cacheFaultsTriggerThreshold for the sampling period. This event will auto-clear when system cache faults drops below the cacheFaultsClearThreshold for the sampling period.

- ```
eventParams:
- name: cacheFaultsTriggerThreshold
 type: double
 value: 10000

- name: cacheFaultsClearThreshold
 type: double
 value: 10000

- name: samplingPeriod
 type: timePeriod
```

---

```
value: 5 Minutes
```

## OSSystemCpuQueueLength

The CPU Queue Length event is generated when the CPU queue length (run queue) is higher than the `queueLengthTriggerThreshold`. This event will auto-clear when the CPU queue length drops below the `queueLengthClearThreshold`.

---

**Tip:** When this event is generated, the system can optionally generate an email notification of the event to MVX users. See [Managing subscriptions](#) for more information.

---

```
eventParams:
- name: queueLengthTriggerThreshold
 type: int
 value: 3
```

```
eventParams:
- name: queueLengthClearThreshold
 type: int
 value: 3
```

## OSSystemCpuUsage

The High CPU Usage event is generated when the average CPU usage for the sampling period is higher than the `processorTimeTriggerThreshold`. This event will auto-clear when the average CPU usage in the sampling period drops below the `processorTimeClearThreshold`.

---

**Tip:** When this event is generated, the system can optionally generate an email notification of the event to MVX users. See [Managing subscriptions](#) for more information.

---

```
eventParams:
- name: processorTimeTriggerThreshold
 type: percent
 value: 80%
```

```
eventParams:
- name: processorTimeClearThreshold
 type: percent
 value: 80%
```

```
eventParams:
- name: samplingPeriod
 type: timePeriod
 value: 5 Minutes
```

## OSSystemDiskQueueLength (Windows only)

The Disk Queue Length event is generated when disk queue length is longer than the `diskQueueLengthTriggerThreshold` for the sampling period. The disk queue length is the number of disk operations waiting to be serviced by the disk subsystem. A high number could indicate that the disk subsystem is a bottleneck. This event will auto-clear when disk queue length drops below the `diskQueueLengthClearThreshold` for the sampling period.

```
eventParams:
```

- name: diskQueueLengthTriggerThreshold  
type: double  
value: 10
- name: diskQueueLengthClearThreshold  
type: double  
value: 5
- name: samplingPeriod  
type: timePeriod  
value: 5 Minutes

## OSSystemDiskUsage

The Disk Usage event is generated when disk space usage is higher than the `diskSpaceUsageTriggerThreshold` for the sampling period. This event will auto-clear when disk space usage drops below the `diskSpaceUsageClearThreshold` for the sampling period.

- ```
eventParams:  
- name: diskSpaceUsageTriggerThreshold  
  type: percent  
  value: 80%  
  
- name: diskSpaceUsageClearThreshold  
  type: percent  
  value: 70%  
  
- name: samplingPeriod  
  type: timePeriod  
  value: 5 Minutes
```

OSSystemMemoryUsage

The High Memory Usage event is generated when the average memory usage for the sampling period exceeds the `memoryUsageTriggerThreshold`. This event will auto-clear when the average memory usage drops below the `memoryUsageClearThreshold`.

Tip: When this event is generated, the system can optionally generate an email notification of the event to MVX users. See [Managing subscriptions](#) for more information.

- ```
eventParams:
- name: memoryUsageTriggerThreshold
 type: percent
 value: 95%

eventParams:
- name: memoryUsageClearThreshold
 type: percent
 value: 95%

eventParams:
- name: samplingPeriod
 type: timePeriod
```

---

```
value: 5 Minutes
```

## OSSystemNonPagedMemoryUsage (Windows only)

The Non-Paged Memory Usage event is generated when non-paged memory usage is higher than the nonPagedMemoryUsageTriggerThreshold for the sampling period. This event will auto-clear when non-paged memory usage drops below the nonPagedMemoryUsageClearThreshold for the sampling period.

```
eventParams:
- name: nonPagedMemoryUsageTriggerThreshold
 type: percent
 value: 50%

- name: nonPagedMemoryUsageClearThreshold
 type: percent
 value: 50%

- name: samplingPeriod
 type: timePeriod
 value: 5 Minutes
```

## OSVMUsage

The VM Usage event is generated when virtual memory usage (Windows: Paging file / Unix: Swap space) is higher than the VMUsageTriggerThreshold for the sampling period. This event will auto-clear when virtual memory usage drops below the VMUsageClearThreshold for the sampling period.

```
eventParams:
- name: VMUsageTriggerThreshold
 type: percent
 value: 95%

- name: VMUsageClearThreshold
 type: percent
 value: 80%

- name: samplingPeriod
 type: timePeriod
 value: 5 Minutes
```

## UniVerseConnectionPoolLicenseLimitWarning

```
eventParams:
- name: connectionLicenseUsageTriggerThreshold
 type: percent
 value: 80%
```

## UniVerseFileBlockedReadsWarning

```
eventParams:
- name: blockedReadsTriggerThreshold
 type: percent
```

```
value: 5%
```

### UniVerseFileBlockedWritesWarning

```
eventParams:
- name: blockedWritesTriggerThreshold
 type: percent
 value: 0%
```

### UniverseFileLockedWarning

```
eventParams:
- name: uvFileLockHoldTimeTriggerThreshold
 type: timePeriod
 value: 10 Minutes
```

### UniVerseFileOversizedReadWarning

```
eventParams:
- name: oversizedReadWarningTriggerThreshold
 type: percent
 value: 15%
```

### UniVerseFileOversizedWriteWarning

```
eventParams:
- name: fileOversizedWriteWarningTriggerThreshold
 type: percent
 value: 10%
```

### UniverseFilePoolUsage

The UniVerse File Pool Usage event is generated when the file pool temp\_close counter is higher than the filePoolUsageTriggerThreshold. This indicates that the UniVerse open file table size should be increased to support the number of files being used by the application. The size of this table is set by the `uvconfig MFILES` parameters. This event will auto-clear when the file pool temp\_close counter drops below the filePoolUsageClearThreshold.

```
eventParams:
- name: filePoolUsageTriggerThreshold
 type: double
 value: 60

- name: filePoolUsageClearThreshold
 type: double
 value: 50
```

### UniVerseFileSeparationWarning

```
eventParams:
- name: oversizedIORatioTriggerThreshold
 type: percent
```

---

```
value: 20%
```

## UniVerseFileUndersizedWarning

```
eventParams:
- name: undersizedBufferScanRatioTriggerThreshold
 type: percent
 value: 15%
```

## UniverseGroupLockHoldWarning

```
eventParams:
- name: uvGroupLockHoldTimeTriggerThreshold
 type: timePeriod
 value: 1 Minute
```

## UniVerseLicenseLimitWarning

```
eventParams:
- name: licenseUsageTriggerThreshold
 type: percent
 value: 80%
```

## UniverseLockBucketHighNodeUsageWarning

```
eventParams:
- name: lockNodesUsedPercentTriggerThreshold
 type: percent
 value: 70%
```

## UniVerseLockRequestWaitingWarning

```
eventParams:
- name: uvLockRequestWaitingTriggerThreshold
 type: timePeriod
 value: 1 Minute
```

## UniverseLockTableMaxedOutWarning

```
eventParams:
- name: bucketUsagePercentTriggerThreshold
 type: percent
 value: 50%
```

## Editing event definition files

Complete these instructions to edit the threshold properties of an event definition file.

This example illustrates editing the `UniVerseConnectionPoolLicenseLimitWarning.yaml` file.

## Procedure

1. Navigate to the `MVAdmin/events` directory in the root MVAdmin installation directory.
2. Open the `UniVerseConnectionPoolLicenseLimitWarning.yaml` file in an editor.
3. Locate the `eventParams` section of the file, and from there the `connectionLicenseUsageTriggerThreshold` property. Make the desired change to the percent value for this property.

---

**Note:** All events have a corresponding `ClearThreshold` property (for example, `connectionLicenseUsageClearThreshold`). `ClearThreshold` properties are not currently used by MVX, and can be ignored.

---

4. When you are done making your edits, save the file.
5. Restart MVAdmin. See [Starting and stopping MVAdmin](#) for more information.

## Configuring the accounts that are monitored

You can configure which accounts will be monitored for file related performance events.

By default, MVX file related performance events are generated for all accounts. However, you can specify which accounts to monitor for such events. The file related events are:

- `UniVerseFileUndersizedWarning`
- `UniVerseFileSeparationWarning`
- `UniVerseFileOversizedReadWarning`
- `UniVerseFileOversizedWriteWarning`
- `UniVerseFileBlockedReadsWarning`
- `UniVerseFileBlockedWritesWarning`

These file related event files are formatted as YAML files and are located in the `MVAdmin/events` directory. These files can be manually edited.

---

**Caution:** Take great care when editing these files as introducing a syntax error could prevent MVX (the MVAdmin service) from reading the file.

---



---

**Note:** If you edit any of the event definitions, the MVAdmin service must be restarted for the changes to take effect.

---

The event *level* property can be set to *Server* or *Account*. If set to *Server*, events are generated for all accounts. If set to *Accounts*, events are generated only for the accounts specified in the *acctName* and *acctPath* properties of the event *accounts* property.

The example below illustrates using the `UniVerseFileUndersizedWarning.yaml` file to specify that a file undersized event should only be generated if the file is in the XDEMO or HS.SALES accounts:

1. Navigate to the `MVAdmin/events` directory in the root MVAdmin installation directory.
2. Open the `UniVerseFileUndersizedWarning.yaml` file in an editor.

3. Locate the level property in the file and edit the property as follows:

```
level: Account
accounts:
- acctName: XDEMO
 acctPath: C:\U2\UV\XDEMO
- acctName: HS.SALES
 acctPath: C:\U2\UV\HS.SALES
```

---

**Note:** Each *acctName* must be preceded with a dash (-) to conform to YAML syntax.

---

4. Save the file and restart MVAdmin for your changes to take effect.

## MV Sessions

The MV Sessions monitoring tile provides insight on the users and processes currently consuming resources on your system.

The MV Sessions monitoring tile and drill-through provides the following information:

- The MV Sessions tile displays the number of active sessions logged in the MVAS and also the license consumption as a percentage and number.
- The MV Sessions table provides additional insight into each of the active sessions by providing the Process ID (PID), Username, User Type, Account Name, Last Cmd, License Taken and Login start date, time and duration.

---

**Tip:** You can download the MV Sessions table as a `.csv` file to your `Downloads` folder by clicking the Download button adjacent to the **Global Search** box. To download a specified subset of the results displayed in the MV Sessions table, type a search string in the **Global Search** box. This search string finds any string existing in any column of the MV Sessions table.

---

- The License Usage chart records license usage over a specified period of time including information on the total licenses available and peak licenses in use. The available display options are Current Day, Current Week, Current Month, Last Month and Custom Range (allows you to specify a start and end date).

## Reports

You can display a report for a specific PID in your browser by clicking the **Report** drop-down menu for the PID and selecting **View Report**. The report opens in a new tab in your browser and includes the following tabs:

- **File Metrics:** Displays the File Name, File Path, Opens, Reads, Writes, Deletes, Overflow %, Split and Merge for the specific PID.
- **File Locks:** Displays the File Name, PID, Lock Owner, Lock Type, Record ID, Lock Time and Waiters for File/Record locks and displays the File Name, PID, Lock Owner, Lock Type, G-Address and Lock Time for Group locks.
- **OS Metrics:** For Linux implementations, displays the User, Command, CPU%, CPU Usage, Elapsed Time, Priority, Memory %, Resident Set Size (kb) and Virtual Memory Size (kb) for the specific File/Record lock. For Windows implementations, displays the Command, Elapsed Time, Memory (kb), CPU %, Paged Pool Usage (kb), Non Paged Pool Usage (kb), Page Faults (/sec), Handles and Page File Usage (kb) for the specific File/Record lock.
- **Call Stack** Displays the Layer Type, Program Name and Address for the most recent functions that have been called on the PID.

---

**Note:** To download the report as a `.xlsx` file to your **Downloads** folder, click the **Report** drop-down menu for the PID and select **Download**.

---

## Locks

The Locks tile provides insight on the file, record and group locks being applied.

The Locks tile and drill-through provides the following information:

- The Locks tile provides the number of group and record locks currently active.
- The File/Record Locks table lists the currently active file and record locks and provides the File Name, File Path, Process ID (PID), Lock Owner, Lock Type, Record ID, Lock Time and Lock Waiters (PIDs in waiting for the locked file or record). Lock types are presented as two-digit codes with the following definitions:

File Lock Types

- FS: Shared
- FX: Exclusive
- IX: Intent

Record Lock Types

- RL: Shared
- RU: Exclusive

---

**Tip:** You can download the File/Record Locks table as a `.csv` file to your **Downloads** folder by clicking the Download button adjacent to the **Global Search** box. To download a specified subset of the results displayed in the File/Record Locks table, type a search string in the **Global Search** box. This search string finds any string existing in any column of the File/Record Locks table.

---

- The Group Locks table lists the currently active group locks and provides the File Name, File Path, Process ID (PID), Lock Owner, Lock Type, G-Address (group address) and Lock Time for each lock. Lock types are presented as two-digit codes with the following definitions:
  - RD: Read
  - WR: Write

---

**Tip:** You can download the Group Locks table as a `.csv` file to your **Downloads** folder by clicking the Download button adjacent to the **Global Search** box.

---

---

**Tip:** The data in the File/Record Locks table and the Group Locks table can be sorted by clicking the column headings.

---

## Reports

You can display a report for a specific File/Record or Group lock in your browser by clicking the **Report** drop-down menu for the File/Record or Group lock and select **View Report**. The report opens in a new tab in your browser and includes the following tabs:

- **File Metrics:** Displays the File Name, File Path, Opens, Reads, Writes, Deletes, Overflow %, Split and Merge for the specific File/Record lock.

- **File Locks:** Displays the File Name, File Path, PID, Lock Owner, Lock Type, Record ID, Lock Time and Waiters for File/Record locks and displays the File Name, File Path, PID, Lock Owner, Lock Type, G-Address and Lock Time for Group locks.
- **OS Metrics:** For Linux implementations, displays the User, Command, CPU%, CPU Usage, Elapsed Time, Priority, Memory %, Resident Set Size (kb) and Virtual Memory Size (kb) for the specific File/Record lock. For Windows implementations, displays the Command, Elapsed Time, Memory (kb), CPU %, Paged Pool Usage (kb), Non Paged Pool Usage (kb), Page Faults (/sec), Handles and Page File Usage (kb) for the specific File/Record lock.
- **Call Stack** Displays the Layer Type, Program Name and Address for the most recent functions that have been called.

---

**Note:** To download that report as a .csv file to your Downloads folder, click the Download button from the report or click the **Report** drop-down menu for the File/record or Group lock and select **Download**.

---

## Host CPU/Memory

The Host CPU/Memory tile provides insight into current memory and CPU usage on your system and allows you to identify any issues that are impacting system performance.

The Host CPU/Memory tile provides the following information:

- The Host CPU/Memory tile provides:
  - current percentage of CPU in use
  - percentage of memory in-use for your system (Windows only)
  - number of currently queued processes

This tile automatically refreshes the CPU data every 3 seconds and the memory data every 60 seconds.

- The CPU Utilization table displays:
  - current percentage of User and System CPU usage
  - Total CPU usage (representing the combined percentage of User and System CPU usage)
  - percentage of CPU usage that is currently Idle
  - I/O Wait percentage for each CPU on your system

The Total row aggregates each of these percentages for all CPU's on your system. This table automatically refreshes the data every 3 seconds.

- The Memory Utilization table displays:
  - current physical and virtual memory being utilized both as a percentage and in MB
  - current physical and virtual memory that is free (in MB)
  - current Cache Size (or Pin for AIX implementations)

This table automatically refreshes the data every 60 seconds.

- The Processes table displays the 10 most active CPU and memory processes on the system and includes the following information:

**For Linux and AIX:**

- the Process ID (PID)
- the Process Name (name and the location where the process is running)
- the User Name of the user running the process
- the Elapsed time that the process has been running
- the percentage of CPU and Memory being used for the process
- the amount of physical and virtual memory (in KB) being used for the process

**For Windows:**

- the Process ID (PID)
- the Process Name (name and the location where the process is running)
- the Elapsed time that the process has been running
- the percentage of CPU and Memory being used for the process
- the amount of physical and virtual memory (in KB) being used for the process
- the handle count
- the number of page faults per second

Click the arrow (>) from the PID column to display the top 10 CPU or Memory processes. This table automatically refreshes the data every 60 seconds.

# Appendix A: mvx.bat and mvx.sh files

The `mvx.bat` and `mvx.sh` files are used to load, run, start, stop or perform other Docker image management operations.

A Windows `.bat` file (`mvx.bat`) and a Linux `.sh` script file (`mvx.sh`) are provided for managing the Docker image. Both of these utilities use the `mvx.ini` configuration file which must exist in the same directory as the downloaded Docker image and the `mvx.bat` or `mvx.sh` file. See [mvx.ini configuration file](#) for more information.

## mvx.bat and mvx.sh command syntax

### Syntax Version 1

```
mvx.bat|mvx.sh load <date> | run <date> | start | stop | status |
delete | deleteimage
```

### Syntax Version 2

```
mvx.bat|mvx.sh config timeout | smtp | setuptls
```

### Parameters

| Parameter      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| load <date>    | Loads the specified image where <date> is the date portion of the Docker image file name (for example, for a file named <code>mvx-docker-SB-12-01-21.tar.gz</code> , the date would be specified as 12-01-21).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| run <date>     | Runs a previously loaded image to start new container where <date> is the date portion of the Docker image file name (for example, for a file named <code>mvx-docker-SB-12-01-21.tar.gz</code> , the date would be specified as 12-01-21).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| start          | Starts a previously stopped container. The message <code>MOVX system has been fully started</code> displays when both the container and the MOVX system have been completely started.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| stop           | Stops a previously started container.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| status         | Provides the status of a container (running or stopped).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| delete         | Deletes a previously created container.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| deleteimage    | Deletes a previously loaded image.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| config timeout | Specifies a new session inactive timeout value. The default is 1800 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| config smtp    | Allows you to setup and configure your SMTP email server for notifications. You will be prompted for the following information: <ul style="list-style-type: none"><li>▪ <b>Enter host name:</b> Host name for your SMTP server.</li><li>▪ <b>Enter Port:</b> Port number used by your SMTP server.</li><li>▪ <b>Enable SSL:</b> Specifies whether or not to use an SSL connection. Valid responses are true or false.</li><li>▪ <b>Enable SMTP Authentication:</b> Specifies whether or not to enable authentication. Valid responses are true or false. If set to true, then you will be prompted for a username and password (see below).</li><li>▪ <b>Enter username:</b> Username to use for SMTP authentication.</li><li>▪ <b>Enter password:</b> Password to use for SMTP authentication.</li><li>▪ <b>Enter email address:</b> The <i>from</i> email address to use for notifications.</li></ul> |

| Parameter              | Description                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| config<br>setuptls     | Allows you to setup and configure TLS for your system. For more information on using this command to install your own SSL certificate, contact <a href="mailto:support@rocketsoftware.com">support@rocketsoftware.com</a> .                                                                                                                                                                                      |
| config<br>clientsecret | Whenever you change the Keycloak mvxapp or mvadminapp client secret from the Keycloak Administration Console, you will need to inform the MVX and MVAdmin servers of the change. You will be prompted for your username and password and the new client secret. Only users with the SuperAdmin role can perform this task. See <a href="#">Changing the Keycloak client secret, on page 34</a> for more details. |

# Appendix B: mvx.ini configuration file

The `mvx.ini` file contains parameters for configuring your MVX server.

Depending on your platform, the `mvx.ini` file will be called by the `mvx.bat` or `mvx.sh` file when loading, running, starting, stopping or performing other Docker image management operations. The `mvx.ini` file must exist in the same directory as the downloaded Docker image and the `mvx.bat` or `mvx.sh` files. See [mvx.bat and mvx.sh files](#) for more information.

## mvx.ini configuration file parameters

| Parameter  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WebPort    | Port that Docker will use for the connection. The default is 9243. The MVX server listens on port 9243, but if your machine already has another process listening on 9243, use this parameter to configure a different port number.                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| DataDir    | <p>Data directory to use to store configuration and log files for MVX. This should be the full path to (and including) the data directory that you created when installing MVAdmin.</p> <p><b>Note:</b> If DataDir is not specified:</p> <ul style="list-style-type: none"><li>▪ Windows will automatically create the files in the <code>%SystemDrive%\programdata\rocketsoftware\mvx</code> directory.</li><li>▪ Linux will automatically create the files in the <code>/opt/rocketsoft/mvx/data</code> directory</li></ul>                                                                                                                                                 |
| DNS        | <p>The IP address for the Docker Container to use as its DNS Server. The IP address can be obtained by:</p> <ul style="list-style-type: none"><li>▪ <b>For Windows:</b> running the <code>ipconfig /all</code> command and checking the DNS Servers entry</li><li>▪ <b>For Linux:</b> opening and finding the IP address in the <code>/etc/resolv.conf</code> file and checking the nameserver entry</li></ul> <p><b>Note:</b> If more than one DNS server is listed, select the appropriate server that will allow MVX to resolve the domain names of the data servers it will be connecting to. You may need to consult your system administrator for this information.</p> |
| DNSSearch0 | <p>Domain name to use as the suffix in a name lookup. The domain can be obtained by:</p> <ul style="list-style-type: none"><li>▪ <b>For Windows:</b> running the <code>ipconfig /all</code> command and checking the DNS Suffix Search List</li><li>▪ <b>For Linux:</b> opening and finding the domain name in the <code>/etc/resolv.conf</code> file and checking the search entry</li></ul> <p><b>Note:</b> If more than one DNS suffix search entry is required, you can also use the <code>DNSSearch1</code> entry property.</p>                                                                                                                                          |
| DNSSearch1 | <p>Optional - Domain name to use as an additional DNS search suffix in a name lookup. The domain can be obtained by:</p> <ul style="list-style-type: none"><li>▪ <b>For Windows:</b> running the <code>ipconfig /all</code> command and checking the DNS Suffix Search List</li><li>▪ <b>For Linux:</b> opening and finding the domain name in the <code>/etc/resolv.conf</code> file and checking the search entry</li></ul>                                                                                                                                                                                                                                                 |

| Parameter      | Description                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UseHostNetwork | If UseHostNetwork is set to no (default), the MVX Server uses your configured DNS entries to resolve host names. If set to yes, then the MVX Server will use the local hosts file on the system to resolve the host names. In this release, setting the value to yes will disable the ability to change the port number(s) defined in the <code>mvx.ini</code> file thus the MVX Server will run using the default port numbers. |