

Community Manager

Release Notes

Version 11.6.12
December 2020

Table of Contents

System requirements.....	3
CM hardware and software requirements.....	3
Lifecycle Manager software requirements.....	5
Documentation.....	6
What's new.....	6
Enhancements in version 11.6.12.....	6
Fixes in version 11.6.12.....	6
Functional impact topics.....	7
Configuring the Executive dashboard.....	7
Setting email options for use with OAuth2.0 authentication mode.....	7
Enabling Microsoft 365-OAuth2.0 for a specific email address for Incoming Email.....	8
Assigning multiple CM tasks to the same LM(e) task.....	9
Enabling Transport Layer Security protocol (TLS) version 1.2.....	9
Downloading and installing IBM Data Server Runtime client version 11 (applies to LM(e) Server running on Linux).....	9
Installing or upgrading CM.....	10
About this task.....	10
Prerequisites.....	10
Procedure.....	11
Migrating CM 11.6.05 data from an SQL Server 2016 computer to CM 11.6.12 on an SQL Server 2019 computer.....	12
About this task.....	12
Prerequisites.....	12
Procedure.....	12

System requirements

Community Manager is a web-based application that runs on Microsoft Windows Server computers and works with Rocket Lifecycle Manager Enterprise Edition or IBM i Edition servers. The size of your self-service community informs the hardware capacity.

CM hardware and software requirements

Confirm that the computer where you plan to install or upgrade CM meets the following requirements.

Platform	<p>You must install:</p> <ul style="list-style-type: none"> Windows Server® (64-bit hardware only) versions 2019, 2016, 2012 R2, or 2012, with latest updates Apache Tomcat® version 9 (64-bit) <p>The CM installation program changes the Tomcat server configuration. If the current Tomcat server instance also serves other applications, the CM change will disrupt service for those applications.</p> <p>To avoid this condition, we recommend installing an instance of Tomcat server exclusively for CM by downloading the .zip file instead of the packaged installer. Later, during the CM installation, you provide path information to redirect CM to the dedicated Tomcat server instance.</p> <p>The recommendation is the same for both new installations and upgrades.</p> <ul style="list-style-type: none"> [OpenJDK version 11 (64-bit)] <p>Install OpenJDK according to the instructions provided with its download.</p>
File System	NTFS-formatted hard drive
Web Server	Internet Information Services (IIS) v7-8.5

Database	Microsoft SQL Server¹
Version	<p>Microsoft SQL Server 2019, 2017, 2016, 2014, 2012 – licensed edition with latest updates</p> <p>For SQL Server and CM installed on different computers: Install the SQL Server Native Client version 11.0 on the CM computer before installing or upgrading CM. To obtain the latest ENU\x64\sqlncli.msi, visit https://www.microsoft.com/en-us/download/details.aspx?id=50402.</p> <p>For information about enabling Transport Layer Security protocol (TLS) 1.2, see ENABLING TRANSPORT LAYER SECURITY PROTOCOL (TLS) VERSION 1.2 on page 9.</p>
Hardware 1 – 20 users ²	<p>SQL Server on a different server:</p> <ul style="list-style-type: none"> 4 GB RAM 1 Xeon® or Opteron™ 2.4 GHz processor or better 20 GB disk space

Database	Microsoft SQL Server¹
Hardware 1 – 20 users ²	SQL Server on the same server: <ul style="list-style-type: none"> • 4 – 8 GB RAM • 1 – 2.4 GHz processor or better • 20 GB disk space
Hardware 21 – 50 users ²	SQL Server on a different server: <ul style="list-style-type: none"> • 4 GB RAM • 2 – 2.4 GHz processor or better • 40 GB disk space

Hardware 21 – 50 users ²	SQL Server on the same server: <ul style="list-style-type: none"> • 4 – 8 GB RAM • 2 – 2.4 GHz processor or better • 40 GB disk space
Hardware Large Volume 51+ Users ²	See the SUGGESTED HARDWARE BASED ON VOLUME chart on page 4.
Email Management	<ul style="list-style-type: none"> • SMTP for email notification (as provided by Microsoft Exchange) • Lotus Domino® POP/IMAP/IMAP-SSL/Microsoft365-OAuth 2.0 for incoming email processing (as provided by Microsoft Exchange and Lotus Domino)
Client Platform	Any supported web browser as defined below. Java version OpenJDK 11 or higher required. For client specifications, refer to the BMC Client Management Technical Specifications.
Web Browser	Microsoft Internet Explorer® 9*, 10*, and 11*, Mozilla® Firefox®, Google Chrome, and Safari® 5.0.x on Mac OS®. *Internet Explorer 10 and 11 are supported in 11.6.01 and later only. Internet Explorer 9 requires compatibility mode.

Suggested hardware based on volume

# of Users ²	Windows 32 or 64 Bit
1-20	4 GB RAM 1 – Xeon or Opteron 2.4 GHz processor or better
21-50	4 GB RAM 2 – Xeon or Opteron 2.4 GHz processor or better
51-150	8 GB RAM 4 – Xeon or Opteron 2.4 GHz processor or better

# of Users ²	Windows 32 or 64 Bit
151-249	8 GB RAM 8 – Xeon or Opteron 2.4 GHz processor or better
250-500	16 GB RAM 16 – Xeon or Opteron 2.4 GHz processor or better
501+	32 GB RAM 32 – Xeon or Opteron 2.4 GHz processor or better
Sample Server for Large Volume ³	HP ProLiant DL500 series, IBM x3850 X5 or Dell® PowerEdge R200 for up to 150 users. HP Integrity Servers, IBM x3950 R2, or Dell PowerEdge R900 for over 150 users.

(1) Use of CM with Microsoft SQL Server may require additional Microsoft licenses. For more information, contact [Microsoft](#).

(2) The number of users refers to the average number of concurrent users on the system at any one time. This should include agents and 1-2 percent of the total number of customers (if using CM for customer service). So, if you have 20 agents and 1000 customers using customer self-service, 30-40 users should be counted. This is only a rough guide. Actual load on the system is dependent upon your usage of CM.

The hardware requirements for large volume usage assume a 2-server install with both the application and database server matching the suggested specifications.

(3) “Sample Server” is not intended to be an inclusive list of authorized hardware or vendors, but examples of possible servers that can be used.

Note: Dual and Quad Core CPUs are equivalent to 2 and 4 processors respectively. 4 Processors can be 4 single CPUs, 2 Dual Core, or 1 Quad Core.

Lifecycle Manager software requirements

To use CM with Lifecycle Manager servers, either or both of the following software products must be installed, configured, and operating on computers in the same local area network as the CM server computer:

- Lifecycle Manager (Enterprise Edition) version 6.6 or later
- Lifecycle Manager (IBM i Edition) version 8.2B or later

Documentation

CM version 11.6.12 is functionally equivalent to the 11.6.05 version. The documentation for features and function is unchanged and remains labeled as version 11.6.05.

Use the information provided in **INSTALLING OR UPGRADING CM** on page 10 of this document to guide your CM installation or upgrade activities. Do not follow the setup instructions in the unchanged CM 11.6.05 documents. However, you might want to use them for information about installation-related choices that are not covered here.

The changes in the new version are either in support of newer versions of required platform software, or fixes. Any information requirements associated with the updated infrastructure or fixes are covered in this release notes document.

What's new

This release of Community Manager includes infrastructure support enhancements and general maintenance fixes.

Enhancements in version 11.6.12

CM 11.6.12 supports the Microsoft 365-OAuth 2.0 authorization framework (Modern Authentication) for Exchange Web Services (EWS) to access Exchange Online for incoming email.

Fixes in version 11.6.12

Category	Title/Description	ID
Documentation	<p>Update Help for changing Chrome pop-up blocker</p> <p>The CM help topic about disabling pop-up blockers now includes instructions for the current versions of Chrome.</p>	ALCM-5853
Escalation	<p>502 error on save of new issue by customer when user is member of multiple workspaces with different address books</p> <p>New issues can now be saved without generating the 502 bad gateway error.</p>	ALCM-6919

Functional impact topics

The information in this section covers installation, configuration, or end use activities that are affected by the infrastructure changes in CM 11.6.11 and CM 11.6.12.

Of these instruction sets, review and address only those that apply to your setup.

Configuring the Executive dashboard

A CM Administrator user who attempts to run reports on the Executive Dashboard with **Reports > Executive Dashboard** might receive the following error:

```
Following error occurred: GeneralError: Failed to get SecureKey 0
```

Follow these instructions to set up the default service.

Procedure

1. Open the Windows server Services tab and select **Footprints Tomcat Service**.
 - a. Open its **Properties** dialog box.
 - b. On the **General** tab, set its Startup type to `Disabled`.
 - c. Select **OK** to save the changes and dismiss the **Properties** dialog.
2. In your services list, select **Apache Tomcat 9.0 Tomcat9**:
 - a. Open its **Properties** dialog box.
 - b. On the **General** tab, set its Startup type to `Automatic` and select **Apply**.
 - c. On the **Log On** tab, set it to run as the `Local System` account and select **Apply**.
 - d. Select **OK** to save the changes and dismiss the **Properties** dialog.
 - e. Restart the Apache Tomcat service.

You can now successfully open the Executive Dashboard.

Setting email options for use with OAuth2.0 authentication mode

If you wish, you can add configuration options to the **MrlocalDefs** file to affect email processing when OAuth2.0 authentication mode is used. This is optional.

```
$OAuth_page_size = 10;
```

Set the paging size for OAuth2. The default paging size is 10.

```
$Print_Oauth_msg_content = 1;
```

A value of 1 prints the contents of the message file to the debug log. The default is 0.

MrlocalDefs is located in `installFolder\cgi\`, for example, `C:\FootPrintsServiceCore\cgi\`.

Enabling Microsoft 365-OAuth2.0 for a specific email address for Incoming Email

Prerequisites

- You must have created a mail account on your server and at least one customer account.
- Your IT team must have created the Client ID, Client Secret, and Tenant ID and provided you with those values. If your IT team is unfamiliar with setting up Microsoft 365-OAuth2.0, refer them to these Microsoft links:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis>

Procedure

1. Log in to CM and select **Administration | System | Features | Email** from the CM toolbar.
2. In the Incoming Email section, click the **Configure Incoming Email** button.
3. On the Incoming Email Setup page, click the **Add** button.
4. Select **Microsoft 365 - OAuth2.0** as the mail retrieval protocol.
5. Enter the field values:
 - **Client ID**, **Client Secret**, and **Tenant ID** should be supplied to you by your IT department.
 - **Support email account id** is the email account that you want Community Manager to read emails from. All emails sent to this address will be processed by Community Manager.
 - **Reply Address** is the email account used to reply to emails.
 - **From Name** is used to populate the From field in email notifications.
 - **Workspace Selection** is the default workspace for incoming email for this account. If this is the only account defined for incoming mail for CM, then all email goes into the Workspace selected here (unless a workspace is defined in the email subject, in the form PROJ=*n*).
6. Enter your password and click **Save**.

For more information about email setup, see Chapter 12, “Email Management,” in the *Community Manager Administrator Guide, Version 11.6.05*. (See “Documentation” on page 6.)

Assigning multiple CM tasks to the same LM(e) task

When reviewing CM tasks and associating them with LM(e) tasks for action, ensure that the desired LM(e) task does not already have a CM task associated with it. A one-to-one relationship is recommended.

Enabling Transport Layer Security protocol (TLS) version 1.2

For complete information, read the article at <https://support.microsoft.com/en-us/help/3135244/tls-1-2-support-for-microsoft-sql-server>.

To use TLS version 1.2 with Microsoft SQL Server and CM, you enable TLS 1.2 on the SQL server and you install the SQL Server Native Client version 11.0 on the CM computer before installing or upgrading CM.

As a prerequisite to CM setup, if CM will use Windows authentication (not sa authentication) and the SQL server is configured to use TLS 1.2, then you must ensure that TLS version 1.0 and TLS 1.2 are both enabled on the SQL server during the CM setup. After setup completes, CM will use TLS 1.2.

Downloading and installing IBM Data Server Runtime client version 11 (applies to LM(e) Server running on Linux)

This procedure is necessary for connecting CM servers on Windows 2008 – 2019 with LM(e) Server version 6.1 or higher running on Linux.

Note: You might need to sign into the IBM support site in order to download the runtime client. If you are not registered, click the **Create IBMid** button to create a user account.

Prerequisites

Before following these instructions, disable the Enhanced Security Configuration option in Internet Explorer on the CM server computer.

Procedure

1. On the CM server, install the DB2 Driver/Runtime client for DB2 Version 11.1 for Windows. The URL to access the download choices from the IBM site is provided here. These instructions refer to 11.1.3.3.

Note: Do not install version 11.5. It is not compatible and will cause connection issues.

You might be prompted to log in with an IBMid:

<https://www.ibm.com/support/pages/ibm-data-server-client-packages-version-111-mod-3-fix-pack-3>

2. Under **IBM Data Server Runtime Client**, select **Windows 64bit**.
3. On the Fix Central page under **Select Fixes**, fill the check box next to item 1, IBM Data Server Runtime Client (Windows/x86-64 64 bit) V11.1.3 Fix Pack 3. Then, select **Continue**.

If the download option is not set to **Download files using HTTPS**, change it to that setting using the **Change download option** link on the right side of the page.

4. On the Download files using HTTPS page, to download the file select the item labeled **v11.1.3fp3_ntx64_rtcl_EN.exe (116.94 MB)**.
5. If you logged in to the IBM site, remember to log out.
6. To install the runtime client, locate the downloaded installation file, right-click it, and select **Run as Administrator**. Follow the wizard instructions to complete the installation.

Installing or upgrading CM

Install or upgrade CM on a Microsoft Windows Server computer where all stated system requirements are met. See **SYSTEM REQUIREMENTS** on page 3.

Upgrade: Upgrade CM to version 11.6.12 directly from version 11.6.05. CM versions earlier than 11.6.05 must upgrade to version 11.6.05 first, and then upgrade to version 11.6.12.

About this task

We recommend performing an upgrade on a test server before upgrading the live server.

It is not necessary to remove the previous Java or Tomcat versions after installing the new required versions. These can remain if they are in use by other web applications.

Prerequisites

Before installing or upgrading CM, ensure that the following requirements are met.

- **Installation or upgrade:** Thoroughly read the contents of this document and all referenced articles that apply, especially the following sections:
 - **SYSTEM REQUIREMENTS** on page 3.
 - **DOCUMENTATION** on page 6.
 - **WHAT'S NEW** on page 6.
 - **FUNCTIONAL IMPACT TOPICS** on page 7.
- **Installation or upgrade:** Confirm that stated system requirements are met (see **SYSTEM REQUIREMENTS** on page 3). In particular:
 - Confirm the Windows Server and SQL Server versions.
 - If SQL Server is or will be installed remotely, ensure that the SQL Server Native Client version 11.0 is installed on the CM computer.
 - Ensure that OpenJDK version 11 (64-bit) is installed on the CM computer. Make sure that you have the path to the OpenJDK executable files; it is required during the CM setup process.

- Ensure that an instance of Tomcat version 9 (64-bit) that is dedicated to CM is installed on the CM computer. Make sure that you have the path to the Tomcat executable files; it is required during the CM setup process.
- If you plan to use TLS 1.2 with Windows authentication (instead of sa authentication), then before running setup ensure that both TLS 1.2 and TLS 1.0 are enabled on the SQL server computer.
- **Installation or upgrade:** Ensure that all appropriate system-wide or context-specific back-ups have been performed.
- **Installation or upgrade:** To support TLS 1.2, enable TLS 1.2 on the SQL Server computer. If during CM setup you plan to select Windows authentication instead of sa authentication, leave TLS 1.0 enabled on the SQL server computer also. For complete information, see **ENABLING TRANSPORT LAYER SECURITY PROTOCOL (TLS) VERSION 1.2** on page 9.
- **Installation or upgrade:** Check for and install any CM PTFs issued since initial product release.
- **Installation only:** The setup program prompts for SMTP server information for sending notification emails. Have the host name of the SMTP server available. If you do not know it, you can enter a nonsense host name and then edit it later.
- Have the sa user credentials (installation) or the FP user credentials (upgrade) available.
- **Upgrade only:** Shut down the IIS web server before updating any of the required software platforms or performing the CM upgrade. Restart the web server after all upgrade activity is complete.
- **UPGRADE WARNING:** Custom changes to the CM Perl code are lost during upgrade. Back up any custom changes before upgrading. After a successful upgrade, re-integrate your backed-up changes into the new Perl code.
- Have credentials for a registered, validated Rocket Community account.

Procedure

1. Ensure that all system requirements (page 3) and all applicable prerequisites (above) are met.
2. Log in as a user with administrator privileges on the CM server computer.

Note: VMWare users should not attempt to upgrade CM using a Remote Desktop connection to the CM server computer. Log in directly on the computer itself.
3. Direct a web browser to the Rocket Community support site at <https://www.rocketsoftware.com/support>, and log in.
4. On the Rocket Community home page, select **Downloads**.
5. On the Downloads page under **Category** select **Aldon Community Manager**. Then in the right pane, select the line item that matches the CM version.
6. On the download page for the selected version, do one of the following:
 - **New installation:** Select the line item for the installation setup file.
 - **Upgrade:** Select the line item for the upgrade setup file.

7. Download and save the setup file to a location on the CM server computer.
8. To perform the installation or upgrade, right-click the saved setup file and select **Run as administrator**. Then, follow the prompts to complete the process.
9. When prompted, supply the required path information for OpenJDK and Tomcat as appropriate.
10. When the **Configure Executive Dashboard** panel displays, accept the defaults. Then select **Next** to continue.
11. **Installation only:** Provide SMTP host information and sa user credentials when prompted.
12. **Upgrade only:** If prompted for an upgrade key, enter 862778.

Migrating CM 11.6.05 data from an SQL Server 2016 computer to CM 11.6.12 on an SQL Server 2019 computer

You can move the CM database from the CM version 11.6.05 installation on an SQL Server 2016 computer to a new, empty CM 11.6.12 database on an SQL Server 2019 computer.

About this task

In these instructions, *source computer* refers to the SQL Server 2016 computer where the 11.6.05 CM database resides, and *target computer* refers to the SQL Server 2019 computer where the 11.6.12 CM database resides.

Prerequisites

To complete this task, the following things are required:

- Credentials for an Administrator user on both computers
- You have installed CM 11.6.12 on the SQL Server 2019 computer and an empty database named **Footprints** exists.

Procedure

1. Log in as an Administrator user on the source computer.
2. To create a backup copy of the CM 11.6.05 **Footprints** database, in Microsoft SQL Server Management Studio take the following steps:
 - a. Expand **Databases** and locate the database named **Footprints**.
 - b. Right-click the Footprints database and select **Tasks** → **Back Up**.
 - c. On the **Back Up Database** window, accept the default values. Then, click **OK**.

The backup file is saved in the default path, for example:

```
C:\Program Files\Microsoft SQL  
Server\MSSQLvv_vv.MSSQLSERVER\MSSQL\Backup\Footprints.bak)
```

Where `vv_vv` represents the SQL Server version.

3. Transfer a copy of the Footprints database backup file to the target computer and store it in a locally accessible folder.
4. On the target computer, do the following:
 - a. Delete the **Footprints** database, if it exists. Make sure to select the **Close existing connections** option on the **Delete Object** display.
 - b. Create a new, empty database named **Footprints** on the target computer.
5. To restore the 11.6.05 database backup into the new 11.6.12 database, take the following steps on the target computer:
 - a. Right-click the newly created **Footprints** database, and then select **Tasks** → **Restore** → **Database**.
 - b. Under **Source** on the **General** tab of the **Restore Database – Footprints** display, select **Device**. Then, browse for and select the file that contains the backed up 11.6.05 Footprints database.
 - c. Under **Destination** on the **General** tab, enter `Footprints` in the **Database** field.
 - d. On the **Files** tab, do the following:
 - Select **Relocate all files to folder**.
 - Verify that the **Restore As** path for both files is `C:\Program Files\Microsoft SQL Server\MSSQLvvv.MSSQLSERVER\MSSQL\DATA\` where `vvv` represents the SQL Server version.
 - Verify that the **Restore As** file names are `Footprints.mdf` and `Footprints_log.LDF`.
 - e. On the **Options** tab, make the following choices:
 - Select **Overwrite the existing database (WITH REPLACE)**.
 - Clear **Take tail-log backup before restore**.
 - f. Select **OK**.
6. To create a new database user FP with default schema dbo and bind the new user to the login user FP, take the following steps:
 - a. On the toolbar, select **New Query**. Then in the new query window, enter the following commands:

```
USE Footprints  
CREATE USER [FP] FOR LOGIN [FP]  
ALTER ROLE [db_owner] ADD MEMBER [FP]
```
 - b. Select **Execute**.
7. To create four additional tables required by CM 11.6.12 after restoring the CM 11.6.05 database, on the target computer open a command window using Run as Administrator, and run the following commands:

```
cd C:\FootPrintsServiceCore\cgi
C:\FootPrintsServiceCore\bin\Perl\bin\perl.exe
MRSearchReportConversion.pl
```

The following new tables are created in the CM 11.6.12 database:

```
dbo.searches_and_reports
dbo.searches_and_reports_ab
dbo.searches_crossproject
dbo.searches_crossproject_projects
```

8. To prepare folder content for copying from the source computer to the target computer, take the following steps on the source computer:

- a. Create a temporary folder in an easily accessible location.
- b. Copy the following folders into the temporary folder:

```
C:\FootPrintsServiceCore\db
C:\FootPrintsServiceCore\etc
C:\FootPrintsServiceCore\Attachments
```

9. If a C:\Footprints\etc\SecurityLogging.txt file exists on the source server, copy the following folder to the temporary folder also:

```
C:\FootPrintsServiceCore\Security
```

10. Make the following file modifications in the temporary location, if necessary:

File name	Change description
MRprojects ABlist.txt	These files reside in the etc folder. If CM was installed to a path on the target computer that is different from the path on the source computer, change the CM installation path that appears in the temporary copy of these files to match the path on the target computer.

11. Remove the following items from the temporary copy of the etc folder, if they exist:

Files	Folders
License imap.txt URLroot AttachmentsRoot V60toV65completed.txt V65toV66completed.txt	wizardtemplates

12. In each of the db\MASTERx\MR folders, remove the following files if they exist:

```
MR.db
```

MRNUMBER

13. When the changes to the temporary copies of the folders are complete, copy each folder to the corresponding location on the target computer, making sure to overwrite the existing folder by selecting the **Replace** option.