Icon

Description automatically generated

Ramp eCDN

Installation Guide

Version 3.3

Copyright ©2022, Ramp Holdings, Inc. All rights reserved. No part of this document may be reproduced, translated into another language or format, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Ramp Holdings, Inc.



Ramp, the Ramp logo and the names and marks associated with Ramp products are trademarks and/or service marks of Ramp, Inc. and are registered and/or common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Ramp.

**License Agreement**

By installing, copying, or otherwise using this product, you acknowledge that you have read, understand and agree to be bound by the terms and conditions of the [Master License Agreement](https://ramp.com/MasterServiceLicenseAgreement) for this product.

**Patent Information**

The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Ramp, Inc.

**Disclaimer**

While Ramp uses reasonable efforts to include accurate and up-to-date information in this document, Ramp makes no warranties or representations as to its accuracy. Ramp assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

**Limitation of Liability**

Ramp and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided “as is” without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Ramp and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Ramp has been advised of the possibility of such damages.

**Customer Feedback**

We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to [support@rampecdn.com](mailto:support@rampecdn.com).

**Ramp Support**

Contact Ramp support at [support@rampecdn.com](mailto:support@rampecdn.com) for software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.

Contents

[Contents i](#_Toc120867408)

[About this Guide iv](#_Toc120867409)

[Audience iv](#_Toc120867410)

[Technical Support iv](#_Toc120867411)

[Comments iv](#_Toc120867412)

[1. What is Ramp eCDN? 5](#_Toc120867413)

[1.1 Components and Operation 5](#_Toc120867414)

[Ramp eCDN Video Delivery Components 5](#_Toc120867415)

[Ramp eCDN Management and Performance Monitoring Components 5](#_Toc120867416)

[1.2 What You Need to Do 6](#_Toc120867417)

[1.3 Product Requirements 6](#_Toc120867418)

[1.4 Ramp eCDN Log Locations 7](#_Toc120867419)

[Installer Logs 7](#_Toc120867420)

[Altimeter Logs 7](#_Toc120867421)

[Analytics Logs 7](#_Toc120867422)

[Multicast+ Sender Logs 8](#_Toc120867423)

[Multicast+ Receiver Logs 8](#_Toc120867424)

[OmniCache Logs 8](#_Toc120867425)

[2. Prepare the Database 9](#_Toc120867426)

[2.1 Upgrade Considerations 9](#_Toc120867427)

[Upgrading From Version 2.5 or Earlier 9](#_Toc120867428)

[Upgrading From Version 2.6 9](#_Toc120867429)

[2.2 Database Requirements 9](#_Toc120867430)

[2.3 Recommended Database Deployment Model 10](#_Toc120867431)

[2.4 Database Installation 10](#_Toc120867432)

[2.5 Database Configuration 11](#_Toc120867433)

[MySQL Configuration Syntax 11](#_Toc120867434)

[Microsoft SQL Server Syntax 11](#_Toc120867435)

[3. Install Ramp eCDN Components 12](#_Toc120867436)

[3.1 Upgrade Considerations 12](#_Toc120867437)

[Upgrading from Ramp eCDN Version 2.6 12](#_Toc120867438)

[Upgrading from Ramp eCDN Version 3.1/3.2 13](#_Toc120867439)

[3.2 Recommended Deployment Order and Model 14](#_Toc120867440)

[3.3 Install the Ramp Components 15](#_Toc120867441)

[Uninstalling Ramp eCDN Components 22](#_Toc120867442)

[4. Verify Ramp eCDN Components 23](#_Toc120867443)

[4.1 Verify Altimeter and Core Analytics 23](#_Toc120867444)

[Start a Session with Altimeter and Core Analytics 23](#_Toc120867445)

[Add the Current Altimeter to the Altimeter Servers List 24](#_Toc120867446)

[4.2 Verify Data Broker 25](#_Toc120867447)

[Check the Data Broker Health Actuator 25](#_Toc120867448)

[Add the Current Data Broker to the Data Broker Cluster List 26](#_Toc120867449)

[Verify Data Broker is Listed in Core Analytics 26](#_Toc120867450)

[4.3 Verify OmniCache 27](#_Toc120867456)

[Check Altimeter for OmniCache 27](#_Toc120867457)

[(Optional) Test OmniCache 28](#_Toc120867458)

[Test OmniCache in Reverse Proxy Mode 28](#_Toc120867459)

[View OmniCache Analytics 30](#_Toc120867460)

[4.4 Verify Multicast+ 31](#_Toc120867461)

[(Optional) Test Multicast+ 31](#_Toc120867462)

[Create a Multicast+ Event 31](#_Toc120867463)

[Install the Multicast+ Receiver 32](#_Toc120867464)

[Test Multicast+ 33](#_Toc120867465)

[View Multicast+ Analytics 34](#_Toc120867466)

[4.5 Troubleshooting 35](#_Toc120867467)

[Altimeter/Core Analytics/Data Broker Connection Issues 35](#_Toc120867468)

[Multicast+ Sender or OmniCache Node Does Not Appear in Altimeter 36](#_Toc120867469)

[5. Post-Installation Configuration 37](#_Toc120867470)

[5.1 Ramp eCDN Component Configuration and Usage 37](#_Toc120867471)

[5.2 Setting Ramp eCDN Java Properties 38](#_Toc120867472)

[5.3 Using Certificates 40](#_Toc120867473)

[5.4 Using MySQL Connector/J 41](#_Toc120867474)

[5.5 Using Data Broker Pass-Through Mode 41](#_Toc120867475)

About this Guide

This guide describes how to install the components of your Ramp eCDN environment.

# Audience

This guide is intended for network administrators who are responsible for determining how to best deploy WAN network video solutions to meet their strategic enterprise performance and optimization goals.

# Technical Support

Contact Ramp Customer Support via the Ramp web site, phone, or e-mail if you have problems using the product, or its documentation.

For more information, see the Ramp web site:

<http://www.rampecdn.com>

# Comments

Ramp welcomes your comments or suggestions on our documentation. To submit feedback, you can send an e-mail to [docs@rampecdn.com](mailto:docs@rampecdn.com). Please include the name of your product, release number (if applicable), and any other relevant information along with your comments.

1. What is Ramp eCDN?

An installation guide for Ramp eCDN

# Components and Operation

## Ramp eCDN Video Delivery Components

Ramp eCDN comprises a set of video delivery solutions that allow you to take control of your video traffic, and maximize the capabilities of your existing network infrastructure:

* **Multicast+** – Provides multicast support to any live video deployment that uses HTTP Live Streaming (HLS) or Dynamic Adaptive Streaming over HTTP (DASH).

Multicast+ sends a single multicast stream that is shared simultaneously by multiple viewers, allowing an event deployment to scale to large audiences, while conserving network bandwidth.

* **OmniCache** – A robust enterprise video caching-proxy that enables the efficient delivery of HLS and DASH streams behind the firewall.

OmniCache greatly reduces the retrieval of video assets from external CDN servers, and shared content is internally distributed to enterprise WAN clients. This allows you to engineer network bandwidth usage, avoid service degradation, and maintain a high-level quality of service (QoS).

* **Ramp P2P** – Provides an easily scalable WebRTC-based P2P solution for enterprise video streaming and collaboration.

Ramp P2P does not require any installation, or complex configuration on the client side. With just a single line of code you can deliver higher quality, scalable live video with minimum bandwidth requirements.

## Ramp eCDN Management and Performance Monitoring Components

Ramp eCDN also provides components that simplify the optimization of your environment, providing centralized performance monitoring functionality:

* **Altimeter** – Works with Multicast+ Senders and OmniCache nodes, creating a scalable, centrally managed infrastructure for enterprise deployments with large numbers of viewers in distributed locations.
* **Core Analytics** – A browser-based reporting application that is installed along with Altimeter, resides on the Altimeter host, and provides performance monitoring reports.
* **Data Broker** – Processes data collected from your environment for Core Analytics.

# What You Need to Do

This section summarizes what you need to do to install or upgrade your Ramp eCDN environment.

***Note:*** *If you are upgrading from Altimeter version 2.5 or earlier, prepare a separately installed database as described in* [*Preparing the Database*](#PreparingtheAltimeterDatabase)*, then install as described in* [*Install Ramp eCDN Components*](#InstallingAltimeter)*.*

|  |  |
| --- | --- |
| Action | Description |
| Prepare the Database | **Altimeter**, **Core Analytics**, and **Data Broker** are used with a separately installed database that must be:   * Installed, running, and configured with the expected users and schemas as described in [Prepare the Database](#PreparingtheAltimeterDatabase). * Available to each Altimeter if Altimeter High Availability Mode is used. |
| Install/Upgrade Ramp eCDN Components | [Install Ramp eCDN Components](#InstallingAltimeter) on the target host system according to the Recommended Deployment Order and Model.  ***Note:***   * ***(Microsoft SQL Server – Windows Authentication only)*** *If you are using Windows Authentication, additional configuration is required after Altimeter and/or Data Broker are installed. For more information, see Tech Note - Using Windows Authentication with Ramp eCDN.* * ***(LDAP Authentication only)*** *Altimeter and Core Analytics support the use of LDAP authentication. For more information, see “LDAP Support Requirements for Altimeter/Core Analytics” in the Ramp eCDN System Requirements Guide.* |
| Verify Ramp eCDN Components | [Verify Ramp eCDN Components](#VerifyComponents) to ensure the components have installed correctly, and perform any additional configuration required. |
| Post-Installation Configuration | Perform any [Post-Installation Configuration](#PostInstallationConfiguration) that may be required according to the needs of your environment. |

# Product Requirements

For product hardware and software requirements, see the *Ramp eCDN System Requirements*.

# Ramp eCDN Log Locations

When contacting Ramp Support, please send the appropriate log files along with your problem description to assist in resolving your issue.

## Installer Logs

The Ramp eCDN Installer creates the following logs for reference and debugging purposes.

|  |  |
| --- | --- |
| Log | Default Location |
| Installer Log | **Linux and Mac:**   * /tmp/installbuilder\_installer\_<*pid*>.log   **Windows:**   * C:\Users\<*user*>\AppData\Local\ installbuilder\_installer\_<*pid*>.log |

## Altimeter Logs

Altimeter maintains the following logs for reference and debugging purposes.

|  |  |
| --- | --- |
| Log | Default Location |
| Tomcat Log | **Linux:**   * /opt/rampecdn/altimeter/tomcat/logs/catalina.*yyyy*-*mm*-*dd*.log * /opt/rampecdn/altimeter/tomcat/logs/catalina.out   **Windows:**   * C:\Program Files\rampecdn\altimeter\tomcat\logs\catalina.*yyyy*-*mm*-*dd*.log |
| Altimeter Log | **Linux:**   * /opt/rampecdn/altimeter/tomcat/logs/vdms/vdms-manager.log   **Windows:**   * C:\Program Files\rampecdn\altimeter\tomcat\logs\vdms\vdms-manager.log |
| Audit Log | **Linux:**   * /opt/rampecdn/altimeter/tomcat/logs/*system\_name*\_access\_log.*yyyy*-*mm*-*dd*   **Windows:**   * C:\Program Files\rampecdn\altimeter\tomcat\logs\*system\_name*\_access\_log.*yyyy*-*mm*-*dd* |

## Analytics Logs

Analytics maintains the following logs for reference and debugging purposes:

|  |  |
| --- | --- |
| Log | Location |
| Data Broker Log | **Linux:**   * /opt/rampecdn/databroker/logs/broker.log   **Windows:**   * C:\Program Files\rampecdn\databroker\logs\broker.log |
| Core Analytics Log | **Linux:**   * /opt/rampecdn/coreanalytics/logs/core-analytics.log   **Windows:**   * C:\Program Files\rampecdn\coreanalytics\logs\core-analytics.log |
| Audit Log | **Linux:**   * /opt/rampecdn/coreanalytics/logs/access\_log.*yyyy*-*mm*-*dd*   **Windows:**   * C:\Program Files\rampecdn\coreanalytics\logs\access\_log.*yyyy*-*mm*-*dd* |

## Multicast+ Sender Logs

The Multicast+ Sender maintains the following logs for reference and debugging purposes.

|  |  |
| --- | --- |
| Log | Default Location |
| Sender Log | **Linux:**   * /opt/rampecdn/multicast/multicastplus/logs/sender.log   **Windows:**   * C:\Program Files\rampecdn\multicast\multicastplus\logs |

## Multicast+ Receiver Logs

The Multicast+ Receiver maintains the following logs for reference and debugging purposes.

|  |  |
| --- | --- |
| Log | Default Location |
| Windows Receiver Log | * C:\Program Files\RAMP\_Multicast\_Receiver\logs\ramp-unifiedclient-*mm-dd-yyyy*.log |
| Mac Receiver Log | * ~/Library/Application Support/RampMulticastPlusReceiver/logs/ramp-unifiedclient-*mm-dd-yyyy*.log |
| Linux Receiver | * ~/Library/Application Support/RampMulticastPlusReceiver/logs/ramp-unifiedclient-*mm-dd-yyyy*.log |

## OmniCache Logs

OmniCache maintains the following logs for reference and debugging purposes.

|  |  |
| --- | --- |
| Log | Default Location |
| OmniCache Logs | **Linux:**   * /opt/rampecdn/omnicache/omnicache/logs/omnicache.log * /opt/rampecdn/omnicache/omnicache/logs/request.log   **Windows:**   * C:\Program Files\rampecdn\omnicache\omnicache\logs\omnicache.log * C:\Program Files\rampecdn\omnicache\omnicache\logs\request.log |

1. Prepare the Database

**Altimeter**/**Core Analytics**, and **Data Broker** are used with a separately installed database that must be:

* Installed, running, and configured with the expected users and schemas as described below **BEFORE** installing the Ramp eCDN components.

# Upgrade Considerations

If you are upgrading Ramp eCDN from a previous version:

## Upgrading From Version 2.5 or Earlier

To upgrade from version 2.5 or earlier, prepare a separately installed database as described in this chapter, then install as described in [Install Ramp eCDN Components](#InstallingAltimeter).

## Upgrading From Version 2.6

To upgrade from version 2.6, perform the steps below, then install as described in [Install Ramp eCDN Components](#InstallingAltimeter):

1. From a database prompt, drop, then create, the mate database. For example:

Drop database mate;

Create database mate;

1. From a database prompt, backup the vdms database. For example:

mysqldump-uroot-p vdms>C:\MySQLBackup\vdms.sql

1. From a database prompt, update the required user privileges:

GRANT ALL on vdms.\* to 'altimeter'@'%' WITH GRANT OPTION;

GRANT ALL on mate.\* to 'mate'@'%' WITH GRANT OPTION;

# Database Requirements

Ramp eCDN supports the following databases:

|  |  |  |
| --- | --- | --- |
| Database Provider | Database Version | JDBC Included in Ramp Installer |
| MySQL | MySQL Community Server 8.0.18 or later. | MariaDB Connector/J 3.0.4 or later.  ***Note:*** *MySQL Connector/J 8.0.28 or later is also supported post-installation.* |
| Microsoft SQL Server | Microsoft SQL Server 2016 or later. | Microsoft JDBC Driver 10.2 or later. |
| Microsoft SQL Server – Windows Authentication | Microsoft SQL Server 2016 or later. | Microsoft JDBC Driver 10.2 or later. |

For database hardware requirements, see “Hardware Summary” in the *Ramp eCDN System Requirements*.

# Recommended Database Deployment Model

Ramp STRONGLY recommends using Altimeter/Core Analytics and Data Broker with an external database server according to the following sizing recommendations:

|  |  |  |
| --- | --- | --- |
| Deployment Type | Characteristics | Ramp Recommendation |
| Small Deployments | * Minimal Proof of Concept (POC) or testing-only deployment. * Less than 5 OmniCache nodes or 2 Senders. * Less than 300 users per OmniCache node or Sender. | * Ramp eCDN database can run on the Altimeter host. * Ramp eCDN database on a separate server preferred. |
| Large Deployments | * Up to 50 OmniCache nodes/5 Senders. * Up to 30000 reporting Receivers/Ramp Plugins. | * Ramp eCDN database on a separate server required. |

# Database Installation

***Note:*** *Altimeter supports High Availability Mode, where a primary and backup Altimeter are deployed to provide failover capability and prevent single point of failure issues.*

*When High Availability Mode is used, each Altimeter shares the same database. Ramp recommends that you use an InnoDB Cluster to provide database failover capability.*

To install the Ramp eCDN database, either:

* Use the instructions recommended by the database provider:
  + **MySQL**:
    - Single MySQL instance: <https://dev.mysql.com/doc/mysql-installation-excerpt/8.0/en/>
    - InnoDB MySQL Cluster: <https://dev.mysql.com/doc/mysql-shell/8.0/en/mysql-innodb-cluster.html>
  + **MS SQL**:
    - Single MS SQL instance: <https://docs.microsoft.com/en-us/sql/database-engine/install-windows/install-sql-server?view=sql-server-ver15>
* (**MySQL only**) See one of the following:
  + *TechNote – Installing a Single MySQL Database for Altimeter.*
  + *TechNote – Installing an InnoDB Cluster for Altimeter.*

# Database Configuration

Use the appropriate syntax to configure the Ramp eCDN database with the required schemas and users.

## MySQL Configuration Syntax

CREATE DATABASE IF NOT EXISTS vdms;

CREATE USER IF NOT EXISTS altimeter identified WITH caching\_sha2\_password by '#MYSQLPASSWORD';

GRANT ALL on vdms.\* to 'altimeter'@'%' WITH GRANT OPTION;

FLUSH PRIVILEGES;

CREATE DATABASE IF NOT EXISTS mate;

CREATE USER IF NOT EXISTS mate identified WITH caching\_sha2\_password by '#MYSQLPASSWORD';

GRANT ALL on mate.\* to 'mate'@'%' WITH GRANT OPTION;

FLUSH PRIVILEGES;

SET PERSIST time\_zone = '+00:00';

SET PERSIST binlog\_expire\_logs\_seconds = 7200;

SET PERSIST max\_connections = 256;

SET global max\_allowed\_packet = 1024\*1024\*10;

## Microsoft SQL Server Syntax

***Note: (Microsoft SQL Server – Windows Authentication only)*** *If you are using Windows Authentication, the service user must have the same permissions as the users below.*

IF NOT EXISTS(SELECT \* FROM sys.databases WHERE name = 'vdms')

CREATE DATABASE vdms;

IF NOT EXISTS(SELECT \* FROM sys.databases WHERE name = 'mate')

CREATE DATABASE mate;

USE vdms;

IF NOT EXISTS(SELECT principal\_id FROM sys.server\_principals WHERE name = 'altimeter')

CREATE LOGIN altimeter WITH PASSWORD = '#SQLPASSWORD';

IF NOT EXISTS(SELECT principal\_id FROM sys.database\_principals WHERE name = 'altimeter')

CREATE USER altimeter;

GRANT CONTROL TO altimeter WITH GRANT OPTION;

USE mate;

IF NOT EXISTS(SELECT principal\_id FROM sys.server\_principals WHERE name = 'mate')

CREATE LOGIN mate WITH PASSWORD = '#SQLPASSWORD';

IF NOT EXISTS(SELECT principal\_id FROM sys.database\_principals WHERE name = 'mate')

CREATE USER mate;

GRANT CONTROL TO mate WITH GRANT OPTION;

1. Install Ramp eCDN Components

This chapter describes how to install the Ramp eCDN components in your environment.

***Note:***

* ***To install Ramp eCDN components using the command line, see   
  TechNote – Ramp eCDN Command Line Installation.***
* ***If you are upgrading, see*** [***Upgrade Considerations***](#_Upgrade_Considerations_1) ***to prepare your database.***

# Upgrade Considerations

To upgrade from an earlier version of Ramp eCDN:

* If you are upgrading Ramp eCDN version 2.6/3.1/3.2, you must preserve some configuration information from your existing environment as it is used during the upgrade process.
* If you are upgrading from Ramp eCDN 3.3 or later, the installer preserves your existing configuration information, and no further action is required.

## Upgrading from Ramp eCDN Version 2.6

Before upgrading, do the following:

1. Preserve the following Database Connection Strings:

* Altimeter:
  + Copy the following file to a safe location that will not be overwritten:

<install\_directory>/tomcat/webapps/vdms/WEB-INF/context.xml

* + In the context.xml file:
    - Locate the Altimeter Database Connection String in the XML element called “resources”.
    - Replace each instance of ‘&amp’ with ‘&’ in the string, then save the file. Use this string during upgrade.
* Core Analytics:
  + Copy the following file to a safe location that will not be overwritten:

<install\_directory>/ConfigServer/R\_\_AddProperties.sql

* + In the R\_\_AddProperties.sql file, locate the Core Analytics Database Connection String on line 2. Use this string during upgrade.

1. (**If LDAP is used only**) Preserve the following LDAP information:

* Altimeter:
  + Copy the following file to a safe location that will not be overwritten:

<install\_directory>/tomcat/webapps/vdms/WEB-INF/context.xml

* + In the context.xml file, locate the LDAP information in the XML element called “realm”. Use this information during upgrade.

1. (**If SSL is used only**) Preserve the following SSL information:

* Altimeter:
  + Copy the .PEM, .PKCS, or Java Key Store file to a safe location that will not be overwritten. Use the location of this file during upgrade.

***Note:*** *PEM files must be converted to .PKCS format for Ramp eCDN version 3.3 and later. Ramp recommends using OpenSSL utility. For example:*

openssl pkcs12 -export -out <output\_file\_name> -inkey <input\_pem\_certificate\_key> -in <input\_pem\_certificate\_file\_name>

*For more information, see the OpenSSL documentation.*

## Upgrading from Ramp eCDN Version 3.1/3.2

Before upgrading, do the following:

1. Preserve the following Database Connection Strings:

* Altimeter:
  + Copy the following file to a safe location that will not be overwritten:

<install\_directory>/coreanalytics/application.properties

* + In the application.properties file, locate the Altimeter Database Connection String in the property called “vdms.database.url”. Use this string during upgrade.
* Core Analytics:
  + Copy the following file to a safe location that will not be overwritten:

<install\_directory>/coreanalytics/application.properties

* + In the application.properties file, locate the Core Analytics Database Connection String in the property called “mate.database.url”. Use this string during upgrade.

1. (**If LDAP is used only**) Preserve the following LDAP information:

* Altimeter:
  + Copy the following file to a safe location that will not be overwritten:

<install\_directory>/tomcat/webapps/vdms/WEB-INF/context.xml

* + In the context.xml file, locate the LDAP information in the XML element called “realm”. Use this information during upgrade.
* Core Analytics:
  + Copy the following file to a safe location that will not be overwritten:

<install\_directory>/coreanalytics/application.properties

* + In the application.properties file, locate the LDAP information. Use this information during upgrade.

1. (**If SSL is used only**) Preserve the following SSL information:

* Altimeter:
  + Copy the .PKCS file to a safe location that will not be overwritten. Use the location of this file during upgrade.

# Recommended Deployment Order and Model

Ramp recommends deploying the Ramp eCDN components in the following order:

|  |  |
| --- | --- |
| Component(s) | Ramp Recommendation |
| 1. Altimeter and Core Analytics | Altimeter and Core Analytics are deployed on the same host, and are connected to the database you configured in [Prepare the Database](#PreparingtheAltimeterDatabase).  ***Note:******To use Altimeter High Availability Mode, during installation, connect each Altimeter to the same database.*** |
| 2. Data Broker | Data Broker can be deployed on the Altimeter/Core Analytics host, but for large environments, Data Broker requires a separate host.  Data Broker is connected to the database you configured in [Prepare the Database](#PreparingtheAltimeterDatabase), but can also be set to forward data to a service (Pass-Though Mode) following installation. |
| 3. OmniCache | OmniCache nodes require separate hosts, deployed in your network architecture where they can best satisfy your throughput, video quality, and optimization requirements. |
| 4. Multicast+ Sender | Multicast+ Senders require separate hosts, deployed in your network architecture where they can best satisfy your throughput, video quality, and optimization requirements. |
| 5. Multicast+ Receiver | Multicast+ Receivers are deployed on clients hosts. For more information, see the *Multicast+ Receiver Deployment Guide*. |

# Install the Ramp Components

To install the Ramp components on the host:

***Note:***

* *You need administrator rights on the target machine to use the Ramp eCDN Installer.*
* *After installation, if component configuration settings must be changed, re-run the installer with the new settings to update the installed component.*

1. Download the Ramp eCDN distribution from http://connect.rampecdn.com (for example, rampecdn-*n.n.n*.zip) to the target host for the component.
2. Using a file compression utility, unzip the distribution.
3. Locate the Ramp eCDN installer file. For example:

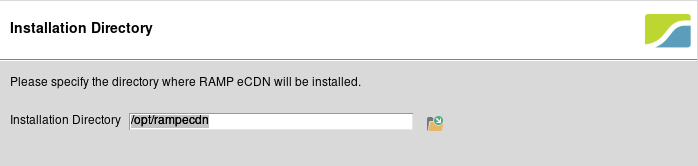
* **Windows:**

C:\*download\_location*\rampecdn-*n.n.n*\rampecdn-n.n.n\   
rampecdn-n.n.n-windows-x64-installer.exe

* **Linux:**

/download\_location/rampecdn-*n.n.n*/rampecdn-n.n.n/  
rampecdn-n.n.n-linux-x64-installer.run

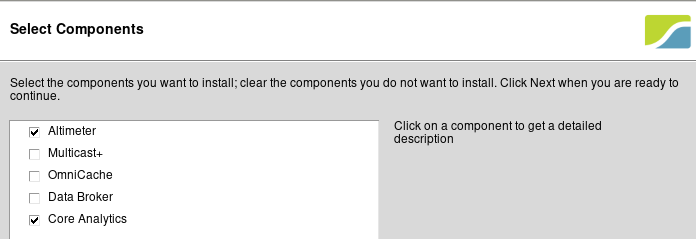
1. Double-click on the installer file. Proceed through the preliminary panels until the Installation Directory panel appears:



Select the installation directory for Ramp eCDN components by doing one of the following, then click Next:

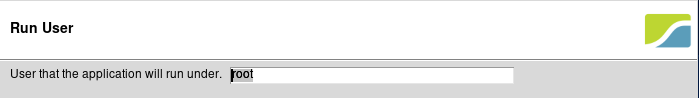
* + Accept the default location:
    - **Windows:** C:\Program Files\rampecdn
    - **Linux:** /opt/rampecdn
  + Edit the path to specify another location.
  + Click the Folder button and navigate to another location.

1. The Select Components panel appears:



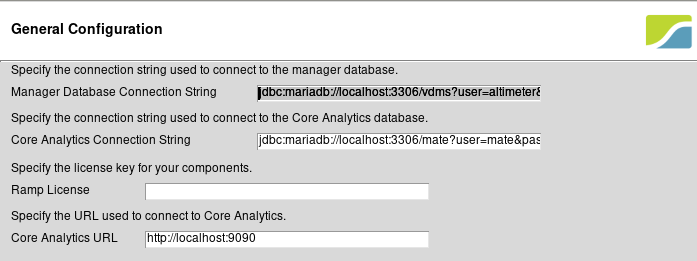
Select the Ramp eCDN components you want to install on the current host, then click Next. For more information, see [Recommended Component Deployment Model](#_Recommended_Component_Deployment).

1. (**Linux only**) The Run User panel appears:



Enter the name of the user that the Ramp eCDN components will run under on the system, then click Next. The Ramp eCDN installer creates and associates this user with the installed components.

1. The General Configuration panel appears:



The fields displayed on the General Configuration panel depend on which components you chose on the Select Components panel. Enter the following information as appropriate, then click Next:

* **Manager Database Connection String** – If you selected Altimeter/Core Analytics, enter the connection string used for the Manager Database. For example:

MySQL Example:

jdbc:mariadb://<hostname>:<port>/vdms?user=altimeter&password=<password>&allowPublicKeyRetrieval=true&useSSL=false&useUnicode=true&serverTimezone=UTC&rewriteBatchedStatements=true

SQL Server Example:

jdbc:sqlserver://<hostname>:<port>;databaseName=vdms;trustServerCertificate=true;user=altimeter;password=<password>

SQL Server with Windows Authentication Example:

jdbc:sqlserver://<hostname>:<port>;databaseName=vdms;trustServerCertificate=true;integratedsecurity=true

Where:

|  |  |
| --- | --- |
| Item | Description |
| <*hostname*> | The hostname of the Ramp eCDN database server. |
| <*port*> | The port number used to connect to the Ramp eCDN database server. |
| <*password*> | The password you specified for the ‘altimeter’ user when configuring the Ramp eCDN database in [Database Configuration](#_Database_Configuration). |

* **Core Analytics Connection String** – If you selected Core Analytics/Data Broker, enter the connection string used for the Core Analytics database. For example:

MySQL Example:

jdbc:mariadb://<hostname>:<port>/mate?user=mate&password=<password>&allowPublicKeyRetrieval=true&useSSL=false&useUnicode=true&serverTimezone=UTC&rewriteBatchedStatements=true

SQL Server Example:

jdbc:sqlserver://<hostname>:<port>;databaseName=mate;trustServerCertificate=true;user=mate;password=<password>

SQL Server with Windows Authentication Example:

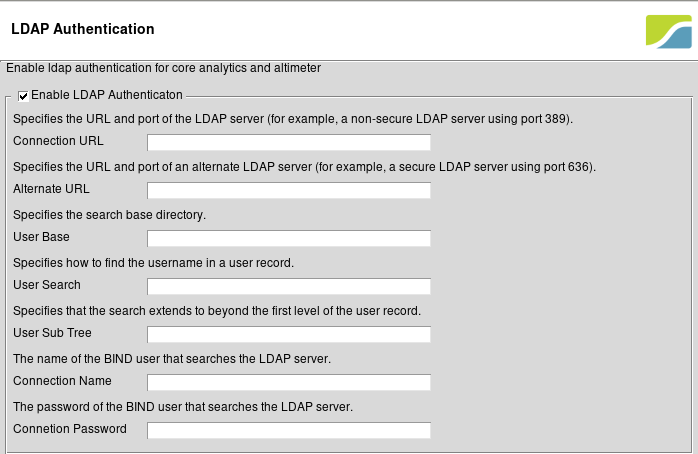
jdbc:sqlserver://<hostname>:<port>;databaseName=mate;trustServerCertificate=true;integratedsecurity=true

Where:

|  |  |
| --- | --- |
| Item | Description |
| <*hostname*> | The hostname of the Ramp eCDN database server. |
| <*port*> | The port number used to connect to the Ramp eCDN database server. |
| <*password*> | The password you specified for the ‘mate’ user when configuring the Ramp eCDN database in [Database Configuration](#_Database_Configuration). |

* **Ramp License** – If you selected Data Broker/Multicast+/OmniCache, copy/paste the license key that was provided by Ramp Support.
* **Core Analytics URL** – If you selected Data Broker/Multicast+/OmniCache, enter the URL used to connect to Core Analytics. For example: http://localhost:9090

1. (**Altimeter/Core Analytics only**) The LDAP Authentication panel appears:



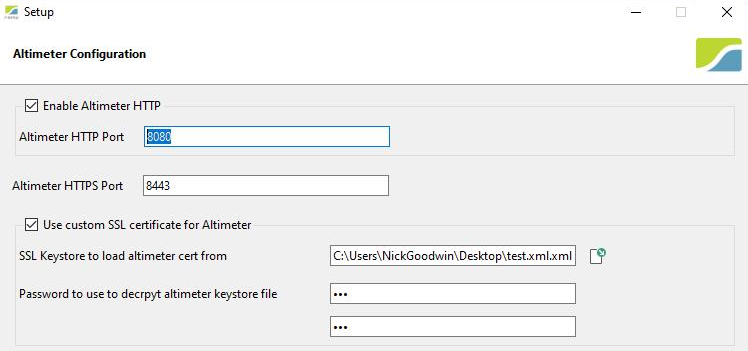
Altimeter and Core Analytics provide basic user authentication, but can be configured to work with your organization’s LDAP deployment.

To use LDAP authentication with Altimeter and Core Analytics:

* See “LDAP Support Requirements for Altimeter/Core Analytics” in the *Ramp eCDN System Requirements Guide*.
* In the LDAP Authentication panel, select the Enable LDAP Authentication check box, enter your site’s LDAP values, then click Next:

|  |  |
| --- | --- |
| Item | Description |
| Connection URL | Specifies the URL and port of the LDAP server. For example, a non-secure LDAP server using port 389:  ldap://YOURLDAPSERVERHERE:389 |
| Alternate URL | Specifies the URL and port of an alternate LDAP server. For example, a secure LDAP server using port 636:  ldap://YOURLDAPSERVERHERE:636 |
| User Base | Specifies the search base directory. For example:  dc=YOURDC,dc=YOURDC |
| User Search | Specifies how to find the username in a user record. For example:  (uid={0}) |
| User Sub Tree | Specifies that the search extends to beyond the first level of the user record. For example:  true |
| Connection Name | The name of the BIND user that searches the LDAP server. For example:  cn=YOURBINDUSER,dc=YOURDC,dc=YOURDC |
| Connection Password | The password of the BIND user that searches the LDAP server. For example:  YOURBINDUSERPASSWORD |

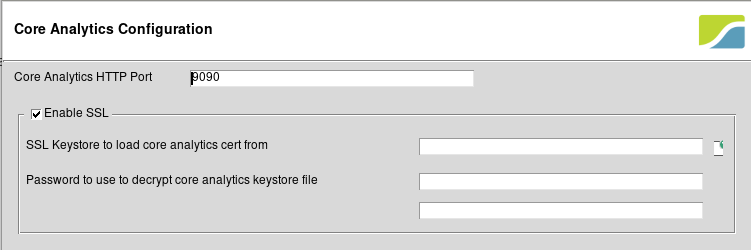
1. (**Altimeter only**) The Altimeter Configuration panel appears:



Enter the following information as appropriate, then click Next:

* **Enable Altimeter HTTP**: To use HTTP with Altimeter, select the check box.
  + **Altimeter HTTP Port**: Enter the port number for HTTP communications with the component. For example: 8080 (default)
* **Altimeter HTTPS Port**: Enter the port number for HTTPS communications with the component. For example: 8443 (default)
* **Use Custom SSL Certificate for Altimeter**: To use your own SSL certificates with Altimeter, select the check box.
  + **SSL Keystore to load…**: Click the Folder button next to the field and navigate to the location of the Java Key Store or PKCS12 certificate file you want to use with the component.
  + **Password to use to decrypt…**: Enter the password associated with the certificate file in the upper field, then re-enter the password in the lower field to ensure your entries match.

1. (**Core Analytics/Data Broker only**) The <Ramp component> Configuration panel appears:

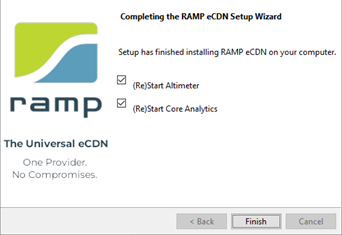


The panel displayed depends on which components you chose on the Select Components panel. Enter the following information as appropriate, then click Next:

* **<Component> HTTP Port**: Enter the port number for HTTP communications with the component. For example:
  + Core Analytics port: 9090 (default)
  + Data Broker port: 30378 (default)
* **Enable SSL**: To use SSL with the component, select the check box.
  + **SSL Keystore to load…**: Click the Folder button next to the field and navigate to the location of the Java Key Store or PKCS12 certificate file you want to use with the component.
  + **Password to use to decrypt…**: Enter the password associated with the certificate file in the upper field, then re-enter the password in the lower field to ensure your entries match.

1. The Ready to Install panel appears. Click Next.
2. Once the installation is complete, the Completion panel appears.

***IMPORTANT:*** ***If you are installing Core Analytics and Data Broker, DO NOT start them simultaneously. Start one component, wait 30 seconds, then start the other component.***



* If the installation was successful:
  + (**Windows**) Ensure that the components you installed are selected to restart, then click Finish.
  + (**Linux**) Click Finish.
  + Verify the installed components:
    - * [Verify Altimeter and Core Analytics](#_Verify_Altimeter_and).
      * [Verify Data Broker](#_Verify_Data_Broker_1).
      * [Verify OmniCache](#_Verify_Multicast+).
      * [Verify Multicast+](#_Verify_Multicast+_1).
      * (**Microsoft SQL Server – Windows Authentication only**) If you are using Windows Authentication, additional configuration is required after Altimeter and/or Data Broker are installed. For more information, see *Tech Note - Using Windows Authentication with Ramp eCDN*.
* If the installation encountered issues:
  + Collect the appropriate component logs listed in [Ramp eCDN Log Locations](#_Ramp_eCDN_Log).

## Uninstalling Ramp eCDN Components

To uninstall the Ramp eCDN components:

1. Locate the Ramp eCDN uninstall file. For example:

* **Windows:**

C:\Program Files\rampecdn\uninstall.exe

* **Linux:**

opt/rampecdn/uninstall

1. Double-click on the installer file.
2. Click Yes to confirm that you want to uninstall the Ramp eCDN components.
3. Click Ok.

1. Verify Ramp eCDN Components

This chapter describes how to verify that the Ramp eCDN components have installed correctly.

# Verify Altimeter and Core Analytics

To verify Altimeter and Core Analytics:

* Start a session with Altimeter and Core Analytics.
* Add the Current Altimeter to the Altimeter Servers List.

## Start a Session with Altimeter and Core Analytics

To start a session with each component:

1. For Altimeter, open a browser, then enter the URI for the Altimeter host using the following format:

http(s)://*hostname*:*port*/vdms

For example:

http://localhost:8080/vdms

1. Authenticate with Altimeter using the default credentials:

* Username: admin
* Password: admin

The following appears:

Text, application

Description automatically generated with medium confidence

The Dashboard display indicates that Altimeter has successfully started and is running.

1. For Core Analytics, open a browser, then enter the URI for the Core Analytics host using the following format:

http(s)://*hostname*:*port*

For example:

http://localhost:9090

1. Authenticate with Core Analytics using the default credentials:

* Username: admin
* Password: P@ssw0rd!

The following appears:

Graphical user interface, application

Description automatically generated

The Dashboard display indicates that Core Analytics have started and are running.

## Add the Current Altimeter to the Altimeter Servers List

Once you have verified Altimeter and Core Analytics, update the Altimeter Servers List so other components can obtain provisioning information from Altimeter.

1. From the Altimeter > Settings tab, click the Edit icon next to the Management Server > Altimeter Servers property:

Graphical user interface, text, application, email

Description automatically generated

The Altimeter Servers property is a comma-separated list of Altimeter Server host names (or load balancers hostnames in front of Altimeter Servers). The list must contain at least one active Altimeter Server. The Altimeter Servers list populates the following:

* The OmniCache provisioningClient and provisioningServer list that define where nodes obtain provisioning updates if needed.
* Populates the vdmsagent.managementServer property that is used by Multicast+ Senders to communicate with Altimeter.

Any change made to the Altimeter Servers list is automatically propagated to the nodes and Senders, and no restart is required.

1. Click Save, then Close.

# Verify Data Broker

To verify Data Broker:

* Check the Data Broker Health Actuator.
* Add the Current Data Broker to the Data Broker Cluster List.
* Verify Data Broker is listed in Core Analytics

## Check the Data Broker Health Actuator

To access the Health Actuator:

1. Open a browser, then enter the URI for the Data Broker Health Actuator using the following format:

http(s)://*hostname*:*port*/actuator/health

For example:

http://localhost:30378/actuator/health

Where 30378 is the default port used by Data Broker. The following appears:

Graphical user interface, text, application

Description automatically generated

The Health Actuator display indicates that Data Broker has successfully started and is running.

## Add the Current Data Broker to the Data Broker Cluster List

Once you have checked the Health Actuator, update the Data Broker Cluster list so other components can send analytics data to Data Broker.

1. From the Altimeter > Settings tab, click the Edit icon next to the Management Server > Data Broker Cluster property:

Graphical user interface, text, application, email

Description automatically generated

The Data Broker Cluster property is a comma-separated list of Data Broker host names that are used to process analytics data. The list must contain at least one active Data Broker, and uses the following format:

http(s)://*databroker\_host1:port*/protobuf,http(s)://*data*

*broker\_host2:port*/protobuf, ...

For example:

http(s)://127.0.0.1:30378/protobuf

Where 30378 is the default port used by Data Broker.

1. Click Save, then Close.

## Verify Data Broker is Listed in Core Analytics

Once you have updated the Data Broker Cluster list, the Data Broker registers with Altimeter. To verify that Data Broker is registered:

1. In Core Analytics, click “Resources > Components” on the Navigation Menu. The following is displayed:

Graphical user interface, text, application

Description automatically generated

1. Verify that the Data Broker you installed is included in the Data Brokers list.

# Verify OmniCache

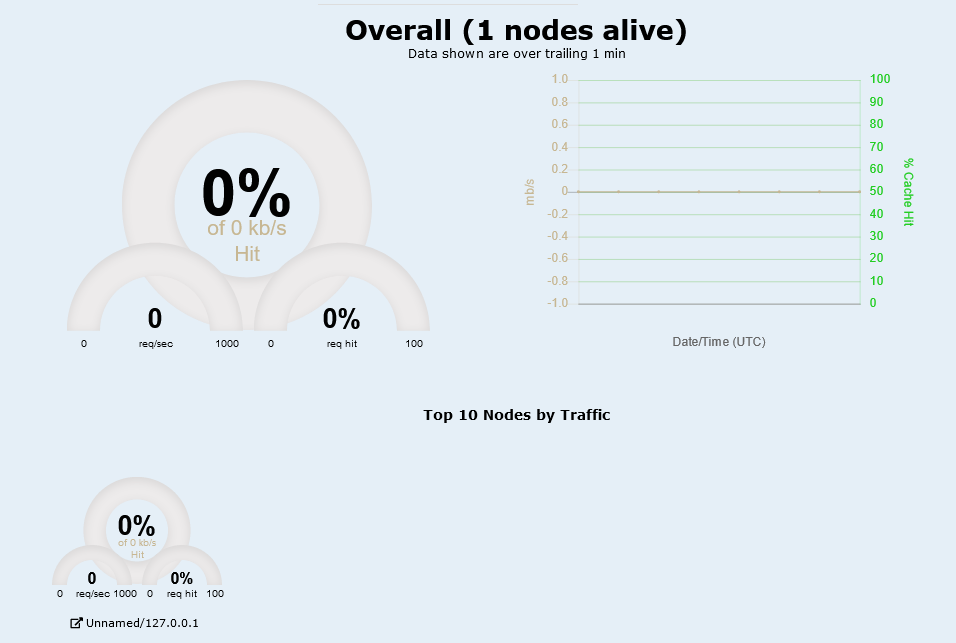
To verify OmniCache:

* Check Altimeter for OmniCache.
* (Optional) Test OmniCache.

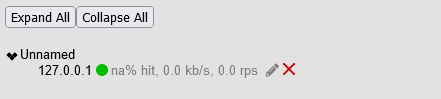
## Check Altimeter for OmniCache

To check that the OmniCache Node has been provisioned by Altimeter:

1. In Altimeter, click OmniCache > Dashboard tab and view that the new node appears:



1. Click OmniCache > Nodes, and view that the new node is listed:



## (Optional) Test OmniCache

To perform an enhanced verification for OmniCache, perform the steps described in the section below.

***Note:*** *This section provides a condensed usage summary. For complete information, see the OmniCache or Altimeter documentation.*

### Test OmniCache in Reverse Proxy Mode

When OmniCache is run in reverse proxy mode (required when integrating a video platform with AltitudeCDN) , requests are sent directly to OmniCache, where the URI in the HTTP request is rewritten to fetch the upstream source of the video stream.

#### Configuring OmniCache with Altimeter

To configure OmniCache to run in reverse proxy mode:

1. Click OmniCache > Proxies.
2. For Mode, select reversehttp.
3. For Port, verify that the value is set to 10000.
4. Click Save, then click Publish. Altimeter provisions the configuration changes and updates the OmniCache node.

#### Test OmniCache

The Ramp LiveTools Portal is an internal testing tool hosted by Ramp, and can be used to validate your OmniCache configuration.

##### Sending Video Stream Requests to Test OmniCache

To test OmniCache, use two separate browsers (for example, Chrome and Firefox) to send video requests to OmniCache with the Ramp LiveTools Portal.

Within each browser, do the following:

1. Enter the URI for the Ramp LiveTools Portal. For example:

http://livetools.rampecdn.com/portal/

The following appears:

Graphical user interface, application

Description automatically generated

1. In the Player section, enter the following:
   * + Allow Fallback – Click the checkbox.
     + Fallback Source: - Select RampTV [HLS].
2. In the Configuration section, enter the following:

* Server URI:
  + Select Add New.
  + Enter the IP address and port for the OmniCache node.

For example: http://127.0.0.1:10000

* Click Apply. The following occurs:
  + The Portal attempts to detect OmniCache.
  + The Portal sends the video request.
  + OmniCache retrieves the video source and begins caching to serve subsequent requests.
  + The video stream is served to fulfill the request. Once complete, the following appears in the Player section:

Graphical user interface

Description automatically generated

* + To view that OmniCache is processing the video stream, see [View OmniCache Analytics](#_View_OmniCache_Analytics).

### View OmniCache Analytics

Once the two browsers are connected through OmniCache and video is served back to the LiveTools Portal, you can view the data sent from OmniCache using Core Analytics:

1. On the Core Analytics Dashboard, view the following:

Graphical user interface, text, application, chat or text message

Description automatically generated

Chart

Description automatically generated

The OmniCache card indicates that OmniCache has processed the test stream, and Unique Viewers indicates the number of users (with unique IP addresses) for the OmniCache node.

# Verify Multicast+

To verify Multicast+:

* Check Altimeter for the Sender.
* (Optional) Test Multicast+.

***Note:*** *This section provides a condensed usage summary. For complete information, see the Multicast+ or Altimeter documentation.*

Check Altimeter for the Sender

To check that the Sender has been provisioned by Altimeter:

1. Click Multicast+ > Dashboard, and view that the new Sender appears:

Text

Description automatically generated

1. Click Multicast+ > Senders, and view that the new Sender is listed:

Chart, bubble chart

Description automatically generated

## (Optional) Test Multicast+

To perform an enhanced verification for Multicast+, perform the steps described in the sections below.

### Create a Multicast+ Event

A Multicast+ event is created in Altimeter, and defines the video source, multicast channel, and Senders that are to be used for the duration of the Event. When the Event begins, the Sender retrieves and broadcasts the video stream to any Receivers that are connected on the same multicast channel.

To create a Multicast+ Event in Altimeter:

1. Create a Multicast Channel by clicking Multicast+ > Channels > Create.
2. In the Details panel, enter the following, then click Save:

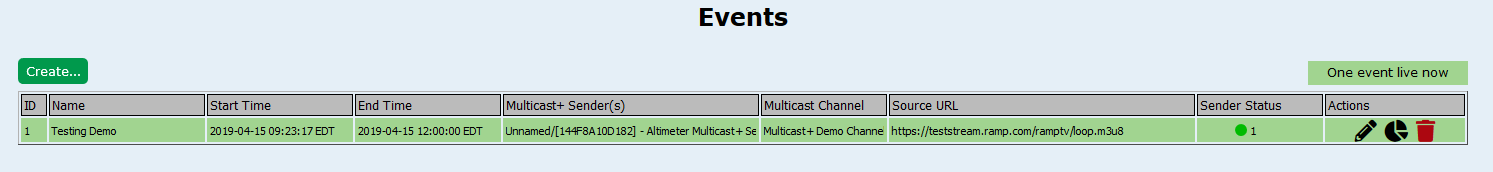
* **Channel Name** – Multicast+ Demo Channel
* **Multicast Address** – 239.0.0.10:12345

1. Create a Multicast+ Event by clicking Multicast+ > Events > Events section > Create.
2. In the Details panel, enter the following:

* **Event Name** – Testing Demo.
* **Start Time** – Select Start immediately.
* **End Time** – Specify an ending time for the Event. For example, one hour from the current date/time.
* **Multicast+ Senders** – Select the Sender that you installed.
* **Multicast Channel** – Select Multicast+ Demo Channel.
* **Content Server URL** – Enter the URL for the video source. For example:

https://teststream.rampecdn.com/ramptv/loop.m3u8

* Click Save. Note that the Event has started, and that the following is displayed within the Events tab:



### Install the Multicast+ Receiver

***Note:*** *This step uses Windows as an example. For* *complete information, see the Multicast+ documentation.*

To install the Receiver:

1. Locate the Receiver installer file. For example:

C:\download\_location\rampecdn-n.n.n\rampecdn-n.n.n\rampreceiver-n.n.n-windows-x64-installer.exe

1. Double-click on the installer file. Proceed through the preliminary panels until the Installation Directory panel appears.
2. Select the installation directory for Ramp eCDN components by doing one of the following:
   * Accept the default location of C:\Program Files\rampecdn
   * Edit the path to specify another location.
   * Click the Folder button and navigate to another location.
3. Click Next. The Ready to Install panel appears.
4. Click Next, then click Finish when the installation is complete.

### Test Multicast+

The Ramp LiveTools Portal is an internal testing tool hosted by Ramp, and can be used to validate your Multicast+ environment.

To test Multicast+:

1. Open a browser, then enter the URI for the Ramp LiveTools Portal. For example:

http://livetools.rampecdn.com/portal/

The following appears:

Graphical user interface, application

Description automatically generated

1. In the Configuration section, enter the following:

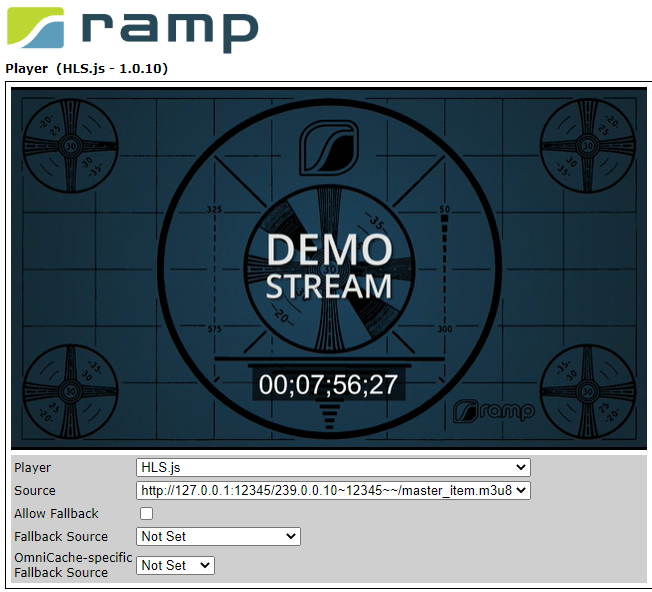
* Multicast Address:
  + Select Add New.
  + Enter the multicast address for the Multicast+ event.

For example: 239.0.0.10:12345

* Receiver Host:
  + Verify that http is selected.
  + Verify that 127.0.0.1 or localhost is selected.
* Click Apply.

The following occurs:

* The Portal attempts to detect the Multicast+ Receiver.
* Upon detection, the Receiver is started and attempts to join the Event on the specified multicast address.
* The Receiver receives segments from the Sender until it has a sufficient amount to start the video player. Once complete, the following appears in the Player section:



1. To view that Multicast+ is processing the video stream, see.

### View Multicast+ Analytics

Once the Receiver has joined the Multicast event and video is served back to the LiveTools Portal, you can view the data sent from Multicast+ using Core Analytics.

1. On the Core Analytics Dashboard, view the following:

Graphical user interface, application

Description automatically generated

Chart

Description automatically generated

The Multicast+ card indicates that Senders and Receivers have processed the test stream, and Unique Viewers indicates the number of users (with unique IP addresses) for the Sender.

# Troubleshooting

This section outlines some common issues that can occur when verifying your Ramp eCDN components.

## Altimeter/Core Analytics/Data Broker Connection Issues

If there appear to be connection issues with Altimeter/Core Analytics/Data Broker:

1. Collect the appropriate component logs listed in [Ramp eCDN Log Locations](#_Ramp_eCDN_Log).
2. Examine the logs.
3. If you see a message similar to the following:

Caused by: java.lang.IllegalStateException: org.springframework.jdbc.support.MetaDataAccessException: Could not get Connection for extracting meta-data;

The message indicates that the database connection string is invalid. Use the Ramp eCDN installer to update the component’s connection string, and restart the component.

***IMPORTANT:*** ***DO NOT start Core Analytics and Data Broker simultaneously. Start one component, wait 30 seconds, then start the other component.***

1. If you see a message similar to the following:

SEVERE [RMI TCP Connection(2)-127.0.0.1] org.apache.tomcat.jdbc.pool.ConnectionPool.init Unable to create initial connections of pool.

com.microsoft.sqlserver.jdbc.SQLServerException: The TCP/IP connection to the host 127.0.0.1, port 1433 has failed. Error: "Connection refused: no further information. Verify the connection properties. Make sure that an instance of SQL Server is running on the host and accepting TCP/IP connections at the port. Make sure that TCP connections to the port are not blocked by a firewall.".

The message indicates that the database server is not reachable or is down. Please verify that the database is running and reachable.

1. If you see a message similar to the following:

WARNING [main] org.apache.naming.NamingContext.lookup Unexpected exception resolving reference

com.microsoft.sqlserver.jdbc.SQLServerException: Login failed for user 'altimeter'. ClientConnectionId:e6247069-db64-4f5f-bfb0-e6c97381d893

The message indicates that the database server is reachable, but the password is incorrect. Please verify that you have the correct password for each user.

1. If you see a message similar to the following:

ERROR org.springframework.boot.SpringApplication [restartedMain] Application run failed

org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'flywayInitializer' defined in class path resource [org/springframework/boot/autoconfigure/flyway/FlywayAutoConfiguration$FlywayConfiguration.class]: Invocation of init method failed; nested exception is org.flywaydb.core.api.FlywayException: Found non-empty schema(s) [dbo] but no schema history table. Use baseline() or set baselineOnMigrate to true to initialize the schema history table.

The message indicates that the existing mate database was not set up correctly. Please drop, then create, the mate database. For example:

* MySQL:

Drop database mate;

Create database mate;

* SQL Server:

DROP DATABASE mate;

CREATE DATABASE mate;

## Multicast+ Sender or OmniCache Node Does Not Appear in Altimeter

Once installed, Multicast+ Senders and OmniCache nodes automatically register with Altimeter. If the components do not appear:

1. Verify that an active Altimeter is included in the Altimeter Servers list, as described in [Add the Current Altimeter to the Altimeter Servers List](#_Add_the_Current).
2. Verify that an active Data Broker is included in the Data Broker Cluster as described in [Add the Current Data Broker to the Data Broker Cluster List](#_Update_the_Data_1).
3. Verify that the correct ramp.manager.url and ramp.license are provided for the component. Update these values, then restart the component service:
   * Sender:   
     <install\_directory>\rampecdn\multicast\multicastplus\  
     component.properties
   * Omnicache: <install\_directory>\rampecdn\omnicache\omnicache\component.properties
4. Post-Installation Configuration

The sections below provide additional post-installation configuration that may be required according to the needs of your environment.

# Ramp eCDN Component Configuration and Usage

For information on configuring and using Ramp eCDN components:

|  |  |
| --- | --- |
| Component | Information Source |
| Altimeter | Altimeter is used to configure and work with other Ramp eCDN components.   * To customize aspects of Altimeter functionality to suit the needs of your environment, see *TechNote – Customizing Altimeter*. |
| Core Analytics | Core Analytics is used to provide performance monitoring reports on your Ramp eCDN environment.   * To customize aspects of Core Analytics functionality to suit the needs of your environment, see *TechNote – Customizing Core analytics and Data Broker*. * To view performance monitoring report information, see the *Core Analytics Monitoring Guide*. |
| Data Broker | Data Broker processes data collected from your environment for Core Analytics.   * To customize aspects of Data Broker functionality to suit the needs of your environment, see *TechNote – Customizing Core analytics and Data Broker*. |
| OmniCache | OmniCache is flexible and robust, and uses many default settings that are intended to work with most environments. However, configuration is required to meet the needs of your environment:   * For background information on OmniCache operation, see the *OmniCache Concepts Guide*. * For examples of common use cases, see the *OmniCache Configuration Guide*. * For information on the configuration tabs, see the *Altimeter Configuration Guide for OmniCache.* * For detailed configuration property information, see the *OmniCache Reference Guide*. |
| Multicast+ | The Sender uses default configuration settings that are intended to work for most environments. However, some configuration may be required to suit the needs of your environment:   * To activate the Program Guide or make changes to the Sender configuration property settings, see the *Multicast+ Sender Configuration Guide*. * For information on the configuration tabs, see the *Altimeter Configuration Guide for Multicast+.* |

# Setting Ramp eCDN Java Properties

This section describes how to use additional Java properties with Ramp eCDN components.

***Note:******Upgrading a Ramp eCDN component overwrites its <component>.properties file. To preserve your changes, you must BACKUP THE FILE in another location.***

To add Java properties to a component:

1. Locate the appropriate file for your component:

|  |  |
| --- | --- |
| Component | Location |
| Altimeter | **Windows:**  C:\Program Files\rampecdn\altimeter\altimeter.properties.sample  **Linux:**  /opt/rampecdn/altimeter/altimeter.properties.sample |
| Core Analytics | **Windows:**  C:\Program Files\rampecdn\coreanalytics\mate.properties.sample  **Linux:**  /opt/rampecdn/coreanalytics/mate.properties.sample |
| Data Broker | **Windows:**  C:\Program Files\rampecdn\databroker\databroker.properties.sample  **Linux:**  /opt/rampecdn/databroker/databroker.properties.sample |
| OmniCache | **Windows:**  C:\Program Files\rampecdn\omnicache\omnicache\_launch.properties.sample  **Linux:**  /opt/rampecdn/omnicache/omnicache\_launch.properties.sample |
| Multicast+ Sender | **Windows:**  C:\Program Files\rampecdn\multicast\multicast.properties.sample  **Linux:**  /opt/rampecdn/multicast/multicast.properties.sample |

1. (Administrator rights required) Copy and rename the file so “.sample” is removed from the name. For example:

* Original file name: <component>.properties.sample
* New file name: <component>.properties

1. (Administrator rights required) Edit the new file. Append your Java properties following the last property in the file. **Ensure that all new properties are added to the same line as the last property, and there are no line breaks**. For example:

… -<last property> -<your property 1> -<your property 2> …

|  |  |
| --- | --- |
| Property Type | Location |
| Heap Size | ***Note:*** *For recommended Java heap settings, see the “Hardware Summary” section of the Ramp eCDN Requirements Guide.*  Ramp eCDN components use Java heap memory to store objects that are created as part of normal operations.  As the amount of heap memory required varies according to the processing load experienced by the component, you may need to allocate more heap memory for the application by adjusting the heap memory settings.  To adjust the heap size for the component, use the following properties:   * -Xms*HEAP\_SIZE* – Defines the initial heap memory allocation. * -Xmx*HEAP\_SIZE* – Defines the maximum heap memory allocation.   For example, -Xms4000m and -Xmx4000m specify a heap size of 4GB. |
| Proxy | If a proxy is required by the Ramp eCDN component, use the following properties:   * -Dhttp.proxyHost=<*http\_proxy*> – Defines the HTTP proxy host. * -Dhttp.proxyPort=<*http\_port*> – Defines the HTTP proxy port. * -Dhttps.proxyHost=<*https\_proxy*> – Defines the HTTPS proxy host. * -Dhttps.proxyPort=<*https\_port*> – Defines the HTTPS proxy port.   ***Note:*** *If you have HTTP requests that should not be routed through the enterprise proxy, those hosts can be included by adding “nonProxyHosts” to the enterprise proxy parameters described below. For example:*   * *-Dhttp.nonProxyHosts=”host1.com|host2.com”* |

***Note:****To update other properties for Core Analytics or Data Broker, see TechNote – Customizing Core Analytics and Data Broker.*

1. Save the file.
2. Restart the service for the Ramp eCDN component:

***IMPORTANT:*** ***DO NOT start Core Analytics and Data Broker simultaneously. Start one component, wait 30 seconds, then start the other component.***

* Windows Services:
  + RAMP\_Altimeter
  + RAMP\_CoreAnalytics
  + RAMP\_DataBroker
  + RAMP\_MulticastPlus
  + RAMP\_OmniCache
* Linux Services:
  + ramp-altimeter
  + ramp-coreanalytics
  + ramp-databroker
  + ramp-multicastplus
  + ramp-omnicache

# Using Certificates

To configure Ramp eCDN components to use HTTPS, refer to the following sections of the documentation:

|  |  |
| --- | --- |
| Component | Description |
| Altimeter | Altimeter uses a self-signed certificate for HTTPS connections that can be updated, if needed.  The location and password for the certificate are set during the initial installation of the component. For more information, see [Install the Ramp Components](#_Install_the_Ramp).  To update the certificate, see “Updating the Altimeter SSL Certificate File” in *TechNote – Customizing Altimeter*. |
| Core Analytics | To use a certificate with Core Analytics for HTTPS connections, the location and password for the certificate are set during the initial installation of the component. For more information, see [Install the Ramp Components](#_Install_the_Ramp).  To update the certificate, see “ Updating the Core Analytics or Data Broker SSL Certificate File” in *TechNote – Customizing Core Analytics and Data Broker*. |
| Data Broker | To use a certificate with Core Analytics for HTTPS connections, the location and password for the certificate are set during the initial installation of the component. For more information, see [Install the Ramp Components](#_Install_the_Ramp).  To update the certificate, see “ Updating the Core Analytics or Data Broker SSL Certificate File” in *TechNote – Customizing Core Analytics and Data Broker*. |
| OmniCache | To use a certificate with OmniCache for HTTPS connections:   * See “Working with Certificates” in the *OmniCache Concepts Guide*. * In Altimeter, go to the OmniCache > Settings tab, then enter the information required for the Top Level Key Store settings.   For more information, see the *Altimeter Management Server Configuration Guide for OmniCache.* |
| Multicast+ Sender | To use a certificate with Multicast+ Sender for HTTPS connections:   * In Altimeter, go to the Multicast+ > Settings tab, then enter the information required for the Sender Key Store settings.   For more information, see the *Altimeter Management Server Configuration Guide for Multicast+.* |
| Multicast+ Receiver | The Receiver includes a default HTTPS certificate so that it can serve HTTPS content from localhost to standard browsers. To update the default certificate, see “Updating the Receiver Certificate” in the *Multicast+ Receiver Configuration Guide*. |

# Using MySQL Connector/J

During installation, Ramp eCDN components that use MySQL are configured using the MariaDB Connector/J JDBC driver that is supplied in the Ramp eCDN installer.

If needed, you can update the Ramp eCDN components to use MySQL Connector/J as described in *TechNote – Updating Ramp eCDN to Use MySQL Connector/J*.

# Using Data Broker Pass-Through Mode

During installation, Data Broker is set to run as the analytics endpoint, processing and writing analytics data collected from the Ramp eCDN components to the database:

* When configured to use Pass-Though Mode, Data Broker forwards data to an external service with a URL endpoint that supports Protocol Buffers or JSON, and the external service stores the data.
* To use Data Broker Pass-Through Mode, update the databroker.properties.sample file with the Packet Forwarding to External URL properties. For more information, see “Data Broker Customization Properties” in *TechNote – Customizing Core Analytics and Data Broker*.