evisions
MAPS
Multiple Application Platform Server

MAPS 6.10 Release Guide

Trademark, Publishing Statement, and Copyright Notice

Table of Contents

What's New in MAPS 6.10?

Evisions is pleased to announce the release of MAPS version 6.10, which includes the following changes:

- OpenSSL version can now be configured.

- Updated incremental searching capabilities.
- Improved the way changes made to IP Restrictions propagate to other clustered nodes.
- Additional enhancements and resolved issues.

We appreciate the feedback received from all of our users. Our products would not be what they are today without your continued support. If you have any comments or suggestions, please do not hesitate to open a case with the HelpDesk and let us know.

MAPS Updates

MAPS 6.10 is an update to the MAPS service and MAPS Config. You should upgrade both components concurrently.

Product versions

The latest versions of MAPS included in this release are:

- MAPS service 6.10.0.2636 / MAPS Config 6.10.0.1477 / MapsDBConfig 2.1.0.107

Installation

1. Prepare test environment and ensure current backup

We highly recommend installing updates in a test environment before applying them to your production environment. You should make sure that a current backup is available in case of any unforeseen issues. To create a full backup of your MAPS environment, go to the **Server** -> **Backups** screen in MAPS and click **Backup Now**.

2. Check for updates

Click the **Check for Updates** button in MAPS Config to view available updates.

> If you need to apply updates prior to the 6.10 update, please refer to the appropriate release guide(s) before proceeding.

It is possible to apply updates when users are on the system; however, to avoid the possibility of losing unsaved work we recommend applying updates during off hours.

3. Allow update process to complete

When applying updates to the MAPS service you will be temporarily disconnected from the server:
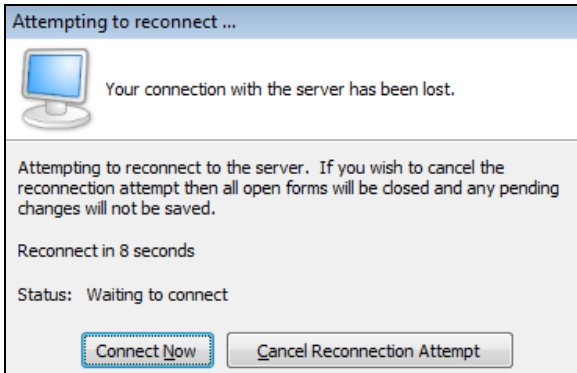
The update process may take a few minutes to complete. **Do NOT cancel the reconnection attempt or manually restart the server.** You will automatically be reconnected to the server once the update has been applied.

4. Verify the latest version is installed

To ensure that you are on the most current version, continue clicking the **Check for Updates** button and applying the updates until no new updates are available.

Please Provide Us with Your Feedback!

As always, we welcome any feedback or suggestions you may have. We very much appreciate your thoughts and suggestions, so please keep the great ideas coming!

HTTP/HTTPS File Server - Advanced

MAPS 6.10 includes several updates to the **HTTP File Server > Advanced Settings** screen in order to support OpenSSL version 1.1.1. These changes include the ability to select the **OpenSSL** version as well as the **Minimum** and **Maximum SSL** versions.

OpenSSL Version

The **OpenSSL Version** dropdown allows to specify the version of OpenSSL that will be used by the MAPS server. The default is version 1.1.1.

Note: When you change the OpenSSL version, SSL version, or ciphers (TLS version or cipher), the web server will restart.

Minimum and Maximum SSL Version

If your organization is required to support older browser versions, you may need to include obsolete SSL protocols. You can specify a minimum and maximum SSL / TLS version depending on the OpenSSL version you have selected. For OpenSSL 1.1.1, the minimum default SSL version is TLS 1, and the maximum default SSL version is 1.3. List of SSL/TLS support by browser

OpenSSL cipher list (TLS 1.2 and below)

The cipher list gives you complete control over the exact SSL ciphers that MAPS is allowed to use for TLS versions 1.2 and below. The cipher list contains one or more cipher strings in the format described in the OpenSSL 1.0.1 documentation.

OpenSSL cipher suites (TLS 1.3)

TLS 1.3 allows you to specify the exact cipher suites that MAPS is allowed to use, prioritized from left to right. The cipher suites contain one or more ciphers in the format described in the OpenSSL 1.1.1 Documentation.

Note: You should ensure there are no typos in the cipher value. Entering an empty cipher value will result in MAPS behaving as though you had entered the default cipher value. Entering an invalid cipher value may result in a failure to load the web server.

3rd-Party Security Checks

Some websites that provide software security checks may not issue a grade above a B+ due to the nature of some of the supported security ciphers. Specifically, RC4 ciphers are currently required to prevent Browser Exploit Against SSL/TLS (BEAST) attacks. It is therefore assumed that RC4 ciphers should be included in the OpenSSL cipher list. However, RC4 has its own security vulnerabilities that may lower the grade provided by security-checking software. If you choose to alter the default cipher list, you should be aware of the advantages and disadvantages provided by the ciphers you include.

MAPS 6.10 Release Notes

MAPS Service 6.10.0.2636 / MAPS Config 6.10.0.1477 / MapsDBConfig 2.1.0.107

MAPS

Enhancements

Area	Description	Issue number
Database	Updated the MAPS Database Configuration utility to support MAPS 6.10.	MAPS-3454
IP Restrictions	Changes made to an IP Restriction will now propagate to all other clustered nodes instantaneously.	MAPS-2100
Searching	Improved incremental searching capabilities for several areas of MAPS Config.	MAPS-3432
Security	Added version 1.1.1 to the list of existing OpenSSL files packaged with MAPS, and included the option to configure the OpenSSL version.	MAPS-1448

Resolved Issues

Area	Description	Issue Number
SSO	Certain SAML server configurations would cause authentication via Single Sign-On to fail with an Invalid Content-Length Header error message.	MAPS-3391

Getting Help

For information on using the software, please refer to the product Help, which contains detailed information on all aspects of the product.

If you are having problems with the installation or configuration, you can search our [support site](#), which includes a knowledge base of common issues. If you are unable to find the solution, submit a HelpDesk request with a detailed explanation of the problem you are experiencing.

Please do not hesitate to contact the Evisions HelpDesk if any questions or problems arise. We are here to help you and want to ensure your success.

Can't find what you're looking for?

We would love to make our documentation better! If you have a moment to let us know what we missed or how we can make the help more useful, please email us at TechDocs@evisions.com.