

Resolver.

PERSPECTIVE UPDATE INSTRUCTIONS

Version 5.10.1

May 2023

Perspective by Resolver Inc.™

Version 5.10.1

Distributed May 2023

Notices and Intellectual Property Information

Notice

The materials contained in this publication are owned or provided by Resolver Inc. and are the property of Resolver or its licensors, and are protected by copyright, trademark, and other intellectual property laws. No trademark or copyright notice in this publication may be removed or altered in any way.

Copyright

Copyright ©2022 Resolver Inc. All rights reserved. All materials contained in this publication are protected by Canadian, the United States, and international copyright laws and no part of this publication may be reproduced, modified, displayed, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of Resolver, 111 Peter Street, Suite 804, Toronto, Ontario M5V 2H1, Canada or, in the case of materials in this publication owned by third parties, without such third party's consent. Notwithstanding the foregoing, to the extent any material in this publication is reproduced or modified in any way (including derivative works and transformative works), by you or on your behalf, then such reproduced or modified materials shall be automatically assigned to without any further act and you agree on behalf of yourself and your successors, assigns, heirs, beneficiaries, and executors, to promptly do all things and sign all documents to confirm the transfer of such reproduced or modified materials to Resolver.

Trademarks

Protect What Matters, RiskVision and/or other products or marks referenced herein are either registered trademarks or trademarks of Resolver Inc. in Canada, the United States and/ or other countries. The names of actual companies, trademarks, trade names, service marks, images and/or products mentioned herein may be the trademarks of their respective owners. Any rights not expressly granted herein are reserved.

Changes

Companies, names, and data used in the examples herein are fictitious unless otherwise noted.

Although every precaution has been taken in preparation of this document, Resolver Inc. assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

Permission to modify and distribute this document strictly for the purpose of internal user training is hereby granted, provided that it is made evident the document has been modified, and that all copies contain all proprietary notices set forth in or on the original version. Resolver Inc. assumes no responsibility for errors or omissions resulting from the modification of this document. Resolver Inc. expressly waives all liability assumed for damages resulting from the modification of the information contained herein. Notwithstanding the permission granted herein, no part of this document may otherwise be reproduced, transmitted, disseminated or distributed, in any form or by any means, electronic or mechanical, for any other purpose, without the express written permission of Resolver Inc.

Table of Contents

System Requirements 2

Inbound & Outbound Ports..... 4

Inbound4

Outbound4

Update Instructions 5

 Database Upgrade 5

 Perspective Services (Application Server Setup) 7

 Configure Perspective Service Manager 11

Configure SSL Certificate Within IIS 16

 SQL Reporting Services Setup 16

Testing Perspective Implementation20

Advanced Configurations21

 Uninstall Dispatch Scheduled Services..... 21

 Connect Device Manager Configurations 21

 Dispatch Service Clustering 22

SAML Authentication for SSO23

Identity Provider Configuration 25

Manual Settings 27

Export Metadata 29

Perspective Configurations 30

Windows Authentication Configuration31

 MIR3 Mass Notifications (DispatchLog) 32

 Everbridge Mass Notifications (Dispatch) 33

Contact Information34

 Technical Support..... 34

 Resolver Inc. 34

System Requirements Version 5.10.1

The following requirements are for Perspective operating in a traditional LAN/WAN environment with the Web server component running on a separate Microsoft IIS box. These specs are for planning purposes only and apply to Perspective™ V.5.10.1, Dispatch, and Connect. Please contact your Resolver representative for a specific assessment of your needs.

NOTE: Meeting the **Minimum** system requirements means you can run the application successfully, but it may not provide the best performance. Meeting the **Recommended** requirements will offer a significantly better experience.

	MINIMUM	RECOMMENDED
CLIENT MACHINE		
Processor Speed	2 GHz dual-core	2.5 GHz dual-core
Memory	2 GB	4 GB
Operating System	Windows 8.1, Windows 10	
.NET Framework	Version 4.8	
Web Browser – Launch Perspective	Edge	
Web Browser – Web Portal	Edge, Google Chrome, Safari iOS 9+, Android Browser 4.2+	
Web Browser – Connect	Google Chrome	
Third Party Application	Adobe Reader 9.4.0+, Sun Java Runtime Environment 7 U71, 8 U25 ¹	
Mobile iOS App	iOS 10, iOS 11	
Officer Mobile	iOS 10 or newer, Android 8.0 or newer	
Resolution	1280x720, 1792 x 1344, 1920x1080, 1920x1440, 2560x1600, or 2736x1824. DPI 100%, 125%, 200%, or 225%.	
WEB SERVER MACHINE² (ON PREMISE ONLY)		
Available Disk Space ³	1 GB	2 GB
Processor Speed	2 GHz dual-core	2.5 GHz quad-core
Memory	8 GB	16 GB
Operating System	Windows Server 2012, Windows Server 2012 R2 ⁴ , Windows Server 2016, Windows Server 2019, IIS with WebSockets enabled ⁵ and Secure-Channel configured (HTTPS/SSL)	
.NET Framework	Version 4.7.2 with HTTP and non-HTTP activation, .NET Core 1.0.4 or 1.1.1 (Windows Hosting) ⁴	
C++ Runtime Libraries	C++ 2010 SP1 Runtime Libraries (x64) 10.40219	

Message Queue – Connect⁴/Dispatch⁵ service clustering	RabbitMQ Server 3.7.7+	
Inbound Ports⁶	443	
Outbound Ports⁶	443, 2195, 2196, 5223, 5228, 5672	
DATABASE SERVER MACHINE² (ON PREMISE ONLY)		
Available Disk Space	2 GB	20+ GB
Processor Speed	2 GHz dual-core	64-bit server dual-core or multi-processors
Memory	2 GB	4+ GB
Database Server⁷	SQL Server 2012 SP3, SQL Server 2014 SP2, SQL Server 2016 SP1, SQL Server 2017, or SQL Server 2019. All versions of SQL Server must include the Full-Text Search feature.	
Reporting Services	SQL Server 2012 Reporting Services, SQL Server 2014 Reporting Services, SQL Server 2016 Reporting Services, SQL Server 2017 Reporting Services	

1. This requirement only applies if you're using Visual Analysis.
2. These requirements apply to systems with up to 25 users. For systems with 25+ users, contact your Resolver account manager for more information.
3. Depending on the size of the Perspective database, more disk space may be needed for Workflow.
4. This requirement only applies if you're using Connect.
5. This requirement only applies if you're using Dispatch.
6. For more information on these requirements, see the [Inbound & Outbound Ports](#) article.
7. Only SQL Server Enterprise Edition is supported for indexing on audit tables.

Notes:

- Internet connectivity on the client machine is required for full functionality.
- The Perspective Client is deployed as a ClickOnce application, launched from Microsoft Edge. It has a zero-client footprint and doesn't require administrative rights to launch.
- If single sign-on authentication or add from Active Directory is used, Active Directory Services must be enabled on the Perspective Web Server.
- Net.TCP binding on port 808 is required only if using DispatchLog.
- For the best performance, do not run the Indexer on the same server where the database is hosted.

Inbound & Outbound Ports

The following ports may be required, depending on the additional components you have installed or will be installing.

Inbound

Port 443 is required for inbound connections to **Integration Services**.

Outbound

- **Perspective/Dispatch:**
 - `dev.virtualearth.net:443` for Bing Maps.
 - `dc.services.visualstudio.com:443` and `dc.applicationinsights.microsoft.com:443`. These ports are required only if **Application Insights** event logging is through **Microsoft Azure**.
- **Connect:** `<RabbitMQ hostname>:5672`. This port is required only if you're running a Connect integration with **Integration Services** 5.10 and up and a firewall exists between **Integration Services** and the configured **RabbitMQ** server.
- **Officer Mobile:** `dc.services.visualstudio.com:443` and `dc.applicationinsights.microsoft.com:443`. These ports are required only if **Integration Services** has been configured to send logs and telemetry to Application Insights.
 - **Officer Mobile (iOS):** All IP addresses on the entire 17.0.0.0/8 address block require 2195, 2196, and 5223 for **Apple Push Notification Services**.
 - **Officer Mobile (Android):** `android.googleapis.com:443` and `mtalk.google.com:5228` for Google Cloud Messaging.
- **Other Integration Services Clustered Instances:** `<Other IS instance hostname>: 443`. This port is required only if service clustering is enabled, and a firewall exists between instances.

Update Instructions

Note: Only SQL Server Enterprise Edition is supported for indexing on audit tables. If you're upgrading Perspective using a non-enterprise version of SQL Server, you'll encounter errors related to indexing on audit tables. However, you will still be able to successfully upgrade despite these error messages, as they will not negatively affect the application.

Database Upgrade

Note: The following instructions are for updating from 4.5 or later to 5.10. To update from Version 4.0 or earlier, visit the [Resolver Support](#) site and refer to the **Perspective Update Instructions 1.0 to 5.10** document.

1. Take a backup of your **Perspective SQL** database.
2. Make a copy of the **Perspective_Default.config** (by default, the file path is: **C:\inetpub\wwwroot\Perspective5.10\PerspectiveServices**) file and save it to your desktop.
3. Check to see the exact version of Perspective you are currently running by **executing** the following statement against your database within **SQL Server Manager**;

```
SELECT * FROM dbo.tblsystemsettings
```

Note: Legacy update scripts are provided in the previous updates folder with this installation. Please verify which version of Perspective you are running before proceeding with upgrading your database. If you require assistance, please reach out to [Resolver Support](#).

4. Update the Perspective database using the **Perspective Install > Database Setup > Update** folder. Using a **SQL query tool** (e.g., SQL Server Management Studio), **execute** update scripts against the Perspective database one at a time beginning from the version you are currently on, to the most current version.

Note: you will be provided with the Perspective Installation/Upgrade files by Resolver support, or you can access them [here](#).

- a. Run **SQLScript_Update_45_To_46.sql**.

- b. Run `SQLScript_Update_4.6.0_to_4.6.1`.
- c. Run `SQLScript_Update_4.6.1_to_4.6.2`.
- d. Run `SQLScript_Update_4.6.2_to_5.0.0.sql`.
- e. Run `SQLScript_Update_5.0.0_to_5.1.0.sql`.
- f. Run `SQLScript_Update_5.1.0_to_5.1.1.sql`.
- g. Run `SQLScript_Update_5.1.1_to_5.2.sql`.
- h. Run `SQLScript_Update_5.2.0_to_5.3.1.1.sql`.
- i. Run `SQLScript_Update_5.3.1.1_to_5.3.1.2.sql`.
- j. Run `SQLScript_Update_5.3.1.2_to_5.4.0.sql`.
- k. Run `SQLScript_Update_5.4.0_to_5.4.1.3.sql`.
- l. Run `SQLScript_Update_5.4.1.3 to 5.5.0.sql`.
- m. Run `SQLScript_Update_5.5.0 to 5.6.0.sql`.
- n. Run `SQLScript_Update_5.6.0 to 5.7.0.sql`.
- o. Run `SQLScript_Update_5.7.0 to 5.80.0.sql`.
- p. Run `SQLScript_Update_5.80.0 to 5.80.1.sql`.
- q. Run `SQLScript_Update_5.80.1 to 5.80.2.sql`.
- r. Run `SQLScript_Update_5.80.2 to 5.8.3.sql`
- s. Run `SQLScript_Update_5.8.3 to 5.90.sql`
- t. Run `SQLScript_Update_5.8.3 to 5.90.sql`
- u. Run `SQLScript_Update_5.90 to 5.10.sql`
- v. Run `SQLScript_Update_5.10 to 5.10.1.sql`

Note: The SQL script **BackFIII_SiteRollups.sql** can be run to check if a child value (Building, Location, or Section) has a latitude and longitude. If it's empty, it will match to the parent value. If all the items in the tier are in the same location and you're comfortable with this being implemented for mapping purposes, you can set up the **Site** only, and then use this to populate the lower tiers. If you're a Hosted client, please make this request via our [Resolver Support](#) team.

Note: The SQL script **Update_Inc_Act_Site_Geos.sql** can be run to populate the Geo Co-ordinates of all **Activities** and **Incidents** with a **SiteRollup** associated to them. This will only be run against **Activities** and **Incidents** without Geo Co-ordinates.

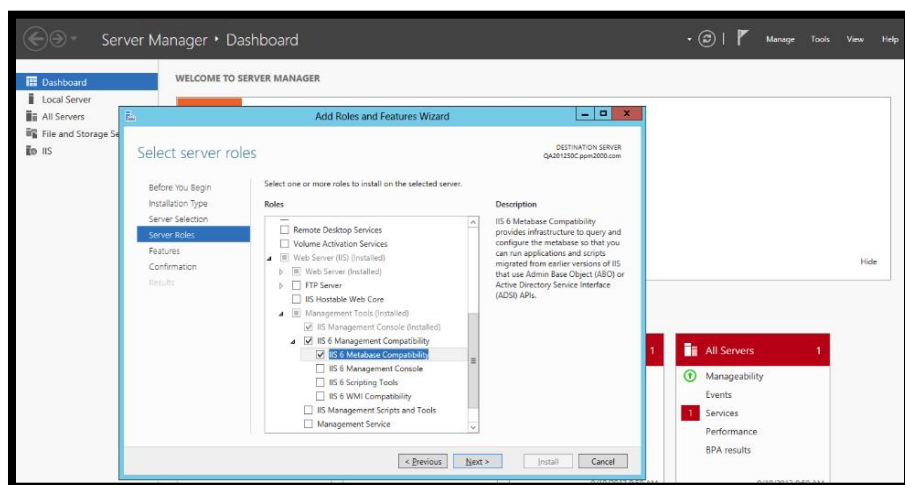
- Repeat step 6 for each Perspective database you're running (e.g., test, production, archive).

Perspective Services (Application Server Setup)

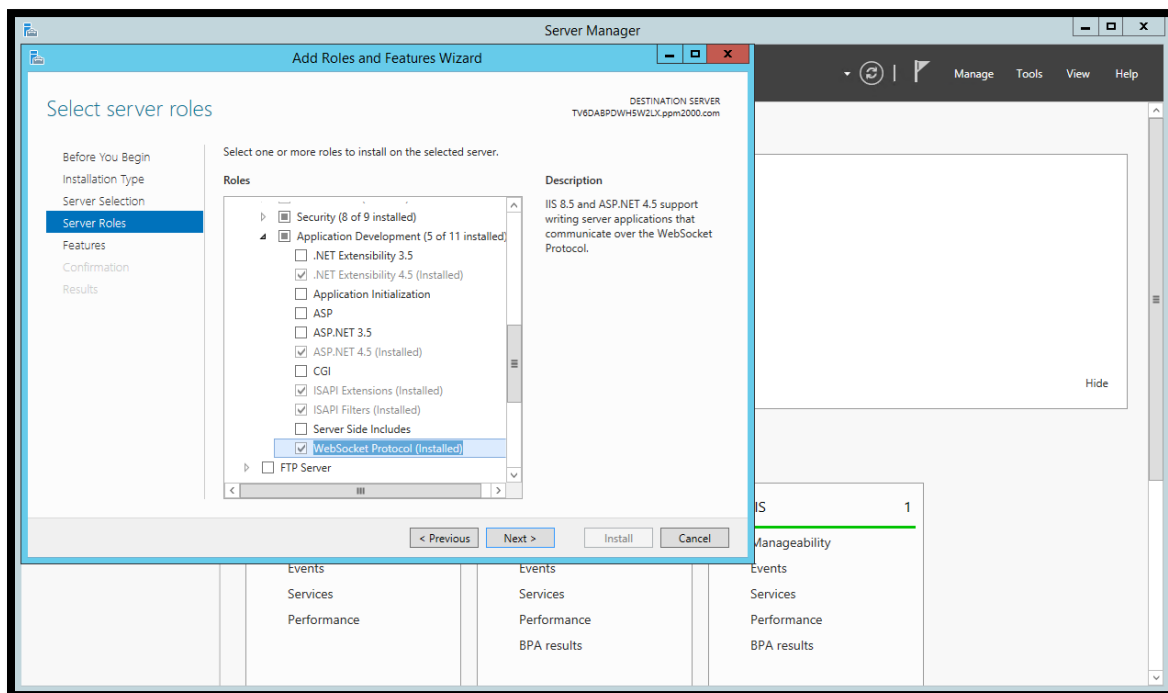
Completing the following steps will install **Perspective Services, Integration Services, Real Time Services, and Web Portal**.

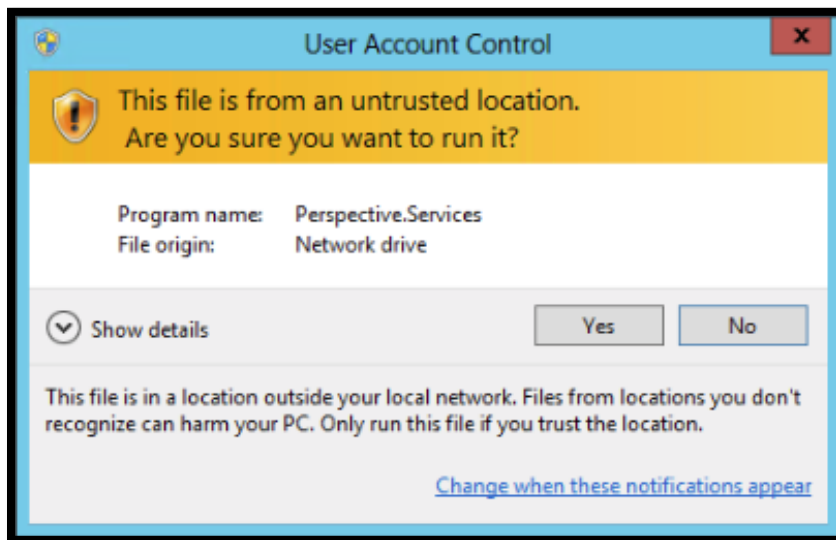
Ensure that **.Net Framework 4.8, IIS 6 Metabase Compatibility, and WebSocket Protocol** are installed on the Application Server via **Server Manager**.

Ensure **Internet Information Services (IIS)** is installed, and that **IIS** has **WCF Activation** turned on.

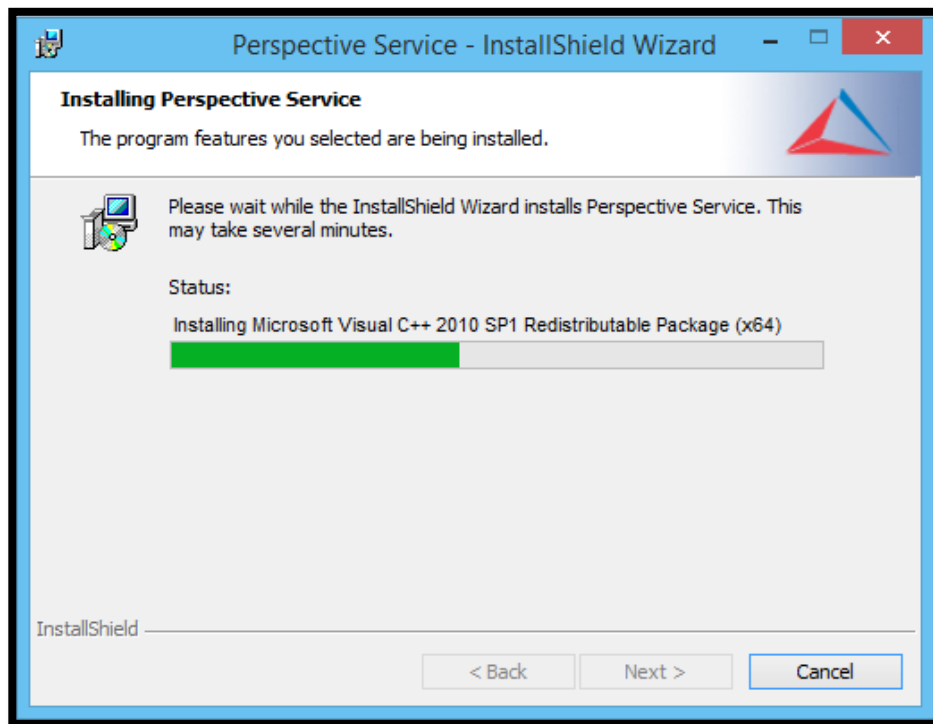


1. Uninstall the current versions of **Perspective.Services.exe** as well as **Perspective.ServiceManager.exe** found on the Application Server.
2. From the **Perspective 5.10** file, navigate to the **Web Service Setup** directory, run as an administrator **Perspective.Services.exe**. To complete the setup, follow the wizard's guidelines.
 - a. If the **User Account Control** screen pop-up window appears, click **Yes**.





- b. Wait for the **Perspective Service Setup Wizard** to start. Click **Next**.
- c. Review and accept the **Terms and Conditions**, and click **Next**.
- d. Select where you would like the application to be installed and click **Next**.
- e. Click **Install** to begin the installation.
- f. If **Visual C++ 2010 SP1 Runtime Libraries (x64)** is not installed, you will be prompted to install the **Runtime Libraries**. If already installed, skip to step 2i.



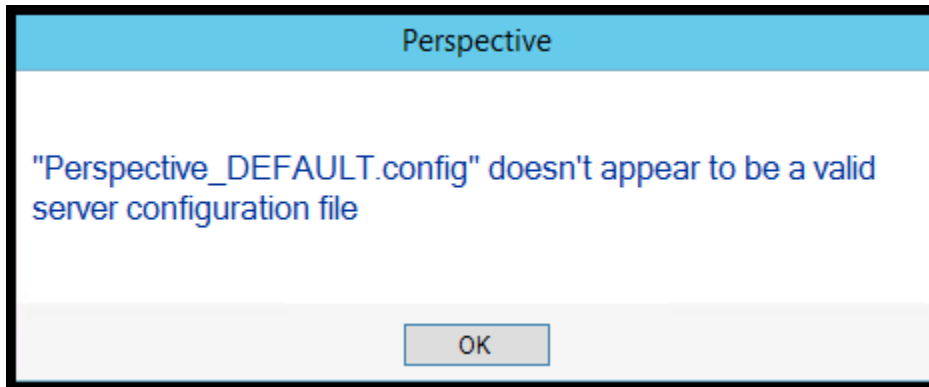
- g. Accept the **Terms and Conditions**, and click **Install**.
- h. When the installation is complete, click **Finish**.
- i. **Perspective Services** installation will continue.
- j. Click **Finish**.

Note: Only check the **Show the Windows Installer log** box if you want to see where the files have been installed.

- 3. From the same folder repeat Step 2 for **Perspective.ServiceManager.exe**. To complete the setup, follow the install wizard's guidelines.

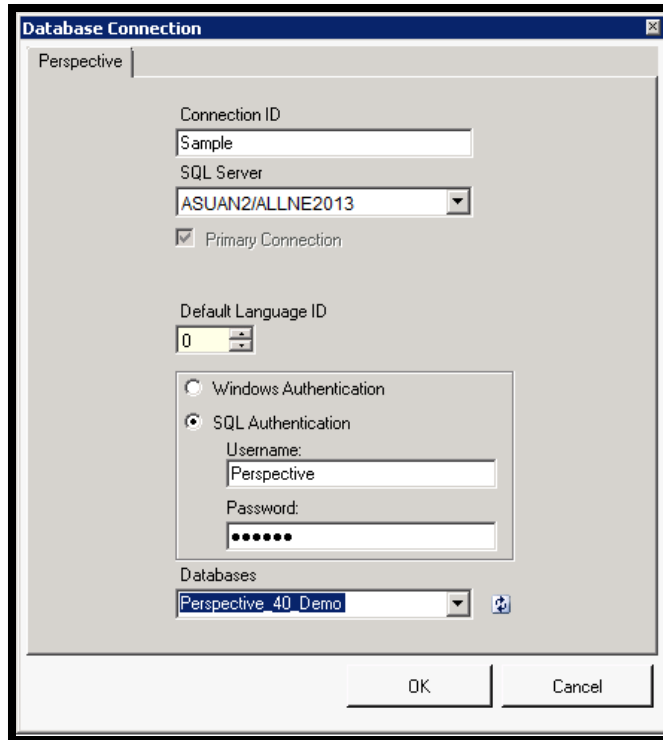
Configure Perspective Service Manager

1. Launch **Perspective Service Manager** from your desktop as an Administrator.
2. You will be prompted with the following notification:



3. Click **OK**.
4. Navigate to the file path where the **Perspective_Default.config** file would be (by default, the file path is: C:\inetpub\wwwroot\Perspective5.10\PerspectiveServices) and open the file.

- You will be prompted to input the database connection information.



- Enter a new name for **Connection ID**.

Note: The Connection ID cannot contain the word "Default".

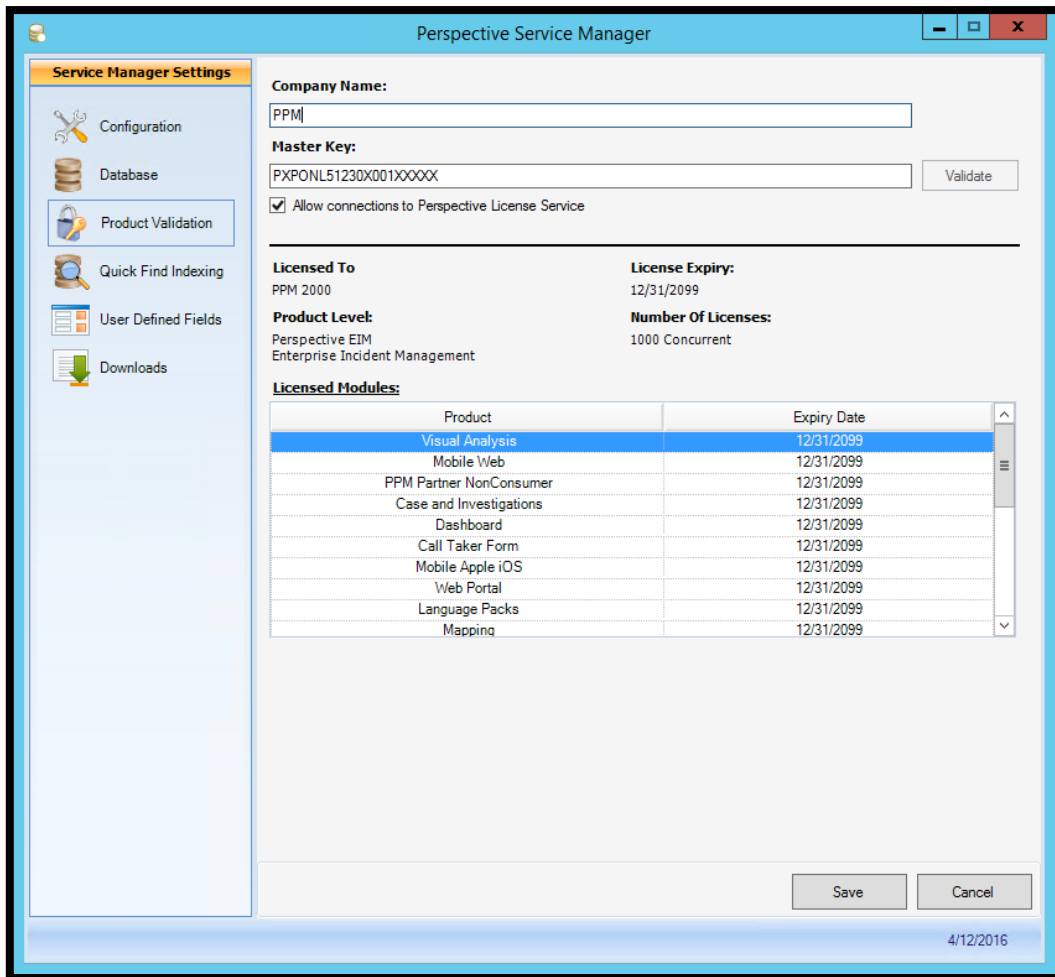
- In the **SQL Server** lookup list, select your SQL Server or type the name of your server in the text box.
- Leave **Default Language ID** set to **0**, unless instructed otherwise by Resolver.
- Ensure **SQL Authentication** is selected and enter the SQL **Username** and **Password** that has db_owner permissions you created when installing the database.
- Select your Perspective database from the **Databases** lookup list.
- Click **OK** to save.
- In the **Product Validation** tab, enter your **Company Name** and **Master Key**. If you do not know this information, you can reach out to [Resolver Support](#) for this information.

Note: The Master Key is case sensitive.

- Click the **Validate** button, if you have input the correct information, you will see your license details.

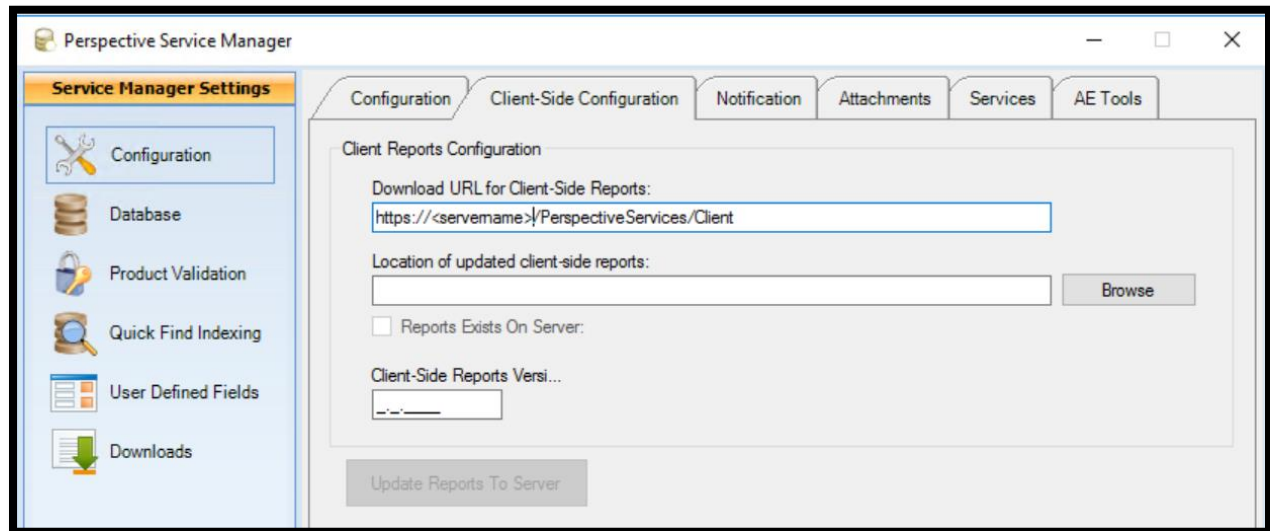
Note: The **Allow connections to Perspective License Service** box is checked by default.

Unchecking this box means a license file must be imported when you click the **Validate** button. If you do not have the file, you can reach out to [Resolver Support](#) for this information.



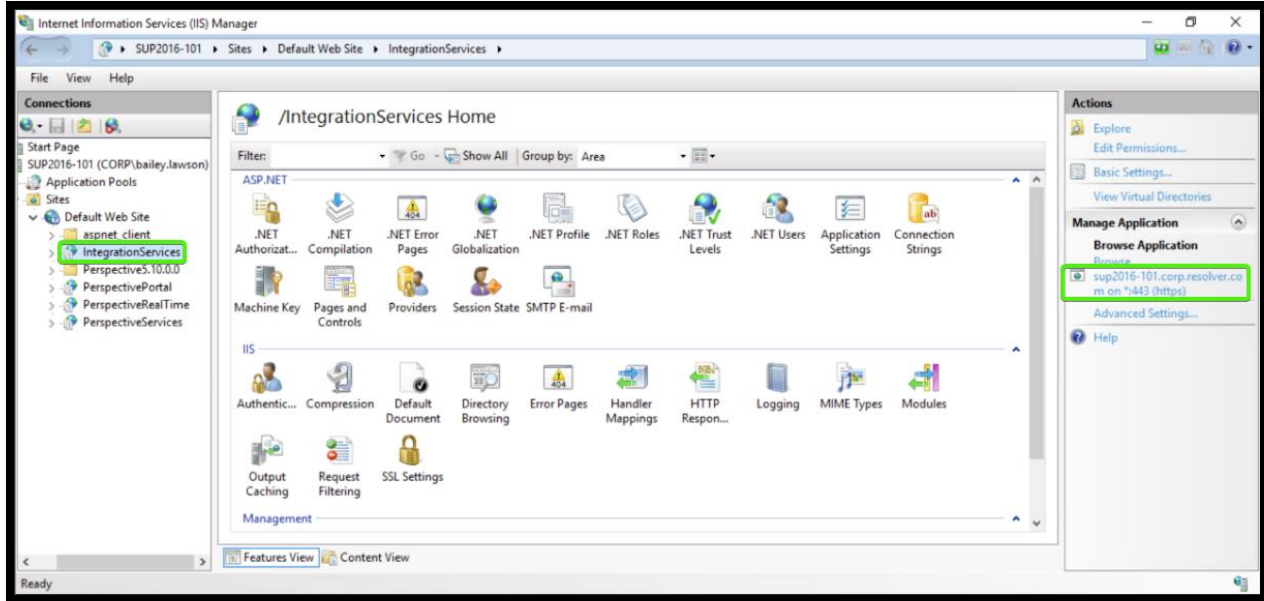
- Select the **Configuration** component from the Perspective Service Manager menu.
- To encrypt the Perspective_Default.config file, check the **Encrypt Configuration?** box.
- Open the **Client-Side Configuration** tab.
- Enter the **Download URL for Client-Side Reports**, this is needed for the client reports configuration files to update automatically (i.e., https://<servername>/perspectiveservices/client).

Note: Make sure that "/client" is appended at the end of the URL

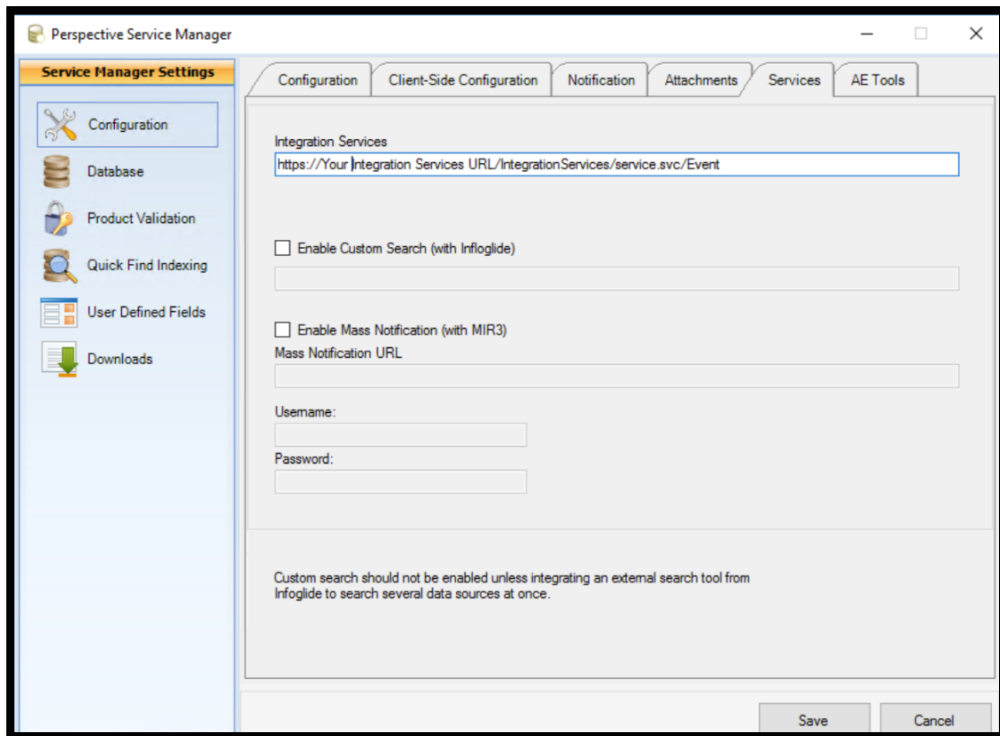


18. Click **Save**.
19. To enable event trigger in Integration Services, select the **Configuration** component from the Perspective Service Manager menu and open the **Services** tab.
20. Enter the URL bound to HTTPS in the **Integration Services** field.

- a. You can find the Integration Services URL by browsing to the **IntegrationServices** section in the **Default Web Site** section within **IIS**.



- b. Make sure to append "service.svc/Event" to the end of the URL.



21. Click **Save** and then close out of **Perspective Service Manager**.
22. Restart **IIS**.
23. Select the **Configuration** component from the **Perspective Service Manager** menu.
24. To encrypt the **Perspective_Default.config** file, check the **Encrypt Configuration?** Box.

Configure SSL Certificate Within IIS

1. Navigate to the **Default Web Site** within IIS.
2. Select **Bindings...**
3. Select **Add...**
4. Fill out each of the fields and select your SSL certificate.

Note: For more information about configuring SSL certificates, please refer to the [Microsoft SSL website](#).

SQL Reporting Services Setup

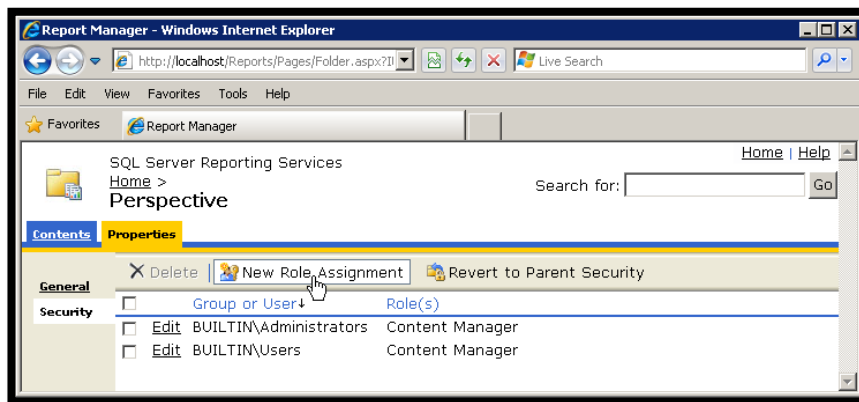
1. Ensure that **SQL Server Reporting Services** is installed.
2. From the Perspective install directory, copy the **Reports Setup** folder and all subfolders to a temporary directory on the Reporting Services computer.
3. Edit the **PublishServerReports.bat** file in the temporary directory. Before making any changes, save a backup copy of the original **PublishServerReports.bat** file.
 - Edit **databaseServerName** to <Name_of_Database_Server>.
 - Edit **databaseName** to <Name_of_Database>.
 - Edit **databaseUserId** to <sql_User_ID>.
 - Edit **databasePassword** to <sql_User_Password>.

4. Save changes and run the **PublishServerReports.bat** file to publish reports to the **Report Manager**. If the file fails to run, see [Troubleshooting Tips](#).

- a. Run the **Command Prompt** as Administrator
- b. Change the directory to the file path of the **Reports Setup** file path (this is the same file path the **PublishServerReports.bat** is saved in)
- c. Press **Enter**.
- d. Select and run the **PublishServerReports.bat** file.

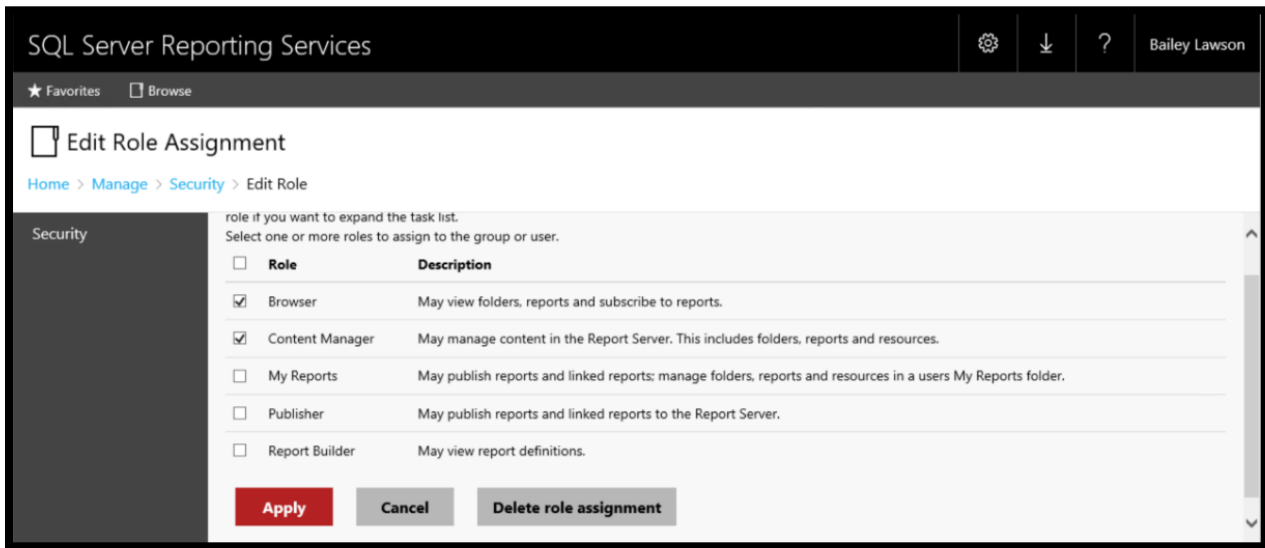
*Note: If you're using **Windows Authentication**, additional configuration of the **Reports** data source may be required.*

5. Browse to your **Reporting Services Web Site** (e.g. <https://localhost/Reports/>).
- a. On the Contents tab, click the **Perspective** folder.
- b. Click **Properties**, **Security** and **New Role Assignment**, then **Edit Item Security**.



- c. Enter a **Windows Service Account** for the Perspective application to use when connecting to **Reporting Services**. Create a new local user if you do not have one already. Ensure that the password is not set to expire.

- d. Select the **Content Manager** and **Browser** roles and click **OK**.



6. Open the **Database** section from the menu on the left, select your database name, and click the **Edit** button.
7. Open the **Services** tab and type the report server URL in the **Report Server URL** box.
8. Enter the name of your **Reports Folder**.
9. Proceed to the Report Service User section below. Enter the **Domain**, **Username** and **Password** that were granted browser rights when setting up the server-side reports.
10. Click the **Test** button. You should receive a prompt telling you the URL is valid. If not, confirm your configuration is correct and try again.

*Note: The account you configure here must also be a local user on the database server. To edit, add, or review your local users search for and open **lusrmgr.msc** within the **task bar search** feature to manage local users on the database server.*

11. Click **OK**.

The image shows a 'Database Connection' dialog box with the 'Authentication Mode' tab selected. The dialog contains the following fields and buttons:

- Report Service Host**: Report Server URL (text box containing 'http://myserver/reportserver') and Test... button.
- Reports Folder**: Perspective (text box).
- Domain**: User_Domain_Name (text box).
- Username**: User_Login_Name (text box).
- Password**: Password (password field with 10 dots).
- Device Manager**: Device Manager URL (text box) and Validate URL button.
- Buttons**: OK and Cancel buttons at the bottom.

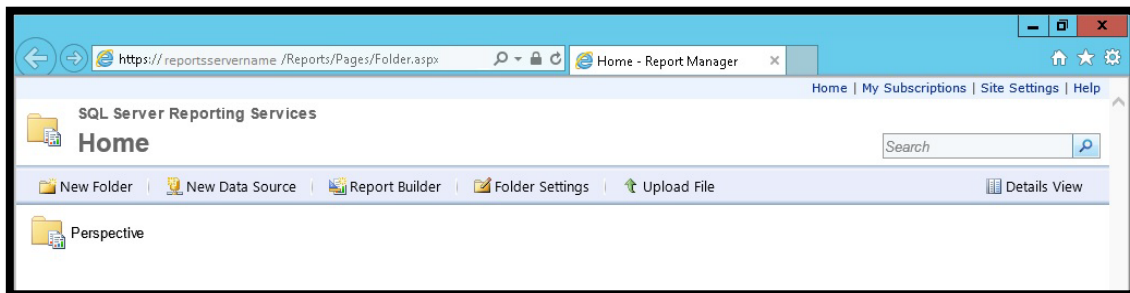
Testing Perspective Implementation

Once you have completed the steps outlined on the previous sections, please go through the following steps to ensure that all Perspective's components have been set up properly.

Note: Following the configuration of the Web Server, please ensure application initialization has taken place so that end users do not experience delays with initial page loading. After any IIS reset or configuration, navigate to <https://<servername>/IntegrationServices/service.svc> to begin the application initialization.

1. Go to the **Perspective Services** URL and confirm that the page loads properly:
<https://<localhost>/perspectiveservices>, where **<localhost>** is the appropriate local host address on your network.
2. Go to the **Perspective Services** page and confirm that the page loads properly:
<https://<localhost>/perspectiveservices/service.asmx>, where **<localhost>** is the appropriate local host address on your network.
3. Go to the **Report Manager** page and confirm that the page loads properly:
<http://<reportservername>/reports>, where **<reportservername>** is the appropriate address for the Reports Server on your network.

*Note: If your **Report Manager** page does not display correctly, run the **PublishServerReports.bat** file included in the **Perspective Install > Reports Setup** folder.*



4. Log on to the **Perspective Client**—preferably not on the server itself—using your Perspective Administrator username and password.
5. Once you have logged on successfully, click on the **Reports** button in the navigation pane and confirm that all reports are listed. The easiest way to confirm that the client-side reports are working is to verify that there are reports listed under the **Detail Reports** heading, such as the **Incident, Person, and Vehicle Reports**.
6. To also confirm you are connected to the correct database, run the **Workgroup List** report and verify the workgroups listed.

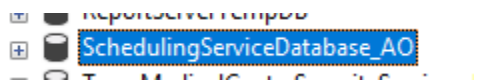
7. To confirm that the server-side reports are working, try running the **Test Report** under the **Administrative Only** section listed. If you receive an error message, see the [Troubleshooting Perspective & SQL Reporting Services](#) article for more information.

Note: Both the Report Version and Database Version should display as 5.1

Advanced Configurations

Uninstall Dispatch Scheduled Services

Dispatch Scheduled Services is now integrated in the **Integration Service** and is no longer required. **Dispatch Scheduled Services** should be **removed** by deleting the scheduling service Database in SQL



Connect Device Manager Configurations

This section applies to users installing an instance of Perspective with the **Dispatch** application, along with **Connect 1.1**. If you're not installing an instance of Perspective with **Dispatch** and **Connect**, skip this section.

Note: To successfully configure the **Device Manager**, the **Perspective_default.config** file cannot be encrypted through **Perspective Service Manager**.

1. Open the **Perspective_default.config** file “by default, the file path is: **C:\inetpub\wwwroot\Perspective5.10\PerspectiveServices**”.
2. Scroll down to the bottom of the file and locate the `<DeviceManagerURL>` tags.
3. Change the URL in the tags to point to the **Connect Server**.

```
<DeviceManagerURL>https://<ConnectServerName>/api/</DeviceManagerURL>
</PerspectiveConfig>
```

Note: Only one **Device Manager URL** is permitted per config file.

4. If you're using the **Alarms** feature in **Connect** and **Dispatch**, enter the following tags below the `<DeviceManagerURL>` tag, entering the RabbitMQ server information within the tags as required:

```
<ConnectQueueConfiguration>
  <HostName>...</HostName>
  <VirtualHost>...</VirtualHost>
  <UserName>...</UserName>
  <Password>...</Password>
  <NetworkRecoveryIntervalInSeconds>...</NetworkRecoveryIntervalInSeconds>
</ConnectQueueConfiguration>
```

5. **Save** your changes, then close the file.

Dispatch Service Clustering

This section applies to users who are installing an instance of Perspective with **Dispatch** and wish to implement **Dispatch Service Clustering**. If you're not installing **Dispatch** or you do not wish to use **Dispatch Service Clustering**, skip this section.

1. Ensure [RabbitMQ 3.7.7](#) or later is installed on the Perspective Application Server.
2. Navigate to the install directory of **Integration Services** (by default the file path is `C:\inetpub\wwwroot\Perspective5.10\IntegrationService`).
3. Open the **Web.config** file.
4. In the `<appSettings>` tags, make changes as needed to the following settings for the deployed web server:
 - a. **PerspectiveConfigFilePath**: The path where Perspective Services is deployed.
 - b. **ServiceClusters**: Enter **true** or **false** to enable or disable service clustering for **Dispatch**.
 - c. **ClusterProcessID**: Enter a number, GUID, or string to identify the instance of **Integration Services**.
5. Copy and paste the `<appSettings>` section and complete the required fields for each instance of **Integration Services**.

Note: Each instance must be assigned a unique number in the `<ClusterProcessID>` tags.

6. Save your changes in the **Web.config** file, then close it.
7. Open the **Perspective_default.config** file (by default, the file path is:
C:\inetpub\wwwroot\Perspective5.10\PerspectiveServices).
8. In the `<ClusterQueueConfiguration>` tags, enter the following information:
 - a. **HostName:** The RabbitMQ hostname.
 - b. **VirtualHost:** The name of the RabbitMQ virtual host that will be used for clustering.
 - c. **User:** The username of the RabbitMQ user with CRUD access to the virtual host.
 - d. **Password:** The RabbitMQ user's password.
 - e. **NetworkRecoveryIntervallInSeconds:** The number of seconds between each network recovery interval.
 - f. **RequestHeartbeatIntervallInSeconds:** The number of seconds between each heartbeat interval.
9. Save your changes in the **Perspective_Default.config** file, then close it.

SAML Authentication for SSO

This section provides instructions on configuring **Perspective Service Manager** to implement **SSO**, however, prior to completing these steps, you must confirm your **Identity Provider (IdP)** supports **SAML 2.0 through service provider initiated SSO**. **SSO** is supported for use with the Enterprise edition of Perspective.

Your IdP will also need to provide you with instructions on adding and configuring new and existing Perspective users directly through their service as IdP configurations will vary.

Note: If you're using AD FS to configure SAML, see the [Set Up SSO with AD FS](#) article on the Resolver Support site for instructions after following the steps below.

1. Open **Perspective Service Manager**.
2. Click **Configuration** component.
3. Select the **Configure Service Provider** checkbox.

4. Enter your **Perspective Services** URL in the **Perspective URL** field, then click **Validate**.

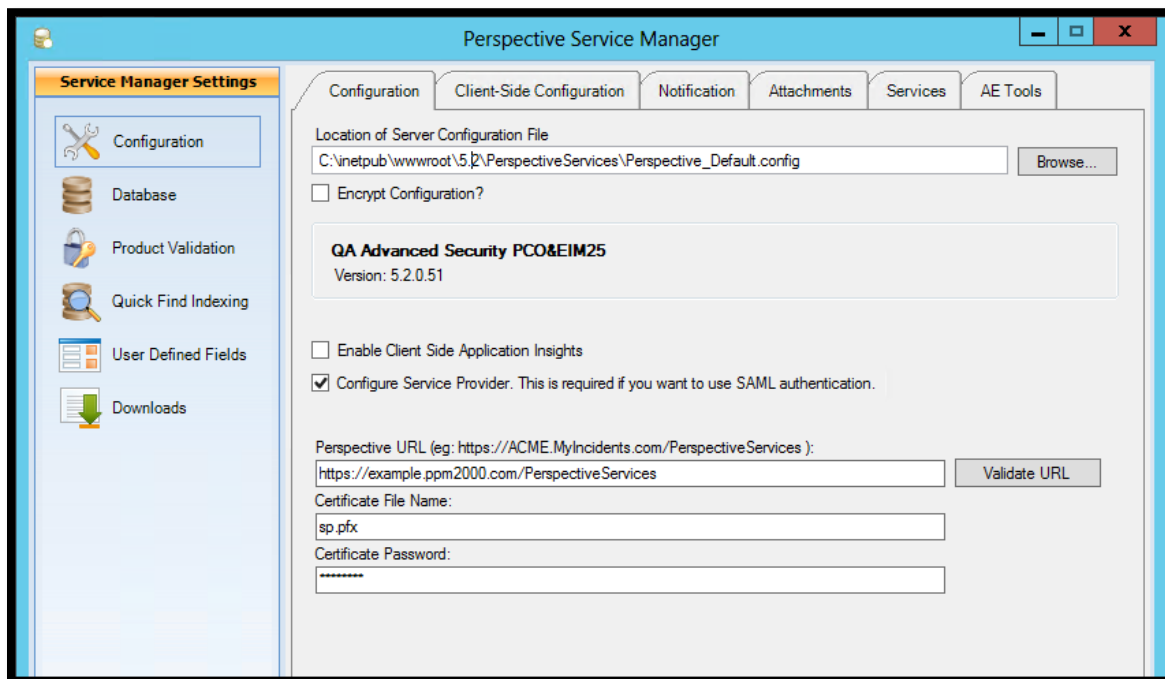
Note: The URL you enter in this field must exactly match what has been entered into your IdP's configurations, including the case (upper-case or lower-case letters) and slash (/ or \) direction.

5. Enter the server certificate file name in personal exchange format (.pfx) in the **Certificate File Name** field and enter a password in the **Certificate Password** field.

Note: For testing purposes, a sample .pfx file has been included in the installation package with a file name of **sp.pfx** and a password of **password**. This information is required so that the services (Perspective, Dispatch, Dashboard, etc.) can securely communicate with the identity provider.

6. Save a copy of the certificate file to ***PerspectiveInstallationPath*\PerspectiveServices\SAML\Certificates**. This file usually has a .PFX extension and will also need to export the private keys.

Note: If you chose the default certificate file, the file was saved at this location during installation.



Note: After completing the above steps, you'll need to select how you will input the identity provider's details.

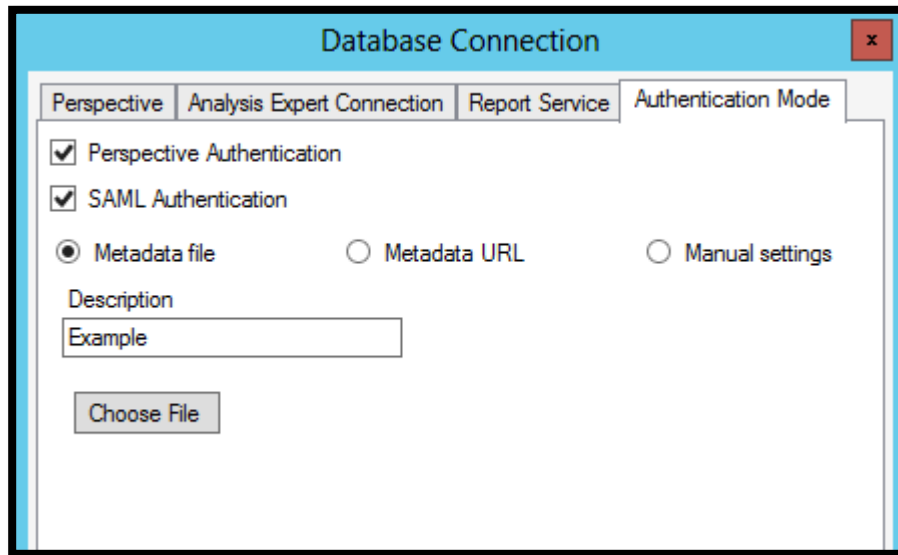
Identity Provider Configuration

The settings below allow you to import your IdP's configurations directly into **Perspective Service Manager** via a metadata file or metadata URL, which is obtained from your IdP.

1. In **Perspective Service Manager**, click the **Database** component.
2. **Edit** one of the configured databases.
3. Click the **Authentication Mode** tab.
4. Select the **SAML Authentication** checkbox.

Note: If this option is unavailable, the service provider information has not been properly configured in steps 3 and/or 4 in the section above.

5. Select how you want to input the identity provider information:
 - 6) **Metadata file:** This option will require that you obtain a metadata file from your IdP to import the **SSO** configurations into **Perspective Service Manager**. When downloading a metadata file from your IdP, the certificate is usually extracted and saved in your **My Documents** folder, but it must be moved to ***PerspectiveInstallationPath*\PerspectiveServices\SAML\Certificates** after it's been downloaded.
 - To use this option, after downloading the file, enter the name of your IdP in the **Description** field, which will appear to users with the phrase "Login with [IdP]" on the login screens, then click **Choose File** to upload the metadata file.

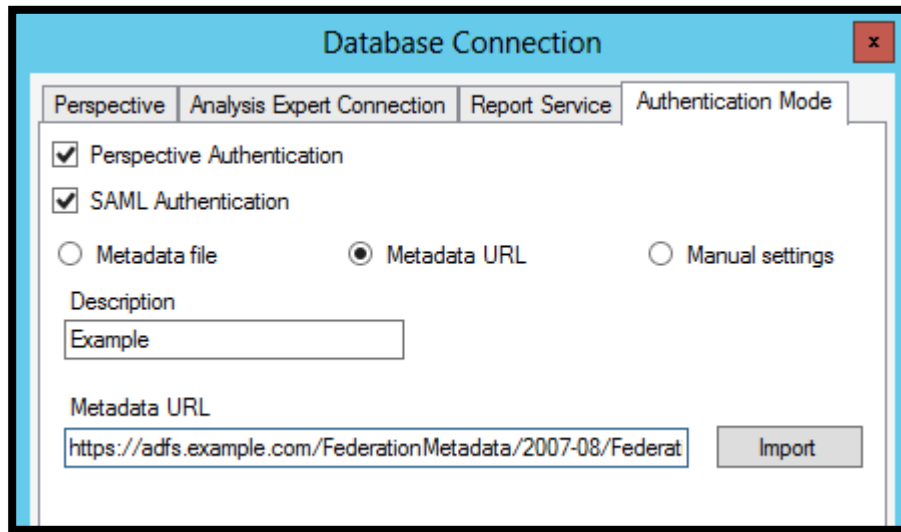


The screenshot shows a 'Database Connection' dialog box with a blue header and a close button (X) in the top right corner. The dialog has four tabs: 'Perspective', 'Analysis Expert Connection', 'Report Service', and 'Authentication Mode'. The 'Perspective' tab is active. Inside the dialog, there are two checked checkboxes: 'Perspective Authentication' and 'SAML Authentication'. Below these are three radio buttons: 'Metadata file' (which is selected), 'Metadata URL', and 'Manual settings'. Under the 'Metadata file' radio button, there is a 'Description' label and a text input field containing the word 'Example'. Below the text field is a 'Choose File' button.

- **Metadata URL:** This option will require that you obtain a metadata URL that will import the SSO configurations into **Perspective Service Manager**. After obtaining the URL, enter the name of your IdP in the **Description** field, which will appear to users with the phrase “Login with [IdP]” on the login screens. Enter a valid metadata URL from your IdP in the **Metadata URL** field, then click **Import**. The URL will import the required configurations and should be similar to the following:

`https://adfs.example.com/FederationMetadata/2007-06/FederationMetadata.xml`

Note: The URL you enter in the **Metadata URL** field must **exactly** match what has been entered into your IdP’s configurations, including the case (upper-case or lower-case letters) and slash (/ or \) direction.



6. Click **OK**, then save your changes.

Manual Settings

If you're not importing metadata via a file or URL, you must configure your IdP's settings manually. Contact your IdP for instructions on obtaining the required information.

1. In **Perspective Service Manager**, click the **Database** component.
2. **Edit** the configured database.
3. Click the **Authentication Mode** tab.
4. Select the **SAML Authentication** checkbox.

*Note: If this option is unavailable, the service provider information has not been properly configured. See the **Identity Provider Configuration** section above for more information.*

5. Select the **Manual settings** option.
6. Complete the following fields:
 - **Description:** The name of your IdP, which will appear to users with the phrase "Login with [IdP]" on the login screens.
 - **Name:** The exact name of the IdP as provided by the IdP.

- **Partner Certificate File:** Used to verify the assertions have come from the IdP. This file must be saved to the ***PerspectiveInstallationPath*\PerspectiveServices\SAML\Certificates** folder.
- **Single Logout URL:** The URL from which the IdP accepts logout requests.
- **Single Sign On Service:** The URL from which the IdP accepts SSO requests.
- **Name ID Format:** The username format provided to the IdP.
- **Single Sign On Service Binding:** The binding used by the IdP to authenticate (usually HTTP Redirect).
- **Sign Authentication Request:** Select this checkbox if the authentication request should be signed.
- **Sign Logout Request:** Select this checkbox if the logout request should be signed.
- **Sign Logout Responses:** Select this checkbox if the logout response should be signed.
- **Sign Assertion:** Select this checkbox if the assertions should be signed.
- **Encrypt Assertions:** Select this checkbox if the assertions should be encrypted.

Database Connection

Perspective | Analysis Expert Connection | Report Service | **Authentication Mode**

Perspective Authentication
 SAML Authentication

Metadata file Metadata URL Manual settings

Description
Example

Name
http://adfs.example.ppm2000.com/adfs/servi

PartnerCertificateFile
555EF9FF58A8EXAMPLE28D283123634.cer

Single Logout Service Url
https://adfs.example.ppm2000.com/adfs/ls

Single Sign On Service Url
https://adfs.example.ppm2000.com/adfs/ls

Name ID Format
Windows Domain Qualified Name

Single Sign On Service Binding
HTTP Redirect

Sign Authentication Request
 Sign Logout Request
 Sign Logout Response
 Sign Assertion
 Encrypt Assertion

Export Metadata

OK Cancel

7. Click **OK** then save your changes.

Export Metadata

Once you've completed the configurations in the previous sections, your IdP will likely require Perspective metadata to complete the **SSO** process. This information can be exported into a file using the **Export Metadata** tool in **Perspective Service Manager**.

1. In **Perspective Service Manager**, click the **Database** component.
2. **Edit** the configured database.
3. Click the **Authentication Mode** tab.
4. Select the **Manual Settings** option.

5. Click **Export Metadata**.
6. Navigate to the ***PerspectiveInstallationPath*\PerspectiveServices\SAML\Certificates** folder.
7. Select a file name and location to export the metadata.

Note: It's recommended that you save the metadata file in

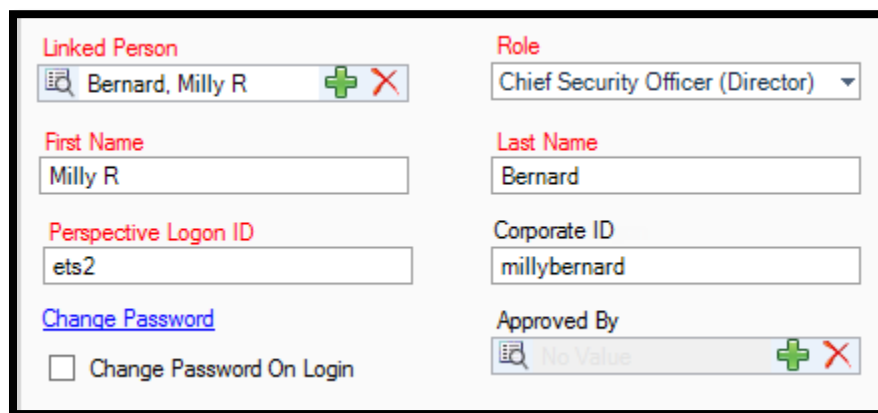
***PerspectiveInstallationPath*\PerspectiveServices\SAML\Metadata** in the **PerspectiveServices** installation directory.

8. Click **OK** and the metadata file will be opened. Either upload a copy of this file to your IdP server or save a copy in the ***PerspectiveInstallationPath*\PerspectiveServices\SAML\Metadata** folder if you did not choose that location in step 6.

Note: The URL in the **<ServiceProviderBaseURL>** tags in the metadata file must **exactly** match what has been entered into your IdP's configurations and Perspective Service Manager, including the case (upper-case or lower-case letters) and slash (/ or \) direction.

Perspective Configurations

Once the **Perspective Service Manager** and IdP configurations are complete, a Perspective administrator must enter each user's **SSO Username** (as it's configured in the IdP's settings) in the **Corporate ID** field by going to **Administration > Users > User Details**.



The screenshot shows a user profile configuration form with the following fields and values:

Linked Person Bernard, Milly R	Role Chief Security Officer (Director)
First Name Milly R	Last Name Bernard
Perspective Logon ID ets2	Corporate ID millybernard
Change Password <input type="checkbox"/> Change Password On Login	Approved By No Value

See the [Perspective Administrator's Guide](#) for more information on entering this information in a user's profile.

Windows Authentication Configuration

Follow the steps below to configure Windows Authentication for your Perspective environment.

Note: If you wish to use single sign-on authentication for all Perspective modules (Perspective, Dispatch, Dashboard, and/or Web Portal) you must enable [SAML authentication](#).

1. Open the **Perspective_default.config** file (by default, this file is located at **C:\inetpub\wwwroot\Perspective5.10\PerspectiveServices**).
2. Locate the `<WindowsAuthentication>` tag.
3. Delete the **false** value in the tag and replace it with **true**.

Note: You **cannot** enable both Windows authentication and SSO in the **Perspective_default.config** file by changing the `<SSOAuthentication>` tag's value to **true**.

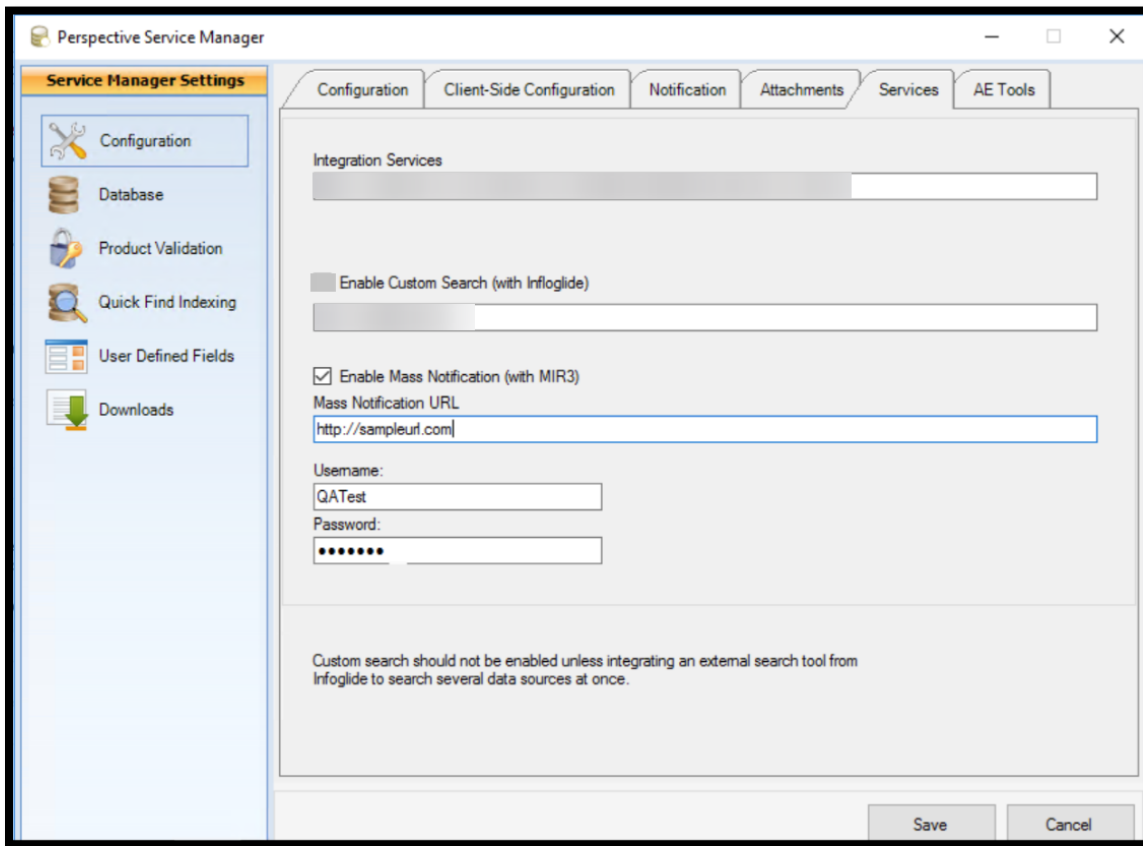
```
<MSReportServiceUser>
  User_Domain_Name;User_Login_Name;User_Password</MSReportServiceUser>
  <PerspectiveAuthentication>true</PerspectiveAuthentication>
  <WindowsAuthentication>false</WindowsAuthentication>
  <SSOAuthentication>false</SSOAuthentication>
  <PartnerIdentityProvider Name="" Description=""
```

4. **Save** the file.
5. **Restart** the server in **IIS** to complete the configuration.
6. Once the above changes are complete, a Perspective administrator must enter each user's **Windows Authentication** username in the **Corporate ID** of the Perspective user account field by going to **Administration > Users > User Details**.

MIR3 Mass Notifications (DispatchLog)

Perspective allows users to integrate their **MIR3 Mass Notifications** into Perspective to send mass notifications about selected activities via Perspective **DispatchLog**. **MIR3 Mass Notifications** are not available in **Dispatch**.

1. Select the **Configuration** component in **Perspective Service Manager**.
2. Open the **Services** tab.
3. Check the **Enable Mass Notification (with MIR3)** box and enter the **Mass Notification URL**,



The screenshot shows the 'Perspective Service Manager' application window with the 'Services' tab selected. The left sidebar contains a 'Service Manager Settings' menu with options: Configuration, Database, Product Validation, Quick Find Indexing, User Defined Fields, and Downloads. The main content area is titled 'Integration Services' and contains the following fields and controls:

- Enable Custom Search (with Infoglide)
- Enable Mass Notification (with MIR3)
- Mass Notification URL:
- Username:
- Password:

At the bottom of the main content area, there is a note: "Custom search should not be enabled unless integrating an external search tool from Infoglide to search several data sources at once." At the bottom right of the window, there are 'Save' and 'Cancel' buttons.

Username and Password provided by MIR3 in the field below.

Linked Person Bernard, Milly R	Role Chief Security Officer (Director)
First Name Milly R	Last Name Bernard
Perspective Logon ID ets2	Corporate ID millybernard
Change Password <input type="checkbox"/> Change Password On Login	Approved By No Value

7. See the [Perspective Administrator's Guide](#) for more information on entering this information in a user's profile.

Everbridge Mass Notifications (Dispatch)

Perspective allows users to integrate their **Everbridge Mass Notification** solution into Perspective to send mass notifications about selected activities via **Dispatch**. **Everbridge Mass Notifications** are not available in **DispatchLog**.

1. Open the **Perspective_default.config** file (by default, it can be found at **C:\inetpub\wwwroot\Perspective5.10\PerspectiveServices**).
2. Locate the **<EverbridgeConnectionInfo>** tags and enter the following information:
 - **ManagerURI:** Enter the Everbridge management URL.
 - **URL:** Enter the Everbridge API URL.
 - **User:** The username of the Everbridge user account that will provide access to the system.
 - **Password:** The user's password.

- **Org:** The Everbridge org ID.

```
<EverbridgeConnectionInfo>ManagerURL=https://manager.everbridge.net;  
URL=https://api.everbridge.net/rest;User=user.name@company.com;  
Pass=EverbridgePassword;Org=12345678912345 </EverbridgeConnectionInfo>
```

3. Save the **Perspective_default.config** file and close.

Contact Information

If you experience any issues along the way when performing your install or upgrade of Perspective, please check out [this FAQ](#) to see if it may solve the issue you are experiencing. If not, feel free to reach out to our support team!

Technical Support

Toll Free: 1-877-776-2995
Phone: (780) 448-0616
Email: support@resolver.com
Website: <https://support.resolver.com>

Resolver Inc.

Toll Free: 1-888-776-9776
Phone: (780) 448-0616
Fax: (780) 448-0618
Email: information@resolver.com
Website: <http://www.resolver.com>