

# **RESOLVER**

## PERSPECTIVE UPDATE INSTRUCTIONS

Version 5.5

August 2018

## Perspective Update Instructions by Resolver Inc.™

Version 5.5

Distributed August 2018

## 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 ©2019 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

<b>SYSTEM REQUIREMENTS .....</b>	<b>1</b>
<b>Inbound &amp; Outbound Ports.....</b>	<b>3</b>
<b>Update Instructions .....</b>	<b>4</b>
Important Notes About SQL Server .....	4
Database Upgrade .....	4
Dispatch Scheduling Services Database Restore .....	6
Dispatch Scheduling Services.....	10
Dispatch Service Clustering .....	13
Everbridge Mass Notifications (Dispatch) .....	15
Connect Device Manager Configurations .....	15
Updating SQL Reports .....	17
<b>SAML Authentication for SSO .....</b>	<b>18</b>
Identity Provider Configuration .....	19
Manual Settings.....	21
Export Metadata.....	23
Perspective Configurations.....	24
Integration Services .....	25
Perspective Services Update .....	25
<b>Windows Authentication .....</b>	<b>29</b>
<b>Testing Perspective Implementation .....</b>	<b>30</b>
<b>Contact Information .....</b>	<b>32</b>
Technical Support.....	32
Resolver Inc. ....	32

# SYSTEM REQUIREMENTS Version 5.5

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.5.5, 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
<b>CLIENT MACHINE</b>		
<b>Processor Speed</b>	2 GHz dual-core	2.5 GHz dual-core
<b>Memory</b>	2 GB	4 GB
<b>Operating System</b>	Windows® 7 SP 1, Windows® 8.1, Windows® 10	
<b>.NET Framework</b>	Version 4.7.1	
<b>Web Browser – Launch Perspective</b>	Internet Explorer® 11, Edge	
<b>Web Browser – Web Portal</b>	Internet Explorer® 11, Edge, Google Chrome®, Safari® iOS 9+, Android® Browser 4.2+	
<b>Web Browser – Connect</b>	Google Chrome®	
<b>Third Party Application</b>	Adobe Reader® 9.4.0+, Sun Java® Runtime Environment 7 U71, 8 U25 <sup>1</sup>	
<b>Mobile iOS App</b>	iOS 10, iOS 11	
<b>Officer Mobile</b>	iOS 10 or newer or Android 5.1, Android 6.0 or newer.	
<b>WEB SERVER MACHINE<sup>2</sup> (ON PREMISE ONLY)</b>		
<b>Available Disk Space<sup>3</sup></b>	1 GB	2 GB
<b>Processor Speed</b>	2 GHz dual-core	2.5 GHz quad-core
<b>Memory</b>	8 GB	16 GB
<b>Operating System</b>	Windows Server® 2012, Windows Server® 2012 R2 <sup>4</sup> , Windows Server® 2016, IIS with WebSockets enabled <sup>5</sup> and Secure-Channel configured (HTTPS/SSL)	
<b>.NET Framework</b>	Version 4.7.1 with HTTP and non-HTTP activation, .NET Core 1.0.4 or 1.1.1 (Windows Hosting) <sup>4</sup>	
<b>C++ Runtime Libraries</b>	C++ 2010 SP1 Runtime Libraries (x64) 10.40219	
<b>Message Queue – Connect<sup>4</sup>/Dispatch<sup>5</sup> service clustering</b>	RabbitMQ Server 3.7.7+	
<b>Inbound Ports<sup>6</sup></b>	443	
<b>Outbound Ports<sup>6</sup></b>	443, 2195, 2196, 5223, 5228, 5672	

DATABASE SERVER MACHINE <sup>2</sup> (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 Server <sup>7</sup>	SQL Server® 2012 SP3, SQL Server® 2014 SP2, SQL Server® 2016 SP1	
Reporting Services	SQL Server® 2012 Reporting Services, SQL Server® 2014 Reporting Services, SQL Server® 2016 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](#) section of this guide.
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 IE. 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 Dispatch experience, it's recommended that dispatchers run the application on two monitors with a resolution of 1920x1080.
- Time synchronization is required for Dispatch visual alerts. NTP is strongly recommended for Hosted customers.
- 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 5.5 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

## Important Notes About SQL Server

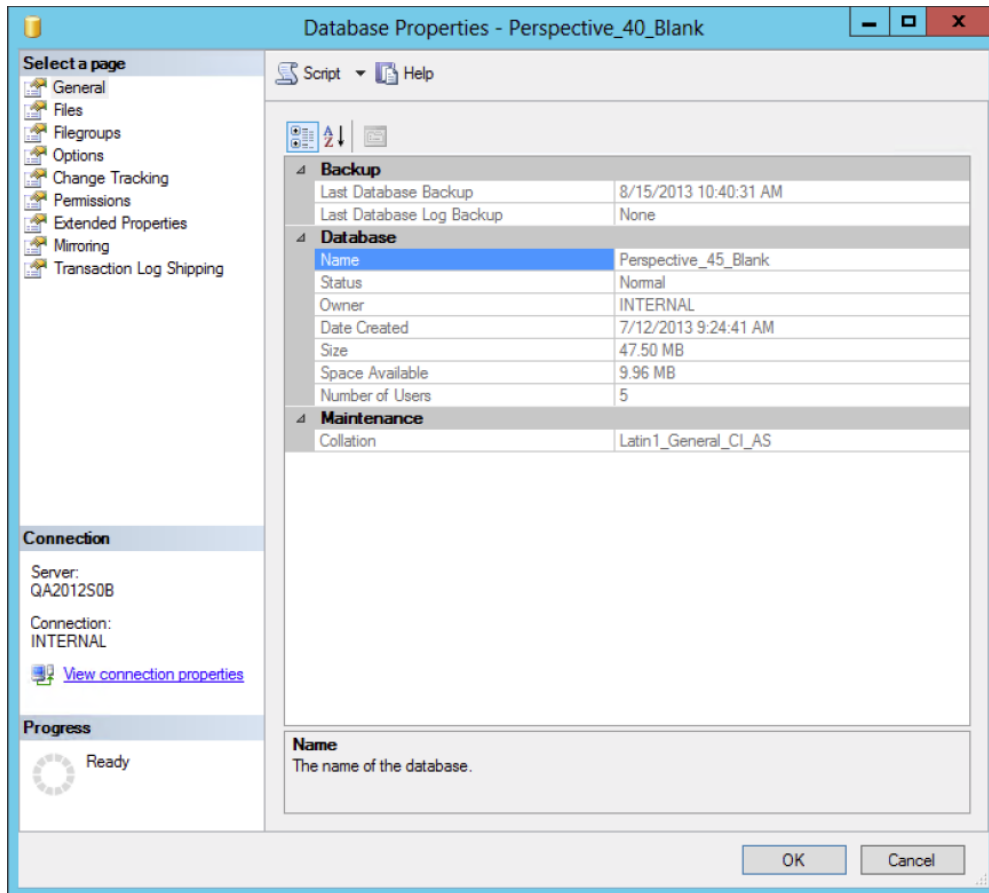
**Only SQL Server Enterprise Edition is supported for indexing on audit tables.** If you're upgrading Perspective using a non-enterprise version of SQL Server, you'll encounter errors related to indexing on audit tables. However, you will still be able to successfully upgrade despite these error messages,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

## Database Upgrade

Note: The following instructions are for updating from 4.5 or later to 5.5. To update from Version 4.0 or earlier, visit the [Resolver Support](#) site and refer to the **Perspective Update Instructions 1.0 to 5.5** document.

1. Back up your Perspective SQL database.
2. Back up the **Perspective\_Default.config** file in the Perspective Services Virtual Directory. This file contains all necessary information on how your system was configured.
3. Ensure that your database is already upgraded to **Perspective v.4.5** (i.e. `SELECT DatabaseVersion_NV FROM tblSystemSettings`).
4. In the **Compatibility Settings** of your SQL database, ensure your database is in compatibility mode for **SQL Server 2012 (110)**.

If it's not, open the **Microsoft SQL Management Studio**, expand **Databases**, right-click your Perspective database and select **Properties**. On the left-hand column, select **Options**. In the **Compatibility level** field, select **SQL Server 2012 (110)**.



5. 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 contact Technical for assistance.
6. 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.
  - 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. **Optional:** The SQL script **BackFill\_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 of 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 Support team at 1-877-776-2995 once you have all of your Site Rollups updated.
  - n. **Optional:** 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.
7. Repeat step 6 for each Perspective database you're running (e.g., test, production, archive).

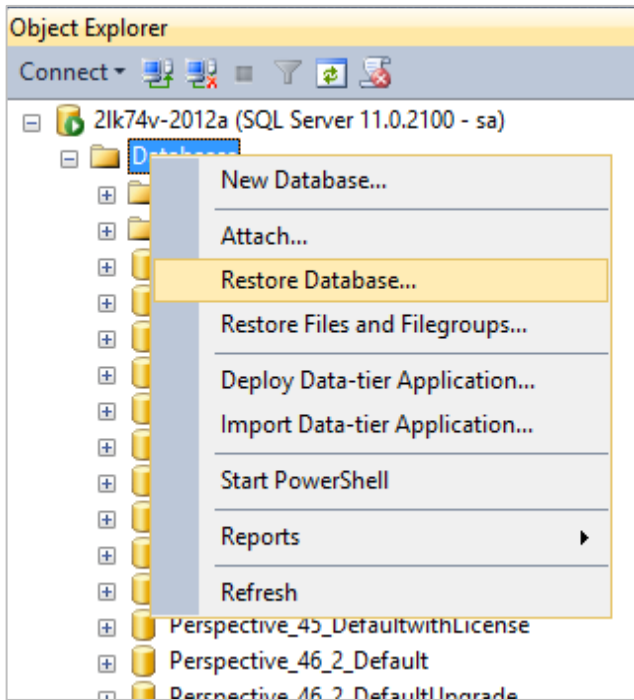
## Set Up Secure Sockets Layer (SSL) on Internet Information Services (IIS)

To set up SSL on IIS, follow the instructions on the [Microsoft IIS](#) website.

## Dispatch Scheduling Services Database Restore

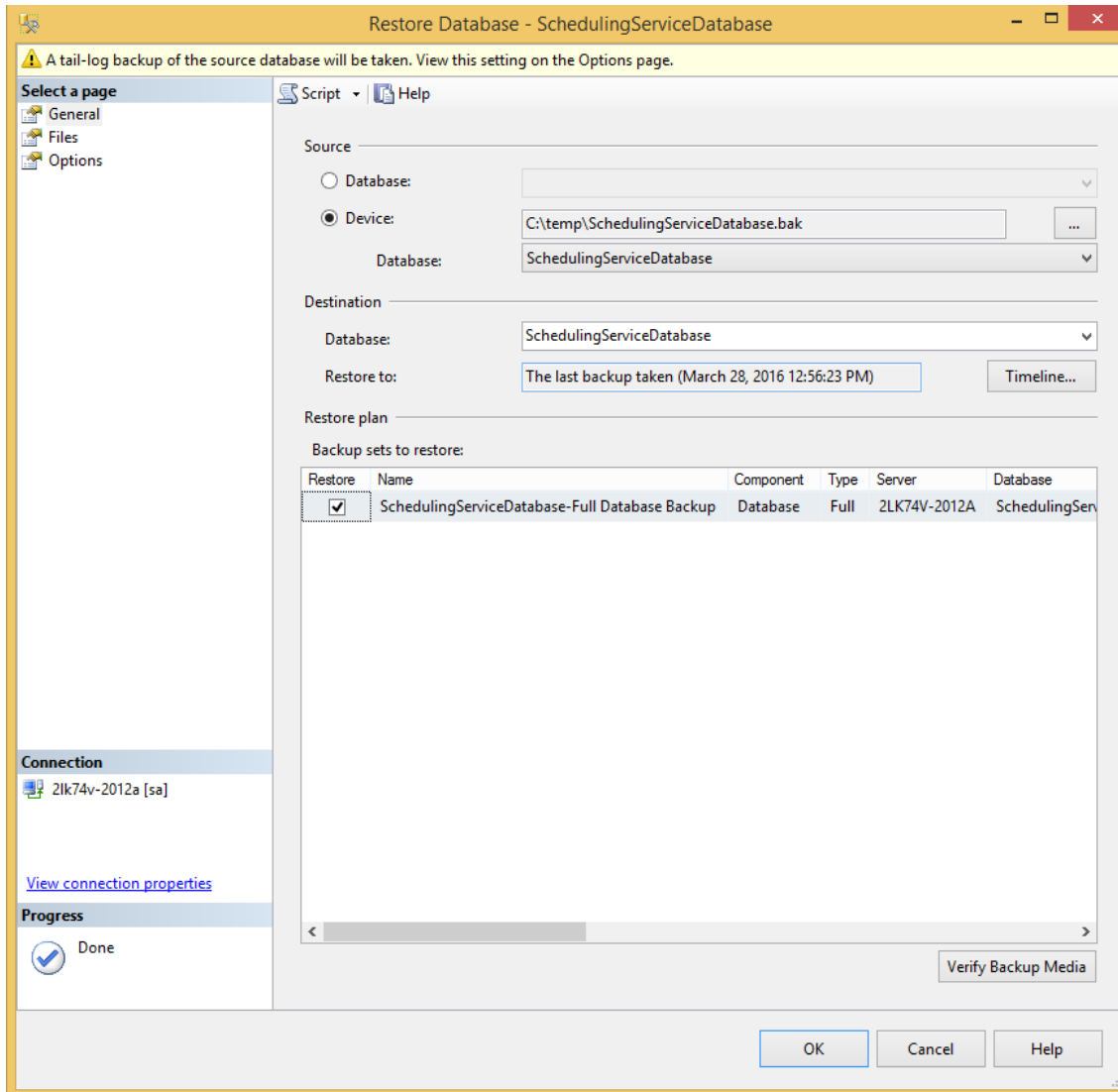
This section applies to users installing an edition of Perspective with Dispatch and those who wish to use the scheduled dispatch feature. If you're not installing Dispatch or you won't be using the scheduled dispatch feature, skip this section.

1. Open **SQL Management Studio**.
2. Right-click **Object Explorer** and click **Restore Database**.

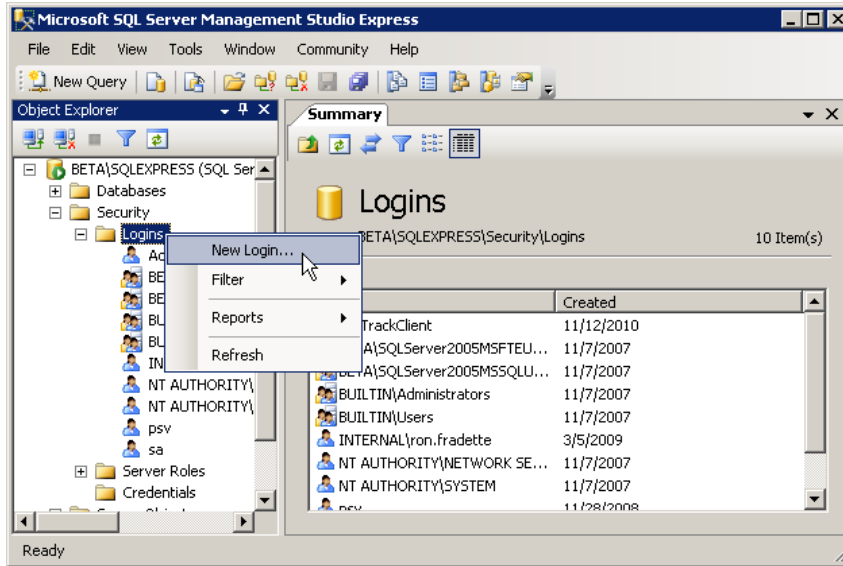


3. Navigate to the location of **Dispatching Schedule Service** database backup file.

Note: Standard backups are found in **Perspective Install > Database Setup > New**. If you're unsure which database to use, contact your Perspective Administrator.

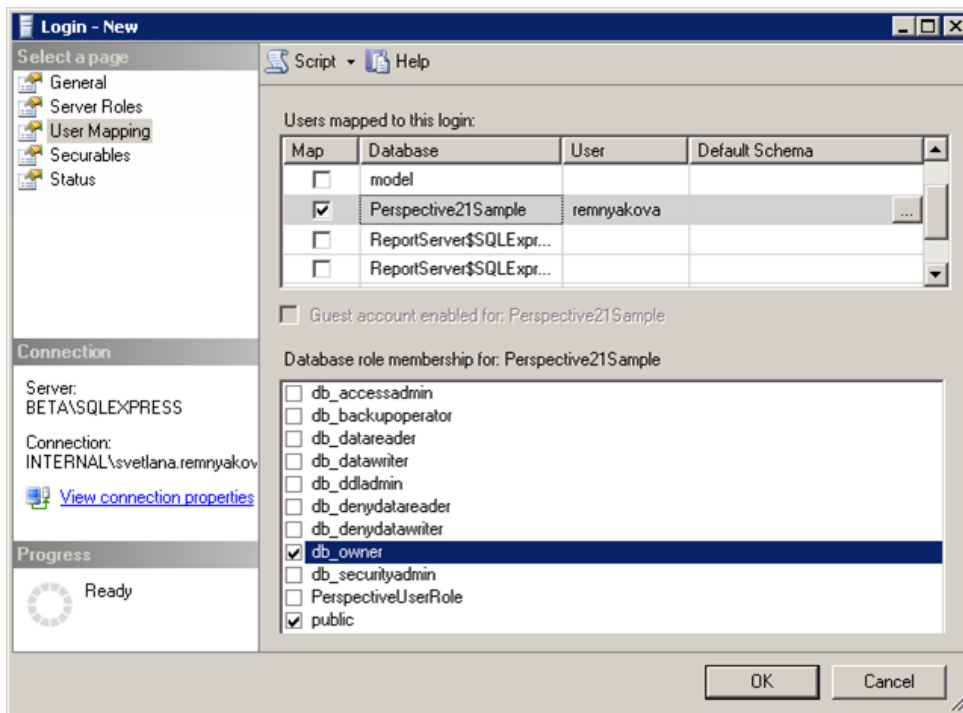


4. Click **OK** to restore.
  
5. Create a new SQL user that will be used by Perspective to connect to the SQL Server:
  - a. Launch Microsoft SQL Server Management Studio. In the menu on your left, expand the **Security** node, right-click **Logins**, and select **New Login**.



- b. In the **Login – New** form, under the **General** page, type in the **Login Name** and modify the rest of the options according to your preference.

Open **User Mapping**. Ensure the account has either **db\_owner** OR **db\_datareader** and **db\_datawriter** role membership rights, then click **OK**.

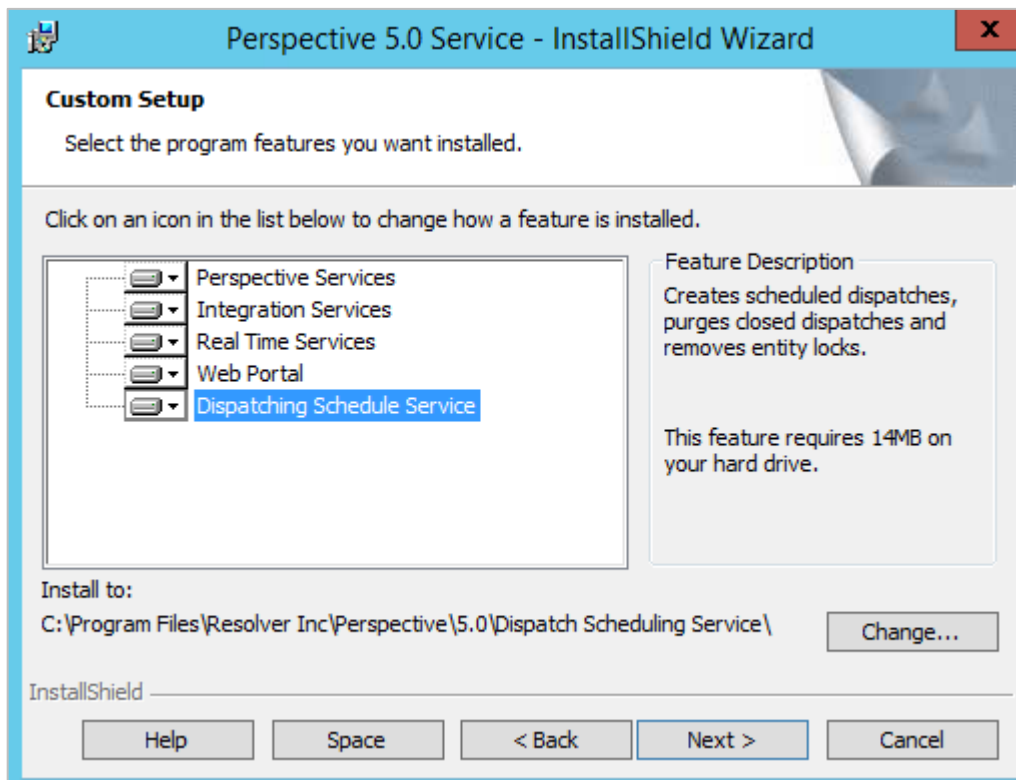


- 6. Complete the steps in the **Dispatch Scheduling Services** section below.

## Dispatch Scheduling Services

This section applies to users installing an edition of Perspective with Dispatch and those who wish to use the scheduled dispatch feature. If you're not installing Dispatch or you won't be using the scheduled dispatch feature, skip this section.

1. Navigate to install location of the scheduling service. If you completed a default installation of Perspective Services, it's located at **C:\Program Files\Resolver Inc\Perspective\5.5\Dispatch Scheduling Service**. If you completed a custom installation, this location is the path that was specified in the InstallShield Wizard.



2. Open the **Connections.xml** file.

```
<?xml version="1.0"?>
<ArrayOfConnectionInfo xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
```

3. Select, copy, then paste the following tags below the `<ArrayOfConnectionInfo>` tag:

```
<ConnectionInfo>
  <ServiceFolder></ServiceFolder>
  <Ssl></Ssl>
  <UserId></UserId>
  <Password></Password>
  <BusinessId></BusinessId>
  <DatabaseId>/DatabaseId>
</ConnectionInfo>
</ArrayOfConnectionInfo>
```

```
<?xml version="1.0"?>
<ArrayOfConnectionInfo xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <ConnectionInfo>
    <ServiceFolder></ServiceFolder>
    <Ssl></Ssl>
    <UserId></UserId>
    <Password></Password>
    <BusinessId></BusinessId>
    <DatabaseId>/DatabaseId>
  </ConnectionInfo>
</ArrayOfConnectionInfo>
|
```

4. Enter the required information in the following tags:

- **ServiceFolder:** Enter the service folder information to show the Integration Services virtual directory (e.g. `<servername>/integrationservices`).

Note: If **Scheduling Services** and **Integration Services** are installed on the same machine, the Service Folder element(s) in the **Connections.xml** file must contain either an IPv4 address or the localhost alias.

- **SSL:** Enter **true** to enable SSL (required).

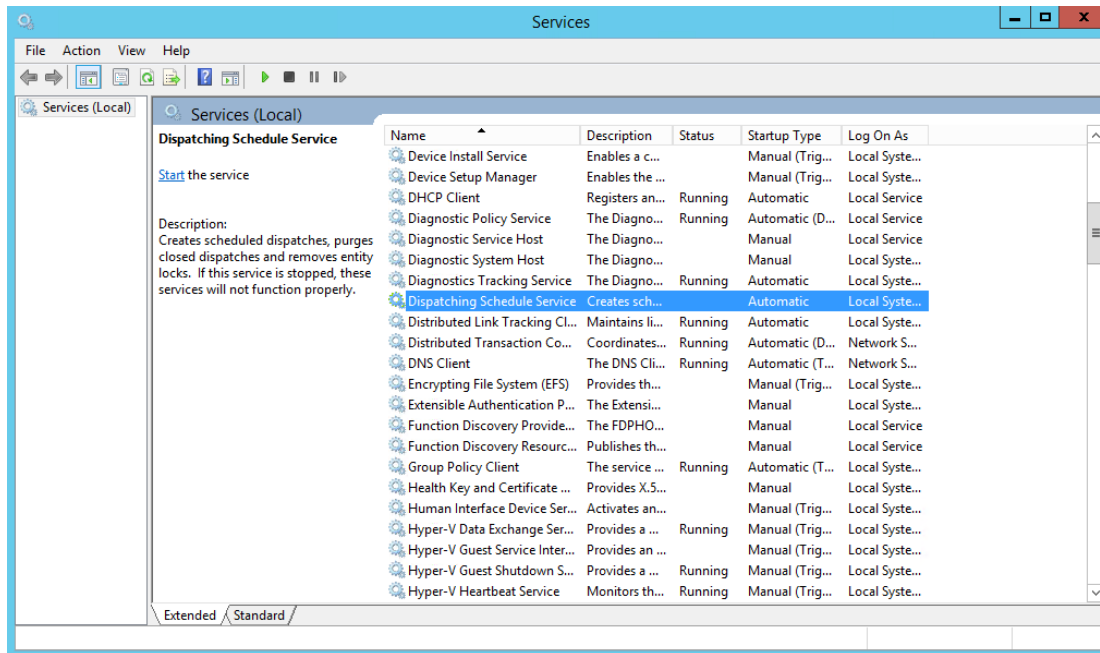
- **UserID:** Enter the username of the ScheduledService Dispatch user who will be triggering the scheduled dispatch.
- **Password:** Enter the service user's password. Once the service begins running, the password will be encrypted and the **<Password>** tags will be converted to **<EncryptedPassword>**.

Note: For security reasons, it's recommended the service user changes their password in Perspective prior to starting the scheduling service. Ensure the password entered in the **<Password>** tags match the Perspective password.

- **BusinessId:** Enter your organization's Perspective business ID.
  - **DatabaseID:** Enter your Perspective database name.
5. Save your changes to the **Connections.xml** file then close.
  6. Open the **SchedulingServices.exe.config** file.
  7. Under **appSettings**, enter the database connection string to point to the Scheduling Service database. For example:

```
<add key="DataBaseConnectionString" value="Data Source==<dbserver\dbname>;Initial Catalog=<dbname>;user id=<user>;password=<password>;Application Name=Integration Services" />
```

8. Save your changes to the **SchedulingServices.exe.config** file then close.
9. Open **Windows Services**.
10. Click on **Dispatching Schedule Service**.



11. Click the  icon or right-click **Dispatching Schedule Service** then click **Start**.

## Dispatch Service Clustering

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

Note that Perspective Services and Integration Services must be deployed on the web servers.

1. Ensure [RabbitMQ 3.7.7](#) or later is installed on the Perspective web server or a separate web server.
2. Navigate to the install directory of **Integration Services**. By default, the directory is located at **C:\inetpub\wwwroot\Perspective5.5\IntegrationServices**.
3. Open the **web.config** file.
4. In the **<appSettings>** tags, make changes as needed to the following settings for the deployed web server:
  - **PerspectiveConfigFilePath**: The physical path where Perspective Services is deployed.
  - **ServiceClusters**: Enter **true** or **false** to enable or disable service clustering for Dispatch.



- **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.

Open the **Perspective\_default.config** file. By default, it can be found at  
C:\inetpub\wwwroot\Perspective5.5\PerspectiveServices.

7. In the **<ClusterQueueConfiguration>** tags, enter the following information:
  - **HostName:** The RabbitMQ hostname.
  - **VirtualHost:** The name of the RabbitMQ virtual host that will be used for clustering.
  - **User:** The username of the RabbitMQ user with CRUD access to the virtual host.
  - **Password:** The RabbitMQ user's password.
  - **NetworkRecoveryIntervallnSeconds:** The number of seconds between each network recovery interval.
  - **RequestHeartbeatIntervallnSeconds:** The number of seconds between each heartbeat interval.
8. Save your changes in the **Perspective\_Default.config** file, then close it.

## Everbridge Mass Notifications (Dispatch)

Perspective allows users to integrate their Everbridge solution into Perspective to send mass notifications about selected activities via Dispatch. If you're not installing an edition of Perspective with Dispatch or you don't use Everbridge, skip this section.

For more details on the information required in step 2 below, see the appropriate Everbridge help documentation.

Open the **Perspective\_default.config** file. By default, it can be found at  
C:\inetpub\wwwroot\Perspective5.5\PerspectiveServices.

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

2. Save the **Perspective\_default.config** file and close.

## Connect Device Manager Configurations

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

To view the Connect devices in Dispatch, the Device Manager URL in the **Perspective\_default.config** file must be edited to show the Connect server. Note that Perspective should only use an instance of

Connect as its Device Manager if the Connect instance is using Perspective's instance of Integration Services for authentication.

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

1. Run **SQLScript\_ConnectDatabaseUpdate**.

Using Notepad, open the **Perspective\_default.config** file. By default, it can be found at `C:\inetpub\wwwroot\Perspective5.5\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 (this information can be obtained from your RabbitMQ administrator):

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

5. Click **File > Save** to save your changes, then close the file.

## Updating SQL Reports

1. Update reports using the **Perspective Install > Reports Setup** folder (please refer to *Perspective Installation Guide* for more detailed outline of SQL reports setup):
  - a. Edit the **PublishServerReports.bat** file to target the SQL Reporting Services server.
  - b. Save and execute the file.

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

# SAML Authentication for SSO

The following 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.

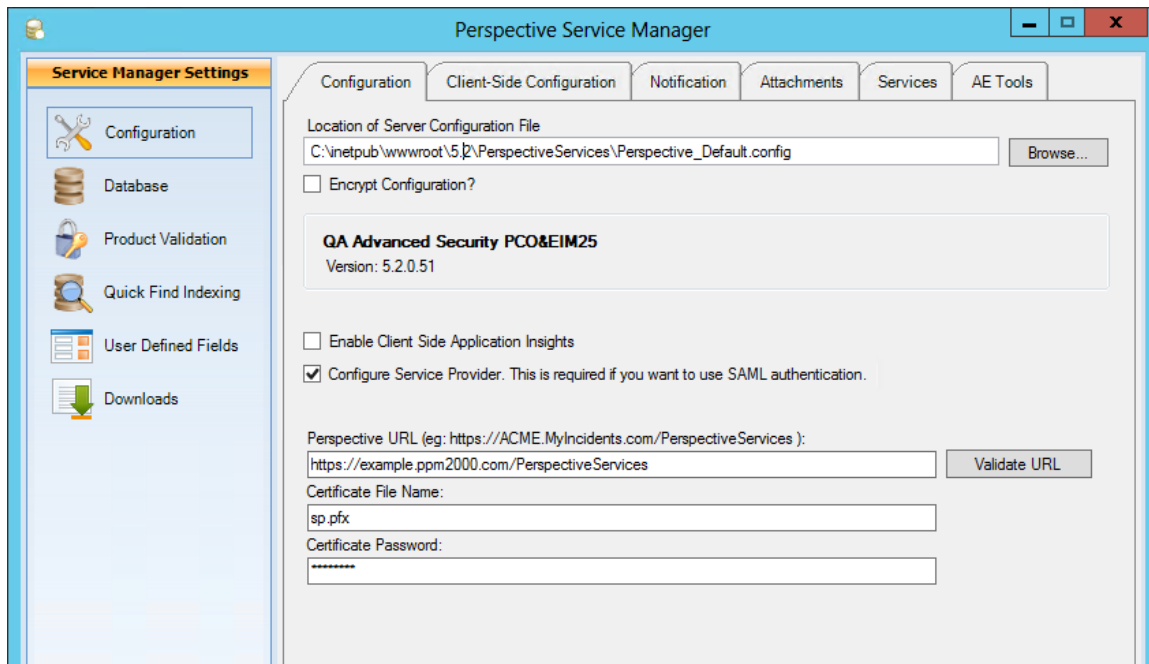
*NOTE: If you're using AD FS to configure SAML, see the [Set Up SSO with AD FS](#) article on the Resolver Support site for instructions after following the steps below.*

1. Open **Service Manager**.
2. Click **Configuration** in the pane to the left if it's not already open.
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. 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.*



After completing the above steps, you'll need to select how you will input the identity provider's details. See the **Identity Provider Configuration** section for information on uploading a metadata file or metadata URL or see **Manual Settings** for instructions on inputting the data manually.

## Identity Provider Configuration

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

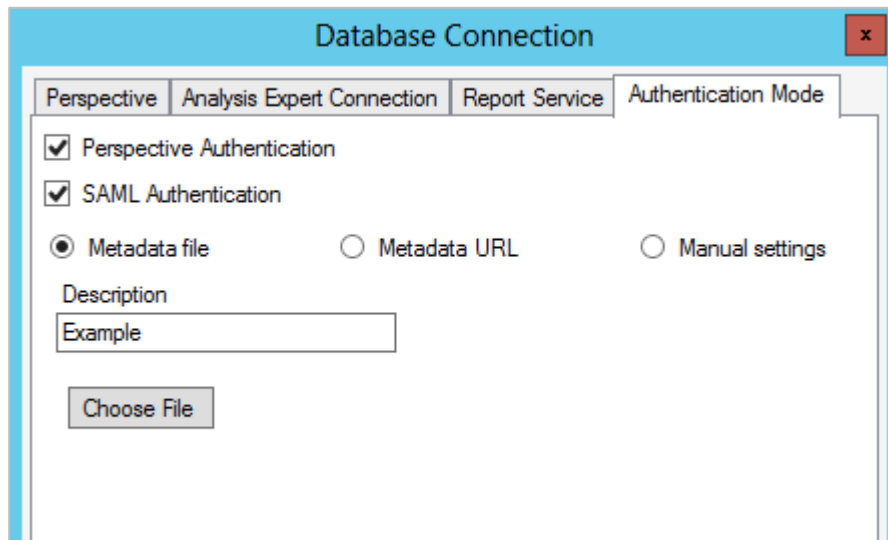
1. In Service Manager, click **Database** in the pane to the left.
2. Double-click a database to edit it.
3. Click the **Authentication Mode** tab.
4. Select the **SAML Authentication** checkbox.

*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:

- Metadata file:** This option will require that you obtain a metadata file from your IdP to import the SSO configurations into 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.

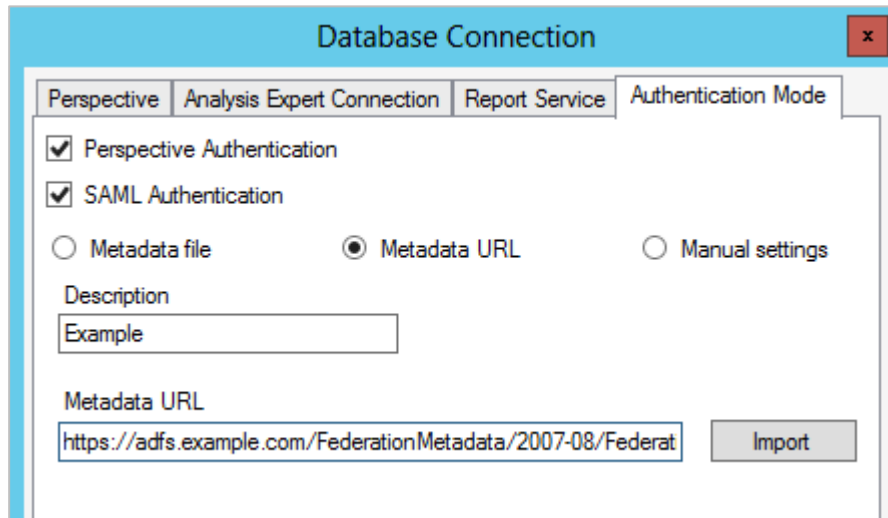
To use this option, after downloading the file, enter the name of your IdP in the **Description** field, which will appear to users with the phrase "Login with [IdP]" on the login screens, then click **Choose File** to upload the metadata file.



- Metadata URL:** This option will require that you obtain a metadata URL that will import the SSO configurations into 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 Service Manager, click **Database** in the pane to the left.
2. Double-click a database to edit it.
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.*

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

Name  
  Sign Authentication Request

PartnerCertificateFile  
  Sign Logout Request

Single Logout Service Url  
  Sign Logout Response

Single Sign On Service Url  
  Sign Assertion

Encrypt Assertion

Name ID Format  
 ▼

Single Sign On Service Binding  
 ▼

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 in order to complete the SSO process. This information can be exported into a file using the **Export Metadata** tool in Service Manager.

1. In Service Manager, click **Database** in the pane to the left.
2. Double-click a database to open it.
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, or an alternate location you may have selected in the previous section.
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 Perspective services 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 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**.

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

If your system was previously configured for Windows authentication, you can use those credentials for SSO, including any values previously saved in the **Corporate ID** field, provided those values match the name ID format selected during setup.

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

## Integration Services

Integration Services should not require any additional configuration as all SAML authentication information should be in the Perspective configuration file.

## Perspective Services Update

For more information on running the installs, refer to the [Perspective Installation Guide](#).

1. If you're installing an edition of Perspective with Dispatch, install the **WebSocket Protocol** on your webserver, if it is not already installed.
2. Uninstall **Perspective Services**. Click **Start** > Launch the **Control Panel** > Navigate to **Programs and Features** > Select **Perspective Services** > **Uninstall** > Follow the prompts displayed onscreen to uninstall **Perspective Services**.
3. If installed, uninstall any earlier versions of **Service Manager**. Check your Perspective directory and IIS for any remnants of your previous Perspective Services installation. Remove any remaining files or folders.
4. Install Perspective Services 5.5 using the **Perspective Install** > **Web Service Setup** > **Perspective Services** folder. Run (as an administrator) **Perspective.Services.exe** to install the updated Perspective Services.

If this is your first time working with Perspective Services, please read through the *Perspective Installation Guide*.

If you're completing a Custom Install and your edition includes the **DispatchLog** component, ensure that Real Time Services is installed. Refer to the Installation Guide for configuration details.

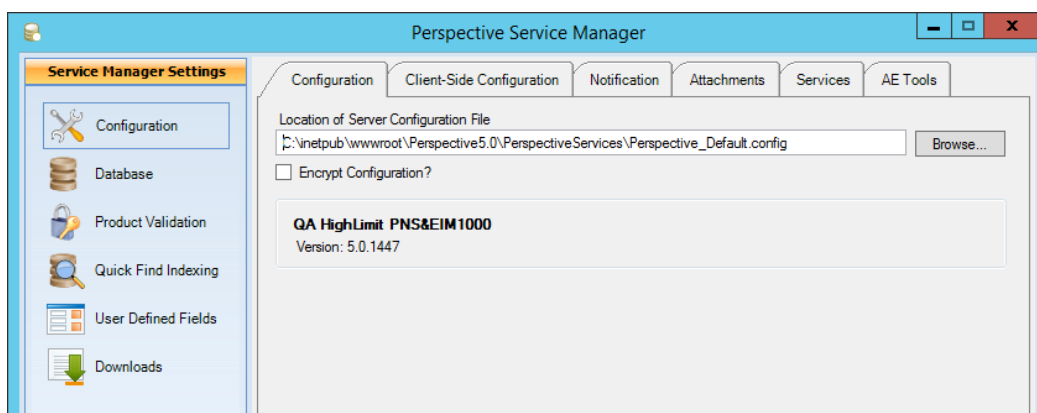
*Note: If Perspective Services prompts you to install C++ runtime libraries, refer to the Standard Install > Perspective Services (Application Web Server) section of the Perspective Installation Guide.*

5. Install Perspective Service Manager (see the *Perspective Installation Guide* for details).

*Note: If you saved a copy of the files from your previous Perspective installation, such as the Perspective\_Default.config file, these files should be used for reference only. **Do not replace the Perspective 5.5 files with files from an older version.***

If you replaced your Perspective 5.5 files and are having trouble logging in, see the [Error: Exception Processing SAML](#) article on the Resolver Support site.

6. Configure connections using Perspective Service Manager:
  - a. To access Perspective Service Manager, open it from your desktop or go to C:\Program Files\Resolver Inc\Perspective\5.5\ServiceManager\Perspective.ServerManager.exe. Launch **Perspective 5.5 Service Manager** as an **administrator**. You will be asked to provide the Database Connection information. Refer to the *Perspective Installation Guide* if needed.
  - b. Under the **Configuration** tab, verify the location specified in the **Location of Server Configuration File** field. The field should be automatically populated with the default location of the **Perspective\_Default.config** file in the **Perspective Services Virtual Directory**. If necessary, use the **Browse** button to point to the correct location.



- c. Under the **Database** tab, enter the primary database information. This information can be copied from within the **Perspective\_Default.config** backup file. Add secondary databases, if required.
- d. Under the **Product Validation** tab, enter your **Company Name** and **Master Key**, and click **Validate**.

*Note: This step requires an Internet connection to download your encrypted license file from the licensing server. If your web server can't access the Internet, contact Technical Support at 1-877-776-2995 to get a license file for validation.*

- e. In the **Client-Side Configuration** sub-tab, enter the **Server URL** for the client folder if the field is empty.
- f. Verify the **Notification** and **Attachments** settings and make any required changes.
- g. Verify the **Quick Find Indexing** and **Services** settings and make any required changes.
- h. Click **Save Changes**, then click **Yes** when prompted for confirmation.
- i. Close Perspective Service Manager and restart IIS.

For detailed instructions on using the Perspective Service Manager, see the [Perspective Installation Guide](#).

7. Launch the Perspective Version 5.5 client from the host Perspective Services default web page (e.g. <https://<servername>/PerspectiveServices>) on each client machine. Your default web page should look like the screenshot below. Refer to the *Perspective Installation Guide* for more information.

*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** (On Premise) to begin the application initialization.*



**IMPORTANT NOTE:** The MSI URL for Version 5.0 and later has changed to `https://<servername>/PerspectiveServices/?opt=0`

If installing clients using the MSI package, ensure that previously installed Perspective applications on client machines have been uninstalled first. To install Perspective on client machines using the MSI package, please refer to the [Perspective Installation Guide](#)

# Windows Authentication

Perspective 5.2 and later continues to support Windows authentication (non-SAML authentication); however, it is available for **Perspective only** and can no longer be enabled through Service Manager.

*Important 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](#).*

Open the **Perspective\_default.config** file. By default, this file is located at  
C:\inetpub\wwwroot\Perspective5.5\PerspectiveServices

Locate the **<WindowsAuthentication>** tag.

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=""
```

Save the file.

Reset IIS to complete the configuration.



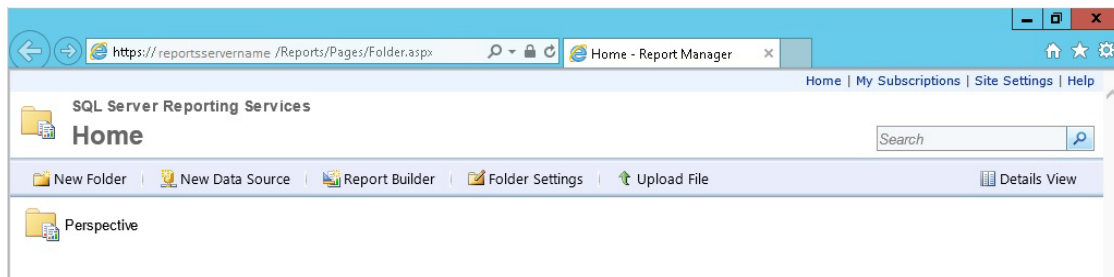
# Testing Perspective Implementation

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 user name and password.

5. Once you have logged on successfully, click on the **Reports** button in the Navigation pane (on the left-hand side of the screen) 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>** node listed. If you receive an error message, see the [Troubleshooting Perspective & SQL Reporting Services](#) on the Resolver Support site for more information.

*Note: Both the Report version and database version should display as 5.5.*

# Contact Information

## Technical Support

**Toll Free:** 1-877-776-2995  
**Phone:** (780) 448-0616  
**Email:** [support@resolver.com](mailto: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](mailto:information@resolver.com)  
**Website:** <http://www.resolver.com>