



Rsam Platform

Installation Guide (Installer Method)

Version: 10.0 | April 2023

© 2023 Relational Security Corporation dba Galvanize. All rights reserved.

www.wegalvanize.com

Contents

Setting up SQL Server Database	3
Pre-Installation Requirements.....	3
Copying Rsam Database Files	3
Creating and Setting up the RSAM_APP Account.....	4
Enabling SQL Authentication	5
Enabling CLR Integration.....	5
Installing and Setting up Rsam Software	6
Pre-Installation Requirements.....	6
Setting up Role Services on Windows 2012/2016/2019/2022 Server	6
Setting up Request Filtering	7
Enabling Microsoft Message Queuing for Syslog	8
Enabling Message Queuing on Windows Server	8
Enabling Message Queuing for Windows 7.....	9
Running the Rsam Installer.....	10
Verifying the Installation	15
Trusted Connection Configuration	15
Reports	18
Install Crystal Reports 2013	18
Enabling Rapid Reports.....	19
Configurations in Rsam	20
Rsam Option for Data Import	20
Setting up Rsam Web URLs	20
Configuring LDAP settings.....	21
Enabling Web Server-based Email Notification.....	24
Enabling Single Sign-on	26
Configuration for Tivoli Access Manager (TAM)	26
Configuring Email Listener.....	27
Creating Email Connection file on Web Server	28
Enabling Assessment Questionnaire Interface	29
Importing Migration File	29
Running Store Procedure and Script files.....	30

Setting up SQL Server Database

Rsam Web Services require access to a live Rsam database. The Rsam database resides on a SQL Server. Configuring a SQL server to use the Rsam database should take 20-30 minutes when using the following simple steps.

This section explains the following topics:

- [Pre-Installation Requirements](#)
- [Copying Rsam Database Files](#)
- [Creating and Setting up the RSAM APP Account](#)
- [Enabling SQL Authentication](#)
- [Enabling CLR Integration](#)

Pre-Installation Requirements

Before attaching / restoring the Rsam database files on the database server, make sure the server meets Rsam's minimum requirements.

- An instance of SQL Server 2014, 2016, or 2019 has been installed.
- Collation has been set to **SQL_Latin1_General_CP1_CI_AS**.
- The latest SQL Service packs have been applied.
- SQL Authentication (mixed mode) has been enabled. For step-by-step instructions on how to enable SQL Authentication, please refer to the Enabling SQL Authentication section.
- Enable CLR Integration. For more information, see [Enabling CLR Integration](#).

Copying Rsam Database Files

To copy the Rsam database files, perform the following steps:

1. Create a custom directory for the Rsam database to reside in, or use SQL default data directory: `|Program Files|Microsoft SQL Server|MSSQL.3|MSSQL|Data|`.
2. Copy the **RSAM.mdf** and **RSAM.ldf** files into the directory.
3. Create a sub-directory for Rsam data backups as **\backups**.
4. Attach Rsam Database to the SQL Service.
5. Launch **SQL Server Management Studio**.
6. Expand the navigation tree to locate your Rsam server instance.
7. Expand your server instance.
8. Right-click **Databases** and select **Attach**.

9. In the **Attach Databases** window, click **Add...** and browse for the **RSAM.mdf** file.
10. Ensure that the following entries are correct:
 - Original File Names: **RSAM.mdf** and **RSAM.Idf**
 - **Attach as RSAM**
 - Owner: Username of the database owner account (or sa)
11. Click **OK**.

Creating and Setting up the RSAM_APP Account

To create and set up the RSAM_APP account, perform the following steps:

1. In the navigation tree, navigate to **Security > Logins**.
2. Right-click **Logins** and select **New Login...**
3. In the **Login - New** dialog box, complete the following information in the **General** tab:
 - a. Provide the **Login name** as **RSAM_APP**.
 - b. Select **SQL Server authentication**.
 - c. Provide a strong **Password**.
 - d. Select the **RSAM** database.
4. Click **User Mapping** tab on the left panel.
 - a. Select the check box corresponding to the RSAM database in the **Users mapped to this login** section.
 - b. In the **Database role membership for** section, select the following check boxes:
 - **public**
 - **db_datareader**
 - **db_datawriter**
 - **rsam_client**
5. Click **OK**.
6. Add the view and alter schema permissions for the RSAM Database by performing the following steps:
 - a. Right-click the RSAM database and select **Properties**. The **Database Properties** dialog box opens.
 - b. Click the **Permissions** tab.
 - c. Select the **RSAM_APP** user and select the check boxes corresponding to **Alter any schema** and **Create View** in the **Permissions for RSAM_APP** section.
 - d. Click **OK**.

Enabling SQL Authentication

To enable SQL Authentication through the SQL Management Studio, perform the following steps:

1. In the **SQL Server Management Studio**, expand the **Object Explorer** panel.
2. Right-click the Rsam server instance and select **Properties**. The **Server Properties** dialog box opens.
3. Click the **Security** page from the left panel.
4. Select **SQL Server and Windows Authentication mode** in the **Server authentication** section.
5. Click **OK**.

Enabling CLR Integration

Some features in Rsam such as Redlining uses CLR integration for exporting redlined values to PDF. To use all capabilities of the Redlining feature successfully, you must enable CLR integration using the `clr enabled` option of the `sp_configure` stored procedure in SQL Server Management Studio.

```
sp_configure 'show advanced options', 1;
```

```
GO
```

```
RECONFIGURE;
```

```
GO
```

```
sp_configure 'clr enabled', 1;
```

```
GO
```

```
RECONFIGURE;
```

```
GO
```

For more information, visit the following URL:

<https://msdn.microsoft.com/en-us/library/ms131048.aspx>

Installing and Setting up Rsam Software

You can use the Rsam installer to install the software. If you cannot use the automated installer (preferred method), refer the *Rsam Installation Guide (Manual Method)*.

This section explains the following topics:

- [Pre-Installation Requirements](#)
- [Setting up Role Services on Windows Server](#)
- [Setting up Request Filtering](#)
- [Enabling Microsoft Message Queuing for Syslog](#)
- [Running the Rsam Installer](#)
- [Verifying the Installation](#)

Pre-Installation Requirements

Before installing the RSAM Web Interface on a server, make sure that the server meets the minimum requirements for Rsam, and that the following tasks have been completed:

- IIS v7.0 or higher has been installed on Windows Server 2012/R2, Windows Server 2016/2019/2022, or Windows 7.
- Microsoft .NET 4.7.2 Framework is installed.
- Crystal Reports 2013 Runtime Files have been installed for Web Reporting. A license key is not needed. Click **Next** button through the pages to finish.
- Latest Windows and IIS Security patches / updates are installed.
- A SQL server hosting the Rsam database is installed and configured.
- Microsoft Access Database engine 2010 or higher is installed.

Note: It is recommended to use HTTPS protocol for Rsam installation for security purposes.

Setting up Role Services on Windows 2012/2016/2019/2022 Server

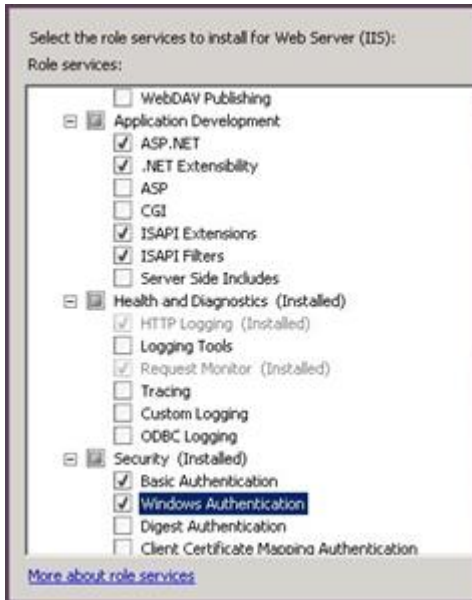
To set up role services on Windows 2012/2016/2019/2022 Server, perform the following steps:

1. Install the required roles by using the **Server Manager** tool.
2. In the navigation pane, expand **Roles**, right-click **Web Server (IIS)** and select **Add Role Services**.
3. Scroll to **Security** section and select the check boxes corresponding to **Basic Authentication** and **Windows Authentication**.

Note: Do NOT clear any already existing selections.

4. Scroll to **Application Development** section and make sure that the check boxes corresponding to **ASP.NET**, **.NET Extensibility**, **ISAPI Extensions**, and **ISAPI Filters** are selected.

Note: Do NOT clear any already existing selections.

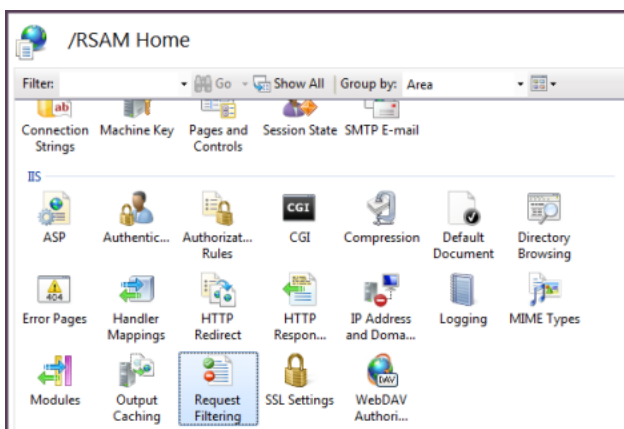


5. In the **Select Role/Services** panel, click **Next**, and then click **Install** on the **Confirm Installations Selections** panel.
6. Click **Close** to exit the Add Role Services wizard.

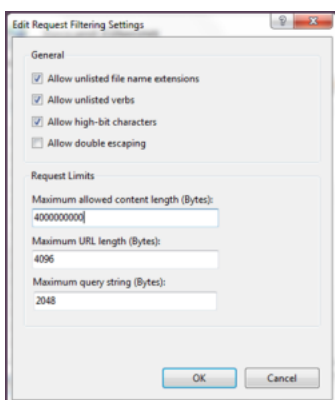
Setting up Request Filtering

If you plan to import large files on a Windows 2012/2016/2019/2022 or IIS7 server, it will require adjusting the **Request Filtering** property of IIS to allow larger files. In some cases, this option may not be available. You can install the package available at <http://www.iis.net/download/AdministrationPack>.

1. In IIS Manager, select the Rsam server.
2. Double-click **Request Filtering**.



3. Click **Edit Feature Settings** on the right panel. The **Edit Request Filtering Settings** dialog box opens.
4. Set the value in **Maximum allowed content length (Bytes)** field to **400000000** and click **OK**.



5. On the system, navigate to **C:|inetpub|wwwroot|RSAM_FINDINGS**.
6. Open the **web.config** file using a text editor.
7. Update the value for **requestLengthDiskThreshold** to **1000000** and save the file.

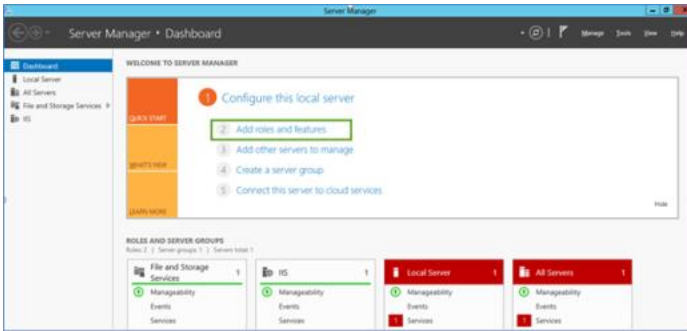
Enabling Microsoft Message Queuing for Syslog

To enable message queuing, perform one of the following:

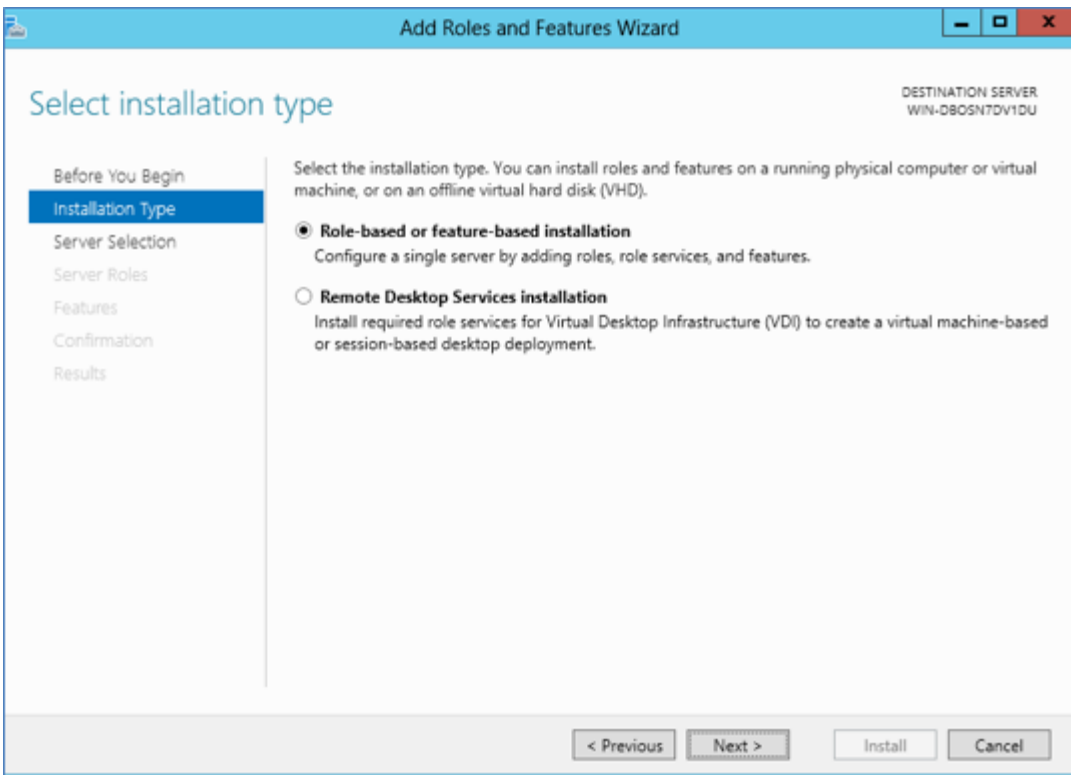
- [Enabling Message Queuing for Windows Server](#)
- [Enabling Message Queuing for Windows 7](#)

Enabling Message Queuing on Windows Server

1. Navigate to **Start > Control Panel > Programs > Turn Windows feature on or off**.
2. In the **Server Manager** Dashboard, click **Add roles and features**.



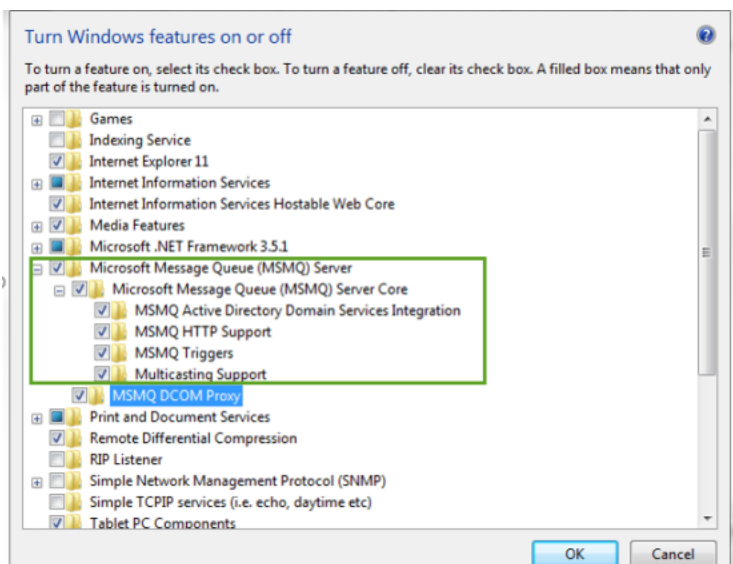
3. In the **Add Roles and Features Wizard**, select the **Installation Type** tab, and select **Role-based or feature-based installation**.



4. Click **Next**.
5. Click **Server Selection** tab and select a server from the **Server Pool** section and click **Next**.
6. Click **Features** tab and in the **Features** section, select the check box corresponding **Message Queuing**. Ensure all the options under **Message Queuing** are enabled.
7. Click **Next**.

Enabling Message Queuing for Windows 7

1. Navigate to **Start > Control Panel > Programs > Turn Windows feature on or off**.
2. Select the check box corresponding to **Microsoft Message Queue (MSMQ) Server**.



3. Click **OK**.

Running the Rsam Installer

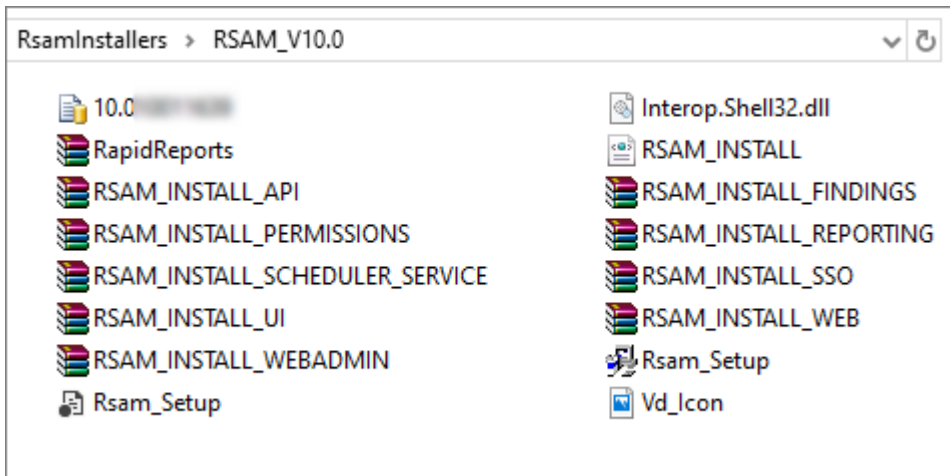
The Rsam Web application includes an automated installer. The goals of this installer are the following:

- Check to ensure the system meets the minimum system requirements.
- Create the required physical directories, and transfer the proper files.
- Create and configure the required IIS virtual directories.
- Set the necessary database and LDAP connection settings.
- Simplify the application of future updates.

Note: It is recommended that customers leverage this installer for rapid deployment of Rsam. Customers may also opt to perform a manual installation as described in the *Rsam Installation Guide (Manual Method)*.

To run the Rsam installer, perform the following steps:

1. Create a temporary folder to hold the Rsam installer files. Extract the Rsam module files (.zip) and the Rsam_Setup (.exe) file into this directory.

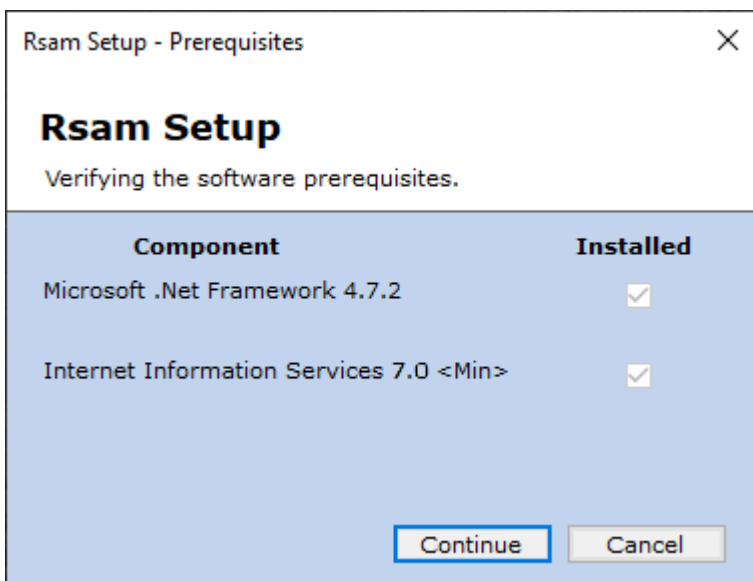


2. Double-click **Rsam_Setup.exe** to launch the Rsam installer.

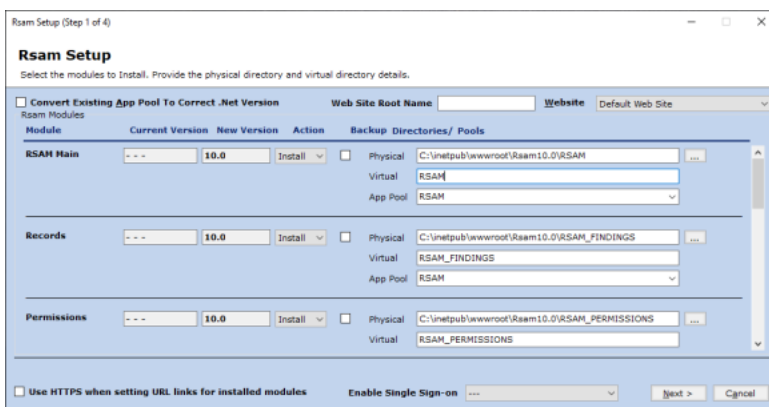
Note: On Windows Server 2012/2016/2019/2022 and Windows 7, right-click **Rsam_Setup.exe** and select **Run as Administrator**.



3. Click **Next**. The License Agreement page appears.
4. Read the **License Agreement** and click **Accept**. The **Rsam Setup** page appears listing the prerequisite verification.



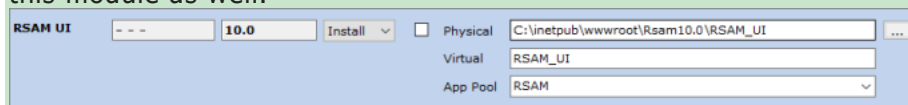
5. Click **Continue**. The page to set the installation details appear.



6. Set the Installation destination and details:

- a. Select the **Physical** and **Virtual** directories and **Application Pool** to use.

Note: Rsam version 10.0 onwards includes the **RSAM UI** module, which is required for the Home Page and Scheduler elements. Provide the physical and virtual directories for this module as well.



When selecting App Pool, select the app pool that has the **Managed Pipeline Mode** set to **Integrated**.

For the easiest install experience, it is recommended that you keep the defaults for Physical, Virtual, and App Pool fields.

Note: Rsam will auto-create any physical directory, virtual directory, and application pool that does not exist.

- b. For each module you wish to install, select **Install** from the drop-down-list in the **Action** column.
- c. If you opt to install the Single Sign-on module, you will be asked to select the type of Single Sign-on in the **Enable Single Sign-on** drop-down field.
- d. Click **Next** to continue.

The page to set the database connection properties appear.

7. Select the Database Connection Settings:

For SQL authentication:

- a. **Database Connection Settings**

- **Database Sever Name** - Enter the fully qualified name of the Rsam database server. Include the *\instance name*, if this is a named instance.
- **Database Name** - Enter the name of the SQL database to use (default = RSAM).
- **Connection File** - Specify the name of the file to store the connection information.

- b. **Database Authentication Settings**

- **Database User ID** - Enter the Database User ID (default = RSAM_APP).
- **Database Password** - Enter and **Confirm** the password used during the Database User account setup.

- c. **LDAP Authentication Settings** (*OPTIONAL*)

- **LDAP User ID** - Enter the LDAP User ID used during LDAP setup.
- **LDAP Password** - Enter and **Confirm** the LDAP password used during the LDAP setup.
- **Connection File** - Specify the name of the file to store the connection information.

- d. Click **Test Connection** to verify whether the connection details are correct and installer is able to establish a connection with the database. If the connection is successful, a **Test Connection Succeeded** message appears. Click **OK**.

- e. Click **Next** to continue.

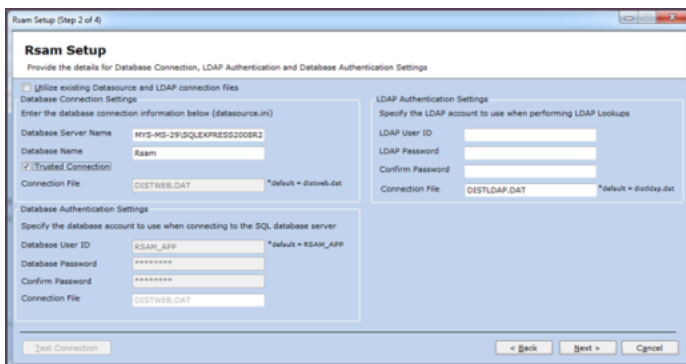
For Trusted connection – This is the recommended method to have the Web Server authenticate to the Database Server.

- a. **Database Connection Settings**

- **Database Sever Name** - Enter the fully qualified name of the Rsam database server. Include the *\instance name*, if this is a named instance.
- **Database Name** - Enter the name of the SQL database to use (default = RSAM).

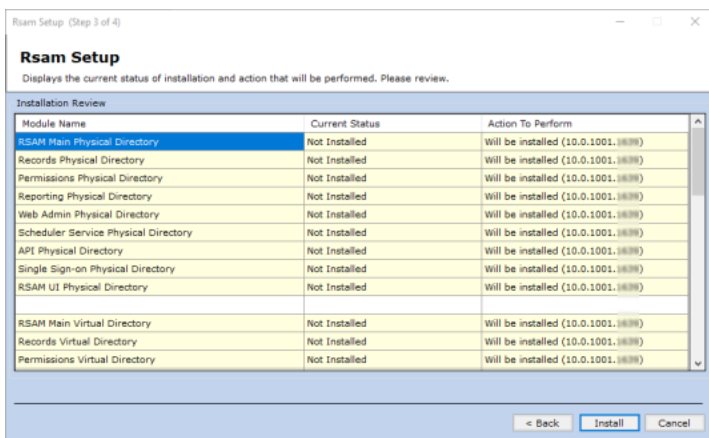
- b. Select the **Trusted Connection** check box. For more information on Trusted Connection, see [Trusted Connection Configuration](#).

- c. Click **Next** to continue.



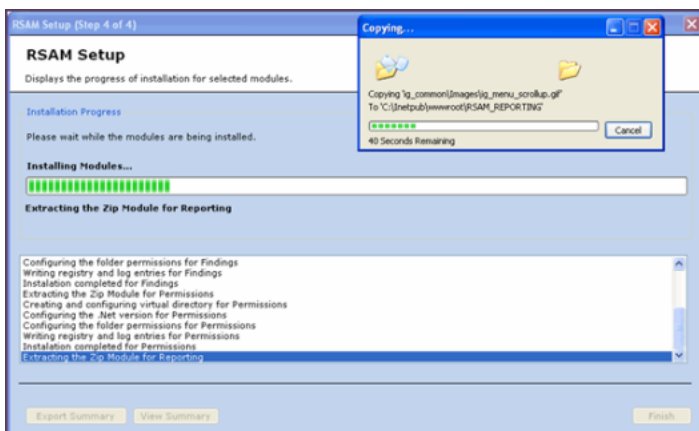
The **Installation Review** section appears.

8. Review the installation selections in the **Current Status** and **Action to Perform** columns for each module.



9. Click **Install** to continue. The installation begins and the status is displayed.

Note: Backup check box in Rsam Setup Step 1 will create a backup of your current virtual directory and store it in a .zip file. When selecting this option, it will increase the time to perform the installation.



Note: If you receive a message prompt to trust the *InstallUtil.exe*, click **Trust** to continue the installation.

The **Installation completed** message appears when the installation is successfully completed.

10. Click **OK**.
11. You can **View** or **Export Summary** of the installation activities after the installation is successful.
12. Click **Finish** and the installation wizard closes.

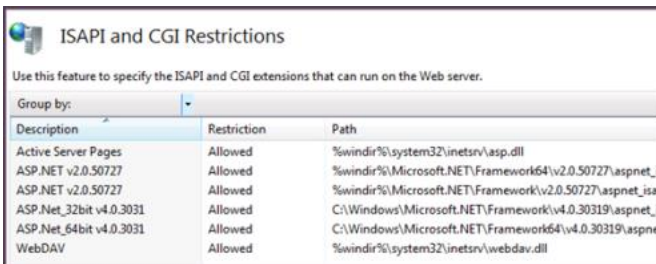
Verifying the Installation

After the Rsam installation is successfully completed, you must verify the **ISAPI and CGI Restrictions** on the web server.

1. In the IIS Manager, double-click **ISAPI and CGI Restrictions**.



2. Verify that the **Restriction** for all ASP.net v4.0.x is set to **Allowed**.



Description	Restriction	Path
Active Server Pages	Allowed	%windir%\system32\inetrv\asp.dll
ASP.NET v2.0.50727	Allowed	%windir%\Microsoft.NET\Framework64\v2.0.50727\aspnet_j
ASP.NET v2.0.50727	Allowed	%windir%\Microsoft.NET\Framework\v2.0.50727\aspnet_isa
ASP.Net_32bit v4.0.3031	Allowed	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_j
ASP.Net_64bit v4.0.3031	Allowed	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspne
WebDAV	Allowed	%windir%\system32\inetrv\webdav.dll

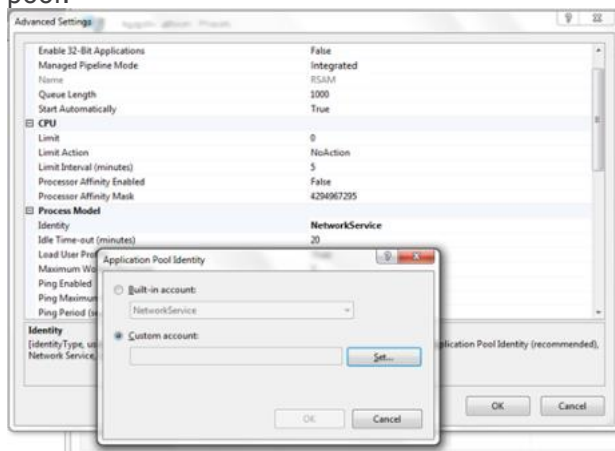
Trusted Connection Configuration

Rsam supports the ability to use a Domain account for the Rsam application to authenticate to the SQL server. This method is more secure and therefore Rsam recommends this method over creating a local authentication.

Perform the following steps to allow Rsam to use the trusted connection configuration:

1. On the web server, navigate to the RSAM main folder (*C:\inetpub\wwwroot\RSAM*).
 - a. Right-click the **datasouce.ini** file and select **Edit**.
 - b. Update the file to contain only the following line:
CONNECTION_STRING_01:
Server=localhost;Database=rsam;Trusted_Connection=True;
 - c. Copy the updated datasouce.ini file into all Rsam folders under **wwwroot**.

2. Use a domain account on your SQL Server and Application pool and perform the following:
 - a. Set your domain account to have the following database role membership on your Rsam database:
 - db_datareader
 - db_datawriter
 - public
 - rsam_client
 - b. On IIS Manager, set the same domain account to be the identity for the Rsam application pool.



3. Navigate to the Rsam Scheduler folder (*C:\inetpub\wwwroot\RSAM_SCHEDULER*):
 - a. Right-click **MAKE_DISTWEB_LDAP.exe** and select **Run as Administrator**.
The Connection file name should be **Trusted.dat**.
 - b. Enter the same credentials for trusted connection and click **Create Connection**.



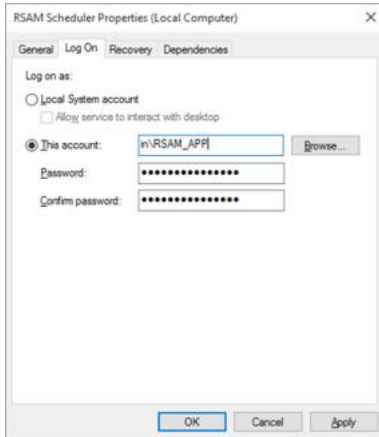
4. Log in to Rsam and navigate to **Manage > Administration > Options > Rsam Options**. Select **Scheduler** in the **Option Categories** drop-down and specify the file name (**Trusted.dat**) for the **Trusted connection file name** option.



The RSAM Options dialog box shows configuration for the Scheduler service. The 'Option Categories' dropdown is set to 'Scheduler'. The 'Timer Interval' is 20. The 'User ID for scheduled task' is empty. The 'Enable Scheduler' checkbox is checked. The 'Scheduler Connection File' is empty. The 'Scheduled Import Timeout (hours)' is 24. The 'Trusted connection file name' is 'Trusted.dat'.

Option	Value
Option Categories	Scheduler
Timer Interval	20
User ID for scheduled task	
Enable Scheduler	<input checked="" type="checkbox"/>
Scheduler Connection File	
Scheduled Import Timeout (hours)	24
Trusted connection file name	Trusted.dat

5. Specify the Scheduler service to run using the same trusted credentials.



The RSAM Scheduler Properties dialog box is shown in the 'Log On' tab. The 'Log on as:' section has 'Local System account' unselected and 'This account:' selected. The 'This account:' field contains 'rsam\RSAM_APP' and has a 'Browse...' button next to it. The 'Password:' and 'Confirm password:' fields are filled with masked characters (dots).

Log on as:

Local System account
 Allow service to interact with desktop

This account: rsam\RSAM_APP [Browse...]

Password: [Masked]

Confirm password: [Masked]

Buttons: OK, Cancel, Apply

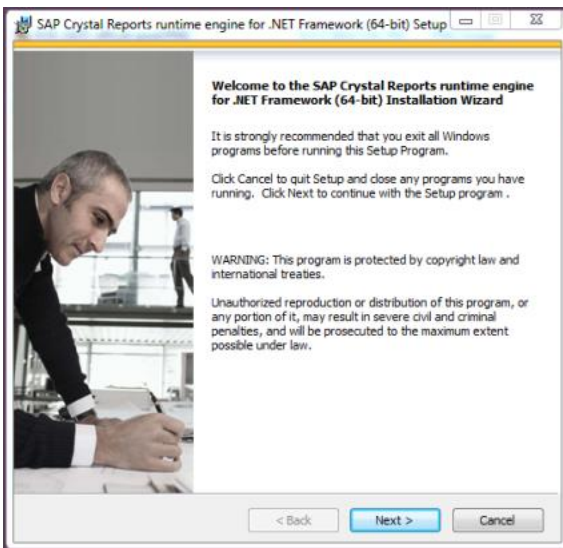
Reports

The following section explains the steps to configure the Reports module in Rsam.

Install Crystal Reports 2013

To install Crystal Reports 2013, perform the following steps:

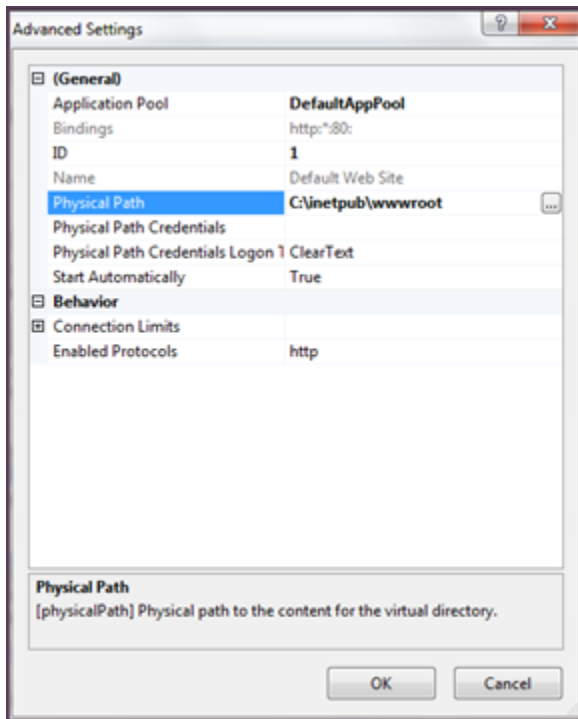
1. Run the Crystal Reports MSI Package (CRRuntime_64bit_13_0_20.msi and later versions) on the FTP link.



2. Copy the sub folder **crystalreportviewers13** to root of WebSite that Rsam is installed, if not available by default.

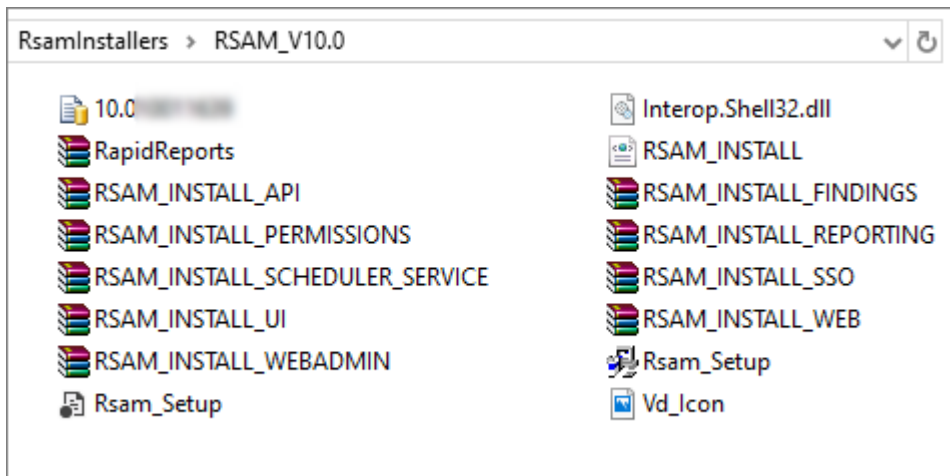
By default, the Crystal MSI package installs the **aspnet_client** folder in the root location of the WebSite that hosts Rsam (*C:\inetpub\wwwroot*). If the root location of the WebSite that hosts Rsam is not *C:\inetpub\wwwroot*, then you must copy the **aspnet_client** folder to the corresponding location.

To determine the root of the WebSite where *RSAM_REPORTING* virtual directory is, right-click **Default Web Site** and select **Manage Web Site > Advanced Settings**. Note the value set for **Physical Path**.



Enabling Rapid Reports

To enable Rapid Reports in your Rsam instance, use the RDL files available in the **RapidReports.zip**.



Configurations in Rsam

This section explains the following topics:

- [Rsam Option for Data Import](#)
- [Setting up Rsam Web URLs](#)
- [Configuring LDAP settings](#)
- [Enabling Web Server-based Email Notification](#)
- [Enabling Single Sign-on](#)
- [Configuring Email Listener](#)
- [Enabling Assessment Questionnaire Interface](#)

Rsam Option for Data Import

If the Scheduler service is installed on a system other than the Web Server, log in to Rsam and navigate to **Manage > Administration > Options > RSAM Options** and select **Data Import Options** in the **Option Categories** drop down list and specify the path in the **Path to temporary store uploaded files during import** field.

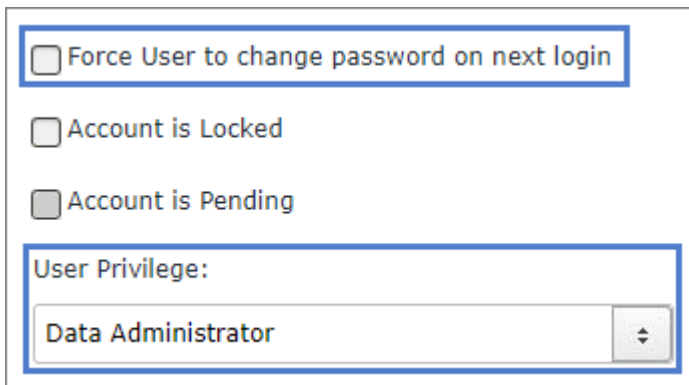
Setting up Rsam Web URLs

After installing Rsam successfully, an Administrator must set up the Web URLs in Rsam. To set up the Web URLs, perform the following steps:

1. Log in to Rsam as an **Administrator**.
2. Navigate to **Manage > Administration > Options > RSAM Options**. Select **URL Links** in the **Option Categories** drop-down list.

RSAM Options	
Option Categories	
URL Links	
RSAM Web Server URL	<input type="text"/>
RSAM Reporting Server URL	<input type="text"/>
RSAM Record Server URL	<input type="text"/>
RSAM SSO Server URL	<input type="text"/>
RSAM Scheduler Administration Server URL	<input type="text"/>
RSAM Permissions Server URL	<input type="text"/>
RSAM Web Administration Server URL	<input type="text"/>
Logout / Session Timeout Redirect URL	<input type="text"/>
RSAM UI Server URL	<input type="text"/>
RSAM Web Server URL use in email notifications for Non-LDAP users (leave blank for default)	<input type="text"/>
<input type="button" value="Save Options"/> <input type="button" value="Cancel"/>	

3. Provide the correct URL links for the specific Rsam Web components configured in your environment on the web server.
4. Click **Save Options** to save the configuration.
5. Log in to the Rsam as an **Account Administrator** (or higher) account.
6. Navigate to **Manage > Users/Groups**.
The list of users appears.
7. Verify if there is an account named **Scheduler**. If it does not exist, **Add** a user with following properties:
 - a. Set **User Privilege** to **Data Administrator**.
 - b. Clear the check box **Force User to change password on next login**.



The screenshot shows a user configuration form with the following elements:

- A checkbox labeled "Force User to change password on next login" which is unchecked.
- A checkbox labeled "Account is Locked" which is unchecked.
- A checkbox labeled "Account is Pending" which is unchecked.
- A section titled "User Privilege:" containing a dropdown menu with "Data Administrator" selected.

- c. **Save** the user details.
8. Navigate to **Manage > Administration > Options > RSAM Options** and select **Scheduler** from the **Option Categories** drop-down list.
 - a. Enter a value for the **Timer Interval** in seconds (default value is 20).
 - b. Type the account (Rsam user ID) to be used to schedule tasks in the **User ID for scheduled task** field. By default, the account name may be set to **Scheduler**.
 - c. Select the check the box corresponding to **Enable Scheduler**.
9. Click **Save Options** to save the configuration.

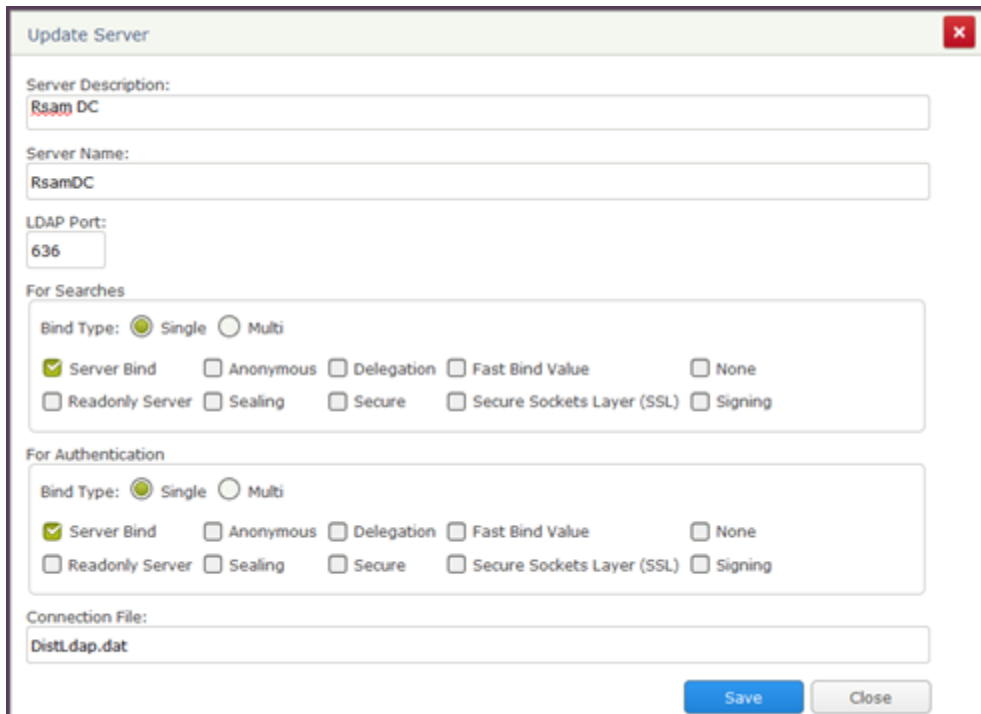
Configuring LDAP settings

The LDAP User ID should be a service account created by the *LDAP Administrator*. If you have multiple LDAP Domains specified in the Rsam Web Admin 'LDAP Admin - Domain' option, additional DISTLDAP files must be created matching the name defined in the 'LDAP Domain - Server' configuration.

To access the configuration pages, log in to Rsam as an *Administrator* and navigate to **Manage > Administration > Options**. **LDAP Admin - Server** and **LDAP Admin - Domain** options are available.

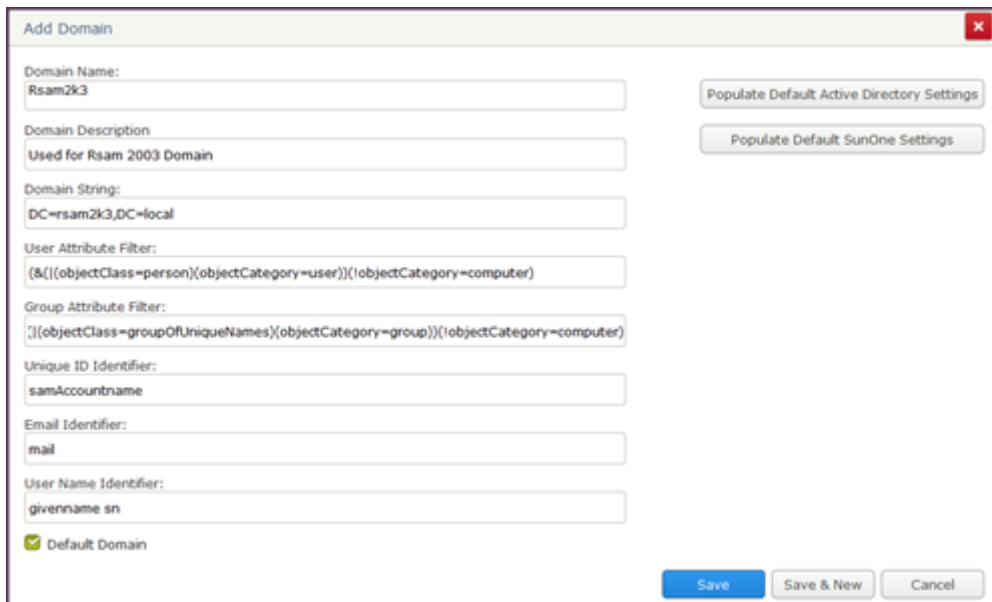
LDAP Server Configuration

To configure the DISTLDAP file name, select **LDAP Admin - Server**. If there is more than one LDAP server, click **Add** to add the additional servers.



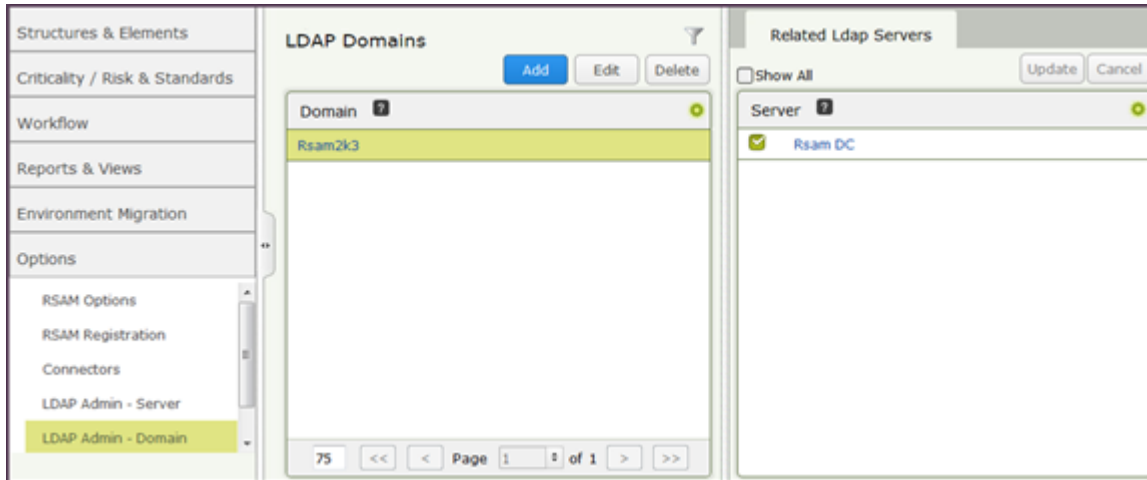
LDAP Domain Configuration

To configure the LDAP domain details, select **LDAP Admin - Domain**. Make sure to enter the **Domain String** in the format as *dc=...,dc=...* or *o=...* (do not enter it like Rsam2k3.local).



Associating LDAP Domains to LDAP Servers

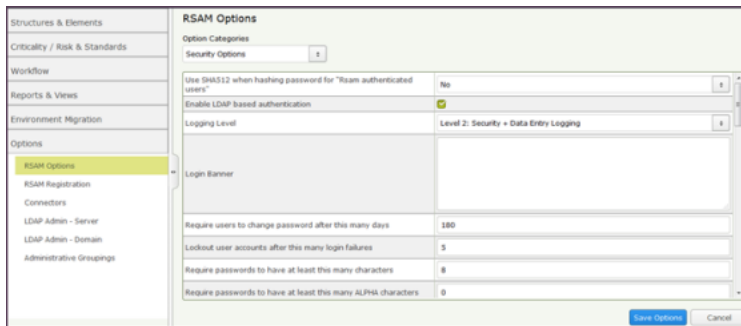
After configuring the LDAP Servers and domains, you must associate them. From one of the LDAP pages, use the **Related LDAP Domains** or **Related LDAP Servers** panel, establish the association.



Enabling LDAP-based Authentication

To enable LDAP-based authentication, go to **Manage > Administration > Options > RSAM Options** and select **Security Options** from the **Option Categories** drop down list.

Select the check box corresponding to **Enabled LDAP based authentication**.



Complete the following steps on the web server (to create the ***DISTLDAP.dat*** file that contains the credentials for the Domain configured):

1. Navigate to the location, *X:\inetpub\wwwroot\RSAM* and launch the application **MAKE_DISTWEB_LDAP.exe** (right-click and select **Run as Administrator**, if the web server is Windows Server 2012/2016/2019/2022).
2. Provide the following information when prompted.

Prompt	Required Information
Connection File	Name of the file to store SQL connection information (the default of DISTLDAP.dat is preferred).

Prompt	Required Information
LDAP User ID	Name of the LDAP user account that Rsam Web must use when querying the LDAP Server. Note: Do not use the format <i>DOMAIN LDAP name</i> . Provide the LDAP name. If that fails, use the fully qualified LDAP name (<i>CN=...</i>).
LDAP Password	Password to use when querying the LDAP Server.

- After providing the details, click **Create Connection** to finish the setup.

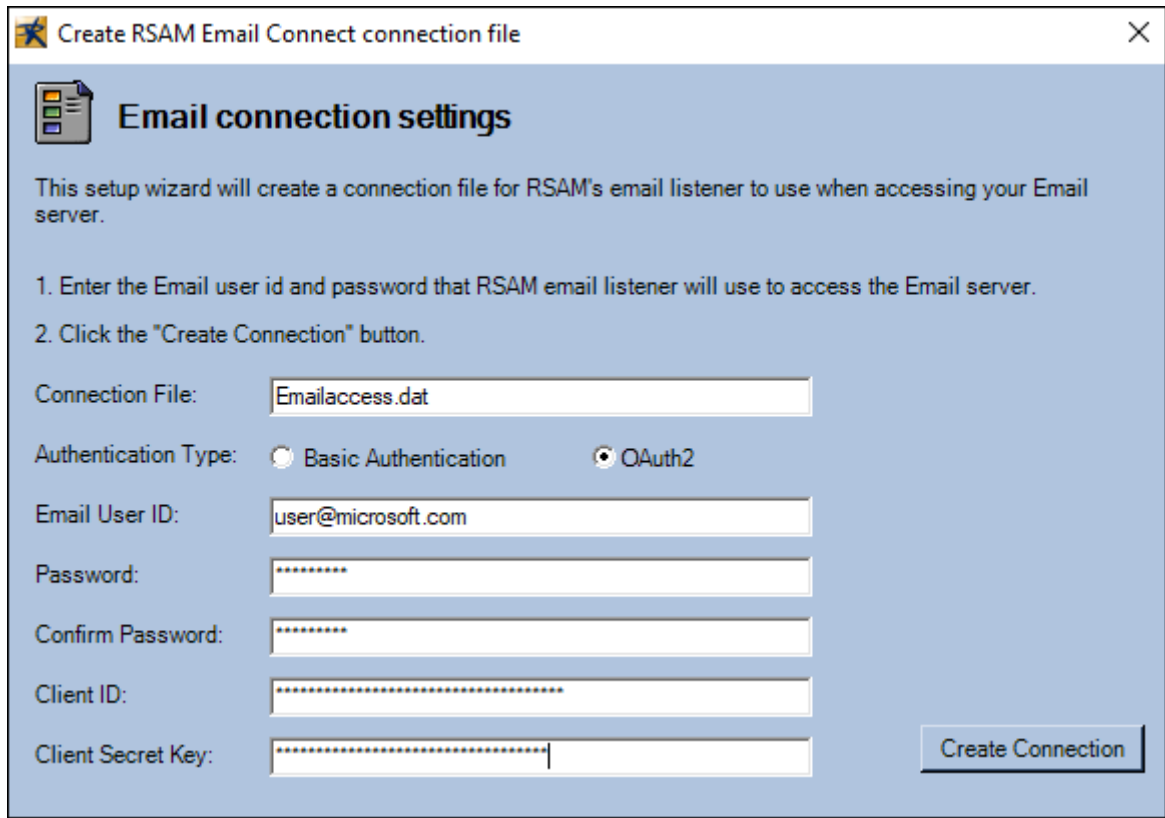


- Copy the **DISTLDAP.dat** file into **RSAM_FINDINGS**, **RSAM_PERMISSIONS**, **RSAM_WEBADMIN**, **RSAM_SSO** (optional), and also into the **RSAM_SCHEDULER** folder.

Enabling Web Server-based Email Notification

To enable web server-based email notification, perform the following steps:

- Navigate to the RSAM Scheduler Service folder (RSAM_SCHEDULER) and perform the following:
 - Right-click **MAKE_EMAIL_CONNECT.exe** and select **Run as Administrator**.
 - Type **Emailaccess.dat** in the **Connection File** field.
 - Select the **Authentication Type**:
 - Basic Authentication**: Requires only email ID and password.
 - OAuth2**: Requires client ID and secret key in addition to email ID and password.
 - Provide an email address in the **Email User ID** field, from which the email notifications will be sent.
 - Provide a password and confirm it.
 - If you have selected **OAuth2** authentication, provide client ID and secret key also.



Create RSAM Email Connect connection file

Email connection settings

This setup wizard will create a connection file for RSAM's email listener to use when accessing your Email server.

1. Enter the Email user id and password that RSAM email listener will use to access the Email server.
2. Click the "Create Connection" button.

Connection File:

Authentication Type: Basic Authentication OAuth2

Email User ID:

Password:

Confirm Password:

Client ID:

Client Secret Key:

- g. Click **Create Connection**.
2. Log in to Rsam as an Account Administrator (or higher) account.
 3. Navigate to **Manage > Administration > Options > Rsam Options** and select **E-mail Notification** from the **Option Categories** drop down list.
 4. Select the check boxes corresponding to **Enable e-mail notification** and **Enable Web Server based emails for RSAM Notification**.
 5. Set the **E-mail Address** and **Reply E-mail Address** (typically the same email address as set in the Emailaccess.dat file).
 6. Set the desired **Display Name** to show in the email.
 7. Set the **Email Server Name** (or IP address) and the **Email Server Port**.
 8. Select the **Use SSL for authentication** option if SSL is required.
 9. Set the **Email connection file name** as **Emailaccess.dat**.
 10. If you selected **OAuth2** authentication, fill in the following fields also:
 - a. Specify the scope of OAuth2 authentication in **OAuth2 - Scope** field.
 - b. Specify the OAuth2 token URL in the **OAuth2 - Token Endpoint URL** field.
 11. Click **Save Options**.

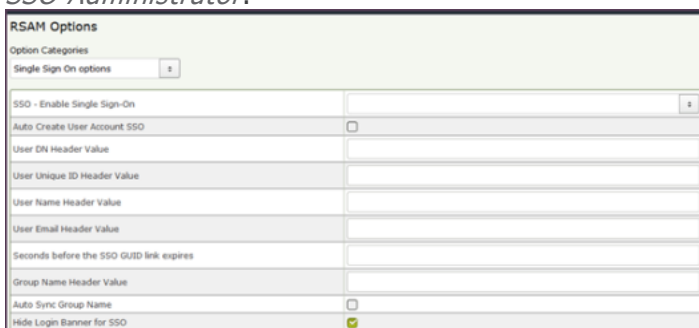
Enabling Single Sign-on

To enable Single Sign-on functionality, perform the following steps:

1. Log in to Rsam as an *Administrator*.
2. Navigate to **Manage > Administration > Options > RSAM Options** and select **Single Sign On options** from the **Option Categories** drop down list.
3. Select an option in the **SSO – Enable Single Sign On** field depending on your applicable scenario.

Single Sign-on Option	Description
Windows Authentication	Select this option if users log in to an Active Directory Domain, and you want Rsam to utilize their same AD login credentials automatically. Then leave all the User...Header Value fields blank. Note: This will work only for users logged into the AD domain. Users outside of the domain can still gain access through the normal username / password prompt.
Other SSO	Select this option if you plan to use a Single Sign-on tool, such as Tivoli Access Manager, SiteMinder, or CoSign. Then set the 'User...Header Value' field to the value provided by your SSO administrator (see screenshot below).
Other SSO (Non LDAP)	This option is used in special cases with more custom methods of Single Sign-on. If Windows Authentication or Other SSO does not work, contact <i>Rsam Customer Support</i> . Then set the User...Header Value fields to the value provided by your <i>SSO Administrator</i> .

4. Set the **User DN Header** value if using either **Other SSO** or **Other SSO (Non-LDAP)** option. This value is variable depending on the SSO technology. It is a value that is configured by your *SSO Administrator*.



Configuration for Tivoli Access Manager (TAM)

Ensure that the following steps are completed prior to using TAM.

The following steps will enable Rsam to utilize the TAM single sign-on feature:

1. Rsam web and administrative console are operational.
2. Rsam can authenticate a user using the LDAP directory.
3. A TAM Junction has been setup for the Rsam server.

Rsam Configuration

Configure the following steps in Rsam:

1. Log in to Rsam as an *Administrator*.
2. Navigate to **Manage > Administration > Options > RSAM Options** and select **Single Sign On options** from the **Option Categories** drop down list.
3. Complete the following options:
 - **SSO - Enable Single Sign-On** = Other SSO
 - **User DN Header Value** = iv-user.
Enter the name of the header variable providing the distinguished name of the user.
 - **User Unique ID Header Value** = iv-user-l
Enter the name of the header variable providing the unique ID name.
 - **User Name Header Value** = XXXX (Optional)
Enter the name of header variable providing the name of the user.
 - **User Email Header Value** = XXXX (Optional)
Enter the name of header variable providing the email address of the user.

Now, using the same user account that was previously set to authenticate on the LDAP, attempt the single sign-on by loading the Rsam Sign In page again.

Example TAM Configuration

The following example TAM statement will provide http header information back to Rsam web server:

```
server task default-webseald-tamwebseal.tamver1.com create -t tcp -c iv-user,iv-user-l -f -x -  
h\www.tamver1.com /
```

Configuring Email Listener

If you purchased the Email Listener module and would like to use this functionality, perform the following steps:

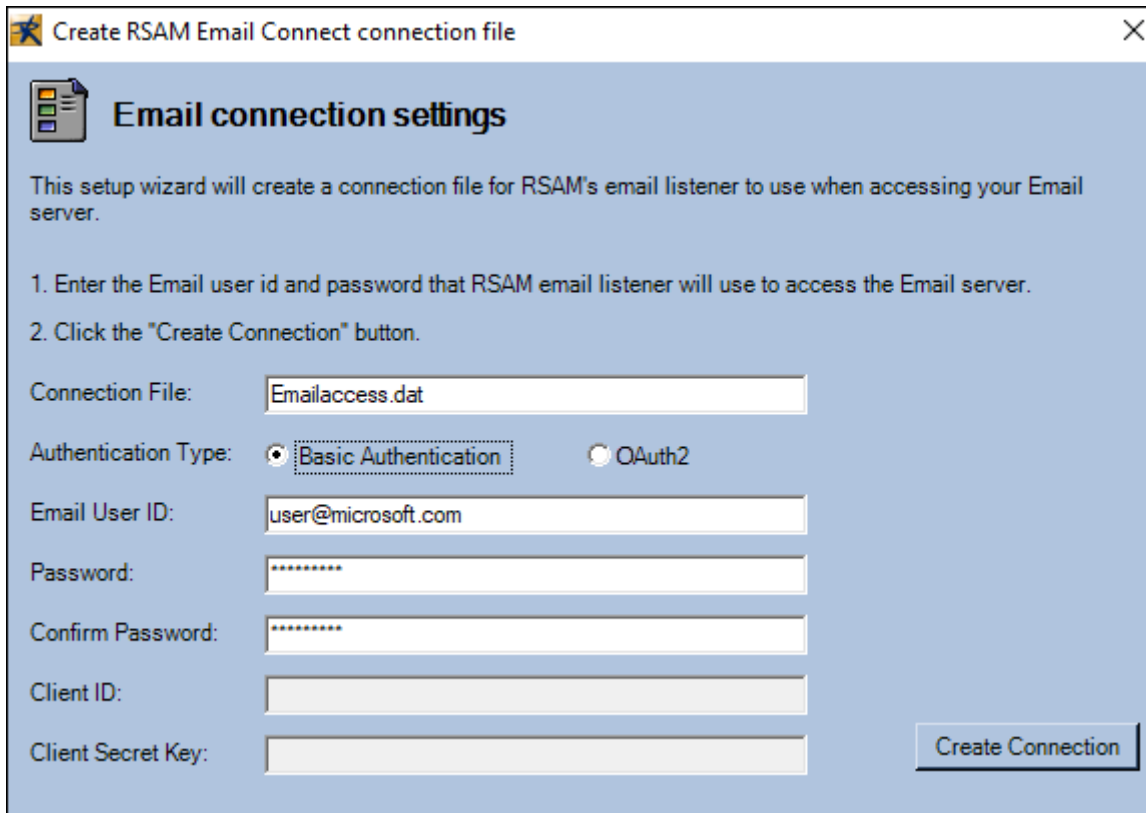
1. Make sure the Email Listener module has been registered on the database.
To verify this, log in to Rsam as an *Administrator* and navigate to **Manage > Administration > Workflow** and check if **Email Listeners** is enabled (if it is disabled then it has not been registered and you must contact the *Rsam Customer Support* to obtain a new license key, if this module was purchased).
2. Enable the Email Listener:

- a. Log in to Rsam as an *Administrator* and navigate to **Manage > Administration > Options > Rsam Options** and select **Email Listener Options** in the **Option Categories** drop down list.
- b. Set the **Email Server Type, Email Server Name, Email Server Port, Email connection file name**, and modify other options as needed.
- c. If you selected **OAuth2** authentication to create the connection file, fill in the following fields also:
 - a. Specify the scope of OAuth2 authentication in **OAuth2 - Scope** field.
 - b. Specify the OAuth2 token URL in the **OAuth2 - Token Endpoint URL** field.
- d. Click **Save Options**.

Creating Email Connection file on Web Server

The email connection file is created by using the **MAKE_EMAIL_CONNECT.exe**. This file can be found in the Rsam Scheduler Service folder (typically either in *C:\Program Files\RSAM_SCHEDULER_SERVICE* or *C:\inetpub\wwwroot\RSAM_SCHEDULER_SERVICE*). You can check the path by opening Services program, right-clicking **Rsam Scheduler** and selecting **Properties**. Note the **Path to executable** value.

1. Type **Emailaccess.dat** in the **Connection File** field.
2. Select the **Authentication Type**:
 - **Basic Authentication**: Requires only email ID and password.
 - **OAuth2**: Requires client ID and secret key in addition to email ID and password.
3. Enter the **Email User ID / Password** of user to access your mailbox.
4. If you selected **OAuth2** authentication, provide client ID and secret key also.
5. Click **Create Connection**.



Enabling Assessment Questionnaire Interface

The following section explains the steps to enable Assessment Questionnaire in Rsam.

Importing Migration File

To import the migration xml file, perform the following steps:

1. Log in to Rsam as *Administrator*.
2. Navigate to **Manage > Administration > Environment Migration > Import**.
3. Click **Browse** to locate the **MigrationFileName.xml** script file and click **Import**.

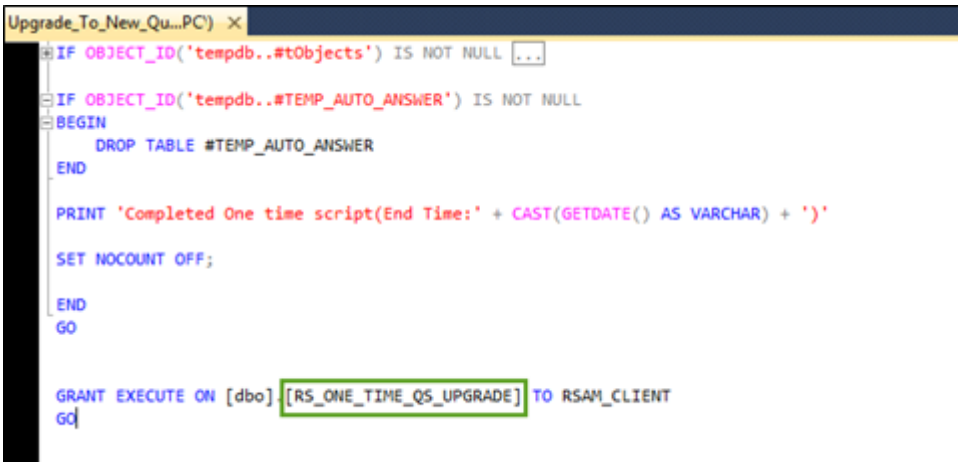
On successfully importing the xml file, corresponding data is migrated to the database for that Rsam instance.



Running Store Procedure and Script files

To run the store procedure and script files, perform the following steps:

1. Obtain the **Upgrade_To_New_Questionnaire.sql** and run the database script file.
2. Execute the **RS_ONE_TIME_QS_UPGRADE** stored procedure.



```
Upgrade_To_New_Qu...PC) x
IF OBJECT_ID('tempdb..#tObjects') IS NOT NULL ...
IF OBJECT_ID('tempdb..#TEMP_AUTO_ANSWER') IS NOT NULL
BEGIN
    DROP TABLE #TEMP_AUTO_ANSWER
END
PRINT 'Completed One time script(End Time:' + CAST(GETDATE() AS VARCHAR) + ')'
SET NOCOUNT OFF;
END
GO

GRANT EXECUTE ON [dbo].[RS_ONE_TIME_QS_UPGRADE] TO RSAM_CLIENT
GO
```

Note: Running the Store Procedure will take substantial amount of time depending on the volume of data.