PERSPECTIVE.

powered by **Resolver**

Connect Installation Guide

Version 1.1

August 2018

Connect by Resolver Inc.™

Distributed August 2018.

Notices and Intellectual Property Information

Notice

Table of Contents

Connect System Requirements

In addition to the requirements outlined in the Perspective System Requirements, Connect requires the following:

- .NET Core 2.2 (Windows Hosting bundle);

- The Application Initialization feature in IIS;

- Google Chrome; and

- RabbitMQ Server 3.7.7 and above.

RabbitMQ Server is a free, open-source message broker software, which can be downloaded, along with their installation guides, from the RabbitMQ website.

Browser Requirements

Connect is run on the latest version of Google Chrome. Visit the Google support site to download Chrome and to ensure your computer meets the Chrome minimum system requirements.

Additional Requirements

As part of the configuration process for Connect, ensure that:

- Any users who will be accessing Connect has a Dispatch user account that has been granted **Connect Access**. A Connect account is required to complete the connector configurations, as outlined in this guide. See the Dispatch Administrator's Guide for more information on creating user accounts.

- The Dispatch locations and indoor locations you wish to associate with the connectors and devices have been created and are fully configured with floorplan or map images uploaded for each master location and indoor location.

- Dispatch templates for the appropriate operational zones and work zones have been created, with a description or notes that indicate the dispatch has been created through Connect.

- See the Lenel OnGuard Connector Installation Guide or the Software House C-Cure Connector Installation Guide for additional requirements.

Introduction

Connect is a module developed by Resolver that uses tools, called **connectors**, to pull event and device data from security systems (Lenel OnGuard and C-Cure 9000) to send that data to Dispatch.

Once Connect and the relevant connectors are installed and configured, the security equipment (**devices**) being monitored by the source systems are registered in Connect so that an administrator can create rules and actions to specify what happens when an event is logged.

Important Notes About This Guide

This guide covers how to install and configure Connect and the Dispatch connector. The Dispatch connector is an **output** connector that sends data to Dispatch.

After completing the steps in this guide, you will need to install and configure at least one additional **input** connector, which receives data from the source system. See the following guides on the Resolver Support site for instructions on installing the appropriate connector:

- **Lenel OnGuard Connector Installation Guide**
- **Software House C-Cure Connector Installation Guide**

For information on editing the connectors, registering and mapping devices, and creating rules, see the Connect User's Guide.

Before You Begin

Who Should Use This Guide

This guide provides instructions on installing and configuring Connect and the Dispatch connector.

See the Lenel OnGuard Connector Installation Guide or Software House C-Cure Connector Guide for instructions on installing additional connectors.

For more information on using Connect once it's been fully installed and configured, see the Connect User's Guide.

Notes, Tips & Warnings

Throughout this guide, you'll see the following symbols:

i	Indicates a **NOTE**.
✔	Indicates a **TIP**.
⚠	Indicates a **WARNING**.

Install Connect

Following the successful installation and configuration of Connect, as outlined below, the Dispatch connector must be configured and activated.
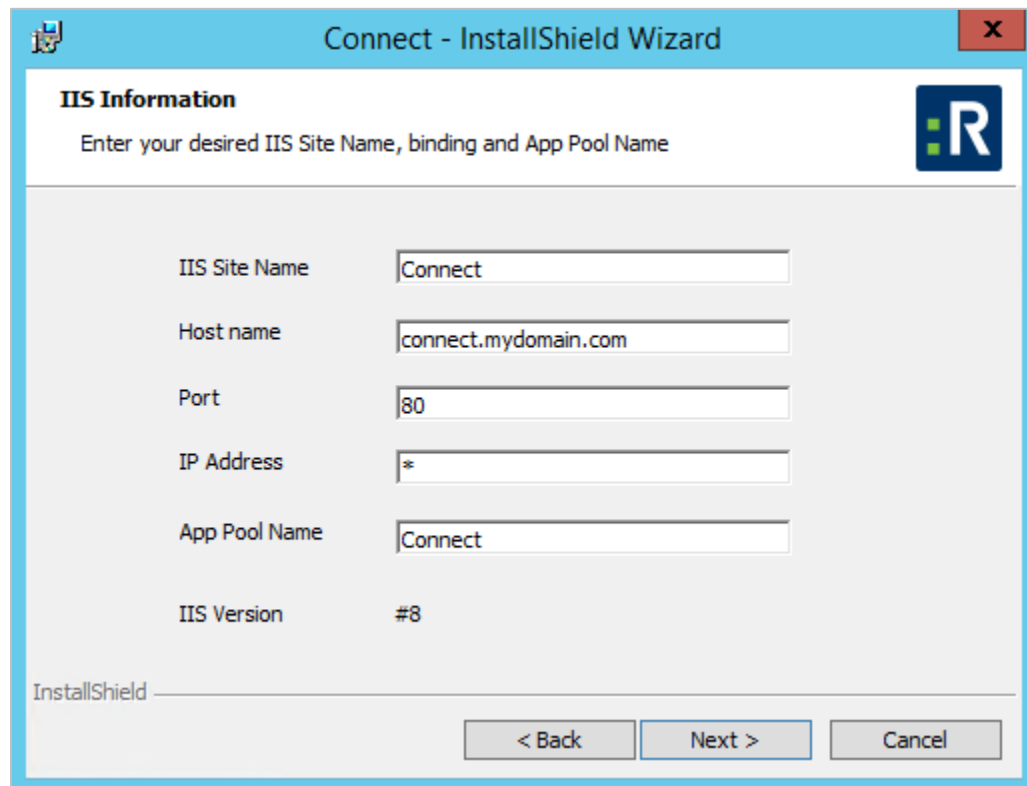
To install Connect:

1. Navigate to the **Connect Setup** folder in the Perspective download package.

2. Run the **Connect.exe** file to open the InstallShield Wizard.

3. Click next to follow the steps in the wizard until you reach the **IIS Information** step. Connect deploys its own site in IIS and requires additional information:

    a. Enter the name of the site in the **IIS Site Name** field.

    b. Enter the host name and port in the **Host name** and **Port** fields.

> *i*   Ensure the host name and port is not currently being used by any other site on the web server.

    c. **Optional:** Enter a specific IP address in the **IP Address** field. If a specific IP address is not required, leave this field with a *****.

    d. **Optional:** Enter an alternate name in the **App Pool Name** field.

*The **IIS Information** step in the install wizard.*

4. Complete the steps in the install wizard.

5. Navigate to the *C:\inteput\wwwroot\Connect\wwwroot*. This is the default location where Connect is installed and may vary depending on the location you selected during installation.

6. Right-click the **config.js** file, then select **Open with** to open the file with Notepad.

7. Change the URL after **CONNECT_API** from *http://localhost/api* to your Connect URL (e.g. *https://<servername>/api*).

8. Click **File > Save**, then close the file.

9. Navigate to *C:\inteput\wwwroot\Connect*.

10. Right-click the **appsettings.json** file, then select **Open with** to open the file with Notepad.

11. Make edits to the following settings in the file:

> ⓘ Ensure your changes are entered in the **appsettings.json** file within the quotations marks after the semi-colon for each setting (e.g. "DatabaseId": "**default**",). Additionally, because this is a JSON file, ensure that any single backslashes (\) are entered as double slashes (\\).

```
{
  "Authentication": {
    "Url": "https://<servername>/IntegrationServices",
    "DatabaseId": "default",
    "BusinessId": "default"
  },
```

*The **appsettings.json** file. Ensure the changes made to the **appsettings.json** file are made between the quotation marks.*

a. **Authentication:**

    i. **Url:** Enter the Integration Services instance used for authentication when logging into Connect (e.g. *https://<servername>/IntegrationServices*).

    ii. **DatabaseId:** Enter the name of your Perspective database.

    iii. **BusinessId:** Enter your Perspective Business ID (e.g. default).

b. **Logging** (optional):

    i. **LogLevel:** Enter one of the following log levels for **Default**, **System**, and **Microsoft** (note that if no values are entered for **System** and/or **Microsoft**, the values entered for **Default** will be applied):

        1. **Debug:** The highest log value. This value is often used by developers and for troubleshooting.

2.   **Information:** Useful to support staff by providing context to errors.

3.   **Error:** Displays critical error logs.

c.   **Application Insights** (optional)**:**

i.   **Instrumentation Key:** Enter the Azure ID to output the logs. This optional configuration allows you to include a monitoring tool for the Connect and connectors.

d.   **ConnectionStrings:**

i.   **ConnectDatabase:** Enter the database connection for the Connect database.

e.   **QueueClients:**

•   **Connectors:**

i.   **VirtualHost:** Enter the name of the RabbitMQ Virtual host name.

ii.   **HostName:** Enter the host name of the server where RabbitMQ is installed.

iii.   **UserName:** Enter the username of the RabbitMQ user who has full access to the RabbitMQ virtual host instance.

iv.   **Password:** Enter the password of the RabbitMQ user.

•   **Perspective:**

i.   **VirtualHost:** Enter the name of the RabbitMQ Virtual host name.

ii.   **HostName:** Enter the host name of the server where RabbitMQ is installed.

iii.   **UserName:** Enter the username of the RabbitMQ user who has full access to the RabbitMQ virtual host instance.

iv.   **Password:** Enter the password of the RabbitMQ user.

> *i*   The RabbitMQ settings above must match the Connector and Perspective config files.

f.   **DataAccessCache:**

i.   **CacheExpiryTimeSeconds:** By default, the Connect cache is set to refresh every 30 seconds and is the minimum required time. Contact Resolver Support should you wish to change the cache refresh rate to fewer than 30 seconds.

g.   **JWTIssuerOptions:**

i.   **Audience:** Enter the Connect URL (e.g. *https://<servername>/*).

ii.   **ValidFor:** Enter the amount of time a Connect session will remain in **hh:mm:ss** format. By default, a Connect session will remain active during a period of inactivity for 5 minutes.

```json
{
  "Authentication": {
    "Url": "                              ",
    "DatabaseId": "        ",
    "BusinessId": "          "
  },
  "Logging": {
    "IncludeScopes": false,
    "LogLevel": {
      "Default": "Debug",
      "System": "Debug",
      "Microsoft": "Debug"
    }
  },
  "ApplicationInsights": {
    "InstrumentationKey": "                          "
  },
  "ConnectionStrings": {
    "ConnectDatabase": "                                                                              "
  },
  "QueueClients": {
    "Connectors": {
      "VirtualHost": "        ",
      "HostName": "                ",
      "UserName": "        ",
      "Password": "        ",
      "NetworkRecoveryIntervalInSeconds": 5,
      "Queues": {
        "Events":
        { "SubscriberChannels": 3 }
      }
    },
    "Perspective": {
      "VirtualHost": "        ",
      "HostName": "                ",
      "UserName": "        ",
      "Password": "        ",
      "NetworkRecoveryIntervalInSeconds": 5,
      "Queues": {
        "Events":
        { "SubscriberChannels": 3 }
      }
    }
  },
  "DataAccessCache": {
    //Minimum is 30 seconds.
    "CacheExpiryTimeSeconds": "30"
  },
  "JwtIssuerOptions": {
    "Issuer": "Connect",
    "Audience": "                              ",
    //Optional setting. Format: hh:mm::ss this is an optional setting. Default is 5 minutes.
    "ValidFor": "01:00:00"
  }
}
```

*A fully configured **appsettings.json** file.*

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

Configure the Application Pool Settings

To ensure Connect is always running, additional configurations will need to be made in IIS.

To configure the application pool settings:

1. Open **Internet Information Services (IIS) Manager** on the web server.

2. Click **Application Pools** in the **Connections** pane to the left.

3. Click to select the **Connect** application pool in the center panel, then click **Advanced Settings...** in the **Actions** pane to the right.

4. From the **General** section, select **AlwaysRunning** from the **Start Mode** dropdown menu.
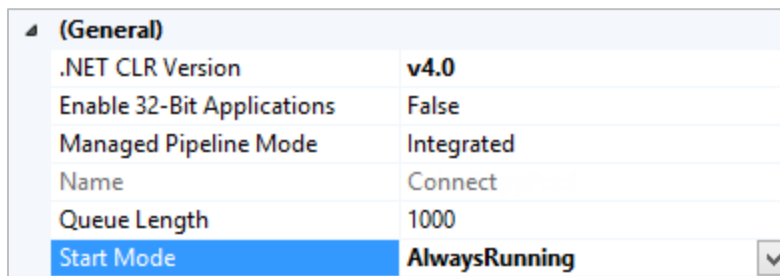
*The **Start Mode** settings in the **Advanced Settings** window.*

5. From the **Process Model** section:

   a. Select **Suspend** from the **Idle Time-out Action** dropdown menu.

   b. Select **True** from the **Load User Profile** dropdown menu.
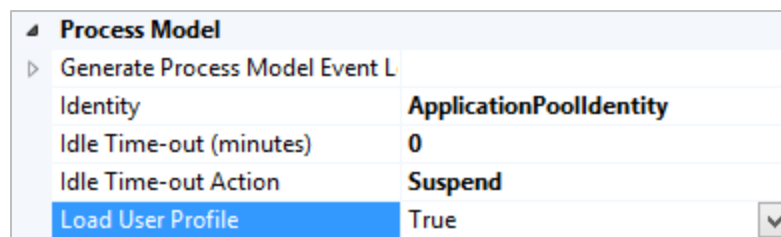
*The **Idle Time-out Action** and **Load User Profile** settings in the **Process Model** section.*

6. Click **OK** to save your changes.

7. Click **Sites** in the **Connections** pane to the left.

8. Click the **Connect** site, then select it in the center pane.

9. Click **Advanced Settings...** in the **Actions** pane to the right.

10. Select **True** from the **Preload Enabled** dropdown menu.

11. Click **OK** to save your changes.

12. Restart the Connect application pool:

     a. Click **Application Pools** in the **Connections** pane.

     b. Click the Connect application pool in the center pane to select it.

     c. Click **Stop** in the **Actions** pane in to the right, then click **Start**.

13. Restart the Connect site:

     a. Click **Sites** in the **Connections** pane.

     b. Click the Connect site in the center pane to select it.

     c. Click **Stop** in the **Actions** pane to the right, then click **Start**.
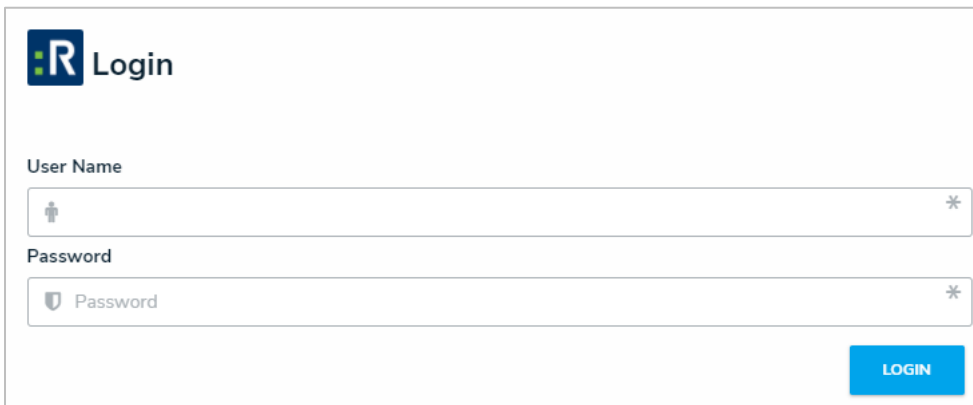
14. Close IIS.

Dispatch Connector

The **Dispatch Connector** allows Connect data to be sent to Dispatch. This connector does not require installation; however, you must log into Connect to configure the connector's settings. As such, ensure you have login credentials for a Dispatch user account that's authorized to access Connect prior to completing the steps below. See the Dispatch Administrator's Guide for more information on creating user accounts.

Activate the Dispatch Connector

To activate the Dispatch connector:

1. Using Google Chrome, navigate to *https://**<servername>**/session**.**

2. Enter your Dispatch user name and password in the **User Name** and **Password** fields.

*The **Connect** login screen.*

3. Click **Login** to display the **Connectors** page.

4. Click **Edit** beside the **Dispatch Connector** to open the **Edit Connector** screen.

*The **Details** tab of the **Edit Connector** screen.*

5. If necessary, change the name of the connector in the **Connector Alias** field. The remainder of the fields in the **Details** tab are read only.

6. Click the **Settings** tab.

7. Enter the user name and password of your Dispatch account in the **User Name** and **Password** fields.

8. Enter the database, service URL, and business ID for Dispatch in the **Database ID**, **Service Folder**, and **Business ID** fields.

> ⚠️ Ensure the prefix **https://** is included when entering the service URL in the **Service Folder** field. If this prefix is not included, the location and indoor location images will not be displayed when mapping devices.

*The **Settings** section of the **Edit Connector** screen.*

9. Click **Save**.

10. Refresh the browser. The circle in the **Status** column beside the connector should be **green** to indicate the connector has been successfully configured.

Contact Information

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