Remote Support
Middleware Engine Installation and Configuration
Table of Contents

BeyondTrust Remote Support Middleware Engine Installation and Configuration ........ 3

Install the BeyondTrust Remote Support Middleware Engine .................................. 4
  Applicable Versions ........................................................................................................ 4
  Network Considerations .................................................................................................... 4
  Server Requirements ........................................................................................................ 4
  Prerequisite Installation and Configuration ................................................................. 4
  BeyondTrust Middleware Engine Installation ............................................................... 5
  BeyondTrust Middleware Engine Installation Verification ............................................. 5

Configure the BeyondTrust Remote Support Middleware Engine ................................. 6
  Starting and Stopping the BeyondTrust Middleware Engine ........................................ 6
  Deploying the Plugin ......................................................................................................... 6
  Launching the Middleware Administration Tool ............................................................ 6
  Overview of the Middleware Administration Tool .......................................................... 6
  Configuring the Middleware Administration Tool .......................................................... 8
  Install the Web Platform Installer 5.0 and Required Components .................................. 12

BeyondTrust Remote Support Middleware Engine Installation and Configuration

The BeyondTrust Middleware Engine is a Windows service that acts as the backbone for integrations with BeyondTrust Remote Support. The BeyondTrust Middleware Engine provides a plugin integration architecture - plugins can be developed and deployed to the product, and the product provides data and administrative services to the plugin.
Install the BeyondTrust Remote Support Middleware Engine

To complete this installation, please ensure that you have the necessary software installed and configured as indicated in this guide, accounting for any network considerations.

Applicable Versions

- BeyondTrust Remote Support: 14.x and newer
- BeyondTrust Middleware Engine: 1.0.0.0

Network Considerations

The following network communication channels must be open for the BeyondTrust Middleware Engine to work properly.

<table>
<thead>
<tr>
<th>Outbound From</th>
<th>Inbound To</th>
<th>TCP Port #</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>BeyondTrust Middleware Engine Server</td>
<td>Secure Remote Access Appliance</td>
<td>443</td>
<td>API calls from the BeyondTrust Middleware Engine server.</td>
</tr>
<tr>
<td>Secure Remote Access Appliance</td>
<td>BeyondTrust Middleware Engine Server</td>
<td>8180 (if using default configuration)</td>
<td>This is needed for plugins which integrate with BeyondTrust outbound events. Please check the documentation for all plugins used. If no plugins use outbound events, then this port does not have to be open.</td>
</tr>
</tbody>
</table>

Server Requirements

The BeyondTrust Middleware Engine requires installation on Windows Server 2012 R2 or higher. See specific requirements below.

<table>
<thead>
<tr>
<th>Component</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>2 GHz or faster</td>
</tr>
<tr>
<td>Memory</td>
<td>2 GB RAM or greater</td>
</tr>
<tr>
<td>Available Disk Space</td>
<td>80 GB or greater</td>
</tr>
<tr>
<td>OS</td>
<td>64-bit</td>
</tr>
</tbody>
</table>

Prerequisite Installation and Configuration

Visual C++ Redistributable Package for Visual Studio 2015 (x86)

- Visual C++ Redistributable Package for Visual Studio 2015 is required by the BeyondTrust Middleware Engine. If not already present when the BeyondTrust Middleware Engine setup file is run, this package is installed automatically.

.NET 4.6.2

- .NET 4.6.2 or higher is required by BeyondTrust Middleware Engine. If not already present when the BeyondTrust Middleware Engine setup file is run, .NET 4.6.2 is installed automatically.
BeyondTrust Middleware Engine Installation

- Run `bomgar-middleware-engine.exe`, following on-screen instructions.
- If Visual C++ Redistributable Package for Visual Studio 2015 and/or .NET 4.5.2 are not already installed on the server, they are installed at this time.

BeyondTrust Middleware Engine Installation Verification

1. Open your services management console by typing `services.msc` in your Windows Run dialog.
2. Locate the service named BeyondTrust Middleware Engine.
3. Start the service.
4. Open a web browser on the server and go to `http://127.0.0.1:53231/`. A page similar to the one pictured should be seen. This is the BeyondTrust Middleware Administration tool. The "No plugins were found!" message is normal at this point, as no plugins have yet been deployed.

This tool is accessible only from the server where the BeyondTrust Middleware Engine is installed. If necessary, the tool can run on a different port, and it can be turned on/off as desired. For more information, please see "Configuring the Middleware Administration Tool" on page 8.
Configure the BeyondTrust Remote Support Middleware Engine

Starting and Stopping the BeyondTrust Middleware Engine

The BeyondTrust Middleware Engine runs as a Windows service. This service must be restarted whenever a new plugin is deployed or a plugin is removed.

Deploying the Plugin

Note: This section describes the general location and makeup of a plugin deployment. Deployment of specific plugins is beyond the scope of this document.

All plugins are deployed into the Plugins folder in the directory where the BeyondTrust Middleware Engine is installed. Each plugin is deployed into its own folder therein.

Once a plugin has been set up with configuration (described below), a file named <plugin name>.config is present. The Plugins folder may contain any number of other files and folders, depending on the plugin.

Launching the Middleware Administration Tool

If the Windows service is running, the middleware administration tool can be launched. Open a web browser on the server and go to http://127.0.0.1:53231/. This tool is accessible only from the server where the BeyondTrust Middleware Engine is installed.

If necessary, the tool can run on a different port, and it can be turned on/off as desired. For more information, please see "Configuring the Middleware Administration Tool" on page 8.

Overview of the Middleware Administration Tool

The front page of the middleware administration tool displays all deployed plugins as well as each plugin's configuration(s). Multiple plugin configurations can be created. Creating multiple plugin configurations allows a single plugin to integrate with multiple systems, such as two different Secure Remote Access Appliances.

Working with Plugin Configurations

To add a new configuration for a plugin, click on the copy icon next to the plugin name. A screen is presented in which a number of configuration items are collected, including connection information to a Secure Remote Access Appliance and any plugin-specific settings. This screen includes an option to disable a plugin configuration.

For a specific plugin configuration, the following options are available:
Edit the plugin configuration.

Test the plugin configuration. Testing confirms that the plugin is configured correctly and that network resources can be accessed.

**Note:** Test output varies between plugins.

Delete the plugin configuration.

**IMPORTANT!**

Please be careful! The configuration cannot be recovered after deletion.

**Note:** Configuration changes made via the middleware administration tool are immediately effective. It is not required to restart the Windows service.

Working with the event history for a plugin

To view the event history for a plugin, click the history icon next to the plugin name. A page is displayed listing the key details of each event the plugin has processed. The amount of history available depends on the event retention configuration. The default is seven days.

For more information on how to change this setting, please see "Configuring the Middleware Administration Tool" on page 8.

On the plugin events page, the following functionality is available:

- Paging and text filtering.
- Viewing the raw event data.
- Viewing the error data if event processing failed.
- Finding the event GUID, an identifier attached to every log message for the event.
Replaying an event (i.e., sending the event to the plugin to reprocess). This can be useful for events that fail for transient reasons such as a network issue.

Working with the event retries for a plugin

To view the active retries for a plugin, click the clipboard icon located next to the history icon. A page displays listing details about each retry.

The retry is removed from this page when the plugin:

- Successfully processes the event.
- Reaches the retry limit.

The retries are attempted using a Fibonacci back off strategy. This strategy spaces out the retries with the first attempt being five (5) seconds after the initial failure. The maximum number of retries are set per plugin configuration. The Retry Events page provides the functionality required to replay the event before the next attempt time.

Configuring the Middleware Administration Tool

You can modify the middleware administration tool to run on a different port, and you can turn it on/off as desired. You also can change the length of time that events are stored.

1. From the home page of the middleware administration tool, click the Edit Middleware Configuration link.
2. The following configuration options are available:
   - **Logging Level**: Defines the logging level for the BeyondTrust Middleware Engine. Modifications to this value take effect immediately. For maximum logging, select DEBUG. For minimum logging, select ERROR.
   - **Outbound Event Base Address**: The base address BeyondTrust Middleware Engine listens to for outbound events from a Secure Remote Access Appliance. If this value is changed, the Windows service must be restarted.
   - **Middleware Administration Tool Enabled**: If disabled, the web-based tool will not be available. If this value is changed, the Windows service must be restarted.
   - **Middleware Administration Tool Base Address**: The base address on which the administration tool runs. If this value is changed, the Windows service must be restarted.
- **Event Retention Days**: The number of days to keep a record of events delivered to plugins. If this value is changed, the Windows service must be restarted.

3. This same configuration can be edited from a file if desired, such as if the administration tool is disabled.
   a. Go to the directory where the BeyondTrust Middleware Engine is installed.
   b. In a text editor, open `MiddlewareConfig.txt`.
   c. Edit the file as needed. The file is in JSON format. Valid LogLevel values are **ERROR, INFO, WARN, and DEBUG**.

   **Note**: When changing the LogLevel from the text file, the change is not immediately effective. The log level can change dynamically only when it is changed from the administration tool user interface.

Below is the default configuration:

```
{
    "LogLevel": "ERROR",
    "EngineBaseAddress": "http://+:8180/",
    "AdminToolEnabled": true,
    "AdminToolBaseAddress": "http://127.0.0.1:53231/",
    "EventRetentionDays": 7
}
```

d. After making any changes, restart the Windows service.

**Using IIS as a Reverse Proxy for the BeyondTrust Middleware Engine**

The following steps show you how to set up and configure IIS to work as a reverse proxy for the BeyondTrust Middleware Engine, to support scenarios where outbound events from the appliance must go over port 443. For example, outbound events from BeyondTrust Cloud must travel over port 443.

**Note**: This document does not cover how to set up an outbound event in BeyondTrust, since it is assumed that setup has already been completed.

1. In the **Server Manager** dashboard, click **Add roles and features**.
2. Click **Next** on the next screen.
3. Under **Select installation type**, select **Role-based or feature-based installation**. Click **Next**.

4. Under **Server Selection**, click **Select a server from the server pool** and select the desired server. Click **Next**.

5. Under **Server Roles**, select **Web Server (IIS)**. Click **Next**.
6. When you select **Web Server (IIS)**, you are prompted to add IIS management tools. Click **Add Features**.

7. Make sure that **.NET Framework 4.6 Features** is checked, then click **Next**. You do not need to select any additional features.

8. Under **Web Server Role (IIS)**, click **Role Services** on the left menu. Check that the necessary default values are checked.

9. Click **Next**, then **Install**.
10. A progress bar indicates that the installation is taking place. When the installation is complete, click Close.

Install the Web Platform Installer 5.0 and Required Components

After installation is complete, download and install the Microsoft Web Platform Installer 5.0 (https://www.microsoft.com/web/downloads/platform.aspx). Using the Web Platform Installer, install the following elements into IIS:

- URL Rewrite 2.x
- Application Request Routing 3.x

**Note:** You need to restart IIS services (or restart the server) after the installation.

Set Up SSL

1. Open the IIS Manager application, then click the server name in the left hand pane.
2. Click **Server Certificates**.
3. In the **Actions** menu, choose to **Import** your certificate. If a CA certificate is not available, or the configuration is for a development/testing site, you may select **Create a Self-Signed Certificate**.
4. From the right hand panel, under **Sites**, select the **Default Web Site**.
5. From the **Actions** menu, click **Bindings**.
6. Add a binding and choose type **https**.
7. Choose the SSL certificate you imported/created in the prior step.

Configure Reverse Proxy

1. In the right hand panel, under **Sites**, select **Default Web Site**.
2. Double-click **URL Rewrite**.
3. Click **Add Rule(s)**...
4. Select **Reverse Proxy**. If prompted to enable proxy functionality, click **OK**.
5. Enter **127.0.0.1:8180** as the server name and leave other options as default.
6. Restart the **Default Web Site**.
Set Up BeyondTrust Outbound Event to Validate the Certificate (optional)

If desired, you may set up the appliance to validate the server certificate when sending an outbound event.

**Note:** You must have a valid CA certificate in IIS for this setting to work.

1. In the appliance, navigate to Management > Outbound Events.
2. Edit the desired outbound event.
3. Enable the CA Certificate option. Click Choose File and select your CA certificate.
BeyondTrust Remote Support Middleware Engine Common Issues and Causes

<table>
<thead>
<tr>
<th>Issue/Symptom</th>
<th>Possible Causes</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>BeyondTrust Middleware Engine Windows service fails to start.</td>
<td>Installation prerequisites have not been met. For information, please see &quot;Install the BeyondTrust Remote Support Middleware Engine&quot; on page 4.</td>
<td>For additional troubleshooting information, open the Windows event viewer and look for any messages in the application log with a source of MiddlewareEngineService or BeyondTrustMiddlewareEngine. You may also go to the directory where the BeyondTrust Middleware Engine is installed and look in \Logs\BeyondTrustMiddlewareEngineService.log for additional error messages. If this is a new installation, you may go to Windows Programs and Features, uninstall the BeyondTrust Middleware Engine, and then reinstall it. If the service no longer starts after the MiddlewareConfig.txt file has been modified, either fix the MiddlewareConfig.txt file and try again or delete the MiddlewareConfig.txt file and start the service. The BeyondTrust Middleware Engine will use the default values for configuration. The service should now start, and the admin tool can be used to modify the configuration.</td>
</tr>
<tr>
<td>Events are not being delivered to a plugin as expected.</td>
<td>Invalid configuration of the plugin.</td>
<td>Enable DEBUG logging by opening the administration tool, clicking Edit Middleware Configuration, changing the log level, and saving. Run a test on the plugin configuration in the middleware administration tool. Read the documentation for the specific plugin and ensure the configuration is correct.</td>
</tr>
<tr>
<td></td>
<td>Invalid API configuration on the Secure Remote Access Appliance (e.g., the API account not having proper privileges or incorrect outbound event configuration). Invalid network configuration.</td>
<td></td>
</tr>
<tr>
<td>An events is delivered to a plugin but is failing.</td>
<td>Invalid configuration of the plugin.</td>
<td>Enable DEBUG logging by opening the administration tool, clicking Edit Middleware Configuration, changing the log level, and saving. Run a test on the plugin configuration in the middleware administration tool. Read the documentation for the specific plugin and ensure the configuration is correct.</td>
</tr>
<tr>
<td></td>
<td>Invalid network configuration.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other issues.</td>
<td>In the administration tool, click the history icon next to the plugin. View the list of events and find the one that is failing. Click the link to view the error detail. If the error detail is not enough to diagnose the issue, note the Event GUID for the event, navigate to the logs under &lt;install_dir&gt;\Logs, look through the logs, and find the log message for the event. All log messages for the event will have the event GUID in the message.</td>
</tr>
</tbody>
</table>

If unable to resolve the issue, contact www.beyondtrust.com/support.