Deltek
Speed. Clarity. Control.

REST APIs for Deltek PPM Products

Installation Guide

May 29, 2026

While Deltek has attempted to verify that the information in this document is accurate and complete, some typographical or technical errors may exist. The recipient of this document is solely responsible for all decisions relating to or use of the information provided herein.

The information contained in this publication is effective as of the publication date below and is subject to change without notice.

This edition published May 2026.

Deltek

Contents

Overview

A secure, read-only REST API is available for selected Deltek PPM products, enabling external applications to access product data for reporting and integration scenarios. The REST API is implemented as a stand-alone service that exposes product data through secure HTTP endpoints for use by client applications.

This guide describes how to install and configure the REST API components in your product environment. It is intended for system administrators and technical users responsible for deployment and preparation for client application use.

Supported PPM Product Versions

This table lists the PPM products and their versions that utilize the REST API.

> **Note:** The versions listed represent the minimum supported versions. Subsequent cumulative update (CU) releases within the same major or minor release are supported unless otherwise specified.

Product	REST API	Supported Version
Cobra	Cobra REST API	8.7 Cumulative Update 05 or later
PM Compass	PM Compass REST API	8.5 Cumulative Update 12 or later
Open Plan	Open Plan REST API	Open Plan 8.8 Cumulative Update 01 or later

OpenAPI Specification Document

The REST API is documented using the OpenAPI Specification (OAS) 3.0, which provides a detailed and standardized overview of the API's endpoints, structures, operations, and data models. This documentation enables developers to effectively understand and interact with the REST API.

The REST API OAS document for your product is available on the Deltek Learning Hub (DLH).

REST API	DLH Document Name	Link
Cobra REST API	Cobra REST Service	https://learning.deltek.com/bundle/CobraRESTService
PM Compass REST API	PM Compass REST Service	https://learning.deltek.com/bundle/PMCompassRESTService
Open Plan REST API	Open Plan REST Service	https://learning.deltek.com/bundle/OpenPlanRESTService

Note: The OAS document is also available in Swagger as part of the REST API deployment detailed in this section of the guide.

Deltek

Prerequisites and Software Requirements

Note: The REST API supports a distributed deployment model and does not require installation on the same server where the PPM product is installed.

Prior to installing the REST API for your product, take note of the following:

- You must install and configure Microsoft Internet Information Services (IIS) on the server where you plan to install the REST API. This includes the SSL certificates you may want to use for the REST API.
- You must have a PPM product version that supports the REST API.
- You must install a supported version of the database client that matches your database platform (for example, SQL Server or Oracle) and environment.

Software Requirements

This table outlines the supported technologies used to deploy the REST API.

Supported Deployment Technology	
Operating System	▪ Microsoft Windows Server® 2025 ▪ Microsoft Windows Server 2022 ▪ Microsoft Windows Server 2019
Web Server	▪ Microsoft Internet Information Services (IIS) 10.0 Role enabled
Database Driver	▪ Microsoft OLE DB Driver for SQL Server ▪ Microsoft OLE DB Driver 19 for SQL Server ▪ Oracle Provider for OLE DB

Deltek

Deploying and Utilizing the REST API

This table outlines the steps required to deploy and use the REST API for your product.

	Step	Location in this guide
1	Install and configure Microsoft Internet Information Services (IIS).	Installing and Configuring Microsoft IIS
2	Install the REST API.	Installing the REST API
3	Test the REST API deployment.	Testing the REST API Deployment

Attention: For more information on the prerequisites and software requirements, see Prerequisites and Software Requirements.

Installing and Configuring Microsoft IIS

You must install and configure Microsoft Internet Information Services (IIS) on the server where you plan to deploy the REST API. This section explains how to check if IIS is already installed and, if not, provides instructions on how to install and configure it.

Check if Microsoft IIS Is Already Installed

If you have already enabled the Web Server role on your web server, you need to check the features and role services.

To check the features and role services on Windows Server:

1. Launch Server Manager.
2. On the left menu, click **IIS**.

   If the **IIS** option is not listed, perform the steps for installing Microsoft IIS for the first time.
3. In the **Roles and Features** group, verify that all of the required role services are installed.

   Attention: For more information, see Step 11 in "Install Microsoft IIS For the First Time" below.

Install Microsoft IIS for the First Time

Follow this procedure to install Microsoft IIS for the first time. These steps are necessary for the proper detection of ASP.NET.

To install Microsoft IIS on Windows Server:

1. Log onto Microsoft Windows Server as a domain or local administrator.
2. Launch Server Manager.
3. Click **Manage » Add Roles and features**.
4. On the Before you begin screen of the Add Roles and Features Wizard, click **Next**.
5. On the Select installation type screen, select **Role-based or feature-based installation** and click **Next**.
6. On the Select destination server screen, select your server and click **Next**.
7. On the Select server roles screen, select **Web Server (IIS)**.
    a. In the Add Roles and Features Wizard dialog box, click **Add Features**.
8. On the Select server roles screen, click **Next**.
9. On the Select Features screen, expand **.NET Framework 4.x Features**, select .**NET Framework 4.x and ASP.NET 4.x**, and click **Next**.
10. On the Web Server Role (IIS) screen, click **Next**.
11. On the Select role services screen, enable the following sub-options:

    Web Server

    - **Common HTTP Features**
        - Default Document
        - Directory Browsing
        - HTTP Errors
        - Static Content
        - HTTP Redirection
    - **Health and Diagnostics**
        - HTTP Logging
        - Request Monitor
        - Tracing
    - **Performance**
        - Static Content Compression
    - **Security**
        - Windows Authentication

- Request Filtering
- **Application Development**
  - NET Extensibility 4.x
  - ASP.NET 4.x

> **Note:** The Add Roles and Features Wizard dialog box displays when you select this option. Click the **Add Features** button.

  - ISAPI Extensions
  - ISAPI Filters
- **Management Tools**
  - IIS Management Console
  - IIS Management Scripts and Tools

12. Click **Next**.
13. In the Confirm Installation Instructions dialog box, click **Install** to begin the process.

> **Note:** On the Confirm installation selections screen, if a message displays about specifying an alternate source path, see the Microsoft KB Article # 2734782 (Method 2).

14. In the Installation Results dialog box, click **Close**.

Install IIS Using Windows PowerShell

Alternatively, you can use Windows PowerShell (Admin) to install IIS.

To install IIS using PowerShell:

1. Open Windows PowerShell (Admin).
2. Run the following command to install the required features:

```
Install-WindowsFeature -Name Web-Server,Web-Http-Redirect,Web-Request-
Monitor,Web-Http-Tracing,Web-Windows-Auth,Web-Net-Ext45,Web-Asp-Net45,Web-
ISAPI-Ext,Web-ISAPI-Filter,Web-Scripting-Tools -IncludeManagementTools
```

3. Run the following command to verify the installed features:

```
Get-WindowsFeature -Name Web-
```

Verify TLS Configuration on the Web Server

You must enable TLS 1.2 on the web server.

In addition, ensure that the following protocols are disabled:

- SSL 2.0
- SSL 3.0
- TLS 1.0
- TLS 1.1

Configure IIS for HTTPS Access on the Web Server

Follow this procedure to configure additional IIS settings to enable HTTPS access using an SSL certificate.

To configure IIS for HTTPS access:

1. Verify that the fully qualified domain name (FQDN) is resolvable and that you can access the FQDN URL.
2. Install an HTTPS (SSL) certificate on the web server.

   The certificate must be issued by a third-party certificate authority (CA), such as VeriSign, DigiCert, Thawte, or Comodo.

   a. Log on to the web server and click **Administrative Tools » IIS Manager**.

   b. In the navigation pane, select the server.

   c. Double-click **Server Certificates**.

   d. In the Actions pane, select one of the following options:

   - **Import**: Select this option if you already have a certificate and want to import it to the server.
   - **Create Certificate Request**: Select this option to generate a certificate request file to submit to a Certificate Authority (CA).
   - **Complete Certificate Request**: Select this option to complete a previously submitted certificate request and install the issued certificate.
   - **Create Domain Certificate**: Select this option if your domain has an internal Certificate Authority.
   - **Create Self-Signed Certificate**: Select this option to test SSL functionality or troubleshoot SSL certificate issues.

3. Create an SSL binding for the website.

   a. Expand **Sites** and select the website.

   b. In the Actions pane, click **Bindings**.

c. In the Site Bindings dialog box, click **Add**.

d. In the Add Site Binding dialog box, select **https** in the **Type** field.

The **Port** value automatically changes to **443**.

e. In the **IP address** field, select the IP address or **All Unassigned** (default).

f. In the **SSL certificate** field, select the certificate.

g. Click **OK**.

h. Verify the configuration by accessing the website using **https://** and confirming that the site loads correctly.

Installing the REST API

Use Deltek Software Manager (DSM) to download the REST API installer for your product. The installer is included as a sub-release under the PPM product version that supports the REST API.

PPM Product	Installer Name
Cobra	DeltekCobraRESTAPI1.0.0700.###.msi
PM Compass	DeltekPMCompassRESTAPI1.0.0700.###.msi
Open Plan	DeltekOpenPlanRESTAPI1.0.0700.###.msi

The installer includes the REST API for your product as part of the standard installation (for example, **CobraRESTAPI**).

Run the REST API Installer

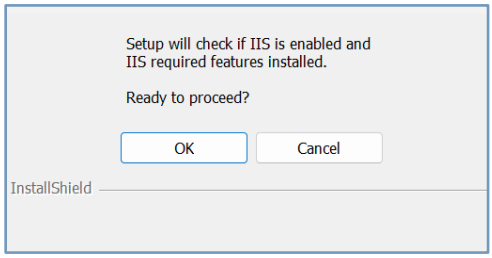
Follow this procedure to run the REST API installer.

To run the installer:

1. Launch DSM, expand the PPM product, click **Sub-Release**, and download the REST API installer for the supported product version.
2. Locate the downloaded installer and note where it is saved.
3. Search for and right-click the Command Prompt, then select **Run as administrator**.
4. Type the full path to the **.msi** file, including its name, then press Enter to start the installation.

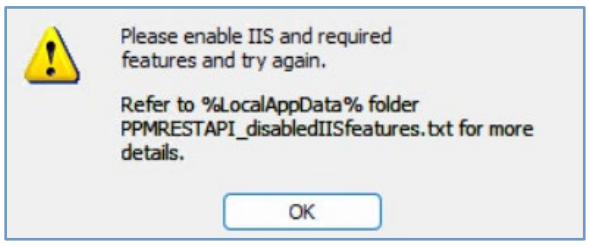
   The installer validates admin rights. Click **Yes** to continue or click **No** to exit.
5. On the Welcome screen, click **Next**.

   The installation wizard checks if IIS is enabled and the required features are installed.



Click **OK**. Once the check is performed and passed, the installation proceeds.

If the installer wizard detects that some required IIS features are missing, it displays a warning and exits.



> **Note:** Clicking **OK** launches the **DeltekPPMRESTAPI_disabledIISfeatures.txt** file, listing the missing required IIS features that caused the warning message. The file is located in the **User\AppData\Local** folder.

6. On the Application and Destination folder screen, select the component to install, specify the installation location for the REST API, and click **Next**.

> **Note:** The REST API is installed in the following default directory: **C:\Program Files\Deltek\PPMRESTAPI\<PPM product>**. Deltek recommends using this default directory.

7. On the Logon Information screen, enter the service account credentials that will be used to configure the IIS application pool.

> **Note:** Deltek strongly recommends that you use your domain account.
>
> - The **Password** field is masked for security (shown as asterisks or dots).
> - Whitespaces are not allowed in either field.
> - The **Username** field follows the format **<DOMAIN\Username>**.
>
> If any of the details (Domain, Username, or Password) are incorrect, an error message displays to help you resolve the issue.

8. On the Ready to Install the Program screen, click **Install**.
9. On the InstallShield Wizard Completed screen, click **Finish**.

Update the Data Source Location After Installation

The REST API does not include a Datasource Management Tool for updating data source connections, which are stored in the **datasources.dat** file. If you need to change the **datasources.dat** file location after installation, you must update it manually in the API's **web.config** file and ensure that it points to a valid **datasources.dat** file.

> **Attention:** For more information, see "Deltek PPM Datasource Management Tool" in the PPM Administrator Help System.

Locate the following entry in the **<appSettings>** section and update the value to the new path:

```
<add key="DATASOURCES" value=" C:\path\to\shared\datasources.dat" />
```

The value can be a relative path (relative to the REST API directory) or an absolute path. After you save the **web.config** file, IIS automatically updates the application.

> **Important:**
>
> - Changes to data source definitions must also be made directly in the **datasources.dat** file referenced in the **web.config** file.
> - The IIS application must be restarted whenever changes are made to the contents of the **datasources.dat** file.

Scope and Considerations

In environments where the REST API is deployed alongside other PPM products, each product accesses the **datasources.dat** file configured for its own deployment. These products may be installed on the same IIS server or on separate machines, depending on your deployment scenario.

You should determine whether to do one of the following:

- Maintain separate **datasources.dat** files per deployment, or
- Store a shared **datasources.dat** file in a centrally accessible location and reference it using an absolute path.

Configure the Log Level

You can control the level of detail of logs generated by the REST API by updating the **nlog.config** file in the REST API directory.

The following log levels are available:

- **Debug**: This level provides detailed diagnostic information for development and troubleshooting and is the default log level.
- **Info**: This level provides general informational messages about normal application operation.
- **Warn**: This level provides warnings about unexpected situations that do not interrupt normal operation.
- **Error**: This level indicates issues that prevent specific operations from completing successfully.
- **Fatal**: This level indicates critical failures that may cause the application to stop functioning.

To configure the log level:

1. Open the **nlog.config** file.
2. Locate the following entry in the **<rules>** section and replace **{log level}** with the desired log level.

   ```
   <logger name="*" writeTo="default" minlevel="{log level}" />
   ```

3. Save the file.

   The REST API automatically detects the change and applies the new log level. You do not need to restart IIS or recycle the application pool.

Testing the REST API Deployment

This section outlines the steps to verify that the REST API for your product is running correctly and that its endpoints are accessible.

Step 1: Start the REST API Application

1. Open IIS Manager.
2. In the Connections pane, click **Sites » Default Web Site » PPMRESTAPI**.
3. Select the child application alias.

> **Note:** This is the alias assigned to the PPM product (for example, **Cobra**).

4. In the Actions pane, click **Browse *:80 (http)**.

Step 2: Verify API Endpoints

Verify that the API endpoints are accessible by opening a web browser and navigating to the following URLs. For local access on the application server, use localhost; for remote access, use the server host name or IP address.

- http://<host>/PPMRESTAPI/<child application>/swagger-ui/
- http://<host>/PPMRESTAPI/<child application>/metadata

Example (for Cobra):

- http://localhost/PPMRESTAPI/cobra/swagger-ui/
- http://localhost/PPMRESTAPI/cobra/metadata

Expected Results

- The ServiceStack metadata page loads successfully.
- No HTTP 500 series errors are returned.

Step 3: Authenticate with the REST API

Before you can invoke the secured endpoints, you must first authenticate with the REST API.

You can authenticate using either of the following options:

- **Option 1**: Authenticate using the login page (Swagger user interface (UI) in a browser)
- **Option 2**: Authenticate using the /auth/credentials endpoint

Authenticate Using the Swagger UI

To run the REST API endpoints through Swagger UI in a web browser, use the built-in login page to authenticate.

To authenticate using the Swagger UI:

1. In a web browser, navigate to the following URL: **http://<host>/PPMRESTAPI/<PPM product>/login.html**.

   Example (for Cobra): http://localhost/PPMRESTAPI/cobra/login.html

2. Fill out the login form with your credentials and submit it.

Upon successful authentication, the REST API returns the session cookies, which the browser stores automatically. You can then run the GET endpoints in Swagger UI as an authenticated user.

Authenticate Using the /auth/credentials Endpoint

To run the REST API endpoints using a tool such as Postman, send a POST request to the **/auth/credentials** endpoint to authenticate.

To authenticate using the endpoint:

1. Send a POST request to the following URL: **http://<host>/PPMRESTAPI/<PPM product>/auth/credentials**.
2. Enter the following parameters in the request body:

```
username=<username>&password=<password>&datasource=<datasource>&productid=<productid>
```

When you use Postman, the authentication cookies returned by the response are retained automatically and applied to subsequent GET requests, allowing you to run the **GET** endpoints as an authenticated user.

Alternatively, to set the session explicitly, copy the session ID returned by the POST /auth/credentials response, then include it as the value of the ppm-session-id header in each subsequent request.

Deltek

Appendix A: If You Need Assistance

If you need assistance installing, implementing, or using the REST API, Deltek makes a wealth of information and expertise readily available to you.

Customer Services

Deltek has always maintained close relationships with client firms, helping with their problems, listening to their needs, and getting to know their individual business environments. A full range of customer services has grown out of this close contact, including the following:

- Extensive self-support options through the Deltek Support Center
- Phone and email support from Deltek Support Services analysts
- Technical services
- Consulting services
- Custom programming
- Classroom, on-site, and Web-based training

Attention: Find out more about these and other services from the Deltek Support Center.

Deltek Support Center

The Deltek Support Center is a support Web site for Deltek customers who purchase an Ongoing Support Plan (OSP).

The following are some of the many options that the Deltek Support Center provides:

- Search for product documentation, such as release notes, install guides, technical information, online help topics, and white papers
- Ask questions, exchange ideas, and share knowledge with other Deltek customers through the Deltek Support Center Community
- Access Cloud-specific documents and forums
- Download the latest versions of your Deltek products
- Search Deltek's knowledge base
- Submit a support case and check on its progress
- Transfer requested files to a Deltek Support Services analyst
- Subscribe to Deltek communications about your products and services
- Receive alerts of new Deltek releases and hot fixes

- Initiate a Chat to submit a question to a Deltek Support Services analyst online

> **Attention:** For more information regarding Deltek Support Center, refer to the online help available from the Web site.

Access Deltek Support Center

To access the Deltek Support Center:

1. Go to https://deltek.custhelp.com.
2. Enter your Deltek Support Center **Username** and **Password**.
3. Click **Login**.

> **Note:** If you forget your username or password, you can click the **Need Help?** button on the login screen for help.