Deltek
Speed. Clarity. Control.

Deltek PPM Administrator 1.0.0

Cumulative Update 02 Release Notes

February 2, 2026

Deltek

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 February 2026.

Deltek

Contents

Deltek

Overview

This PPM Administrator 1.0.0 Cumulative Update (CU) 02 release includes all the enhancements and software issues resolved were made in PPM Administrator 1.0.0 CU 01 through 02.

Software Requirements (Compatibility Matrix)

To see the list of the supported and compatible technologies, see “System Requirements” in the Deltek PPM Administrator 1.0 Installation Guide.

For a complete list of the recommended minimum software requirements, see the Deltek Product Support Compatibility Matrix document, which you can download from the Deltek Support Center site.

Deltek

PPM Administrator 1.0.0 Cumulative Update 02

Released: February 2, 2026

Enhancements

OAuth 2.0 Support for SMTP Email

You can now configure PPM Administrator to send email messages via SMTP using OAuth 2.0, replacing the old, less secure method of sharing and storing username and password. This update improves security with token-based authentication, enables enhanced permissions, supports multi-factor authentication, and ensures compatibility as providers end basic authentication.

OAuth Authentication for SMTP Email Settings

You can now configure OAuth authentication for your SMTP email settings, providing more secure email delivery options.

Updated Communication Email Tab

The Email tab on the **Communication** menu has been updated to support **Basic**, **OAuth**, and **Anonymous** authentication types.

Field	Description
OAuth Flow	The new **OAuth Flow** drop-down list lets you select how to authenticate with your email provider. Each option suits different security needs and service setups. ▪ **None** (traditional SMTP) ▪ **Authorization Code** ▪ **Authorization Code with PKCE** (Proof Key for Code Exchange) ▪ **Client Credentials** The tab adapts automatically based on your **OAuth Flow** selection. When you select **None**, you configure email using the familiar **Basic SMTP Settings** (SMTP Server, Port, Username, Password) section. When you select an option other than **None**, the **Basic SMTP Settings** become optional, and the new OAuth-specific sections **OAuth SMTP Settings** (for your email server details) and **Authentication Settings** (for your OAuth credentials) are required. This field defaults to **None**.

Deltek

Field	Description
Basic SMTP Settings	This group box contains settings that enable you to set up your default email server. ▪ **Default Sender Email:** Use this field to enter a valid host name or IP address of the SMTP (Simple Mail Transfer Protocol) server that will be used to send emails from PPM Administrator and other PPM products. This field allows up to **254** alphanumeric characters. ▪ **Display Name:** Use this field to enter the display name when sending email from the System Email address. This field allows up to **254** alphanumeric characters. ▪ **SMTP Server:** Use this field to enter a valid host name or IP address of the SMTP server that will be used to send emails from PPM Administrator and other PPM products. ▪ **Port:** Use this field to enter a port number for SMTP communication. Typically, you use port **25** for non-secure communication and port **587** for secure communication. This field accepts values from **0** to **65, 535**. ▪ **Use TLS:** Select this option to enable TLS encryption for your email communication. ▪ **Username:** Use this field to enter the username that will be used to access the email server. ▪ **Password:** Use this field to enter the password associated with the username used to access the email server. The **Username** and **Password** fields are optional. The **Password** field is required only if the **Username** field contains a value.
OAuth SMTP Settings	This group box enables you to set up your Open Authorization (OAuth) email server. ▪ **Default Sender Email:** When the application sends a user an email message, the message comes from this email address. The same email address receives an error message when the recipient's email address is invalid. ▪ **Display Name:** This field displays the name of the sender for outgoing emails.

Field	Description
	▪ **SMTP Server:** This field displays the host name or IP address of an SMTP-compliant email server, for example, smtp.yahoo.com. ▪ **Port:** This field displays the SMTP port that the specified SMTP server uses. ▪ **Use TLS:** Select this option to enable TLS encryption for your email communication. If you set **OAuth Flow** to **Authorization Code**, **Authorization Code with PKCE**, or **Client Credentials**, the fields are required.
Authentication Settings	This group box enables you to initiate the Open Authorization (OAuth) process from SMTP settings. ▪ **Client ID:** Use this field to specify the ID of the client for the OAuth server. This value will be hidden as you enter it. ▪ **Client Secret:** Use this field to specify the character string of the client secret manually obtained from the server. This value will be hidden as you enter it. ▪ **Authorization Endpoint:** Use this field to specify the endpoint where the user is redirected to grant permission. Enter a valid URL. This field allows up to **500** characters. ▪ **Token Endpoint:** Use this field to specify the endpoint used in the OAuth authorization process where a client application exchanges an authorization code for an access token. Enter a valid URL. This field allows up to **500** characters. ▪ **Redirect URI:** Use this field to specify the specific permissions an application can request from a user. Enter a valid string value or URL. This field allows up to **500** characters and is case-sensitive. ▪ **Scope:** Use this field to specify and limit the exact permissions or level of access that the client application is requesting from the user. Enter a valid string value or URL. This field allows up to **500** characters. All these fields are required. If you set **OAuth Flow** to **Client Credentials**, the **Authorization Endpoint** and **Redirect URI** fields become disabled.
OAuth Token Management	This group box contains options that allow you to manage your OAuth access token for secure email authentication. The access token enables the

Field	Description
	application to send emails on your behalf through your email provider without storing your password. ▪ **Get Auth Token:** Click this button to initiate the OAuth process and retrieve a new access token. While the form is being edited, this button is disabled. When you click **Save**, this button becomes enabled. When you click this button, the application helps you authenticate with your email provider and safely saves your access token. If you update your SMTP settings afterward, a warning message displays to let you know that updating will delete your current OAuth token, requiring you to get a new one. ▪ **Token Status: <Expired or Valid>**: This field displays the current state of your token. ▪ If the value is **Expired**, the displayed text is red. ▪ If the value is **Valid**, the text is green. ▪ **Token Expires: <Token expiration date and time>:** This field displays the validity period of your current token. The displayed value follows the date format set in My Preferences + Time.
Send Test Email	Click this button to send an email message to verify that the configured settings are accurate and that the application can successfully send email to the user account. Clicking this button sends the email to the currently logged in user's email address.

Attention: For more information, see the Communication Email Tab section in the *Deltek PPM Administrator Help*.

Ollama AI Service Provider Support

You can now configure Ollama connection settings in PPM Administrator.

While you can configure Ollama connections now, you cannot use Ollama functionality until your specific PPM product (such as Acumen, Cobra, or PM Compass) releases its Ollama feature support. Actual Ollama availability depends on each product's release schedule and capabilities.

Deltek

Attention: For further information regarding the availability of Ollama within your product, see the relevant product's release documentation.

Ollama is an open-source AI platform that lets you deploy large language models directly on your own servers or your private cloud. Unlike cloud-based AI services, Ollama keeps all your data within your organization— nothing is sent to external providers. You can choose from a variety of language models, including open-source options like Llama 3 and Mistral, proprietary models, or even custom-tuned models tailored to your specific business needs. This Bring Your Own Large Language Model (BYO LLM) approach gives you the flexibility to select the AI model that works best for your organization while maintaining complete control over privacy, security, and customization.

New fields are added to the AI Tab of the **System** menu form in PPM Administrator to support this latest update.

AI Tab on System Menu

The AI tab (under the **System** menu) has been updated to support integration with Ollama.

Field	Description
AI Service Provider	This drop-down list now includes options for both Azure OpenAI and Ollama It specifies the AI Service Provider to be used. You can select one of the following options: ▪ **None** ▪ **Azure OpenAI** ▪ **Ollama**
Endpoint URL	This field has been repositioned below **AI Service Provider**. Use this field to define the endpoint URL of the Azure OpenAI resource or Ollama resource. The value is case-sensitive and must be a valid URL with up to **900** characters.
API Key	This field has been repositioned below **Endpoint URL**. Use this field to specify the API key used to authenticate requests to Azure OpenAI. The value is case-sensitive and accepts up to **900** characters.
Deployment	This field indicates the name of the deployed AI model within Azure OpenAI. If this is enabled, you need to enter a value with **2**–**64** characters.

Field	Description
Model	Use this field to specify the name of the model deployed on the Ollama service. If this is enabled, you need to enter a value with 2–64 characters.
Maximum Concurrent Prompt Requests	Use this field to set the maximum number of concurrent client requests allowed. You can enter a value between **0** and **65,535**. By default, it is set to **0** (disables the concurrency limit and allows all requests to be sent simultaneously).
Custom HTTP Request Headers	Use this field to define custom HTTP headers to be included in client requests. The value is case-sensitive and specified as Key-Value pairs formatted in JSON text. ▪ For keys, enter keys that are valid HTTP headers based on RFC 7230 with at least **2** characters and a maximum of **900** characters. ▪ Values are optional. If a value is defined, enter values that are valid HTTP headers based on RFC 7230 with up to **4,096** characters. There is no limit on the number of rows on the grid. There is a limit of **16,384** characters to the entire HTTP headers. PPM Administrator stores the data in the AI_CUSTOM_REQUEST_HEADERS system preference.

Additionally, the **Azure OpenAI Authentication** header is no longer included.

Attention: For more information, see the System Settings AI Tab section in the *Deltek PPM Administrator Help*.

Software Issues Resolved

There are no software issues resolved in this release.

Database Changes

There are no database changes in this release.

Documentation Changes

This section includes details of sections changed in the printed documentation.

Deltek

Documentation Module	Description of Change
Deltek PPM Administrator 1.0 Help	Updated the following topics: ▪ Configure System Email Settings ▪ Communication Email Tab ▪ System AI Tab ▪ Users General Tab

Deltek

PPM Administrator 1.0.0 Cumulative Update 01

Released: October 29, 2025

Enhancements

Enable Authorized Control Countries Validation

The option label **Enable Control Country Validation** on the System Settings tab has been updated to **Enable Authorized Control Countries Validation** to ensure naming consistency across all PPM products.

SYSADMIN Control Country Assignment Restrictions

You can no longer assign control countries to the SYSADMIN user or group. PPM Administrator now disables the **Authorized Control Countries** field whenever you view or edit SYSADMIN in both the **Users Detail View** and **Users List View**. Similarly, the **Group Authorized Control Country** field is disabled for the SYSADMIN group in both the **Groups Detail View** and **Groups List View**. This ensures that system administrators always retain unrestricted access and prevents accidental permission limitations.

Disable Authentication Type and Default Windows Domain for Basic Authentication

Selecting **Basic** authentication on the System Authentication tab now automatically disables unrelated fields: the **Authentication Type** drop-down, **Group Membership**, and **Default Windows Domain**. This enhancement helps prevent confusion by ensuring you only see options relevant to your chosen mode.

Importantly, your previous selections are not lost. Any values entered in those fields before switching to **Basic** authentication are retained. This allows you to toggle between authentication modes—**Basic**, **Mixed**, or **Windows**—without having to enter your settings again. When you return to either **Mixed** or **Windows** authentication, the fields become enabled again and display your saved configurations, ready to use.

Password Expiration Policy

PPM Administrator verifies your password at each login. Once your password expires, you cannot access PPM Administrator until you update your password.

If your password is set to never expire (0), no update is required. However, if your password exceeds the number of days allowed by your organization's policy, you are prompted to change it on login.

When your password has expired, a notification dialog box displays. After you click **OK**, the Change Password dialog box displays, allowing you to update your password and regain access.

Cookie Consent

Deltek has enhanced cookie transparency in certain PPM products that use cookies, including wInsight Analytics. PPM Administrator, and Acumen Touchstone.

Deltek

PPM uses only necessary cookies to ensure proper operation of its products. These cookies support essential functionality like authentication, session management, and secure access. They are required for the service and therefore do not track or store personal data for marketing or analytics purposes. No tracking, advertising, or marketing cookies are used.

PPM Administrator now displays a message that certain cookies are necessary for proper function. When you first access PPM Administrator through a browser, a new Cookie Settings dialog box displays to explain that authentication cookies are stored temporarily and either deleted when the browser closes or retained for future sessions, depending on your browser settings. By clicking OK, you can proceed and use the PPM Administrator uninterrupted.

> **Note:** Cookie deletion and retention depend on how your browser is configured. If your browser is set to clear cookies when it closes, or if you switch to a different browser and access the PPM Administrator (via URL) for the first time, the Cookie Settings dialog box displays again.

Automatic Acumen Touchstone License Notifications

When you assign an Acumen Touchstone license to users using the **Licenses** form, they automatically receive an email with access details. PPM Administrator sends this notification whether a URL is set, but does not resend emails to existing users or notify when licenses are removed.

Software Issues Resolved

Database Configuration Wizard

Defect 2492909

Description: When you ran the Database Configuration Wizard on an Oracle database that contained two or more PPM products fully supporting PPM Administrator, an error occurred.

Customers Impacted: This defect affects PPM Administrator users using a shared Oracle database with multiple compatible products.

Workaround Before Fix:

Modify the query in the COPY_EPMSA_PREF_TO_SYSTEM_PREF procedure to include a WHERE clause with ROWNUM = 1 to ensure only one record is returned.

Defect 2493826

Description: When you ran the Database Configuration Wizard and selected the option to automatically run PPM database scripts, the admin console window briefly displayed your database username and password credentials. This issue occurred specifically when configuring a new data source where PPM Administrator had not yet been installed in the database.

In this release, the console window now remains hidden during script execution, ensuring your database credentials remain secure during PPM Administrator installation and configuration.

Customers Impacted: This defect affects PPM Administrator users using the Database Configuration Wizard.

Workaround Before Fix: None.

Defect 2516089

Description: When you ran the Database Configuration Wizard and it encountered an error, every subsequent run displayed the same error message—even when the wizard completed successfully.

Customers Impacted: This defect affects all PPM Administrator users using the Database Configuration Wizard.

Workaround Before Fix: Delete the errors.txt files under the sub-folders of C:\Program Files\Deltek\PPMAdministrator\Database\Scripts.

Additional Notes: Whenever the Database Configuration Wizard runs a script, it backs up and overwrites the errors.txt file.

Users

Defect 2478966

Description: When you saved a new user record without configuring the Communications settings properly, PPM Administrator would incorrectly display the message "Temporary password sent."

Customers Impacted: This defect affects PPM Administrator creating new users.

Workaround Before Fix: None.

Defect 2476451

Description: The **Assigned Users** count displayed on the **Groups List View** did not match the **Assigned Users** grid in the Assigned Users dialog box.

Customers Impacted: This defect affects PPM Administrator users assigning users to new or existing groups.

Workaround Before Fix: None,

Defect 2397391

Description: When you set the **Authentication Mode** on the System Authentication tab to **Windows** from **Basic** or **Mixed**, the **Set Password** button remained enabled on the **User Authentication** tab for users who had been set with basic authentication.

Customers Impacted: This defect affects PPM Administrator users creating new users.

Workaround Before Fix: None.

Defect 2423625

Description: When you tried to remove or unassign the SYSADMIN group from the Group tab while editing a user record that is not the SYSADMIN account, PPM Administrator displayed the message "SYSADMIN can't be deleted from the SYSADMIN user."

Customers Impacted: This defect affects PPM Administrator users unassigning the SYSADMIN group from user records.

Workaround Before Fix: None,

Defect 2432038

Description: On **Users List View**, if you edited a user record and saved it with either a duplicate or an invalid email address, PPM Administrator would not display an error message.

Customers Impacted: This defect affects PPM Administrator users saving user records with duplicate or invalid email addresses.

Workaround Before Fix: None.

Communication

Defect 2421468

Description: When you entered only whitespaces or left the **System Email Display Name** field blank and saved the record on the **Communication** form, PPM Administrator would allow it, even though it was a required field.

Customers Impacted: This defect affects PPM Administrator users updating the **System Email Display Name** field.

Workaround Before Fix: None.

Login

Defect 2473093

Description: When you logged in with an expired password, PPM Administrator displayed the dashboard first before showing the Change Password dialog box, instead of remaining on the Login page to display a warning message prior to prompting for a password change.

Customers Impacted: This defect affects PPM Administrator users logging in with expired passwords.

Workaround Before Fix: None.

Defect 2493831

Description: When you tried to log in to PPM Administrator using an invalid data source, it displayed an incorrect error message.

Customers Impacted: This defect affects PPM Administrator users logging in to an invalid data source.

Workaround Before Fix: None.

Installer

Defect 2429620

Description: When you tried to install DeltekPPMAdministrator1.0.0.1036.msi using a local account, an error message related to invalid user name and password displayed.

Customers Impacted: This defect affects PPM Administrator users using a local account to run an Internet Information Services (IIS) application pool.

Workaround Before Fix: Specify a domain account and manually change to local account after the installation is completed.

Database Changes

There are no database changes in this release.

Documentation Changes

This section includes details of sections changed in the printed documentation.

Documentation Module	Description of Change
Deltek PPM Administrator 1.0 Help	Added the following topic: ▪ Cookie Consent Updated the following topics:

Documentation Module	Description of Change
	▪ Groups General Tab ▪ Licenses ▪ System Settings Tab ▪ System Authentication Tab

Deltek

Appendix A: For Additional Information

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.