Deltek
Speed. Clarity. Control.

Deltek EPM Security Administrator 8.6

Cumulative Update 02 Release Notes

April 22, 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 April 2026.

Deltek

Contents

Deltek

Overview

This EPM Security Administrator 8.6 Cumulative Update (CU) 02 release includes all the enhancements and software issues resolved were made in EPM Security Administrator 8.6 CU 01 through 02.

Software Requirements (Compatibility Matrix)

To see the list of the supported and compatible technologies, see “System Requirements” in the Deltek EPM Security Administrator 8.6 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

EPM Security Administrator 8.6 Cumulative Update 02

Released: April 22, 2026

Enhancements

System-Level Authentication Now Defaults to Mixed After Upgrade

After you upgrade your PPM product to a version compatible with PPM Administrator, the system-level authentication now sets to **Mixed** by default. In addition, system-level authentication takes priority; user-level authentication is checked only when the system-level authentication mode is set to **Mixed**.

Temporary Password Functionality Now Aligns with Your Authentication Settings

The ability to send temporary passwords is now controlled by your system and user-level authentication configuration, ensuring password reset actions stay consistent with how your environment is set up.

If the **Basic Authentication** option is selected on Authentication tab of the User Details form, EPM SA sends temporary passwords to users.

- When the system-level authentication mode is set to **Basic**, the user-level authentication defaults to **Basic Authentication** and the **Windows Authentication** option is disabled.
- When the system-level authentication mode is set to **Mixed**, temporary passwords are still sent as long as the user-level authentication remains set to **Basic Authentication**.

> **Note:** These rules are enforced consistently across all related password functions, including **Forgot Password**, **Set Password**, license and user temporary password sending, and other password reset workflows.

Domain Field in System Settings Dialog Box Is Now Optional

The **Domain** field in the System Settings dialog box is now optional when configuring or updating user-level authentication settings, with no validation tied to authentication type.

- The **Domain** field is not required for any user-level authentication mode.
- Leaving **Domain** empty does not prevent saving settings.
- By default, the user-level **Domain** inherits its value from the system-level setting if specified.

Deltek

Removal of Windows Authentication Mode at System Level

The **Windows** option is no longer available as one of the authentication modes in the System Settings dialog box.

> **Note:** Users can still use Windows Authentication by setting the authentication mode in the System Settings dialog box to **Mixed** and selecting the **Windows Authentication** option on the Authentication tab of the **User Details** form.

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.

Documentation Module	Description of Change
Deltek EPM Security Administrator 8.6 Help	Updated the following topics: ▪ Enable Security ▪ Enable Windows Authentication ▪ Password Policies Dialog Box ▪ System Settings Dialog Box ▪ User Details Form: Authentication Tab

Deltek

EPM Security Administrator 8.6 Cumulative Update 01

Released: February 3, 2026

Enhancements

OAuth 2.0 Support for SMTP Email

You can now configure EPM SA 8.6 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 Email Configuration Dialog Box

The Email Configuration dialog box (**System » Communication**) now supports **Basic**, **OAuth**, and **Anonymous** authentication types.

Field	Description
OAuth Flow	The new **OAuth Flow** drop-down 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 dialog box 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 EPM SA 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 EPM SA 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 to 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 Email Configuration Dialog Box section in the *Deltek EPM Security Administrator Help*.

Ollama AI Service Provider Support

You can now configure Ollama connection settings in EPM SA 8.6.

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.

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 dropdown 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 accepts 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.
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.

Field	Description
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.

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.

Documentation Module	Description of Change
Deltek EPM Security Administrator 8.6 Help	Updated the following topics: ▪ System AI Tab ▪ Email Configuration Dialog Box

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.