

# EyeDash Integration Agent Installation Guide

Applicable for EyeDash Pro, Pro+ & Enterprise Versions

This Guide is Intended for  
Milestone XProtect Integration



For further information or support please visit [datawaresys.com](https://datawaresys.com)  
or contact us on [support@datawaresys.com](mailto:support@datawaresys.com)

Agent Overview .....	3
Prerequisites.....	3
Authentication Options.....	4
1. Basic User .....	4
Step 1 : .....	4
2. Windows User .....	5
Step 1: .....	5
3. Default Windows User .....	5
User Creation and Permission Setup in Milestone XProtect .....	7
A. For Basic Users.....	7
1. Create Basic User.....	7
2. Assign to Administrator Role .....	8
3. Save and Confirm.....	8
B. For Windows Users.....	8
Using the User During Agent Installation .....	11
Agent Application Status.....	12
1. Stopped .....	12
2. Running.....	12
Troubleshooting Notes.....	13
Security Recommendations .....	13
Establishing Connection Between Agent and EyeDash .....	13
1. Configure VMS in EyeDash.....	13
2. Verify EyeDash System Status.....	14
3. Configure API URL in Agent Settings.....	14
4. Restart the Agent Application .....	14

# Agent Overview

This guide explains how to install and set up the EyeDash Integration Agent (EIA). Install the EIA on each Milestone XProtect Management Server to integrate with the EyeDash platform. The EIA gathers necessary data for EyeDash's full functionality and securely transmits it.

Proper network connectivity and security settings are crucial for a reliable and secure connection between the Integration Agent and the EyeDash platform. The Agent needs a dedicated Milestone XProtect user account with specific permissions to function correctly.

## Prerequisites

Before installing and running the Agent application, ensure the following:

- Milestone XProtect products and access to the XProtect Management Server
- Windows administrator to install the Agent on the machine
- Network traffic is allowed between 80 (default) and EyeDash. Network port can be customized.
- Access to Milestone XProtect Management Client with administrative privileges
- Basic understanding of Milestone XProtect roles and permissions
- Installer for the EyeDash Integration Agent (EIA)

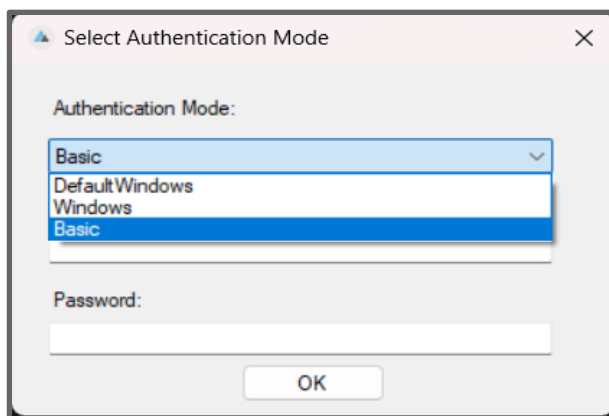
# Authentication Options

Upon launching the Agent application, a dropdown menu will be displayed allowing the user to select one of the following authentication methods:

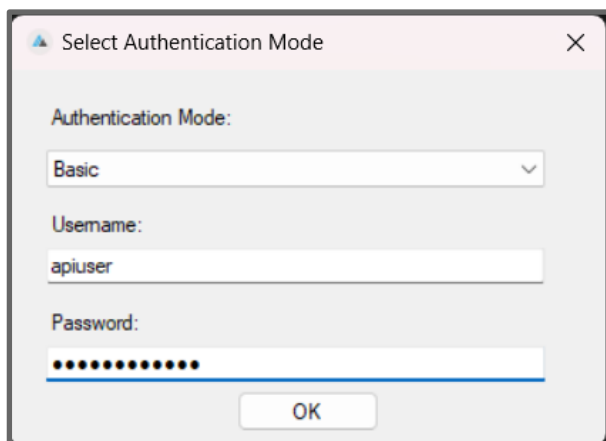
## 1. Basic User

- This refers to a user created within the Milestone XProtect Management Client.
- The application will prompt the username and password created specifically for integration.

### Step 1:



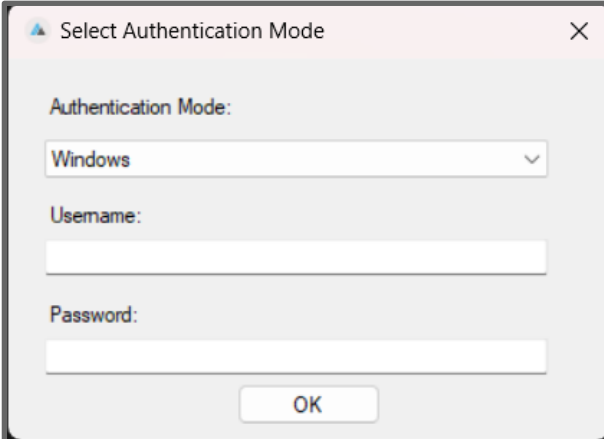
### Step 2 :



## 2. Windows User

- The user will be prompted to enter a valid Windows username and password.
- This allows integration using Windows Authentication.

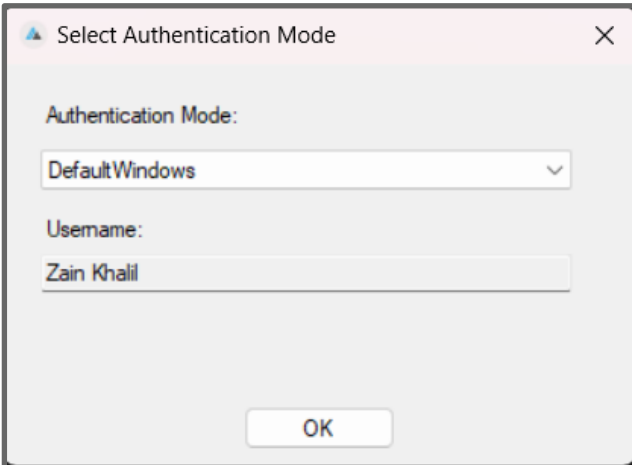
Step 1:



The screenshot shows a dialog box titled "Select Authentication Mode" with a close button (X) in the top right corner. Inside the dialog, there is a label "Authentication Mode:" followed by a dropdown menu currently showing "Windows". Below this, there is a label "Username:" followed by an empty text input field. Underneath the username field is a label "Password:" followed by another empty text input field. At the bottom center of the dialog is an "OK" button.

## 3. Default Windows User

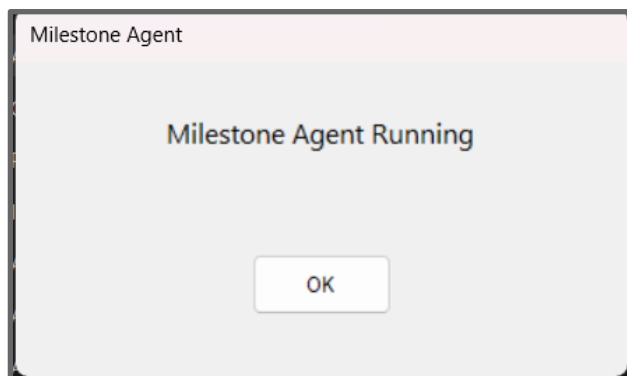
- No additional input is required.
- The currently logged-in Windows user will be used to run the Agent.



The screenshot shows the same "Select Authentication Mode" dialog box. The "Authentication Mode" dropdown now shows "DefaultWindows". The "Username" field is no longer empty; it contains the text "Zain Khalil". The "Password" field is not visible in this view. The "OK" button remains at the bottom center.

Once the appropriate authentication method is selected and the credentials are validated, a confirmation popup will display:

"Milestone XProtect Agent running."



At this point, the user can locate the Agent icon in the system tray. The icon initially displays a red dot, indicating the Agent is not yet active.

By right clicking the EIA system tray icon, the following options will be available:

- Show (Display the Agent UI)
- Hide (Hide UI)
- Start HTTP Listener (Listen to EyeDash incoming request via HTTP)
- Stop HTTP Listener (Stops to EyeDash incoming request via HTTP)
- Show Status (Show the current status of EIA)
- Show Live Logs (Show live logs/events)
- Settings (Settings and configuration)
- Exit (Ends the process and exit EIA)

Click "Start HTTP Listener" to begin the Agent service.

The icon's dot will turn green, indicating that the Agent is now up and running.

# Agent Application Status

The EyeDash Integration Agent provides visual indicators of its current status via its icon in the Windows system tray. There are two possible states:

## 1. Stopped

- Indicator: A red dot appears over the Agent application icon in the system tray.
- Meaning: The Agent is installed but not actively running. HTTP listener and data transmission are inactive.
- Action Required: Right-click the icon and select “Start HTTP Listener” to initiate the Agent.



## 2. Running

- Indicator: A green dot appears over the Agent application icon.
- Meaning: The Agent is fully operational, and the HTTP listener is active.
- Confirmation: After the Agent starts, logs and live status can be accessed via the system tray options.



These visual cues allow users to quickly determine the operational state of the Agent without opening the full interface.

# User Creation and Permission Setup in Milestone XProtect

Important: Whether you're using Basic or Windows authentication, the user must be assigned the correct roles and permissions at the time of creation. Changing permissions afterward does not guarantee proper functionality.

It is preferable that the user used for Agent and EyeDash API be assigned in the Administration group in Milestone XProtect due to some limitations from Milestone XProtect MIP SDK and API.

You can create either a Windows Authentication (local), Active Directory service account or Basic user.

e.g. for user naming eyedash or yourdomain\eyedash

Make sure the basic account is not blocked in Milestone XProtect, password is not expired. For assistance to creation of Windows Authentication, refer to your System Administrator and make sure that the account is not locked out and assigned inside Milestone XProtect administrators.

## Using the User During Agent Installation

During the agent setup:

- Select authentication type from dropdown
- Enter credentials as required and Explained in above steps.
- Upon successful validation, the agent will confirm it is running.

## Troubleshooting Notes

- If the Agent cannot fetch logs, re-check that read log permissions were granted during user creation
- Re-adding permissions later will not resolve the issue; recreate the user with all required permissions from the start



# Security Recommendations

- Use a dedicated user for Agent operations
- Avoid sharing credentials across applications
- Set strong, rotating passwords
- Periodically audit user access in the Milestone XProtect Management Client

## Establishing Connection Between Agent and EyeDash

To establish a successful connection between the EyeDash Integration Agent and the EyeDash application, follow these steps:

### 1. Configure VMS in EyeDash

- Open the EyeDash application and navigate to the VMS Integration section.
- Add a new VMS entry using the IP address of the server where the Agent application is installed.
- Fill in the required fields as described in the EyeDash Installation Guide.
- Once the VMS is added successfully, proceed to verify system behavior.

### 2. Verify EyeDash System Status

- Navigate to key screens such as System Status and Dashboard within the EyeDash application.
- Confirm that data is flowing correctly and the integration is functioning as expected.

### 3. Configure API URL in Agent Settings

- Go to the system tray and right-click the Agent application icon.
- Select Settings from the context menu.
- In the settings window, locate the field labeled API URL.

Enter the full API endpoint of your EyeDash application. The format should be:

**API URL:**

<https://<eyeDash-server-ip>/api/status>

- Replace [<eyeDash-server-ip>](#) with the actual IP address or hostname of the server where EyeDash is running.
- Click Save after entering the correct URL.

## 4. Restart the Agent Application

- To finalize the configuration, exit the Agent application.
- Restart the Agent and re-enable the HTTP Listener as previously described.
- Once the Agent is running and the green dot appears on the icon, the integration is complete.

For Any support required, please contact your account manager or reach to support directly on [support@datawaresys.com](mailto:support@datawaresys.com)