EPM and Beyond Identity

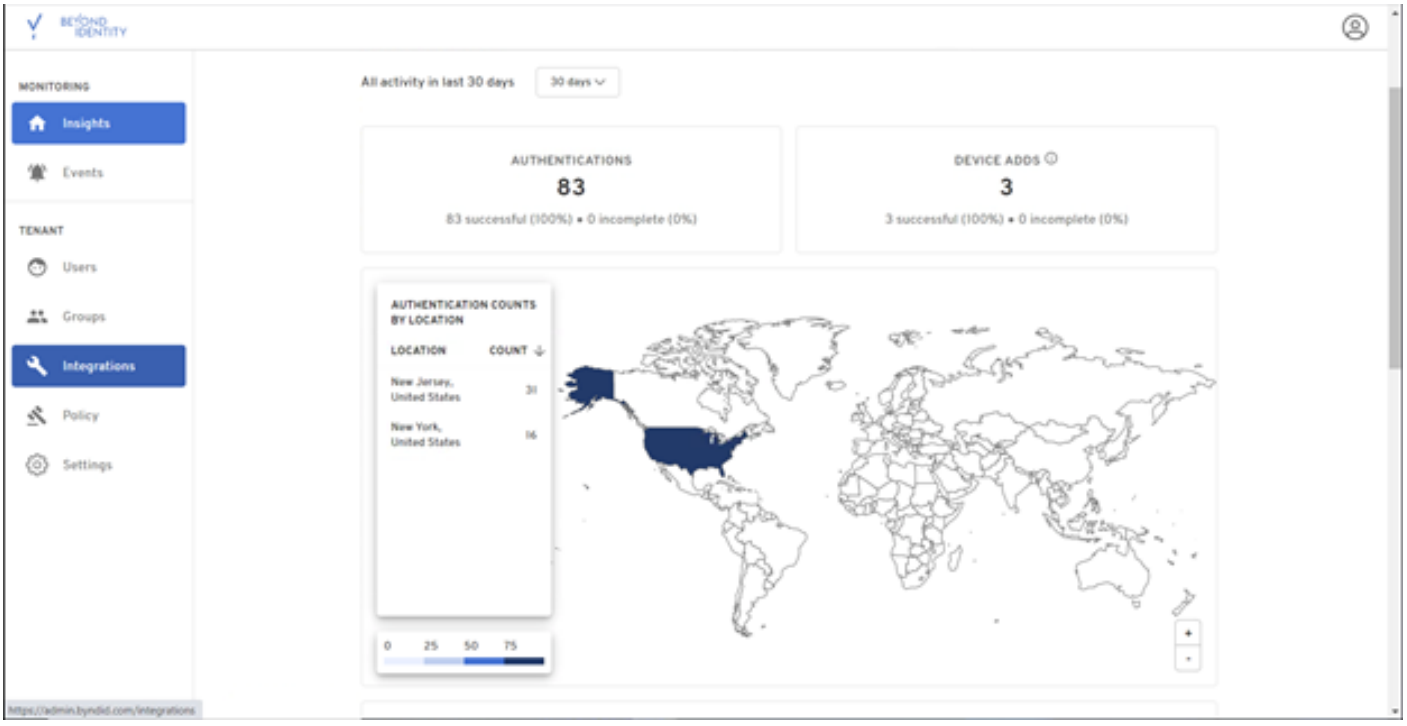
This guide provides details on configuring the OIDC identity provider Beyond Identity with EPM.

Overview

The key benefits of an EPM and Beyond Identity integration:

- Implement strong, unphishable, multifactor authentication (MFA) and policy-based access controls to ensure high-trust authentication for end user elevation requests.
- Ensure only devices that meet the company's security policy have access to application or process elevation.
- Establish identity before privileged actions on an endpoint are allowed, using a frictionless step-up authentication.
- Create a zero-trust PAM architecture, which doesn't trust the user until they pass a high-assurance authentication and doesn't trust their device unless it meets security policies.
- Eliminate one-time passwords and the corresponding vulnerabilities associated with elevation requests and approvals.

Beyond Identity can validate a device's security posture before allowing access to EPM.

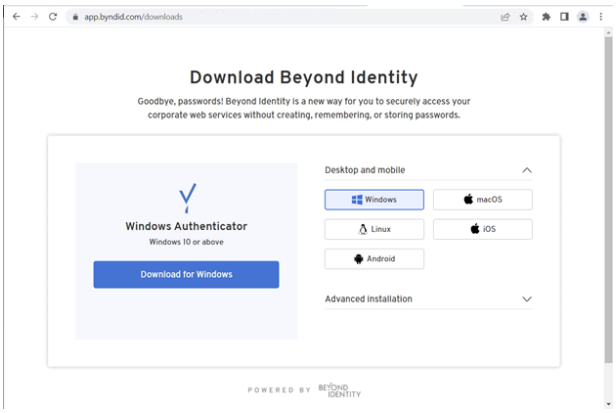


Download and Configure Beyond Identity App on Your Device

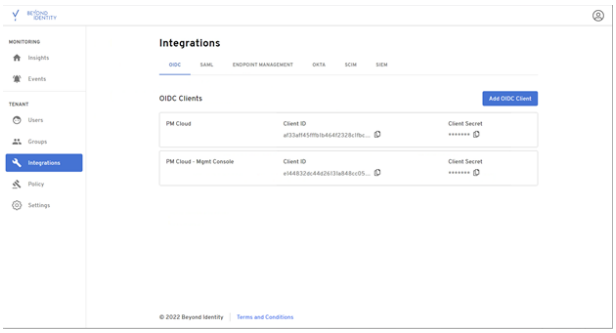
An instance of Beyond Identity is required to configure the app.

1. Download and configure the Beyond Identity app.

   Now you can use the Beyond Identity app to authenticate to your instance of Beyond Identity.



2. Click **Integrations** to add EPM as an OIDC client.

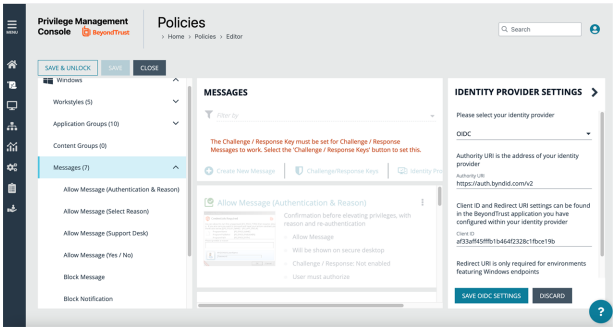


For more information, visit Download Beyond Identity at https://app.byndid.com/downloads.

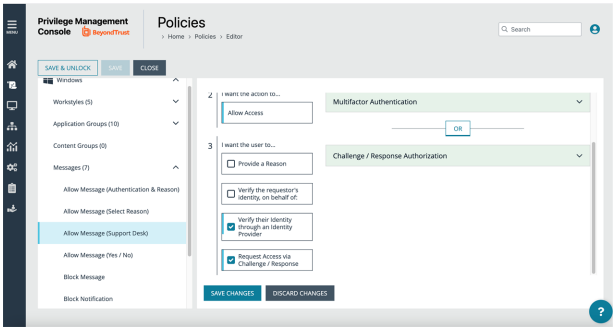
Configure Your EPM Instance

You also need to access your EPM instance.

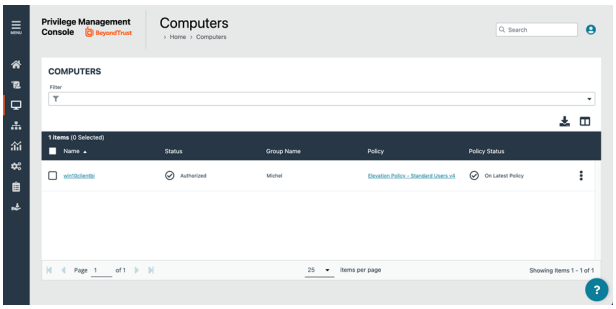
1. In EPM, open the Policy Editor.
2. Edit a policy and configure Identity Provider (IdP) Authentication.
3. Provide the **Authority URI**, **Client ID** generated earlier, and **Redirect URI**.



4. In the EPM Policy Editor, configure the message(s) that will use IdP settings.



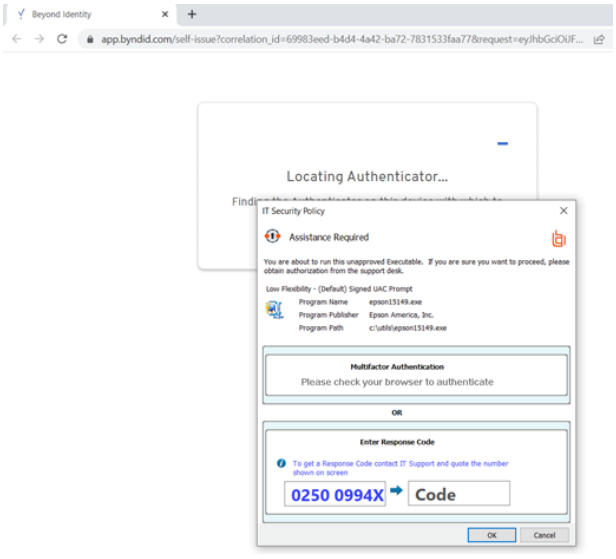
5. Validate that your test endpoint is on the latest policy. In EPM, go to the **Computers** page and check the policy status on the endpoint.



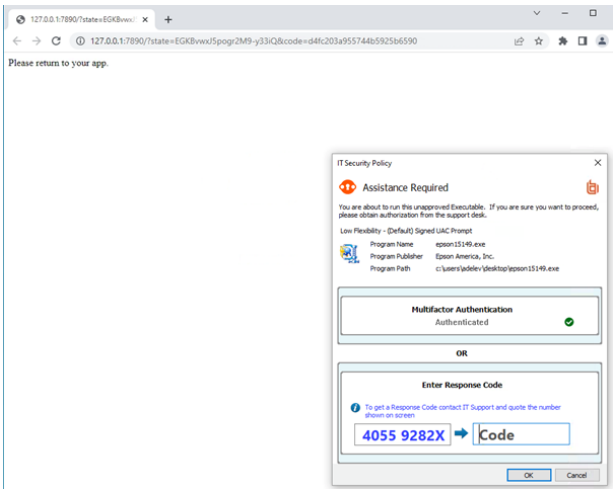
Test the Configuration

1. With a non-admin user account on the managed computer, try to run an installer that requires administrator credentials via the Windows User Account Control message.The attempt is blocked and you are presented with a configurable BeyondTrust message.

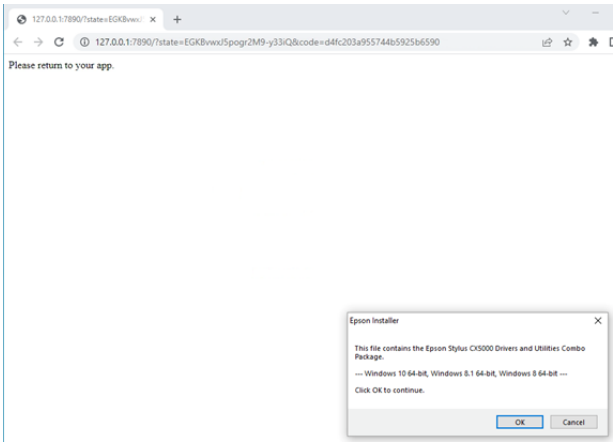
   By selecting **Multifactor Authentication**, instead of one-time Response Code, the user is authorized to elevate the installer.



2. Authentication is redirected to the browser. If Beyond Identity can find the proper credentials on the computer for the end user and validate endpoint rules, the user is authenticated.



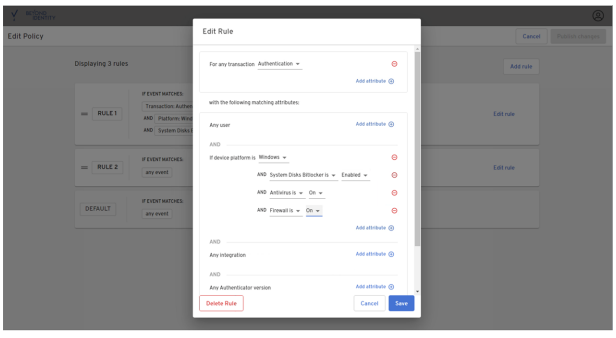
3. The installer is elevated for the end user without granting permissions to the end user directly.



Beyond Identity Policy and Rules

Beyond Identity policy and rules can be configured to validate that the end user endpoint or computer meets security corporate policies and standards.

> *For more information about the Beyond Identity policy and rules, see Risk Policies and Step-Up Authentication at https://www.beyondidentity.com/resources/risk-policies-and-step-authentication.*



Send feedback or questions to integrations@beyondtrust.com