Privileged Behavior Analytics

Administrator Guide

Version: 2023

Publication Date: 12/11/2024

Privileged Behavior Analytics Administrator Guide

Version: 2023, Publication Date: 12/11/2024

Warranty Disclaimer

DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, MAKE NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION CONTAINED IN THE DOCUMENTS AND RELATED GRAPHICS, THE SOFTWARE AND SERVICES, AND OTHER MATERIAL PUBLISHED ON OR ACCESSIBLE THROUGH THIS SITE FOR ANY PURPOSE. ALL SUCH MATERIAL IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH REGARD TO SUCH MATERIAL, INCLUDING ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT.

THE MATERIAL PUBLISHED ON THIS SITE COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN. DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE MATERIAL DESCRIBED HEREIN AT ANY TIME.

Disclaimer of Liability

IN NO EVENT SHALL DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, BE LIABLE FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, PROFITS OR OTHER ECONOMIC ADVANTAGE) OR ANY DAMAGES WHATSOEVER, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE, OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF SOFTWARE, DOCUMENTS, PROVISION OF OR FAILURE TO PROVIDE SERVICES, OR MATERIAL AVAILABLE FROM THIS SITE.

Table of Contents

Welcome to Privileged Behavior Analytics Technical Assistance

See the "Overview" below for a quick product orientation.

"Getting Started" on page 5 explains the setup steps required for PBA to work with your Secret Server.

"PBA Applications for Secret Server" on page 24 describes how to use PBA for Secret Server applications, while "PBA Responsive Actions" on page 98 explains how PBA automates your organization’s response when user behavior varies from normal.

"PBA Applications for Privilege Manager" on page 56 describes how to use PBA for Privilege Manager applications

Support Resources connects you to available product support.

"Release Notes" on page 110 provides the most recent Privileged Behavior Analytics Release Notes.

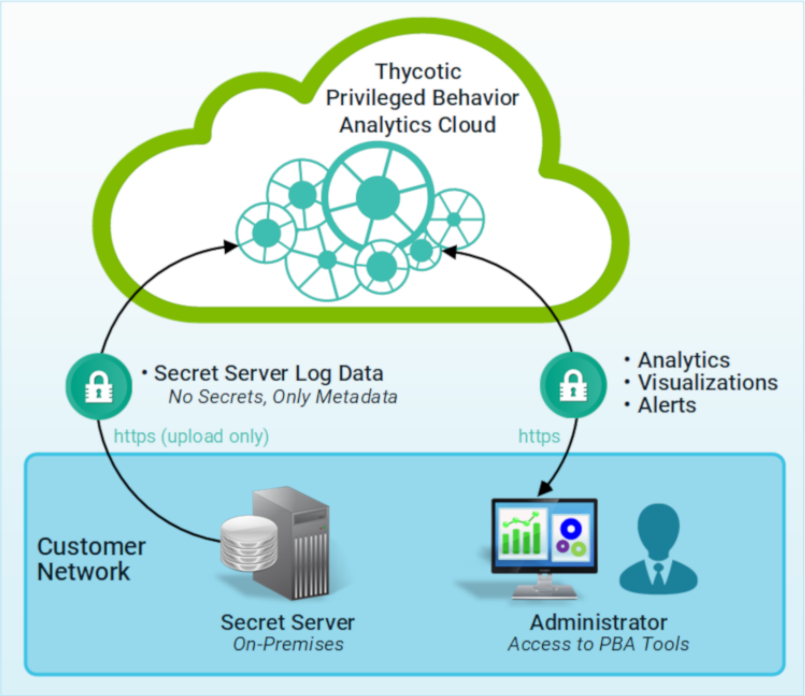
Overview

Privileged Behavior Analytics works with your Secret Server to improve the security of your enterprise systems by helping to **visualize**, **detect**, **interrupt**, and **announce** threatening activity and behavior across your IT infrastructure.

- **visualize**: by applying algorithms to Secret Server log files, PBA visualizes data relationships to help your staff recognize and respond to security threats
- **detect**: PBA learns patterns of activity–‘behaviors’–associated with security threats and continuously monitors for such threat indicators
- **interrupt**: by mounting **Access Challenges** of several types, PBA automatically interrupts concerning behaviors
- **announce**: as it detects possible threats, PBA uses several contact methods to notify appropriate staff

Architecture

Privileged Behavior Analytics uses the Amazon AWS Cloud and advanced algorithms to provide its features.



As in the illustration:

- Your Secret Server uploads activity logs to PBA in the Cloud (AWS).
- PBA applies advanced algorithms to the data to deliver alerts, analytics, and visualizations.
- To access these, your administrative staff use a browser to authenticate with PBA.

Secret Categories

Privileged Behavior Analytics categorizes secrets into the following categories:

- Ignore
- Low
- Standard
- High
- Critical

The difference between these categories is the secret importance setting, which is a numerical value, assigned to the secret as its importance value. All secret importance values start out at 2, which is Standard importance. The table below shows the corresponding numerical values for each of the above categories:

Category	Corresponding Importance Value
Ignore	0

Category	Corresponding Importance Value
Low	1
Standard	2
High	3
Critical	4

All possible Alerts are *Warning* or *Critical*, per User. Those are detailed on the Settings / System Settings / Responsive Actions page in the PBA UI.

Secret Server Metadata and PBA Data Security

Delinea Secret Server secures access to your company's most important resources. Privileged Behavior Analytics further secures those resources by generating insights about how your privileged users access the most protected resources. Given training against a suitable data set, PBA will alert you when a privileged user is behaving atypically, which could signal an intruder or an inside malefactor.

PBA also secures those resources by adhering to stringent standards for data security.

PBA Resides in the Cloud

As a Cloud service, Privileged Behavior Analytics is easily accessed and highly secure.

Secret Server Uploads Only Metadata

Once configured to work with PBA, your Secret Server securely uploads data to your organization's tenancy with the PBA service. PBA uses the event log data generated by Secret Server, so that only **metadata**–data about your data, not your data itself–go to the Cloud for analysis by PBA.

This means that no actual Secret fields, such as passwords, private keys, notes, or other first-order data ever leaves your Secret Server. Instead, only data **about** these things–literal **metadata**–upload to PBA.

- For example, for a Secret that is a Windows account, fields uploaded for analysis by PBA in the Cloud would include the Secret Name, Secret Template, Secret Folder, Secret Policy ID, and Permissions.
  - These are fields about the Secret, but not about the Windows account it contains.
- Fields like Machine, Username, Password, Notes, Site, or any attached files, extra fields, or Secret keys do not upload, as these comprise the actual content of the Secret.

PBA Users Log In to the PBA Cloud Service

Your organization's designated users securely log in to the PBA service to use its analytics tools and configure alerts. PBA continuously processes the log data and applies analytics to deliver insights and alert on anomalous behavior.

Data Protections and Security Applied Throughout

The design and build of Privileged Behavior Analytics maintains at all times the security of your Secret Server.

Security Provisions Apply to Data Uploads

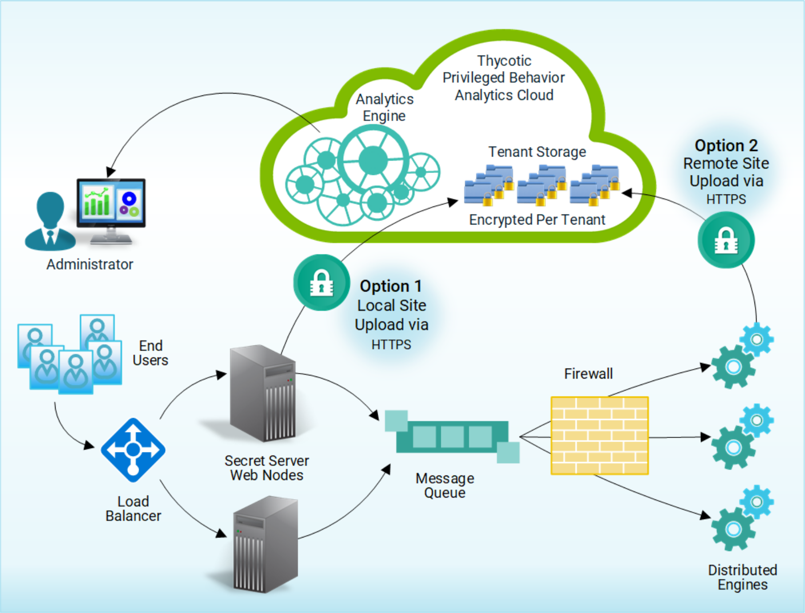
Significant protection applies to data uploads by Secret Server to Privileged Behavior Analytics.

- Data sent to the cloud is via a one-way upload that can only be initiated by Secret Server.
- The data upload mechanism provides no means for remote access into your Secret Server.
- In addition, the data uploads to a Cloud location to which only your organization's Secret Server can write.
- PBA encrypts your organization's uploaded data with a key unique to your PBA tenancy.

Alternative Data Upload via Distributed Engine Architecture

If your organization disallows outbound connections from Secret Server's network segment, you can instead upload using Delinea's Distributed Engine architecture.

- Option 1 in the illustration shows the default manner of upload by the Secret Server web node in the local site.
- Option 2 shows a remote site upload using a Distributed Engine.



Security Provisions Apply to Connections to the Cloud

To secure your data end-to-end, all connections to PBA are encrypted with industry-standard Transport Layer Security (TLS) encryption. This includes all data uploads to the Cloud and all use of PBA.

Built on Amazon Web Services

PBA relies on the best-in-class security provided by Amazon Web Services. You can find out more about the underlying security of AWS at:

- https://aws.amazon.com/security/

Strict Access Control and Tenant Isolation

PBA features tenant isolation and exacting internal access controls that provide multiple safeguards against unauthorized access to any organization’s data.

- PBA isolates each organization’s data from that of other organizations.
- Strong access controls give each PBA operational component only the rights required to perform its role.

These layers of defense ensure that even were unauthorized parties to gain access to a part of the PBA Cloud, their access would be isolated to that tenant and to the abilities of the compromised component.

Proactive Monitoring

Delinea continuously applies proactive monitoring protocols to the PBA service.

- Administrators will receive alerts on any indication that someone *might* be trying to gain unauthorized access.
- Atypical behavior patterns among Delinea’s own administrative staff would likewise be flagged for review to guard against the emergence of inside malefactors.

Encryption at Rest

PBA encrypts data at rest in the cloud. This additional layer of protection safeguards information in PBA even should an unimaginable series of events somehow leave such data exposed.

Getting Started

To get started using Privileged Behavior Analytics:

1. Make sure you have the "Requirements" on the next page Secret Server version.
2. "Secret Server Configuration" on the next page.
3. "Privileged Behavior Analytics Configuration" on page 16
4. Set up "Single Sign-On (Version 10.4 and Later, Cloud)" on page 18
5. Set up "Access Challenges" on page 19

Privileged Behavior Analytics resides on the Amazon AWS platform as a Cloud application. To use PBA requires no hardware installation and no COTS installation on your premises.

However, it does require that you configure Secret Server to send metadata to Privileged Behavior Analytics, and this process is version-dependent.

This articles in this section detail the required setup.

Requirements

Requirements include:

- Secret Server v10.2 or higher *or* Secret Server Cloud
- Secret Server Professional Edition or higher
- Receipt of an email with your Privileged Behavior Analytics account login information
  - Provided you have purchased or been approved for a trial of Privileged Behavior Analytics
  - Single Sign On requiresSecret Server v10.4 or higher

Secret Server Configuration

Steps to configure Secret Server with PBA:

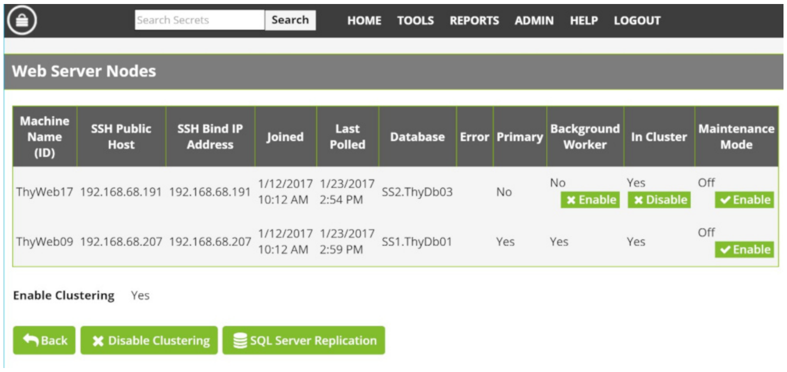
1. Setup the "Data Uploader Setup Steps" on the next page. The Data Uploader provides data from Secret Server to PBA and is version-dependent.
2. Configure PBA for "Proxied Environments" on page 12 if your Secret Server has outbound access through a proxy.

   Secret Server provides data to Privileged Behavior Analytics through the **Data Uploader**, which requires version-dependent configuration.
3. Import "Historical Data Import" on page 10 for PBA to analyze.
4. Set up the "Background Worker (Clustered Environments)" below for clustered environments.

Background Worker (Clustered Environments)

After enabling PBA, navigate to **AdminClustering.aspx** and ensure that at least one of your web nodes has the **Background Worker** column enabled, as below.

- In Secret Server versions prior to 10.1.000000, all nodes process web requests, but only the Primary Node runs background tasks.
- In 10.1.000000 and later, the Background Worker feature allows you to specify the Secret Server nodes that run background tasks.



Web Server Nodes

Machine Name (ID)	SSH Public Host	SSH Bind IP Address	Joined	Last Polled	Database	Error	Primary	Background Worker	In Cluster	Maintenance Mode
ThyWeb17	192.168.68.191	192.168.68.191	1/12/2017 10:12 AM	1/23/2017 2:54 PM	SS2.ThyDb03		No	No ✖ Enable	Yes ✖ Disable	Off ✔ Enable
ThyWeb09	192.168.68.207	192.168.68.207	1/12/2017 10:12 AM	1/23/2017 2:59 PM	SS1.ThyDb01		Yes	Yes	Yes	Off ✔ Enable

Enable Clustering Yes

Data Uploader Setup Steps

Privileged Behavior Analytics (PBA) processes event data from Secret Server using a data upload.

Integrating Secret Server and PBA requires an **Integration Key**. This key:

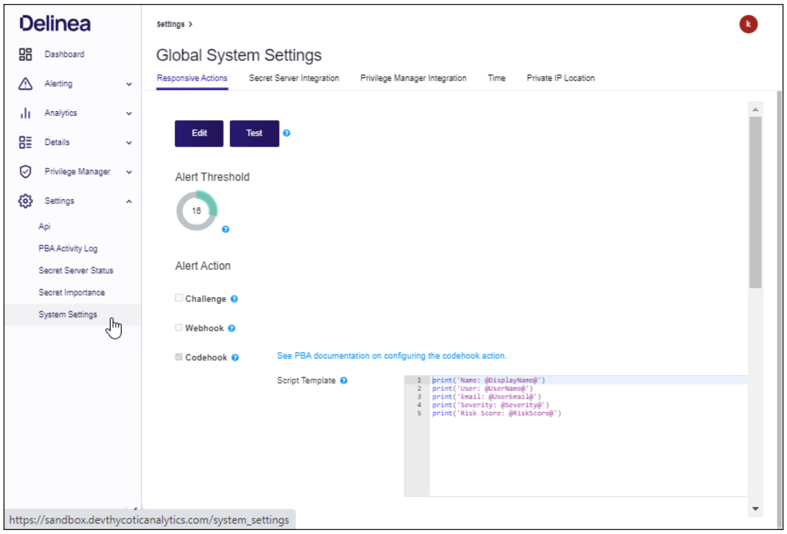
- contains the secret access key and other parameters for uploading data to Delinea PBA.
- is encrypted for protection in transit.
- is encrypted and saved when entered into Secret Server using standard Secret Server encryption (AES-256 and DPAPI/HSM if configured).
- can never be loaded again through the UI, but can be updated if the linked PBA account needs to be changed.

Version 10.4 and Later, and Cloud

For Secret Server Installed Version 10.4 and for Secret Server Cloud, event data is uploaded to PBA via queues and micro-loading, and is closer to real-time. Prior versions of Secret Server data upload followed the more typical data warehouse design of file upload and small batch-loading.

Use these steps to obtain the Integration Key from PBA that will be used by Secret Server to authenticate and upload data to PBA:

1. Log into your PBA instance and select **Settings** in the left navigation panel, then select **System Settings**.



Global System Settings

Alert Threshold

16

Alert Action

□ Challenge

□ Webhook

☑ Codehook

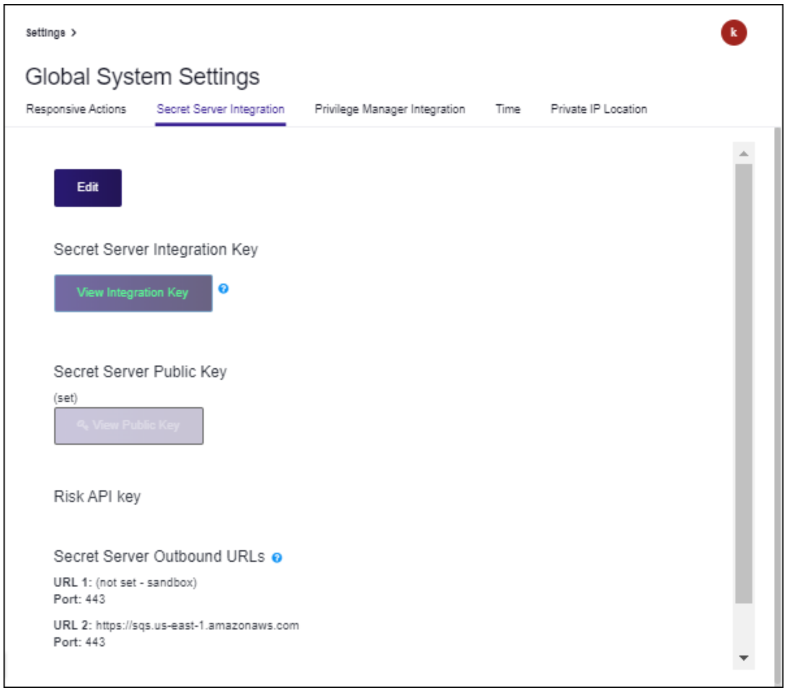
See PBA documentation on configuring the codehook action.

Script Template

```
print('Name: @DisplayName@')
print('User: @UserName@')
print('Email: @UserEmail@')
print('Severity: @Severity@')
print('Risk Score: @RiskScore@')
```

https://sandbox.devthycoticanalytics.com/system_settings

2. From the Global System Settings page, select the **Secret Server Integration** tab.



Settings >

Global System Settings

Secret Server Integration Key

Secret Server Public Key

(set)

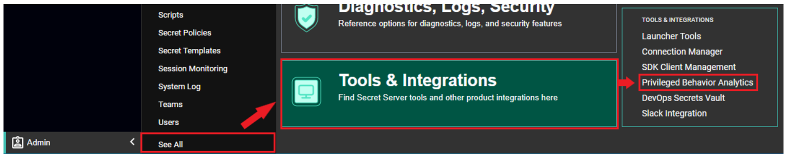
Risk API key

Secret Server Outbound URLs

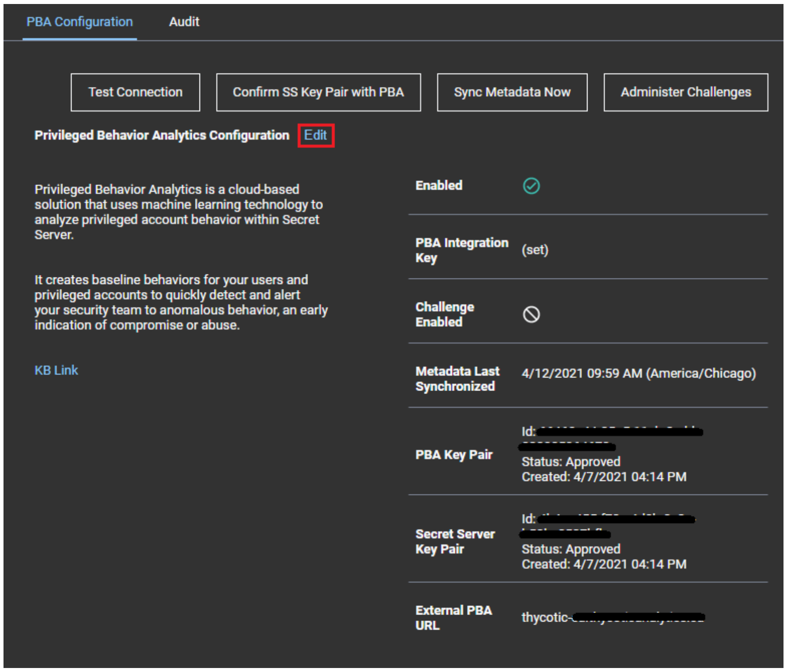
URL 1: (not set - sandbox)
Port: 443

URL 2: https://sqs.us-east-1.amazonaws.com
Port: 443

3. Click **View Integration Key**. If you are prompted to specify whether Secret Server is on version 10.4.000000, click *Yes.*
4. Copy the **Integration Key Value**.
5. Open Secret Server and navigate to **Admin > See All > Tools & Integrations > Privileged Behavior Analytics**.



6. On the PBA Configuration page, click **Edit**.



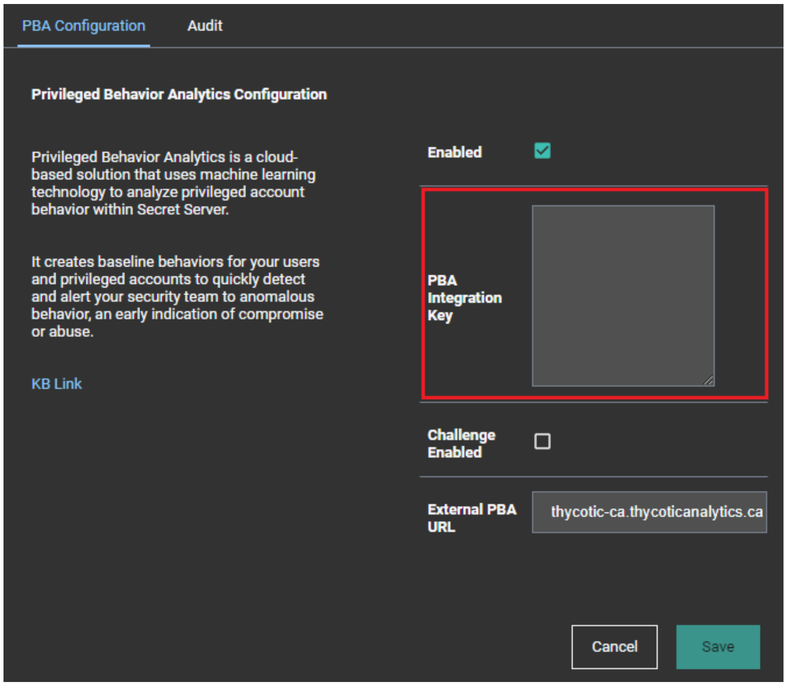
Privileged Behavior Analytics Configuration

Privileged Behavior Analytics is a cloud-based solution that uses machine learning technology to analyze privileged account behavior within Secret Server.

It creates baseline behaviors for your users and privileged accounts to quickly detect and alert your security team to anomalous behavior, an early indication of compromise or abuse.

Enabled	✓
PBA Integration Key	(set)
Challenge Enabled	⃠
Metadata Last Synchronized	4/12/2021 09:59 AM (America/Chicago)
PBA Key Pair	Id: [redacted] Status: Approved Created: 4/7/2021 04:14 PM
Secret Server Key Pair	Id: [redacted] Status: Approved Created: 4/7/2021 04:14 PM
External PBA URL	thycotic-[redacted]

7. Check **Enabled** to enable Privileged Behavior Analytics.
8. Paste the **PBA Integration Key** that you copied in step 4.



Privileged Behavior Analytics Configuration

Privileged Behavior Analytics is a cloud-based solution that uses machine learning technology to analyze privileged account behavior within Secret Server.

It creates baseline behaviors for your users and privileged accounts to quickly detect and alert your security team to anomalous behavior, an early indication of compromise or abuse.

Enabled	☑
PBA Integration Key	
Challenge Enabled	□
External PBA URL	thycotic-ca.thycoticanalytics.ca

9. Check **Challenge Enabled** to enable Secret Server Access Challenges. See the "Access Challenges" on page 19 article for further information.

10. Input the **External PBA URL**. This is the URL of your Privileged Behavior Analytics cloud instance. **It is set automatically by the integration key but may be overridden.** It is used for Single Sign On, redirecting to PBA from the Tools menu, and on the **Access Challenges** page to create links to the PBA events that spawned Access Challenges.
11. Set the **Metadata Interval (Installed Only)**. The frequency that metadata is uploaded to PBA.
    - The recommended interval is at least 60 minutes.
    - The minimum interval is 5 minutes.
    - Metadata frequency should vary based on how often new Users and Secrets are added in Secret Server; typically it should not need to be less than 60 minutes.
    - For Cloud, this setting is unavailable and defaults to 60 minutes.
12. Click **Save** to confirm the configuration.
13. When the configuration is saved and PBA is set to enabled, the configuration will be validated. It can also be manually validated by clicking **Confirm SS key Pair with PBA**.

Special Case: PBA Already Enabled

If PBA was already enabled in Secret Server prior to upgrading to version 10.4.000000 or later, you must copy the integration key from PBA to Secret Server in order to enable Single Sign On.

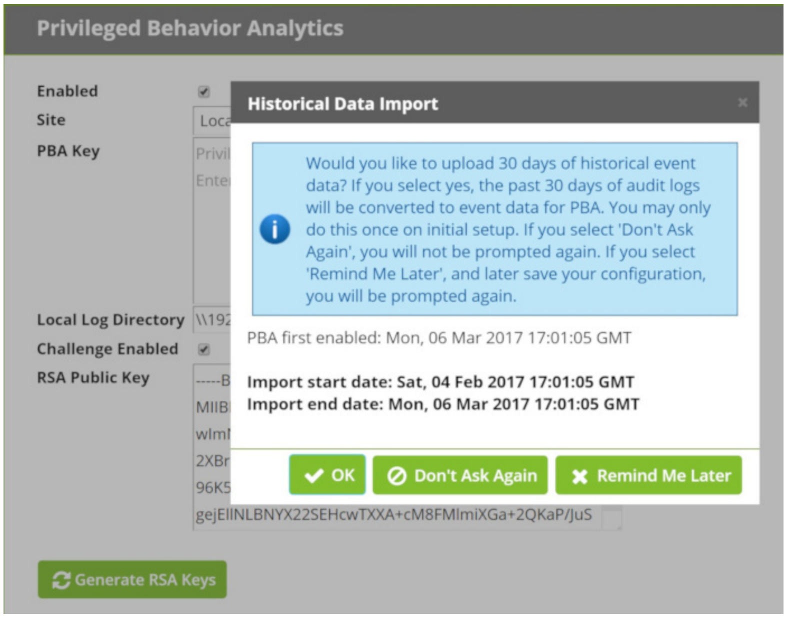
Single Sign On requires a key exchange in order for PBA to use Secret Server as an identity provider, and a new integration key is provided with PBA’s public key in order to initiate this key exchange.

Historical Data Import

When you first enable Privileged Behavior Analytics, you will be prompted whether to import the last 30 days of event data.

- Importing historical data reduces the learning period and potentially enables you to begin analyzing user behavior from day one, assuming Secret Server has been installed long enough to meet the learning period requirement.
- Event data is not persisted in Secret Server, but audit data is persisted. Accordingly, PBA derives events from audit data.
- By default, only 30 days of historical event data is imported because this is typically the most relevant data for learning about user behavior.

- If you seek to import more than 30 days of historical data, please contact Delinea Support for assistance.



Enabled ☑
Site Loca
PBA Key Privi Ente
Local Log Directory \\192
Challenge Enabled ☑
RSA Public Key -----B MIIB wlm 2XBr 96K5 gejEIINLBNYX22SEHcwTXXA+cM8FMlmiXGa+2QKaP/JuS

Would you like to upload 30 days of historical event data? If you select yes, the past 30 days of audit logs will be converted to event data for PBA. You may only do this once on initial setup. If you select 'Don't Ask Again', you will not be prompted again. If you select 'Remind Me Later', and later save your configuration, you will be prompted again.

PBA first enabled: Mon, 06 Mar 2017 17:01:05 GMT

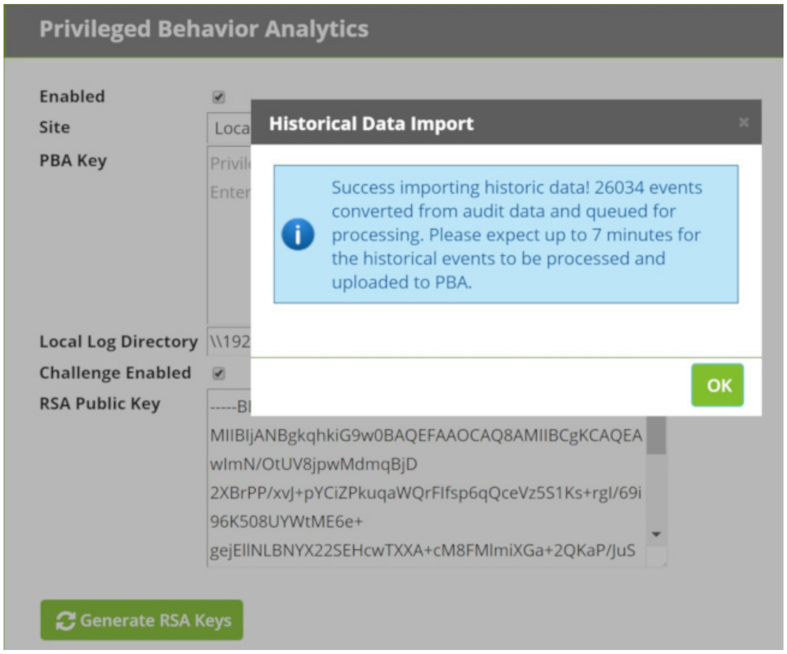
Import start date: Sat, 04 Feb 2017 17:01:05 GMT
Import end date: Mon, 06 Mar 2017 17:01:05 GMT

When you receive the prompt about whether to import historical data, select:

- **OK** to import 30 days of historical data
- **Don’t Ask Again** to permanently dismiss the query
- **Remind Me Later** to receive the prompt again the next time you save a PBA configuration with PBA enabled.
  - If you select **Remind Me Later** and come back on a later date to import historical data, the original 30-day time range will be used for the import, that is, the 30 days immediately prior to the first date that you enabled PBA. This ensures data continuity.

If you click **OK** to begin the import, you will see a dialog like the one below, stating the number of events to be imported and a time estimate for the import to complete. Immediately queued for processing, all the events must pass through the data pipeline for upload to Privileged Behavior Analytics.

- For Secret Server v10.3.000015 and earlier, note that the **Event Log Upload Frequency** may affect the total processing time. A shorter interval will decrease the time and a longer interval will increase the time.



Enabled ☑

Site Loca

PBA Key Privil Enter

Local Log Directory \\192

Challenge Enabled ☑

RSA Public Key
-----Bl
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
wlmN/OtUV8jpwMdmqBjD
2XBrPP/xvJ+pYCiZPkuqaWQrFlfsp6qQceVz5S1Ks+rgI/69i
96K508UYWtME6e+
gejEllNLBNYX22SEHcwTXXA+cM8FMlmiXGa+2QKaP/JuS

Success importing historic data! 26034 events converted from audit data and queued for processing. Please expect up to 7 minutes for the historical events to be processed and uploaded to PBA.

Proxied Environments

If your Secret Server has outbound access through a proxy, its web.config must be modified to specify the proxy configuration.

- If Secret Server is also clustered and has multiple worker roles enabled (see the Background Worker article), the web.config must be updated for each Secret Server in the cluster.

Microsoft has more information on this.

Note: For more information about using a distributed engine through a proxy, please refer to the Secret Server documentation.

The other option in a clustered environment is to specify a remote site for the data upload, and upload data through a Distributed Engine. If the distributed engine's host server is also behind a proxy, however, the engine's DelineaDelinea.DistributedEngine.Service.exe.config must be modified similarly to the web.config in order to specify the proxy settings.

- For Secret Server v10.4 or later, the web-proxy.config can be uncommented and updated to specify the proxy settings.

  For Secret Server v10.3.000015 or earlier, you must add proxy-related XML to the web.config file immediately following the file's closing \</configSections\> tag, as depicted here:

```
</configsections>
    <system.net>
        <defaultproxy enabled="true" usedefaultcredentials="true">
             <proxy
usesystemdefault="false" proxyaddress="https://proxy:port" bypassonlocal="true"/>
```

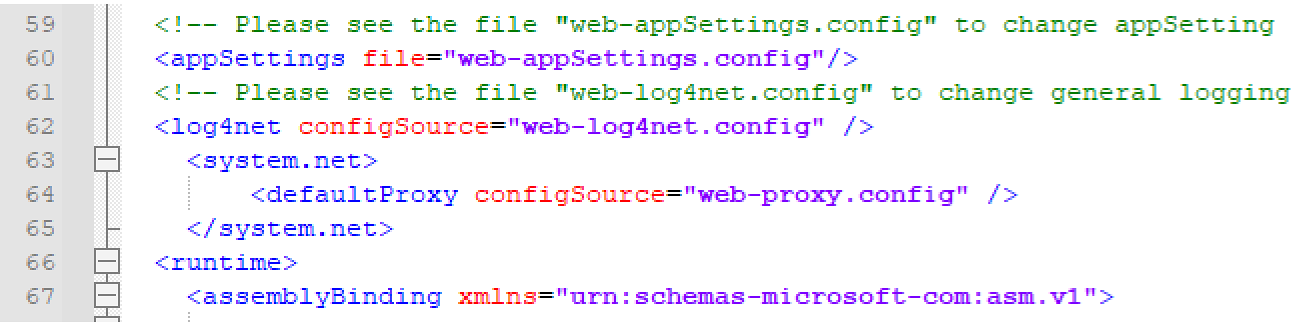
```
            </defaultproxy>
        </system.net>
    <configuration type="thycotic.foundation.configuration, thycotic.foundation">
```

Using Webnode with Proxied Environments

If you are using a webnode, you will need to add the following code:

```
<system.net>
    <defaultProxy configSource="web-proxy.config" />
</system.net>
```

Example:



```
<!-- Please see the file "web-appSettings.config" to change appSetting
<appSettings file="web-appSettings.config"/>
<!-- Please see the file "web-log4net.config" to change general logging
<log4net configSource="web-log4net.config" />
  <system.net>
      <defaultProxy configSource="web-proxy.config" />
  </system.net>
<runtime>
  <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
```

Distributed Engine (DE) Configuration

Note: Delinea suggests that you review any exception in the proxy configuration for both web nodes and DEs as a bypass. The configuration files may be overwritten with product updates and changes will be need to be reviewed, and possibly implemented again.

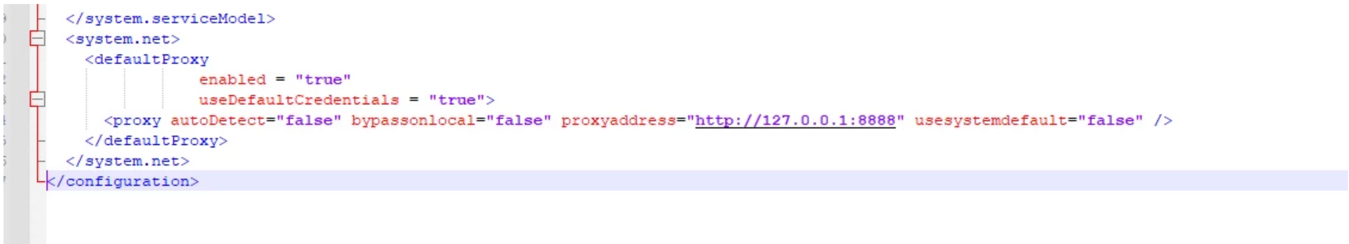
When Secret Server and DEs are behind a proxy, certain settings need to be added to webnodes and DEs if they exist in the environment.

To use with the Distributed Engine through a proxy, you will need to add proxy info to Delinea.DistributedEngine.Service.exe.config between </system.serviceModel> and located in the C:\Program Files\Thycotic Software Ltd\Distributed Engine\ folder on the distributed engine. You may need to refer to this article for other proxy related settings:

Element (Network Settings)

Note: For more information about using a distributed engine through a proxy, please refer to the Secret Server documentation.

```
<system.net>
    <defaultProxy>
        <proxy usesystemdefault="true" />
    </defaultProxy>
</system.net>
```



```
</system.serviceModel>
<system.net>
  <defaultProxy
              enabled = "true"
              useDefaultCredentials = "true">
    <proxy autoDetect="false" bypassonlocal="false" proxyaddress="http://127.0.0.1:8888" usesystemdefault="false" />
  </defaultProxy>
</system.net>
</configuration>
```

Important: You will need to restart the DE service after this update and the setting will need to be reapplied after any DE upgrade.

Webnode Configuration

Main Proxy settings are stored in the web-proxy.config file in the Secret Server folder on each webnode. Microsoft's article on Proxy configuration explains all settings.

[Element (Network Settings)]

Example #1

```
<?xml version="1.0" encoding="utf-8" ?>
<defaultProxy enabled="true">
<proxy
    usesystemdefault="true"
    proxyaddress="http://192.168.1.1:8080"
    bypassonlocal="true"
  />
</defaultProxy>
```

Example #2

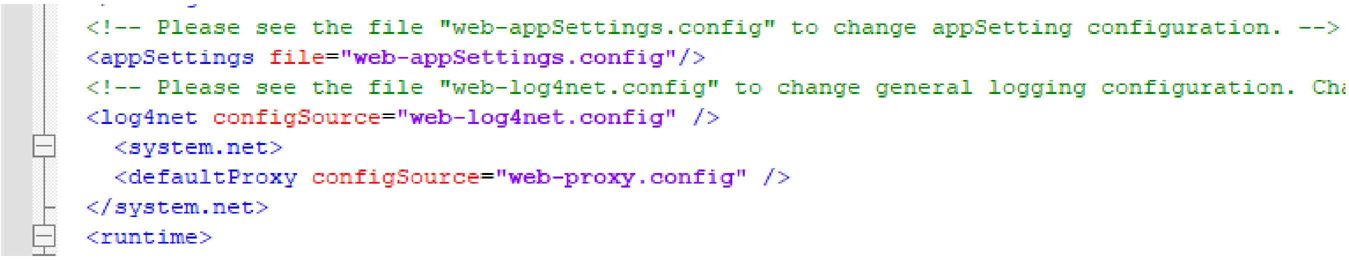
```
<defaultProxy enabled="true">
    <proxy proxyaddress–"http://proxy.domain.com:80" bypassonlocal-"true" / >
</defaultProxy>
```

Now, the following files need to be edited to point to the web-proxy.config file.

- web-embeddedRole-backgroundScheduler.config
- web-embeddedRole-backgroundWorker.config
- web-embeddedRole-engineWorker.config
- web-embeddedRole-messageBroker.config
- web-embeddedRole-sessionRecordingWorker.config

The code used in these files can be as follows:

```
<system.net>
    <defaultProxy configSource="web-proxy.config" />
</system.net>
```



```
<!-- Please see the file "web-appSettings.config" to change appSetting configuration. -->
<appSettings file="web-appSettings.config"/>
<!-- Please see the file "web-log4net.config" to change general logging configuration. Cha
<log4net configSource="web-log4net.config" />
  <system.net>
  <defaultProxy configSource="web-proxy.config" />
</system.net>
<runtime>
```

Note: Placement of this setting may effect connection. Make sure this setting is placed before the <runtime> element has been confirmed to make the configuration work.

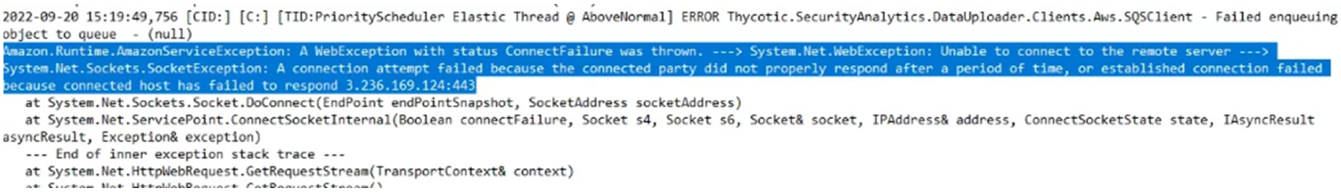
PBA Troubleshooting Tips

Search logs files for "Analytics" or "Amazon," as PBA integration reaches out to AWS and often you can find log entries specifically mentioning AWS connection issues.

DEs

Check the SSDE.log file.

Example:

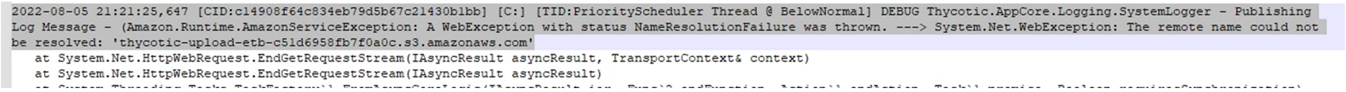


```
2022-09-20 15:19:49,756 [CID:] [C:] [TID:PriorityScheduler Elastic Thread @ AboveNormal] ERROR Thycotic.SecurityAnalytics.DataUploader.Clients.Aws.SQSClient - Failed enqueuing
object to queue  - (null)
Amazon.Runtime.AmazonServiceException: A WebException with status ConnectFailure was thrown. ---> System.Net.WebException: Unable to connect to the remote server --->
System.Net.Sockets.SocketException: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed
because connected host has failed to respond 3.236.169.124:443
   at System.Net.Sockets.Socket.DoConnect(EndPoint endPointSnapshot, SocketAddress socketAddress)
   at System.Net.ServicePoint.ConnectSocketInternal(Boolean connectFailure, Socket s4, Socket s6, Socket& socket, IPAddress& address, ConnectSocketState state, IAsyncResult
asyncResult, Exception& exception)
   --- End of inner exception stack trace ---
   at System.Net.HttpWebRequest.GetRequestStream(TransportContext& context)
```

Webnodes

Check the SS-BWSR.log file

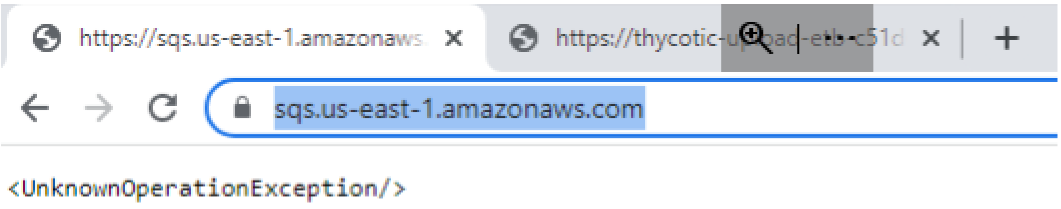
Example:



```
2022-08-05 21:21:25,647 [CID:c14908f64c834eb79d5b67c21430b1bb] [C:] [TID:PriorityScheduler Thread @ BelowNormal] DEBUG Thycotic.AppCore.Logging.SystemLogger - Publishing
Log Message - (Amazon.Runtime.AmazonServiceException: A WebException with status NameResolutionFailure was thrown. ---> System.Net.WebException: The remote name could not
be resolved: 'thycotic-upload-etb-c51d6958fb7f0a0c.s3.amazonaws.com'
   at System.Net.HttpWebRequest.EndGetRequestStream(IAsyncResult asyncResult, TransportContext& context)
   at System.Net.HttpWebRequest.EndGetRequestStream(IAsyncResult asyncResult)
```

Check to see if the machine can pull up the IP/URL in the logs in web browsers. While these do not specifically show full communication between systems, they can help narrow down the issue.

Example #1:

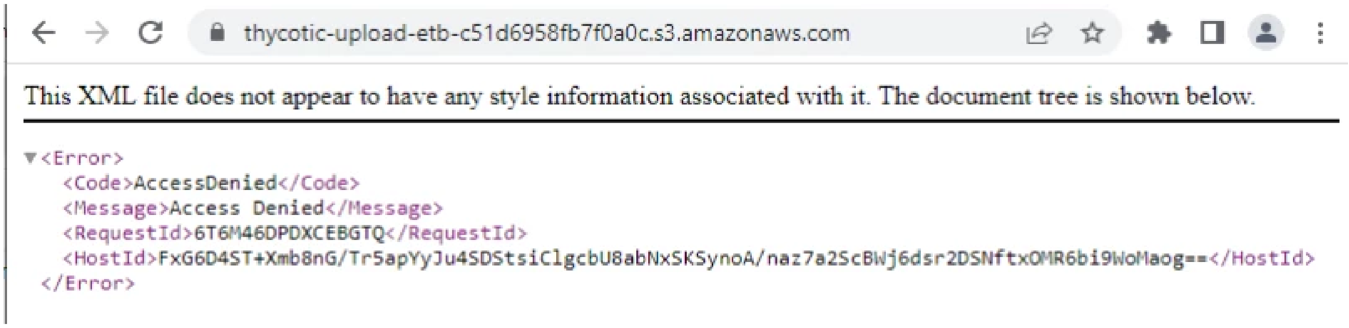


https://sqs.us-east-1.amazonaws
https://thycotic-upload-etb-c51d

sqs.us-east-1.amazonaws.com

```
<UnknownOperationException/>
```

Example #2:



This XML file does not appear to have any style information associated with it. The document tree is shown below.

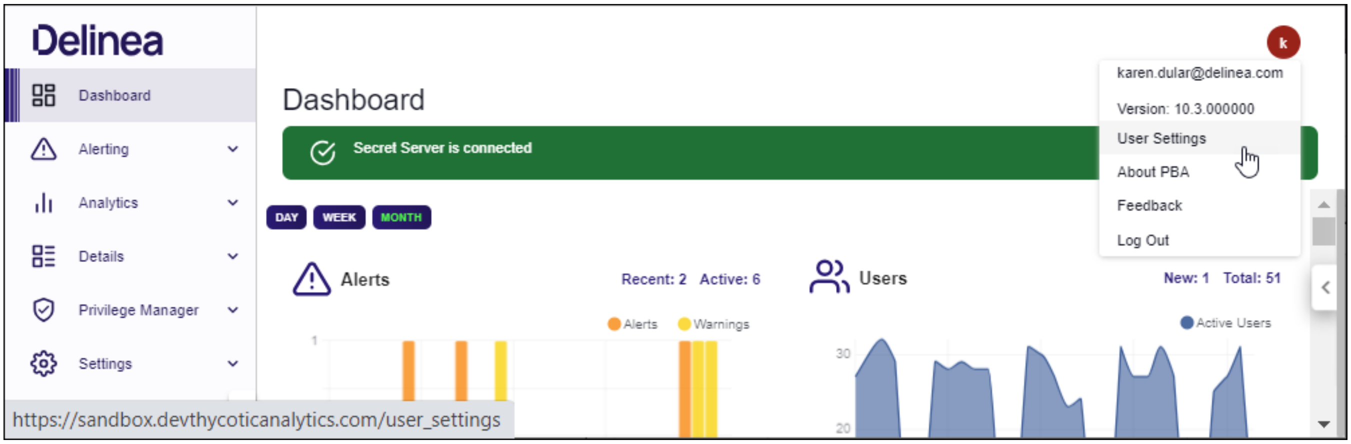
```
▼<Error>
   <Code>AccessDenied</Code>
   <Message>Access Denied</Message>
   <RequestId>6T6M46DPDXCEBGTQ</RequestId>
   <HostId>FxG6D4ST+Xmb8nG/Tr5apYyJu4SDStsiClgcbU8abNxSKSynoA/naz7a2ScBWj6dsr2DSNftxOMR6bi9WoMaog==</HostId>
 </Error>
```

Privileged Behavior Analytics Configuration

In PBA, the **User Settings** allow password changes and configuration of per-user alert notifications. The **System Settings** allow the configuration of Secret Server integration, global alert and challenge callback, and time settings.

User Settings

You can navigate to **User Settings** by clicking your profile icon at the top right of any PBA page and choosing **User Settings**.



Dashboard

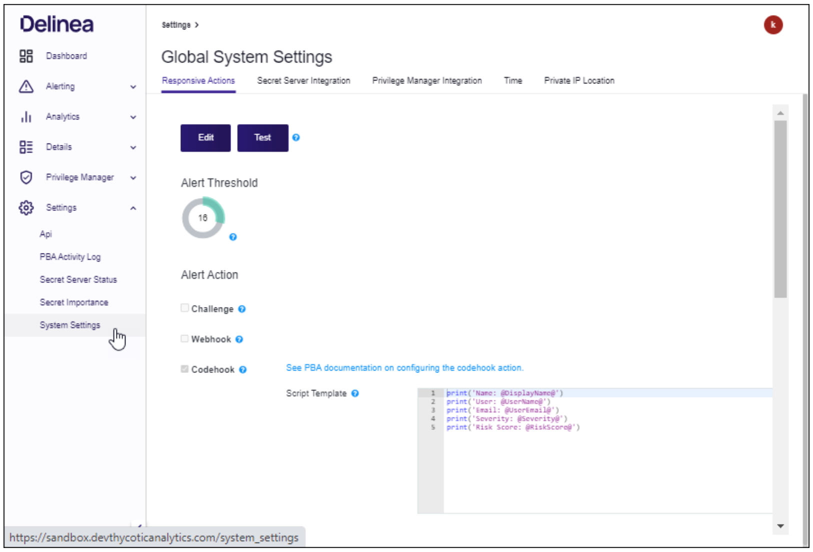
Secret Server is connected

Account Settings: Lets you change the password on your account used to access PBA.

Alert Notification Settings: You can set the email address to receive alerts and specify whether you want to receive alerts and warnings as they occur.

System Settings

Select **Settings** in the left navigation panel, then select **System Settings**



```
print('Name: @DisplayName@')
print('User: @UserName@')
print('Email: @UserEmail@')
print('Severity: @Severity@')
print('Risk Score: @RiskScore@')
```

Each tab provides access to the following system settings.

Responsive Actions

Alert Threshold: The numerical value an alert needs to meet or exceed to send an email.

Alert Action: Whether you wish to Challenge a Secret Server User if their actions cause PBA to generate an alert for them that meets or exceeds the Alert Threshold. To use Challenges, you must configure it on Secret Server as well. More information on the configuration can be found in the following Access Challenges section.

Warning Threshold: The numerical value a warning needs to meet or exceed to send an email.

Warning Action: Whether you wish to Challenge a Secret Server User if their actions cause PBA to generate a warning for them that meets or exceeds the Warn Threshold.

Secret Importance: Brings you to a page that lists all of your Secrets and lets you change any of their importance settings in PBA.

User Watch List: Check the boxes to automatically watchlist users with active alerts and warnings or new users. If the status of the user changes (for example, their active alert is cleared, or a new user reaches 30 days), then the user will be automatically removed from the User Watch List.

Secret Server Integration

Secret Server Integration Key

View Integration Key: This key is copied to Secret Server and provides access information for Secret Server to authenticate with and upload data to PBA.

- **Version 10.4.000000 and Later**
  - **PBA Key Pair /Secret Server Key Pair:** Key exchange is used by PBA during Single Sign On in order to verify Secret Server's (as an identity provider) user claims. In the opposite direction, it is used by Secret Server as an additional layer of security to verify that Access Challenges were signed by the authorized PBA

instance.

- **Initiate Key Rotation:** PBA initiates a key rotation in which both Secret Server and PBA generate a new key pair and exchange the new public key with each other using the last public key to sign this new exchange. Keys are typically rotated periodically as a security best practice.
- **Clear Keys**: This is used *only* when migrating from one Secret Server instance to a completely new Secret Server instance while using the same PBA instance *or* when troubleshooting issues with key exchange. CAUTION: This clears all key pairs (both Secret Server and PBA) from PBA's database. After clearing, the integration key is copied to the target Secret Server and the initial key exchange is conducted, the same as with a fresh configuration of PBA-Secret Server integration.

Secret Server Public Key

- **Version 10.3.000015 and Earlier**
  - **View Public Key**: The public key from **/AdminAnalyticsEdit.aspx** in Secret Server must be copied to PBA and saved in order to use Access Challenges.

Secret Server Outbound URLs

The two URLs displayed, URL 1 and 2, are the URLs that Secret Server needs to access to communicate with the PBA applications on AWS. If restrictions are placed on Secret Server's outbound connections, ensure that these endpoints are allowed for PBA functionality.

Single Sign-On (Version 10.4 and Later, Cloud)

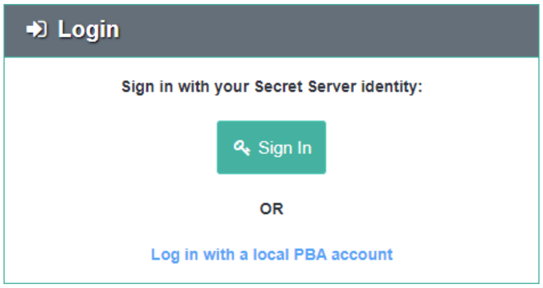
As of version 10.4.000000, Secret Server can act as an identity provider for PBA.

- Any user with the *View Security Analytics* role permission in Secret Server may log into PBA.
- Additionally, any user with *Administer Security Analytics* role permission is able to perform administrative actions once logged into PBA through Single Sign-On (SSO).
- Local PBA users (the initial users prior to integrating PBA into Secret Server) still have administrative rights as well.

Typically, Single Sign On will start working without additional configuration.

Verify Single Sign On

Verify that on *both* of these pages–**<SECRET SERVER>/AdminAnalyticsView.aspx** and **<PBA>/system_settings**–the PBA and Secret Server key pairs *both* show a status of **Confirmed**. This key exchange is used for verification of Secret Server as an identity provider.


Login
Sign in with your Secret Server identity:
Sign In
OR
Log in with a local PBA account

In order to verify that the SSO claim was signed by Secret Server, PBA must have a copy of Secret Server's public key.Secret Server versions 10.4.000000 or later have infrastructure for key exchange and rotation between Secret Server and PBA.

- When the integration key is first copied from PBA and saved to Secret Server, it contains PBA's initial public key.
- Secret Server then generates its own key pair and sends its public key to PBA.
- PBA registers Secret Server's public key and sends confirmation back to Secret Server.

When a key rotation is initiated, PBA generates a new key pair and sends a signed request to Secret Server. The rest of the process is the same as the initial key exchange, except that each message is signed and verified during the rotation.

Troubleshooting

If Secret Server or PBA shows that its Key Pair status is **Pending Confirmation**, try the **Resend Confirmation** button in either application.

- For example, if in Secret Serverits key pair is **Pending**, then you would click the **Resend Confirmation** button in PBA, so that PBA will retry communicating to Secret Server that PBA did register Secret Server's latest public key.

Access Challenges

Privileged Behavior Analytics can automatically issue **Access Challenges** on detection of anomalous behavior in Secret Server.

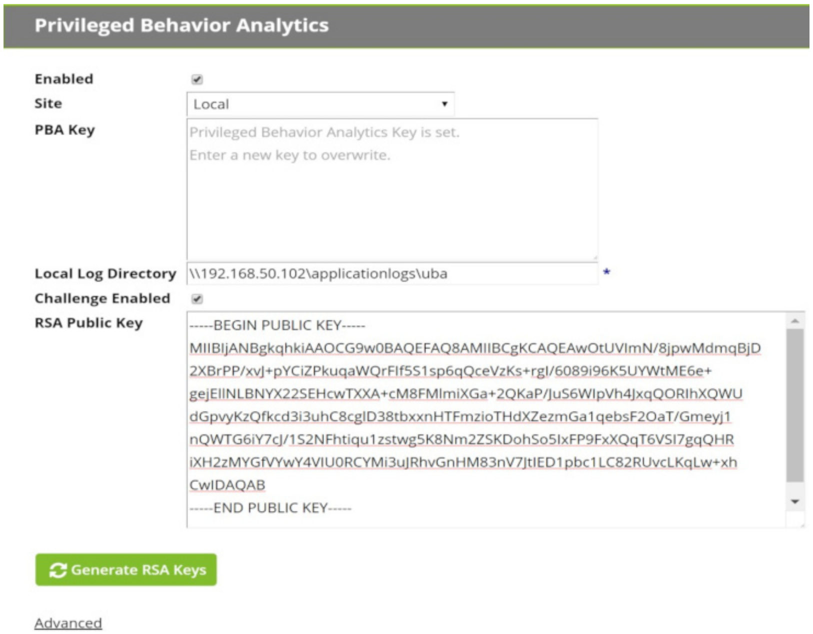
- Rule-based Challenges allow you to directly specify what qualifies as anomalous, for example, you can set a rule to issue a Challenge when a user's risk level exceeds a pre-determined threshold.
- When PBA sends a Challenge to a Secret Server user, it can temporarily suspend the user's access to Secret Server. The user or an administrator must clear the Challenge for the user to regain access.

PBA can challenge only users with the Secret Server **Allow Access Challenge** Role permission. This Role permission applies by default to all users except those with the **Unlimited Administrator** role permission.

Secret Server Configuration for Access Challenges

Version 10.3.000015 and Earlier

Navigate to **<SECRET SERVER>/AdminAnalyticsEdit.aspx** and check **Challenge Enabled**. Generate a new RSA key pair and copy the public key before saving. This public key will be saved in PBA.



Privileged Behavior Analytics

Enabled ☑

Site: Local

PBA Key: Privileged Behavior Analytics Key is set. Enter a new key to overwrite.

Local Log Directory: \\192.168.50.102\applicationlogs\uba *

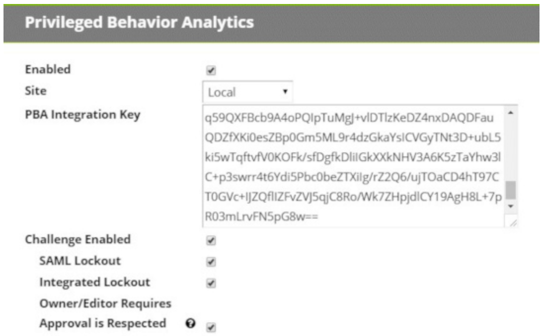
Challenge Enabled ☑

RSA Public Key:

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiAAOCG9w0BAQEFAQ8AMIIBCgKCAQEAwOtUVlmN/8jpwMdmqBjD
2XBrPP/xvJ+pYCiZPkuqaWQrFIf5S1sp6qQceVzKs+rgI/6089i96K5UYWtME6e+
gejEllNLBNYX22SEHcwTXXA+cM8FMlmiXGa+2QKaP/JuS6WIpVh4JxqQORIhXQWU
dGpvyKzQfkcd3i3uhC8cgID38tbxxnHTFmzioTHdXZezmGa1qebsF2OaT/Gmeyj1
nQWTG6iY7cJ/1S2NFhtiqu1zstwg5K8Nm2ZSKDohSo5IxFP9FxXQqT6VSI7gqQHR
iXH2zMYGfVYwY4VIU0RCYMi3uJRhvGnHM83nV7JtIED1pbc1LC82RUvcLKqLw+xh
CwIDAQAB
-----END PUBLIC KEY-----
```

Version 10.4.000000 and Later, Cloud

Navigate to **<SECRET SERVER>/AdminAnalyticsEdit.aspx** and check **Challenge Enabled**.



Privileged Behavior Analytics

Enabled ☑

Site: Local

PBA Integration Key:

```
q59QXFBcb9A4oPQIpTuMgJ+vlDTlzKeDZ4nxDAQDFau
QDZfXKi0esZBp0Gm5ML9r4dzGkaYsICVGyTNt3D+ubL5
ki5wTqftvfV0KOFk/sfDgfkDliIGkXXkNHV3A6K5zTaYhw3l
C+p3swrr4t6Ydi5Pbc0beZTXiIg/rZ2Q6/ujTOaCD4hT97C
T0GVc+IJZQflIZFvZVJ5qjC8Ro/Wk7ZHpjdlCY19AgH8L+7p
R03mLrvFN5pG8w==
```

Challenge Enabled ☑

SAML Lockout ☑

Integrated Lockout ☑

Owner/Editor Requires Approval is Respected ☑

Additional Settings

SAML Lockout: When this is set, authentication attempts via SAML can be blocked pursuant to a Lockout Challenge. If this setting is disabled, Lockout Challenges will apply only to non-SAML local authentication attempts where Secret Server is the identity provider. Delinea recommends this setting be enabled.

Integrated Lockout: When this is set, authentication attempts via Active Directory can be blocked pursuant to a Lockout Challenge. If this setting is disabled, Lockout Challenges will apply only to non-AD local authentication attempts where Secret Server is the identity provider. Delinea recommends this setting be enabled.

Respect Owner/Editor Requires Approval: This setting relates to Secrets subject to an **Owner Requires Approval** or **Editor Requires Approval** condition based on a global setting, a Secret Policy, or a setting in the Secret itself.

- If this setting is disabled, such **Requires Approval** conditions on a Secret *will not* be respected during a **Requires Approval Access Challenge**.
- If this setting is enabled, such conditions *will* be respected during such a challenge.
    - **Example:** A user is an editor of a Secret, and the effective setting on the Secret is *Editor Requires Approval=True*. However, the PBA setting to **Respect Owner/Editor Requires Approval** is not active. Therefore, when a **Requires Approval Access Challenge** is processed for this user, the user will be able to access the Secret despite being subject in Secret Server to an *Editor Requires Approval=True* condition.
        - In this example, if the PBA setting *was* active, the user would need to request approval to access the Secret until the Challenge is cleared, because PBA would respect the Secret Server *Editor Requires Approval=True* condition.
    - **Example:** A user is an editor of a Secret, and the effective setting on the Secret is *Editor Requires Approval=False*. However, the PBA setting to **Respect Owner/Editor Requires Approval** settings is still not active. Therefore, when a **Requires Approval Access Challenge** is processed for this user, the user will *not* be able to access the Secret despite having in Secret Server an *Editor Requires Approval=False* condition, because PBA is not set to honor that setting.
        - In this example, if the PBA setting *was* active, the user would need to request approval to access the Secret until the Challenge is cleared, because PBA would respect the Secret Server *Editor Requires Approval=True* condition.

PBA Configuration for Access Challenges

Log into your PBA instance and navigate to **System Settings** by clicking on the cogwheel symbol at the top right of any PBA page and choosing **System Settings**.

Under **Global System Settings**, you can set triggers for Event Actions (an Alert or Warning) when conditions meet a certain risk threshold.

- Step only for Secret Server 10.3.000015 and earlier: Click **Edit** and paste your public key copied from Secret Server's **AdminAnalyticsEdit.aspx** page into the Secret Server **Public Key** field. If you ever generate and save new keys, you must update the public key in PBA.

Currently, two simple rules may be set, a **Warning Threshold** and an **Alert Threshold**, with the Warning Threshold naturally lower than the Alert Threshold. For both, there are options to set up a Secret Server Challenge or run a Webhook or Codehook.

In setting up a Challenge, you must specify the Challenge **Type.** Secret Server Version 10.2.000000 has only one Challenge Type:

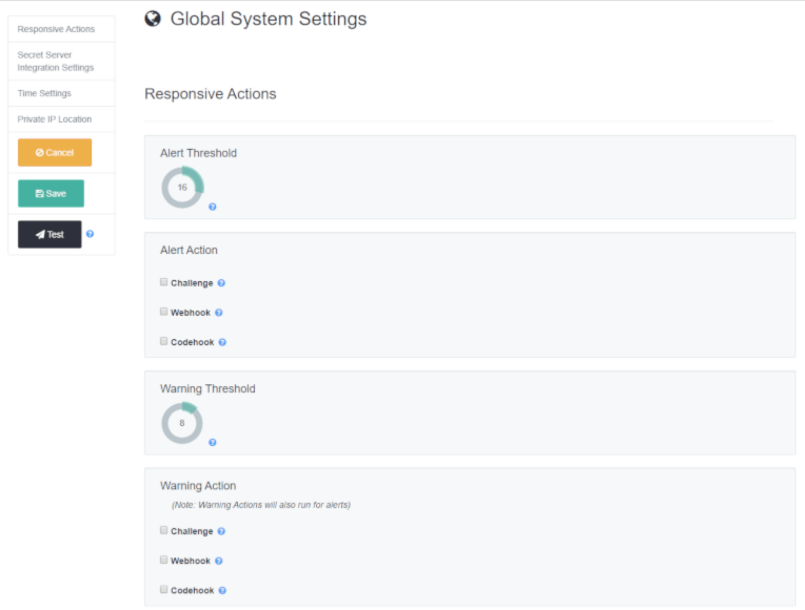
- **Login**: the user must re-authenticate with Secret Server

Secret Server Versions 10.3.000015 and later have the **Login** Challenge Type, plus several more:

- **Two Factor**: the user must re-authenticate with Secret Server and the **Two Factor Remember Me** is expired (if set)
- **Require Approval**: the user must request approval for accessing any Secrets unless:
  - they are the only Approver for that Secret, *or*
  - they are the Owner or Editor; the Secret has *Editor/Owner Requires Approval* disabled; and PBA Configuration has *Respect Editor/Owner Requires Approval* enabled
- **Lockout**: the user is locked out from Secret Server until expiration of the Challenge or until it is cleared by an Admin user (a user having the **Administer Security Analytics** Role permission in Secret Server)
- **Record Session**: for Secrets that are capable of session recording the user will have their session recorded surreptitiously

You must also specify the Challenge **Duration** in minutes.

- If Duration is set to 0 minutes, the Challenge will never expire and the target Secret Server user will be denied access until they or an Admin clears the Challenge.



Global System Settings

Responsive Actions

Alert Threshold

16

Alert Action

□ Challenge

□ Webhook

□ Codehook

Warning Threshold

8

Warning Action

(Note: Warning Actions will also run for alerts)

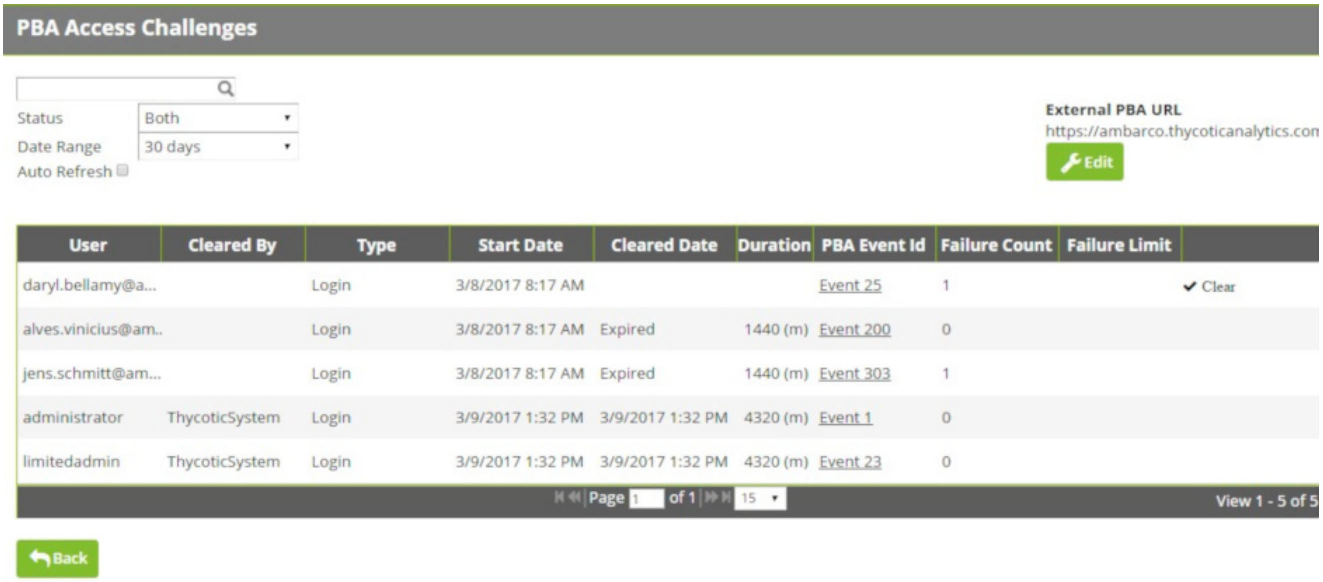
□ Challenge

□ Webhook

□ Codehook

Access Challenge Administration

Challenges processed by Secret Server may be viewed and administered on **<SECRET SERVER>/AdminChallengeView.aspx**. This page is accessed by clicking the **Administer Challenges** button on **AdminAnalyticsView.aspx**.



PBA Access Challenges

Status: Both

Date Range: 30 days

Auto Refresh □

External PBA URL
https://ambarco.thycoticanalytics.con

User	Cleared By	Type	Start Date	Cleared Date	Duration	PBA Event Id	Failure Count	Failure Limit	
daryl.bellamy@a...		Login	3/8/2017 8:17 AM			Event 25	1		✓ Clear
alves.vinicius@am..		Login	3/8/2017 8:17 AM	Expired	1440 (m)	Event 200	0		
jens.schmitt@am...		Login	3/8/2017 8:17 AM	Expired	1440 (m)	Event 303	1		
administrator	ThycoticSystem	Login	3/9/2017 1:32 PM	3/9/2017 1:32 PM	4320 (m)	Event 1	0		
limitedadmin	ThycoticSystem	Login	3/9/2017 1:32 PM	3/9/2017 1:32 PM	4320 (m)	Event 23	0		

- Challenges may be filtered by username and status (Cleared or Uncleared).
- If the External PBA URL is set, the **PBA Event Id** column will display a link to the Event Details page in PBA for the Event that triggered the Challenge.

The following additional columns are displayed:

- **Cleared By**: This is the user (if any) that cleared the Challenge.
  - For a Login Challenge, all of a user's Secret Server sessions are ended and they must log into Secret Server successfully to clear the Challenge.
  - If a user does not have the **Allow Access Challenge** Role permissions in Secret Server, the Challenge will still be recorded, but will be listed as cleared by the **ThycoticSystem** user.
  - Finally, if an Administrator clears a Challenge on this page, that Administrator's username will be listed.
- **Type**: This is the Challenge Type as specified in the rule configured in PBA.
- **Start Date**: The time that an Event occurred in PBA and triggered the Challenge Event Action.
- **Cleared Date**: The date (if ever), the Challenge was cleared. If the Challenge has not been cleared, but Duration (in minutes) has passed, the Challenge will be listed as **Expired**.
- **Failure Count**: The number of times the user failed to clear the challenge, such as by failing to successfully authenticate.
- **Clear Button**: This is visible if you have the **Administer Security Analytics** Role permission in Secret Server. It allows you to clear a Challenge for another user.

Access Challenge Security

Because Access Challenge affects Secret Server user access from an external system, the architecture is heavily focused on security.

PBA Applications for Secret Server

Once you have setup Secret Server and Privileged Behavior Analytics to work together, you can begin normal operations. During a typical session with PBA, you will use various tools, including the tools summarized in the table below.

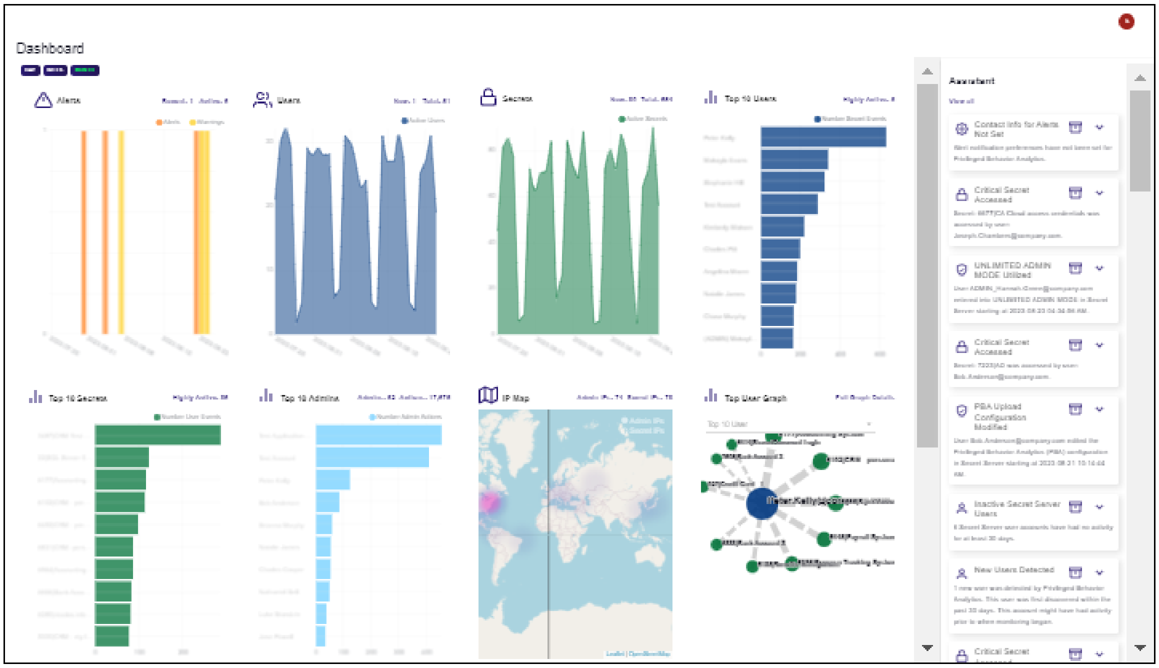
Name	Description
"Dashboard" on the next page	Displays several key indicators neatly assembled on quick-view tiles
"Privileged Behavior Alerts" on page 27	Lists PBA-issued alerts based on abnormal Secret access and Admin action patterns, according to thresholds you set; includes current alerts and access to retired alerts
"User Watch List" on page 30	Assembles information about users whose activity accessing Secrets has attracted your specific scrutiny
"Secret Event Clock" on page 31	Displays temporal patterns and filters data by User, Secret, and IP/location
"Secret Event Graph" on page 32	Shows users accessing Secrets, designed to reveal anomalous patterns
"Secret Event IP Map" on page 38	Maps out Secret accesses, aggregated by IP address and location
"Most Active Secrets" on page 43	Reveals which Secrets have been most accessed
"Most Active Users" on page 44	Identifies users accessing more Secrets than most other users
"Admin Actions" on page 45	Contains a suite of analytics on administrative activity, including: Clock, Graph, IP Map, and Most Active Admins and Actions
"Secret Details" on page 46	Runs down all recent access activity for specific Secrets as well as characteristics of the Secret
"User Details" on page 49	Allows you to explore in detail information collected about a specific user’s activity
"IP Address Details" on page 52	Shows IP address activity summary and location information (for Secret Server instances that record user IP)

Name	Description
	Enables data query for secrets and allows export for criteria you specify
"Query" on page 55	Enables data query for administrator actions and allows export for criteria you specify.

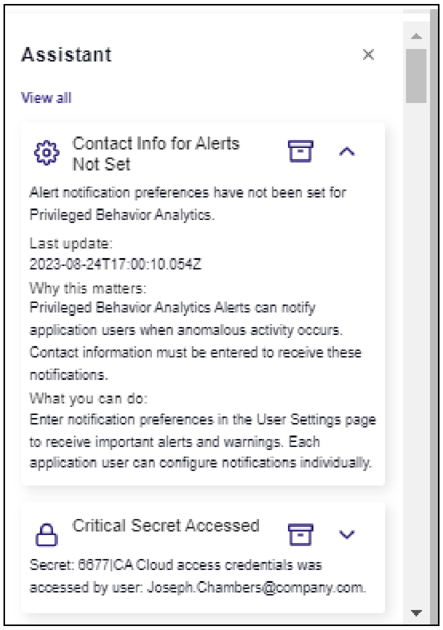
Dashboard

PBA's **Analytics Dashboard** landing page collects commonly used tools and views so you can easily recognize anything that would be out of the ordinary for your Secret Server environment.

- Multiple widgets present at-a-glance data visuals that cycle through views of activity for the last day, week, and month.
- The widgets activate or deactivate when you click the controls for each on the left side of the Dashboard.
- Cycling pauses on the data view for the last day, week, and month when you click on the Day, Week, and Month controls.
- Additional settings (dashboard theme, widget settings, cycle duration) are accessible through the three horizontal bars icon on the top left side.



The Dashboard **Assistant** displays recent events and provides the following functionality.



Assistant

View all

Contact Info for Alerts Not Set

Alert notification preferences have not been set for Privileged Behavior Analytics.

Last update:
2023-08-24T17:00:10.054Z

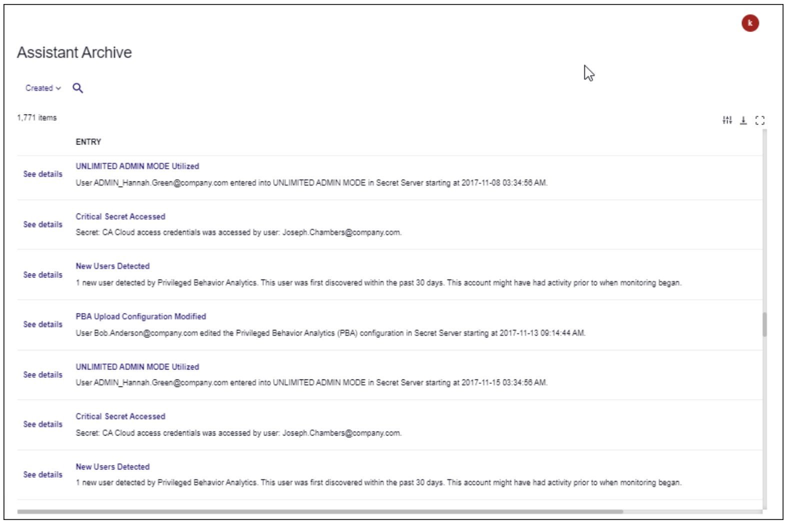
Why this matters:
Privileged Behavior Analytics Alerts can notify application users when anomalous activity occurs. Contact information must be entered to receive these notifications.

What you can do:
Enter notification preferences in the User Settings page to receive important alerts and warnings. Each application user can configure notifications individually.

Critical Secret Accessed

Secret: 6677|CA Cloud access credentials was accessed by user: Joseph.Chambers@company.com.

- The Dashboard Assistant focuses on recent events. Click the title displayed on each card to access a record of that event.
- The downward facing arrow icons on each card expands the record area to show additional information for that event that includes guidance on why the event has significance and what steps you should consider.
- Click **View all** to display the Assistant Archive page. All events in the archive are displayed in a table that allows sorting and filtering. Click **See details** for an event to display additional details.

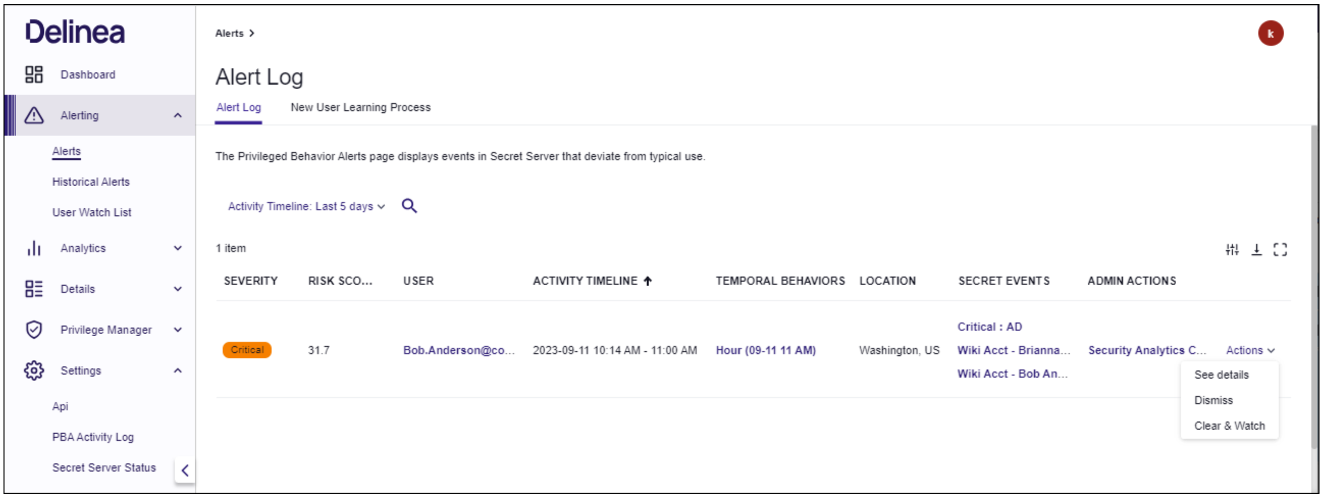


Assistant Archive

1,771 items

	ENTRY
See details	UNLIMITED ADMIN MODE Utilized User ADMIN_Hannah.Green@company.com entered into UNLIMITED ADMIN MODE in Secret Server starting at 2017-11-08 03:34:56 AM.
See details	Critical Secret Accessed Secret: CA Cloud access credentials was accessed by user: Joseph.Chambers@company.com.
See details	New Users Detected 1 new user detected by Privileged Behavior Analytics. This user was first discovered within the past 30 days. This account might have had activity prior to when monitoring began.
See details	PBA Upload Configuration Modified User Bob.Anderson@company.com edited the Privileged Behavior Analytics (PBA) configuration in Secret Server starting at 2017-11-13 09:14:44 AM.
See details	UNLIMITED ADMIN MODE Utilized User ADMIN_Hannah.Green@company.com entered into UNLIMITED ADMIN MODE in Secret Server starting at 2017-11-15 03:34:56 AM.
See details	Critical Secret Accessed Secret: CA Cloud access credentials was accessed by user: Joseph.Chambers@company.com.
See details	New Users Detected 1 new user detected by Privileged Behavior Analytics. This user was first discovered within the past 30 days. This account might have had activity prior to when monitoring began.

Privileged Behavior Alerts

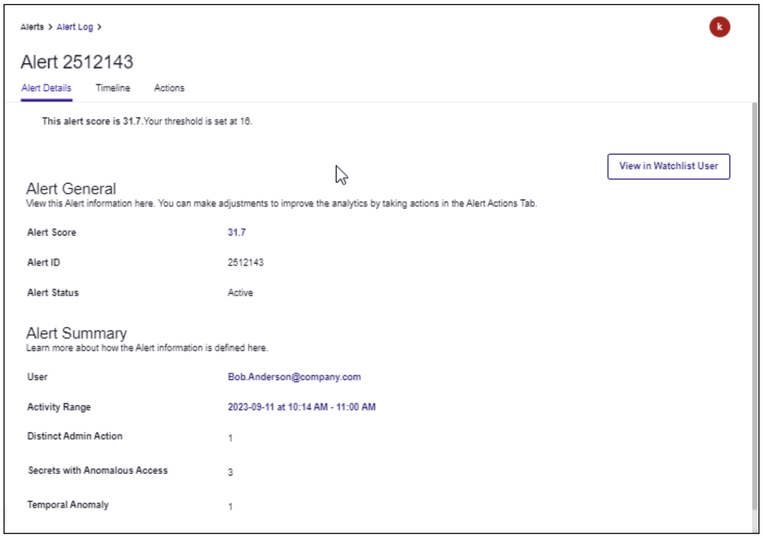


The Privileged Behavior Alerts page displays events in Secret Server that deviate from typical use.

SEVERITY	RISK SCO...	USER	ACTIVITY TIMELINE ↑	TEMPORAL BEHAVIORS	LOCATION	SECRET EVENTS	ADMIN ACTIONS
Critical	31.7	Bob.Anderson@co...	2023-09-11 10:14 AM - 11:00 AM	Hour (09-11 11 AM)	Washington, US	Critical : AD Wiki Acct - Brianna... Wiki Acct - Bob An...	Security Analytics C...

Use the search field to locate specific Alerts by searching on text from any of the rows in the table. Columns include:

- **Severity**: whether the event justified an Alert (serious event) or a Warning (minor event)
- **Score**: the numerical score given to the event depending on its severity and the severity of incorporated events
- **User**: the Secret Server User who caused the Alert; clicking their name opens the **User Details** page
- **Range of Activity**: the time span within which the Alert occurred; includes an optional timeline graphic
- **IP Addresses**: the IP addresses used during the alert period with links to each IP Details page
- **Secret Accesses**: any Secrets accessed during the time span of the Alert that contributed to the Alert; clicking on the Secrets opens the **Secret Details** page
- **Admin Actions**: any administrative actions taken in Secret Server during the time span of the Alert that may have contributed to the Alert; clicking on the Admin Actions listed displays the table of all administrative activity for that User
- **Temporal Behavior**: a time entry will be listed here if the Alert occurred at a time the User does not normally access the Secrets involved in the Alert; clicking on the time entry will display the User’s Temporal Data.
- **Actions**: provides options to **See details** bout the alert, **Dismiss** the alert as normal behavior, or **Clear & Watch** the alert as abnormal behavior
  - To further investigate the Alert, view details and a timeline, log actions you have taken on the Alert, adjust the importance of any involved Secrets, or provide feedback to Delinea on the usefulness of the Alert, click **See details**.



Alert 2512143

This alert score is 31.7.Your threshold is set at 16.

Alert General

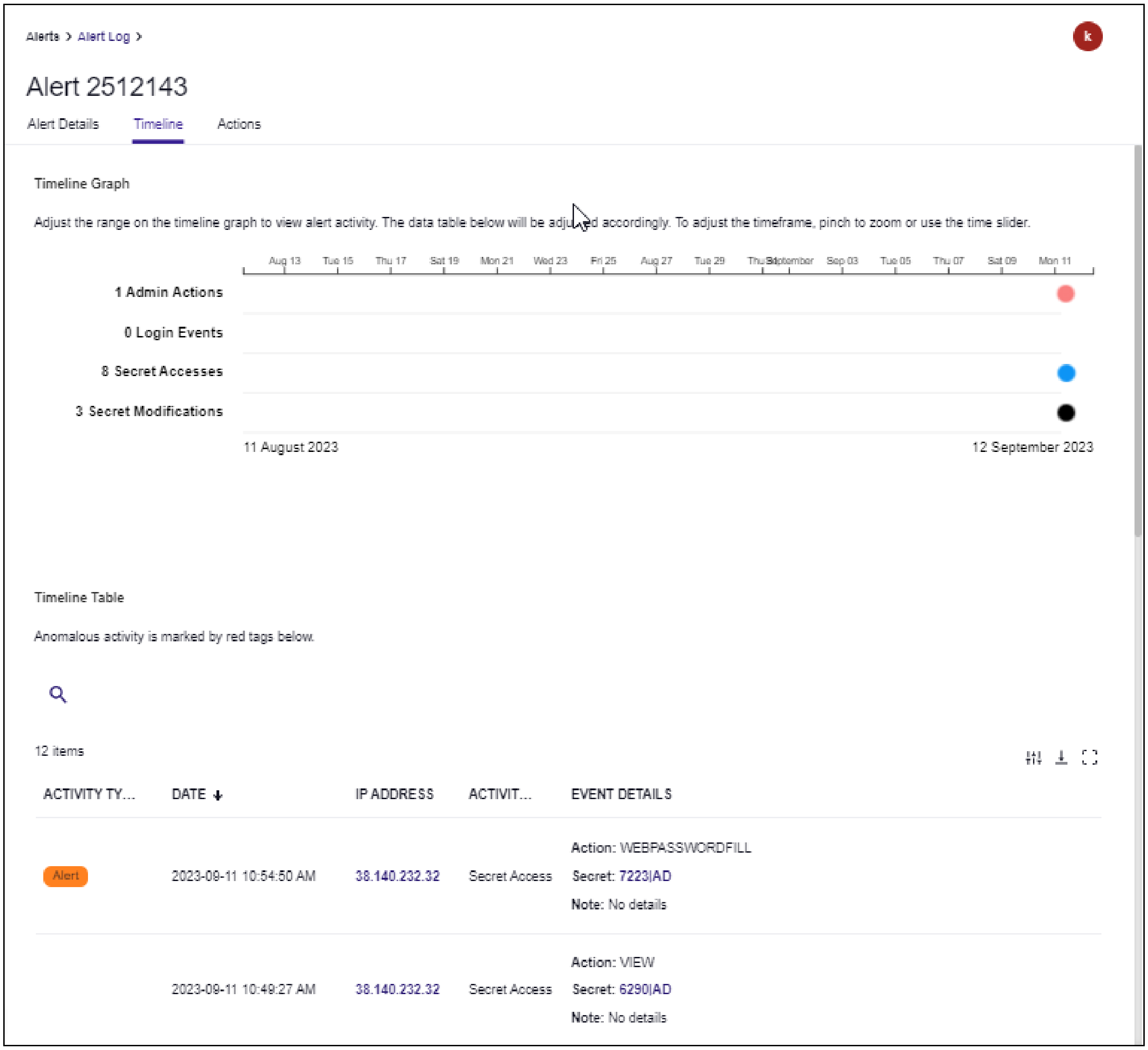
View this Alert information here. You can make adjustments to improve the analytics by taking actions in the Alert Actions Tab.

Alert Score	31.7
Alert ID	2512143
Alert Status	Active

Alert Summary

Learn more about how the Alert information is defined here.

User	Bob.Anderson@company.com
Activity Range	2023-09-11 at 10:14 AM - 11:00 AM
Distinct Admin Action	1
Secrets with Anomalous Access	3
Temporal Anomaly	1



Alert 2512143

Timeline Graph

Adjust the range on the timeline graph to view alert activity. The data table below will be adjusted accordingly. To adjust the timeframe, pinch to zoom or use the time slider.

Timeline Table

Anomalous activity is marked by red tags below.

12 items

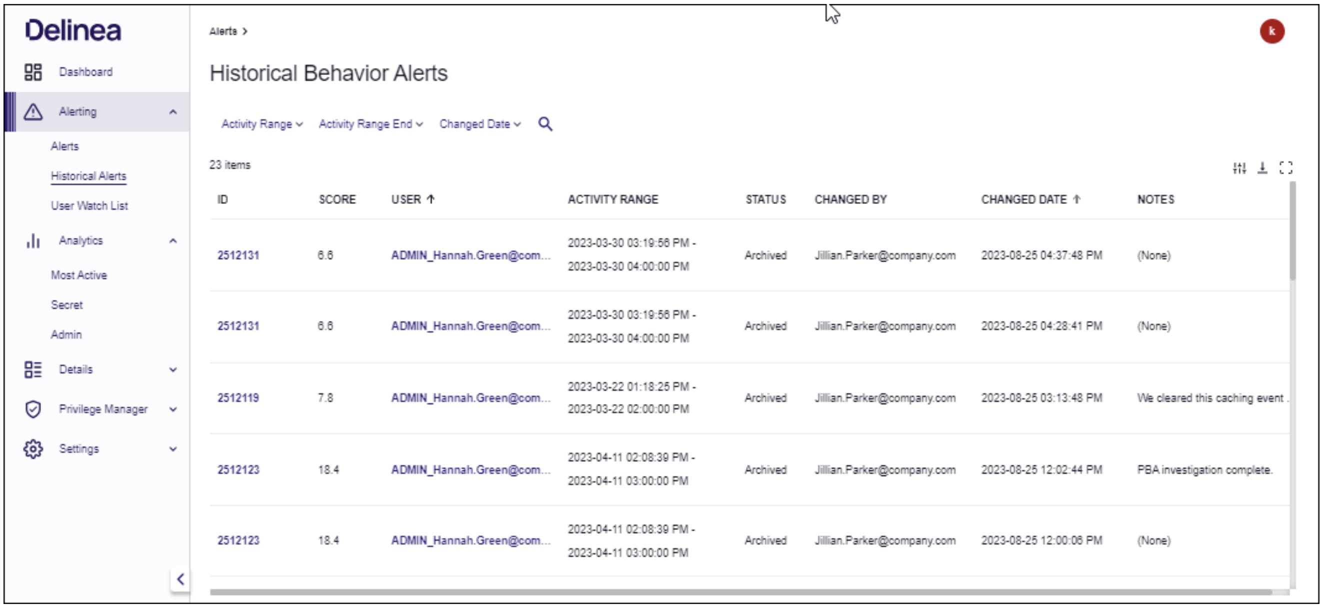
ACTIVITY TY...	DATE ↓	IP ADDRESS	ACTIVIT...	EVENT DETAILS
Alert	2023-09-11 10:54:50 AM	38.140.232.32	Secret Access	Action: WEBPASSWORDFILL Secret: 7223|AD Note: No details
	2023-09-11 10:49:27 AM	38.140.232.32	Secret Access	Action: VIEW Secret: 6290|AD Note: No details

- Clicking **Dismiss** or **Clear & Watch** removes the alert from the page and saves it to **Historical Behavior Alerts**

Historical Behavior Alerts

The Historical Behavior Alerts page archives Alerts after they have been cleared from an Active state.

You can reach the Historical Behavior Alerts by navigating to **Alerts** > **Historical Behavior Alerts**.



Historical Behavior Alerts

23 items

ID	SCORE	USER ↑	ACTIVITY RANGE	STATUS	CHANGED BY	CHANGED DATE ↑	NOTES
2512131	6.6	ADMIN_Hannah.Green@com...	2023-03-30 03:19:56 PM - 2023-03-30 04:00:00 PM	Archived	Jillian.Parker@company.com	2023-08-25 04:37:48 PM	(None)
2512131	6.6	ADMIN_Hannah.Green@com...	2023-03-30 03:19:56 PM - 2023-03-30 04:00:00 PM	Archived	Jillian.Parker@company.com	2023-08-25 04:28:41 PM	(None)
2512119	7.8	ADMIN_Hannah.Green@com...	2023-03-22 01:18:25 PM - 2023-03-22 02:00:00 PM	Archived	Jillian.Parker@company.com	2023-08-25 03:13:48 PM	We cleared this caching event ...
2512123	18.4	ADMIN_Hannah.Green@com...	2023-04-11 02:08:39 PM - 2023-04-11 03:00:00 PM	Archived	Jillian.Parker@company.com	2023-08-25 12:02:44 PM	PBA investigation complete.
2512123	18.4	ADMIN_Hannah.Green@com...	2023-04-11 02:08:39 PM - 2023-04-11 03:00:00 PM	Archived	Jillian.Parker@company.com	2023-08-25 12:00:06 PM	(None)

In viewing Historical Behavior Alerts, note these fields:

- **Changed by**: the PBA User who cleared the Alert
- **Notes**: notes left on the Alert before it was cleared

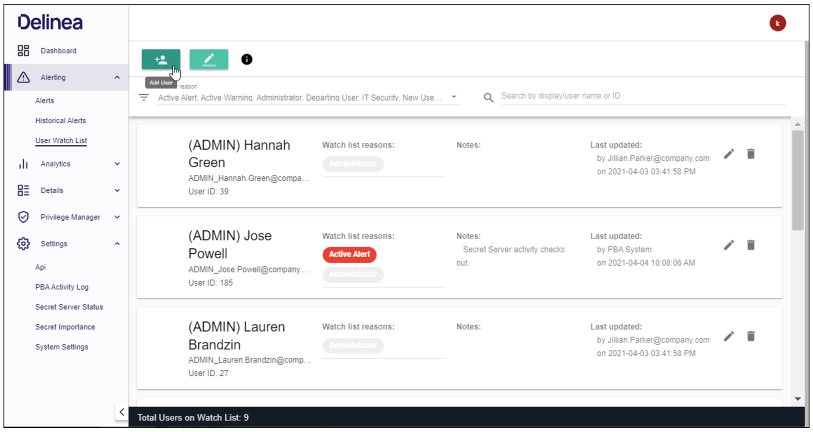
User Watch List

The **User Watch List** page provides a convenient location to track users of interest and easily access information about each.

By default, the Privileged Behavior Analytics (PBA) System adds to the Watch List new users and those with active Alerts and Warnings.

Upon clearing Alerts and Warnings, or when a new User has been active for 30 days, the System removes them from the Watch List. These automated actions can be disabled from the **System Settings** page (see "Privileged Behavior Analytics Administration " on page 100 for more information).

On the right side of each User’s Watch List entry are buttons to edit (reasons and notes) or delete the entry. For Secret Server customers that have a Secret Server Custom URL, an additional lock icon will appear, which links to the User’s Edit page in Secret Server.



(ADMIN) Hannah Green
ADMIN_Hannah.Green@compa...
User ID: 39
Watch list reasons:
Notes:
Last updated:
by Jillian.Parker@company.com
on 2021-04-03 03:41:58 PM

(ADMIN) Jose Powell
ADMIN_Jose.Powell@company....
User ID: 185
Watch list reasons: Active Alert
Notes:
Secret Server activity checks out.
Last updated:
by PBA System
on 2021-04-04 10:08:06 AM

(ADMIN) Lauren Brandzin
ADMIN_Lauren.Brandzin@comp...
User ID: 27
Watch list reasons:
Notes:
Last updated:
by Jillian.Parker@company.com
on 2021-04-03 03:41:58 PM

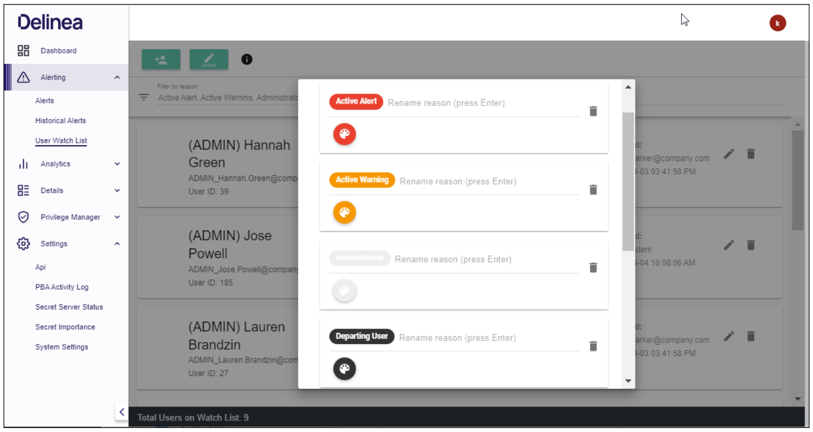
To add a Secret Server URL for direct linking:

- in Secret Server, hover over the Admin button in the toolbar
- select Configuration > Edit
- set the **Secret Server Custom URL**—the URL will be passed to Privileged Behavior Analytics in the next metadata upload

Users can be added to the Watch List by clicking the Add User icon at the top right of the page. Multiple new or existing users can be added to the list along with a list of reasons and notes.

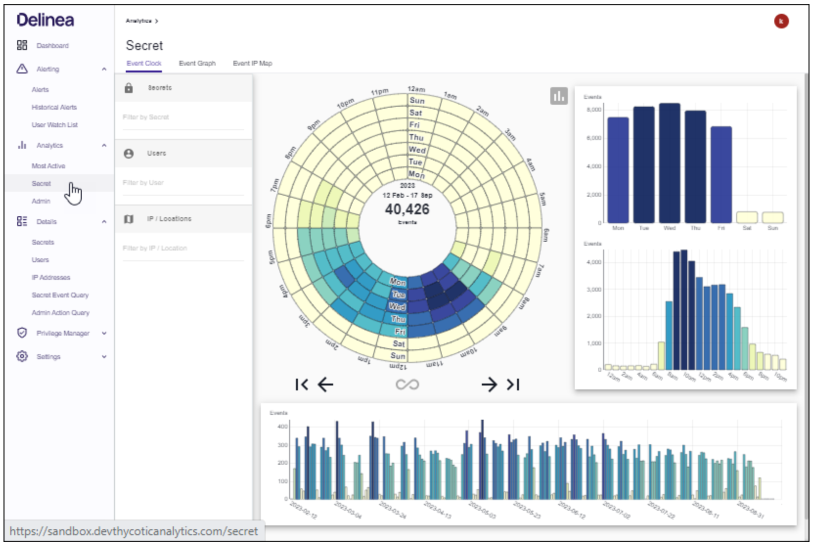
- For existing Watch List users, the reasons and notes will be appended to their current reasons list and notes.

To make changes to a reason, click the **Edit Reasons** button on the top right side of the toolbar. The current list of reasons will appear with options to change the name or color or to delete the reason from the Watch List. These changes affect all Watch Listed Users with the edited reason and are not tracked in the Last Updated information.



Secret Event Clock

The **Secret Event Clock**, in the Analytics section of PBA (**Analytics** > **Secret** > **Event Clock** tab), provides a temporal overview of Secret Server activity. It visualizes the distribution and concentration of activities for a given time range.



The coloring of the graphs range from white to dark blue.

- White means no activity.
- Dark blue means a lot of activity.

The center of the circular chart displays the number of events represented and the date range when they occurred.

- You can filter the temporal data by searching in the three boxes on the left for a:
  - Secret, Folder, or Secret Importance Level
  - User, Account Type, Group, Name, or User ID
  - IP address, City, Region, or Country
- This will refresh the graphs to reflect only events within the data range that are related to that Secret, User, or IP.
- If you refine by a Secret and wish to see which Users accessed that Secret on a particular day or at a certain time, you can right-click on the corresponding bar in any of the graphs and then click on the name of the Secret.
- Likewise, if you refine by a User and wish to see which Secrets they accessed on a particular day or at a certain time, you can right-click on the corresponding bar and click on the name of the User.

To move back and forth through specific weeks, use the left and right arrows at the base of the circular chart. If you wish to hide the side and bottom bar charts from the display, you can click the gray chart button to the top right of the circular chart.

Secret Event Graph

The Secret Event Graph can be used to explore the behaviors of Secret Server users at a glance.

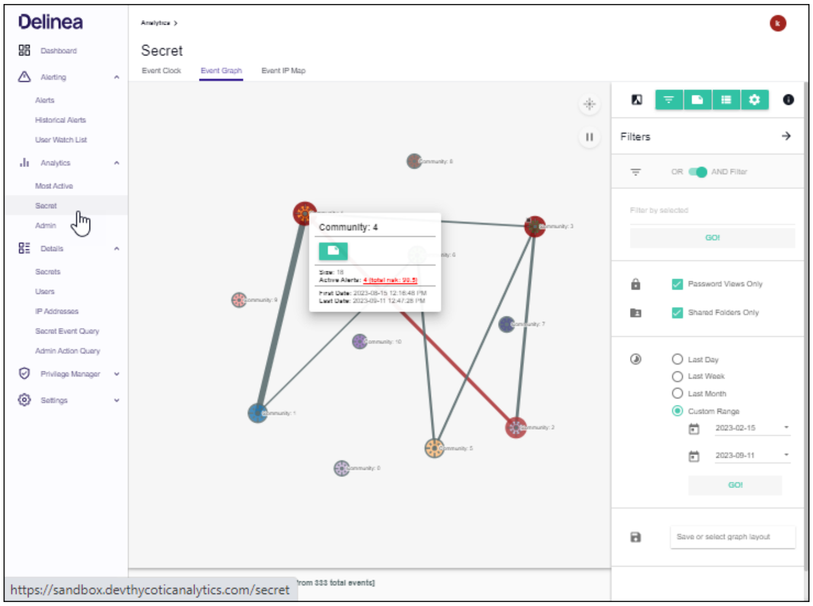
The graph is animated by default. You can pause the animation by clicking on the pause button at the top right of the graph area. Above the pause button is another button that will allow you to expand or collapse all nodes with a single click. You can also expand or collapse individual clusters by double clicking on them.

Each initial node circle, or Community, is a collection of users who are accessing similar Secrets. The larger the Community, the more users and Secrets there are inside it.

Communities may also have lines, or links, connecting them to other Communities. The links are an indication that a user or users within a Community are accessing Secrets that exist in another Community, indicating a possibility of accesses outside a user's responsibility. Thicker links represent more accesses between Communities.

When you expand (double-click) a Community, you can see all the users and Secrets it contains. The size of each node indicates how many accesses it has and the thickness of links follows the same principal.

Community, User, and Secret nodes may be outlined by a shade of red. If this is the case, there is an active alert for a user and/or Secret and more information can be found by right clicking on the affected nodes and observing active alerts or by navigating to the **Alerts > Privileged Behavior Alerts** page.



Community: 4

Size: 18
Active Alerts: 4 (total risk: 90.5)
First Date: 2023-08-15 12:16:48 PM
Last Date: 2023-09-11 12:47:28 PM

☑ Password Views Only
☑ Shared Folders Only

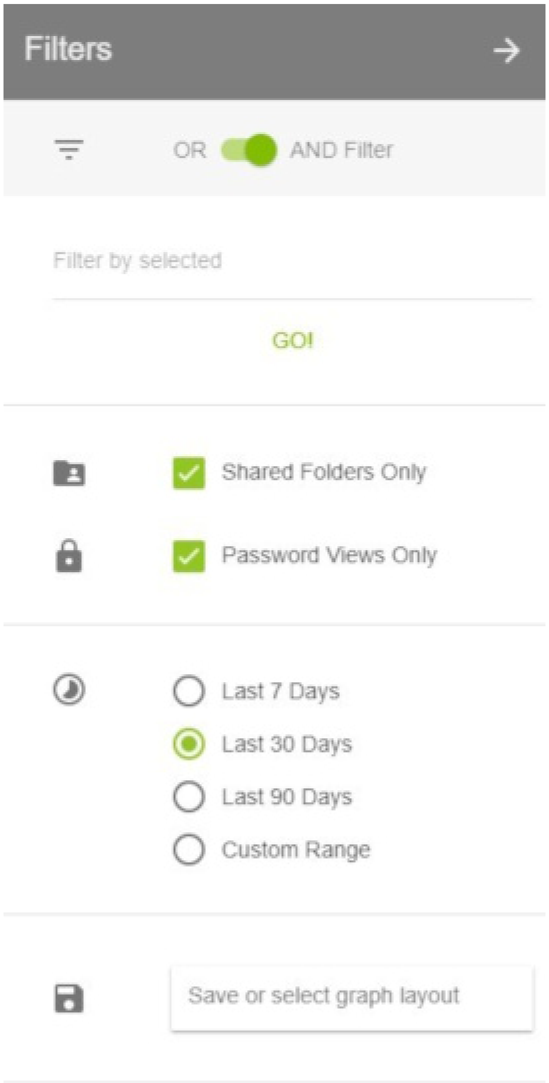
○ Last Day
○ Last Week
○ Last Month
● Custom Range
2023-02-15
2023-09-11

Whether a Community is expanded or not, you can right click on any node or link on the Secret Event Graph to add notes or see further details.

The icon to the left of the menu buttons will toggle the Graph between light and dark themes.

Filters

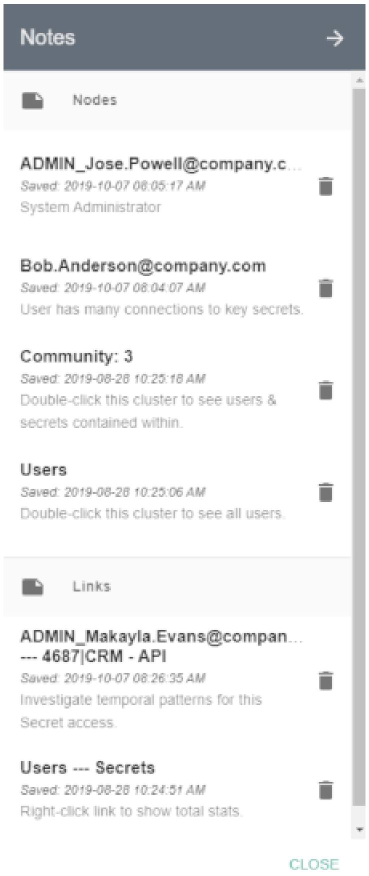
The Filters menu (three horizontal lines button) provides options to limit the number of nodes and links displayed.



- **OR AND Filter**: determines how filters will be applied to the Secret Event Graph
- **Filter by selected**: lets you filter the Secret Event Graph display by Secret, User, Group, Folder, IP Address, Secret Importance, and Template
- **Shared Folders Only**: unchecking this box will add Secret access activity from users' Personal Folders in Secret Server
- **Password Views Only**: turned on by default, this shows only Secret accesses, which include: web launches, passwords displayed, passwords copied to clipboard, Secrets edited, and Secrets exported; if turned off, all other Secret activity will be shown
- **Time Ranges**: by default, the Secret Event Graph will show activity from the last week; the Custom Range option allows selecting a start and end date to refine activity displayed
- **Save or select graph layout**: you may choose to save filtered views of the Secret Event Graph to quickly recall significant access landscapes

Notes

The Notes menu can be accessed by clicking the green button depicting a note with a folded corner at the top right of the Secret Event Graph page.



Notes →

Nodes

ADMIN_Jose.Powell@company.c...
Saved: 2019-10-07 08:05:17 AM
System Administrator

Bob.Anderson@company.com
Saved: 2019-10-07 08:04:07 AM
User has many connections to key secrets.

Community: 3
Saved: 2019-08-28 10:25:18 AM
Double-click this cluster to see users & secrets contained within.

Users
Saved: 2019-08-28 10:25:06 AM
Double-click this cluster to see all users.

Links

ADMIN_Makayla.Evans@compan...
--- 4687|CRM - API
Saved: 2019-10-07 08:26:35 AM
Investigate temporal patterns for this Secret access.

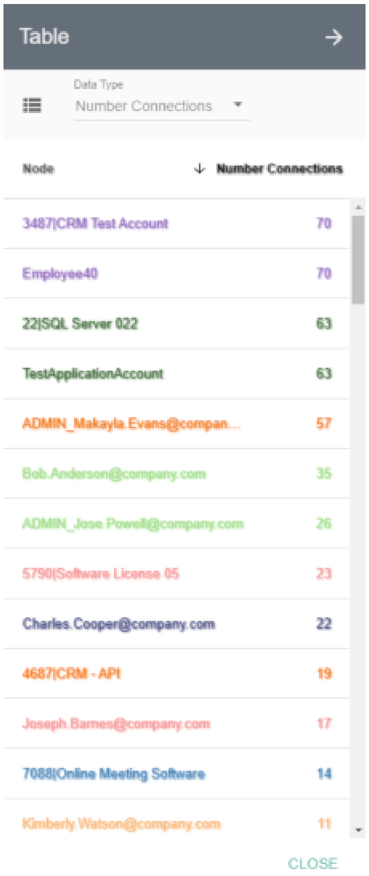
Users --- Secrets
Saved: 2019-08-28 10:24:51 AM
Right-click link to show total stats.

CLOSE

- All notes on nodes and links are listed here. You can edit any note by clicking on it or delete a note by clicking on the trashcan icon to the right of the note.
- Notes can be created by right-clicking on a node (circle) or link (line) in the Secret Event Graph. A small square of the color selected will appear on the node or link after the note is created.
- Hovering over the square or a note in the Notes menu will briefly highlight the note square on the Graph.

Table

The Table menu can be accessed by clicking the green button between the Notes and Tools buttons at the top right of the Secret Event Graph page.



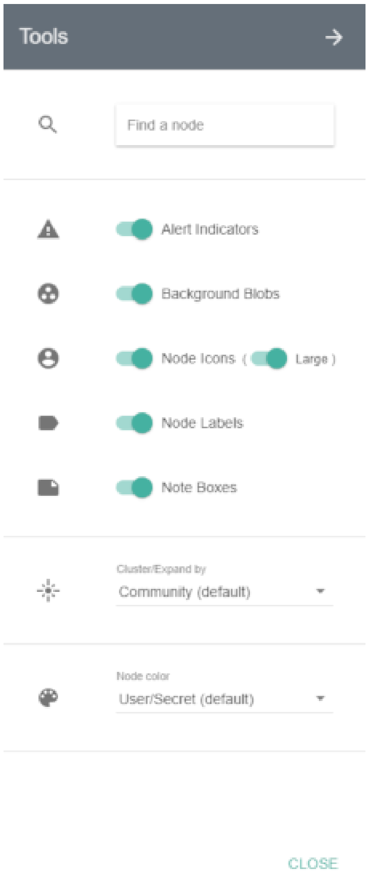
Node	Number Connections
3487|CRM Test Account	70
Employee40	70
22|SQL Server 022	63
TestApplicationAccount	63
ADMIN_Makayla.Evans@compan...	57
Bob.Anderson@company.com	35
ADMIN_Jose.Powell@company.com	26
5790|Software License 05	23
Charles.Cooper@company.com	22
4687|CRM - API	19
Joseph.Barnes@company.com	17
7088|Online Meeting Software	14
Kimberly.Watson@company.com	11

This menu gives you a full, sortable text-based list of all User and Secret node metrics. Placing your mouse over any of the node names in the lists will highlight that node on the Secret Event Graph if the Community it is in is expanded.

- **Community** lists User and Secret nodes and the Community number they are in
- **Secret/User** lists User and Secret node names and whether each is a User or Secret
- **Number Connections** lists User and Secret nodes and how many accesses they have had or performed on other nodes
- **Number Unique** lists User and Secret nodes and how many unique Secrets or users, respectively, they are connected to
- **Last Active** lists User and Secret nodes and the timestamp of the last activity each had
- **First Active** lists User and Secret nodes and the timestamp of the first activity each had recorded in PBA
- **Social Network Metrics** lists User and Secret nodes and the numerical value of the selected metric

Tools

The Tools menu (cogwheel button) allows you to customize what is displayed on the graph.



Tools

Find a node

Alert Indicators

Background Blobs

Node Icons (Large)

Node Labels

Note Boxes

Cluster/Expand by: Community (default)

Node color: User/Secret (default)

- **Search**: At the top of the menu is a search field where you can enter the name of a User or Secret to highlight that specific node on the Secret Event Graph. Press Enter to repeat the animation.
- **Alert Indicators**: turned on by default, this will outline Secret and User nodes in a shade of red based on whether it has an active alert; the redder a node is the higher the total alert risk
- **Background Blobs**: turned on by default, these surround all nodes in an expanded Community with a color similar to that of the collapsed Community
- **Node Icons**: turned on by default, this shows icons in place of circles for each user or Secret node. The size of the icon can be changed using the **Large** switch.
- **Node Labels**: turned on by default, these are Community numbers, Secret names, and User names shown next to each node
- **Note Boxes**: turned on by default, these represent notes that have been placed on any nodes or links
- **Cluster/Expand by**: by default, all nodes will be clustered by Communities; you can select the dropdown here to choose to cluster nodes by Secrets and users
- **Node Color**: there are multiple options for choosing how the nodes within an expanded Community are colored:
  - **Community**: all Secret and User nodes will be the color of the Community when it is collapsed
  - **Secret/User**: the User nodes are colored blue and Secret nodes are colored green (default coloring)

- **Number Connections**: Secret and User node colors will range from white to red; the redder a node is, the more active it is
- **Number Unique**: Secret nodes will always be white; User nodes will range from white to red, and the redder a node is, the more unique accesses it has
- **Last Active**: Nodes will range from white to red with recent activity being more red
- **First Active**: Nodes will range from white to red with earlier activity being more red
- **Social Network Metrics**: these options can reveal important Secrets or users in the network

Secret Event IP Map

The **Secret Event IP Map** summarizes Secret Server activity by IP address and location. This is useful for Secret Servers that allow access from external IP addresses.

Summary views and information provide a high-level understanding of recent and historical Secret events. Any anomalous locations in the data can be quickly observed, analyzed, and acted upon.

Map Key

The map shows by default the last week of IP address counts (purple circles) and active alerts (red triangles). You can click these features for further information.

Circle features sometimes have a gray or black outline, which means they are located only to the region (state) or country level, respectively.

Map Navigation

The Map can be navigated like most web-based maps:

- Pan to different locations by clicking on an open area and dragging the mouse
- Zoom in or out using the mouse wheel, the buttons on the upper left, double-clicking (+ Shift), or dragging the mouse while holding Shift to select a zoom box

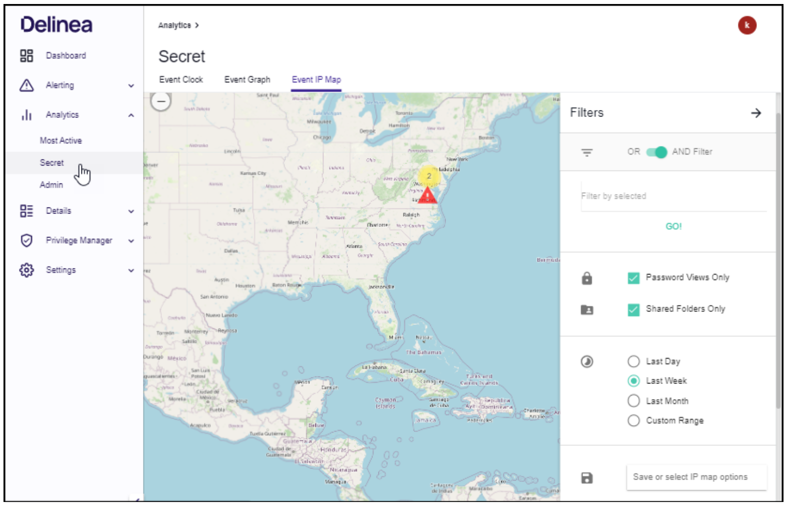
Note: If no data appear, please go to the Filters menu and try turning off filters or expanding the time range. From the System Settings page, a default location can be entered for cases where only internal (private) IP addresses are present in the data.

Filters

The **Filters** menu (first menu button) provides options to limit data displayed based on user, Secret, IP address, location, and several related attributes.

- **OR AND Filter**: determines whether selected filters will be considered separately (OR) or together (AND)
- **Filter by selected**: filters the Map display by Secret, user, group, folder, IP Address, location, Secret importance, and template
- **Shared Folders Only**: unchecking this box will add Secret activity from users’ personal folders in Secret Server

- **Password Views Only**: turned on by default, this shows only Secret accesses, which include: web launches, passwords displayed, passwords copied to clipboard, Secrets edited, and Secrets exported; if turned off, all other Secret activity will be shown
- **Time Ranges**: by default, the Map will show activity from the last week; the Custom Range option allows selecting a start and end date to refine activity displayed
- **Save or select IP map options**: save filtered views of the Map to quickly recall significant events or complex filter combinations



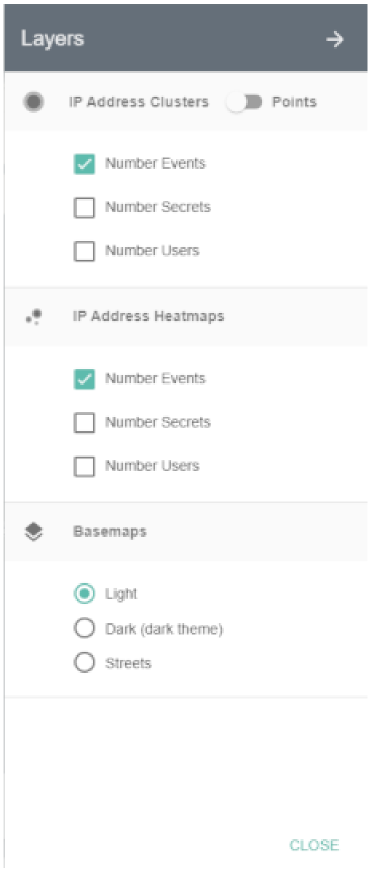
☑ Password Views Only
☑ Shared Folders Only
○ Last Day
● Last Week
○ Last Month
○ Custom Range

Layers

The **Layers** menu (second menu button) contains options to show circle layers as clusters (aggregated nearby points) or as individual points for the number of events, Secrets, or users active at each IP address.

There are also heatmaps and different basemaps that can be selected.

- Selecting the **Dark** basemap will change the entire map application to the dark theme.



Layers →

● IP Address Clusters ⬤ Points

☑ Number Events

□ Number Secrets

□ Number Users

IP Address Heatmaps

☑ Number Events

□ Number Secrets

□ Number Users

Basemaps

● Light

○ Dark (dark theme)

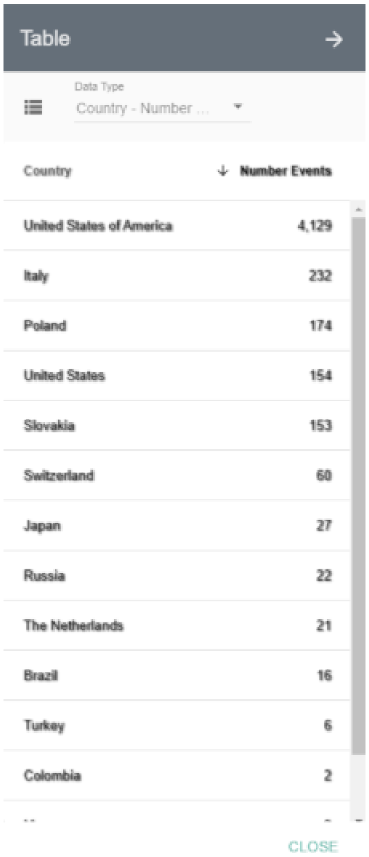
○ Streets

CLOSE

Table

The Table menu (third menu button) provides a sortable text-based list of key metrics (below) related to IP addresses. Placing your mouse over any of the rows in the lists will highlight a point or country on the Map.

- **Country – Number Events**: shows the total number of IP events within each country
- **IP – Number Events**: shows list of IP addresses with the total number of events for each
- **IP – Number Secrets**: shows list of IP addresses with the total number of Secrets accessed or modified from each
- **IP – Number Users**: shows list of IP addresses with the total number of users for each
- **IP – First Active**: shows IP address list with date of first activity observed
- **IP – Last Active**: shows IP address list with date of last activity observed
- **IP – City**: shows IP address list with city of the location (if available)
- **IP – Region**: shows IP address list with region (state) of the location (if available)
- **IP – Country**: shows IP address list with country of the location



Data Type
Country - Number ...

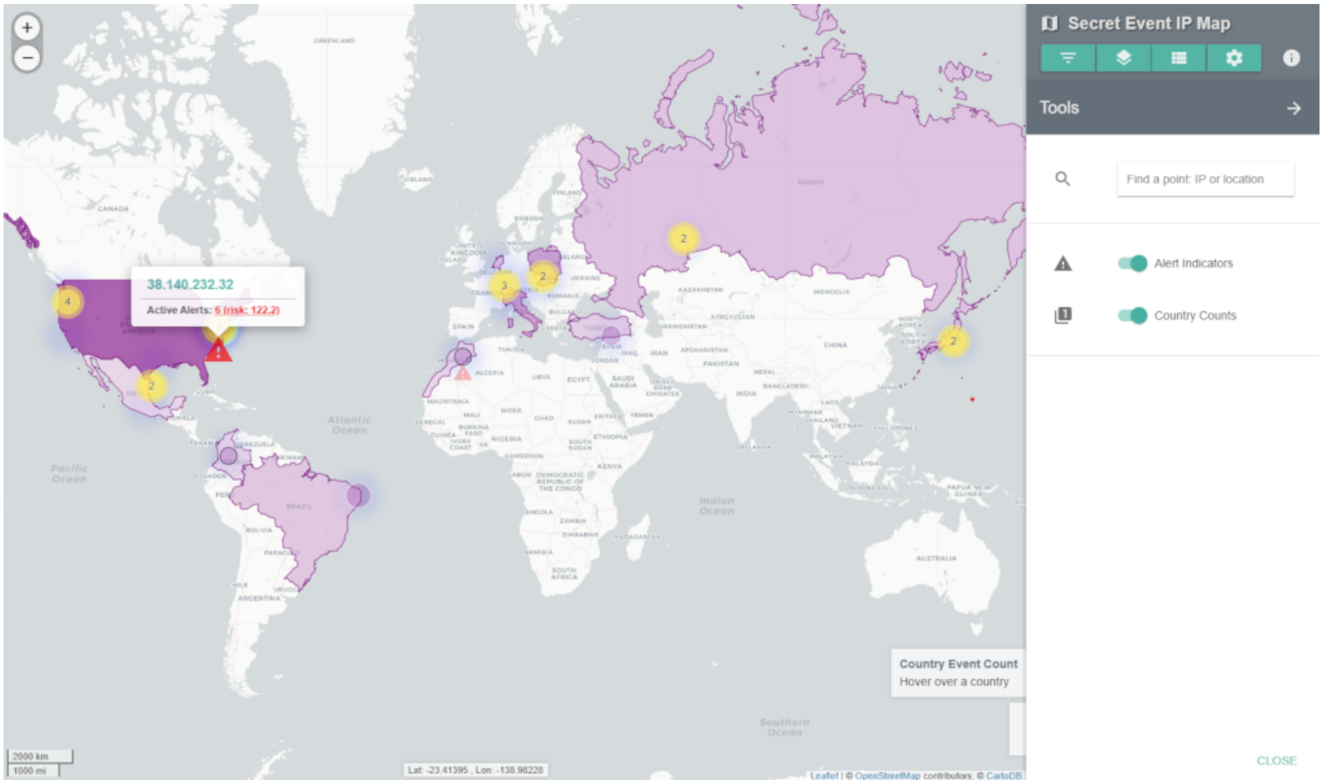
Country	Number Events
United States of America	4,129
Italy	232
Poland	174
United States	154
Slovakia	153
Switzerland	60
Japan	27
Russia	22
The Netherlands	21
Brazil	16
Turkey	6
Colombia	2

Tools

The **Tools** menu (fourth menu button) provides a search function to find a specific IP address, city, region (state), or country among the data points currently loaded to the Map. Clicking on a result will pop up details and re-zoom the map to the selected IP address.

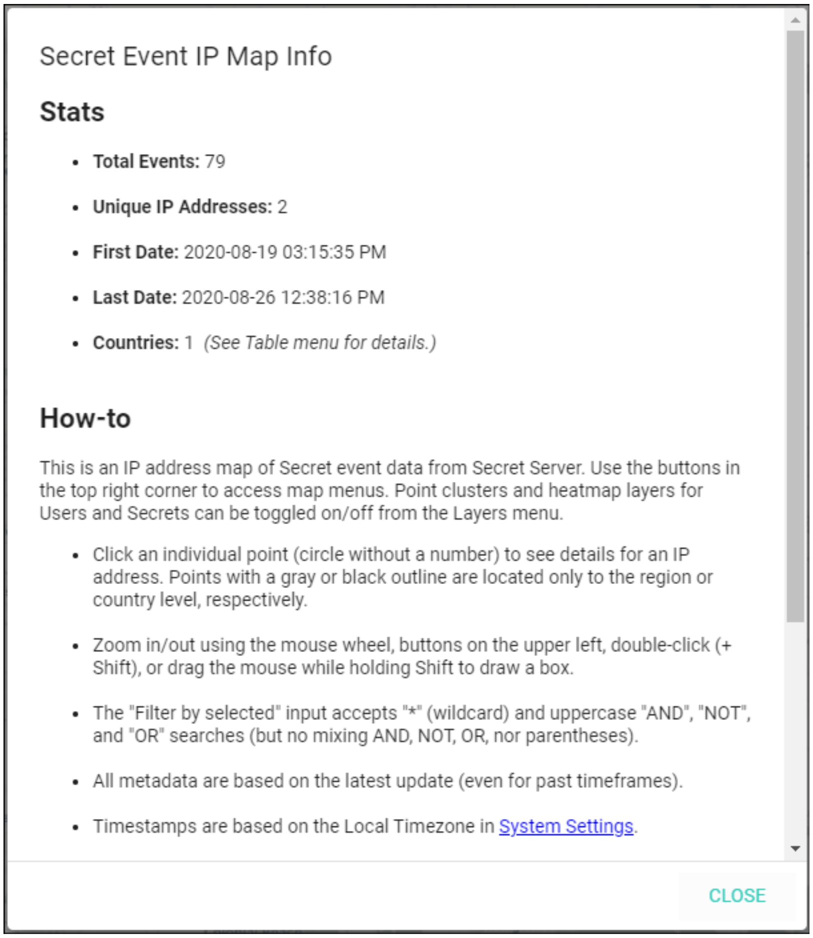
The Tools menu also contains two additional data layer options:

- **Alert Indicators** show red triangles for IP addresses that have active alerts or warnings. Clicking on a triangle will show details on the number of alerts and total risk score.
- **Country Counts** show a semi-transparent layer shaded by the number of events taking place in each country. Clicking on a country will re-zoom the map to the selected country, and hovering the mouse over it will show the country name, flag, and number of events.


Secret Event IP Map
Tools
Find a point: IP or location
Alert Indicators
Country Counts
CLOSE
38.140.232.32
Active Alerts: 6 (risk: 122.2)
Country Event Count
Hover over a country
2000 km
1000 mi
Lat: -23.41395 , Lon: -138.98228
Leaflet | © OpenStreetMap contributors, © CartoDB

Secret Event IP Map Info

Next to the menu buttons is an info icon that launches the **Secret Event IP Map Info** box, which contains basic statistics on the map data displayed, map instructions, and disclaimers.



Secret Event IP Map Info

Stats

- **Total Events:** 79
- **Unique IP Addresses:** 2
- **First Date:** 2020-08-19 03:15:35 PM
- **Last Date:** 2020-08-26 12:38:16 PM
- **Countries:** 1 *(See Table menu for details.)*

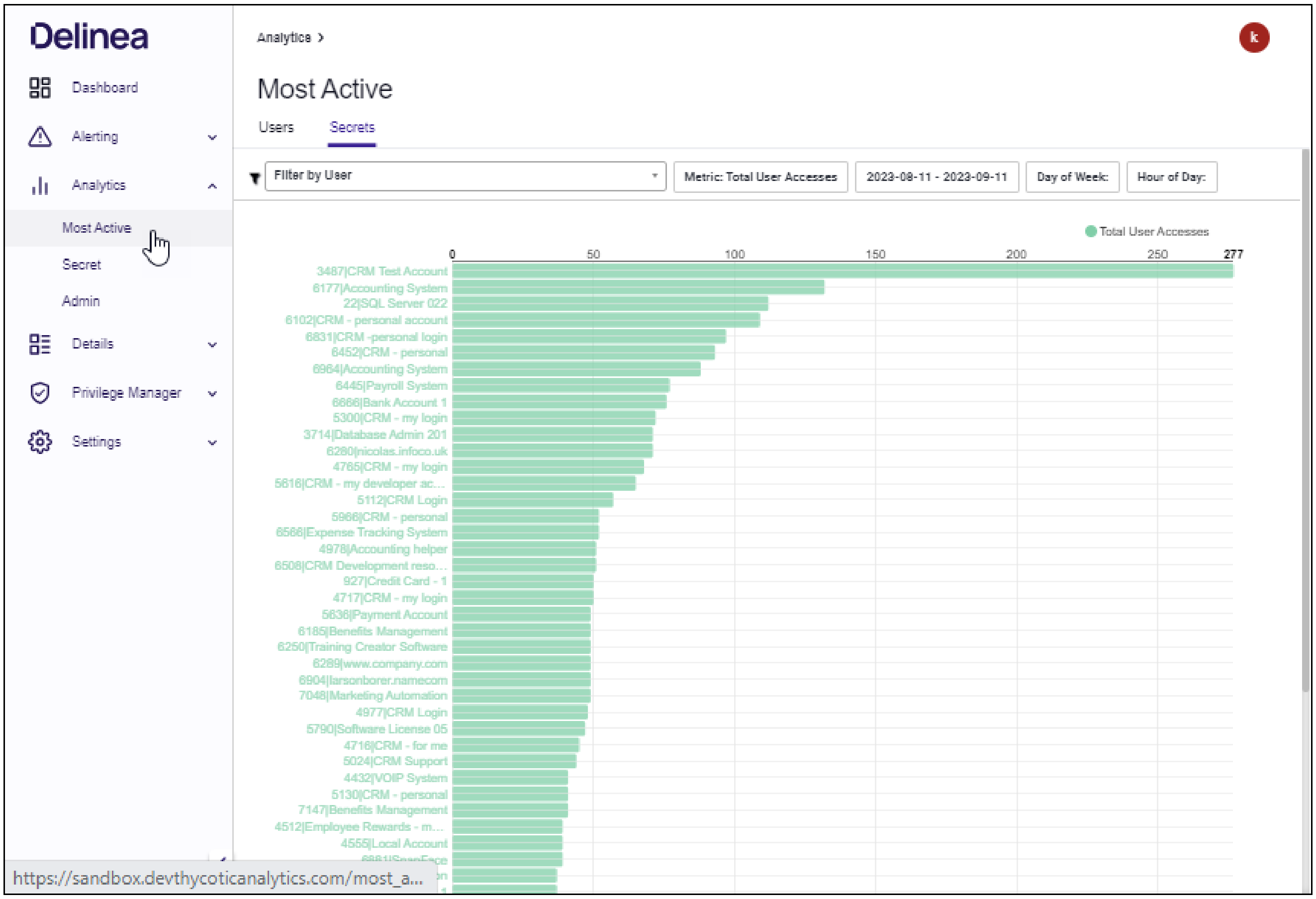
How-to

This is an IP address map of Secret event data from Secret Server. Use the buttons in the top right corner to access map menus. Point clusters and heatmap layers for Users and Secrets can be toggled on/off from the Layers menu.

- Click an individual point (circle without a number) to see details for an IP address. Points with a gray or black outline are located only to the region or country level, respectively.
- Zoom in/out using the mouse wheel, buttons on the upper left, double-click (+ Shift), or drag the mouse while holding Shift to draw a box.
- The "Filter by selected" input accepts "*" (wildcard) and uppercase "AND", "NOT", and "OR" searches (but no mixing AND, NOT, OR, nor parentheses).
- All metadata are based on the latest update (even for past timeframes).
- Timestamps are based on the Local Timezone in System Settings.

Most Active Secrets

Most Active Secrets ranks the top 50 most accessed Secrets. To see this, navigate to **Analytics** > **Most Active**. Then, click the **Secrets** tab.

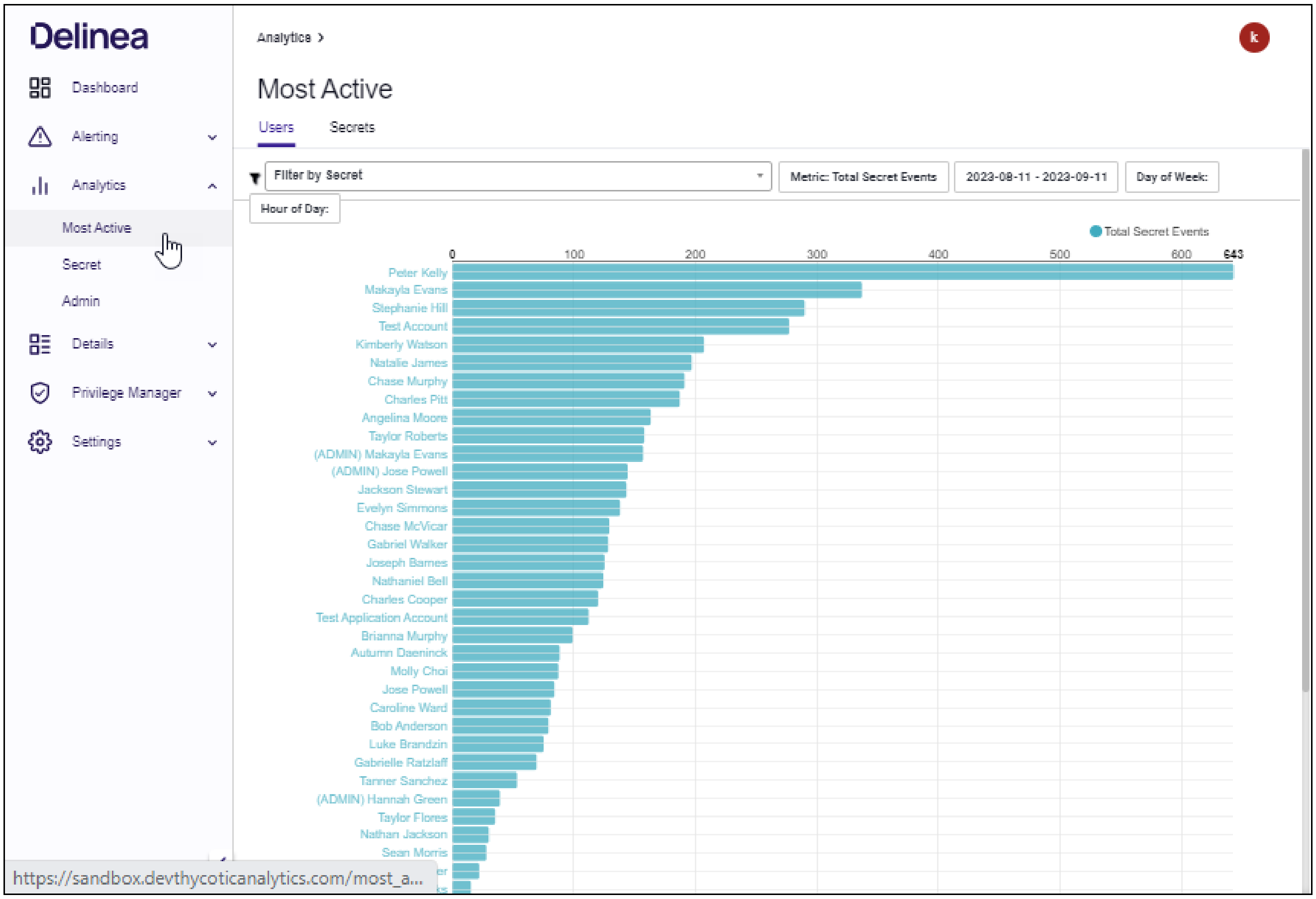


The list contains the Secret ID, Secret Name, and number of access events for each of the 50 secrets, using a bar chart as visual reference.

- By default, you will see the top 50 Secrets in your Secret Server environment for the past month.
- You can further filter the list by User, total or distinct accesses, or specific timeframe.
- Clicking on a Secret in the list will take you to its **Secret Details** page.

Most Active Users

Most Active Users ranks the top 50 most active Users in your Secret Server environment. You can see your top 50 most active users by navigating to **Analytics** > **Most Active**. Then, click the **Users** tab.



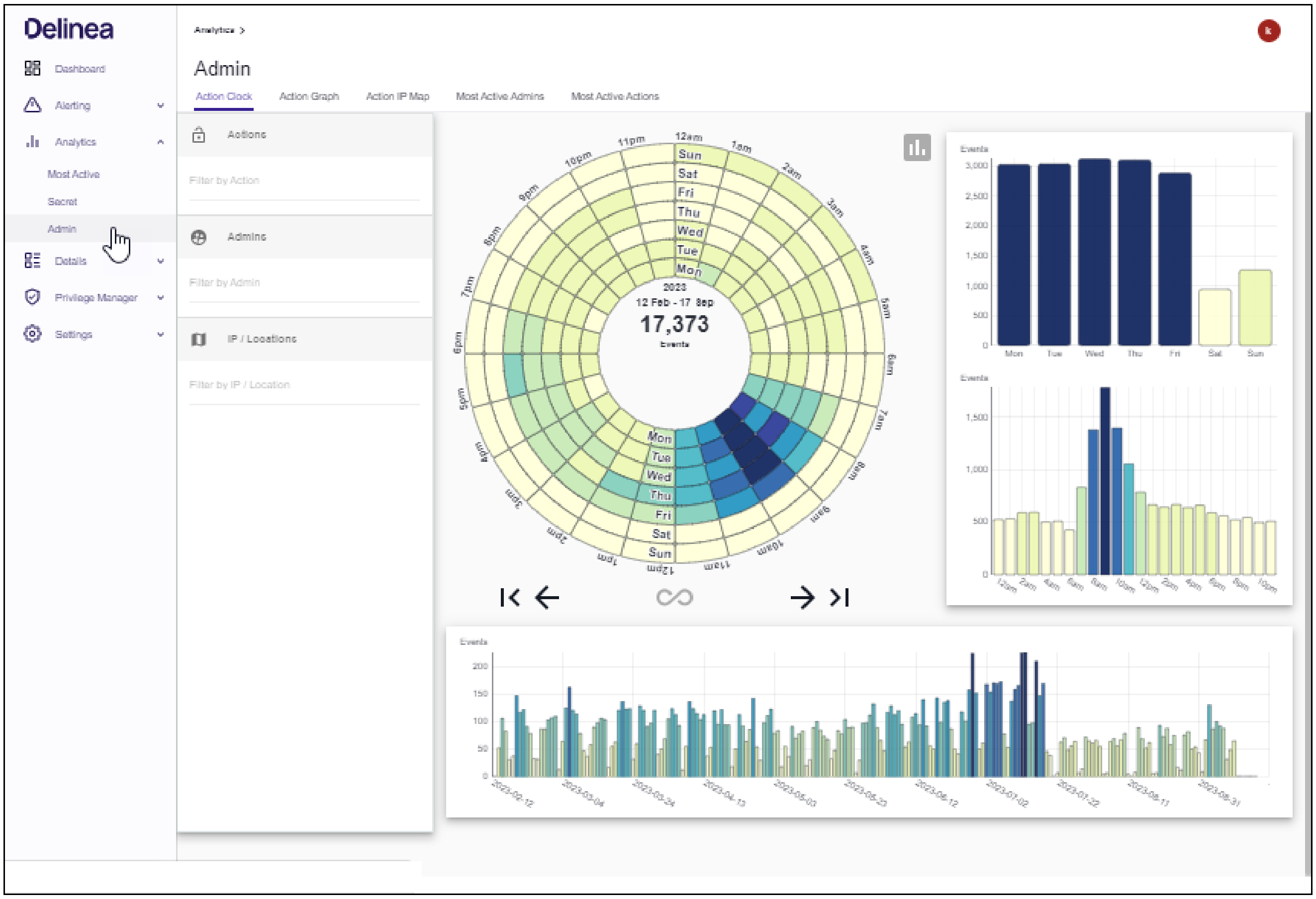
The list contains the User Display Name, and number of Accesses to Secrets, with a bar chart as visual reference.

- By default, you will see the top 50 Users in your Secret Server environment for the past month.
- You can further filter the list by Secret, total or distinct accesses, or specific timeframe.
- Clicking on a User in the list will take you to the **User Details** page for that User.

Admin Actions

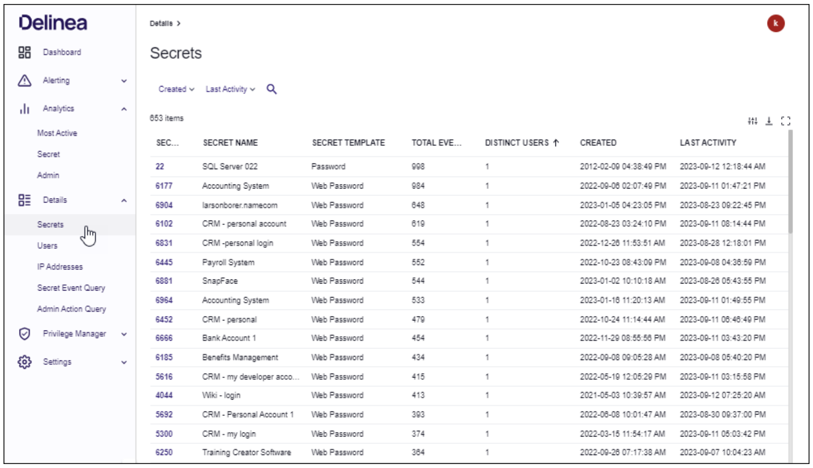
PBA also contains a suite of analytics based on Administrator Actions in Secret Server. Navigate to **Analytics > Admin** to view the available pages.

Similar to the Secret Event Clock, Graph, and IP Map, there are pages that show administrators and Secret Server Actions instead of users and Secrets. Likewise, the Most Active Actions and Most Active Admins pages allow you to filter down the top 50 of each and easily access details pages.



Secret Details

The **Secret Details** page can be used to investigate how a Secret is being accessed from the perspective of many types of data collected on it. You can access Secret Details by navigating to **Details** > **Secrets**.



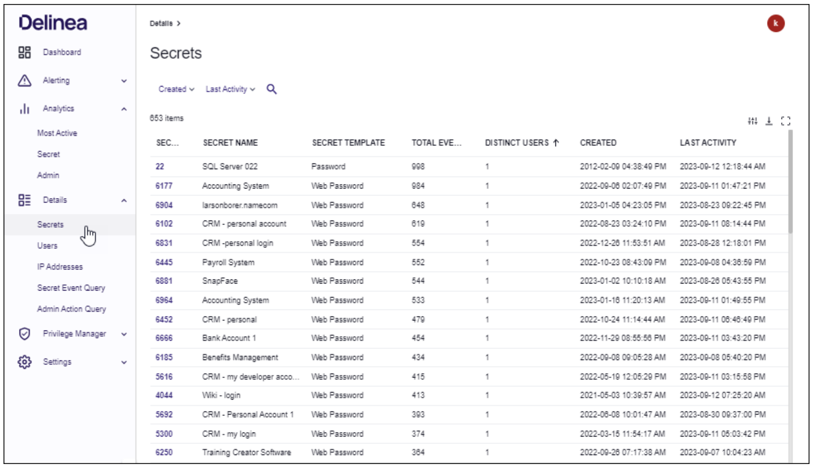
Secrets

653 items

SEC...	SECRET NAME	SECRET TEMPLATE	TOTAL EVE...	DISTINCT USERS ↑	CREATED	LAST ACTIVITY
22	SQL Server 022	Password	998	1	2012-02-09 04:38:49 PM	2023-09-12 12:18:44 AM
6177	Accounting System	Web Password	984	1	2022-09-06 02:07:49 PM	2023-09-11 01:47:21 PM
6904	larsonborer.namecom	Web Password	648	1	2023-01-05 04:23:05 PM	2023-08-23 09:22:45 PM
6102	CRM - personal account	Web Password	619	1	2022-08-23 03:24:10 PM	2023-09-11 08:14:44 PM
6831	CRM -personal login	Web Password	554	1	2022-12-26 11:53:51 AM	2023-08-28 12:18:01 PM
6445	Payroll System	Web Password	552	1	2022-10-23 08:43:09 PM	2023-09-08 04:36:59 PM
6881	SnapFace	Web Password	544	1	2023-01-02 10:10:18 AM	2023-08-26 05:43:55 PM
6964	Accounting System	Web Password	533	1	2023-01-16 11:20:13 AM	2023-09-11 01:49:55 PM
6452	CRM - personal	Web Password	479	1	2022-10-24 11:14:44 AM	2023-09-11 06:46:49 PM
6666	Bank Account 1	Web Password	454	1	2022-11-29 08:55:56 PM	2023-09-11 03:43:20 PM
6185	Benefits Management	Web Password	434	1	2022-09-08 09:05:28 AM	2023-09-08 05:40:20 PM
5616	CRM - my developer acco...	Web Password	415	1	2022-05-19 12:05:29 PM	2023-09-11 03:15:58 PM
4044	Wiki - login	Web Password	413	1	2021-05-03 10:39:57 AM	2023-09-12 07:25:20 AM
5692	CRM - Personal Account 1	Web Password	393	1	2022-06-08 10:01:47 AM	2023-08-30 09:37:00 PM
5300	CRM - my login	Web Password	374	1	2022-03-15 11:54:17 AM	2023-09-11 05:03:42 PM
6250	Training Creator Software	Web Password	364	1	2022-09-26 07:17:38 AM	2023-09-07 10:04:23 AM

The Secret Details page lists all Secrets with Secret ID, Secret Name, Secret Template, the total number of events (Secret accesses plus modifications), number of Distinct Users that have accessed the Secret, the Created date, and the date of Last Activity.

If you click on any of the Secret names you will be directed to that Secret's Details page. The **Secret Details** tab lists key statistics such as total number of events and users, time range, and last event action



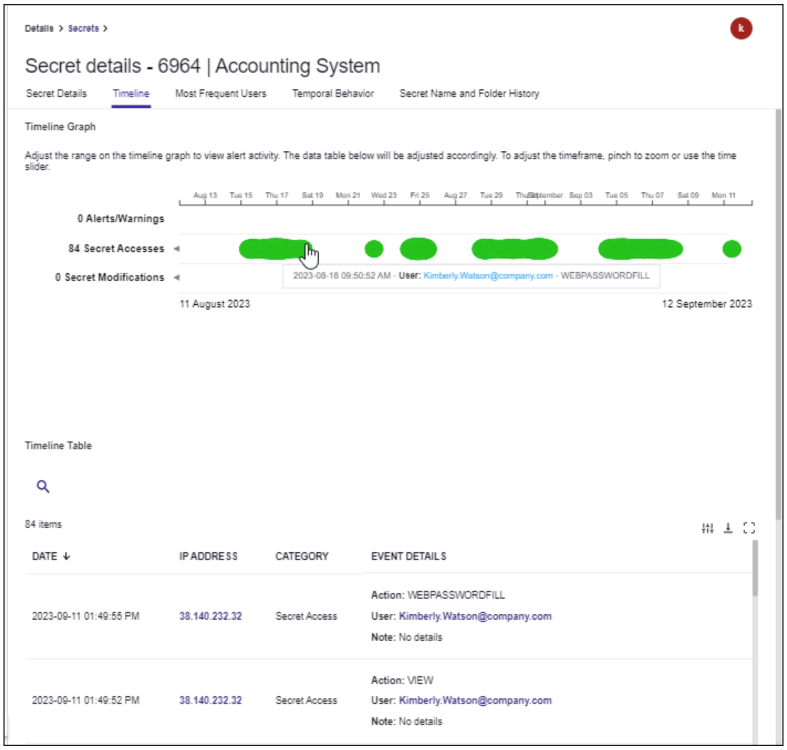
Secrets

653 items

SEC...	SECRET NAME	SECRET TEMPLATE	TOTAL EVE...	DISTINCT USERS ↑	CREATED	LAST ACTIVITY
22	SQL Server 022	Password	998	1	2012-02-09 04:38:49 PM	2023-09-12 12:18:44 AM
6177	Accounting System	Web Password	984	1	2022-09-06 02:07:49 PM	2023-09-11 01:47:21 PM
6904	larsonborer.namecom	Web Password	648	1	2023-01-05 04:23:05 PM	2023-08-23 09:22:45 PM
6102	CRM - personal account	Web Password	619	1	2022-08-23 03:24:10 PM	2023-09-11 08:14:44 PM
6831	CRM -personal login	Web Password	554	1	2022-12-26 11:53:51 AM	2023-08-28 12:18:01 PM
6445	Payroll System	Web Password	552	1	2022-10-23 08:43:09 PM	2023-09-08 04:36:59 PM
6881	SnapFace	Web Password	544	1	2023-01-02 10:10:18 AM	2023-08-26 05:43:55 PM
6964	Accounting System	Web Password	533	1	2023-01-16 11:20:13 AM	2023-09-11 01:49:55 PM
6452	CRM - personal	Web Password	479	1	2022-10-24 11:14:44 AM	2023-09-11 06:46:49 PM
6666	Bank Account 1	Web Password	454	1	2022-11-29 08:55:56 PM	2023-09-11 03:43:20 PM
6185	Benefits Management	Web Password	434	1	2022-09-08 09:05:28 AM	2023-09-08 05:40:20 PM
5616	CRM - my developer acco...	Web Password	415	1	2022-05-19 12:05:29 PM	2023-09-11 03:15:58 PM
4044	Wiki - login	Web Password	413	1	2021-05-03 10:39:57 AM	2023-09-12 07:25:20 AM
5692	CRM - Personal Account 1	Web Password	393	1	2022-06-08 10:01:47 AM	2023-08-30 09:37:00 PM
5300	CRM - my login	Web Password	374	1	2022-03-15 11:54:17 AM	2023-09-11 05:03:42 PM
6250	Training Creator Software	Web Password	364	1	2022-09-26 07:17:38 AM	2023-09-07 10:04:23 AM

The tabs on the Secret Details page includes the following tabs:

- **Activity Timeline**: shows all activity for the Secret, including alerts and warnings, accesses, and modifications as well as timestamps, IP address, and event details. Mouse over a colored circle for details on a particular event. the chart can be panned left and right by dragging; zooming is achieved by scrolling, which also filters data in the table.



Secret details - 6964 | Accounting System

Timeline Graph

Adjust the range on the timeline graph to view alert activity. The data table below will be adjusted accordingly. To adjust the timeframe, pinch to zoom or use the time slider.

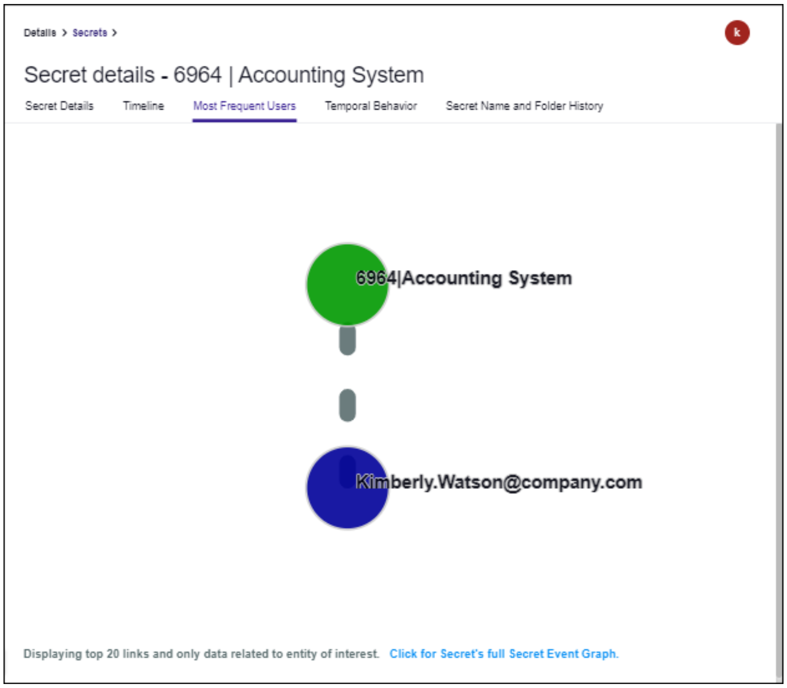
2023-08-18 09:50:52 AM - **User:** Kimberly.Watson@company.com - WEBPASSWORDFILL

Timeline Table

84 items

DATE ↓	IP ADDRESS	CATEGORY	EVENT DETAILS
2023-09-11 01:49:55 PM	38.140.232.32	Secret Access	**Action:** WEBPASSWORDFILL **User:** Kimberly.Watson@company.com **Note:** No details
2023-09-11 01:49:52 PM	38.140.232.32	Secret Access	**Action:** VIEW **User:** Kimberly.Watson@company.com **Note:** No details

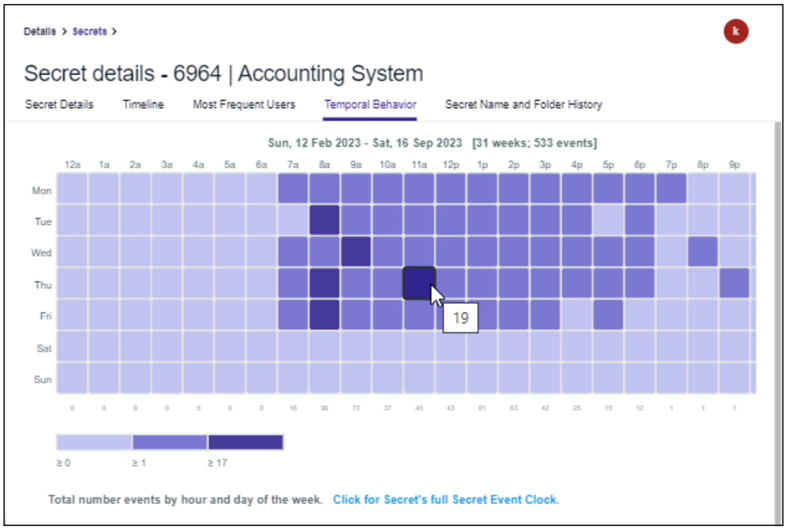
- **Most Frequent Users**: an animated representation of the top 20 users accessing the Secret the most; you can zoom into the graph by scrolling or right-click on any node or link to view more details



Secret details - 6964 | Accounting System

Displaying top 20 links and only data related to entity of interest. Click for Secret's full Secret Event Graph.

- **Temporal Behavior**: a chart showing all temporal data for the Secret organized by time of day and day of the week. The numbers across the bottom indicate the total events involving that Secret for that time of day. The values across the right side indicate the number of events involving that Secret for that day of the week. The legend at the bottom shows the number of events that correlate to the coloring of the chart blocks. Mouse over a block to get the tital number of events for that day and hour.



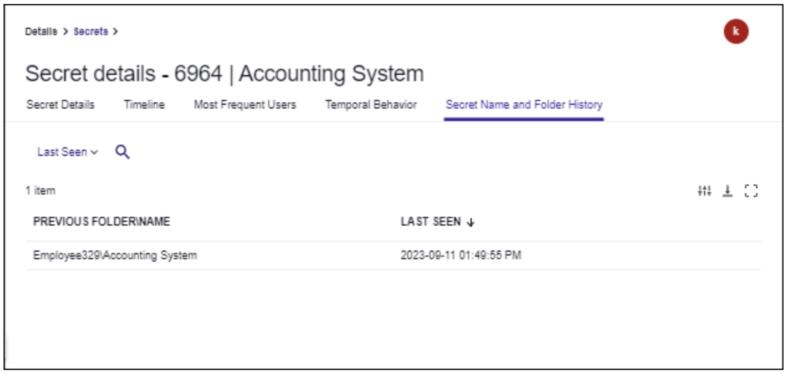
Details > Secrets >

Secret details - 6964 | Accounting System

Sun, 12 Feb 2023 - Sat, 16 Sep 2023 [31 weeks; 533 events]

Total number events by hour and day of the week. Click for Secret's full Secret Event Clock.

- **Secret Name and Folder History**: lists any changes that have been made to the name of the Secret or the folder it is kept in inside Secret Server.



Details > Secrets >

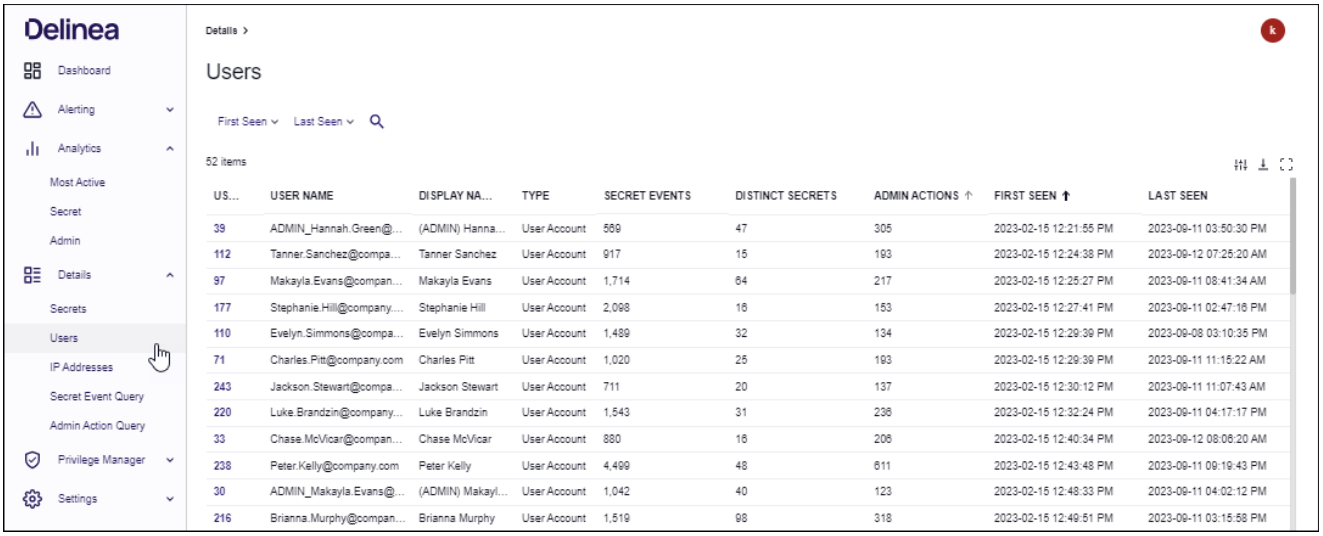
Secret details - 6964 | Accounting System

1 item

PREVIOUS FOLDER\NAME	LAST SEEN ↓
Employee329\Accounting System	2023-09-11 01:49:55 PM

User Details

The **Active Users** page lists all Users, their Display Names, Account Type, total number of times they have accessed or modified Secrets, number of unique Secrets they have accessed, total number of administrative actions they have performed, when they were first seen in Privileged Behavior Analytics, and when they were last active.



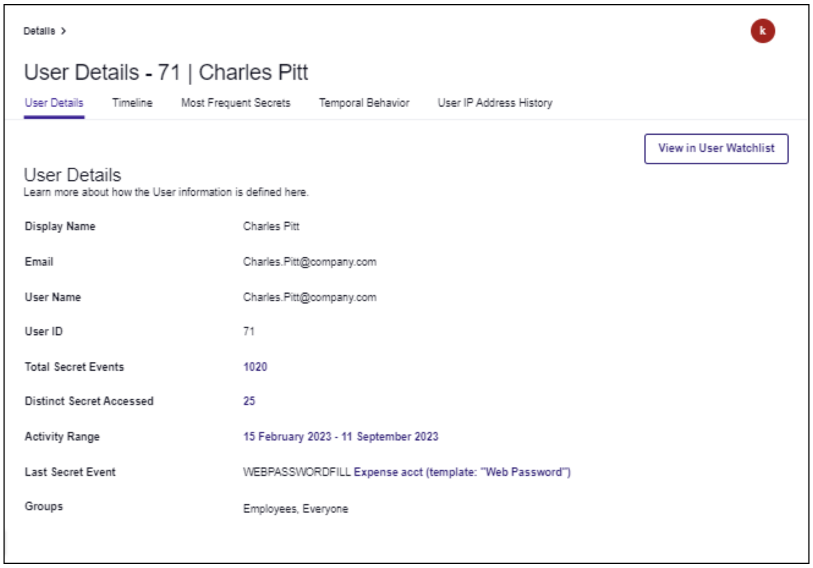
Details >

Users

52 items

US...	USER NAME	DISPLAY NA...	TYPE	SECRET EVENTS	DISTINCT SECRETS	ADMIN ACTIONS ↑	FIRST SEEN ↑	LAST SEEN
39	ADMIN_Hannah.Green@...	(ADMIN) Hanna...	User Account	569	47	305	2023-02-15 12:21:55 PM	2023-09-11 03:50:30 PM
112	Tanner.Sanchez@compa...	Tanner Sanchez	User Account	917	15	193	2023-02-15 12:24:38 PM	2023-09-12 07:25:20 AM
97	Makayla.Evans@compan...	Makayla Evans	User Account	1,714	64	217	2023-02-15 12:25:27 PM	2023-09-11 08:41:34 AM
177	Stephanie.Hill@company....	Stephanie Hill	User Account	2,098	16	153	2023-02-15 12:27:41 PM	2023-09-11 02:47:16 PM
110	Evelyn.Simmons@compa...	Evelyn Simmons	User Account	1,489	32	134	2023-02-15 12:29:39 PM	2023-09-08 03:10:35 PM
71	Charles.Pitt@company.com	Charles Pitt	User Account	1,020	25	193	2023-02-15 12:29:39 PM	2023-09-11 11:15:22 AM
243	Jackson.Stewart@compa...	Jackson Stewart	User Account	711	20	137	2023-02-15 12:30:12 PM	2023-09-11 11:07:43 AM
220	Luke.Brandzin@company...	Luke Brandzin	User Account	1,543	31	236	2023-02-15 12:32:24 PM	2023-09-11 04:17:17 PM
33	Chase.McVicar@compan...	Chase McVicar	User Account	880	16	206	2023-02-15 12:40:34 PM	2023-09-12 08:06:20 AM
238	Peter.Kelly@company.com	Peter Kelly	User Account	4,499	48	611	2023-02-15 12:43:48 PM	2023-09-11 09:19:43 PM
30	ADMIN_Makayla.Evans@...	(ADMIN) Makayl...	User Account	1,042	40	123	2023-02-15 12:48:33 PM	2023-09-11 04:02:12 PM
216	Brianna.Murphy@compan...	Brianna Murphy	User Account	1,519	98	318	2023-02-15 12:49:51 PM	2023-09-11 03:15:58 PM

The **User Details** page is the ideal place to dive deeper into a specific User's behavior from the perspective of many types of data collected on them. To see a user's details page, click on the user's name in the list of users.



Details >

User Details - 71 | Charles Pitt

User Details

Learn more about how the User information is defined here.

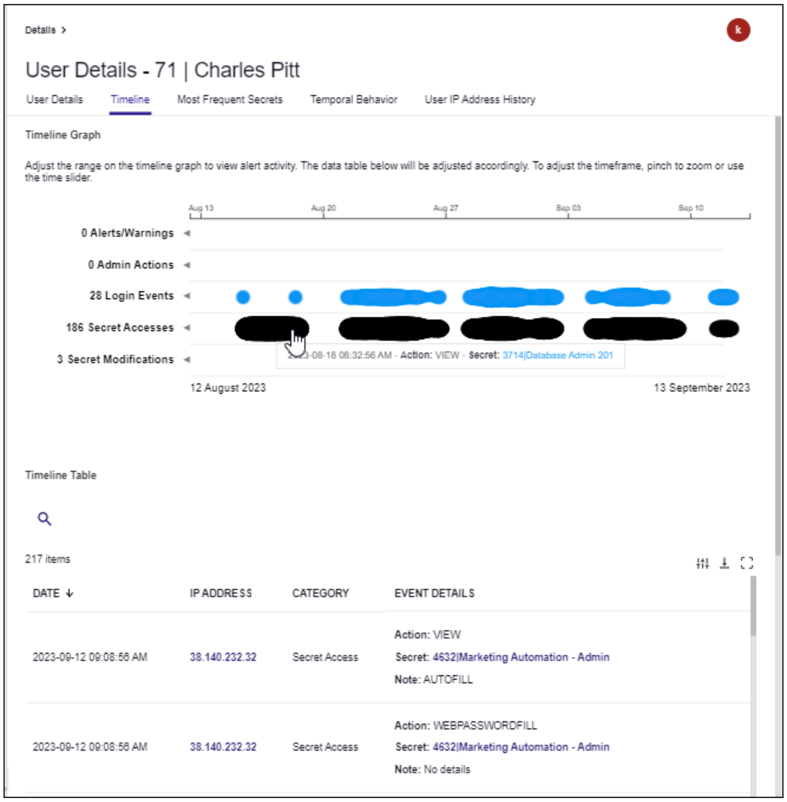
Display Name	Charles Pitt
Email	Charles.Pitt@company.com
User Name	Charles.Pitt@company.com
User ID	71
Total Secret Events	1020
Distinct Secret Accessed	25
Activity Range	15 February 2023 - 11 September 2023
Last Secret Event	WEBPASSWORDFILL Expense acct (template: "Web Password")
Groups	Employees, Everyone

Click the tabs on the User Details page to access additional information.

Activity Timeline: a chart showing when a User has performed Secret accesses, Secret modifications, or administrative actions in Secret Server, or has logged in or out of Secret Server over time.

- each activity is denoted by a symbol shown in the legend at the top
- placing your mouse over any of the symbols in the graph provides more details on what the user did at that time

- grabbing and moving the side buttons on the bottom chart zooms the top chart



Details >

User Details - 71 | Charles Pitt

User Details Timeline Most Frequent Secrets Temporal Behavior User IP Address History

Timeline Graph

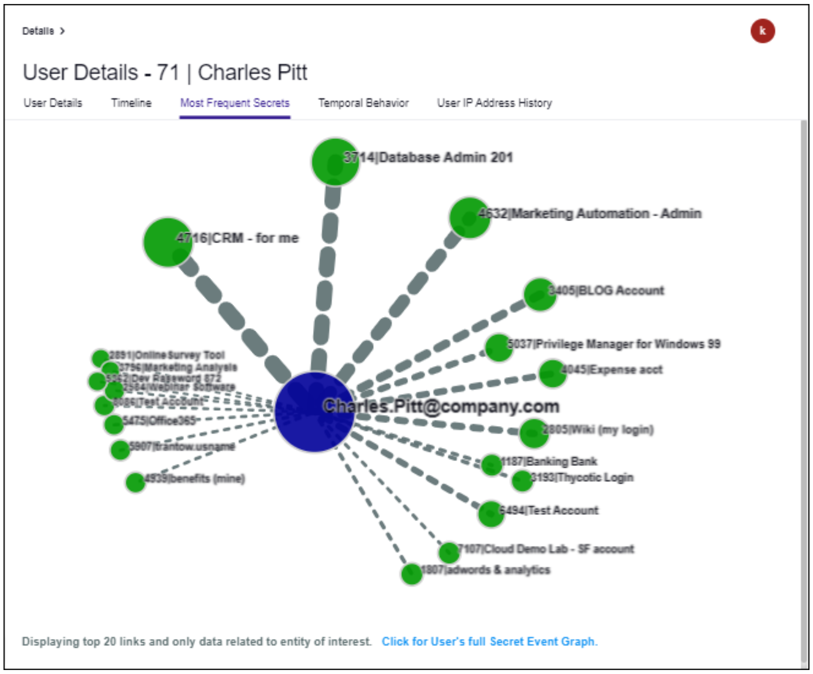
Adjust the range on the timeline graph to view alert activity. The data table below will be adjusted accordingly. To adjust the timeframe, pinch to zoom or use the time slider.

Timeline Table

217 items

DATE ↓	IP ADDRESS	CATEGORY	EVENT DETAILS
2023-09-12 09:08:56 AM	38.140.232.32	Secret Access	Action: VIEW Secret: 4632|Marketing Automation - Admin Note: AUTOFILL
2023-09-12 09:08:56 AM	38.140.232.32	Secret Access	Action: WEBPASSWORDFILL Secret: 4632|Marketing Automation - Admin Note: No details

Most Frequent Secrets: an animated representation of the top 20 most accessed Secrets by the User; you can zoom the graph by scrolling, or right-click on any node or link to view more details.



Details >

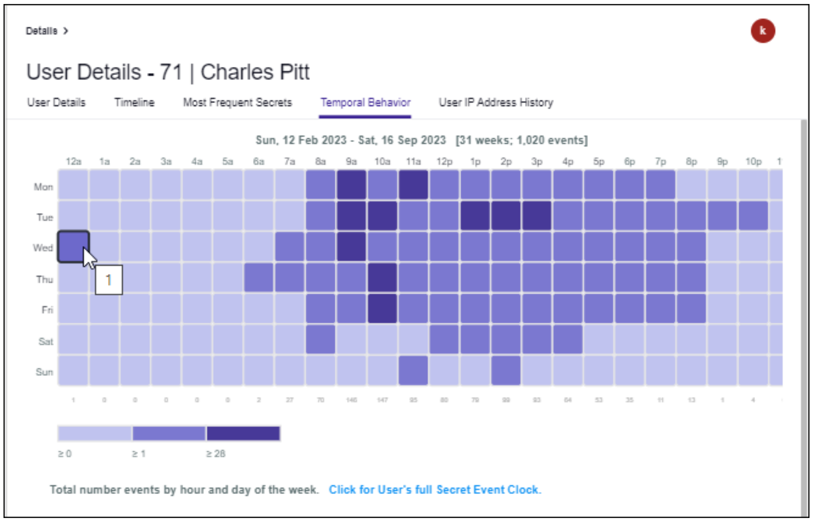
User Details - 71 | Charles Pitt

User Details Timeline Most Frequent Secrets Temporal Behavior User IP Address History

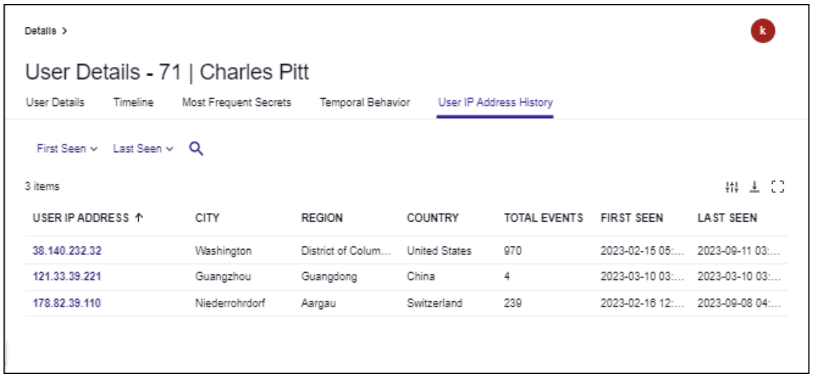
Displaying top 20 links and only data related to entity of interest. Click for User's full Secret Event Graph.

Temporal Behavior: a chart showing all temporal data for the User organized by time of day and day of the week.

- the numbers across the bottom indicate the total events involving the User for that time of day
- the values across the right side indicate the number of events involving the User for that day of the week
- the legend at the bottom shows the number of events that correlate to the coloring of the chart blocks
- mouse over a block to get the total number of accesses for that day of week and hour of day


Details >
k
User Details - 71 | Charles Pitt
User Details
Timeline
Most Frequent Secrets
Temporal Behavior
User IP Address History
Sun, 12 Feb 2023 - Sat, 16 Sep 2023 [31 weeks; 1,020 events]
12a 1a 2a 3a 4a 5a 6a 7a 8a 9a 10a 11a 12p 1p 2p 3p 4p 5p 6p 7p 8p 9p 10p 1
Mon
Tue
Wed
Thu
Fri
Sat
Sun
1
1 0 0 0 0 0 2 27 70 146 147 95 80 79 99 93 64 53 35 11 13 1 4
≥ 0
≥ 1
≥ 28
Total number events by hour and day of the week. Click for User's full Secret Event Clock.

User IP Address History: lists any IP addresses the user accessed Secret Server from.



User Details - 71 | Charles Pitt

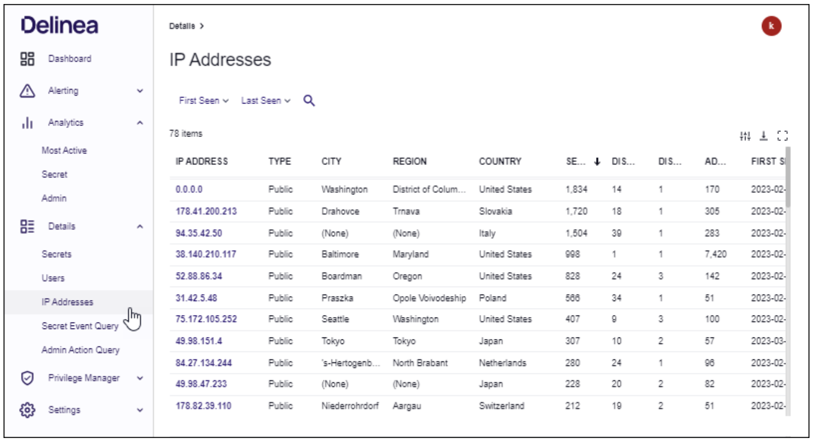
3 items

USER IP ADDRESS ↑	CITY	REGION	COUNTRY	TOTAL EVENTS	FIRST SEEN	LAST SEEN
38.140.232.32	Washington	District of Colum...	United States	970	2023-02-15 05:...	2023-09-11 03:...
121.33.39.221	Guangzhou	Guangdong	China	4	2023-03-10 03:...	2023-03-10 03:...
178.82.39.110	Niederrohrdorf	Aargau	Switzerland	239	2023-02-16 12:...	2023-09-08 04:...

IP Address Details

The **IP Addresses** page (**Details** > **IP Addresses**) lists all IP addresses, their type (Public or Private), City, Region, Country, the number of Secret accesses plus modifications, the number of unique Secrets accessed, the number of unique users accessing Secrets, the number of administrator actions performed (including logins), and the first and last time PBA observed the IP address in data.

The **Private** IP location is used to set a default location for cases where only internal (private) IP addresses are present in the data. This is particularly useful for visualizing and analyzing activity by IP address and location, especially when dealing with internal networks. Private IP addresses have no geographic location values. Instead, values reflect IP configuration.



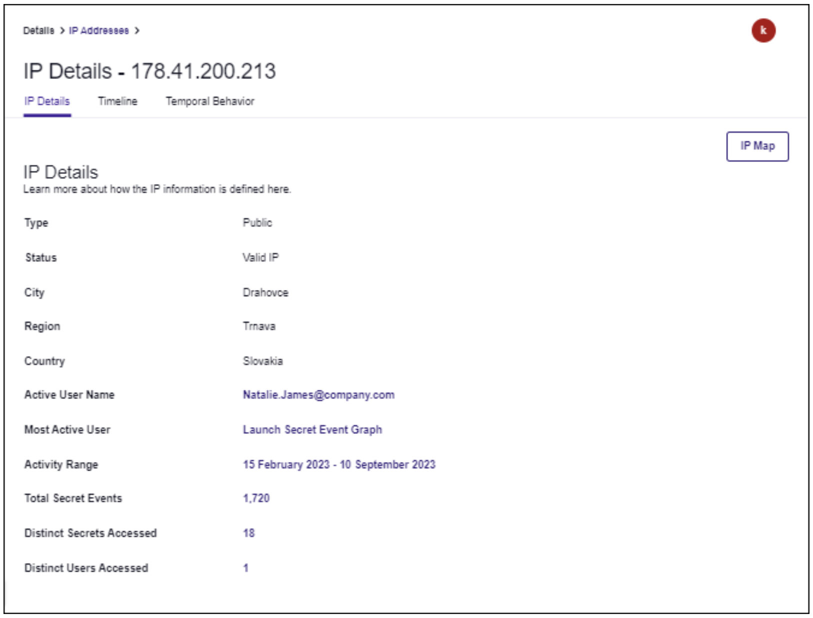
Details >

IP Addresses

78 items

IP ADDRESS	TYPE	CITY	REGION	COUNTRY	SE...	DIS...	DIS...	AD...	FIRST S
0.0.0.0	Public	Washington	District of Colum...	United States	1,834	14	1	170	2023-02-
178.41.200.213	Public	Drahovce	Trnava	Slovakia	1,720	18	1	305	2023-02-
94.35.42.50	Public	(None)	(None)	Italy	1,504	39	1	283	2023-02-
38.140.210.117	Public	Baltimore	Maryland	United States	998	1	1	7,420	2023-02-
52.88.86.34	Public	Boardman	Oregon	United States	828	24	3	142	2023-02-
31.42.5.48	Public	Praszka	Opole Voivodeship	Poland	566	34	1	51	2023-02-
75.172.105.252	Public	Seattle	Washington	United States	407	9	3	100	2023-02-
49.98.151.4	Public	Tokyo	Tokyo	Japan	307	10	2	57	2023-03-
84.27.134.244	Public	's-Hertogenb...	North Brabant	Netherlands	280	24	1	96	2023-02-
49.98.47.233	Public	(None)	(None)	Japan	228	20	2	82	2023-02-
178.82.39.110	Public	Niederrohrdorf	Aargau	Switzerland	212	19	2	51	2023-02-

Click on an IP address to open the IP Details page.



Details > IP Addresses >

IP Details - 178.41.200.213

IP Details

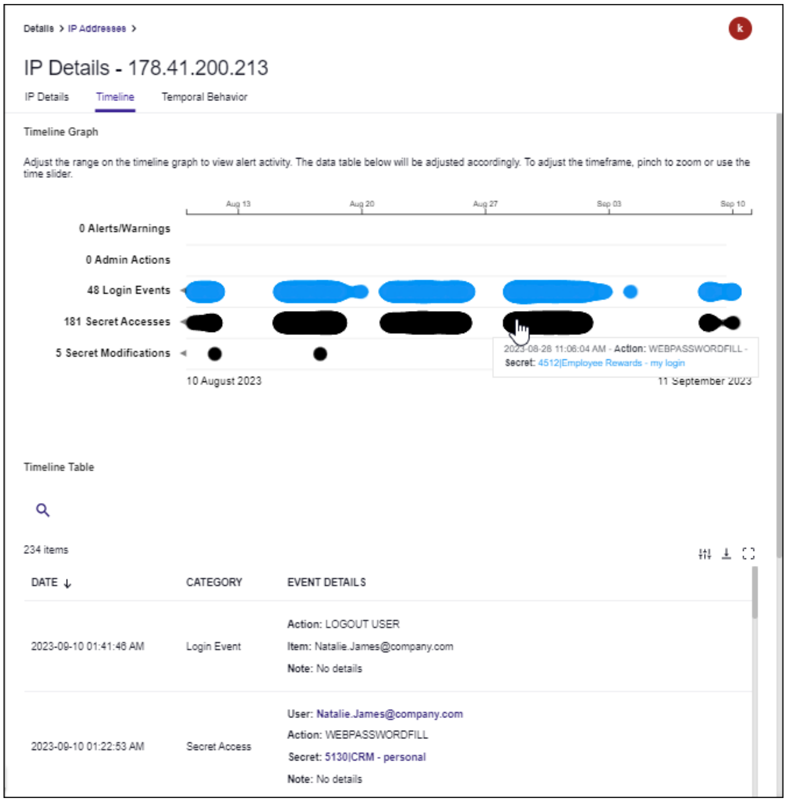
Learn more about how the IP information is defined here.

Type	Public
Status	Valid IP
City	Drahovce
Region	Trnava
Country	Slovakia
Active User Name	Natalie.James@company.com
Most Active User	Launch Secret Event Graph
Activity Range	15 February 2023 - 10 September 2023
Total Secret Events	1,720
Distinct Secrets Accessed	18
Distinct Users Accessed	1

The sections display a variety of detailed information.

Activity Timeline: a chart showing when an IP address was used to perform Secret accesses, modifications, and administrative actions in Secret Server (including login events). Any active or past alerts or warnings are shown as well.

- mouse over a colored circle for details on a particular event
- the chart can be panned left and right by dragging or zoomed by scrolling, which also filter data in the table



Details > IP Addresses >

IP Details - 178.41.200.213

IP Details | Timeline | Temporal Behavior

Timeline Graph

Adjust the range on the timeline graph to view alert activity. The data table below will be adjusted accordingly. To adjust the timeframe, pinch to zoom or use the time slider.

2023-08-28 11:06:04 AM - **Action:** WEBPASSWORDFILL - **Secret:** 4512|Employee Rewards - my login

Timeline Table

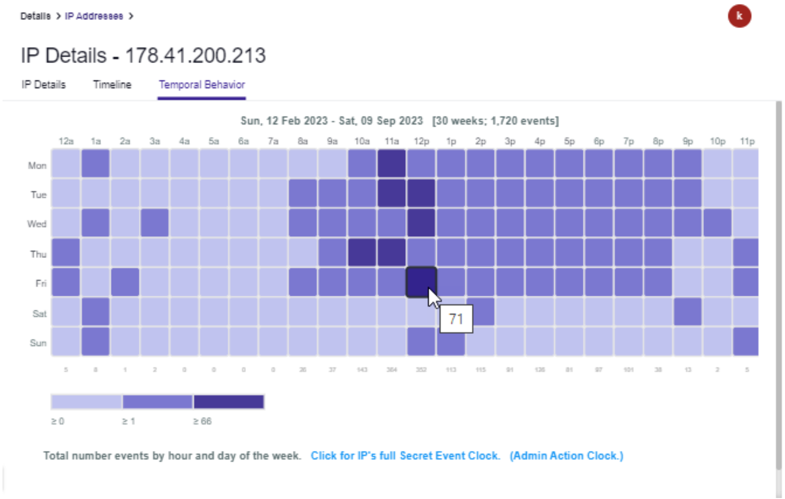
234 items

DATE ↓	CATEGORY	EVENT DETAILS
2023-09-10 01:41:46 AM	Login Event	**Action:** LOGOUT USER **Item:** Natalie.James@company.com **Note:** No details
2023-09-10 01:22:53 AM	Secret Access	**User:** Natalie.James@company.com **Action:** WEBPASSWORDFILL **Secret:** 5130|CRM - personal **Note:** No details

Temporal Behavior: a chart showing all temporal data for the IP address organized by time of day and day of the week

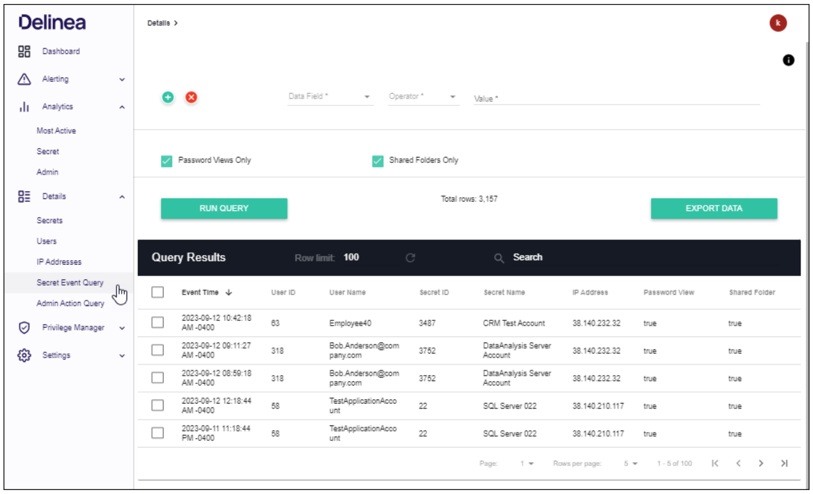
- the numbers across the bottom indicate the total events involving the IP address for that time of day
- the values across the right side indicate the number of events involving the IP address for that day of the week
- the legend at the bottom shows the number of events that correlate to the coloring of the chart blocks

- mouse over a block to get the total number of events for that day of week and hour of day



Query

Secret Event Query allows you to retrieve data that meet criteria you specify for secrets. A table shows results of the query, and data can be exported for offline analysis or auditing.



☑ Password Views Only ☑ Shared Folders Only

Total rows: 3,157

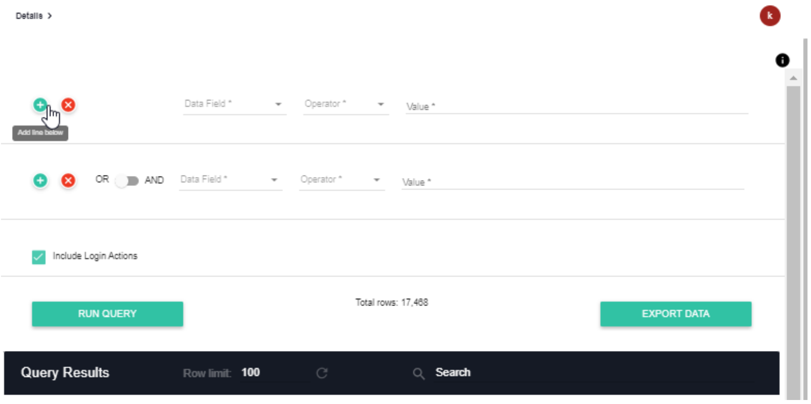
Row limit: 100

□	Event Time ↓	User ID	User Name	Secret ID	Secret Name	IP Address	Password View	Shared Folder
□	2023-09-12 10:42:18 AM -0400	63	Employee40	3487	CRM Test Account	38.140.232.32	true	true
□	2023-09-12 09:11:27 AM -0400	318	Bob.Anderson@company.com	3752	DataAnalysis Server Account	38.140.232.32	true	true
□	2023-09-12 08:59:18 AM -0400	318	Bob.Anderson@company.com	3752	DataAnalysis Server Account	38.140.232.32	true	true
□	2023-09-12 12:18:44 AM -0400	58	TestApplicationAccount	22	SQL Server 022	38.140.210.117	true	true
□	2023-09-11 11:18:44 PM -0400	58	TestApplicationAccount	22	SQL Server 022	38.140.210.117	true	true

Page: 1 Rows per page: 5 1 - 5 of 100

Click the Toggle Theme button to change between light and dark themes.

On each query line, click the Add Line button to insert a line below the current line. Click the Remove Line button to delete the current line.



Select **OR** or **AND** using the switch to apply that condition to the line above plus the current line. The **AND** lines will be grouped together as if they were enclosed in parentheses with **OR** applied between each group.

All three options: **Data Field**, **Operator**, and **Value** (or Temporal selection) must be set for the line to be included in the query. A check mark will appear on the right side when all selections are valid.

The **Value** search input accepts "*" (wildcard) and uppercase **AND**, **NOT**, and **OR** searches (but no mixing **AND**, **NOT**, **OR**, nor parentheses). Some data field types show their values with a prefix (e.g., "IP: 127.0.0.1"). When using the "contains" and "not contains" operators, wildcards ("*") are allowed in the search term.

Enable **Password Views Only** to include only password view events; disable the check box to include all Secret events.

Enable **Shared Folders Only** to include only Secrets in shared folders; disable the check box to include Secrets in personal folders.

For "Event Time" entries, most time formats are accepted. For "Temporal" data types the application assumes timestamps are in the Local Timezone set in System Settings.

Press **Run Query** to display a table of results. Rows can be selected for export (**Export Data**). The **Row Limit** input allows changing the maximum number of rows stored in the table. The Search box filters any matching table rows.

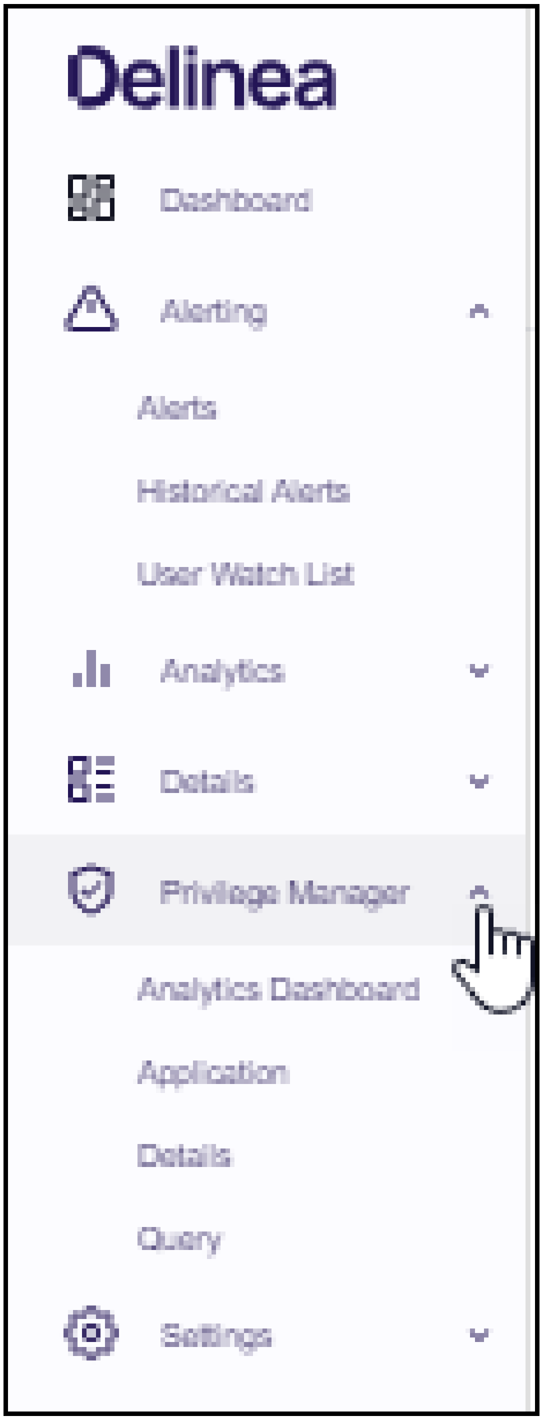
Data returned are the most recent events based on the latest update and could be delayed several minutes from the current time.

Important: IP address locations are prone to change and can be inaccurate and imprecise, sometimes located to only the region or country level. This app shows only the most recent available IP address location information, which might have been updated since the time an IP address was last accessed. Location data are derived from MaxMind's GeoLite2.

PBA Applications for Privilege Manager

Once you have setup Privilege Manager and Privileged Behavior Analytics to work together, you can begin normal operations.

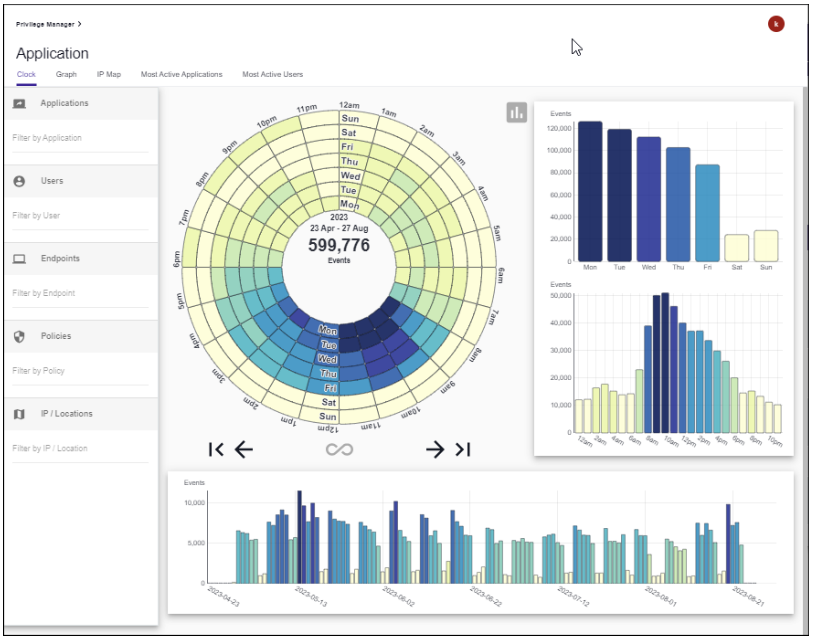
Click Privilege Manager in the left navigation panel.



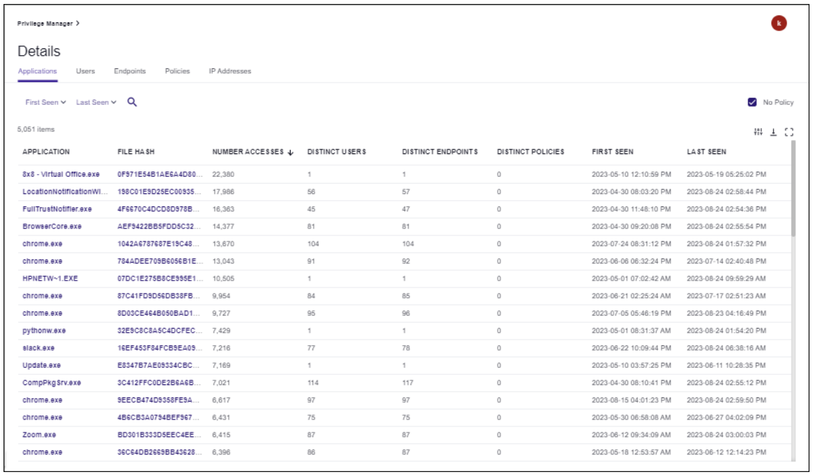
The available tools include:

Analytics Dashboard provides drill-down quadrants for: User Details, Application Details, Most Active Users, Most Active Applications, Top User Graph, Top Application Graph, and a Temporal Heatmap. Refer to "Privilege Manager Analytics Dashboard" on page 64.

Applications are reported for "Application Clock" on page 65, "Application Graph" on page 67,"Application IP Map" on page 74, "Most Active Applications" on page 82, and "Most Active Users" on page 82.



Details provide analytics for Applications, Users, Endpoints, Policies, and IP Addresses.


Privilege Manager >

Details

Applications Users Endpoints Policies IP Addresses

First Seen Last Seen

☑ No Policy

5,051 items

APPLICATION	FILE HASH	NUMBER ACCESSES ↓	DISTINCT USERS	DISTINCT ENDPOINTS	DISTINCT POLICIES	FIRST SEEN	LAST SEEN
8x8 - Virtual Office.exe	0F971E54B1AE6A4D80...	22,380	1	1	0	2023-05-10 12:10:59 PM	2023-05-19 05:25:02 PM
LocationNotificationWi...	198C01E9D25EC00935...	17,986	56	57	0	2023-04-30 08:03:20 PM	2023-08-24 02:58:44 PM
FullTrustNotifier.exe	4F6670C4DCD8D978B...	16,363	45	47	0	2023-04-30 11:48:10 PM	2023-08-24 02:54:36 PM
BrowserCore.exe	AEF9422BB5FDD5C32...	14,377	81	81	0	2023-04-30 09:20:08 PM	2023-08-24 02:55:54 PM
chrome.exe	1042A6787687E19C48...	13,670	104	104	0	2023-07-24 08:31:12 PM	2023-08-24 01:57:32 PM
chrome.exe	784ADEE709B6056B1E...	13,043	91	92	0	2023-06-06 06:32:24 PM	2023-07-14 02:40:48 PM
HPNETW~1.EXE	07DC1E275B8CE995E1...	10,505	1	1	0	2023-05-01 07:02:42 AM	2023-08-24 09:59:29 AM
chrome.exe	87C41FD9D56DB38FB...	9,954	84	85	0	2023-06-21 02:25:24 AM	2023-07-17 02:51:23 AM
chrome.exe	8D03CE464B050BAD1...	9,727	95	96	0	2023-07-05 05:46:19 PM	2023-08-23 04:16:49 PM
pythonw.exe	32E9C8C8A5C4DCFEC...	7,429	1	1	0	2023-05-01 08:31:37 AM	2023-08-24 01:54:20 PM
slack.exe	16EF453F84FCB9EA09...	7,216	77	78	0	2023-06-22 10:09:44 PM	2023-08-24 06:38:16 AM
Update.exe	E8347B7AE09334CBC...	7,169	1	1	0	2023-05-10 03:57:25 PM	2023-06-11 10:28:35 PM
CompPkgSrv.exe	3C412FFC0DE2B6A6B...	7,021	114	117	0	2023-04-30 08:10:41 PM	2023-08-24 02:55:12 PM
chrome.exe	9EECB474D9358FE9A...	6,617	97	97	0	2023-08-15 04:01:23 PM	2023-08-24 02:59:50 PM
chrome.exe	4B6CB3A0794BEF967...	6,431	75	75	0	2023-05-30 06:58:08 AM	2023-06-27 04:02:09 PM
Zoom.exe	BD301B333D5EEC4EE...	6,415	87	87	0	2023-06-12 09:34:09 AM	2023-08-24 03:00:03 PM
chrome.exe	36C64DB2669BB43628...	6,396	86	87	0	2023-05-18 12:53:57 AM	2023-06-12 12:14:23 PM

These tools summarized in the table below.

> **Note:** If you are already using PBA for Secret Server, select the Privilege Manager Analytics menu. If you are using PBA for Privilege Manager only, your Privilege Manager Analytics Dashboard opens by default.

Name	Description
"Privilege Manager Analytics Dashboard" on page 64	Displays several key indicators neatly assembled on quick-view tiles
"Application Clock" on page 65	Displays temporal patterns and filters data by Application, User, Endpoint, Policy, and IP/location
"Application Graph" on page 67	Shows users accessing applications, designed to reveal anomalous patterns
"Application IP Map" on page 74	Maps out application activity, aggregated by IP address and location
"Most Active Applications" on page 82	Reveals which applications have seen the most executions
"Most Active Users" on page 82	Identifies users accessing more applications than most other users
"Application Details" on page 83	Runs down all recent access activity for specific applications and their characteristics
"User Details" on page 92	Allows you to explore in detail information collected about a specific user’s activity
"Endpoint Details" on page 87	Summarizes endpoint activity by user and application
"Policy Details" on page 90	Provides details about policies triggered by users accessing applications
"IP Address Details" on page 94	Shows IP address activity summary and location information
"Query" on page 97	Enables data query and export for criteria you specify

Configuring Privileged Behavior Analytics With Privilege Manager

Delinea's Privileged Behavior Analytics (PBA) SaaS product can be integrated with Privilege Manager cloud instances.

For the integration to work correctly, independent of your Privilege Manager instance, you need to have a Delinea enabled PBA instance.

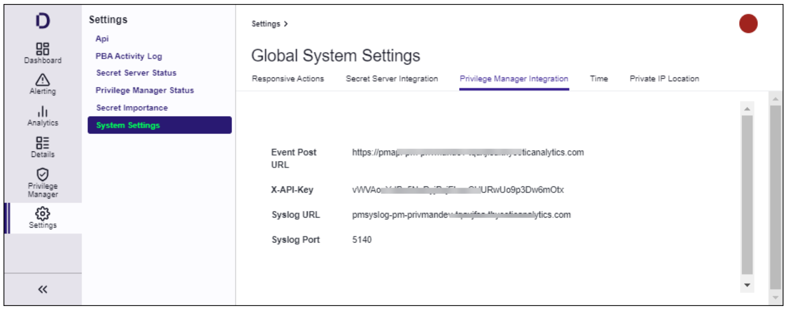
To configure Privilege Manager with Privileged Behavior Analytics (PBA), you need to integrate the two systems. This involves the following:

- "PBA System Settings Details" on the next page
- "Setting Up PBA Integration on Privileged Behavior Analytics" on the next page
- "Enable Send Application Events to PBA" on page 63

PBA System Settings Details

You will need to retrieve the PBA System Settings details required for setting up the integration in Privileged Behavior Analytics.

1. Navigate to the **PBA Systems Settings** page (/system_settings/).



Global System Settings

Event Post URL https://pmap[redacted]ticanalytics.com

X-API-Key vWVAo[redacted]URwUo9p3Dw6mOtx

Syslog URL pmsyslog-pm-privmande[redacted]lytics.com

Syslog Port 5140

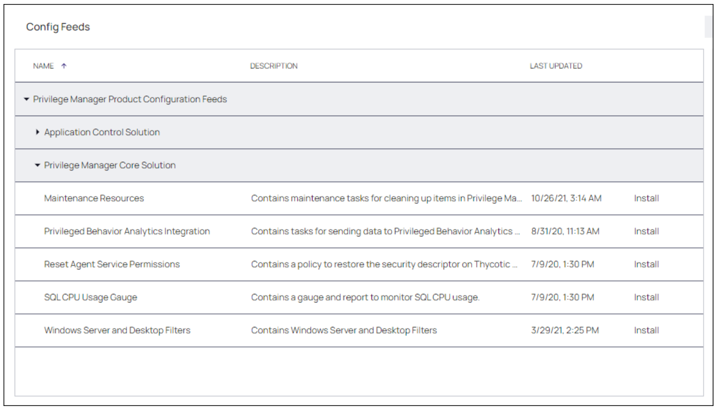
2. Use the Syslog URL and port information when setting up the **SysLog Foreign System** below. Use the Event Post Url and the X-API-Key when setting up the **Send Application Events to PBA** below.

Setting Up PBA Integration on Privileged Behavior Analytics

Required PBA resources are provided via Privilege Manager Configuration Feeds.

Downloading and Installing the PBA Config Feed

1. In your Privilege Manager console, navigate to **Admin | Config Feeds**.
2. Expand **Privilege Manager Product Configuration Feeds**.
3. Expand **Privilege Manager Core Solution**.
4. Install **Privileged Behavior Analytics Integration**.



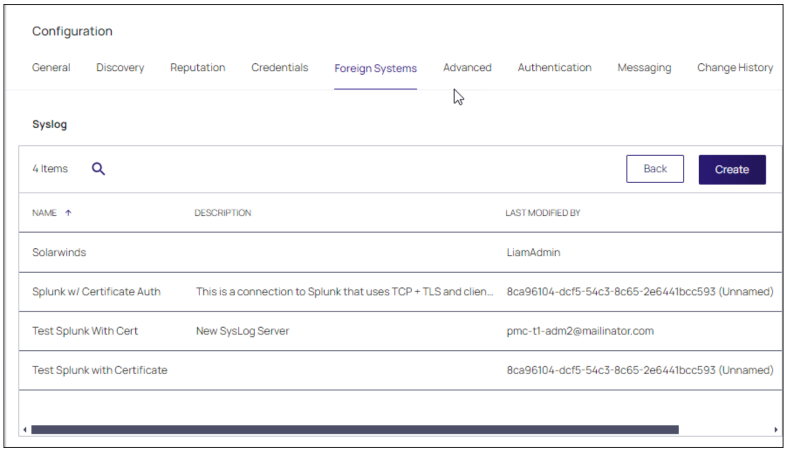
Config Feeds

NAME ↑	DESCRIPTION	LAST UPDATED	
▾ Privilege Manager Product Configuration Feeds			
▸ Application Control Solution			
▾ Privilege Manager Core Solution			
Maintenance Resources	Contains maintenance tasks for cleaning up items in Privilege Ma...	10/26/21, 3:14 AM	Install
Privileged Behavior Analytics Integration	Contains tasks for sending data to Privileged Behavior Analytics ...	8/31/20, 11:13 AM	Install
Reset Agent Service Permissions	Contains a policy to restore the security descriptor on Thycotic ...	7/9/20, 1:30 PM	Install
SQL CPU Usage Gauge	Contains a gauge and report to monitor SQL CPU usage.	7/9/20, 1:30 PM	Install
Windows Server and Desktop Filters	Contains Windows Server and Desktop Filters	3/29/21, 2:25 PM	Install

After the installation, proceed to the foreign systems setup.

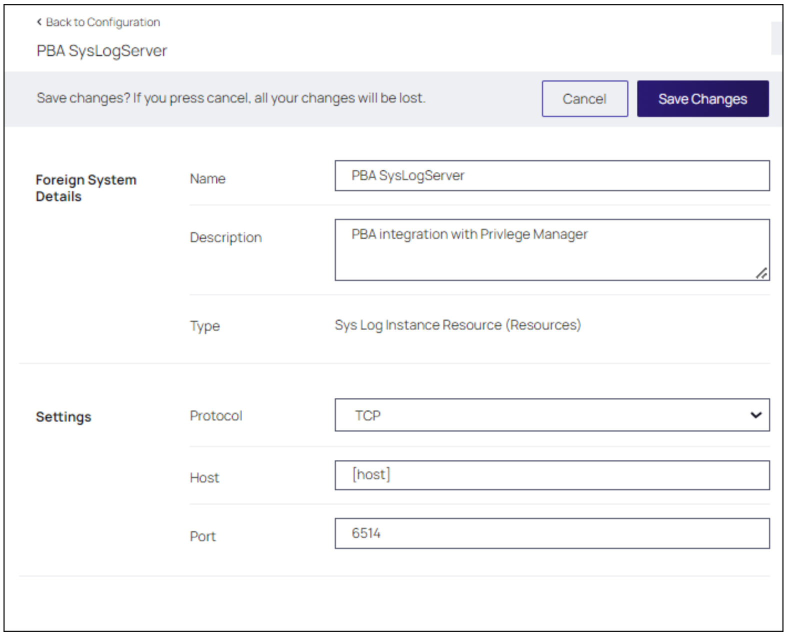
Setting up the PBA SysLog Foreign System

1. In your Privilege Manager console, navigate to **Admin | Config** and select **Foreign Systems**.
2. Select **SysLog**.
3. Click **Create**.



NAME ↑	DESCRIPTION	LAST MODIFIED BY
Solarwinds		LiamAdmin
Splunk w/ Certificate Auth	This is a connection to Splunk that uses TCP + TLS and clien...	8ca96104-dcf5-54c3-8c65-2e6441bcc593 (Unnamed)
Test Splunk With Cert	New SysLog Server	pmc-t1-adm2@mailinator.com
Test Splunk with Certificate		8ca96104-dcf5-54c3-8c65-2e6441bcc593 (Unnamed)

4. Enter a name and your SysLog server details.
5. Click **Create**.
6. Verify that your Protocol, Host, and Port match your SysLog server details (**SysLog URL** and **SysLog Port** from the PBA System Settings details).

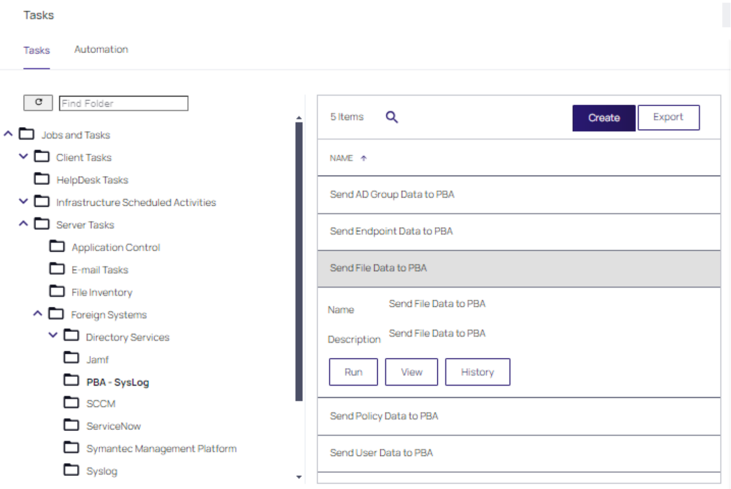


Save changes? If you press cancel, all your changes will be lost.

Foreign System Details	Name	PBA SysLogServer
	Description	PBA integration with Privlege Manager
	Type	Sys Log Instance Resource (Resources)
Settings	Protocol	TCP
	Host	[host]
	Port	6514

Using the PBA Send Tasks

1. In your Privilege Manager console, navigate to **Admin | Tasks** and from the folder tree select **Server Tasks | Foreign Systems**.
2. Click **PBA - SysLog**.
3. For Privilege Manager to send data based on any of these tasks, the PBA SysLog server you created as a foreign system, needs to be added as the SysLog System ID. This can be done in either of these ways.
   - **On Demand** when running the task:
     a. Select a PBA Data Send tasks and click **Run**.

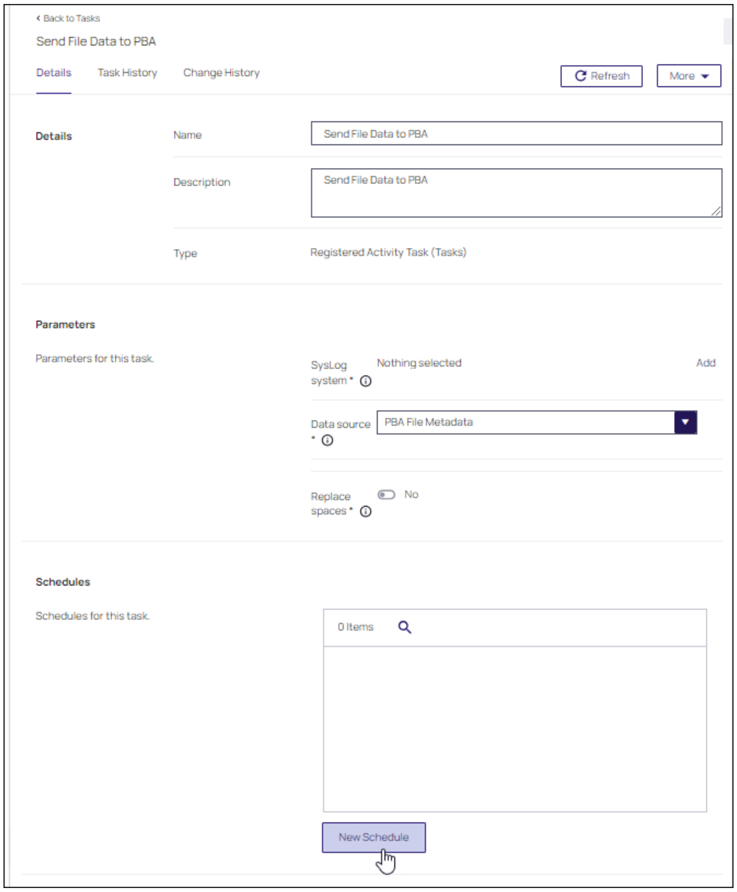


Name Send File Data to PBA

Description Send File Data to PBA

     b. Specify the SysLog System ID.
     c. Click **Run Task**.

- **By setting up a schedule**:
  a. Select a PBA Data Send tasks and click **View**.
  b. Under **Parameters** specify the SysLog System ID.
  c. Define a **Schedule**, by clicking **New Schedule**



Send File Data to PBA

Details

Name: Send File Data to PBA

Description: Send File Data to PBA

Type: Registered Activity Task (Tasks)

Parameters

Parameters for this task.

SysLog system *: Nothing selected

Data source *: PBA File Metadata

Replace spaces *: No

Schedules

Schedules for this task.

0 Items

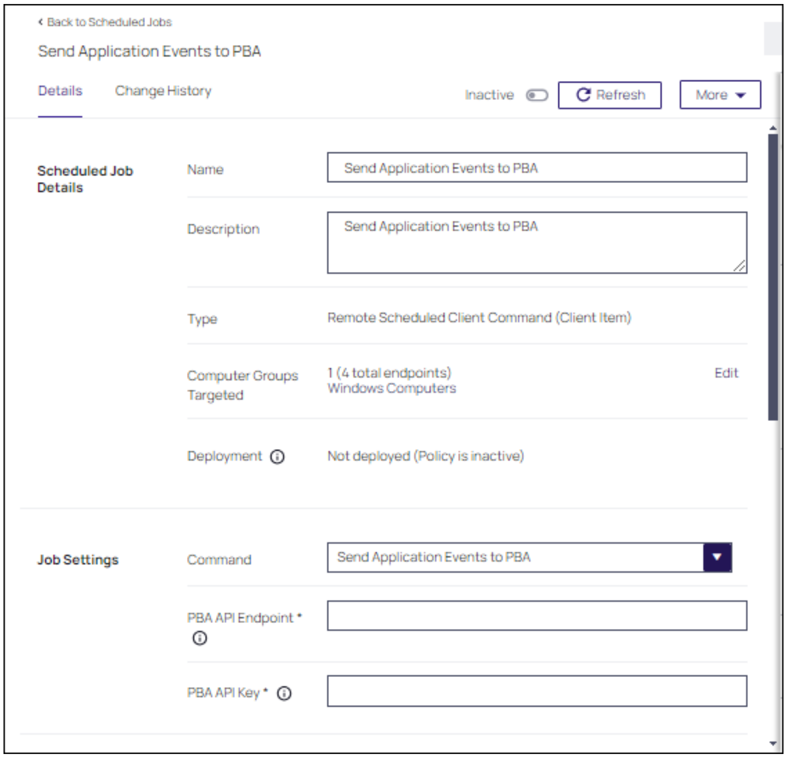
  d. Click **Save Changes**.

Repeat for each of the data sets you want to use in PBA.

Enable Send Application Events to PBA

The config feeds installation also add a remote scheduled client command for PBA to Privileged Behavior Analytics. The **Send Application Events to PBA** policy is by default disabled.

1. In your Privilege Manager console, under your computer group, navigate to **Scheduled Jobs**.
2. On the **Scheduled Jobs** page search for PBA and select **Send Application Events to PBA**.



Send Application Events to PBA

Scheduled Job Details

Name: Send Application Events to PBA

Description: Send Application Events to PBA

Type: Remote Scheduled Client Command (Client Item)

Computer Groups Targeted: 1 (4 total endpoints)
Windows Computers

Deployment: Not deployed (Policy is inactive)

Job Settings

Command: Send Application Events to PBA

PBA API Endpoint *

PBA API Key *

- Under **Job Settings**, enter the PBA**Event Post URL** and **X-API-Key** details from the PBA system settings information.
- Modify the **Job Schedule** if customization is required.
- Customize any of the **Job Conditions** to better fit your implementation.

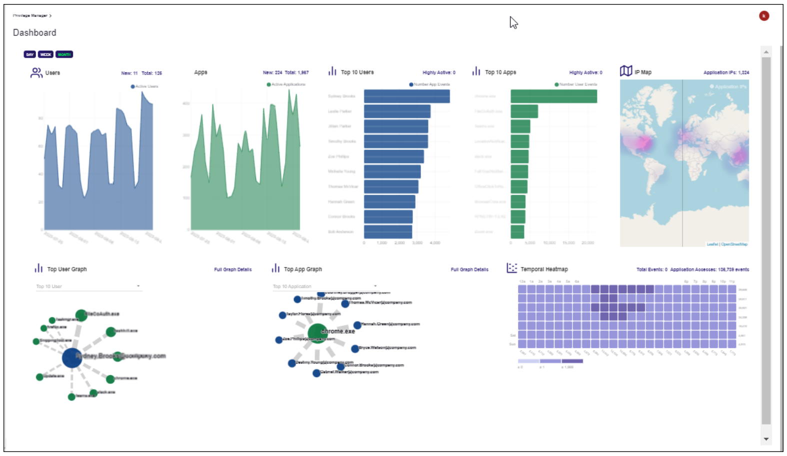
3. Click **Save Changes**.
4. Set the **Inactive** switch to **Active**.
5. Next to **Deployment**, click the **i** icon and select the **Resource and Collection Targeting Update** task to run.

Privilege Manager Analytics Dashboard

PBA's **Analytics Dashboard** page collects commonly used tools and views so you can easily recognize anything that would be out of the ordinary for your Privilege Manager environment.

- Multiple widgets present at-a-glance data visuals that cycle through views of activity for the last day, week, and month.
- The widgets activate or deactivate when you click the controls for each on the left side of the Dashboard.
- Cycling pauses on the data view for the last day, week, and month when you click on the Day, Week, and Month controls.
- Additional settings (dashboard theme, widget settings, cycle duration) are accessible through the three horizontal bars icon on the top left side.

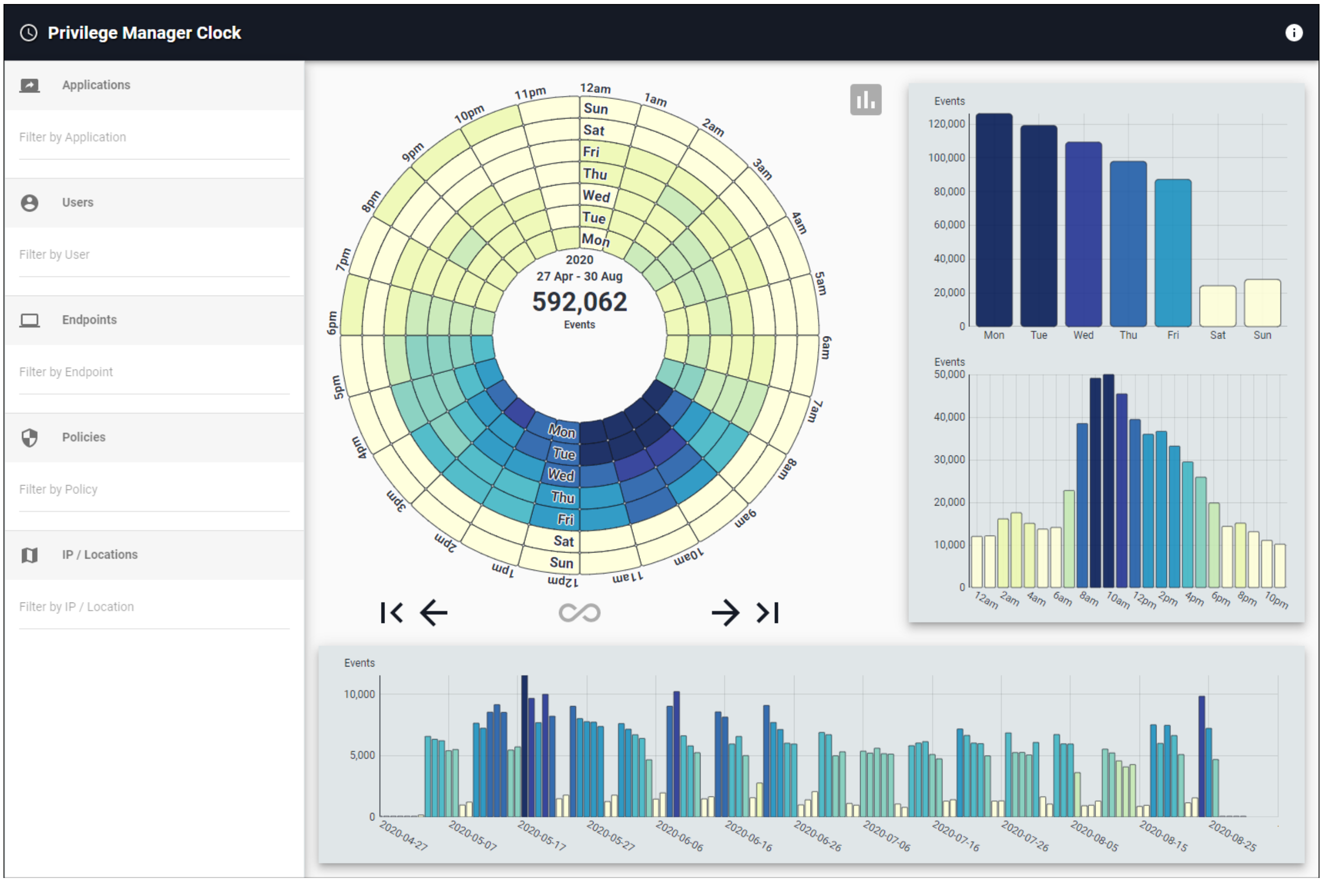
- The Alerts tile is currently only available for Secret Server. In the left sidebar, click the alert icon to toggle off the tile.



Application Clock

The **Application Clock** provides a temporal overview of Privilege Manager event data organized by: Application, User, Endpoint, Policy, and IP / Location. It visualizes the distribution and concentration of activities for a given time range.

The circular chart is called a data clock and shows event counts by hour and day of the week (starting with the inner ring and spiraling clockwise outward). The charts in the right panel show totals by day of the week and hour of the day. The bottom panel shows daily totals for the entire activity period.



The coloring of the graphs range from white to dark blue.

- White means no activity.
- Dark blue means a lot of activity.

The center of the data clock displays the number of events represented and the date range when they occurred. Click this text to change units in the upper three charts. ("% of Total" is the amount contained within each bar compared to the selected week's total. "% of Max" is the amount contained within each bar compared to the selected week's max bar value for a given chart. Bar coloring for the default Events (count) option is relative to all weeks' data if a single week is selected.)

To move back and forth through specific weeks, use the left and right arrows at the base of the data clock. If you wish to hide the side and bottom bar charts from the display, you can click the gray chart button to the top right of the data clock. The bottom chart allows panning (click and drag left/right) and zooming (scroll up/down). Double-click to reset the view.

- You can filter the temporal data by clicking into one of the input lines on the left side and typing the name of:
  - Application, File Hash, or File Name
  - User, Group, Name, or User ID
  - Endpoint or Endpoint ID

  - Policy or Policy ID
  - IP address, City, Region, or Country
- Each "Filter by ___" input also accepts "*" (wildcard) and uppercase "AND", "NOT", and "OR" searches (but no mixing AND, NOT, OR, nor parentheses).
- Selecting a filter from one of the lists will refresh the graphs to reflect only events within the data range that are related to that application, user, endpoint, policy, or IP.
- If you refine by an application and wish to see which users accessed it on a particular day or at a certain time, you can right-click on the corresponding bar in any of the graphs and then click on the name of the application.
- Likewise, if you refine by a user and wish to see which applications they accessed on a particular day or at a certain time, you can right-click on the corresponding bar and click on the name of the user.
- Adding a filter from two different data types will perform an "AND" operation between them. For example, filtering on an application and a user will only show events where the user accessed that application.

Note: All charts and timestamps are based on the Local Timezone in System Settings.

Application Graph

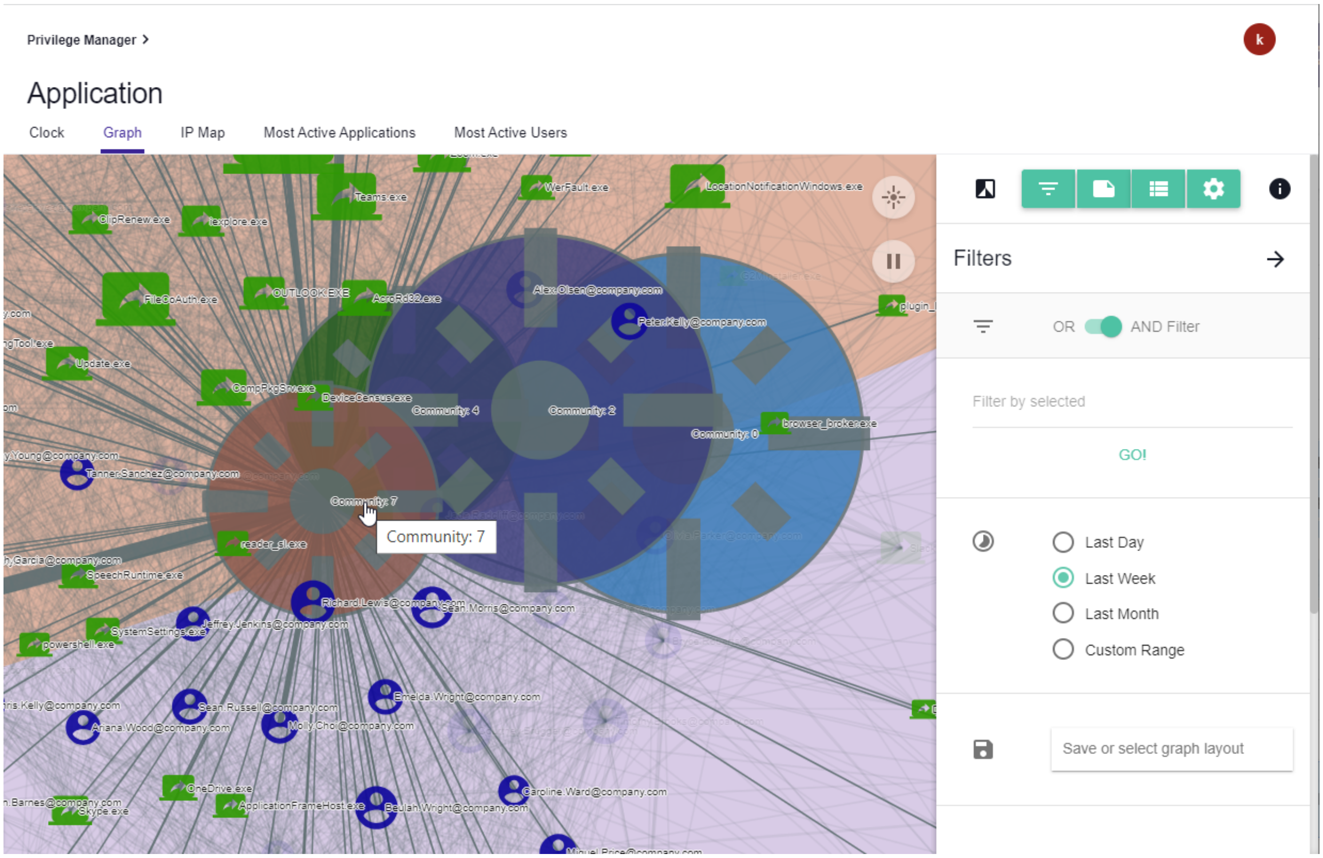
The **Application Graph** can be used to explore the behaviors of Privilege Manager users and activity of applications, endpoints, and policies at a glance.

The graph is animated by default. You can pause the animation by clicking on the pause button at the top right of the graph area. Above the pause button is another button that will allow you to expand or collapse all nodes with a single click. You can also expand or collapse individual clusters by double clicking on them.

Each initial node circle, or Community, is a collection of users who are accessing similar applications. The larger the Community, the more users and applications there are inside it.

Communities may also have lines, or links, connecting them to other Communities. The links are an indication that a user or users within a Community are accessing applications that exist in another Community, indicating a possibility of accesses outside a User’s responsibility. Thicker links represent more accesses between Communities.

When you expand (double-click) a Community, you can see all the users and applications it contains. The size of each node indicates how many accesses it has and the thickness of links follows the same principal.



Privilege Manager >

Application

Clock | Graph | IP Map | Most Active Applications | Most Active Users

Filters

○ OR ● AND Filter

Filter by selected

GO!

○ Last Day
● Last Week
○ Last Month
○ Custom Range

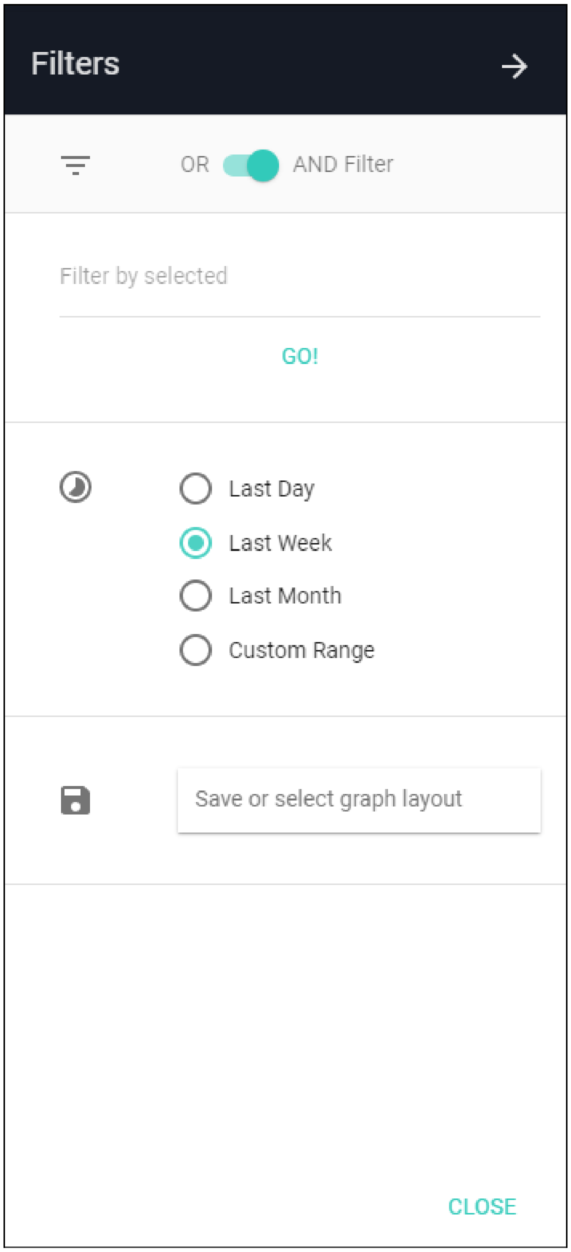
Save or select graph layout

Whether a Community is expanded or not, you can right click on any node or link on the Application Graph to add notes or see further details.

The icon to the left of the menu buttons will toggle the Graph between light and dark themes.

Filters

The Filters menu (three horizontal lines button) provides options to limit the number of nodes and links displayed.



Filters

OR AND Filter

Filter by selected

GO!

○ Last Day
● Last Week
○ Last Month
○ Custom Range

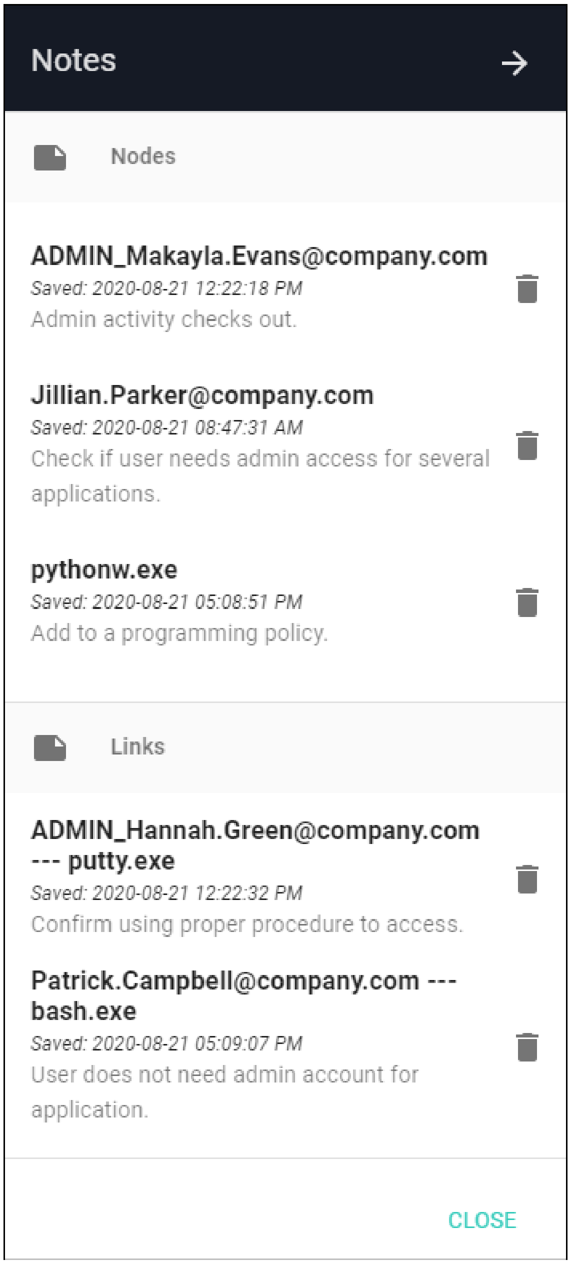
Save or select graph layout

CLOSE

- **OR AND Filter**: determines how filters will be applied to the Graph
- **Filter by selected**: lets you filter the Graph display by Application, User, Endpoint, Group, IP Address (and City, Region, Country), or Policy
- **Time Ranges**: by default, the Graph will show activity from the last week; the Custom Range option allows selecting a start and end date to refine activity displayed
- **Save or select graph layout**: you may choose to save filtered views of the Graph to quickly recall significant access landscapes

Notes

The Notes menu can be accessed by clicking the button depicting a note with a folded corner at the top right of the Application Graph page.



Notes →

Nodes

ADMIN_Makayla.Evans@company.com
Saved: 2020-08-21 12:22:18 PM
Admin activity checks out.

Jillian.Parker@company.com
Saved: 2020-08-21 08:47:31 AM
Check if user needs admin access for several applications.

pythonw.exe
Saved: 2020-08-21 05:08:51 PM
Add to a programming policy.

Links

ADMIN_Hannah.Green@company.com --- putty.exe
Saved: 2020-08-21 12:22:32 PM
Confirm using proper procedure to access.

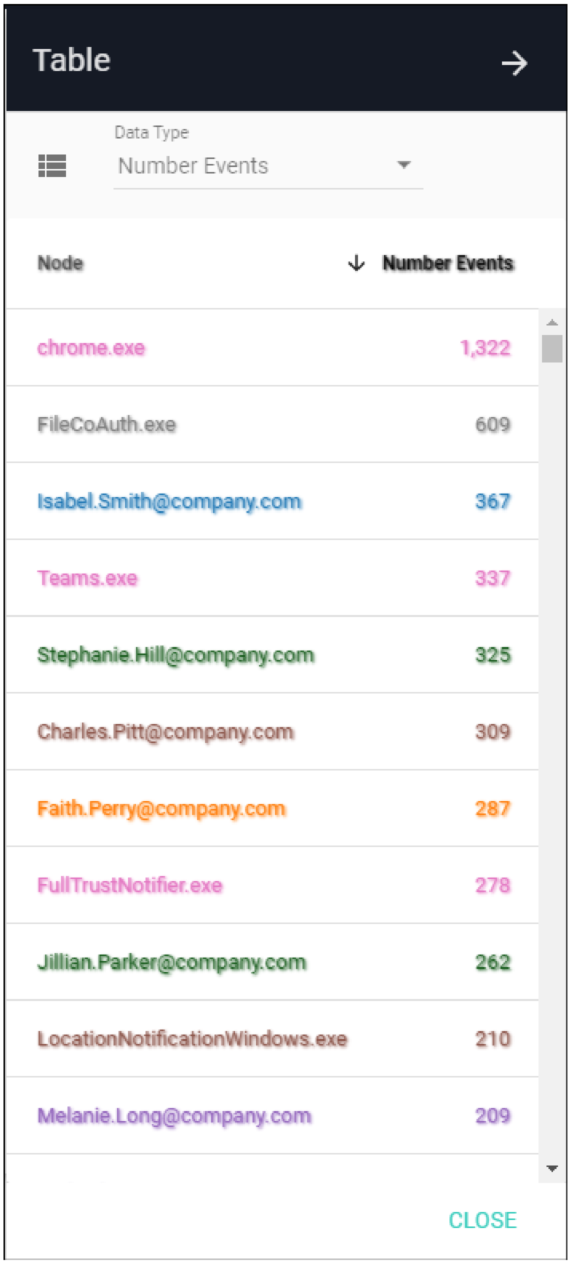
Patrick.Campbell@company.com --- bash.exe
Saved: 2020-08-21 05:09:07 PM
User does not need admin account for application.

CLOSE

- All notes on nodes and links are listed here. You can edit any note by clicking on it or delete a note by clicking on the trashcan icon to the right of the note.
- Notes can be created by right-clicking on a node (circle) or link (line) in the Application Graph. A small square of the color selected will appear on the node or link after the note is created.
- Hovering over the square or a note in the Notes menu will briefly highlight the note square on the Graph.

Table

The Table menu can be accessed by clicking the icon between the Notes and Tools buttons at the top right of the Application Graph page.



Node	Number Events
chrome.exe	1,322
FileCoAuth.exe	609
Isabel.Smith@company.com	367
Teams.exe	337
Stephanie.Hill@company.com	325
Charles.Pitt@company.com	309
Faith.Perry@company.com	287
FullTrustNotifier.exe	278
Jillian.Parker@company.com	262
LocationNotificationWindows.exe	210
Melanie.Long@company.com	209

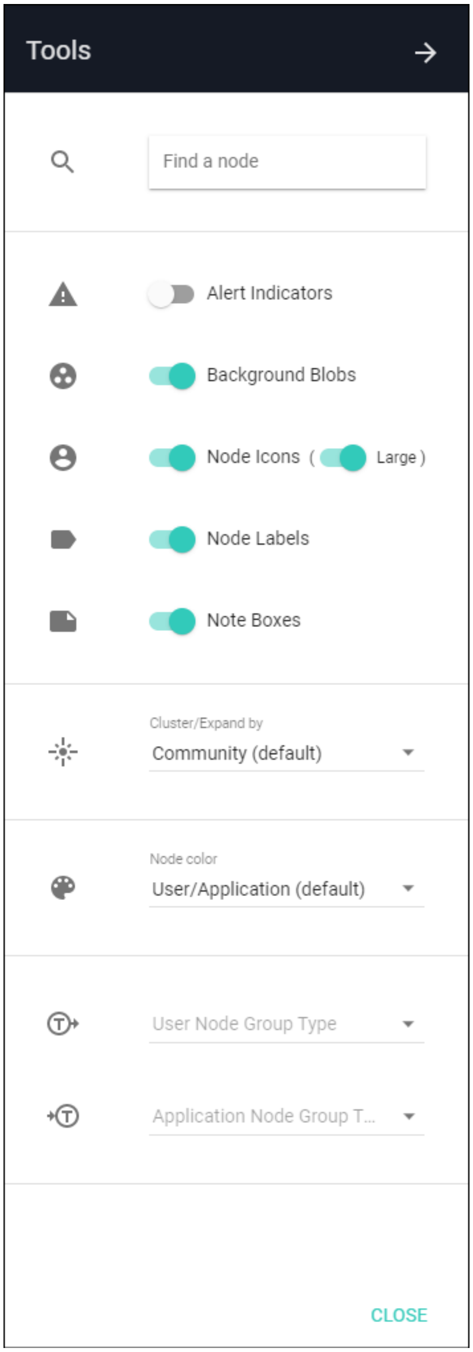
This menu gives you a full, sortable text-based list of all User and Application node metrics. Placing your mouse over any of the node names in the lists will highlight that node on the Application Graph if the Community it is in is expanded.

- **Community** lists User and Application nodes and the Community number they are in
- **User/Application** lists User and Application node names and whether each is a User or Application

- **Number Connections** lists User and Application nodes and how many accesses they have had or performed on other nodes
- **Number Unique** lists User and Application nodes and how many unique applications or users, respectively, they are connected to
- **Last Active** lists User and Application nodes and the timestamp of the last activity each had
- **First Active** lists User and Application nodes and the timestamp of the first activity each had recorded in PBA
- **Social Network Metrics** lists User and Application nodes and the numerical value of the selected metric

Tools

The Tools menu (cogwheel button) allows you to customize what is displayed on the Graph.



- Alert Indicators: ○ off
- Background Blobs: ● on
- Node Icons: ● on (● Large)
- Node Labels: ● on
- Note Boxes: ● on
- Cluster/Expand by: Community (default)
- Node color: User/Application (default)
- User Node Group Type
- Application Node Group T...

- **Search**: At the top of the menu is a search field where you can enter the name of a User or Application to highlight that specific node on the Application Graph. Press Enter to repeat the animation.
- **Alert Indicators**: turned on by default, this will outline nodes in a shade of red based on whether it has an active alert; the redder a node is the higher the total alert risk
- **Background Blobs**: turned on by default, these surround all nodes in an expanded Community with a color similar to that of the collapsed Community

- **Node Icons**: turned on by default, this shows icons in place of circles for each user or application node. The size of the icon can be changed using the **Large** switch.
- **Node Labels**: turned on by default, these are Community numbers, application names, and user names shown next to each node
- **Note Boxes**: turned on by default, these represent notes that have been placed on any nodes or links
- **Cluster/Expand by**: by default, all nodes will be clustered by Communities; you can select the dropdown here to choose to cluster nodes by applications and users
- **Node Color**: there are multiple options for choosing how the nodes within an expanded Community are colored:
  - **Community**: all Application and User nodes will be the color of the Community when it is collapsed
  - **User/Application**: the User nodes are colored blue and Application nodes are colored green (default coloring)
  - **Number Connections**: Application and User node colors will range from white to red; the redder a node is, the more active it is
  - **Number Unique**: Nodes will range from white to red, and the redder a node is, the more unique accesses it has
  - **Last Active**: Nodes will range from white to red with recent activity being more red
  - **First Active**: Nodes will range from white to red with earlier activity being more red
  - **Social Network Metrics**: these options can reveal important applications or users in the network
- **User Node Group Type**: Select a user type to change nodes to that metric (e.g. selecting Endpoint will show endpoint nodes connected to application nodes)
- **Application Node Group Type**: Select an application type to change nodes to that metric (e.g. selecting Policy will show user nodes connected to policy nodes)

Application IP Map

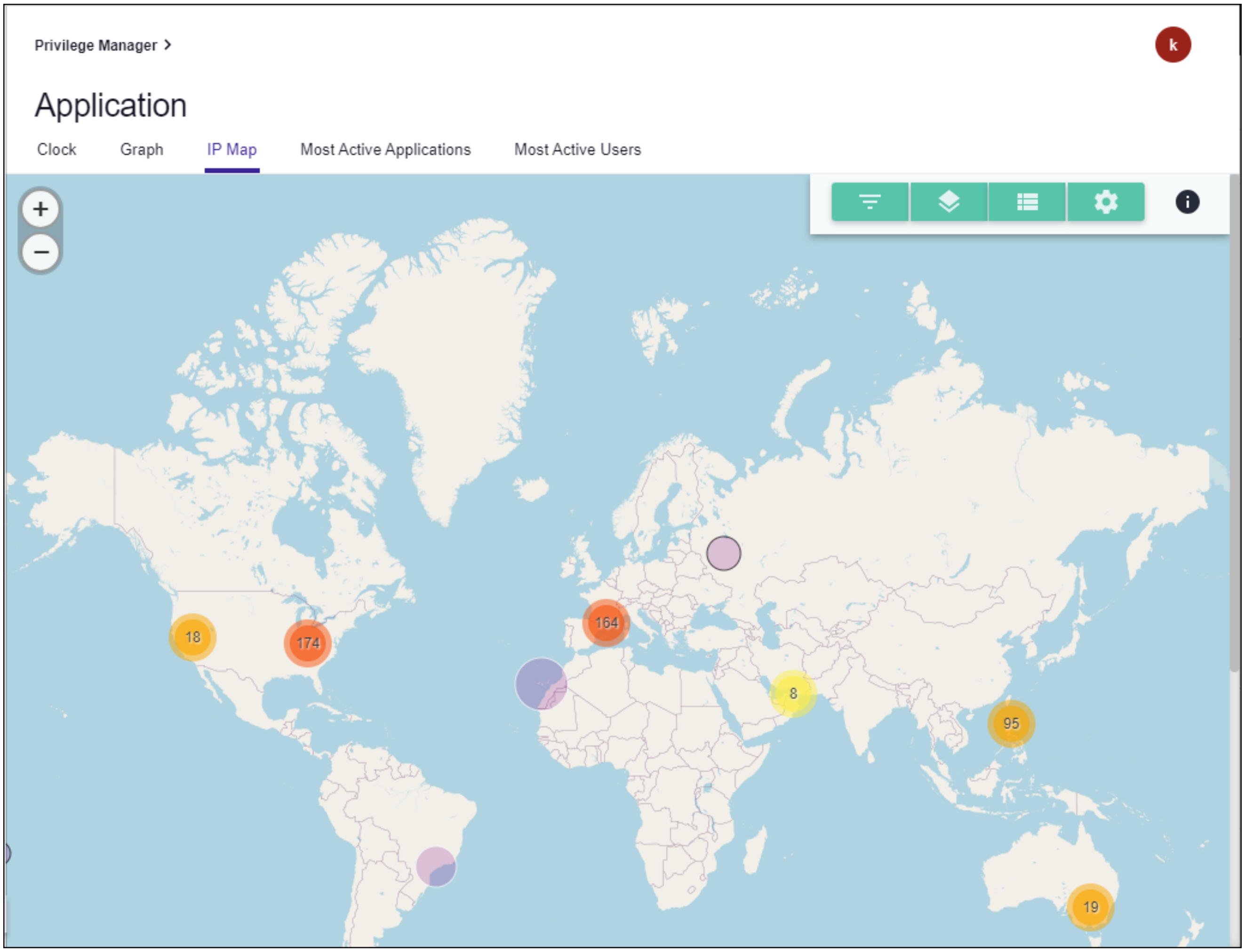
The **Application IP Map** summarizes user to application activity by IP address and location. This is useful for Privilege Manager endpoints that access applications from public IP addresses.

Summary views and information provide a high-level understanding of recent and historical events. Any anomalous locations in the data can be quickly observed, analyzed, and acted upon.

Map Key

The map shows by default the last week of IP address counts (purple circles) and active alerts (red triangles). You can click these features for further information.

Circle features sometimes have a gray or black outline, which means they are located only to the region (state) or country level, respectively.



Map Navigation

The Map can be navigated like most web-based maps:

- Pan to different locations by clicking on an open area and dragging the mouse
- Zoom in or out using the mouse wheel, the buttons on the upper left, double-clicking (+ Shift), or dragging the mouse while holding Shift to select a zoom box

Filters

The **Filters** menu (first menu button) provides options to limit data displayed based on user, application, IP address, location, and several related attributes.

- **OR AND Filter**: determines whether selected filters will be considered separately (OR) or together (AND)
- **Filter by selected**: filters the Map display by application, user, endpoint, group, IP Address, location, and policy
- **Time Ranges**: by default, the Map will show activity from the last week; the Custom Range option allows selecting a start and end date to refine activity displayed

- **Save or select IP map options**: save filtered views of the Map to quickly recall significant events or complex filter combinations

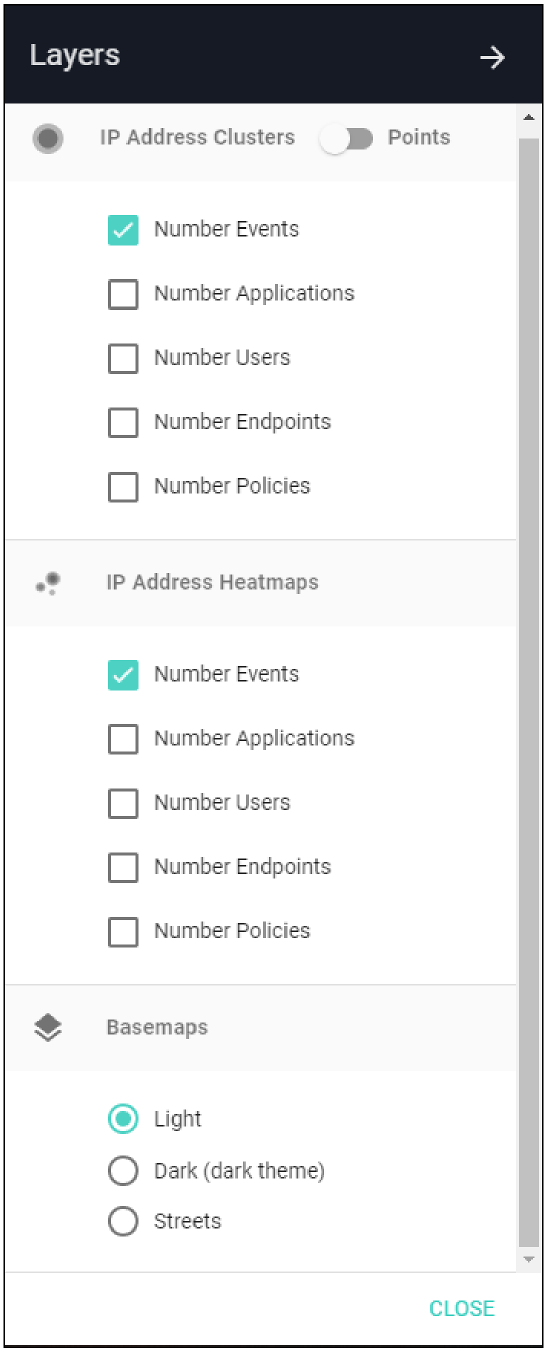
Tip: If no data appear, try turning off filters or expanding the time range. From the System Settings page, a default location can be entered for cases where only internal (private) IP addresses are present in the data.

Layers

The **Layers** menu (second menu button) contains options to show circle layers as clusters (aggregated nearby points) or as individual points for the number of events, applications, users, endpoints, or policies active at each IP address.

There are also heatmaps and different basemaps that can be selected.

- Selecting the **Dark** basemap will change the entire map application to the dark theme.



Layers

● IP Address Clusters Points

☑ Number Events

□ Number Applications

□ Number Users

□ Number Endpoints

□ Number Policies

IP Address Heatmaps

☑ Number Events

□ Number Applications

□ Number Users

□ Number Endpoints

□ Number Policies

Basemaps

● Light

○ Dark (dark theme)

○ Streets

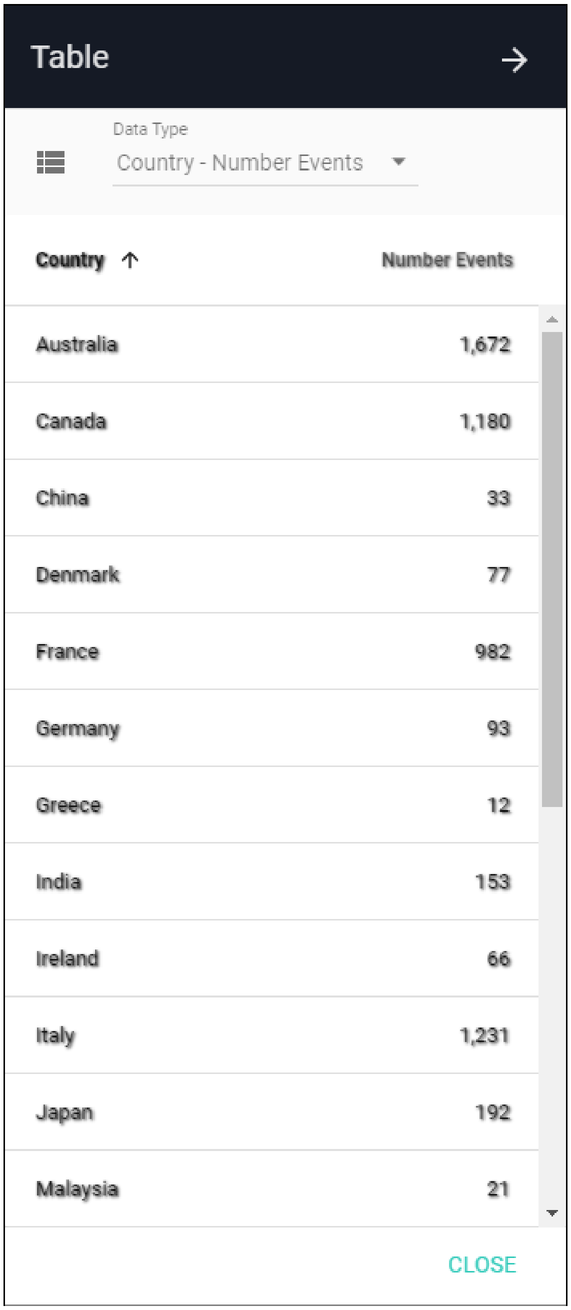
CLOSE

Table

The Table menu (third menu button) provides a sortable text-based list of key metrics (below) related to IP addresses. Placing your mouse over any of the rows in the lists will highlight a point or country on the Map.

- **Country – Number Events**: shows the total number of IP events within each country
- **IP – Number Events**: shows list of IP addresses with the total number of events for each
- **IP – Number Applications**: shows list of IP addresses with the total number of Secrets accessed or modified from each
- **IP – Number Users**: shows list of IP addresses with the total number of users for each
- **IP – Number Endpoints**: shows list of IP addresses with the total number of endpoints for each
- **IP – Number Policies**: shows list of IP addresses with the total number of policies for each
- **IP – First Active**: shows IP address list with date of first activity observed
- **IP – Last Active**: shows IP address list with date of last activity observed
- **IP – City**: shows IP address list with city of the location (if available)
- **IP – Region**: shows IP address list with region (state) of the location (if available)

- **IP - Country**: shows IP address list with country of the location



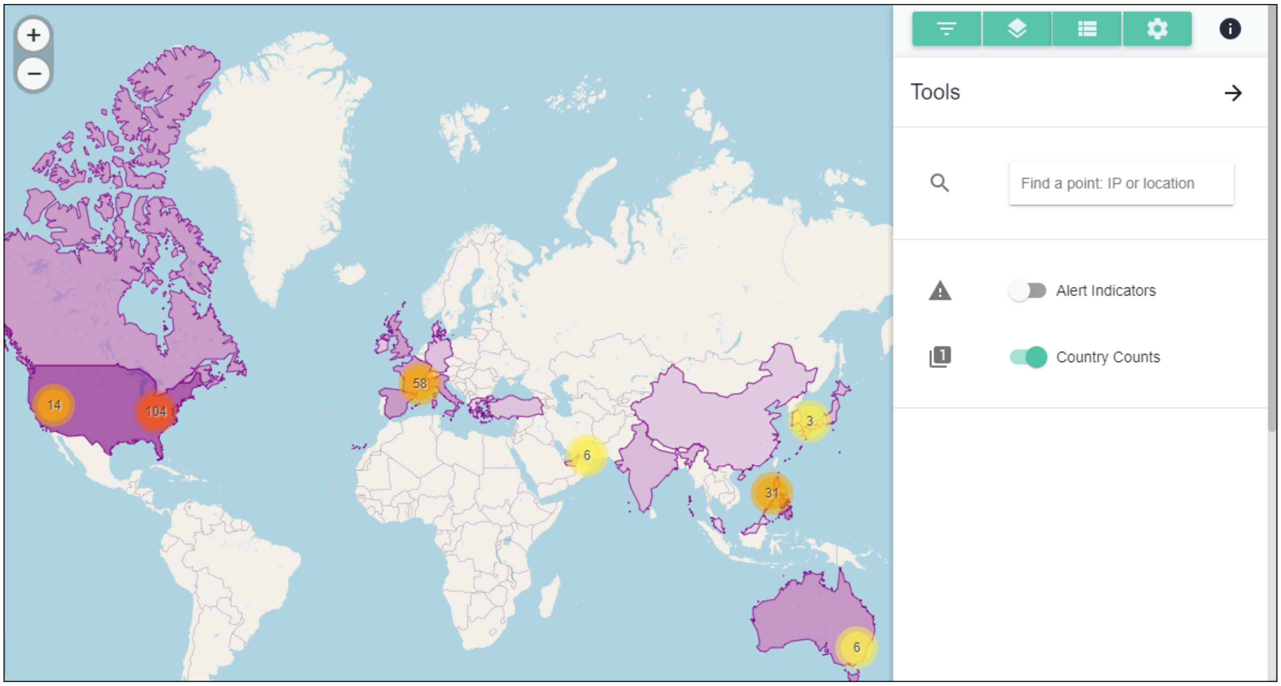
Country ↑	Number Events
Australia	1,672
Canada	1,180
China	33
Denmark	77
France	982
Germany	93
Greece	12
India	153
Ireland	66
Italy	1,231
Japan	192
Malaysia	21

Tools

The **Tools** menu (fourth menu button) provides a search function to find a specific IP address, city, region (state), or country among the data points currently loaded to the Map. Clicking on a result will pop up details and re-zoom the map to the selected IP address.

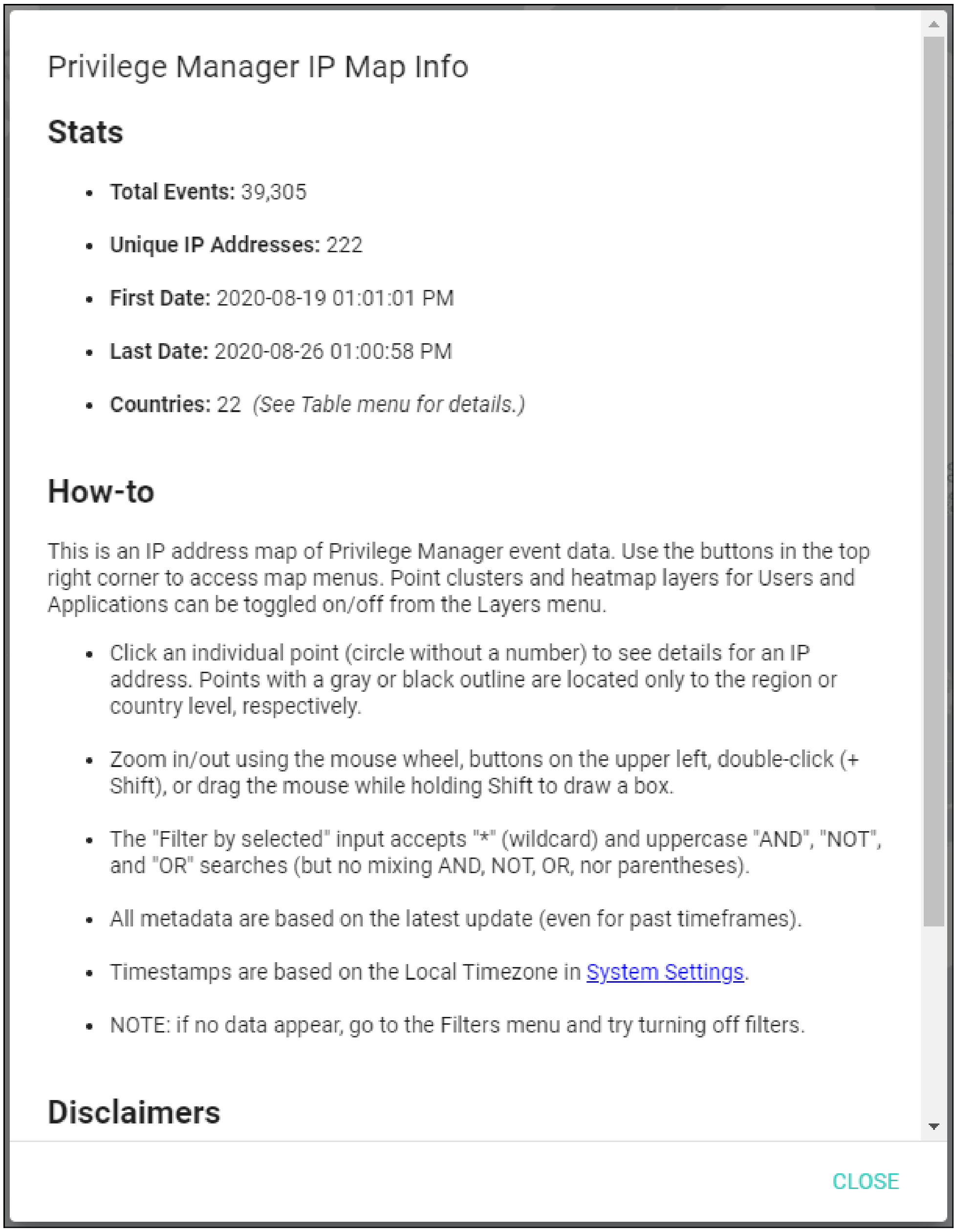
The Tools menu also contains two additional data layer options:

- **Alert Indicators** show red triangles for IP addresses that have active alerts or warnings. Clicking on a triangle will show details on the number of alerts and total risk score.
- **Country Counts** show a semi-transparent layer shaded by the number of events taking place in each country. Clicking on a country will re-zoom the map to the selected country, and hovering the mouse over it will show the country name, flag, and number of events.



Application IP Map Info

Next to the menu buttons is an info icon that launches the **Application IP Map Info** box, which contains basic statistics on the map data displayed, map instructions, and disclaimers.



Privilege Manager IP Map Info

Stats

- **Total Events:** 39,305
- **Unique IP Addresses:** 222
- **First Date:** 2020-08-19 01:01:01 PM
- **Last Date:** 2020-08-26 01:00:58 PM
- **Countries:** 22 *(See Table menu for details.)*

How-to

This is an IP address map of Privilege Manager event data. Use the buttons in the top right corner to access map menus. Point clusters and heatmap layers for Users and Applications can be toggled on/off from the Layers menu.

- Click an individual point (circle without a number) to see details for an IP address. Points with a gray or black outline are located only to the region or country level, respectively.
- Zoom in/out using the mouse wheel, buttons on the upper left, double-click (+ Shift), or drag the mouse while holding Shift to draw a box.
- The "Filter by selected" input accepts "*" (wildcard) and uppercase "AND", "NOT", and "OR" searches (but no mixing AND, NOT, OR, nor parentheses).
- All metadata are based on the latest update (even for past timeframes).
- Timestamps are based on the Local Timezone in System Settings.
- NOTE: if no data appear, go to the Filters menu and try turning off filters.

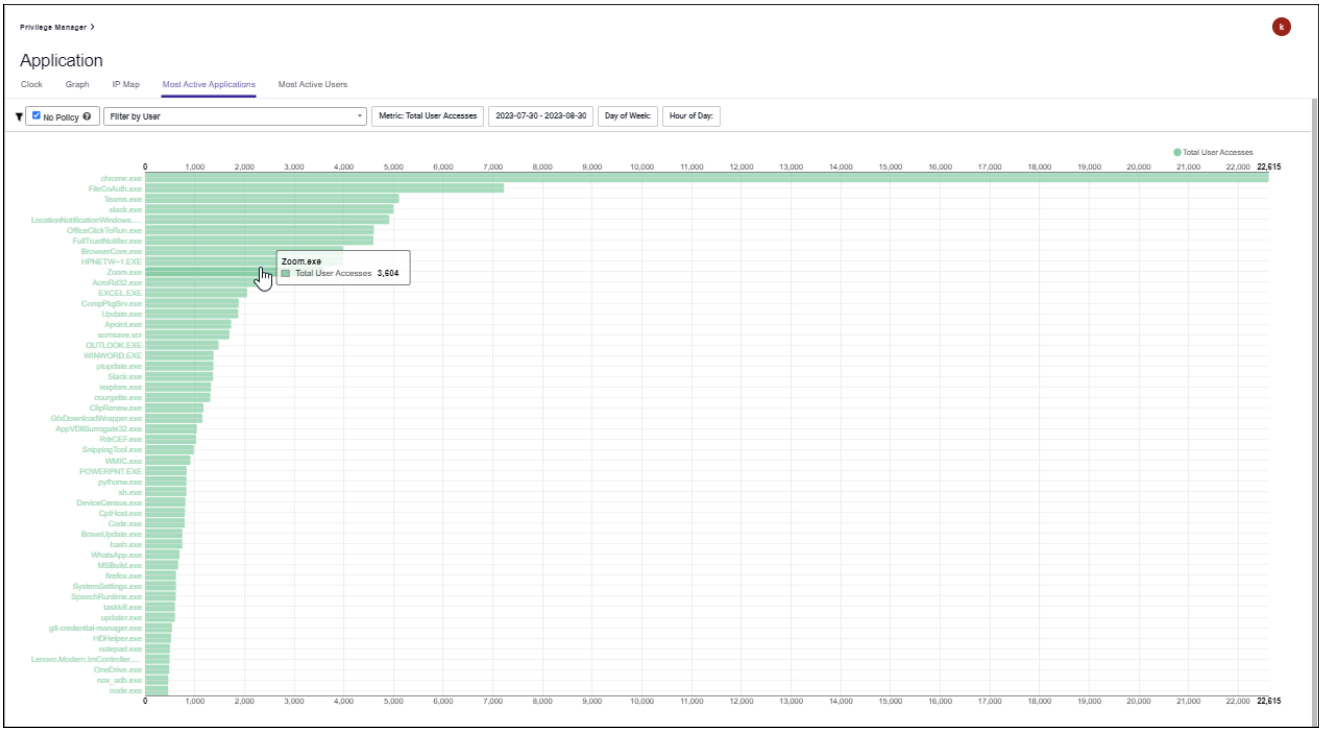
Disclaimers

Disclaimers

IP address locations are prone to change and can be inaccurate and imprecise, sometimes located to only the region or country level. This app shows only the most recent available IP address location information, which might have been updated since the time an IP address was last accessed. Location data are derived from MaxMind's GeoLite2. All metadata are based on the latest update (even for past timeframes). Timestamps are based on the Local Timezone in System Settings.

Most Active Applications

Most Active Applications ranks the top 50 most accessed applications for given filter criteria. To see this page, navigate to **Privilege Manager Analytics** or **Analytics** > **Most Active Applications**.



Privilege Manager >

Application

☑ No Policy

Filter by User

Metric: Total User Accesses

2023-07-30 - 2023-08-30

Day of Week:

Hour of Day:

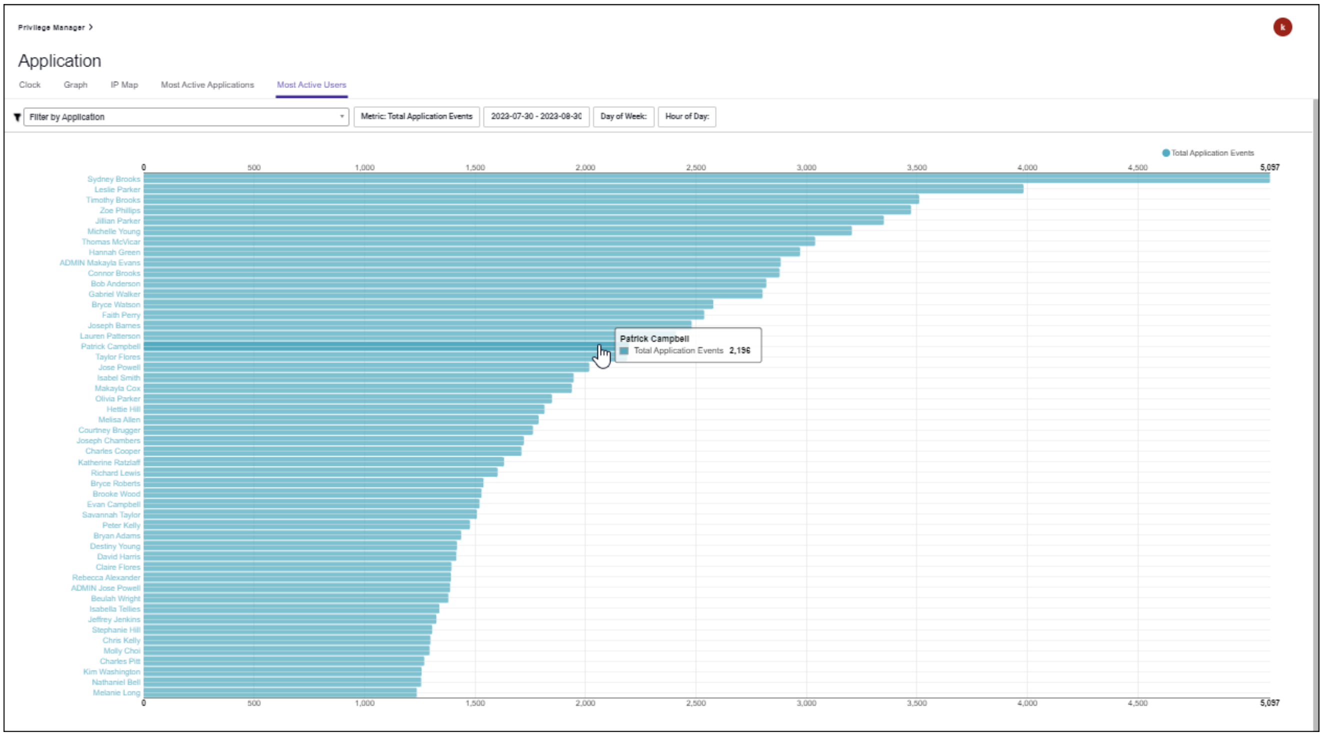
Zoom.exe
🟩 Total User Accesses 3,604

The list contains the application name and number of events for each of the top 50 applications, using a bar chart as visual reference.

- By default, you will see the top 50 applications in your Privilege Manager environment for the past month.
- The "No Policy" checkbox shows by default the applications accessed that have no policy applied. Uncheck to see all application events.
- You can further filter the list by a user, total or distinct accesses, or a specific timeframe.
- Clicking on an application name or bar in the list will take you to its **Application Details** page.

Most Active Users

Most Active Users ranks the top 50 most active users for given filter criteria. To see this page, navigate to **Privilege Manager Analytics** or **Analytics** > **Most Active Users**.

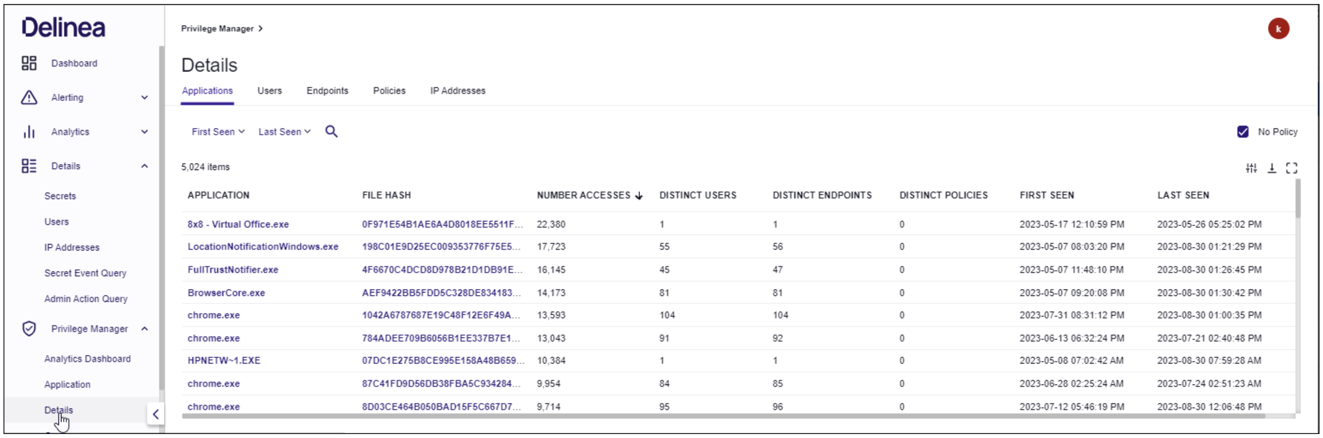


The list contains the user display name and number of events for each of the top 50 users, using a bar chart as visual reference.

- By default, you will see the top 50 users in your Privilege Manager environment for the past month.
- You can further filter the list by an application, total or distinct accesses, or a specific timeframe.
- Clicking on a user name or bar in the list will take you to its **User Details** page.

Application Details

The **Application Details** page can be used to investigate how an application is being accessed from the perspective of many types of data collected on it. You can access Application Details by navigating to **(Privilege Manager Analytics) | Details | Applications**.



☑ No Policy

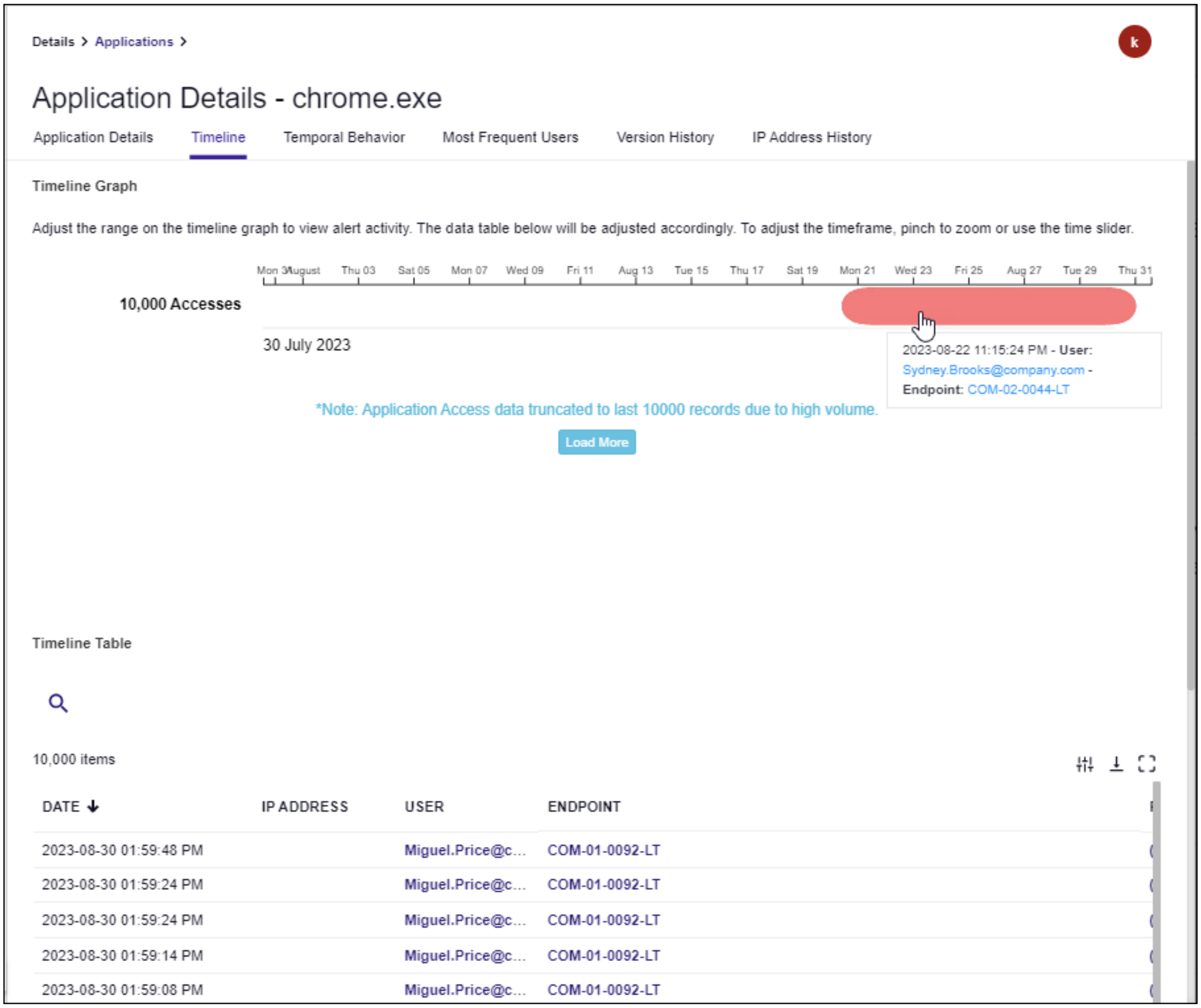
5,024 items

APPLICATION	FILE HASH	NUMBER ACCESSES ↓	DISTINCT USERS	DISTINCT ENDPOINTS	DISTINCT POLICIES	FIRST SEEN	LAST SEEN
8x8 - Virtual Office.exe	0F971E54B1AE6A4D8018EE5511F...	22,380	1	1	0	2023-05-17 12:10:59 PM	2023-05-26 05:25:02 PM
LocationNotificationWindows.exe	198C01E9D25EC009353776F75E5...	17,723	55	56	0	2023-05-07 08:03:20 PM	2023-08-30 01:21:29 PM
FullTrustNotifier.exe	4F6670C4DCD8D978B21D1DB91E...	16,145	45	47	0	2023-05-07 11:48:10 PM	2023-08-30 01:26:45 PM
BrowserCore.exe	AEF9422BB5FDD5C328DE834183...	14,173	81	81	0	2023-05-07 09:20:08 PM	2023-08-30 01:30:42 PM
chrome.exe	1042A6787687E19C48F12E6F49A...	13,593	104	104	0	2023-07-31 08:31:12 PM	2023-08-30 01:00:35 PM
chrome.exe	784ADEE709B6056B1EE337B7E1...	13,043	91	92	0	2023-06-13 06:32:24 PM	2023-07-21 02:40:48 PM
HPNETW~1.EXE	07DC1E275B8CE995E158A48B659...	10,384	1	1	0	2023-05-08 07:02:42 AM	2023-08-30 07:59:28 AM
chrome.exe	87C41FD9D56DB38FBA5C934284...	9,954	84	85	0	2023-06-28 02:25:24 AM	2023-07-24 02:51:23 AM
chrome.exe	8D03CE464B050BAD15F5C667D7...	9,714	95	96	0	2023-07-12 05:46:19 PM	2023-08-30 12:06:48 PM

The Application Details page lists all applications and includes summary statistics and links to further details. The **No Policy** check box is enabled by default and shows only applications without a policy applied. Disable the check box to see all applications.

If you click on any of the application names or file hashes you will be directed to that entity's details page, which shows the following:

- **Application Details**: lists key statistics such as total number of events and users, time range, and last event action.
- **Timeline**: shows all activity for the application, including timestamp, user, endpoint, policy, and IP address.
  - mouse over a colored circle for details on a particular event
  - the chart can be panned left and right by dragging or zoomed by scrolling, which also filters data in the table



Application Details - chrome.exe

Timeline Graph

Adjust the range on the timeline graph to view alert activity. The data table below will be adjusted accordingly. To adjust the timeframe, pinch to zoom or use the time slider.

2023-08-22 11:15:24 PM - **User:** Sydney.Brooks@company.com - **Endpoint:** COM-02-0044-LT

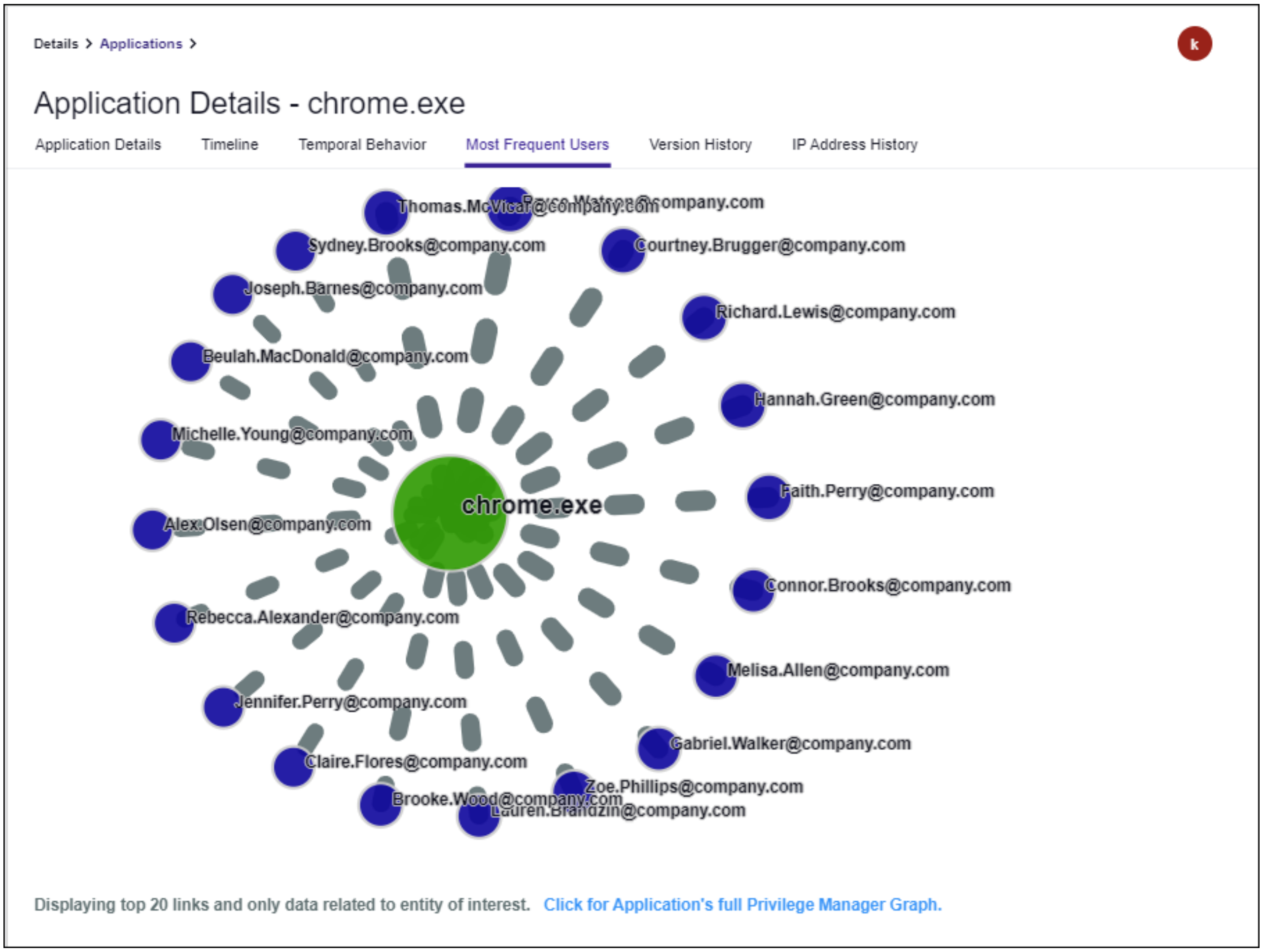
*Note: Application Access data truncated to last 10000 records due to high volume.

Timeline Table

10,000 items

DATE ↓	IP ADDRESS	USER	ENDPOINT
2023-08-30 01:59:48 PM		Miguel.Price@c...	COM-01-0092-LT
2023-08-30 01:59:24 PM		Miguel.Price@c...	COM-01-0092-LT
2023-08-30 01:59:24 PM		Miguel.Price@c...	COM-01-0092-LT
2023-08-30 01:59:14 PM		Miguel.Price@c...	COM-01-0092-LT
2023-08-30 01:59:08 PM		Miguel.Price@c...	COM-01-0092-LT

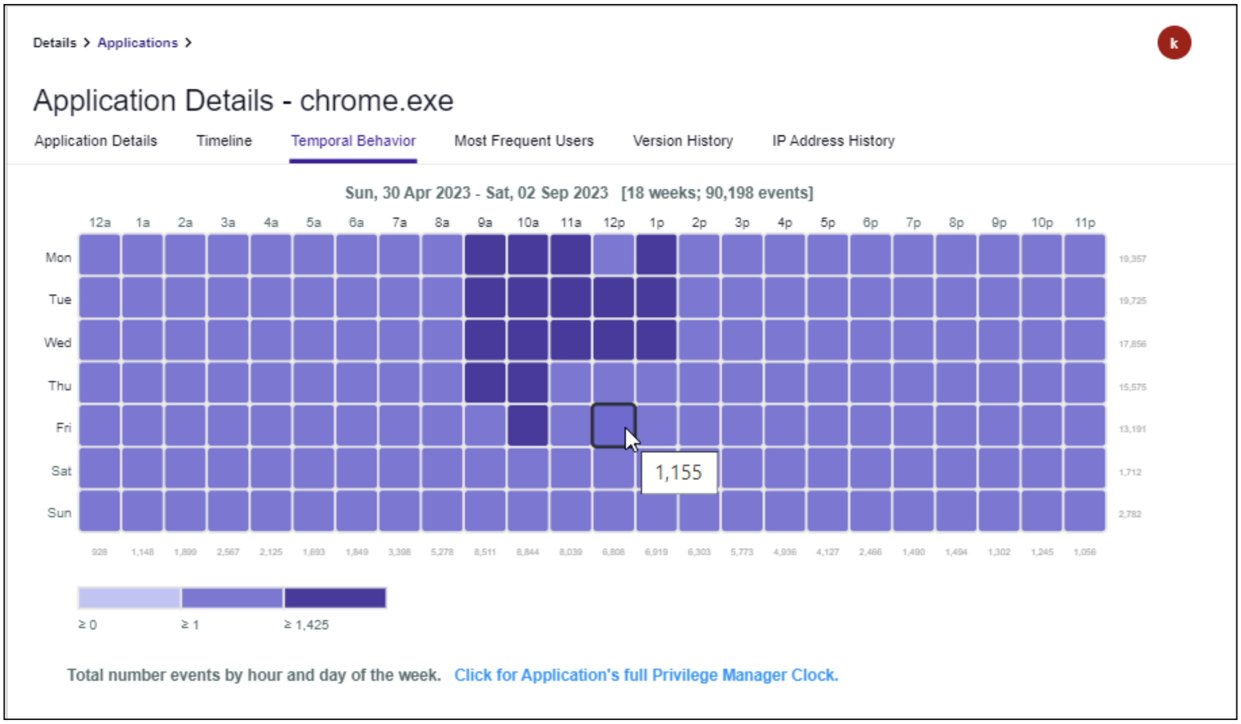
- **Most Frequent Users**: an animated representation of the top 20 users accessing the application the most; you can zoom into the graph by scrolling or right-click on any node or link to view more details.


Details > Applications >
k
Application Details
Timeline
Temporal Behavior
Most Frequent Users
Version History
IP Address History
chrome.exe
Thomas.McVicar@company.com
Royce.Watson@company.com
Sydney.Brooks@company.com
Courtney.Brugger@company.com
Joseph.Barnes@company.com
Richard.Lewis@company.com
Beulah.MacDonald@company.com
Hannah.Green@company.com
Michelle.Young@company.com
Faith.Perry@company.com
Alex.Olsen@company.com
Connor.Brooks@company.com
Rebecca.Alexander@company.com
Melisa.Allen@company.com
Jennifer.Perry@company.com
Gabriel.Walker@company.com
Claire.Flores@company.com
Zoe.Phillips@company.com
Brooke.Wood@company.com
Lauren.Brandzin@company.com

Application Details - chrome.exe

Displaying top 20 links and only data related to entity of interest. Click for Application's full Privilege Manager Graph.

- **Temporal Behavior**: a chart showing all temporal data for the application organized by hour of day and day of the week.
  - the numbers across the bottom indicate the total events involving that application for that hour of day
  - the values across the right side indicate the number of events involving that application for that day of the week
  - the legend at the bottom shows the number of events that correlate to the coloring of the chart blocks
    - mouse over a block to get the total number of events for that day of week and hour of day

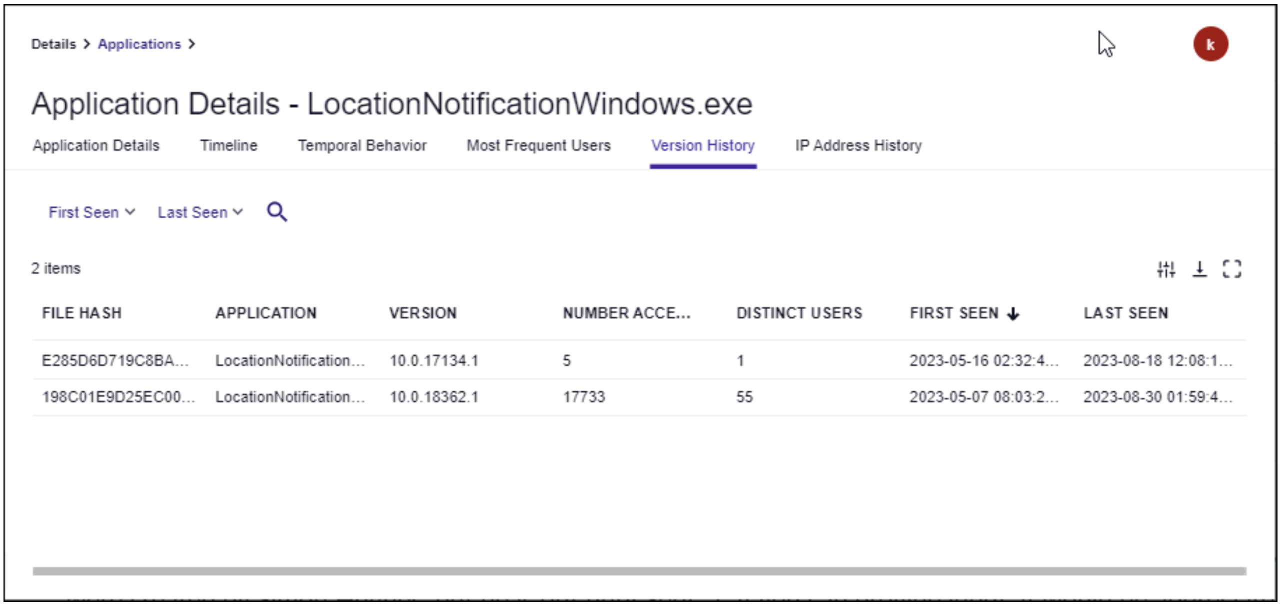


Application Details - chrome.exe

Sun, 30 Apr 2023 - Sat, 02 Sep 2023 [18 weeks; 90,198 events]

Total number events by hour and day of the week. Click for Application's full Privilege Manager Clock.

- **Version History (optional)**: a table of the various version numbers, number of users, and time range for each file hash (when an application name (not hash) details page was selected).

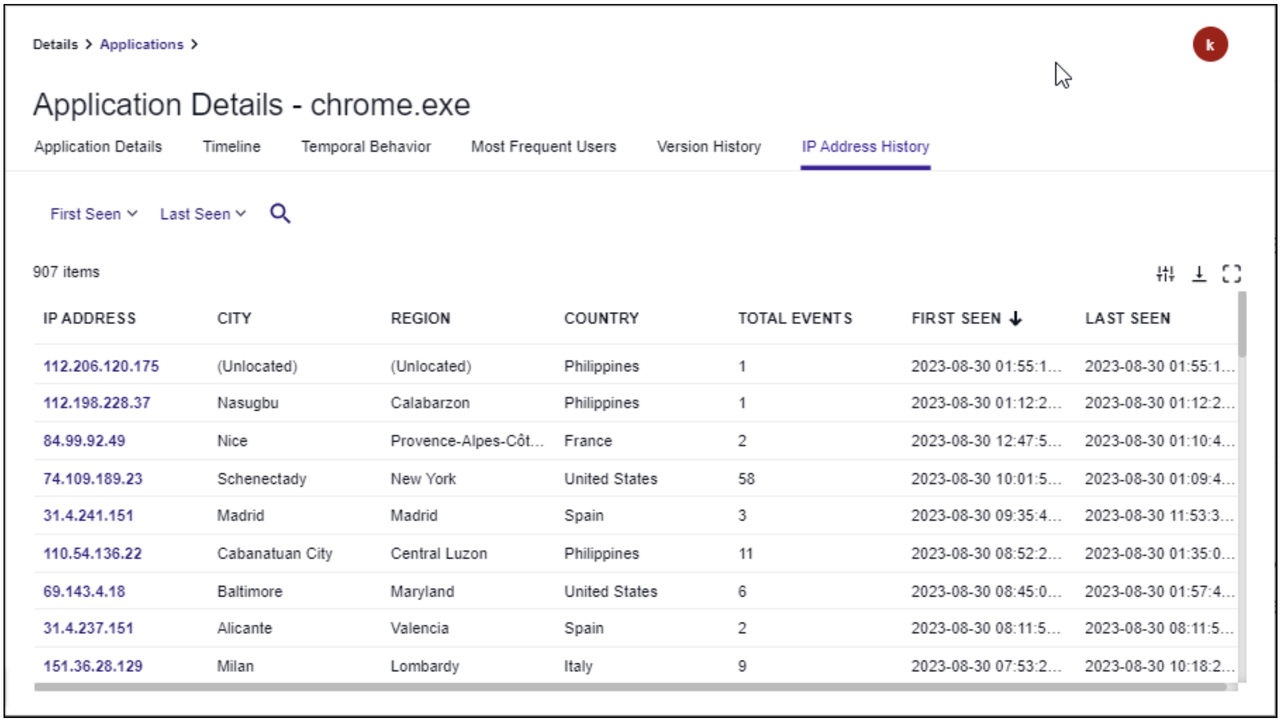


Application Details - LocationNotificationWindows.exe

2 items

FILE HASH	APPLICATION	VERSION	NUMBER ACCE...	DISTINCT USERS	FIRST SEEN ↓	LAST SEEN
E285D6D719C8BA...	LocationNotification...	10.0.17134.1	5	1	2023-05-16 02:32:4...	2023-08-18 12:08:1...
198C01E9D25EC00...	LocationNotification...	10.0.18362.1	17733	55	2023-05-07 08:03:2...	2023-08-30 01:59:4...

- **IP Address History**: a table of locations, total number of events, and time range of each IP address used to access the application.



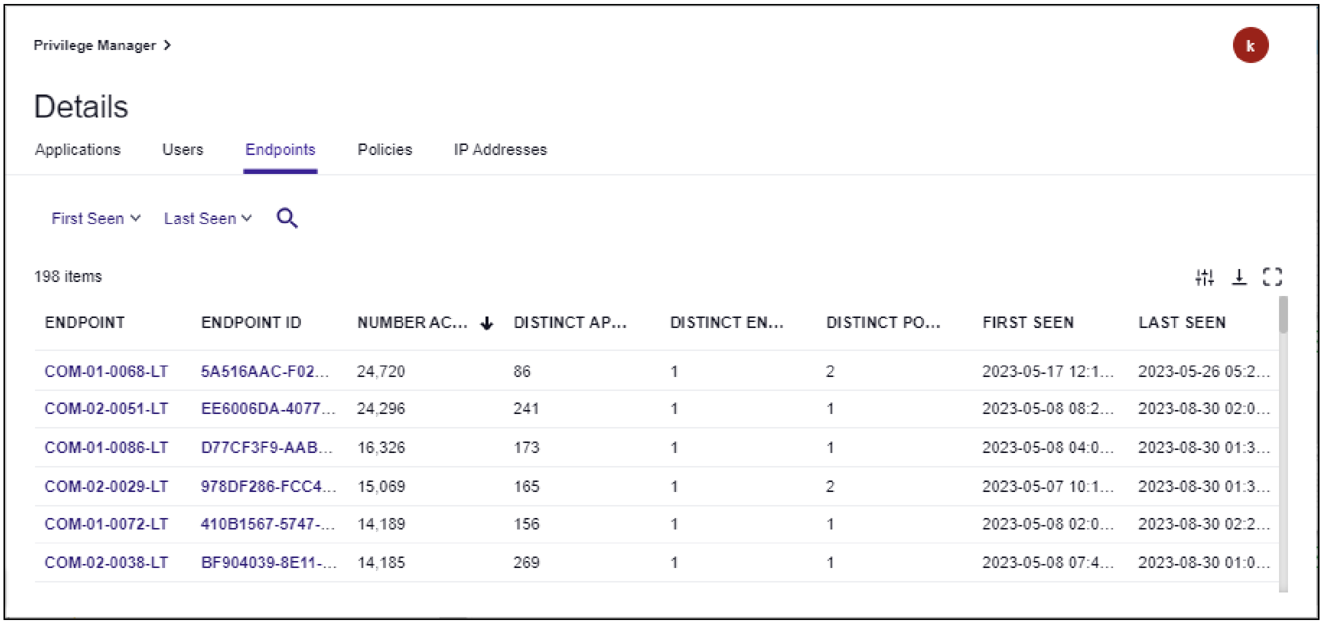
Application Details - chrome.exe

907 items

IP ADDRESS	CITY	REGION	COUNTRY	TOTAL EVENTS	FIRST SEEN	LAST SEEN
112.206.120.175	(Unlocated)	(Unlocated)	Philippines	1	2023-08-30 01:55:1...	2023-08-30 01:55:1...
112.198.228.37	Nasugbu	Calabarzon	Philippines	1	2023-08-30 01:12:2...	2023-08-30 01:12:2...
84.99.92.49	Nice	Provence-Alpes-Côt...	France	2	2023-08-30 12:47:5...	2023-08-30 01:10:4...
74.109.189.23	Schenectady	New York	United States	58	2023-08-30 10:01:5...	2023-08-30 01:09:4...
31.4.241.151	Madrid	Madrid	Spain	3	2023-08-30 09:35:4...	2023-08-30 11:53:3...
110.54.136.22	Cabanatuan City	Central Luzon	Philippines	11	2023-08-30 08:52:2...	2023-08-30 01:35:0...
69.143.4.18	Baltimore	Maryland	United States	6	2023-08-30 08:45:0...	2023-08-30 01:57:4...
31.4.237.151	Alicante	Valencia	Spain	2	2023-08-30 08:11:5...	2023-08-30 08:11:5...
151.36.28.129	Milan	Lombardy	Italy	9	2023-08-30 07:53:2...	2023-08-30 10:18:2...

Endpoint Details

The **Endpoint Details** page can be used to investigate endpoint activity from the perspective of many types of data collected on it. You can access Endpoint Details by navigating to **(Privilege Manager Analytics)** > **Details** > **Endpoints**.



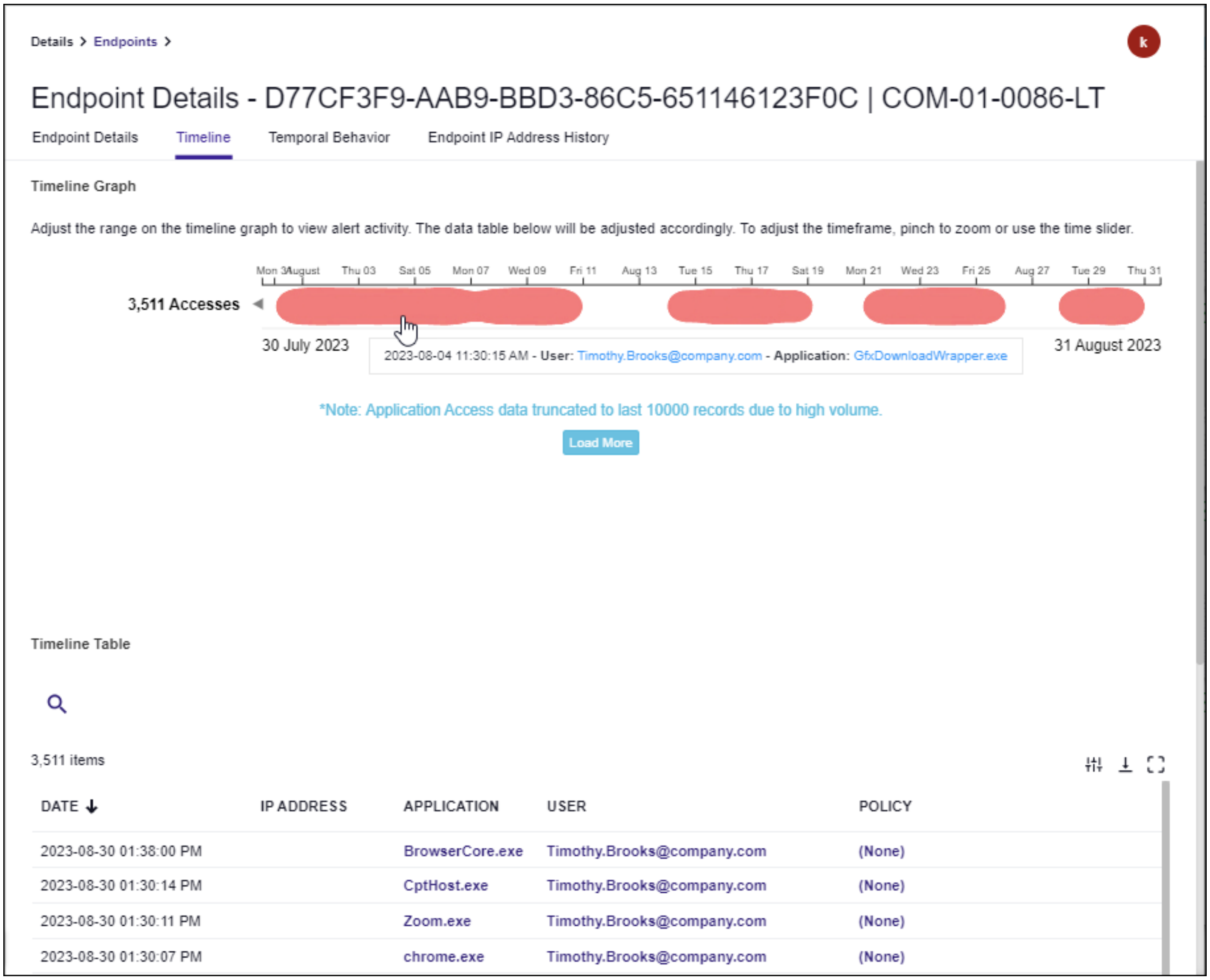
Details

198 items

ENDPOINT	ENDPOINT ID	NUMBER AC...	DISTINCT AP...	DISTINCT EN...	DISTINCT PO...	FIRST SEEN	LAST SEEN
COM-01-0068-LT	5A516AAC-F02...	24,720	86	1	2	2023-05-17 12:1...	2023-05-26 05:2...
COM-02-0051-LT	EE6006DA-4077...	24,296	241	1	1	2023-05-08 08:2...	2023-08-30 02:0...
COM-01-0086-LT	D77CF3F9-AAB...	16,326	173	1	1	2023-05-08 04:0...	2023-08-30 01:3...
COM-02-0029-LT	978DF286-FCC4...	15,069	165	1	2	2023-05-07 10:1...	2023-08-30 01:3...
COM-01-0072-LT	410B1567-5747-...	14,189	156	1	1	2023-05-08 02:0...	2023-08-30 02:2...
COM-02-0038-LT	BF904039-8E11-...	14,185	269	1	1	2023-05-08 07:4...	2023-08-30 01:0...

The Endpoint Details page lists all endpoints and includes summary statistics and links to further details. If you click on any of the endpoint names or IDs you will be directed to that entity's details page, which shows the following:

- **Endpoint Details**: lists key statistics such as total number of events, time range, and most active user.
- **Timeline**: shows all application access activity for the endpoint, including timestamp, policy, user, and IP address.
  - mouse over a colored circle for details on a particular event
  - the chart can be panned left and right by dragging or zoomed by scrolling, which also filters data in the table



Endpoint Details - D77CF3F9-AAB9-BBD3-86C5-651146123F0C | COM-01-0086-LT

Timeline Graph

Adjust the range on the timeline graph to view alert activity. The data table below will be adjusted accordingly. To adjust the timeframe, pinch to zoom or use the time slider.

2023-08-04 11:30:15 AM - **User:** Timothy.Brooks@company.com - **Application:** GfxDownloadWrapper.exe

*Note: Application Access data truncated to last 10000 records due to high volume.

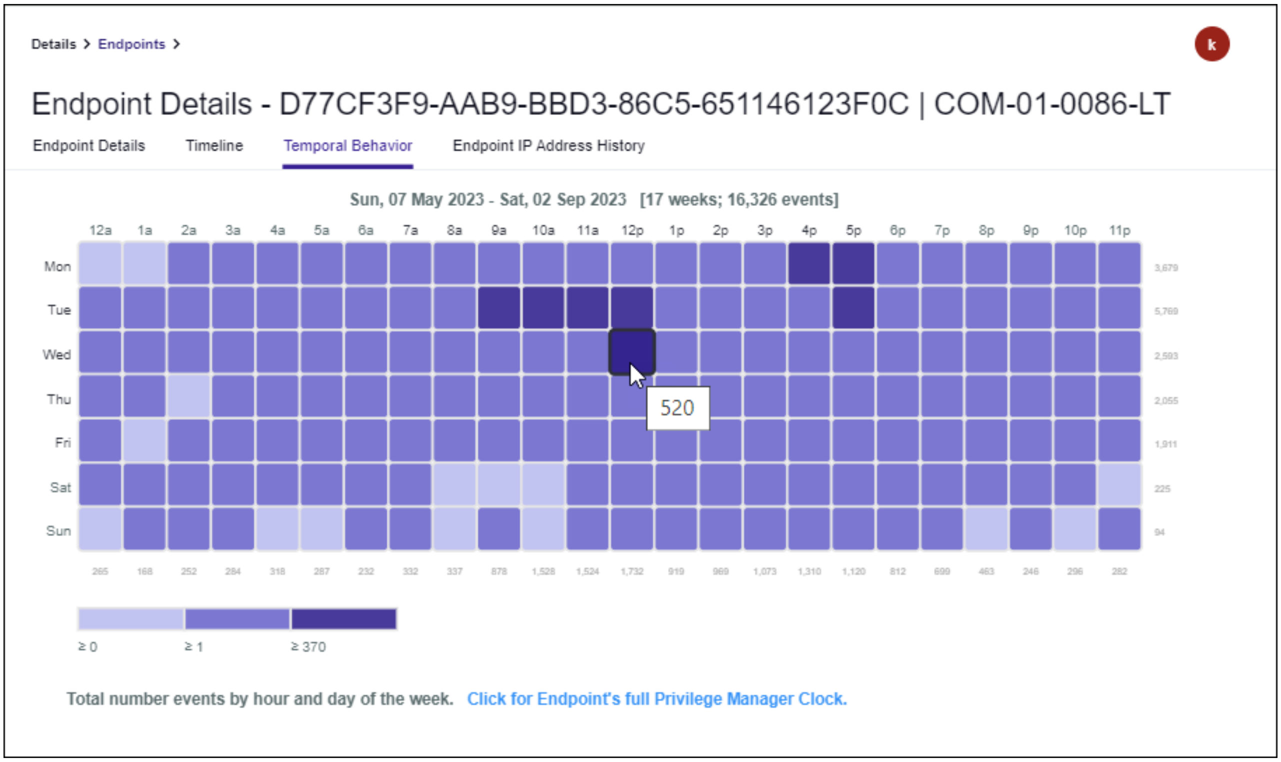
Timeline Table

3,511 items

DATE ↓	IP ADDRESS	APPLICATION	USER	POLICY
2023-08-30 01:38:00 PM		BrowserCore.exe	Timothy.Brooks@company.com	(None)
2023-08-30 01:30:14 PM		CptHost.exe	Timothy.Brooks@company.com	(None)
2023-08-30 01:30:11 PM		Zoom.exe	Timothy.Brooks@company.com	(None)
2023-08-30 01:30:07 PM		chrome.exe	Timothy.Brooks@company.com	(None)

- **Temporal Behavior**: shows a chart of all temporal data for the endpoint, organized by hour of day and day of the week.
  - the numbers across the bottom indicate the total events involving that endpoint for that hour of day
  - the values across the right side indicate the number of events involving that endpoint for that day of the week

- the legend at the bottom shows the number of events that correlate to the coloring of the chart blocks
    - mouse over a block to get the total number of events for that day of week and hour of day



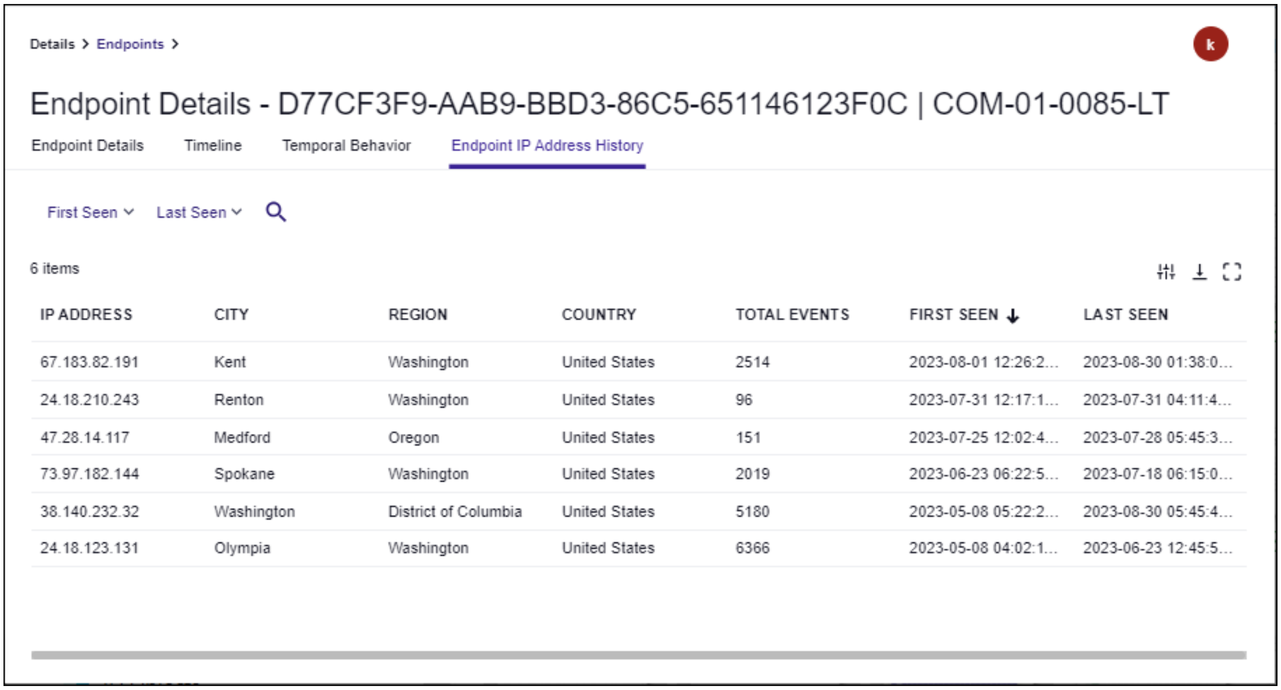
Details > Endpoints >

Endpoint Details - D77CF3F9-AAB9-BBD3-86C5-651146123F0C | COM-01-0086-LT

Sun, 07 May 2023 - Sat, 02 Sep 2023 [17 weeks; 16,326 events]

Total number events by hour and day of the week. Click for Endpoint's full Privilege Manager Clock.

- **Endpoint IP Address History**: shows a table of locations, total number of events, and time range of each IP address the endpoint was active on.



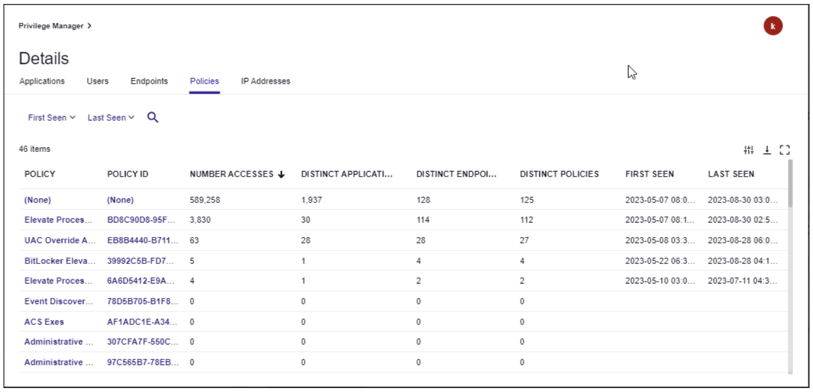
Endpoint Details - D77CF3F9-AAB9-BBD3-86C5-651146123F0C | COM-01-0085-LT

6 items

IP ADDRESS	CITY	REGION	COUNTRY	TOTAL EVENTS	FIRST SEEN	LAST SEEN
67.183.82.191	Kent	Washington	United States	2514	2023-08-01 12:26:2...	2023-08-30 01:38:0...
24.18.210.243	Renton	Washington	United States	96	2023-07-31 12:17:1...	2023-07-31 04:11:4...
47.28.14.117	Medford	Oregon	United States	151	2023-07-25 12:02:4...	2023-07-28 05:45:3...
73.97.182.144	Spokane	Washington	United States	2019	2023-06-23 06:22:5...	2023-07-18 06:15:0...
38.140.232.32	Washington	District of Columbia	United States	5180	2023-05-08 05:22:2...	2023-08-30 05:45:4...
24.18.123.131	Olympia	Washington	United States	6366	2023-05-08 04:02:1...	2023-06-23 12:45:5...

Policy Details

The **Policy Details** page can be used to investigate policy activity from the perspective of many types of data collected on it. You can access Policy Details by navigating to **(Privilege Manager Analytics)** > **Details** > **Policies**.



Details

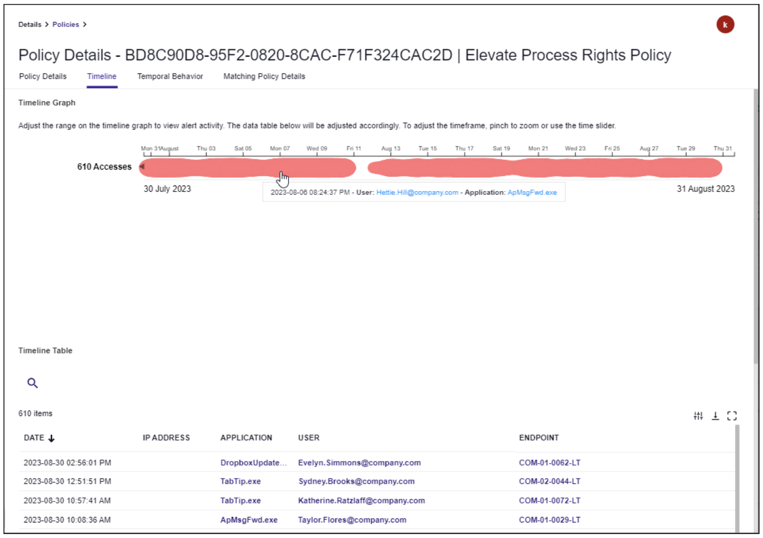
46 items

POLICY	POLICY ID	NUMBER ACCESSES	DISTINCT APPLICATI...	DISTINCT ENDPOI...	DISTINCT POLICIES	FIRST SEEN	LAST SEEN
(None)	(None)	589,258	1,937	128	125	2023-05-07 08:0...	2023-08-30 03:0...
Elevate Proces...	BD8C90D8-95F...	3,830	30	114	112	2023-05-07 08:1...	2023-08-30 02:5...
UAC Override A...	EB8B4440-B711...	63	28	28	27	2023-05-08 03:3...	2023-08-28 06:0...
BitLocker Eleva...	39992C5B-FD7...	5	1	4	4	2023-05-22 06:3...	2023-08-28 04:1...
Elevate Proces...	6A6D5412-E9A...	4	1	2	2	2023-05-10 03:0...	2023-07-11 04:3...
Event Discover...	78D5B705-B1F8...	0	0	0	0		
ACS Exes	AF1ADC1E-A34...	0	0	0	0		
Administrative ...	307CFA7F-550C...	0	0	0	0		
Administrative ...	97C565B7-78EB...	0	0	0	0		

The Policy Details page lists all policies and includes summary statistics and links to further details. If you click on any of the policy names or IDs you will be directed to that entity's details page, which shows the following:

- **Policy Details**: lists key statistics such as total number of events, time range, and most active user.
- **Timeline**: shows all application access activity for the policy, including timestamp, endpoint, user, and IP address.

- mouse over a colored circle for details on a particular event
- the chart can be panned left and right by dragging or zoomed by scrolling, which also filters data in the table



Policy Details - BD8C90D8-95F2-0820-8CAC-F71F324CAC2D | Elevate Process Rights Policy

Timeline Graph

Adjust the range on the timeline graph to view alert activity. The data table below will be adjusted accordingly. To adjust the timeframe, pinch to zoom or use the time slider.

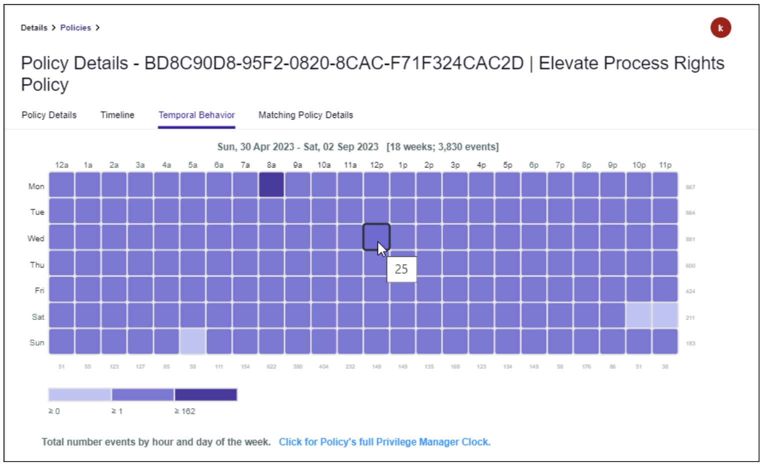
2023-08-06 08:24:37 PM - User: Hettie.Hill@company.com - Application: ApMsgFwd.exe

Timeline Table

610 items

DATE ↓	IP ADDRESS	APPLICATION	USER	ENDPOINT
2023-08-30 02:56:01 PM		DropboxUpdate...	Evelyn.Simmons@company.com	COM-01-0062-LT
2023-08-30 12:51:51 PM		TabTip.exe	Sydney.Brooks@company.com	COM-02-0044-LT
2023-08-30 10:57:41 AM		TabTip.exe	Katherine.Ratzlaff@company.com	COM-01-0072-LT
2023-08-30 10:08:36 AM		ApMsgFwd.exe	Taylor.Flores@company.com	COM-01-0029-LT

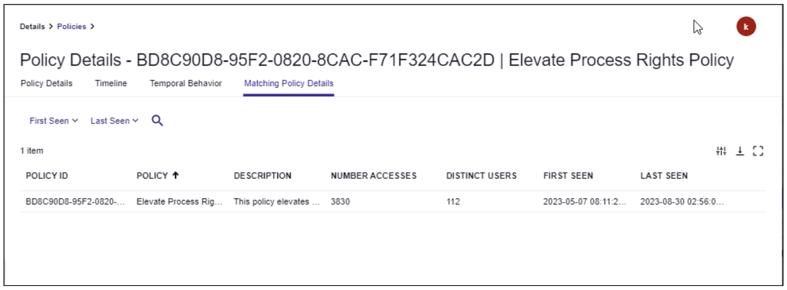
- **Temporal Behavior**: shows a chart of all temporal data for the policy organized by hour of day and day of the week.
  - the numbers across the bottom indicate the total events involving that policy for that hour of day
  - the values across the right side indicate the number of events involving that policy for that day of the week
  - the legend at the bottom shows the number of events that correlate to the coloring of the chart blocks
    - mouse over a block to get the total number of events for that day of week and hour of day



Policy Details - BD8C90D8-95F2-0820-8CAC-F71F324CAC2D | Elevate Process Rights Policy

Total number events by hour and day of the week. Click for Policy's full Privilege Manager Clock.

- **Matching Policy Details** - lists any policy with the same details as the selected policy.



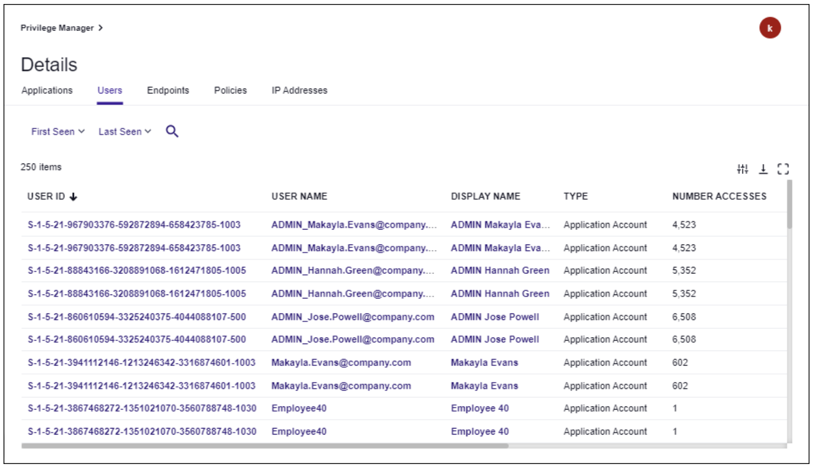
Policy Details - BD8C90D8-95F2-0820-8CAC-F71F324CAC2D | Elevate Process Rights Policy

1 item

POLICY ID	POLICY ↑	DESCRIPTION	NUMBER ACCESSES	DISTINCT USERS	FIRST SEEN	LAST SEEN
BD8C90D8-95F2-0820-...	Elevate Process Rig...	This policy elevates ...	3830	112	2023-05-07 08:11:2...	2023-08-30 02:56:0...

User Details

The **User Details** page can be used to investigate user activity from the perspective of many types of data collected on it. You can access User Details by navigating to **(Privilege Manager Analytics)** > **Details** > **Users**.



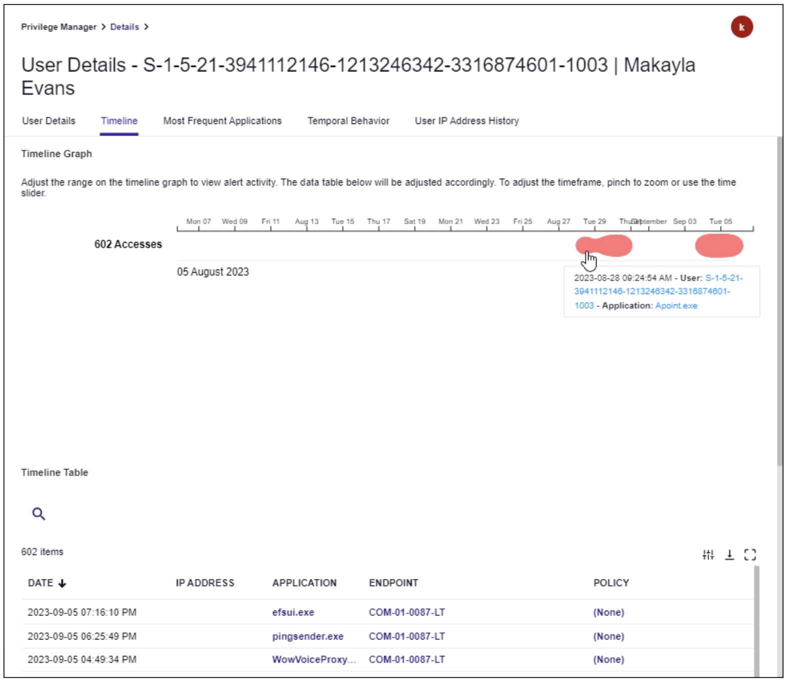
Details

250 items

USER ID ↓	USER NAME	DISPLAY NAME	TYPE	NUMBER ACCESSES
S-1-5-21-967903376-592872894-658423785-1003	ADMIN_Makayla.Evans@company....	ADMIN Makayla Eva...	Application Account	4,523
S-1-5-21-967903376-592872894-658423785-1003	ADMIN_Makayla.Evans@company....	ADMIN Makayla Eva...	Application Account	4,523
S-1-5-21-88843166-3208891068-1612471805-1005	ADMIN_Hannah.Green@company....	ADMIN Hannah Green	Application Account	5,352
S-1-5-21-88843166-3208891068-1612471805-1005	ADMIN_Hannah.Green@company....	ADMIN Hannah Green	Application Account	5,352
S-1-5-21-860610594-3325240375-4044088107-500	ADMIN_Jose.Powell@company.com	ADMIN Jose Powell	Application Account	6,508
S-1-5-21-860610594-3325240375-4044088107-500	ADMIN_Jose.Powell@company.com	ADMIN Jose Powell	Application Account	6,508
S-1-5-21-3941112146-1213246342-3316874601-1003	Makayla.Evans@company.com	Makayla Evans	Application Account	602
S-1-5-21-3941112146-1213246342-3316874601-1003	Makayla.Evans@company.com	Makayla Evans	Application Account	602
S-1-5-21-3867468272-1351021070-3560788748-1030	Employee40	Employee 40	Application Account	1
S-1-5-21-3867468272-1351021070-3560788748-1030	Employee40	Employee 40	Application Account	1

The User Details page lists all users and includes summary statistics and links to further details. If you click on any of the user names or IDs you will be directed to that entity's details page, which shows the following:

- **User Details**: lists key statistics such as total number of events and applications, time range, and last event action
- **Timeline**: shows all application access activity for the user, including timestamp, endpoint, policy, and IP address
  - mouse over a colored circle for details on a particular event
  - the chart can be panned left and right by dragging or zoomed by scrolling, which also filters data in the table



Privilege Manager > Details >

User Details - S-1-5-21-3941112146-1213246342-3316874601-1003 | Makayla Evans

Timeline Graph

Adjust the range on the timeline graph to view alert activity. The data table below will be adjusted accordingly. To adjust the timeframe, pinch to zoom or use the time slider.

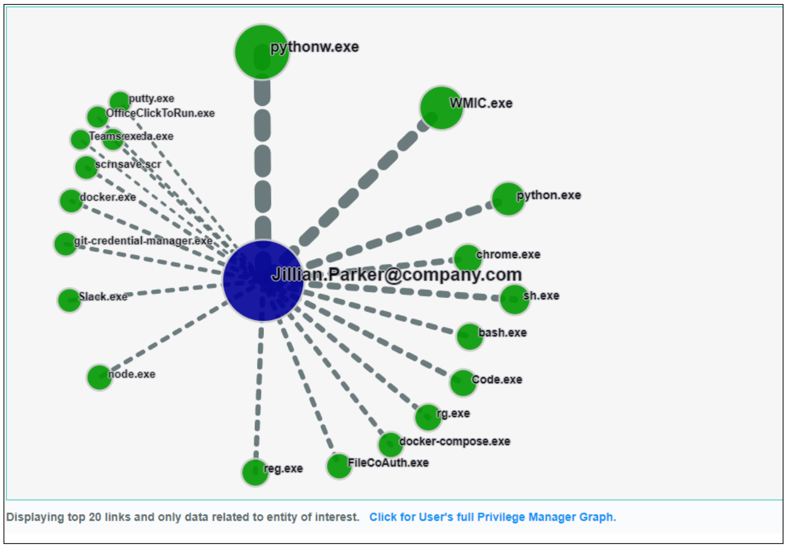
2023-08-28 09:24:54 AM - User: S-1-5-21-3941112146-1213246342-3316874601-1003 - Application: Apoint.exe

Timeline Table

602 items

DATE ↓	IP ADDRESS	APPLICATION	ENDPOINT	POLICY
2023-09-05 07:16:10 PM		efsui.exe	COM-01-0087-LT	(None)
2023-09-05 06:25:49 PM		pingsender.exe	COM-01-0087-LT	(None)
2023-09-05 04:49:34 PM		WowVoiceProxy...	COM-01-0087-LT	(None)

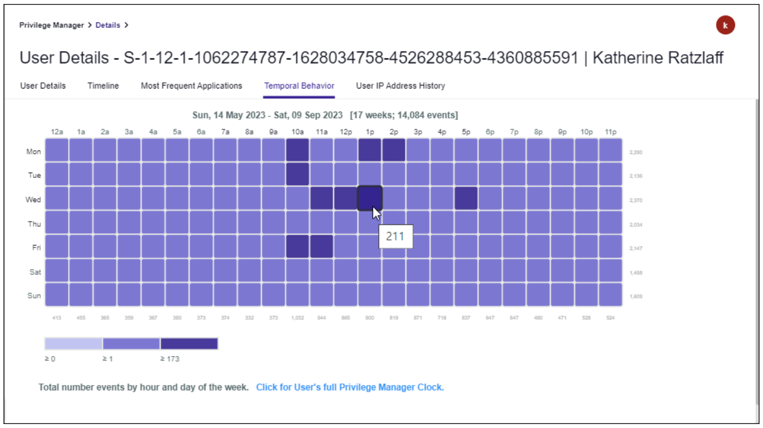
- **Most Frequent Applications**: an animated representation of the top 20 applications the user accesses most; you can zoom into the graph by scrolling or right-click on any node or link to view more details



Displaying top 20 links and only data related to entity of interest. Click for User's full Privilege Manager Graph.

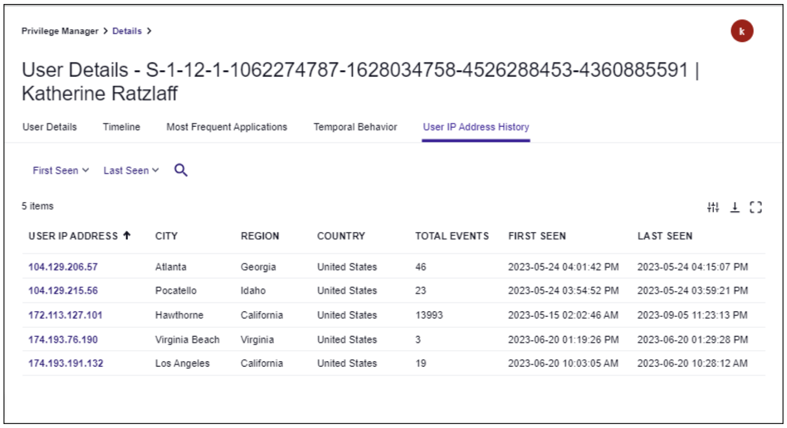
- **Temporal Behavior**: a chart showing all temporal data for the user organized by hour of day and day of the week
  - the numbers across the bottom indicate the total events involving that user for that hour of day
  - the values across the right side indicate the number of events involving that user for that day of the week

- the legend at the bottom shows the number of events that correlate to the coloring of the chart blocks
  - mouse over a block to get the total number of events for that day of week and hour of day


Privilege Manager > Details >
k
User Details - S-1-12-1-1062274787-1628034758-4526288453-4360885591 | Katherine Ratzlaff
User Details
Timeline
Most Frequent Applications
Temporal Behavior
User IP Address History
Sun, 14 May 2023 - Sat, 09 Sep 2023 [17 weeks; 14,084 events]
12a 1a 2a 3a 4a 5a 6a 7a 8a 9a 10a 11a 12p 1p 2p 3p 4p 5p 6p 7p 8p 9p 10p 11p
Mon
Tue
Wed
Thu
Fri
Sat
Sun
2,290
2,136
2,370
2,034
2,147
1,498
1,609
413 455 365 359 367 380 373 374 332 373 1,032 944 865 900 819 871 718 837 647 647 490 471 528 524
211
≥ 0
≥ 1
≥ 173

Total number events by hour and day of the week. Click for User's full Privilege Manager Clock.

- **IP Address History**: a table of locations, total number of events, and time range of each IP address the user was active on



User Details - S-1-12-1-1062274787-1628034758-4526288453-4360885591 | Katherine Ratzlaff

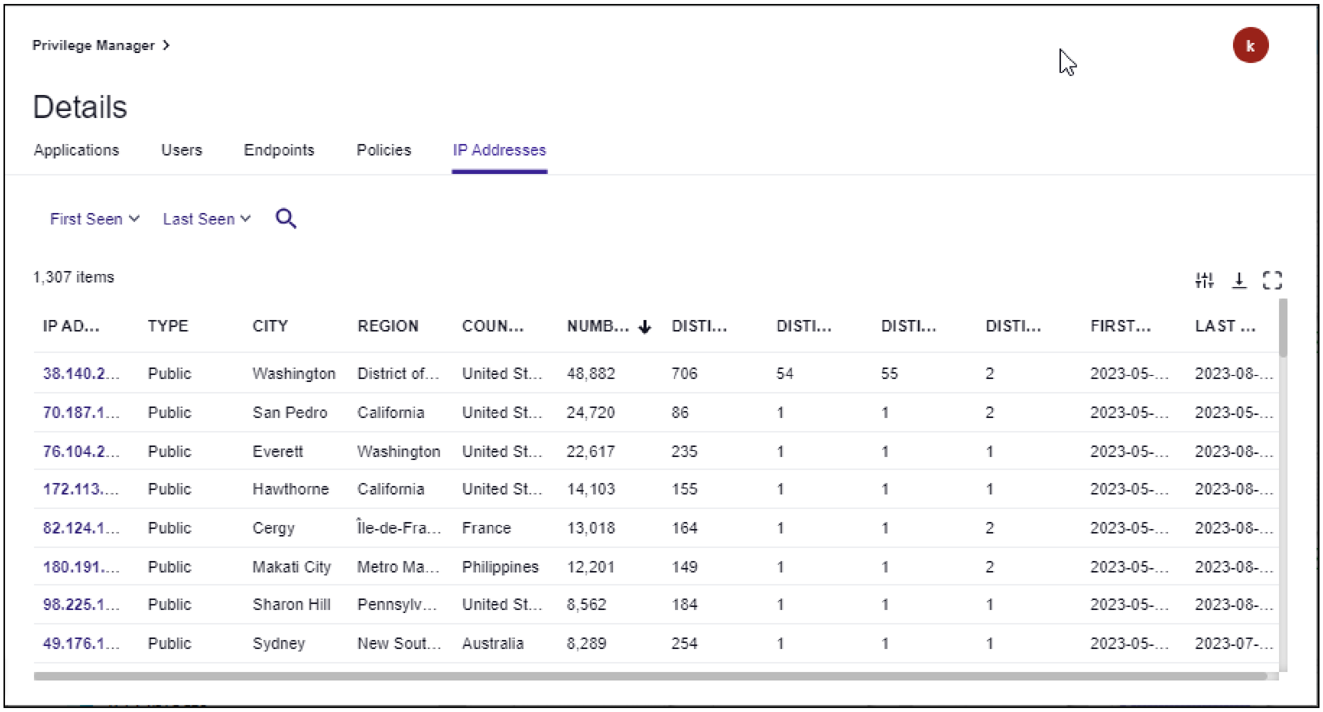
5 items

USER IP ADDRESS ↑	CITY	REGION	COUNTRY	TOTAL EVENTS	FIRST SEEN	LAST SEEN
104.129.206.57	Atlanta	Georgia	United States	46	2023-05-24 04:01:42 PM	2023-05-24 04:15:07 PM
104.129.215.56	Pocatello	Idaho	United States	23	2023-05-24 03:54:52 PM	2023-05-24 03:59:21 PM
172.113.127.101	Hawthorne	California	United States	13993	2023-05-15 02:02:46 AM	2023-09-05 11:23:13 PM
174.193.76.190	Virginia Beach	Virginia	United States	3	2023-06-20 01:19:26 PM	2023-06-20 01:29:28 PM
174.193.191.132	Los Angeles	California	United States	19	2023-06-20 10:03:05 AM	2023-06-20 10:28:12 AM

IP Address Details

The **IP Address Details** page can be used to investigate IP address activity from the perspective of many types of data collected on it. You can access IP Address Details by navigating to **(Privilege Manager Analytics)** > **Details** > **IP Addresses**.

The **Private** IP location is used to set a default location for cases where only internal (private) IP addresses are present in the data. This is particularly useful for visualizing and analyzing activity by IP address and location, especially when dealing with internal networks. Private IP addresses have no geographic location values. Instead, values reflect IP configuration.



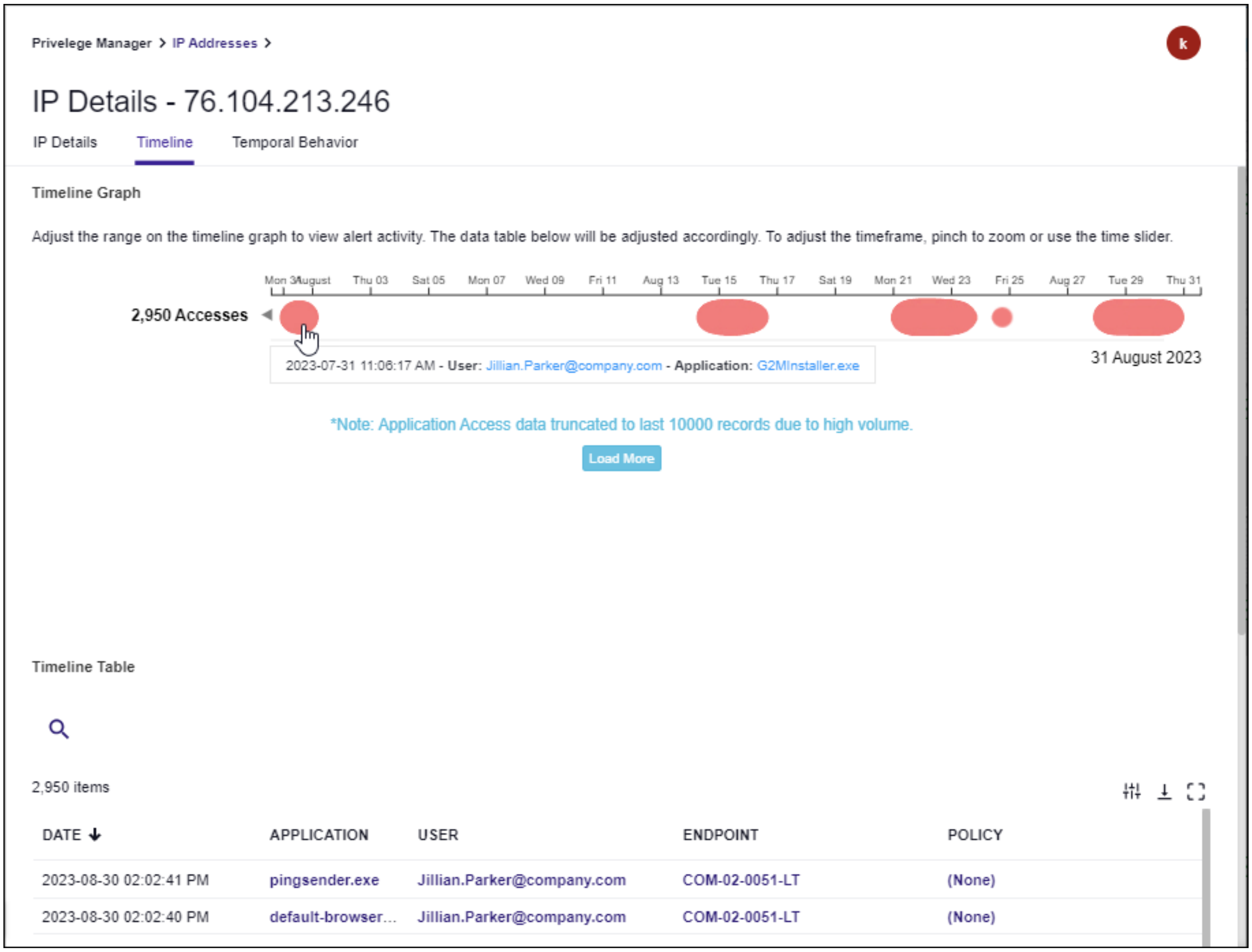
Details

1,307 items

IP AD...	TYPE	CITY	REGION	COUN...	NUMB... ↓	DISTI...	DISTI...	DISTI...	DISTI...	FIRST...	LAST ...
38.140.2...	Public	Washington	District of...	United St...	48,882	706	54	55	2	2023-05-...	2023-08-...
70.187.1...	Public	San Pedro	California	United St...	24,720	86	1	1	2	2023-05-...	2023-05-...
76.104.2...	Public	Everett	Washington	United St...	22,617	235	1	1	1	2023-05-...	2023-08-...
172.113....	Public	Hawthorne	California	United St...	14,103	155	1	1	1	2023-05-...	2023-08-...
82.124.1...	Public	Cergy	Île-de-Fra...	France	13,018	164	1	1	2	2023-05-...	2023-08-...
180.191....	Public	Makati City	Metro Ma...	Philippines	12,201	149	1	1	2	2023-05-...	2023-08-...
98.225.1...	Public	Sharon Hill	Pennsylv...	United St...	8,562	184	1	1	1	2023-05-...	2023-08-...
49.176.1...	Public	Sydney	New Sout...	Australia	8,289	254	1	1	1	2023-05-...	2023-07-...

The IP Address Details page lists all IP addresses and includes summary statistics and links to further details. If you click on any of the IP addresses you will be directed to the details page, which shows the following:

- **IP Details**: lists key statistics such as total number of events, time range, and most active user.
- **Timeline**: shows all application access activity for the IP address, including timestamp, endpoint, user, and IP address.
  - mouse over a colored circle for details on a particular event
  - the chart can be panned left and right by dragging or zoomed by scrolling, which also filters data in the table



IP Details - 76.104.213.246

IP Details | Timeline | Temporal Behavior

Timeline Graph

Adjust the range on the timeline graph to view alert activity. The data table below will be adjusted accordingly. To adjust the timeframe, pinch to zoom or use the time slider.

2023-07-31 11:06:17 AM - **User:** Jillian.Parker@company.com - **Application:** G2MInstaller.exe

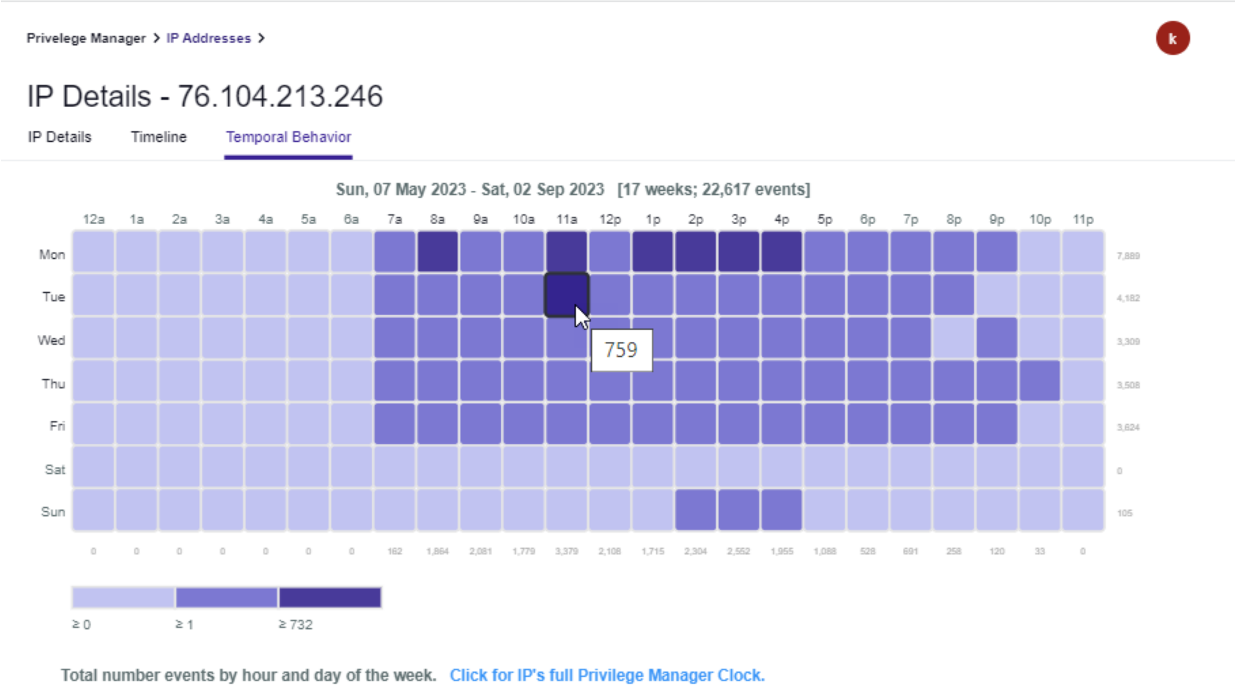
*Note: Application Access data truncated to last 10000 records due to high volume.

Timeline Table

2,950 items

DATE ↓	APPLICATION	USER	ENDPOINT	POLICY
2023-08-30 02:02:41 PM	pingsender.exe	Jillian.Parker@company.com	COM-02-0051-LT	(None)
2023-08-30 02:02:40 PM	default-browser…	Jillian.Parker@company.com	COM-02-0051-LT	(None)

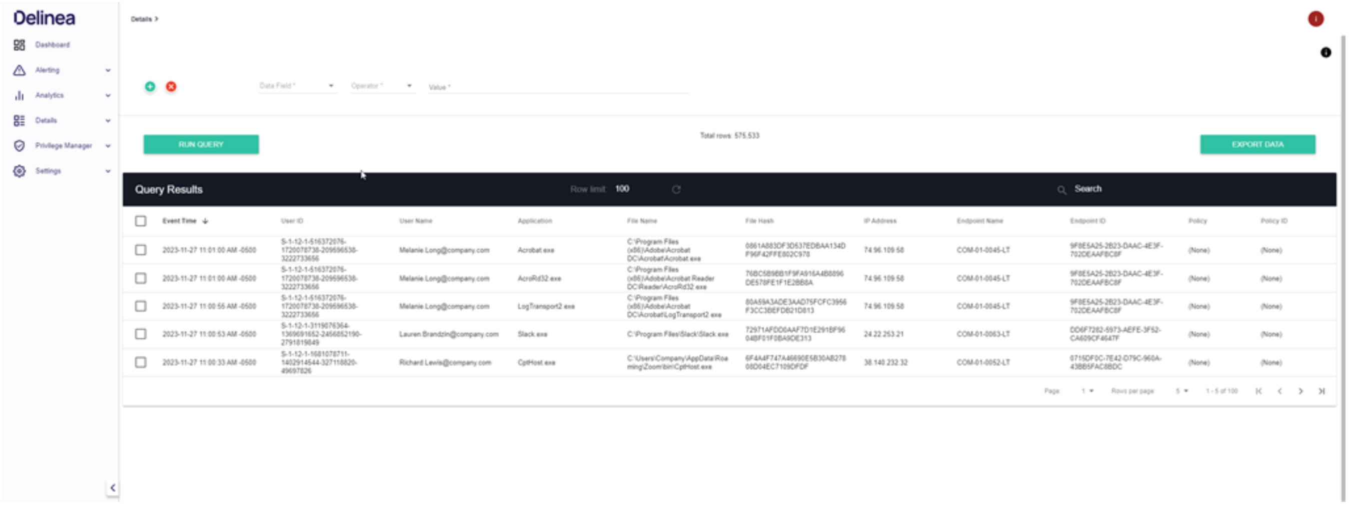
- **Temporal Behavior**: shows a chart of all temporal data for the IP address organized by hour of day and day of the week.
  - the numbers across the bottom indicate the total events involving that IP address for that hour of day
  - the values across the right side indicate the number of events involving that IP address for that day of the week
  - the legend at the bottom shows the number of events that correlate to the coloring of the chart blocks
    - mouse over a block to get the total number of events for that day of week and hour of day



Total number events by hour and day of the week. Click for IP's full Privilege Manager Clock.

Query

Queries allow you to retrieve data that meet criteria you specify for application executions. A table shows results of the query, and data can be exported for offline analysis or auditing.



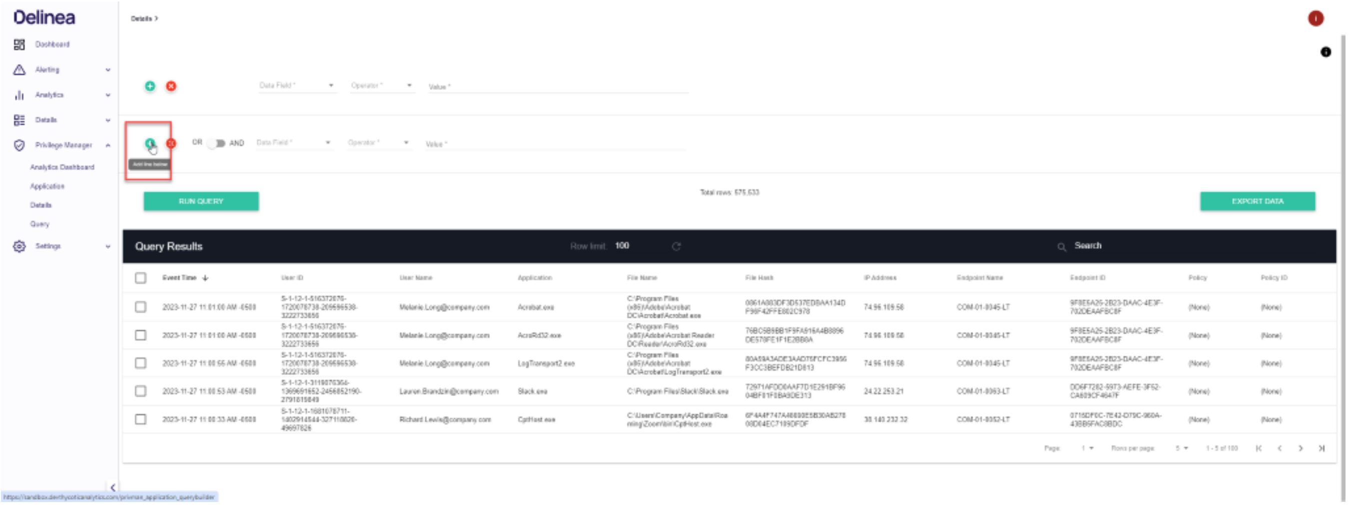
Total rows: 575,533

□	Event Time ↓	User ID	User Name	Application	File Name	File Hash	IP Address	Endpoint Name	Endpoint ID	Policy	Policy ID
□	2023-11-27 11:01:00 AM -0500	S-1-12-1-516372076-1720078738-209596538-3222733656	Melanie.Long@company.com	Acrobat.exe	C:\Program Files (x86)\Adobe\Acrobat DC\Acrobat\Acrobat.exe	0861A883DF3D537EDBAA134DF96F42FFE802C978	74.96.109.58	COM-01-0045-LT	9F8E5A25-2B23-DAAC-4E3F-702DEAAFBC8F	(None)	(None)
□	2023-11-27 11:01:00 AM -0500	S-1-12-1-516372076-1720078738-209596538-3222733656	Melanie.Long@company.com	AcroRd32.exe	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	76BC5B9BB1F9FA916A4B8896DE578FE1F1E2BB8A	74.96.109.58	COM-01-0045-LT	9F8E5A25-2B23-DAAC-4E3F-702DEAAFBC8F	(None)	(None)
□	2023-11-27 11:00:55 AM -0500	S-1-12-1-516372076-1720078738-209596538-3222733656	Melanie.Long@company.com	LogTransport2.exe	C:\Program Files (x86)\Adobe\Acrobat DC\Acrobat\LogTransport2.exe	80A59A3ADE3AAD75FCFC3956F3CC3BEFDB21D813	74.96.109.58	COM-01-0045-LT	9F8E5A25-2B23-DAAC-4E3F-702DEAAFBC8F	(None)	(None)
□	2023-11-27 11:00:53 AM -0500	S-1-12-1-3119076364-1369691652-2456852190-2791819849	Lauren.Brandzin@company.com	Slack.exe	C:\Program Files\Slack\Slack.exe	72971AFDD0AAF7D1E291BF9604BF01F0BA9DE313	24.22.253.21	COM-01-0063-LT	DD6F7282-5973-AEFE-3F52-CA609CF4647F	(None)	(None)
□	2023-11-27 11:00:33 AM -0500	S-1-12-1-1681078711-1402914544-327118820-49697826	Richard.Lewis@company.com	CptHost.exe	C:\Users\Company\AppData\Roaming\Zoom\bin\CptHost.exe	6F4A4F747A46690E5B30AB27808D04EC7109DFDF	38.140.232.32	COM-01-0052-LT	0715DF0C-7E42-D79C-960A-43BB5FAC8BDC	(None)	(None)

Page: 1 ▾ Rows per page: 5 ▾ 1 - 5 of 100

Click the Toggle Theme button to change between light and dark themes.

On each query line, click the Add Line button to insert a line below the current line. Click the Remove Line button to delete the current line.



Total rows: 575,633

Query Results — Row limit: 100

Event Time	User ID	User Name	Application	File Name	File Hash	IP Address	Endpoint Name	Endpoint ID	Policy	Policy ID
2023-11-27 11:01:00 AM -0600	S-1-12-1-516372876-1720078738-209596538-3222733656	Melanie.Long@company.com	Acrobat.exe	C:\Program Files (x86)\Adobe\Acrobat DC\Acrobat\Acrobat.exe	0061A003DF3D537EDBAA134DF98F42FFE802C978	74.96.109.58	COM-01-0045-LT	9F8E5A25-2B23-DAAC-4E3F-702DEAAFBC8F	(None)	(None)
2023-11-27 11:01:00 AM -0600	S-1-12-1-516372876-1720078738-209596538-3222733656	Melanie.Long@company.com	AcroRd32.exe	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	76BC5B9BB1F9FA916A4B8896DE578FE1F1E2BB8A	74.96.109.58	COM-01-0045-LT	9F8E5A25-2B23-DAAC-4E3F-702DEAAFBC8F	(None)	(None)
2023-11-27 11:00:56 AM -0600	S-1-12-1-516372876-1720078738-209596538-3222733656	Melanie.Long@company.com	LogTransport2.exe	C:\Program Files (x86)\Adobe\Acrobat DC\Acrobat\LogTransport2.exe	80A59A3ADE3AAD75FCFC3956F3CC3BEFDB21D813	74.96.109.58	COM-01-0045-LT	9F8E5A25-2B23-DAAC-4E3F-702DEAAFBC8F	(None)	(None)
2023-11-27 11:00:53 AM -0600	S-1-12-1-3119076364-1369691652-2456852190-2791815849	Lauren.Brandzin@company.com	Slack.exe	C:\Program Files\Slack\Slack.exe	72971AFDD0AAF7D1E291BF9604BF81F0BA9DE313	24.22.253.21	COM-01-0063-LT	DD6F7282-59T3-AEFE-3F52-CA809CF4847F	(None)	(None)
2023-11-27 11:00:33 AM -0600	S-1-12-1-1681078711-1402914544-327110826-49697826	Richard.Lewis@company.com	CptHost.exe	C:\Users\Company\AppData\Roaming\Zoom\bin\CptHost.exe	6F4A4F747A46890E5B30AB27808D04EC7189DFDF	38.140.232.32	COM-01-0052-LT	0716DF0C-7E42-D79C-960A-43BB6FAC8BDC	(None)	(None)

Page: 1 ▾ Rows per page: 5 ▾ 1 - 5 of 100

Select **OR** or **AND** using the switch to apply that condition to the line above plus the current line. The **AND** lines will be grouped together as if they were enclosed in parentheses with **OR** applied between each group.

All three options: **Data Field**, **Operator**, and **Value** must be set for the line to be included in the query. A check mark will appear on the right side when all selections are valid.

The **Value** search input accepts "*" (wildcard) and uppercase **AND**, **NOT**, and **OR** searches (but no mixing **AND**, **NOT**, **OR**, nor parentheses). Some data field types show their values with a prefix (e.g., "IP: 127.0.0.1"). When using the "contains" and "not contains" operators, wildcards ("*") are allowed in the search term.

For "Event Time" entries, most time formats are accepted. For "Temporal" data types the application assumes timestamps are in the Local Timezone set in System Settings.

Press **Run Query** to display a table of results. Rows can be selected for export (**Export Data**). The **Row Limit** input allows changing the maximum number of rows stored in the table. The Search box filters any matching table rows.

Data returned are the most recent events based on the latest update and could be delayed several minutes from the current time.

> Important: IP address locations are prone to change and can be inaccurate and imprecise, sometimes located to only the region or country level. This app shows only the most recent available IP address location information, which might have been updated since the time an IP address was last accessed. Location data are derived from MaxMind's GeoLite2.

PBA Responsive Actions

In Privileged Behavior Analytics, anomalous behavior is characterized as an event and assigned a risk level. If this risk level exceeds a pre-defined threshold, the following response actions may be used to triage the potential threat:

- Notification Actions
  - Email Notifications
- Dynamic Actions

- Access Challenges
- Webhooks
- Codehooks

Email Notifications

Each PBA user may set an email and choose to be notified when an event occurs. Upon receipt of an email notification, the anomalous activity should be investigated and remediated if necessary.

Access Challenges

Access Challenges provide automated responses in Secret Server to PBA events. They allow for the dynamic configuration of the trust level in the Secret Access Workflow which is built into Secret Server.

- For example, it may be infeasible to configure Session Recording on every Secret (disk space and CPU limitations) and it may be considered onerous to configure the Approval workflow on every Secret (administrators become desensitized to approving access to every single request).

  With Access Challenges, however, these workflows can be enabled dynamically when a user's behavior has become suspicious, helping to ease the tension operationally between security and efficiency.

An expiration duration may be specified for the Challenge, or the Challenge may be valid indefinitely.

- For the **Login** and **Two Factor** Challenges, the challenged user may clear the Challenge by re-authenticating.
- For the other Challenge types, a Secret Server user with PBA permissions must clear the Challenge for the user, or the user must wait for expiration.

  For example, a **Requires Approval** Challenge may be configured with a two-hour expiration. This gives the security team a buffer of time to investigate the anomalous activity, while allowing the user to still access their usual Secrets, but in a more restricted workflow.

Challenges in Version 10.2.000000 and Later

- **Login**: User must re-authenticate with Secret Server.

Challenges in Version 10.3.000015 and Later

- **Two Factor**: User must re-authenticate with Secret Server and the Two Factor Remember Me is expired if set.
- **Require Approval**: User must request approval for accessing any secrets unless they are the only Approver for that secret.
- **Lockout**: User is locked out from Secret Server. This may be configured to include Secret Servers that use SAML and integrated authentication.

Challenges in Version 10.4.00000X and Later

- **Session Recording**: User has their sessions recorded for any secrets that are capable of session recording.
  - This session recording is surreptitious, and there is no indicator to the user that they are being recorded.

Webhook

The Webhook action HTTP posts the metadata associated with the anomalous activity event (the user, the time, the actions or secrets accessed) to a user-defined HTTP endpoint.

The Webhook provides the capability to integrate PBA events into many other workflow and security systems. Examples include sending a message to a messaging application such as Slack or creating a case in a ticketing system like ServiceNow.

See the PBA Administration Section’s "Webhooks" on page 102 article for more about Webhooks.

Codehook

Codehooks allow integration with external workflow and security systems where a Webhook is insufficient for the desired behavior. They are user-defined scripts that execute in response to the anomalous activity event.

- Currently Python 2.7 scripts are supported, and Node.js support will be added in a future release.

An example of a Codehook response action is suspending the user’s Okta account. This action cannot be achieved by a simple Webhook, despite Okta’s REST API, because it requires a two-step process of looking up the user by email, and then using the user’s internal Okta identifier to suspend the account.

See the PBA Administration Section’s "Codehooks" on page 105 article for more about Codehooks.

Privileged Behavior Analytics Administration

In Privileged Behavior Analytics, most administrative tasks will occur on the System Settings page, which is used to set basic configurations for alert notifications and other general settings.

You can navigate to System Settings by clicking on the cogwheel symbol at the top right of any Privileged Behavior Analytics page and choosing System Settings.

Responsive Actions Settings

The Responsive Actions section of System Settings is used to configure Privileged Behavior Analytics to take automated action based on user risk score.

Alert Threshold: The numerical value an alert needs to meet or exceed to send an email and log the event on the Alerts page.

Alert Action: Provides three different automated actions that Privileged Behavior Analytics can take in response to an Alert Event.

- The **Challenge** response can be configured to automatically impose additional controls on a Secret Server user if their actions cause Privileged Behavior Analytics to generate an alert that meets or exceeds the Alert Threshold. The current version of Privileged Behavior Analytics can challenge a user by
  - logging them out of Secret Server
  - forcing them to do 2-factor authentication

- locking a user out of Secret Server
- forcing them to request access to any Secrets they access Challenges must be configured on Secret Server as well. More information on how to configure Challenges can be found in "Getting Started" on page 5.

- The Webhook response can be configured to integrate with external systems by sending an HTTP post when Privileged Behavior Analytics has a user alert event. Additional information can be found in the Privileged Behavior Analytics"PBA Responsive Actions" on page 98 article.
- The **Code Hook** response can be configured to integrate with external systems by executing a user provided script when Privileged Behavior Analytics has a user alert event. Additional information can be found in the Privileged Behavior Analytics"PBA Responsive Actions" on page 98 article.

Warn Threshold: The numerical value a warning needs to meet or exceed to send an email and log the event on the Alerts page.

Warn Action: Provides three different automated actions that Privileged Behavior Analytics can take in response to an Alert Event. See the above Alert Action list item for details on automated actions.

Test Actions: Provides an ability to test Responsive Actions to ensure your configuration is correct.

Secret Importance: A page that lists all Secrets and enables changing any of their importance settings for Privileged Behavior Analytics. More important Secrets are more likely to trigger alerts upon User access.

User Watch List: Configuration options to automatically populate the User Watch List with new users and/or users with active alerts and warnings.

Privileged Behavior Analytics Integration Settings

The Privileged Behavior Analytics integrations settings section is used to configure secure communications between your Secret Server and Privileged Behavior Analytics.

- Privileged Behavior Analytics integration key: A key that provides your Privileged Behavior Analytics with credentials and configuration information to upload log data to Privileged Behavior Analytics.
- Privileged Behavior Analytics public key: A one-time RSA public key is entered here to establish communication between Secret Server and Privileged Behavior Analytics.

Time Settings

The **Time Settings** section is used to configure the Timezone and time display format.

- Local Timezone: The display of all timestamps can be adjusted to your local time zone. The default time zone is UTC.
- Hour Display: 12-hour (AM/PM) or 24-hour (international or “military”) time display.

User Settings

The **User Settings** section has password and alert preferences settings.

- **Account Settings**: The link enables changing the password for the account used to access Privileged Behavior Analytics.

- **Alert Notification Settings**: Enables setting the email address for receiving alerts and whether you want to receive alerts or warnings as they occur.

Webhooks

Privileged Behavior Analytics integrates into external workflow and security systems via webhooks. A webhook is a user-defined callback which is executed in response to an event (alert or warning in Privileged Behavior Analytics). Along with Access Challenges and email notifications, webhooks comprise the responsive actions in Privileged Behavior Analytics in response to detection of anomalous activity.

Configuration

URL

This is the URL to which a POST request is sent when an event is created.

Signing the Secret

This is optional. If set, a header is set (x-hub-signature) with the SHA256 signature of the body of the email.

Example Signature Verification in Python 2.7:

```
from Crypto.Hash import SHA256
from Flask import requests
\# receive the request
signature = request.headers.get('x-hub-signature',None)
payload = request.data.decode('utf-8')
hmac = SHA256.new(secret)
hmac.update(payload)
expected_signature = "sha256="+hash.hexdigest()
assert signature == expected_signature
```

Encoding

Encoding may be set to either application/json or application/x-www-form-urlencoded.

However, only application/json supports mapped templates (customized POST body; see below).

Custom Headers

This is optional. This field takes JSON formatted headers and adds them to the POST request. For example, to configure basic authentication with username admin and password admin, you would generate the base64 string of username:password (admin:admin) using the Python example code below, and then set the custom header field to:

```
{"Authorization" : "Basic YWRtaW46YWRtaW4="}
import base64
base64.b64encode("admin:admin")
\# output is: YWRtaW46YWRtaW4='
```

Mapping a Template

This is optional. The Mapping Template takes a string as an argument which will be used as the body of the POST. Before doing the POST, Verify Privilege Vault Analytics will substitute any tokens specified in the mapping template with data from the event. Here are the supported tokens:

- EventId
- UserId
- UserName
- UserEmail
- DisplayName
- StartDate
- EndDate
- RiskScore
- Interval
- Severity
- Threshold
- Hostname

Note: When using Privileged Behavior Analytics, these are enclosed in @ signs, for example: @Severity@

If omitted:

If the Mapping Template is not set, then the event (alert or warning) will be serialized and posted as either JSON or urlencoded form data.

- This out-of-the-box formatting of the POST body may be fine for integrating with custom-built REST endpoints, but it is less useful for integrating directly with other products.
- As an example, see the configuration for Creating an Incident with ServiceNow, below.

Example: Creating a SlackBot

The full instructions for creating a Slack Webhook consumer are available here:

- https://api.slack.com/incoming-webhooks

In this example, we forward the Verify Privilege Vault Analytics events to Slack and they are posted to a channel using a SlackBot in our specified format.

1. Navigate to https://api.slack.com/apps create a new app.
2. Turn on Incoming Webhooks.
3. Copy your Webhook URL.

4. Click on Oauth & Permissions and under Scope > Select Permission Scopes, add Post to a specific channel in Slack for the channel to which you want the messages posted.
5. In Verify Privilege Vault Analytics, enable Webhook, and paste the Webhook URL from Step 3 into the URL field.
6. Create a Mapping Template with a single JSON field, text, and set its value to the format you want the SlackBot to use. For example:

```
{
"text":" Verify Privilege Vault Analytics Alert: https://@Hostname@/handle_ub_
alert/@EventId@\n
 Verify Privilege Vault User: @DisplayName@ (User ID:@UserId@)\n
Time Range: @StartDate@ - @EndDate@\n
Interval: @Interval@\n
Risk Score: @RiskScore@\n
Severity: @Severity@\n
Threshold: @Threshold@"
}
```

Example: Creating an Incident in ServiceNow

The configuration displayed below is an example of Webhook settings that would create an incident in ServiceNow. Here is the Mapping Template:

```
{"assignment_group":"security",
"caller_id":"6816f79cc0a8016401c5a33be04be441",
"description":" Verify Privilege Vault Analytics Alert\n Verify Privilege Vault User:
@UserName@ (UserId:@UserId@)\n
 Verify Privilege Vault Analytics Event: https://@Hostname@/eventdetails/@EventId@\n
Activity Start: @StartDate@\n
Activity End: @EndDate@\nInterval: @Interval@\n
Risk Score: @RiskScore@\nSeverity: @Severity@\n
Threshold: @Threshold@", "impact":"1",
"short_description":" Verify Privilege Vault Analytics Alert on Verify Privilege Vault
User @UserName@. Risk Score: @RiskScore@",
"work_notes":"reported Verify Privilege Vault Analytics alert"}
```

Notes

Be aware that:

ServiceNow’s REST API uses basic authentication.

The caller_id field should be set to the id of the ServiceNow service account used for authentication.

Delineaprovides a callback link in the incident description: https://@Hostname@/eventdetails/@EventId@ It is also possible to configure an html URL field in ServiceNow and format this as a proper anchor tag.

Codehooks

Privileged Behavior Analytics integrates into external workflow and security systems via Codehooks. A Codehook is a user-defined script which is executed in response to an event (alert or warning in Privileged Behavior Analytics).

Along with Access Challenges, Email Notifications and Webhooks, Codehooks comprise the responsive actions in Privileged Behavior Analytics to detection of anomalous activity. A Codehook has the same use case as a Webhook, but is used for an integration which requires more than just an HTTP POST request.

Configuration

The **Script Template** is the script that will be executed as a hook in response to a Privileged Behavior Analytics event.

- It must be written in Python 2.7, and use the pip packages listed here.
- If an unsupported pip package is needed by the script, contact Delinea Support to request that it be added.
- Each script invocation has a 30 second timeout.
- Any files added to /tmp should also be removed when finished (i.e. os.remove('path_to_file')).
- Before executing the script, Privileged Behavior Analytics will substitute any tokens specified in the mapping template with data from the event. Here are the supported tokens:
  - EventId
  - UserId
  - UserName
  - UserEmail
  - DisplayName
  - StartDate
  - EndDate
  - RiskScore
  - Interval
  - Severity
  - Threshold
  - Hostname Note that in use, these are enclosed in @ signs, for example: @Severity@
- All of the above tokens except Hostname are event fields. Hostname denotes the hostname of the Privileged Behavior Analytics instance, and may be used to configure a link back to the Verify Privilege Vault Analytics event from the system targeted by the Code Hook.

Example: Suspending an Okta User Account

The script template displayed below is an example of a Python script that looks up an Okta user by email (UserEmail token) and suspends the user. This example would be the equivalent of a Lockout Challenge in Secret Server, but extrapolated to an external system (Okta). Other potential codehook actions in Okta would include resetting a user's password or security questions.

```
import urllib2
import urllib
import json
opener = urllib2.build_opener()
user = '@UserEmail@'
opener.addheaders = [('Authorization', 'SSWS <BASE 64 TOKEN>')]
response_str = opener.open('https://<OKTA URL>/api/v1/users?q={0}'.format(user))
response = json.loads(response_str.read())
body = response[0]
user_id = body.get('id',None)
if not user_id:
    print('user not found')
else:
    # suspend user
    url = 'https://<OKT ULR>/api/v1/users/{0}/lifecycle/suspend'.format(user_id)

    handler = urllib2.HTTPHandler()
    opener = urllib2.build_opener(handler)

    data = urllib.urlencode({})
    request = urllib2.Request(url, data=data)
    request.add_header('Authorization', 'SSWS <BASE 64 TOKEN>')
    request.get_method = lambda: "POST"

    try:
        connection = opener.open(request)
        except urllib2.HTTPError,e:
        connection = e

    if connection.code == 200:
        data = connection.read()
        print('Successfully suspended user: {}'.format(user))
    else:
        print('Failed to suspend user: {}'.format(user))
```

Example: Fax Alerts

Privileged Behavior Analytics supports Fax notifications via codehooks. Codehooks are user-defined scripts that are executed in response to an event (alert or warning in Privileged Behavior Analytics). In this example on configuring Fax Alerts, we use a third-party service, InterFAX, which is an online Fax service with an excellent API.

Configuration

Below is the script that uses the **xhtml2pdf** Python library to convert an HTML document into a PDF for the Fax.

Make sure to replace your InterFAX API credentials and Fax number in the script below, and also to modify the Fax document header in the HTML template with your company and contact information.

Note: Remember to remove files stored in /tmp when you are finished.

```
from interfax import InterFAX
```

```
import os
import shutil
from uuid import uuid4
from xhtml2pdf import pisa
from cStringIO import StringIO
filename = "alert-fax{}.pdf".format(uuid4())
filepath = "/tmp/" + filename

fax_html = """<html><head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<meta http-equiv="X-UA-Compatible" content="IE=8">
<title>bcl_1363603926.htm</title>
<meta name="generator" content="BCL easyConverter SDK 5.0.08">
<style type="text/css">

body {margin-top: 0px;margin-left: 0px;}

#page_1 {position:relative; overflow: hidden;margin: 102px 0px 174px 120px;padding:
0px;border: none;width: 696px;}
@page {
 size: a4 portrait;
 @frame header_frame { /* Static Frame */
 -pdf-frame-content: header_content;
 left: 50pt; width: 512pt; top: 50pt; height: 40pt;
 }
 @frame content_frame { /* Content Frame */
 left: 50pt; width: 512pt; top: 90pt; height: 632pt;
 }
 @frame footer_frame { /* Another static Frame */
 -pdf-frame-content: footer_content;
 left: 50pt; width: 512pt; top: 722pt; height: 150px;
 }
 }

.ft0{font: bold 19px 'Times New Roman';line-height: 22px;}
.ft1{font: bold 14px 'Times New Roman';line-height: 14px;}
.ft2{font: 15px 'Times New Roman';line-height: 17px;}
.ft3{font: bold 14px 'Times New Roman';line-height: 17px;}
.ft4{font: 1px 'Times New Roman';line-height: 1px;}
.ft5{font: bold 16px 'Times New Roman';line-height: 19px;}
.ft6{font: 16px 'Times New Roman';line-height: 19px;}
.ft7{font: 13px 'Times New Roman';line-height: 15px;}

.p0{text-align: left;padding-left: 150px;margin-top: 0px;margin-bottom: 0px;}
.p1{text-align: left;padding-left: 180px;margin-top: 49px;margin-bottom: 0px;}
.p2{text-align: left;margin-top: 0px;margin-bottom: 0px;white-space: nowrap;}

.td0{padding: 0px;margin: 0px;width: 384px;vertical-align: bottom;}
.td1{padding: 0px;margin: 0px;width: 54px;vertical-align: bottom;}

.tr0{height: 26px;}
.tr1{height: 31px;}
.tr2{height: 33px;}
```

```
.t0{width: 438px;margin-top: 42px;font: bold 15px 'Times New Roman';}

</style>
</head>
<body>
<div id="header_frame">
<p class="p0 ft0"> Verify Privilege Vault Analytics Alert</p>
<p class="p1 ft1">{AMBARCO IT DEPARTMENT}</p>
<table cellpadding="0" cellspacing="0" class="t0">
<tbody><tr>
    <td class="tr0 td0"><p class="p2 ft1">DATE: %s</p></td>
    <td class="tr0 td1"><p class="p2 ft1">TIME: %s</p></td>
</tr><tr>
    <td class="tr1 td0"><p class="p2 ft1">TO: %s</p></td>
    <td class="tr1 td1"><p class="p2 ft1"></p></td>
</tr><tr>
    <td class="tr2 td0"><p class="p2 ft1">FROM: %s</p></td>
    <td class="tr2 td1"><p class="p2 ft1"><span class="ft2"></p></td>
</tr><tr>
    <td class="tr2 td0"><p class="p2 ft1">PHONE: %s</p></td>
    <td class="tr2 td1"><p class="p2 ft3">EMAIL: %s</p></td>
</tr><tr>
    <td class="tr2 td0"><p class="p2 ft1">Number Pages: 1</p></td>
    <td class="tr2 td1"><p class="p2 ft4">&nbsp;</p></td>
</tr>
</tbody></table>
</div><br>
<div id="content_frame">
<p class="p3 ft5">MESSAGE:</p>
<p class="ft1"> Verify Privilege Vault User: @UserName@ (UserId:@UserId@)</p>
<p class="ft1">Pba Event: https://@Hostname@/eventdetails/@EventId@</p>
<p class="ft1">Activity Start: @StartDate@</p>
<p class="ft1">Activity End: @EndDate@</p>
<p class="ft1">Interval: @Interval@</p>
<p class="ft1">Risk Score: @RiskScore@</p>
<p class="ft1">Severity: @Severity@</p>
<p class="ft1">Threshold: @Threshold@</p>
</span>
</div>
<div id="footer_content">
<p class="p5 ft5">DISCLAIMER:</p>
<p class="p6 ft7">The information contained in this fax is confidential and property of
Ambarco Inc. Please do not distribute outside the organization.</p>
<p class="p7 ft7">Please check that you have received all pages per the page number
above.</p>
</div>
</body></html>"""

to_name = "Security Administrator"
from_name = "Pba Service Account"
from_phone = "+1 669-221-6251 "
from_email = "pbaalerts@ambarco.com"
```

```
event_date, event_time = "@StartDate@".split('T')
event_time = event_time[:8]

formatted_fax_html = fax_html % (event_date, event_time, to_name, from_name, from_phone,
from_email)

pdf = StringIO()
pisa.CreatePDF(StringIO(formatted_fax_html.encode('utf-8')), pdf)
resp = pdf.getvalue()

with open(filepath, 'w') as fd:
    pdf.seek(0)
    shutil.copyfileobj(pdf, fd)
interfax = InterFAX(username="<API USERNAME>", password="<API PASSWORD>")
fax = interfax.deliver(fax_number="+99999990", files=[filepath])
fax = fax.reload()    # resync with API to get latest status
print('Status:', str(fax.status), '  (Success if 0. Pending if < 0. Error if > 0)')
os.remove(filepath)   # remove pdf from /tmp
```

Analytics Platform Risk API

The Delinea Analytics Risk API can be used to get estimates of risk scores based on behavioral logic used to monitor activity and determine what can be considered as a ‘fraudulent' or ‘risky’ activity or event. The analysis done in the analytics system produces parameters that are used to score activities and events. Various ‘machine learning’ algorithms are processed and scores from the data used or a risk score from the event stream are being monitored. The monitoring processes generate notification alerts. The Risk API allows the customer to use these measures for their purpose and systems monitoring. This documentation gives an overview of the Risk API system and provides guidance for the customer.

API Contract Details

Version	v 0.1.0	
	Method	POST
	URI	/api/risk_score
	Content Type	application/json
	Header	Content-Type: application/json
	Header	x-api-key: <x-api-key value saved in tenant system settings, x_api_key>

Version	v 0.1.0	
	json schema	json example
Request	{ “user”: { “id”:”string”, “attributes”: { “name”:”string”, “osType”:”string”, “deviceType”:”string” } }, “secret”: [{ “id”:”string”, “attributes”: { “folder”:”string”, “name”:”string”, “template”:”string”, “time”:”string” } }], “action”: [{ “attributes”: { “name”:”string”, “code”:”int”, “time”:”string” } }], “location”: [{ “attributes”: { “longitude”:”string”, “latitude”:”string”, “countryCode”:”string”, “time”:”string” } }] }	{ “user”: { “id”: “167”, “attributes”: { “name”: “fake.user@thycotic.com“, “osType”: “macOS”, “deviceType”: “Macbook Pro” } }, “secret”: [{ “id”: “6521”, “attributes”: { “folder”: “”, “name”: “AWS password”, “template”: “”, “time”: “2021-09-28 17:00:00” } }, { “id”: “6531”, “attributes”: { “folder”: “”, “name”: “AWS certificate”, “template”: “”, “time”: “2021-09-28 18:00:00” } }], “action”: [{ “attributes”: { “name”: “View account”, “code”: “444”, “time”: “2021-09-28 18:30:00” } }], “location”: [{ “attributes” :{ “longitude”: “113.5514”, “latitude”: “40.7336”, “countryCode”: “USA”, “time”: “2021-09-28 14:00:00” } }] }

Release Notes

Delinea periodically updates the PBA service to introduce new features and fix problems. This section includes the most recent Privileged Behavior Analytics Release Notes.

Starting with the June 2020 release the product version number reflected in the documentation will not be changed. PBA as a SaaS product does not reflect or change version references going forward.

- "April 25th, 2022 - Release Notes" on page 112
- "December 2nd, 2021 - Release Notes" on page 112
- "August 20th, 2020 - Release Notes" on page 114
- "June 4th, 2020 - Release Notes" on page 113

Changelog

This topic provides a chronological list of documentation changes, to help track additions, deletions, and contents edits other than spelling and grammar corrections.

April 2022:

- Added "April 25th, 2022 - Release Notes" on the next page for the April 25 release.

December 2021:

- Added "December 2nd, 2021 - Release Notes" on the next page for the December 2nd release.

August 2020:

- Added Privilege Manager integration information.
- Added "August 20th, 2020 - Release Notes" on page 114 for the August 20th release.

June 2020:

- Added "June 4th, 2020 - Release Notes" on page 113 for June 4th release.

3.2 Release Notes

Enhancements

- Improved audit logging and error handling

Usability Improvements

- New country count layer added to IP Maps
- Public/Private IP address indicators added to IP Maps, List, and Details pages
- More actions and details added to PBA Log & Historical Alerts
- Improved tooltips and details

Bug Fixes

- Fixed layout issues caused by browser update
- Fixed display and sizing of the Activity Timeline

3.1 Release Notes

Bug Fixes

- Corrected an issue with IP address processing

3.0 Release Notes

Enhancements

- New IP Address Analytics that include:
  - Map feature that visualizes Secret accesses by location
  - Detailed reports of actions by IP address

  - Searchable and filterable list of IP addresses, locations, and statistics
- New Administrator Action Analytic Suite that includes:
  - Map to visualize Secret Server administrators’ actions by location
  - Clock to visualize Secret Server administrators’ actions by time
  - Graph to visualize links between Secret Server administrators and their actions
  - Charts with filters to visualize the most active Admins and Actions
- New Dashboard widgets for administrator actions and an IP address map
- PBA Activity Log for internal auditing purposes
- Several design, security, and speed improvements

April 25th, 2022 - Release Notes

Site Reliability

- Additional disaster recovery regions added.
- Failover for cross-region web compute automated.

Performance Improvements

- Various improvements to the UI resulting in improved response times throughout the application.
- Enhanced Privilege Manager query performance.
- IP details page response improved.

Bug Fixes

- Responsive action threshold now persists consistently.
- The Timeline Grid links have been updated.
- Minor UI and visual fixes.

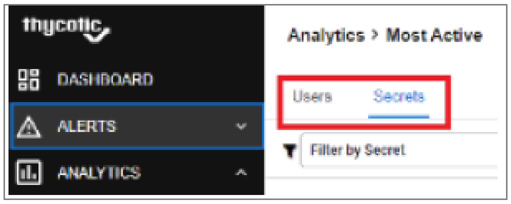
December 2nd, 2021 - Release Notes

Enhancements

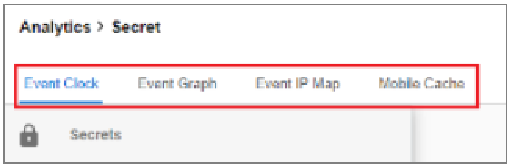
Front-end Improvements

- Navigation Improvements:
  - Main Navigation menu, which has been a top navigation menu, has moved to the left navigation menu.

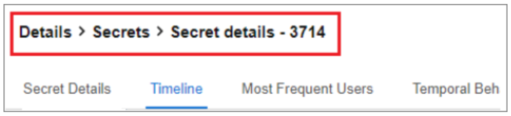
- Grouped related data and view toggling.



- Tabbed menus.



- Breadcrumb navigation to improve drill-down into details and back navigation.



- Dashboard modifications, to represent information via a modernized view.
- Watch List modernization to align with other Delinea products.
- Column options to view historical behavior alert data.

Back-end Improvements

- PBA is introducing a confidence score that will accompany risk scores. The confidence score is an amalgam of data variety, data volume, and temporal factors. As PBA becomes more familiar with the actions of a given user, the system's confidence in the reported risk score of the user's action will increase towards full confidence.
- The Risk API introduces an endpoint that will return the Risk score of the event for external consumption. For example, a third-party identity provider could request the risk score programmatically and send an MFA challenge if the score were to exceed a set threshold.

June 4th, 2020 - Release Notes

Enhancements

Application

- Updated colors and logos to latest Delinea schema, switched to Roboto font.
- Improved security and error handling across application.
- Added PBA Log client-side processing for faster response time.

Backend

- Security enhancements for better isolation and provisioning.
- Regular data update processing speed-up.

Bug Fixes

Application

- Security and application protection improvements (from internal pentests):
  - Stored cross-site scripting vulnerability.
  - Cache control to prevent caching of sensitive data.
  - Reducing session time to 1 hour.
  - Preventing HTML injection in settings.
  - Numerous minor fixes and application improvements.

Backend

- Fixed IP Geo DB update issue.
- Fixed CloudControl region setup.

August 20th, 2020 - Release Notes

Enhancements

Application

- Added Privilege Manager application suite to analyze endpoint executions and patterns
- Added Query Builder tool to enable viewing records or exporting data for offline analysis and auditing

Backend

- Speed and security improvements

Bug Fixes

Application

- Fix for System Settings page errors
- Fixes for CSS issues caused by browser interpretation changes

Backend

- Handle potential large graph save errors

2.1.3 Release Notes

Analytics Improvements

- Graph Visualization: added Node Icons, additional data available for each node, and various other small improvements
- Data Clock Visualization: improved filter options and ability to link into filtered views
- Most-Active Analytics: swapped out library for cohesive feel with Dashboard
- Details Timeline Analytics: updated library for better visualization and data filtering

Usability Improvements:

- alerts indicator now displays on all pages
- improved layout on the Alerts page
- the Details Pages now have a stats card to display a summary of User and Secret activity

2.0.2 Release Notes

Enhancements

- User Watch List
  - added a User Watch List page to help admins keep a closer eye on key users and provide a centralized starting point to dive into analytics. By default, the Watch List automatically adds users with open alerts or warnings as well as new users
  - can manually add users to User Watch List with customizable notes and reasons (e.g. "Departing User, Suspicious"); to enable quick action, each user's entry includes links to their PBA Details' page, Active Alerts, and the Secret Server User Edit page
- Webhook Response Actions
  - now PBA can send alert data to a web endpoint, such as ServiceNow or Slack, to make responding to an alert easier; PBA can also run a script to execute additional actions not possible with a webhook, for example, a Codehook can be configured in PBA to take actions (e.g. locking accounts of a user with suspicious activity) in any combination of systems including Human Resources, Security, Identity, or Workflow
- Email Enhancements
  - redesigned Alert Emails include details of each alert or warning along with links to take immediate action like **Investigate**, **Dismiss**, or **View User Activity**
  - the PBA alerting system can now trigger faster alerts, so admins will know within moments whether a user is acting out of the ordinary
- UI Updates
  - pages for User Details and Secret Details pages are enhanced with new statistics boxes that show key information and action links

1.1.0 Release Notes

Enhancements

- Secret Server can act as an identity provider for PBA
    - any user with the **View Security Analytics** role permission in Secret Server may log in to PBA
    - any user with **Administer Security Analytics** role permission is able to perform administrative actions once logged into PBA through Single Sign-On (SSO)
    - local PBA users (the initial users prior to integrating PBA into Secret Server) still have administrative rights
- PBA can now integrate with Secret Server Cloud
- the Dashboard now has a **Dashboard Assistant**, a feed of the important events that have occurred in a customer’s Secret Server environment that details why those events are important to see and what should be done as a result
- PBA has integrated with **AppCues** to provide useful product tours throughout each page
- Secret Access Graph Enhancements
    - nodes on the Secret Access Graph are now outlined by varying shades of red if there is an active alert affecting them
    - filter configurations can now be saved and recalled for convenient views of the Secret Access Graph