# BeyondTrust

### Remote Support SIEM Integration Guide

#### **Table of Contents**

Configure and Administer the BeyondTrust SIEM Tool Plugin	3
Review Prerequisites	3
Configure BeyondTrust Remote Support for Using the SIEM Plugin	4
Verify the API Is Enabled	4
Create an OAuth API Account	4
Add an Outbound Event URL	5
Configure the BeyondTrust Remote Support SIEM Tool Plugin	6
Configure Communication between the SIEM Plugin and the BeyondTrust Appliance B Series	6
SIEM Tool Instance	7
Report Templates	7
BeyondTrust SIEM Tool Message Reference List	8

#### Configure and Administer the BeyondTrust SIEM Tool Plugin

The Security Information and Event Management (SIEM) tool plugin for BeyondTrust Remote Support enables the processing and transmission of session event data to your preferred SIEM tool. This complements tools that gather syslog data, which includes only appliance events. The plugin can customize the output message format for special needs and/or use cases.

#### **Review Prerequisites**

Before using this plugin, you must:

- Install and configure the BeyondTrust Middleware Engine, which supports this and other plugins.
- Install this plugin following the instructions in the Middleware Guide.
- Review the network considerations for your preferred SIEM tool.

For more information about installing and configuring the BeyondTrust Middleware Engine and installing plugins, please see the <u>BeyondTrust Remote Support Middleware Engine Installation and Configuration Guide</u> at https://www.beyondtrust.com/docs/remote-support/documents/integrations/rs-middleware-engine.pdf.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/4/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

#### Configure BeyondTrust Remote Support for Using the SIEM Plugin

All of the steps in this section take place in the BeyondTrust /login administrative interface. Access your Remote Support interface by going to the hostname of your B Series Appliance followed by /login (e.g., https://support.example.com/login).

SIEM plugin configuration is required for each B Series Appliance configured in the application's configuration file.

#### Verify the API Is Enabled

🛐 Management

API CONFIGURATION

This integration requires the BeyondTrust XML API to be enabled. This feature is used by the BeyondTrust Middleware Engine to communicate with the BeyondTrust APIs.

🖌 Enable XML API 🏮	Cinable Archive API	
--------------------	---------------------	--

Go to /login > Management > API Configuration and verify that Enable XML API is checked.

#### **Create an OAuth API Account**

👌 Management

**API CONFIGURATION** 

The SIEM Tool API account is used from within SIEM Tool to make Remote Support Command API calls to Remote Support.

- 1. In /login, navigate to Management > API Configuration.
- 2. Click Add.

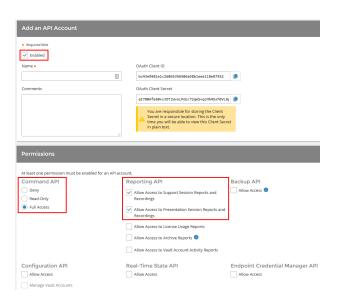
tware S	iecurity Site Configuration	Email Configuration	Outbound Events	Failover	API Configuration	Support	
API Config							
<ul> <li>Enable XML</li> </ul>	471	Cinable Archive API					
- Children And		Charle Preside Preside Part					
Allow HTTP	Access to XML API						
• View the Co	nfiguration API Documentation						
	he Configuration API's OpenAPI YAML f	1					
E Download ti	ne contiguration APTS OpenAPT YAML 1	ie.					
API Accou	nts 🕂 Add						
	30 API Accounts.						
	30 API Accounts. OAuth Client ID		Peri	nissions		Enabled	
Configure up to		8		missions		Enabled Yes	,
Configure up to	OAuth Client ID						,
Configure up to	OAuth Client ID	8					/
Configure up to	OAuth Client ID	8					1

4

<sup>©2003-2024</sup> BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/4/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

## BeyondTrust

- 3. Check Enabled.
- 4. Enter a name for the account.
- OAuth Client ID and OAuth Client Secret is used during the OAuth configuration step in SIEM Tool.
- 6. Under **Permissions**, check the following:
  - Command API: Full Access.
  - Reporting API: Allow Access to Support Session Reports and Recordings, and Allow Access to Presentation Session Reports and Recordings.
- 7. Click Save at the top of the page to create the account.



#### Add an Outbound Event URL

#### 🔯 Management

**OUTBOUND EVENTS** 

- 1. Go to /login > Management > Outbound Events.
- 2. In the HTTP Recipients section, click **Add** and name it **Integration** or something similar.
- 3. Enter the URL to use:
  - If using the default appliance ID:
    - http://<middleware-host>:<port>/ERSPost.
    - The default port is 8180.
  - If using an appliance ID other than the default:
    - http://<middleware-</li>

*host>:<port>/ERSPost?appliance=<appliance-id>* where *<middleware-host>* is the hostname where the BeyondTrust Middleware Engine is installed.

- The default port is 8180.
- The *<appliance-id>* is an arbitrary name, but note the value used, as it is required later in the plugin configuration. This name accepts only alphanumeric values, periods, and underscores.

Cancel

Required fiel

Enabled

Integration
Use a CA Certificate

Events to Send Support Session Star Support Session End Someone Joins a Sup

Someone Leaves a Support Sessio Support Session Ownership Chang

act 🕕

Customer Exit Survey is Complete

- 4. Scroll to Events to Send and check the following event: Support Session End
- 5. Click Save.
- The list of outbound events contains the event just added. The Status column displays a value of OK if communication is working. If communication is not working, the Status column displays an error which you can use to repair communication.

HTTP Recipie						
Configure up to 10 e	external HTTP servers that w	If be notified when certain session events occur. These ser	vers must respond to each event with HT	TP 200 in order to be considered successful.		
Name *	Disabled	URL	Events to Send	Status		
Integration	No	https://middleware.host	Access Session End	The given remote hast was not resolved.	1	
integration2	840	https://middleware.host/8180	Access Session End	The given remote hast was not resolved.	1	
168	840	https://middleware.host/8180	Access Session End	The given remote hest was not resolved.	1	
Testing	No	https://tcpam1.qa.borngar.com/	Access Session End	The requested unit was not found or returned another error with the HTTP error code being 400 or above.	1	

After 1 Hour

Every 2 Hours

5

<sup>©2003-2024</sup> BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/4/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

#### Configure the BeyondTrust Remote Support SIEM Tool Plugin

All of the steps in this section take place in the BeyondTrust Middleware Administration Tool. Access this tool by going to a browser on the server where the Middleware Engine is installed, and entering the address *http://127.0.0.1:53231/*.

To begin configuration, and click the clipboard icon next to the plugin name.

#### Configure Communication between the SIEM Plugin and the BeyondTrust Appliance B Series

Enter the settings for communication between the plugin and the appliance. Configuration sections include:

- 1. **Plugin Configuration Name:** Any desired value. Because multiple configurations can be created for a single plugin, allowing different environments to be targeted, provide a descriptive name to indicate how this plugin is to be used.
- 2. **Appliance Id:** This can be left as **default** or can be given a custom name. This value must match the value configured on the outbound event URL in the BeyondTrust Appliance B Series. If outbound events are not being used, this value is still required, but any value may be used.
- 3. **B Series Appliance Host Name:** The hostname of the B Series Appliance. Do not include https:// or other URL protocol elements. For example, enter *www.example.com*.
- BeyondTrust Integration API OAuth Client ID: This field must contain the Client ID of the OAuth account.
- 5. **BeyondTrust Integration API OAuth Client Secret:** This field must contain the client secret of the OAuth account
- 6. **BeyondTrust Integration API User Name:** The username of the API service account created on the .
- 7. **BeyondTrust Integration API Password:** The password of the above user.
- 8. **Locale Used for BeyondTrust API Calls:** This value directs the B Series Appliance to return session data in the specified language.
- 9. Disabled: Enable or disable this plugin configuration. It must be enabled to function.
- 10. Allow Invalid Certificates: Leave unchecked unless there is a specific need to allow. If enabled, invalid SSL certificates are allowed in calls performed by the plugin. This would allow, for example, self-signed certificates. This is not recommended in production environments.
- 11. Use Non-TLS Connections: Leave unchecked unless it is the specific goal to use non-secure connections to the B Series Appliance. If checked, TLS communication is disabled altogether. If non-TLS connections are allowed, HTTP access must be enabled on the BeyondTrust /login > Management > API Configuration page. Using non-secure connections is discouraged.

Note: When using OAuth authentication, TLS cannot be disabled.

12. **Outbound Events Types:** Check which types of events the plugin processes when received by the middleware engine. Event types selected here must also be configured to be sent in BeyondTrust. The middleware engine receives any events configured to be sent in BeyondTrust but passes them off to the plugin only if the corresponding event type is selected in this section.

Indexes Id         Image: Setting from the subgrandses. This should match the appliance parameter appended to the Outbound Event (of one exists). For example if the Outbound Event was setting lates in the subfrandses for the subfrandses. The Subfrand Event was should be "appliance. The Subfrand Event Was should be start was should be "appliance. The Subfrand Event Was should be should be appliance. The Subfrand Event Was should be start was should be appliance. The Subfrand Event Was should be should be appliance. The Subfrand Event Was should be should be appliance. The Subfrand Event Was should be should be appliance. The Subfrand Event Was should be should be appliance. The Subfrand Event Was should be should be appliance. The Subfrand Event Was should be should be appliance. The Subfrand Event Was should be should be should be appliance. The Subfrand Event Was should be should be appliance. The Subfrand Event Was should be should be appliance. The Subfrand Event Was should be should be appliance. The Subfrand Event Was should be should be appliance. The Subfrand Event Was should be applient. The Was should be should be applient. The Was should be should be applient. The Was should applient the Subfrand Event Was should be applient.		
Applace 14 <ul></ul>	QA Environment	E 🗸
defaul           defaul         defaul	Descriptive name for this configuration.	
January Sequence North Security Sequences (The Net Net Net Net Net Net Net Net Net Ne	Appliance Id	
his high his holographical best Ministry Registers expectations of their head best we should be "applications". Pappose tearings com The host name of the applicant. Suppose tearings com Suppose tearing com Suppose te	default	4
Pageboot example com Pageboot		
Iha boar name of the applicate.	Appliance Host Name	
typeSecence API Outwork Cleared ID           park20254545054511321021010020150207           TypeSecence API Outwork Cleared Secence           TypeSecence API Outwork Cleared Secence In API Automotication.           SpeSecence API Outwork Cleared Secence In API Automotication.           TypeSecence API Outwork Cleared Secence In API Automotication.           TypeSecence API Processored           The Use Training Cleared TypeSecence           The Use Training Cleared TypeSecence           The Apine Secence In API Automotication. Entities of the dire only if using useer nametapasseericd API Automotication. NOTE: Outwith is the preferred mechanism.           Appained API Automotication. Entities the field only if using useer nametapasseericd API Automotication. NOTE: Outwith is the preferred mechanism.           SpeSecence In API Automotication. Entities the field only if using useer nametapasseericd API Automotication. NOTE: Outwith is the preferred mechanism.           SpeSecence In Apparet Automotication. Entities The Intel only of using useer nametapasseericd API Automotication. NOTE: Outwith the resolution of the Intel only of using useer nametapasseericd API Automotication. NOTE: Outwith the resolution of the Intel only of using useer nametapasseericd API Automotication. NOTE: Outwith the resolution of the Intel only of using useer nametapasseericd API Automotication. Intel only of	support.example.com	~
a APCIDIAESIdat/DMAINERSEARCH. a APCIDIAESIDATION APPRIATE AND APPRIA	The host name of the appliance.	
The OAuth Clears for API Authentication.	Appliance API OAuth Client ID	
typiance API Obdath Clant Secret  The Out-Out Clant Secret  The Out-Out Clant Secret  The Out-Out Clant Secret  The Out-Name Secret	ae94203e53e5af5204c112d3202150f29152d29f	*
	The OAuth Client Id for API Authentication.	
	Appliance API OAuth Client Secret	
In Court Clear Beard for API Automatication.		(i) <b>v</b>
typeSance API User Kanne  typeSance API Australization. Enter this field only if using user ramelpasseord API Authentication. NOTE: OAuth is the preferred mechanism.  typeSance API Passeord  The Passeord for API Authentication. Enter this field only if using user ramelpasseord API Authentication. NOTE: OAuth is the preferred mechanism.  typeSance API Passeord  The Passeord for API Cash  English  Cash User Cash Sance Cash  Cash Sance Cash Sance Cash  Cash Sance C	The QAuth Client Secret for API Authentication	
The User Yame for API Authentication. Enter this field only if using user name)password API Authentication. NOTE: OAuth is the preferred mechanism.		
Appliance APP Passeed <ul> <li>Implicit Passeed</li> <li>Passeed for APT Authentication. NOTE: OUth is the preferred mechanism.</li> <li>Casking Casking Casking</li></ul>	Appliance API User Name	
Appliance APP Passeed <ul> <li>Implicit Passeed</li> <li>Passeed for APT Authentication. NOTE: OUth is the preferred mechanism.</li> <li>Casking Casking Casking</li></ul>		
Password for API Authentication. Inter this field only if using user name/password API Authentication. NOTE: CAuch is the preferred mechanism.     Council Veel for API Cata     Explin     To able     To ab	The User Name for API Authentication. Enter this field only if using user name/passwo	rd API Authentication. NOTE: OAuth is the preferred mechanism.
Password for API Authentication. Inter this field only if using user name/password API Authentication. NOTE: CAuch is the preferred mechanism.     Council Veel for API Cata     Explin     To able     To ab	Appliance API Password	
The Person of API Authentication. Enter this field only if using user name/passed API Authentication. NOTE: CAuth is the preferred mechanism.		
Lease Used for API Cast  Explain  Constant  Second		0
English    English  English  Characterized and a set of se	The Descured for ADI Authoritation Enter this field ash. If using user providences	
Dashed		
Ten disake the configuration. J Adv hurld Catalog Frankler, Ladie National Catalog Frankler, Ladie National Catalog Frankler, Ladie National Status et al. In a stower in cath performed by the plugih. This would allow, for example, self-agreed certificates. This is not recommended in production and the TL Gal in refs used on observed calls to the applicate. This is not recommended. Note this storing is only applicable when using user rame/passeword,API authentication. If Cather Cather Cath	Locale Used for API Calls	
Allow Index Certificate     (add Scientificate)	Locale Used for API Calls	
Feedball, noted SSL conflictes all be allowed in cells performed by the ptigin. This would allow for example, self-agreed certificates. This is not recommended in production () Let North IS Constantion () The North IS Constantion () Let North IS	Locale Used for API Calls English	
University of the second of the septence. This is not resommended. Note this setting is only applicable when using user namelpassword API authentication. If and CLB with a be used to not the septence. This is not resommended. Note this setting is only applicable when using user namelpassword API authentication. If and CLB with the septence measures them are communication with the licketing system will be captured and logged. Note these messages are logged at a DEBUO level, so the Stochastic Development and the septence of the setting of the setting is not resommended. Note these messages are logged at a DEBUO level, so the Debuted Development Development and the setting applied to set them. Debuted Development Development and the setting applied to set them. Debuted Development Development and the setting applied to set them. Debuted Development Development Development Development Development Development Development Development Development g support Development Development Development Development Development Development Development Development Development Development De	Locale Used for API Calls English Disabled Set to disable this configuration.	-
11 Us Son-13.5 Conventors. Text LDB vice because on underwise calls to the application. This is not recommended. Note this setting is only applicable when using user name/password API authentication. If 2 calcuts GAV Center Wessages Text nequest and response messages from any communication with the tolering system will be captured and logged. Note these messages are logged at a DEBUO level, so the Middeament to genitry my sete to be adjusted to see them. Databased Event Types 0 calcutomer End Story adjusted to see them. Databased Event Types 0 calcutomer End Story adjusted to see them. Databased Event Types	Looble Used for API Calls Explan Disbled Set to disable this Alone Inside Certificates	AP Authentication. NOTE: OAuth is the preferred mechanism.
uning OAAnn, this value is groved (OAAnn all always use TLS). () goalnes GAAP Careford Researces fare, request and response messages more to assigned at a DEBUO level, so the difference in guelening week to be adjusted to see them. Defaunce defaunces g alsopont Session End Q existence End Storyes a Compared R expressed Defaunce Laws a Support Session. Paling Event Types	Lease Used for API Calls Explain Dashed Set for shale this configuration. And invited Centificates Readed, muld Size (entraces will be allowed in calls performed by the plugin. This	AP Authentication. NOTE: OAuth is the preferred mechanism.
Far treates do response missioges from any communication with the foldering system will be captured and logged. Note these messages are logged at a DEBUG level, so the dollarent to guint my reset to be adjusted to see them. Datiound Event Types Q stappet faits ways Completed Q Responsedant's Survey a Completed Q Responsedant's Survey a Completed D Responsed by Support Bession Paling Event Types	Leak Used for API Cats English Contained Constant Constan	AP Authentication. NOTE: OAuth is the preferred mechanism.
Middhwarin (gi wwel hit) week lit is ediginal to see them. Disclosed Exect Types S Support Execution Fact S August State (S Support Section S Support S S Support S S S S S S S S S S S S S S S S S S S	Leak Use for API Cals Englis Dobbel D	API Authentication. NOTE: CAuch is the preferred mechanism.
ga Bagoon Basano Bind go colomente Esta Variery a Companied De Regressantato Survey a Companied S Somerce Jone a Support Beaston Palling Event Type	Leader Used for APT Calls Explin Desided Set Gealable His configuration. Allow Involute Certificates Allow Tables, and Statistications, and the advance of t	API Authentication. NOTE: CAuch is the preferred mechanism.
III Customer Eur Sunvey & Complexed IIII Ageneratarile Sunvey & Complexed Desmore Joins a Sulgoot Beason Poling Event Types	Least Used for API Cast English English Consolid	APP Authentication, NOTE. OAuth is the preferred mechanism.
Di Representaria Survey III Competed Somere John a Support Session Velling Event Type	Locale Used for APT Calls English Disability	APP Authentication, NOTE. OAuth is the preferred mechanism.
☐ Someone Join's a Support Session Polling Event Types	Leack Used for API Cast English 2 Instable 2 Instable 2 Instable Control (1997) 1 Instable Control (1997) 2 Instable Control	APP Authentication, NOTE. OAuth is the preferred mechanism.
Polling Event Types	Leale Used for API CaSe  Explain  Constant  Description  Constant  Description  Constant  Description  Descri	APP Authentication, NOTE. OAuth is the preferred mechanism.
	Lease Used for API CaSt Englis  Dasket Dask bio configuration. Dasket bio configuration and bio configuration. Dasket bio configuration. D	APP Authentication, NOTE. OAuth is the preferred mechanism.
Support Session End	Leastle Used for API Cast English 2 Installed Bert disable this conflictions: I standbell, multiple Conflictions: I standbell, multiple Conflictions: J and Tools (Societarians) J and Tools (J and Tools and Tools and the standbell and the standbell J and Tools (J and Tools and Tools) J and Tools (J and Tools) J and Tools (J and Tools) J and Tools (J and Tools) J and Tools) J and Tools (J and Tools) J and Tools) J and Tools (J and Tools) J and J	APP Authentication, NOTE. OAuth is the preferred mechanism.
	Lease Used for API Cals English Construction Description Descripti	APP Authentication. NOTE: OAuth is the preferred mechanism.

- 13. **Polling Event Types:** If network constraints limit connectivity between the B Series Appliance and the middleware engine such that outbound events cannot be used, an alternative is to use polling. The middleware engine regularly polls the B Series Appliance for any sessions that have ended since the last session was processed, however only the **Support Session End** event type is supported.
- 14. **Polling Interval:** Enter only if polling is used. This determines how often the middleware engine polls the B Series Appliance for sessions that have ended. Too frequent polling may cause performance issues.
- 15. **Retry Attempt Limit:** Enter the number of retries that can be attempted if the plugin fails to process an event. Too many retries may cause performance issues.
- 16. Retry Outbound Event Types: Specify which outbound events the plugin retries if it fails to process the event.
- 17. Retry Polling Event Types: Specify which polling events the plugin retries if it fails to process the event.

For more information about configuring the BeyondTrust Middleware Engine and plugins, please see the <u>BeyondTrust</u> <u>Remote Support Middleware Engine Installation and Configuration Guide</u> at <u>https://www.beyondtrust.com/docs/remote-</u> support/documents/integrations/rs-middleware-engine.pdf.

#### **SIEM Tool Instance**

These are the fields and selections needed to configure the plugin for integration with your SIEM tool. Please see your SIEM installation guide for the values to provide.

- 1. Target SIEM System : Select the target SIEM tool from the list.
- 2. SIEM Syslog Host: Enter the hostname or IP address of the SIEM instance that should receive the messages.
- 3. SIEM Syslog Port: Enter the port used by the SIEM instance to receive syslog messages.
- 4. SIEM Syslog Protocol: Select the appropriate protocol from the list.
- 5. Events to Process: BeyondTrust session data can contain many different event types. All types are available; however, a subset may be desired in the SIEM tool. Select only the events you would like sent to the tool. Events matching unchecked event types are ignored.

For a complete list of available events, please see <u>"BeyondTrust SIEM Tool Message Reference List" on page 8</u>.

#### **Report Templates**

On the BeyondTrust Middleware Engine server, in the **<install dir>\Plugins\<integration>\Templates** folder, there are multiple files ending with **\*.hbs**. These are Handlebars template files. These files are used by the plugin to format the session report and exit surveys that are added to the corresponding ticket each time a BeyondTrust session ends or each time a survey is submitted. The templates can be edited if desired.

**Note:** If you are editing a template, we recommend copying and saving the original in case the changes need to be reverted.

For more information on Handlebars templates, please see the Handlebars website at handlebarsjs.com.

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/4/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

#### BeyondTrust SIEM Tool Message Reference List

Callback Button Deployed10Callback Button Removed20Chat Message30	
Chat Message 30	
Command Shell Session Started 40	
Conference Member Added 50	
Conference Member Departed 60	
Conference Member State Changed 70	
Conference Owner Changed 80	
Credential Injection Attempt Failed 90	
Credential Injection Attempt 100	)
Customer Exit Survey 110	)
Directory Created 120	)
External Key 130	)
File Deleted 140	)
File Download Failed 150	)
File Download 160	)
File Moved 170	)
File Upload Failed 180	)
File Upload 190	)
Files Shared 200	)
Jump Item Authorization Request Utilized 210	)
Jump Item Authorization Request 220	)
Legal Agreement Response 230	)
Pinned Session Moved Away from Queue 240	)
Pinned Session Moved to Queue 250	)
Pinned Session Password Modified 260	)
Registry Exported 270	)
Registry Imported 280	)
Registry Key Added 290	)
Registry Key Deleted 300	)
Registry Key Renamed 310	)
Registry Value Added 320	)
Registry Value Deleted 330	)
Registry Value Modified 340	)

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

## BeyondTrust

9

Event Name	Event ID
Registry Value Renamed	350
Remote Shell Event	355
Representative Exit Survey	360
Representative Monitoring Started	370
Representative Monitoring Stopped	380
Screen Recording	390
Screenshot Captured	400
Service Access Allowed	410
Session Assigned	420
Session Assignment Response	430
Session End	440
Session Foreground Window Changed	450
Session Note Added	460
Session Pinned to Queue	470
Session Start	480
Session Transferred Away from Queue	490
Session Transferred to Queue	500
Session Unpinned from Queue	510
Show My Screen Recording	520
System Information Retrieved	530

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/4/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.