BeyondTrust

Privileged Remote Access 22.2
Syslog Message Reference

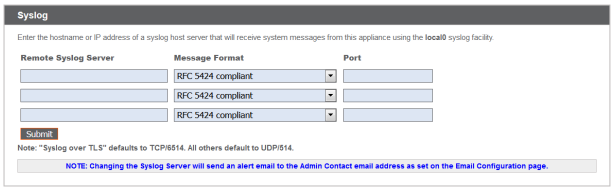
TC:6/1/2022

Table of Contents

Syslog Message Reference Guide

This document is intended to provide a reference for the syslog messages that are generated by the /login and /appliance interfaces of the B Series Appliance, as well as any clients that generate syslog messages such as the access console. It is assumed that the reader is familiar with the syslog concept and functionality. This document lists the different events that are logged by the syslog service that resides on the B Series Appliance and describes what the events mean as well as what triggers them.

To enable syslog messages from the B Series Appliance, go to **/appliance > Security > Appliance Administration** and scroll down to the **Syslog** section.



You can configure your B Series Appliance to send log messages to up to three syslog servers. Enter the hostname or IP address of the syslog host server receiving system messages from this B Series Appliance in the **Remote Syslog Server** field. Select the data format for the event notification messages. Choose from the standards specification **RFC 5424**, one of the legacy **BSD formats**, or **Syslog over TLS**. Syslog over TLS defaults to using TCP port 6514. All other formats default to using UDP 514. However, the defaults can be changed. The B Series Appliance logs are sent using the **local0** facility.

For Cloud-specific settings, please see B Series Appliance Administration: Set Syslog over TLS at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/cloud/syslog-over-tls.htm.

***Note:** When changing or adding a syslog server, an alert is emailed to the administrator's email address. The administrator's information is configured at **Security > Email Configuration > Security :: Admin Contact**.*

Syslog Message Format

All syslog messages follow a specific format. Below is an example of a message as well as an explanation of its parts.

```
Oct 12 14:58:35 example_host BG: 1234:01:01:site=access.example.com;who=John Smith(jsmith);who_
ip=192.168.1.1; event=login;target=web/login;status=success
```

The example above represents one message on one line. Messages can be broken down into two parts: a header followed by a payload of fields and values.

The header is made up of the date, time, hostname, and the characters **BG:**, which designate that this message is a BeyondTrust-specific syslog message. The remaining header information is made up of a unique 4-digit site ID, a segment number, and the total number of segments. If your B Series Appliance has only one site installed, all messages will have the same site ID. All three of these data are followed by colons. So from the example above, the entire header is:

Following the header is the payload. The format of the payload is essentially **field1=value1;field2=value2**;… This format is better suited to provide an order-independent set of data than a comma-separated format would provide, since some of the messages may contain upwards of 70 fields of data.

Finally, note also the escaping of "**=**", "**;**", and "****" characters. If any payload values include any of these characters, those characters will be prefixed with a backslash character ("\") to indicate that the next character is part of the value data, not a delimiter. For example, if a username were changed to **user;s=name\id** in the web interface, then the payload field/value pair in the syslog message would read **...new _ username=user\;s\=name\\id;**.

Syslog Message Segmentation

As mentioned above, certain syslog messages can be much larger than others. As a result, the syslog service will segment any messages that are larger than 1KB into multiple messages. In this guide, these messages will be referred to as segments.

Since the message example above is less than 1024 bytes, the header shows a value of 01:01:, indicating that this is the first segment and that there is only one segment in this message. A larger example message which does show segmentation is used in the Old/New Nomenclature section of this guide.

Syslog Payload Format

Examination of the payload shows that there are several standard data fields in every message. Messages will also contain non-standard data fields that provide more information about the syslog message. Here, we discuss the standard data fields.

site	The hostname for which the BeyondTrust software was built.
who	The username associated with this event.
who_ip	The IP address of the system that caused the event.
event	The name of the event that occurred.

Again, each of these fields will be present somewhere within the payload, but the order is not specifically set. Of these four fields, the most significant is the event field. The value associated with the event field indicates what actually occurred.

```
Oct 12 14:58:35 example_host BG: 1234:01:01:site=access.example.com;who=John Smith(jsmith);who_
ip=192.168.1.1;event=login;target=web/login;status=success
```

From the example, it can be determined that this particular message was generated by a login attempt. The remaining payload provides information about that event. In this case, the login attempt was for the /login administrative interface (**target=web/login**), and it was a successful attempt (**status=success**).

Syslog messages stack in order of occurrence. In the example below, a user attempts to log in but is required to change their password. The user tries to use an invalid password before setting one that matches the site's security policy and then log in successfully. Where the string ...**<data truncated>**... occurs, extraneous data was removed to make the example messages more readable.

```
Oct 12 14:53:24 example_host BG: 1234:01:01:site=access.example.com;…<data
truncated>…event=login;status=failure;reason=change_password
Oct 12 14:53:43 example_host BG: 1234:01:01:site=access.example.com;…<data
truncated>…event=change_password;status=failure;reason=invalid password
Oct 12 14:54:02 example_host BG: 1234:01:01:site=access.example.com;…<data
truncated>…event=change_password;status=success
Oct 12 14:54:03 example_host BG: 1234:01:01:site=access.example.com;…<data
truncated>…event=login;status=success
```

Integrated Login Syslog Messages

If a user attempts to log in via integrated login, such as LDAP, RADIUS, or Kerberos, and is unsuccessful, a login failure message will be generated even if that user can subsequently log in using local credentials.

The message below would be generated if the user could not be obtained because the failure happened too early in the integrated process or if the exchange succeeded but the security provider configuration denied the user access. In the example below, **<method>** will be either **password** for LDAP or RADIUS or **gssapi** for Kerberos.

```
Oct 12 14:53:24 example_host BG: 1234:01:01:site=access.example.com;…<data truncated>…who=unknown
() using <method>; event=login;status=failure;reason=failed
```

Such a scenario could cause the following sequence to occur. A user attempts integrated authentication, fails because of a technical reason, such as being unable to supply a proper service ticket for Kerberos, and as a result, no username is available. However, the user then logs in using a local account or an account on another security provider.

```
Oct 12 14:53:24 example_host BG: 1234:01:01:site=access.example.com;…<data truncated>…who=unknown
() using gssapi; event=login;status=failure;reason=failed
Oct 12 14:53:28 example_host BG: 1234:01:01:site=access.example.com;…<data truncated>…who=John
Smith(jsmith); event=login;status=success
```

An alternate scenario could occur if a security provider is not configured with a proper default policy or group lookup for an integrated login, or if it explicitly denies that user.

```
Oct 12 14:53:24 example_host BG: 1234:01:01:site=access.example.com;…<data truncated>…who=John
Smith(jsmith@EXAMPLE.LOCAL);event=login;status=failure;reason=failed
Oct 12 14:53:28 example_host BG: 1234:01:01:site=access.example.com ;…<data truncated>…who=John
Smith(jsmith); event=login;status=success
```

Old/New Nomenclature in Syslog Messages

One important note should be made concerning a common nomenclature that is frequently used within syslog messages. When a change is made to an existing setting, the change is often notated by prefixing the original setting with old _ and the new setting with new _ . The example below demonstrates a display name change. Note that this example message is split into two segments because the amount of data exceeds 1KB.

```
Oct 12 14:53:24 example_host BG: 1234:01:02:site=access.example.com;…<data truncated>…event=user_
changed;old_username=jsmith;old_display_name=John Smith;old_permissions:suppor
Oct 12 14:53:24 example_host BG: 1234:02:02:t=1;old_permissions:support:canned_scripts=1;…<data
truncated>…new_display_name=John D. Smith
```

This event shows that the display name was changed. The syslog process takes a snapshot of the user's current settings and prefixes those settings with old _ . It then takes a snapshot of only the changes that are about to take effect and prefixes those settings with new _ . Because, in this example, only the display _ name setting has been changed, only that setting will have both an old _ entry and a new _ entry. However, all of the other unchanged settings will also be listed, prefixed with old _ .

Localized Strings in Syslog Messages

Another note concerns fields that refer to text in a specific language. When an event containing one of these fields is triggered, the resulting value is a localized string. When a localized string field is returned, the field name will change to include the value's language.

For example, the subject field of an access invite event returns a localized string. If an access invite's subject is changed, the resulting message would appear in the following format:

```
Oct 12 14:53:24 example_host BG: 1234:01:01:site=access.example.com;…<data
truncated>…event=customizable_text_changed;public_site:id=1;old_user:invite:email:subject:en-
us=Access Session Invitation from %USER_NAME%;old_user:invite:email:subject:it=Invito alla
sessione di accesso da %USER_NAME%;new_ user:invite:email:subject:en-us=Join %USER_NAME%'s
Session;new_ user:invite:email:subject:it=Partecipa a Sessione di %USER_NAME%
```

Note that even if your B Series Appliance does not have multiple languages installed, all applicable messages will be formatted as localized strings.

Syslog Events

Each syslog message contains the name of an event that triggered the message. While a number of syslog events are defined by the BeyondTrust Appliance B Series, most of the event types are defined within the /login administrative interface and are triggered by actions such as login attempts, creating users, and so forth. The access console also triggers syslog messages, but only for login and logout attempts.

Below is a comprehensive list of the possible events included with this version of BeyondTrust software, accompanied by a brief description of each event. Note that some events may be caused by multiple triggers. In those cases, the triggers are identified below.

Syslog Events

Event	Trigger
account_added	A new account has been added and saved.
account_changed	An existing account has been modified and saved.
account_removed	An existing account has been deleted.
account_group_added	A new account group has been added and saved.
account_group_changed	An existing account group has been modified and saved.
account_group_removed	An existing account group has been deleted.
account_jump_item_association_added	An association with a Jump Item was added for the account.
account_jump_item_association_changed	An association with a Jump Item was changed for the account.
account_jump_item_direct_association_added	The account is allowed to be injected for the specific Jump Items.
account_jump_item_direct_association_removed	The account is removed from the allowed list to be injected for the specific Jump Items.
accounts_changed	The group of one or more accounts was modified.
admin_password_reset_to_factory_default	The **Reset Admin Account** button has been clicked, reverting a site's administrative account to its default credentials.
api_account_added	A new API account has been added and saved.
api_account_changed	An existing API account has been modified and saved.
api_account_removed	An existing API account has been deleted.
backup_created	A backup of the current software configuration has been saved.
canned_script_added	A new canned script has been added and saved.
canned_script_category_added	A canned script has been newly assigned to a category, and the script has been saved.
canned_script_category_removed	A previously assigned canned message has been unassigned from a category, and the script has been saved.
canned_script_changed	An existing canned script's name, description, or command sequence has been

Event	Trigger
	changed, and the change has been saved.
canned_script_file_added	A resource file has been newly associated with a canned script, and the script has been saved.
canned_script_file_removed	A previously associated resource file has been removed from a canned script, and the script has been saved.
canned_script_removed	An existing canned script has been deleted.
canned_script_team_added	A team has been newly assigned to a canned script, and the script has been saved.
canned_script_team_removed	A previously assigned team has been unassigned from a canned script, and the script has been saved.
canned_scripts_category_added	A new canned scripts category has been created.
canned_scripts_category_removed	An existing canned scripts category has been deleted.
canned_scripts_file_added	A new canned script resource file has been uploaded.
canned_scripts_file_removed	An existing canned script resource file has been deleted.
certificate_export	An SSL certificate has been exported from the B Series Appliance.
change_display_name	A user has attempted to change their display name.
change_password	A user has attempted to change their password.
change_username	A user has attempted to change their username.
command_shell_filtering_regex_list	The list of Shell Prompt patterns.
custom_rep_link_added	A new custom link has been added and saved.
custom_rep_link_changed	An existing custom link has been edited and saved.
custom_rep_link_removed	An existing custom link has been deleted.
custom_session_attribute_added	A new custom field for API integration has been added and saved.
custom_session_attribute_changed	An existing custom field for API integration has been edited and saved.
custom_session_attribute_removed	An existing custom field for API integration has been removed.
custom_session_policy_added	Custom session permissions have been added to a user account, and the user account has been saved.
custom_session_policy_changed	Existing custom session permissions have been edited, and the user account has been saved.
custom_session_policy_removed	Existing custom session permissions have been removed from a user account, and the user account has been saved.
custom_special_action_added	A new custom special action has been added and saved.

Event	Trigger
custom_special_action_changed	An existing custom special action has been edited and saved.
custom_special_action_removed	An existing custom special action has been removed.
customizable_text_changed	An existing login agreement has been changed.
domain_added	A new vault domain has been added and saved.
domain_changed	An existing account has been modified and saved.
domain_removed	An existing vault domain has been deleted.
downloaded_rep_client	A user has clicked the link to download the access console.
ecm_group_added	An ECM Group has been added.
ecm_group_changed	An ECM Group has been changed.
ecm_group_removed	An ECM Group has been removed.
endpoint_changed	An existing endpoint has been modified and saved.
endpoint_removed	An existing endpoint has been deleted.
eula_accepted	The BeyondTrust PRA Cloud end user license agreement (EULA) has been accepted by a user, and the username has been recorded.
file_removed_from_file_store	A file has been deleted from the file store.
file_uploaded_to_file_store	A file has been added to the file store.
group_policy_add_to_jump_group_added	A Jump Group has been added to a group policy's **Add To Jump Groups** list.
group_policy_add_to_jump_group_removed	A Jump Group has been removed from a group policy's **Add To Jump Groups** list.
group_policy_add_to_jumpoint_added	A Jumpoint has been added to a group policy's **Add To Jumpoints** list.
group_policy_add_to_jumpoint_removed	A Jumpoint has been removed from a group policy's **Add To Jumpoints** list.
group_policy_add_to_support_teams_added	A team has been added to a group policy's **Add To Teams** list.
group_policy_add_to_support_teams_removed	A team has been removed from a group policy's **Add To Teams** list.
group_policy_added	A new group policy has been created and saved.
group_policy_changed	An existing group policy's priority level has changed, and the change has been saved.
group_policy_member_added	A new member has been added to a group policy, and the policy has been saved.
group_policy_member_removed	An existing member has been removed from a group policy, and the policy has been saved.
group_policy_remove_from_jump_group_added	A Jump Group has been added to a group policy's **Remove From Jump Groups** list.

Event	Trigger
group_policy_remove_from_jump_group_removed	A Jump Group has been removed from a group policy's **Remove From Jump Groups** list.
group_policy_remove_from_jumpoint_added	A Jumpoint has been added to a group policy's **Remove From Jumpoints** list.
group_policy_remove_from_jumpoint_removed	A Jumpoint has been removed from a group policy's **Remove From Jumpoints** list.
group_policy_remove_from_support_teams_added	A team has been added to a group policy's **Remove From Teams** list.
group_policy_remove_from_support_teams_removed	A team has been removed from a group policy's **Remove From Teams** list.
group_policy_removed	An existing group policy has been deleted.
jump_item_role_added	A new Jump Item Role has been created and saved.
jump_item_role_changed	An existing Jump Item Role has been modified and saved.
jump_item_role_removed	An existing Jump Item Role has been deleted.
jump_policy:schedule_entry_added	A new schedule entry has been added to a Jump Policy, and the policy has been saved.
jump_policy:schedule_entry_removedlbid.	An existing schedule entry has been removed from a Jump Policy, and the policy has been saved.
jump_policy_added	A new Jump Policy has been created and saved.
jump_policy_changed	An existing Jump Policy has been modified and saved.
jump_policy_removed	An existing Jump Policy has been deleted.
jumpoint_cluster_added	A new Jumpoint or Jumpoint cluster has been created and saved.
jumpoint_cluster_changed	An existing Jumpoint or Jumpoint cluster has been changed.
jumpoint_cluster_removed	An existing Jumpoint or Jumpoint cluster has been deleted.
jumpoint_user_added	A new member has been added to a Jumpoint, and the Jumpoint has been saved.
jumpoint_user_removed	An existing member has been removed from a Jumpoint, and the Jumpoint has been saved.
kerberos_keytab_added	A new Kerberos keytab has been uploaded.
kerberos_keytab_removed	An existing Kerberos keytab has been deleted.
login	A login attempt has been made.
login_schedule_entry_added	A new login schedule entry has been added to a user's group policy's login schedule, and the user account or group policy has been saved.
login_schedule_entry_removed	An existing login schedule entry has been removed from a user's group policy's login schedule, and the user group policy has been saved.

Event	Trigger
logout	A user has logged out of the access console, whether by deliberate action, by an administrator, or as the result of a lost connection to the B Series Appliance.
management_account_added	A new management account has been added and saved.
management_account_changed	An existing management account has been modified and saved.
management_account_removed	An existing management account has been deleted.
msgraph_http_recipient_added	A new service principal has been added and saved.
msgraph_http_recipient_changed	An existing service principal has been modified and saved.
msgraph_http_recipient_removed	An existing service principal has been deleted.
network_address_added	A new IP address has been added and saved.
network_address_changed	An existing IP address has been modified and saved.
network_address_removed	An existing IP address has been deleted. Note that you cannot delete the default route.
network_changed	The global network configuration has been changed, and the change has been saved.
network_route_changed	A static route has been added, modified, or removed.
outbound_event_email_recipient_added	A new email outbound event has been added and saved.
outbound_event_email_recipient_changed	An existing email outbound event has been modified and saved.
outbound_event_email_recipient_removed	An existing email outbound event has been deleted.
outbound_event_email_trigger_added	A new trigger has been added for an email outbound event, and the event has been saved.
outbound_event_email_trigger_removed	An existing trigger for an email outbound event has been removed, and the event has been saved.
outbound_event_http_recipient_added	A new HTTP outbound event has been added and saved.
outbound_event_http_recipient_changed	An existing HTTP outbound event has been modified and saved.
outbound_event_http_recipient_removed	An existing HTTP outbound event has been deleted.
outbound_event_http_trigger_added	A new trigger has been added for an HTTP outbound event, and the event has been saved.
outbound_event_http_trigger_removed	An existing trigger for an HTTP outbound event has been removed, and the event has been saved.
pending_vendor_user_added	A vendor user registration request was made.
pending_vendor_user_deleted	A pending vendor user was deleted.
perm_remote_shell_Allow list	A command filtering option has been Allow listed or Deny listed. Or, all commands are allowed.

Event	Trigger
perm_remote_shell_filter_commands	The list of Allow listed or Deny listed command patterns.
public_site_portal_logo_uploaded	A new logo image for the public site has been uploaded.
reboot	The B Series Appliance has been rebooted.
rep_client_connection_terminated	An administrator has terminated a user's connection.
rep_console_setting_added	A managed access console setting has been defined for the first time, and the settings have been saved.
rep_console_setting_changed	A managed access console setting has been changed, and the settings have been saved.
rep_console_setting_removed	A managed access console setting has been marked as undefined, and the settings have been saved.
rep_invite_added	A session policy has been made available for access invites, and the session policy has been saved.
rep_invite_removed	A session policy has been made unavailable for access invites and has been saved, or a session policy available for access invites has been deleted.
repinvite_setting_added	An access invite setting has been added because a session policy has been made available for access invites, and the session policy has been saved.
repinvite_setting_removed	An access invite setting has been removed either because a session policy has been made unavailable for access invites and has been saved, or because a session policy available for access invites has been deleted.
reporting_erasure	Session reports have had representative or customer data anonymized.
restored_from_backup	The software configuration has been successfully restored from its backup file.
restoring_from_backup	The software configuration is in the process of restoring from its backup file.
scheduled_discovery_job_added	The domain scheduled discovery has been added.
scheduled_discovery_job_changed	The domain scheduled discovery has changed.
security_provider_added	A new security provider configuration has been added and saved.
security_provider_changed	An existing security provider configuration's priority level has changed, and the change has been saved.
security_provider_removed	An existing security provider configuration has been deleted.
security_provider_setting_added	A security provider setting has been added as part of the initial configuration, and the configuration has been saved.
security_provider_setting_changed	An existing security provider configuration has been modified and saved.
security_provider_setting_removed	A security provider setting has been removed as part of the deletion of a security provider configuration.
server_software_restarted	The BeyondTrust software has been restarted.

Event	Trigger
session_policy_added	A new session policy has been added and saved.
session_policy_changed	An existing session policy has been modified and saved.
session_policy_removed	An existing session policy has been deleted.
setting_added	A setting has been defined and saved for the first time.
setting_changed	A setting has been modified and saved.
shared_jump_group_added	A new Jump Group has been added and saved.
shared_jump_group_changed	An existing Jump Group has been modified and saved.
shared_jump_group_removed	An existing Jump Group has been deleted.
SNMP_changed	The SNMPv2 Server has been changed.
starting_support_tunnel	A support tunnel has been initiated from the B Series Appliance.
support_session_detail_generated	A detailed report has been run for an access session.
support_session_report_generated	A report of access sessions has been run.
support_session_summary_report_generated	A summary report of support sessions has been run.
support_team_added	A team has been added.
support_team_changed	A team has been changed.
support_team_member_added	A new member has been added to a team, and the team has been saved.
support_team_member_changed	An existing member has been assigned a different role in a team, and the team has been saved.
support_team_member_removed	An existing member has been deleted from a team, and the team has been saved.
support_team_removed	An existing team has been deleted.
syslog_server_changed	The remote syslog server setting has been changed and saved.
team_activity_report_generated	A team activity report has been run.
user_account_report_generated	A user account report has been generated.
user_added	A new local user has been created and saved. Event fields differ between /login users and /appliance users.
user_changed	An existing local user has been modified and saved. Event fields differ between /login users and /appliance users.
user_removed	An existing local user has been deleted. Event fields differ between /login users and /appliance users.
user_session_policy_added	A session policy has been applied to a user account, and the user account has been

Event	Trigger
	saved.
user_session_policy_removed	A session policy has been removed from a user account, and the user account has been saved.
vault_account_password_rotation	Vault account password has been rotated.
vendor_activity_report_generated	A vendor report was generated.
windows_service_changed	A Windows service has been changed and saved.
windows_service_removed	A Windows service was removed.

Syslog Fields

Many of the triggering events related to the BeyondTrust Administrative Interface (/login) and the B Series Appliance Interface (/appliance) result in syslog messages. These syslog messages have additional fields associated.

You can configure your B Series Appliance to send these log message to an existing syslog server. B Series Appliance logs are sent using the **local0** facility.

Account Fields

These fields apply to the **account_added**, **account_changed**, and **account_removed** events.

Field	Value	Explanation
name	string	The name of the vault account.
username	string	The username of the vault account.
password	****	Indicates if the password has changed. The actual string is never supplied.
auto_rotate_credentials	**1** or **0**	**1:** Enables the automatic rotation for this vault account. **0:** Disables the automatic rotation for this vault account.
allow_simultaneous_checkout	**1** or **0**	**1:** Account can be checked out and used by multiple users or sessions at the same time. **0:** Account can be checked out and used by a single user at one time.
personal	**1** or **0**	**1:** Is a personal account. **0:** Is a shared account.
group	string	The unique identifier of the account group.

Account Group Fields

These fields apply to the **account_group_added**, **account_group_changed**, and **account_group_removed** events.

Field	Value	Explanation
id	string	The unique identifier of the account group.
name	string	The name of the account group.
description	string	The description of the account group.

Account Group Membership Fields

These fields apply to the **accounts_changed** event.

Field	Value	Explanation
accounts_id	comma-delimited list	The unique identifier of the vault accounts.
new_group	string	The unique identifier of the target account group.

Account Jump Item Association

These fields apply to the **account_jump_item_association_added** and **account_jump_item_association_removed** events.

Field	Value	Explanation
id	number	The unique identifier of the association.
account_group_id	number	The unique identifier of the account group.
account_id	number	The unique identifier of the account.
criteria	string	A JSON representation of the filters Eg. {"name":["name"],"host":["hostname"],"tag":["tag"],"comment":["comments"],"shared_jump_groups":[3]} Valid only when the filter type is criteria.
filter_type	applicable, not_injectable or criteria	The filter type of the association.

Account User Fields

These fields apply to the **account_user_added** and **account_user_removed** events.

Field	Value	Explanation
account:id	string	The unique identifier of the vault account.
role	string	The role associated with the vault account. The two possible options are **Inject** and **Inject and Checkout**.
user:id	string	The unique identifier of the user associated with this vault account.

API Account Fields

These fields apply to the **api_account_added**, **api_account_changed**, and **api_account_removed** events.

Field	Value	Explanation
client_id	string	The OAuth client ID.
client_secret	******	Indicates the OAuth client secret. The actual string is never supplied.
comments	string	Any comments associated with this API account.
ecm_group	string	The ID of the ECM Group that the account belongs to.
enabled	**1** or **0**	**1:** This API account is enabled. **0:** This API account is disabled.
id	string	The unique identifier of the API account.
ip_addresses	comma-delimited list	The list of network address prefixes from which this account can authenticate.
name	string	The name of the API account.
permissions:backup	**1** or **0**	**1:** This API account may use the backup API. **0:** This API account may not use the backup API.
permissions:command	**deny** **read_only** **full_access**	Whether this API account is disallowed to use the command API, may have read-only access to the command API, or may have full access to the command API.
permissions:ecm	**1** or **0**	**1:** This API account may use the Endpoint Credential Manager API. **0:** This API account may not use the Endpoint Credential Manager API.
permissions:reporting:support	**1** or **0**	**1:** This API account may use the reporting API. **0:** This API account may not use the reporting API.
permissions:scim	**1** or **0**	**1:** The API account may use the SCIM API. **0:** The API account may not use the SCIM API.

Canned Script Category Fields

These fields apply to the **canned_script_category_added** and **canned_script_category_removed** events.

Field	Value	Explanation
canned_script:id	string	The unique identifier of the canned script to which this category is being applied.
canned_script:name	string	The name of the canned script to which this category is being applied.
category	string	The name of the category being applied to this canned script.

Canned Script Fields

These fields apply to the **canned_script_added**, **canned_script_changed**, and **canned_script_removed** events.

Field	Value	Explanation
allowed_in_view_only	**1** or **0**	**1:** This canned script is available in view-only screen sharing, as a special action. **0:** This canned script is not available in view-only screen sharing.
commands	string	The commands to be executed when this script is run.
description	string	The description of this canned script as displayed to the user before being run.
elevation_mode	**Both** **Elevated Only** **Unelevated Only**	Whether this canned script is available only in elevated mode, only in unelevated mode, or in both elevated and unelevated modes.
id	string	The unique identifier of this canned script.
name	string	The name of this canned script.

Canned Script File Fields

These fields apply to the **canned_script_file_added** and **canned_script_file_removed** events.

Field	Value	Explanation
canned_script:id	string	The unique identifier of the canned script with which this file is being associated.
canned_script:name	string	The name of the canned script with which this file is being associated.
filename	string	The name of the file being associated with this canned script.

Canned Script Team Fields

These fields apply to the **canned_script_team_added** and **canned_script_team_removed** events.

Field	Value	Explanation
canned_script:id	string	The unique identifier of the canned script to which this team is being given access.
canned_script:name	string	The name of the canned script to which this team is being given access.
team:id	string	The unique identifier of the team being given access to this script.
team:name	string	The name of the team being given access to this script.

Canned Scripts Category Fields

These fields apply to the **canned_scripts_category_added** and **canned_scripts_category_removed** events.

Field	Value	Explanation
category	string	The name of this canned script category.

Canned Scripts File Fields

These fields apply to the **canned_scripts_file_added** and **canned_scripts_file_removed** events.

Field	Value	Explanation
filename	string	The filename of the file uploaded for canned script use.

Certificate Export Fields

These fields apply to the **certificate_export** event.

Field	Value	Explanation
friendly_name	string	The friendly name of the certificate being exported.
exported_with_private_key	**1** or **0**	**1:** The private key is included in this export. **0:** The private key is not included in this export.

Change Display Name

These fields apply to the **change_display_name** event.

Field	Value	Explanation
status	**success failure**	Whether the display name change attempt succeeded or failed.
reason	**failed** **invalid display name**	Indicates whether the new display name failed to meet formatting requirements.
target	**web/api** **web/login**	The authentication area from which the username change attempt was made.

Change Password Fields

These fields apply to the **change_password** event.

Field	Value	Explanation
status	**success** **failure**	Whether the password change attempt succeeded or failed.
reason	**failed** **invalid password**	Indicates whether the old password supplied was incorrect or the new password failed to meet complexity requirements.
target	**web/api** **web/appliance** **web/login**	The authentication area from which the password change attempt was made.

Change Username Fields

These fields apply to the **change_username** event.

Field	Value	Explanation
status	**success** **failure**	Whether the username change attempt succeeded or failed.
reason	**failed** **invalid password**	Indicates whether the supplied password was incorrect or the new username failed to meet formatting requirements.
target	**web/api** **web/appliance** **web/login**	The authentication area from which the password change attempt was made.

Custom Session Attribute Fields

These fields apply to the **custom_session_attribute_added**, **custom_session_attribute_changed**, and **custom_session_attribute_removed** events.

Field	Value	Explanation
code_name	string	The code name of the custom session attribute.
display_name	string	The display name of the custom session attribute.
id	string	The unique identifier of the custom session attribute.
show_in_rep	**1** or **0**	**1:** The custom session attribute will be displayed in the access console during an access session. **0:** The custom session attribute will not be displayed in the access console.

Custom Session Policy Fields

These fields apply to the **custom_session_policy_added**, **custom_session_policy_changed**, and **custom_session_policy_removed** events. Custom session policy events also include the "Support Permissions Fields" on page 67.

Field	Value	Explanation
code_name	string	The code name of this custom session policy.
description	string	The description of the object to which this custom session policy is applied in the form of object(type):name. The object may be one of **users** or **policies**. A **users** object is followed by **@** and the ID of its security provider. The type is either **attended** or **unattended**. The name is the name of the object.
id	string	The unique identifier of this custom session policy.
name	string	The name of this custom session policy. This name is assigned by the B Series Appliance and cannot be modified.

Custom Special Action Fields

These fields apply to the **custom_special_action_added**, **custom_special_action_changed**, and **custom_special_action_removed** events.

Field	Value	Explanation
arguments	list	Command line arguments to apply the command.
command	string	The full path of the application to run.
confirm	**1** or **0**	**1:** Require users to answer a confirmation prompt before the action runs. **0:** Do not prompt before running the action.
id	string	The unique identifier of this custom special action.
name	string	The name of this custom special action.
run_elevated	**1** or **0**	**1:** Show the special action only when the endpoint client is running in elevated mode, and run the action with elevated privileges. **0:** Always show the action, and run the action with user privileges.

Customizable Text Fields

These fields apply to the **customizable_text_changed** event.

Field	Value	Explanation
pre_login_agreement:body:[language]	string	The existing message for the /login prerequisite login agreement has changed.
pre_login_agreement:title:[language]	string	The existing title for the /login prerequisite login agreement has changed.
rep:invite:email:body:[language]	string	The existing message for an access invitation email has changed.
rep:invite:email:subject:[language]	string	The existing subject for an access invitation email has changed.

Note: *Macros appear as %MACROS% to indicate use.*

Custom Rep Link Fields

These fields apply to the **custom_rep_link_added**, **custom_rep_link_changed**, and **custom_rep_link_removed** events.

Field	Value	Explanation
id	string	The unique identifier of the custom link.
name	string	The name of the custom link.
url	string	The URL of the custom link.

Domain Fields

These fields apply to the **domain_added**, **domain_changed**, and **domain_removed** events.

Field	Value	Explanation
name	string	The name of the domain.
jumpoint:id	string	The unique identifier of the Jumpoint.

ECM Group Fields

Field	Value	Explanation
id	string	The unique identifier of the ECM Group.
name	string	The name of the ECM Group.

Endpoint Fields

These fields apply to the **endpoint_changed** and **endpoint_removed** events.

Field	Value	Explanation
distinguished_name	string	The distinguished name of the endpoint.
domain:id	string	The name of the domain.
unique_id	string	The unique identifier of the endpoint.
name	string	The name of the endpoint.
hostname	string	The hostname of the endpoint.
description	string	The description of the endpoint.
is_domain_controller	**1** or **0**	**1:** The endpoint is a domain controller. **0:** The endpoint is not a domain controller.
operating_system	string	The operating system of the endpoint.

EULA Accepted Syslog Field

Field	Value	Explanation
auth_username	string	The username of the individual who accepted the BeyondTrust PRA Cloud end user license agreement (EULA).

File Store Fields

These fields apply to the **file_removed_from_file_store** and **file_uploaded_to_file_store** events.

Fields marked with an asterisk apply only to **file_uploaded_to_file_store** events.

Field	Value	Explanation
filename	string	The name of the file being uploaded to or removed from the file store.
size*	integer	The size in bytes of the file being uploaded to the file store.

Group Policy Add to Jump Group Fields

These fields apply to the **group_policy_add_to_jump_group_added** and **group_policy_add_to_jump_group_removed** events.

Field	Value	Explanation
group_policy:id	string	The unique identifier of this group policy.
group_policy:name	string	The name of this group policy.
jump_group:id	string	The unique identifier of the Jump Group to which members of this group policy should be added.
jump_group:name	string	The name of the Jump Group to which members of this group policy should be added.
jump_item_role:id	string	The unique identifier of the Jump Item Role to assign to members of this group policy specific to this Jump Group.
jump_item_role:name	string	The name of the Jump Item Role to assign to members of this group policy specific to this Jump Group.
jump_policy:id	string	The unique identifier of the Jump Policy to assign to members of this group policy specific to this Jump Group.
jump_policy:name	string	The name of the Jump Policy to assign to members of this group policy specific to this Jump Group.

Group Policy Add to Jumpoint Fields

These fields apply to the **group_policy_add_to_jumpoint_added** and **group_policy_add_to_jumpoint_removed** events.

Field	Value	Explanation
group_policy:id	string	The unique identifier of this group policy.
group_policy:name	string	The name of this group policy.
jumpoint:id	string	The unique identifier of the Jumpoint to which members of this group policy should be added.
jumpoint:name	string	The name of the Jumpoint to which members of this group policy should be added.

Group Policy Add to Teams Fields

These fields apply to the **group_policy_add_to_support_teams_added** and **group_policy_add_to_support_teams_removed** events.

Field	Value	Explanation
group_policy:id	string	The unique identifier of this group policy.
group_policy:name	string	The name of this group policy.
role	**member** **lead** **manager**	The role assigned to members of this group policy specific to the team.
support_team:id	string	The unique identifier of the team to which members of this group policy should be added.
support_team:name	string	The name of the team to which members of this group policy should be added.

Group Policy Fields

These fields apply to the **group_policy_added**, **group_policy_changed**, and **group_policy_removed** events. Group policy events also include the "Permission Fields" on page 44.

Field	Value	Explanation
account:disabled	**1** or **0**	**1:** The accounts associated with this group policy are disabled. **0:** The accounts associated with this group policy are active.
account:expiration	Unix timestamp	The date and time the accounts associated with this group policy will expire, if ever.
allow_override	**1** or **0**	**1:** This setting can be overridden by a policy with a lower priority. **0:** This setting cannot be overridden by a policy with a lower priority.
comments	string	Any comments associated with this group policy.
id	string	The unique identifier for this group policy.
idle_timeout	integer or **site_wide_setting**	The maximum number of seconds these users can be idle within the access console before being logged out. The **site_wide_setting** option defaults to the timeout set on the **Management > Security** page. If no timeout, uses **none**.
jumpoints	serialized labeled list	The group's Jumpoint access in the form of permission:id:name, where permission is one of **added**, **removed**, or **unknown**; id is the unique identifier of the Jumpoint; and name is the name of the Jumpoint.
login_code:enabled	**1** or **0**	**1:** Users must enter an emailed login code to log in. **0:** Users may log in without an emailed login code.
name	string	The name of this group policy.
policy:id	string	The unique identifier of the group policy for which this setting is configured.
policy:name	string	The name of the group policy for which this setting is configured.
priority	integer	The priority of this group policy, in order of execution, starting from **1**.
tz	string	The time zone to use for the login schedule for this group policy.

Group Policy Member Fields

These fields apply to the **group_policy_member_added** and **group_policy_member_removed** events.

Field	Value	Explanation
policy:id	string	The unique identifier of the policy to which this member belongs.
policy:name	string	The name of the policy to which this member belongs.
provider:id	string	The unique identifier of the security provider against which this member authenticates.
provider:name	string	The name of the security provider against which this member authenticates.
user:external_id	string	The unique identifier of this group policy member.

Group Policy Remove from Jump Group Fields

These fields apply to the **group_policy_remove_from_jump_group_added** and **group_policy_remove_from_jump_group_removed** events.

Field	Value	Explanation
group_policy:id	string	The unique identifier of this group policy.
group_policy:name	string	The name of this group policy.
jump_group:id	string	The unique identifier of the Jump Group from which members of this group policy should be removed.
jump_group:name	string	The name of the Jump Group from which members of this group policy should be removed.
jump_item_role:id	string	The unique identifier of the Jump Item Role to assign to members of this group policy specific to this Jump Group.
jump_item_role:name	string	This field will always be empty.
jump_policy:id	string	The unique identifier of the Jump Policy to assign to members of this group policy specific to this Jump Group.
jump_policy:name	string	This field will always be empty.

Group Policy Remove from Jumpoint Fields

These fields apply to the **group_policy_remove_from_jumpoint_added** and **group_policy_remove_from_jumpoint_removed** events.

Field	Value	Explanation
group_policy:id	string	The unique identifier of this group policy.
group_policy:name	string	The name of this group policy.
jumpoint:id	string	The unique identifier of the Jumpoint from which members of this group policy should be removed.
jumpoint:name	string	The name of the Jumpoint from which members of this group policy should be removed.

Group Policy Remove from Teams Fields

These fields apply to the **group_policy_remove_from_support_teams_added** and **group_policy_remove_from_support_teams_removed** events.

Field	Value	Explanation
group_policy:id	string	The unique identifier of this group policy.
group_policy:name	string	The name of this group policy.
role	**member** **lead** **manager**	The role assigned to members of this group policy specific to the team.
support_team:id	string	The unique identifier of the team from which members of this group policy should be removed.
support_team:name	string	The name of the team from which members of this group policy should be removed.

Jump Item Role Fields

These fields apply to the **jump_item_role_added**, **jump_item_role_changed**, and **jump_item_role_removed** events.

Field	Value	Explanation
description	string	The description of this Jump Item Role.
id	string	The unique identifier of this Jump Item Role.
name	string	The name of this Jump Item Role.
perm_add	**1 or 0**	**1:** This role grants permission to create and deploy Jump Items. **0:** This role does not grant permission to create Jump Items.
perm_assign_jump_group	**1** or **0**	**1:** This role grants permission to move Jump Items into and out of Jump Groups. **0:** This role does not grant permission to move Jump Items between Jump Groups.
perm_edit_behavior	**1** or **0**	**1:** This role grants permission to edit Jump Item behavior and experience settings. **0:** This role does not grant permission to edit behavior and experience settings.
perm_edit_comments	**1** or **0**	**1:** This role grants permission to edit Jump Item comments. **0:** This role does not grant permission to edit comments.
perm_edit_identity	**1** or **0**	**1:** This role grants permission to edit Jump Item connectivity and authentication settings. **0:** This role does not grant permission to edit connectivity and authentication settings.
perm_edit_jump_policy	**1** or **0**	**1:** This role grants permission to assign Jump Policies to Jump Items. **0:** This role does not grant permission to assign Jump Policies to Jump Items.
perm_edit_session_policy	**1** or **0**	**1:** This role grants permission to assign session policies to Jump Items. **0:** This role does not grant permission to assign session policies to Jump Items.
perm_edit_tag	**1** or **0**	**1:** This role grants permission to edit Jump Item tags. **0:** This role does not grant permission to edit tags.
perm_remove	**1** or **0**	**1:** This role grants permission to delete Jump Items. **0:** This role does not grant permission to delete Jump Items.
perm_start	**1** or **0**	**1:** This role grants permission to start sessions with Jump Items. **0:** This role does not grant permission to start sessions with Jump Items.
perm_view_jump_item_report	**1** or **0**	**1:** This role grants permission to view Jump Item reports. **0:** This role does not grant permission to view Jump Item reports.

Jump Policy Fields

These fields apply to the **jump_policy_added**, **jump_policy_changed**, and **jump_policy_removed** events.

Field	Value	Explanation
authorization:allowed_to	**1** or **0**	**1:** Access approval applies to anyone with permission to request access. **0:** Access approval applies only to the requester.
authorization:approver_name	string	The name of the approval email recipient.
authorization:email_addresses	string	The email addresses to which approval emails are sent.
authorization:enabled	**1** or **0**	**1:** Require approval before a session starts. **0:** Do not require approval.
authorization:locale_code	string	Values are the language abbreviations (e.g. en-us for English) used with approval emails.
authorization:max_duration	integer	The maximum length of time in seconds for which a user can request access.
authorization:ticket_system_enabled	**1** or **0**	**1:** Require a ticket ID before a session can start. **0:** Do not require a ticket ID.
code_name	string	The code name of this Jump Policy.
description	string	The description of this Jump Policy.
display_name	string	The display name of this Jump Policy.
id	string	The unique identifier of this Jump Policy.
notification:email_addresses	string	The email addresses to which notification emails are sent.
notification:locale_code	string	Values are the language abbreviations (e.g. en-us for English) used with notification emails.
notification:recipient_name	string	The name of the notification email recipient.
notify_on_customer_leave	**1** or **0**	**1:** Notify recipients when a session ends. **0:** Do not notify recipients when a session ends.
notify_on_session_start	**1** or **0**	**1:** Notify recipients when a session starts. **0:** Do not notify recipients when a session starts.
schedule:enabled	**1** or **0**	**1:** Users are disallowed to access Jump Items controlled by this policy outside of the set schedule. **0:** Users may access Jump Items controlled by this policy at any time.
schedule:force_end	**1** or **0**	**1:** Open sessions with Jump Items controlled by this policy are automatically terminated at the end of the scheduled time. **0:** Open sessions with Jump Items controlled by this policy may continue past the end of the scheduled time.
session_recordings_disabled	**1** or **0**	**1:** Disable session recordings for Jump Items controlled by this policy. **0:** Do not disable session recordings.

Jump Policy Schedule Entry Fields

These fields apply to the **jump_policy:schedule_entry_added** and **jump_policy:schedule_entry_removed** events.

Field	Value	Explanation
jump_policy:display_name	string	The display name of the Jump Policy to which this Jump schedule entry applies.
jump_policy:id	string	The unique identifier of the Jump Policy to which this Jump schedule entry applies.
schedule:end_day_of_week	**Monday** **Tuesday** **Wednesday** **Thursday** **Friday** **Saturday** **Sunday**	The end day for this Jump schedule entry.
schedule:end_time_of_day	hh:mm (24-hour format)	The end time for this Jump schedule entry.
schedule:start_day_of_week	**Monday** **Tuesday** **Wednesday** **Thursday** **Friday** **Saturday** **Sunday**	The start day for this Jump schedule entry.
schedule:start_time_of_day	hh:mm (24-hour format)	The start time for this Jump schedule entry.

Jumpoint Cluster Fields

These fields apply to the **jumpoint_cluster_added**, **jumpoint_cluster_changed**, and **jumpoint_cluster_removed** events.

Field	Value	Explanation
allows_multiple_nodes	**1** or **0**	**1:** This is a Jumpoint cluster. **0:** This is a standalone Jumpoint.
code_name	string	The code name of this Jumpoint or Jumpoint cluster.
comments	string	Any comments associated with this Jumpoint or Jumpoint cluster.
disabled	**1** or **0**	**1:** This Jumpoint or Jumpoint cluster is disabled. **0:** This Jumpoint or Jumpoint cluster is enabled.
external_jump_item_network_id	string	The unique identifier of the external Jump Item.
id	string	The unique identifier of this Jumpoint or Jumpoint cluster.
name	string	The name of this Jumpoint or Jumpoint cluster.
network_tunnel	**1** or **0**	**1:** This Jumpoint or Jumpoint cluster can be configured to allow Protocol Tunnel Jumps". **0:** This Jumpoint or Jumpoint cluster does not allow Protocol Tunnel Jumps.
platform	string	The platform of the Jumpoint cluster.
rdp_service_account_id	string	The Vault Account ID used to deploy an ad hoc client to RDP servers when Session Forensics is enabled.
shelljump	**1** or **0**	**1:** This Jumpoint or Jumpoint cluster can be configured to allow Shell Jump. **0:** This Jumpoint or Jumpoint cluster does not allow Shell Jump.

Jumpoint User Fields

These fields apply to the **jumpoint_user_added** and **jumpoint_user_removed** events.

Field	Value	Explanation
jumpoint:id	string	The unique identifier of the Jumpoint to which this user is being added or removed.
jumpoint:name	string	The name of the Jumpoint to which this user is being added or removed.
user:id	string	The unique identifier of the user being added or removed.
user:username	string	The name of the user being added or removed.

Kerberos Keytab Fields

These fields apply to the **kerberos_keytab_added** and **kerberos_keytab_removed** events.

Fields marked with an asterisk apply only to **kerberos_keytab_added** events.

Field	Value	Explanation
enctype*	string	The encryption type of the keytab.
principal	string	The service principal of the keytab.
timestamp*	Unix timestamp	The timestamp of the keytab.
vno*	integer	The key version number of the keytab.

Login Fields

These fields apply to the **login** event, triggered from the administrative interface or the access console.

Field	Value	Explanation
status	**success** **failure**	Whether the login attempt succeeded or failed.
reason	**failed** **account disabled** **account expired** **exceeded failed login attempts** **change password**	Appears only if login failed. Indicates the reason for the failure, such as the account being disabled or expired, the number of failed login attempts having exceeded the permissible amount, or the password requiring reset.
target	**web/api** **web/appliance** **web/login** **rep_client**	The authentication area from which the login attempt was made.

Login Schedule Entry Fields

These fields apply to the **login_schedule_entry_added** and **login_schedule_entry_removed** events.

Field	Value	Explanation
schedule:end_day_of_week	**Monday** **Tuesday** **Wednesday** **Thursday** **Friday** **Saturday** **Sunday**	The end day for this login schedule entry.
schedule:end_time_of_day	hh:mm (24-hour format)	The end time for this login schedule entry.
schedule:start_day_of_week	**Monday** **Tuesday** **Wednesday** **Thursday** **Friday** **Saturday** **Sunday**	The start day for this login schedule entry.
schedule:start_time_of_day	hh:mm (24-hour format)	The start time for this login schedule entry.
user:id	string	The unique identifier of the user to whom this login schedule entry applies.
user:username	string	The username of the user to whom this login schedule entry applies.

Management Account Fields

These fields apply to the **management_ account_added**, **management_account_changed**, and **management_account_removed** events.

Field	Value	Explanation
domain_account:id	string	The unique identifier of the domain account.
domain:id	string	The unique identifier of the domain.

Network Address Fields

These fields apply to the **network_address_added**, **network_address_changed**, and **network_address_removed** events.

Field	Value	Explanation
enabled	**1** or **0**	**1:** This IP address is enabled. **0:** This IP address is disabled.
interface	string	The NIC to use as the interface.
ip	string	The IP address of the interface.
netmask	string	The netmask for this IP address.
permit:http	**1** or **0**	**1:** Permit HTTP traffic through this IP and interface. **0:** Do not permit HTTP traffic through this IP and interface.
permit:https	**1** or **0**	**1:** Permit HTTPS traffic through this IP and interface. **0:** Do not permit HTTPS traffic through this IP and interface.
permit:session	**1** or **0**	**1:** Permit BeyondTrust session traffic, such as access console and endpoint client connections, through this IP and interface. **0:** Do not permit BeyondTrust session traffic through this IP and interface.

Network Fields

These fields apply to the **network_changed** event.

Field	Value	Explanation
default_route	string	The default network route for the B Series Appliance.
dns:1	string	The IP address of the primary DNS server.
dns:2	string	The IP address of the secondary DNS server.
dns:3	string	The IP address of the tertiary DNS server.
dns:opendns	**1** or **0**	**1:** The B Series Appliance should fall back to OpenDNS servers if the configured DNS servers fail to reply. **0:** The B Series Appliance should never fall back to OpenDNS servers.
gateway:interface	string	The interface to use as the default gateway.
gateway:ip	string	The IP address of the default gateway.
hostname	string	The hostname of the B Series Appliance.
icmp_echo	**1** or **0**	**1:** The interface will respond to ICMP echoes. **0:** The interface will not respond to ICMP echoes.
ntp_server	string	The IP address of the NTP server.
ssl:ciphers	comma-delimited list	The set of ciphersuites supported by the B Series Appliance for HTTPS/SSL traffic.
ssl:v2	**1** or **0**	**1:** SSLv2 is enabled. **0:** SSLv2 is not enabled.
ssl:v3	**1** or **0**	**1:** SSLv3 is enabled. **0:** SSLv3 is not enabled.

Network Route Descriptor

This field applies to the **network_route_changed** event.

Field	Value	Explanation
[ip/bit=gw@NIC]	string	The IP address and CIDR bitmask, along with the gateway address at a particular interface.

Outbound Event Email Recipient Fields

These fields apply to the **outbound_event_email_recipient_added**, **outbound_event_email_recipient_changed**, and **outbound_event_email_recipient_removed** events.

Field	Value	Explanation
disabled	**1** or **0**	**1:** The outbound event email recipient is disabled. **0:** The outbound event email recipient is enabled.
email_address	string	The email address to which the outbound event is sent.
id	string	The unique identifier of this outbound event email recipient.
name	string	The name of this outbound event email recipient.
require_external_key	**1** or **0**	**1:** Emails are sent only for sessions that have an external key at the time the event occurs. **0:** Emails are sent for all sessions, even those that do not have an external key.

Outbound Event Email Trigger Fields

These fields apply to the **outbound_event_email_trigger_added** and **outbound_event_email_trigger_removed** events.

Field	Value	Explanation
event:email:body	string	The body of the email sent to the recipient.
event:email:enabled	**1** or **0**	**1:** The email event is enabled. **0:** The email event is disabled.
event:email:subject	string	The subject of the email sent to the recipient.
recipient:id	string	The unique identifier of the recipient to which this event will be emailed.
recipient:name	string	The name of the recipient to which this event will be emailed.

Outbound Event HTTP Recipient Fields

These fields apply to the **outbound_event_http_recipient_added**, **outbound_event_http_recipient_changed**, and **outbound_event_http_recipient_removed** events.

Field	Value	Explanation
cert	**<data>** **none**	Indicates that a certificate has been uploaded or changed. Only the value <data> will be displayed for a changed certificate.
disabled	**1** or **0**	**1:** The outbound event recipient is disabled. **0:** The outbound event recipient is enabled.
failure:email	string	The email address to which to send a failure notification if the outbound event cannot be posted.
failure:first_notice	integer	The number of seconds that must have elapsed since the first error before sending a failure notification email.
failure:repeat_interval	integer	The number of seconds that must have elapsed since the last alert was sent before sending another failure notification email if the event is still failing.
id	string	The unique identifier of this outbound event recipient.
name	string	The name of this outbound event recipient.
retry:duration	integer	The number of seconds that must have elapsed since the first error before the event stops retrying and is marked as failed.
retry:interval	integer	The number of seconds between each retry attempt.
url	string	The URL of the outbound event recipient to which the event will be posted.

Outbound Event HTTP Trigger Fields

These fields apply to the **outbound_event_http_trigger_added** and **outbound_event_http_trigger_removed** events.

Field	Value	Explanation
event:name	**support_conference_begin** **support_conference_end** **support_conference_owner_changed** **support_conference_member_added** **support_conference_member_departed**	The event to send to the recipient. There will be one event per post, with multiple events resulting in multiple posts to the recipient.
recipient:id	string	The unique identifier of the recipient to which this event will be posted.
recipient:name	string	The name of the recipient to which this event will be posted.

Permission Fields

These fields apply to both user and group policy events.

Field	Value	Explanation
permissions:admin	**1** or **0**	**1:** The user is an administrator. **0:** The user is not an administrator.
permissions:api:command	**1** or **0**	**1:** The user is allowed to use the command API. **0:** The user is not allowed to use the command API.
permissions:api:reporting	**1** or **0**	**1:** The user is allowed to use the reporting API. **0:** The user is not allowed to use the reporting API.
permissions:api:state	**1** or **0**	**1:** The user is allowed to use the real-time state API. **0:** The user is not allowed to use the real-time state API.
permissions:canned_scripts	**1** or **0**	**1:** The user may create and edit canned scripts. **0:** The user may not create or edit canned scripts.
permissions:change_display_name	**1** or **0**	**1:** The user may change their display name. **0:** The user may not change their display name.
permissions:custom_rep_links	**1** or **0**	**1:** The user may create and edit custom rep links. **0:** The user may not create or edit custom rep links.
permissions:file_store	**1** or **0**	**1:** The user may add or remove files from the file store. **0:** The user may not edit the file store.
permissions:issues	**1** or **0**	**1:** The user may create and edit issues. **0:** The user may not create or edit issues.
permissions:jump_groups	**1** or **0**	**1:** The user may edit Jump Groups. **0:** The user may not edit Jump Groups.
permissions:jump_item_role:default:id	string	The unique identifier of this user's default Jump Item Role.
permissions:jump_item_role:default:name	string	The name of this user's default Jump Item Role.
permissions:jump_item_role:personal:id	string	The unique identifier of this user's personal Jump Item Role.
permissions:jump_item_role:personal:name	string	The name of this user's personal Jump Item Role.
permissions:jump_item_role:system:id	string	The unique identifier of this user's system Jump Item Role.
permissions:jump_item_role:system:name	string	The name of this user's system Jump Item Role.
permissions:jump_item_role:teams:id	string	The unique identifier of this user's team Jump Item Role.

Field	Value	Explanation
permissions:jump_item_role:teams:name	string	The name of this user's team Jump Item Role.
permissions:rep_to_rep_screen_sharing	**1** or **0**	**1:** The user is allowed to show their screen to other users outside of a session. **0:** The user is not allowed to show their screen to other users.
permissions:rep_to_rep_screen_sharing:control	**1** or **0**	**1:** When showing their screen to another user, the user is allowed to grant control to the viewing user. **0:** When showing their screen to another user, the user is not allowed to grant control to the viewing user.
permissions:reporting:license_reports	**1** or **0**	**1:** The user is allowed to view license usage reports. **0:** The user is not allowed to view license usage reports.
permissions:reporting:recordings	**1** or **0**	**1:** The user is allowed to view support session recordings. **0:** The user is not allowed to view session recordings.
permissions:reporting:support_reports	**none** **user_sessions** **team_sessions** **all_sessions**	Whether the user is disallowed to generate reports or is allowed to generate reports only for sessions in which they were the primary user, for sessions in which one of their teammates was the primary user or one of their teams was the primary team, or for all sessions.
permissions:support	**not_allowed** **full_support**	Whether the user is disallowed to offer support or is allowed to offer full remote support.
permissions:support:extended_availability_mode	**1** or **0**	**1:** The user is allowed to enable extended availability. **0:** The user is not allowed to enable extended availability.
permissions:support:external_key*	**1** or **0**	**1:** The user is allowed to edit the external key. **0:** The user is not allowed to edit the external key.
permissions:support:invite_temp_rep	**1** or **0**	**1:** The user is allowed to invite an external user into a single session. **0:** The user is not allowed to invite an external user into a session.
permissions:support:jump:clients	**1** or **0**	**1:** The user is allowed to Jump to unattended systems via preinstalled Jump Clients. **0:** The user is not allowed to Jump to unattended systems via pre-installed Jump Clients.
permissions:support:jump:local	**1** or **0**	**1:** The user is allowed to Jump to unattended computers on the same network without Jump Clients or a Jumpoint.

Field	Value	Explanation
		0: The user is not allowed to Jump to computers on the same network without Jump Clients or a Jumpoint.
permissions:support:jump:remote	**1** or **0**	**1:** The user is allowed to Jump to unattended remote computers through a Jumpoint. **0:** The user is not allowed to Jump to unattended remote computers through a Jumpoint.
permissions:support:jumpoint:admin	**1** or **0**	**1:** The user is allowed to create and edit Jumpoints. **0:** The user is not allowed to create or edit Jumpoints.
permissions:support:jumpoint:shell	**1** or **0**	**1:** The user is allowed to use Shell Jump. **0:** The user is not allowed to use Shell Jump.
permissions:support:rdp:remote	**1** or **0**	**1:** The user is allowed to use BeyondTrust to start a Remote Desktop Protocol (RDP) session with a computer on a remote network. **0:** The user is not allowed to use BeyondTrust for RDP on a remote network.
permissions:support:team_share	**1** or **0**	**1:** The user can share sessions with teams to which they do not belong. **0:** The user cannot share sessions with teams to which they do not belong.
permissions:support:vnc:remote	**1** or **0**	**1:** The user is allowed to use BeyondTrust to start a VNC session with a computer on a remote network. **0:** The user is not allowed to use BeyondTrust for VNC on a remote network.
permissions:support:vpro	**1** or **0**	**1:** The user is allowed to control a computer using Intel® vPro Technology. **0:** The user is not allowed to control a computer using Intel® vPro Technology.
permissions:teams	**1** or **0**	**1:** The user is allowed to create and edit teams. **0:** The user is not allowed to create or edit teams.
permissions:users:set_passwords	**1** or **0**	**1:** The user is allowed to reset other users' passwords. **0:** The user is not allowed to reset other users' passwords.

Perm Remote Shell Filter Commands Fields

This field applies to the **perm_remote_shell_filter_commands** event.

Field	Value	Explanation
support:permissions:command_shell_commands	string	List of the command patterns that are white-listed or black-listed.

Perm Remote Shell Allow List Field

This field applies to the **perm_remote_shell_Allow list** event.

Field	Value	Explanation
support:permissions:command_shell_is_Allow list	**0**, **1**, or **2**	Integer denoting command filtering options. **0:** Allow all commands **1:** White-list command **2:** Black-list command

Public Site Portal Logo Fields

These fields apply to the **public_site_portal_logo_uploaded** event.

Field	Value	Explanation
site:id	string	The unique identifier of the public site to which this logo image is assigned. This will always be **1**.
site:name	string	The name of the public site to which this logo image is assigned. This will always be **Default**.
size	integer	The size in bytes of the custom logo image. Applies only to new images being uploaded.

Access Console Connection Fields

These fields apply to the **rep_client_connection_terminated** event.

Field	Value	Explanation
display_name	string	The display name of the user whose connection to the access console has been terminated.
username	string	The username of the user whose connection to the access console has been terminated.

Access Console Setting Fields

These fields apply to the **rep_console_setting_added**, **rep_console_setting_changed**, and **rep_console_setting_removed** events.

Field	Value	Explanation
rep_console_setting:alerts:chat_audible:enabled	**1** or **0**	**1:** Play a sound when a chat message is received. **0:** Do not play a sound when a chat message is received.
rep_console_setting:alerts:chat_audible:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.
rep_console_setting:alerts:chat_visual:enabled	**1** or **0**	**1:** Flash the application icon when a chat message is received. **0:** Do not flash the application icon when a chat message is received.
rep_console_setting:alerts:chat_visual:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.
rep_console_setting:alerts:queue_audible:enabled	**1** or **0**	**1:** Play a sound when a session enters any queue. **0:** Do not play a sound when a session enters any queue.
rep_console_setting:alerts:queue_audible:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.
rep_console_setting:alerts:queue_visual:enabled	**1** or **0**	**1:** Flash the application icon when a session enters any queue. **0:** Do not flash the application icon when a session enters any queue.
rep_console_setting:alerts:queue_visual:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.
rep_console_setting:automatic:local_jumps_elevate:enabled	**1** or **0**	**1:** Automatically elevate local network Jump attempts. **0:** Do not automatically elevate local network Jump attempts.
rep_console_setting:automatic:local_jumps_elevate:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.
rep_console_setting:automatic:screen_sharing:enabled	**1** or **0**	**1:** Automatically request screen sharing. **0:** Do not automatically request screen sharing.
rep_console_setting:automatic:screen_sharing:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.
rep_console_setting:automatic:session_window_detach:enabled	**1** or **0**	**1:** Automatically detach new session tabs into separate windows. **0:** Do not automatically detach new session tabs into separate windows.

Field	Value	Explanation
rep_console_setting:automatic:session_window_detach:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.
rep_console_setting:chat_show_support_session_pop-up_notifications:enabled	**1** or **0**	**1:** Display a pop-up notification when a session chat is received. **0:** Do not display pop-up notifications for session chat.
rep_console_setting:chat_show_support_session_pop-up_notifications:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.
rep_console_setting:chat_show_team_pop-up_notifications:enabled	**1** or **0**	**1:** Display a pop-up notification when a team chat is received. **0:** Do not display pop-up notifications for team chat.
rep_console_setting:chat_show_team_pop-up_notifications:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.
rep_console_setting:chat_show_team_status_messages:enabled	**1** or **0**	**1:** Show status messages in team chat windows. **0:** Do not show status messages in team chat windows.
rep_console_setting:chat_show_team_status_messages:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.
rep_console_setting:command_history_length	integer	The number of lines of available command history.
rep_console_setting:command_history_length:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.
rep_console_setting:enable_dockable_widgets:enabled	**1** or **0**	**1:** The session sidebar can be configured. **0:** The session sidebar cannot be configured.
rep_console_setting:enable_dockable_widgets:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.
rep_console_setting:pop-up:personal_queue_shared_session:enabled	**1** or **0**	**1:** Display a pop-up notification when a session is shared in the personal queue. **0:** Do not display a pop-up notification when a session is shared in the personal queue.
rep_console_setting:pop-up:personal_queue_shared_session:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.
rep_console_setting:pop-up:session_duration:enabled	integer	The number of seconds that pop-up notifications should appear.
rep_console_setting:pop-up:session_duration:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.
rep_console_setting:pop-up:session_location	**bottom_left** **bottom_right** **top_left** **top_right**	The location where pop-up notifications should appear.

Field	Value	Explanation
rep_console_setting:pop-up:session_location:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.
rep_console_setting:pop-up:team_queue_shared_session:enabled	**1** or **0**	**1:** Display a pop-up notification when a session is shared in a team queue. **0:** Do not display a pop-up notification when a session is shared in a team queue.
rep_console_setting:pop-up:team_queue_shared_session:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.
rep_console_setting:screen_sharing_fullscreen:enabled	**1** or **0**	**1:** Automatically enter full screen mode when screen sharing starts. **0:** Do not automatically enter full screen mode when screen sharing starts.
rep_console_setting:screen_sharing_fullscreen:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.
rep_console_setting:screen_sharing_quality	**low** **performance_color** **performance_quality** **quality** **performance** **lossless**	**low:** Black and white **performance_color:** Few colors **performance_quality:** More colors **quality:** Full color **performance:** Best performance **lossless:** Lossless
rep_console_setting:screen_sharing_quality:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.
rep_console_setting:screen_sharing_scaling	**scaled** **actual**	Whether screen sharing starts with the remote screen scaled to fit or at actual size.
rep_console_setting:screen_sharing_scaling:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.
rep_console_setting:screen_sharing_sidebar_collapse:enabled	**1** or **0**	**1:** Automatically collapse the sidebar when full screen mode is used. **0:** Do not automatically collapse the sidebar when full screen mode is used.
rep_console_setting:screen_sharing_sidebar_collapse:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.
rep_console_setting:spell_checking:enabled	**1** or **0**	**1:** Spell checking is turned on. **0:** Spell checking is not turned on.
rep_console_setting:spell_checking:forced	**1** or **0**	**1:** The associated setting is forced. **0:** The associated setting is not forced.

Access Invite Fields

These fields apply to the **rep_invite_added** and **rep_invite_removed** events.

Field	Value	Explanation
comments	string	The description associated with the session policy used for this access invite.
name	string	The name of the session policy used for this access invite.

Access Invite Setting Fields

These fields apply to the **repinvite_setting_added** and **repinvite_setting_removed** events.

Field	Value	Explanation
permissions:admin	**0**	An access invite user will never be an administrator.
permissions:support	**full_support**	An access invite user will always be allowed to offer full remote support.
repinvite:id	string	The unique identifier of the rep invite session policy to which this setting applies.
repinvite:name	string	The name of the rep invite session policy to which this setting applies.

Report Fields

These fields apply to the **support_session_report_generated**, **support_session_detail_generated**, **support_session_summary_report_generated**, and **team_activity_report_generated** events.

Field	Value	Explanation
api	**1** or **0**	**1:** The report query was made via the API. **0:** The report query was not made via the API.
computer_name	string	The computer name filter used in the query, if specified.
end_time	date	The readable date and time of the last date to be included in the report, if date filters were specified.
end_timestamp	Unix timestamp	The exact timestamp of the last date to be included in the report, if date filters were specified.
external_key	string	The external key filter used in the query, if specified.
lseq	integer	The session sequence number used to query for a detailed session report, if specified.
lsid	string	The unique session identifier used to query for a detailed session report, if specified.
lsids	comma-separated strings	A comma-separated list of unique session identifiers used to query for multiple detailed session reports, if specified.
members_of_team_id	string	The unique identifier of the team used to filter the query to include only sessions that involved users who are members of the specified team.
members_of_team_name	string	The name of the team specified by **members_of_team_id**.
only_completed	**1** or **0**	**1:** The report contains only completed sessions. **0:** The report contains both completed and uncompleted sessions.
primary_rep	**1** or **0**	**1:** The users specified by **rep_id** or **members_of_team_id** must be the primary users in the sessions returned. **0:** The users specified by **rep_id** or **members_of_team_id** can be any participating user in the sessions returned.
private_ip	string	The private IP address filter used in the query, if specified.
public_ip	string	The public IP address filter used in the query, if specified.
rep_id	string	The user filter value, if specified. The value is either a unique user identifier, the string **any**, or the string **none**.
rep_name	string	The display name of the representative specified by **rep_id**, when applicable.
row_count	integer	The maximum number of rows to display at one time.
row_start	integer	The first row shown on this page of the report.

Field	Value	Explanation
session_count	integer	The number of session detail reports returned in search results. This will be **0** or **1** for web requests and **0** or more for API requests.
start_time	date	The readable date and time of the first date to be included in the report, if any date filters were used.
start_timestamp	Unix timestamp	The exact timestamp of the first date to be included in the report, if any date filters were used.
team_id	string	The team filter value, if specified. The value is either a unique team identifier, the string **all**, or the string **none**.
team_name	string	The name of the team specified by **team_id**, when applicable.

Reporting Erasure Fields

These fields apply to the **reporting_erasure** event.

Field	Value	Explanation
request_date	Unix timestamp	The timestamp presented in reports for the anonymization action.
subject	**user** or **customer**	An identifier of what type of person was anonymized, either a user or an endpoint.
user_name	string	The original private display name or username of the anonymized user.
user_id	string	The user ID of the anonymized user.
support_sessions_affected	integer	The number of support session affected by the anonymization action.
support_sessions_replace	string	A comma-separated list of replacement terms used.
team_activity_affected	integer	The number of teams affected by the anonymization action.
team_activity_replace	string	A comma-separated list of replacement terms used.

Scheduled Discovery Job Fields

These fields apply to the **scheduled_discovery_job_added** and **scheduled_discovery_job_changed** events.

Field	Value	Explanation
domain:id	number	The unique identifier of the domain.
enabled	**1** or **0**	The scheduled discovery job is either enabled or disabled.
endpoint_search_path	string	The LDAP search path to discovery endpoints.
endpoint_search_ldap_filter	string	The LDAP filter to discovery endpoints.
id	number	The unique identifier of the scheduled job.
include_domain_accounts	**1** or **0**	The discovery must include domain accounts.
include_endpoints	**1** or **0**	The discovery must include endpoints.
include_local_accounts	**1** or **0**	The discovery must include local accounts.
include_services	**1** or **0**	The discovery must include Windows services.
frequency	number	The days when discovery will run.
start_time	time	Hours and minutes when the discovery will run.
template	string	Internal use only.
push_agent_id	number	The unique identifier of the Jumpoint.
domain_distinguished_name	string	The distinguished name of the domain.
username	string	The user for the discovery.
credential_id	number	The unique identifier of the scheduled job.
domain_unique_id	string	The unique identifier of the domain.
domain_dns_name	string	The domain DNS name.
user_unique_id	string	The user unique ID.
user_distinguished_name	string	The distinguished name of the user.
management_account_domain	string	The parent domain account.
user_search_ldap_filter	string	The LDAP filter to discovery users.
user_search_path	string	The LDAP search path to discovery users.

Security Provider Fields

These fields apply to the **security_provider_added**, **security_provider_changed**, and **security_provider_removed** events.

Field	Value	Explanation
enabled	**1** or **0**	**1:** The security provider is enabled. **0:** The security provider is disabled.
id	string	The unique identifier of the security provider to which this setting applies.
name	string	The name of the security provider to which this setting applies.
priority	integer	The priority of this security provider configuration, in the order in which authentication should be attempted, starting from **1**. Two providers may share the same priority but only if one of these providers is a user provider and the other is a group provider.
provider_type	**local** **cluster** **kerberos** **ldap** **radius** **saml** **scim**	The type of service this provider configuration is set to access.
service_type	**users** **groups**	The type of authentication or authorization information this provider supplies.

Security Provider Setting Fields

These fields apply to the **security_provider_setting_added**, **security_provider_setting_changed**, and **security_provider_setting_removed** events.

Field	Value	Explanation
cluster:mode	**failover** **random**	The mode in which this cluster is set to operate.
cluster:retry:delay	integer	The number of seconds to wait after a cluster member becomes unavailable before trying that cluster member again.
default_group_policy:id	string	The unique identifier of the default group policy to apply to users who authenticate against this security provider.
default_group_policy:name	string	The name of the default group policy to apply to users who authenticate against this security provider.
kerberos:spns:list	string	The list of SPNs by which this provider is identified if the Kerberos SPN handling mode is set to **list**.
kerberos:spns:mode	**all** **list**	The way SPNs are matched to this provider. **All** handles any SPN recognized by the keytab, while **list** handles only the specified list of SPNs.
kerberos:strip_realm	**1** or **0**	**1:** The REALM portion will be stripped from the User Principal Name when constructing the username and (optionally) the display name. **0:** The REALM portion will not be stripped from the User Principal Name.
kerberos:users:mode	**all** **list** **regex**	The way users are matched to this provider. **All** handles any valid authentication attempt, **list** handles only the specified list of users, and **regex** handles only users who match the specified regular expression.
kerberos:users:regex	string	The Perl-compatible regular expression that user principals must match to be considered part of this provider if the Kerberos user handling mode is set to **regex**.
ldap:agent	**1** or **0**	**1:** A connection agent is being used to enable communication. **0:** The LDAP server and the B Series Appliance communicate directly.
ldap:agent:password	****	The readable date and time of the first date to be included in the report.
ldap:binding:anonymous	**1** or **0**	**1:** Anonymous binding is being used. **0:** A bind username and password are required.
ldap:binding:password	****	The password used for binding.
ldap:binding:username	string	The username used for binding.
ldap:cache	**1** or **0**	**1:** LDAP object cache is enabled. **0:** LDAP object cache is disabled.
ldap:cert	**<data>** or blank	Indicates that a certificate has been uploaded or changed. Only the value **<data>** will be displayed.

Field	Value	Explanation
ldap:display_name	string	The set of LDAP attributes used to populate group display names.
ldap:display_query	string	The LDAP query used to determine which users and groups to display when browsing via group policies.
ldap:encryption	**none** **ssl** **starttls**	The type of security encryption to use. **None** indicates non-encrypted LDAP, **ssl** indicates LDAPS, and **starttls** indicates LDAP with TLS.
ldap:groups:objects	string	The LDAP objectClasses that are considered valid groups.
ldap:groups:recursive	**1** or **0**	**1:** Perform recursive group lookup, searching for group members of groups until no results are returned. **0:** Execute only one group lookup query.
ldap:groups:search_base	string	The distinguishedName at which to start searching for groups.
ldap:groups:unique_id	string	The set of LDAP attributes used to uniquely identify groups in the LDAP server.
ldap:groups:user_to_group_relationship	string	The mapping of LDAP attributes used to determine a user's group memberships.
ldap:host	string	The hostname of the LDAP server.
ldap:port	string	The port through which to connect to the LDAP server.
ldap:user_display_query	string	The LDAP query used to define which results are displayed when adding users to a group policy.
ldap:users:objects	string	The LDAP objectClasses that are considered valid users.
ldap:users:query	string	The LDAP query used to map a particular username to an LDAP user object.
ldap:users:search_base	string	The distinguishedName at which to start searching for users.
ldap:users:user_id	string	The set of LDAP attributes used to uniquely identify users in the LDAP server.
provider:id	string	The unique identifier of the provider to which this setting applies.
provider:name	string	The name of the provider to which this setting applies.
radius:host	string	The hostname of the RADIUS server.
radius:port	string	The port through which to connect to the RADIUS server.
radius:shared_secret	****	The shared secret to use in connecting to the RADIUS server.
radius:timeout	integer	The number of seconds allowed to elapse before the RADIUS server has timed out.
radius:users:mode	**all** **list**	The way users are matched to this provider. **All** handles any valid authentication attempt, and **list** handles only the specified list of users.
saml:email	string	The user attribute to use as the email address.
saml:groups:list	delimited string	The list of groups associated with the identity provider. The delimiter is set in the

Field	Value	Explanation
		user interface.
saml:groups:lookup	string	The name of the attribute that contains the names of groups to which users should belong.
saml:idp:cert	string	The identity provider's certificate. When you first create a SAML security provider, this value will be **metadata**. Once you have uploaded the identity provider's metadata, the value will appear in the form of **provider_cert.<provider_id>.server_cert.cert**.
saml:idp:entity_id	string	The unique identifier for the identity provider you are using.
saml:idp:login_url	string	The URL where you are automatically redirected to sign into BeyondTrust using SAML.
saml:idp:request_bind	string	Either **urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect** or **urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST**.
saml:name_id_format	string	Will always be **urn:oasis:names:tc:SAML:2.0:nameid-format:persistent**.
saml:sp:entity_id	string	The URL of your public site. This uniquely identifies the service provider.
saml:user_name	string	The user attribute to use as the username.
users:list	string	The list of users allowed to authenticate against this provider to access your BeyondTrust software.
sync_display_name	**1** or **0**	**1:** Every time a user logs in, their display name should be synchronized with the available remote information. **0:** A user's display name should be synchronized with the available remote information only the first time the user logs in.
scim:email	string	The user attribute to use as the email address.
scim:user_name	string	The user attribute to use as the username.
scim:private_display_name	string	The user attribute to use as the private display name.
scim:public_display_name	string	The user attribute to use as the public display name.
scim:vendor	string	The SCIM system being used for privileged identity management, such as SailPoint.
scim:users:query_id	id	The {id} element used for simple GET queries for users.
scim:group:query_id	id	The {id} element used for simple GET queries for groups.
scim:users:id_case_insensitive	**Enabled** **Disabled**	The attribute indicating whether the case is sensitive or insensitive. The value is **Disabled** by default.
scim:users:user_id	string	The set of SCIM attributes used to uniquely identify users.
scim:users:provision	boolean	Boolean denoting if the provisioning of a user is enforced.

Service Principal Fields

These fields apply to the **msgraph_http_recipient_added**, **msgraph_http_recipient_changed**, and **msgraph_http_recipient_removed** events.

Field	Value	Explanation
client_id	string	The client ID of this service principal.
disabled	**1** or **0**	**1:** Enable team chat history. **0:** Disable team chat history.
current_status	string	The last status of this service principal.
domain_name	string	The domain name of this service principal.
name	string	Internal descriptive name to easily identify the service principal.
tenant_id	string	The tenant ID of this service principal.

Session Policy Fields

These fields apply to the **session_policy_added**, **session_policy_changed**, and **session_policy_removed** events. Session policy events also include the "Support Permissions Fields" on page 67.

Field	Value	Explanation
code_name	string	The code name of this session policy.
description	string	The description of this session policy.
id	string	The unique identifier of this session policy.
name	string	The name of this session policy.

Setting Fields

These fields apply to the **setting_added** and **setting_changed** events.

Field	Value	Explanation
alert_interval	integer	The number of seconds between sending the last alert and sending another failure notification email, as long as failover synchronization has not yet occurred.
alerts:daily	**1** or **0**	**1:** Send a daily email notification to verify that communication is working correctly. **0:** No daily communications will be sent.
alerts:email	string	The list of email addresses to which to send email alerts.
api	**1** or **0**	**1:** The API is enabled. **0:** The API is disabled.
api:http	**1** or **0**	**1:** The API is enabled over HTTP. **0:** The API is enabled only over HTTPS.
auto	**1** or **0**	**1:** If the primary B Series Appliance goes down, automatic failover will occur. **0:** If the primary B Series Appliance goes down, automatic failover will not occur.
backup_enabled	**1** or **0**	**1:** Automatic data synchronization between a primary and a backup B Series Appliance is enabled. **0:** Automatic data synchronization is disabled.
bandwidth	integer	The maximum number of bytes per second that should be used for data synchronization between a primary and a backup B Series Appliance.
become_backup	none	Given when the failover role is changed to backup by a user.
become_primary	none	Given when the failover role is changed to primary by a user.
connection_test_ips	comma-delimited list	The list of IP addresses for the backup B Series Appliance to use to test network connectivity before failing over.
email:encryption	**none** **ssl** **tls**	The type of encryption used for the SMTP email server.
email:host	string	The SMTP server through which to send emails.
email:password	* * * *	Indicates if the password has changed. The actual string is never supplied.
email:port	integer	The SMTP server port through which to connect.
email:user	string	The username used to authenticate with the SMTP server.
external_key:crm_url	string	The URL configured to use in conjunction with the custom link button in the access console.

Field	Value	Explanation
file_store:listing	**1** or **0**	**1:** Show the file store at the /file directory. **0:** Do not allow web access to the file store.
ips	comma-delimited list	IP addresses shared between the primary B Series Appliance and the backup B Series Appliance.
localization:default_language	string	The default language for the site.
login_restrictions:list	string	A list of IPs which should be allowed or denied access to the **/login** and **/api** interfaces. This may also be combined with access console login restrictions.
login_restrictions:list_type	**allow_all** **allow_list** **deny_list**	Whether to allow all IP addresses, to allow only specified IP addresses, or to deny specified IP addresses access to the **/login** and **/api** interfaces of the B Series Appliance. This may also be combined with access console login restrictions.
login_restrictions:rep	**always** **first_authentication** **never**	Whether log into the access console is restricted to allowed networks every time, only the first time, or never.
login_restrictions:web	**always** **none**	Whether access to **/login**, **/api**, and the access console is restricted or not. This is combined with the other login restriction messages above.
login_ restrictions:web:ports:allow	string	A list of ports that are allowed to access the **/login** interface.
login_ restrictions:web:ports:deny	string	A list of ports that are not allowed to access the **/login** interface.
networks:list	string	A list of IP addresses which should be allowed or denied.
networks:type	**allow_all** **allow_list** **deny_list**	Whether to allow all IP addresses, to allow only specified IP addresses, or to deny specified IP addresses access to the /appliance administrative interface of the B Series Appliance.
outbound_event:email_retry_ duration	integer	The number of seconds between each email retry attempt.
p2p	**1** or **0**	**1:** Peer-to-peer connections are enabled. **0:** Peer-to-peer connections are disabled.
p2p_stunserver_address	**stun.bomgar.com** **undefined**	If the BeyondTrust hosted peer-to-peer server is used, the value is **stun.bomgar.com**. If the B Series Appliance is used, the value is **undefined**.
p2p_ui_state	**0**, **1**, or **2**	**0:** Peer-to-peer is disabled. **1:** The BeyondTrust hosted peer-to-peer server is being used. **2:** The B Series Appliance is being used as the peer-to-peer server.
ports:http	comma-delimited list	A list of ports that will respond to HTTP traffic.
ports:https	comma-delimited list	A list of ports that will respond to HTTPS traffic.

Field	Value	Explanation
ports:management:allowed	comma-delimited list	A list of ports that are allowed to access the /appliance interface.
ports:management:denied	comma-delimited list	A list of ports that are not allowed to access the /appliance interface.
ports:management:http	integer	The port to use when generating a URL that should be viewed over HTTP.
ports:management:https	integer	The port to use when generating a URL that should be viewed over HTTPS.
pre_login_agreement:enabled	**1** or **0**	**1:** The /login prerequisite login agreement has been enabled. **0:** The /login prerequisite login agreement has been disabled.
probe:max_timeout	integer	The number of seconds between the first failure to reach the primary B Series Appliance and fail over to the backup B Series Appliance.
relationship_broken	array of semicolon separated values	Generated when failover relationship is broken. Values: • this:hostname=hostname where entry is made • this:port=port used by current host • peer:hostname=hostname of peer in failover relationship • peer:port=port of peer in failover_relationship
relationship_established	array of semicolon separated values	Generated when failover is established. Values: • this:hostname=hostname where entry is made • this:port=port used by current host • peer:hostname=hostname of peer in failover relationship • peer:port=port of peer in failover_relationship
rep:custom_link	string	The URL that will appear as a button in the access console during a support session.
rep:dashboard:monitor	**disabled** **enabled:only_rep_console**	Whether team managers and leads are disallowed to monitor team members or are allowed to view team members' access consoles..
rep:dashboard:transfer	**1** or **0**	**1:** Allow team managers and team leads to take over team members' sessions. **0:** Do not allow transferring of team members' sessions.
rep:mobile	**1** or **0**	**1:** Mobile access consoles are allowed to connect. **0:** Mobile access consoles are not allowed to connect.
rep:history:enabled	**1** or **0**	**1:** Enable team chat history. **0:** Disable team chat history.
rep:history:hours	integer from 1 to 24	Hours of team chat history to replay.
rep:private_queue_exit_check	**1** or **0**	**1:** A user cannot log out or quit the access console until their personal

Field	Value	Explanation
		queue is empty. **0:** A user can log out or quit the access console with sessions still in their personal queue.
rep:saved_logins	**1** or **0**	**1:** Allow users to have the access console remember their credentials. **0:** Do not allow the access console to remember representatives' credentials.
rep_console_settings_applied	integer	An incrementing number indicating when managed access console settings have been applied to all representatives.
reporting:history_limit	integer	The number of days to keep logging information, expressed as seconds.
service.syslog.remote.format	**syslog** **bsd** **bsd_no_ts** **tls**	**syslog:** The syslog data format is RFC 5424 compliant. **bsd:** The syslog data format is legacy BSD format. **bsd_no_ts:** The syslog data format is legacy BSD format without timestamp. **tls:** The syslog data format is Syslog over TLS (RFC 5425).
ssl:certificate_verify	**1** or **0**	**1:** Validate the SSL certificate chain for security. **0:** Do not validate the SSL certificate chain.
support:clipboard_sync_mode	**disabled** **manual:rep_to_cust** **manual:both_directions** **auto:both_directions**	**disabled:** The user cannot synchronize the clipboards with the customer's clipboard during a support session. **manual:rep_to_cust:** The user can send the clipboard manually to the customer's clipboard during a session. **manual:both_directions:** The user can send the clipboard to the customer's clipboard during a session, and the customer can send their clipboard to the user manually. **auto:both_directions:** The clipboard is sent automatically from the user to the customer, and from the customer to the user.
support:inactive_rep:timeout	integer	The number of seconds with no session activity before a user is removed from a specific session.
support:jump_client:active_interval	integer	The number of seconds to wait between each Jump Client statistics update.
support:jump_client:allow_wake_on_lan	**1** or **0**	**1:** Users can attempt to wake up a Jump Client. **0:** Users cannot attempt to wake up Jump Clients.
support:jump_client:concurrent_upgrades	integer	The maximum number of Jump Clients whose statistics can be updated simultaneously.
support:jump_client:connection_type	**active** **passive**	The default client connection type for Jump Clients deployed in a session: **active** or **passive.**
support:jump_client:listening_port	integer	The default port that passive Jump Clients use to listen for requests to start a session on the customer systems.
support:jump_client:removal_behavior	**uninstalled** **remove**	**uninstalled:** A Jump Client deleted by an end user remains visible in the access console. **remove:** A Jump Client deleted by an end user is removed from the access console.

Field	Value	Explanation
support:jump_client:stats	comma-delimited list	The statistics to collect from each Jump Client. Currently recognized statistics include **pss_os** (operating system), **pss_ut** (uptime), **pss_cpu** (central processing unit usage), **pss_cu** (console user), **pss_fd** (disk usage), and **pss_tn** (screen thumbnail image).
support:jump_client:stats:active_interval	integer	The number of seconds to wait between active Jump Client statistics updates.
support:jump_client:ticket_system:ticket_id_sensitive	**1** or **0**	**1:** The ticket ID is treated as sensitive information. **0:** The ticket ID is not treated as sensitive information.
support:jump_item:simultaneous_jump_behavior	**join** **disallow**	**join:** Multiple users can Jump to the same Jump Item simultaneously. **disallow:** Only one user at a time can Jump to a Jump Item without an invitation from the first user to share the session.
support:jump_item:simultaneous_rdp_jump_behavior	**start** **disallow**	**start:** Multiple users can Jump to the same RDP Jump Item simultaneously. **disallow:** Only one user at a time can Jump to an RDP Jump Item without an invitation from the first user to share the session.
support:recordings:command_shell	**1** or **0**	**1:** Record a video of command shells. **0:** Do not record command shells.
support:recordings:command_shell:resolution	**320x240** **640x480** **800x600** **1024x768** **1280x1024**	The resolution selected to convert command shell recordings when viewing or downloading them.
support:recordings:screen_sharing	**1** or **0**	**1:** Record a video of screen sharing during sessions. **0:** Do not record sessions.
support:recordings:screen_sharing:resolution	**320x240** **640x480** **800x600** **1024x768** **1280x1024**	The resolution to which to convert session recordings when viewing or downloading.
support:recordings:show_my_screen	**1** or **0**	**1:** Record a video of Show My Screen sessions. **0:** Do not record Show My Screen sessions.
support:special_actions:builtins	**1** or **0**	**1:** Show the built-in special actions in support sessions. **0:** Hide the built-in special actions in support sessions.
support:system_info:auto_log	**1** or **0**	**1:** Automatically log the remote computer's system information at the beginning of a session. **0:** Do not log system information.
support:system_info:auto_log:mobile	**Standard** **Full**	**Standard:** Provide standard logging for mobile platforms. **Full:** Provide extended logging for mobile platforms. This option is the **Extended** dropdown option in the user interface.
sync_interval	**minute** **hour**	**minute**=Every x minutes **hour**=Every x hours

Field	Value	Explanation
	day **week**	**day**=Every day at x time **week**=Once a week at x day and y time.
sync_interval:days	integer from **1** to **7**	If sync_interval = **week**, it denotes the day of the week on which the auto data sync will occur. 1 = Sunday, 7 = Saturday.
sync_interval:hours	integer from **1** to **24**	If sync_interval = **week** or **day**, then this value tells the hour of the day that the data sync will run. If sync_interval = **hour**, then it tells how many hours will be between every data sync (Every x hours).
sync_interval:minutes	integer from **1** to **60**	If sync_interval = **week** or **day**, then this value tells the minute of the hour that the data sync will run. If sync_interval = **minute**, then it tells how many minutes will be between every data sync (Every x minutes).
syslog	string	The address of the remote syslog server to which to send messages.
system.auth.local.failed-login-lockout-duration	integer	The number of minutes an /appliance account is locked out after the maximum number of failed logins is exceeded. If **0**, the account is locked out until an administrator unlocks the account.
system.auth.local.failed-login-lockout-threshold	integer	The number of failed login attempts after which the /appliance user will be locked out of their account. If **0**, the user will never be locked out.
system.auth.local.password-expire-duration	integer	The number of days after which an /appliance user's password expires. If **0**, the password never expires.
system.auth.local.password-history-count	integer	The number of prior passwords that an /appliance user cannot use when changing their password. If **0**, there is no restriction.
system.pre-login-agreement.enabled	**1** or blank	**1:** The /appliance prerequisite login agreement has been enabled.
system.pre-login-agreement.text	string	The text of the login agreement that user must accept before accessing the /appliance administrative interface.
system.pre-login-agreement.title	string	The title of the login agreement that user must accept before accessing the /appliance administrative interface.
timezone	string	The time zone in which this B Series Appliance renders system times.
users:idle_timeout	integer	The maximum number of seconds a access console can be idle before that user will be logged out.
users:lockout_duration	integer	The length of time in minutes a locked-out user must wait before being allowed to reattempt login. **0** indicates that an admin must unlock the account.
users:max_failed_logins	integer	The number of failed login attempts after which the account will be locked out.
users:passwords:complex	**1** or **0**	**1:** Require complex passwords. **0:** Do not require complex passwords.
users:passwords:default_expiration	integer	The default number of days a password can be used before it expires and must be reset.

Field	Value	Explanation
users:passwords:minimum_ length	integer	The minimum number of characters required for a password.
users:passwords:reset	**1** or **0**	**1:** Users can reset forgotten passwords by correctly answering a security question. **0:** Users cannot reset forgotten passwords.
users:terminate_if_user_ logged_in	**1** or **0**	If a user attempts to log into the access console using an account that is already in use in another access console: **1:** Terminate the existing connection so that the new user can log in. **0:** Maintain the existing connection and do not allow the new user to log in.

Shared Jump Group Fields

These fields apply to the **shared_jump_group_added**, **shared_jump_group_changed**, and **shared_jump_group_removed** events.

Field	Value	Explanation
code_name	string	The code name of this Jump Group.
comments	string	Any comments associated with this Jump Group.
ecm_group	string	The ID of the ECM Group assigned to the group.
id	string	The unique identifier of the Jump Group.
name	string	The name of the Jump Group.

SNMP Fields

These fields apply to the **SNMP_changed** event.

Field	Value	Explanation
snmp_v2_ enabled	**1** or **0**	**1:** The B Series Appliance has SNMP_v2 Server enabled. **0:** The B Series Appliance has SNMP_v2 Server disabled.
snmp_v2_syslocation	string	The location of this B Series Appliance for the SNMP MIB.
snmp_v2_rocommunity	string	The community name the SNMPv2 Server should respond to.
snmp_v2_netACL	string	The list of IP addresses allowed to access SNMP on this B Series Appliance.

Support Permissions Fields

These fields apply to session policy and custom session policy events.

Field	Value	Explanation
support:permissions:allow_pinned_clients	**yes** **no**	Whether this session policy may be applied to Jump Clients or not.
support:permissions:allow_rep_invite	**yes** **no**	Whether this session policy may be applied to access invites or not.
support:permissions:allow_users	**yes** **no**	Whether this session policy may be applied to users or not.
support:permissions:canned_scripts	**allow** **deny** **not_defined**	Whether this policy's permission to run canned scripts is allowed, denied, or not defined.
support:permissions:command_shell	**allow** **deny** **not_defined**	Whether this policy's permission to use the command shell is allowed, denied, or not defined.
support:permissions:file_transfers:cust	**any_path** list of paths **not_defined**	Whether the user is allowed to access any path on the remote computer's file system for the purpose of file transfer, only specified paths, or not defined.
support:permissions:file_transfers:download	**allow** **deny** **not_defined**	Whether this policy's permission to download files using file transfer is allowed, denied, or not defined.
support:permissions:file_transfers:rep	**any_path** list of paths **not_defined**	Whether the user is allowed to access any path on their local file system for the purpose of file transfer, only specified paths, or not defined.
support:permissions:file_transfers:upload	**allow** **deny** **not_defined**	Whether this policy's permission to upload files using file transfer is allowed, denied, or not defined.
support:permissions:registry_access	**allow** **deny** **not_defined**	Whether this policy's permission to access the remote registry editor is allowed, denied, or not defined.
support:permissions:screen_sharing	**view_and_control** **view_only** **not_allowed** **not_defined**	Whether this policy's permission to screen share allows view and control, allows view only, is denied, or is not defined.
support:permissions:screen_ sharing:annotations	**allow** **deny** **not_defined**	Whether this policy's permission to use annotations is allowed, denied, or not defined.
support:permissions:screen_ sharing:privacy_mode	**input_only** **privacy_screen,input**	Whether this policy's allowed customer restrictions are set to mouse and keyboard only; display, mouse, and

Field	Value	Explanation
	none **not_defined**	keyboard; none; or not defined.
support:permissions:system_info	**allow** **deny** **not_defined**	Whether this policy's system information permission is set to allowed, denied, or not defined.
support:permissions:system_info:actions	**allow** **deny** **not_defined**	Whether this policy's system information actions permission is set to allowed, denied, or not defined.

Support Team Fields

These fields apply to the **support_team_added**, **support_team_changed**, and **support_team_removed** events.

Field	Value	Explanation
code_name	string	The code name of this team.
comments	string	Any comments associated with this team.
id	string	The unique identifier of the team.
name	string	The name of the team.

Support Team Member Fields

These fields apply to the **support_team_member_added**, **support_team_member_changed**, and **support_team_member_removed** events.

Field	Value	Explanation
role	**member** **lead** **manager**	The role this user plays in the team.
team:id	string	The unique identifier of the team to which this user belongs.
team:name	string	The name of the team to which this user belongs.
user:id	string	The unique identifier of the user being added to or removed from this team.
user:username	string	The name of the user being added to or removed from this team.

Syslog Server Fields

These fields apply to the **syslog_server_changed** event.

Field	Value	Explanation
message_format	**RFC 5424 compliant** **Legacy BSD format** **Legacy BSD format without timestamp** **Syslog over TLS (RFC 5425)**	The data format for syslog event notification messages.
syslog_servers	comma-delimited list	A list of IP addresses that receive syslog messages from this B Series Appliance.

User Account Report Generated Fields

These fields apply to the **user_account_report_generated** event.

Field	Value	Explanation
report_type	**all** **local** **security_provider**	Whether the downloaded report was for all users, only local users, or only a security provider.

/appliance User Fields

These fields apply to the **user_added**, **user_changed**, and **user_removed** events. These fields apply to users added to the /appliance interface.

Field	Value	Explanation
displayname	string	The display name of this user.
failed_login_attempts	integer	The number of consecutive failed attempts to log into this account.
lockout_release	date or **0**	The readable date and time that an administrator reset the number of failed login attempts back to zero. **0** indicates that the number of failed login attempts has not just been reset.
password	* * * *	Indicates if the user's password has been changed.
password_changed_date	date	The readable date and time that the password was last changed.
password_force_reset	**1** or **0**	**1:** The user must create a new password upon next login. **0:** The password need not be changed.
username	string	The username the user last used to authenticate to the BeyondTrust /appliance interface. Not necessarily unique.

/login User Fields

These fields apply to the **user_added, user_changed**, and **user_removed** events. User events also include the "Permission Fields" on page 44. These fields apply to users added to the /login interface.

Field	Value	Explanation
account:created	Unix timestamp	The date and time this user account was created.
account:disabled	**1** or **0**	**1:** This local user account is disabled. **0:** This local user account is active.
account:email:address	string	The email address set for notifications.
account:email:locale	string	Values are the language abbreviations (e.g. en-us for English) used with emails.
account:expiration	Unix timestamp or **never**	The date and time this local user account will expire, if ever.
account:failed_logins	integer	The number of consecutive failed attempts to log into this local account.
comments	string	Any comments associated with this user.
external_id	string	An internal representation of a remote user's identifying information, such as an LDAP attribute, RADIUS username, or Kerberos principal name.
id	string	The unique identifier for this user.
idle_timeout	integer or **site_wide_setting**	The maximum number of seconds this representative can be idle within the access console before being logged out. The **site_wide_setting** option defaults to the timeout set on the **Management > Security** page. If no timeout, uses **none**.
login_code:enabled	**1** or **0**	**1:** The user must enter an emailed login code to log in. **0:** The user may log in without an emailed login code.
login_schedule:enabled	**1** or **0**	**1:** The user is disallowed to log into the access console outside of the set schedule. **0:** The user may log into the access console at any time.
login_schedule:force_logout	**1** or **0**	**1:** The user is automatically logged out of the access console at the end of the scheduled time. **0:** The user is not forced to log out of the access console at the end of the scheduled time.
login_schedule:timezone	string	The timezone for which the login schedule is set.
password	* * * *	Indicates if the local user's password has been changed by an administrator.
password:expiration	Unix timestamp	The date and time the local user's password will expire, if ever.
password:reset	**1** or **0**	**1:** The local user must create a new password upon next login. **0:** The password need not be changed.
password:will_expire	**1** or **0**	**1:** The local user's password is set to expire on a certain date.

Field	Value	Explanation
		0: The local user's password has no expiration set.
provider:id	string	The unique identifier of the security provider against which this user last authenticated, or **1** for a local user.
provider:name	string	The name of the security provider against which this user last authenticated.
security_answer	* * * *	Indicates if the local user's security answer was changed by an administrator.
security_question	string	The security question the local user can answer to reset their password.
two_factor_auth:required	**1** or **0**	**1:** This user is required to use two-factor authentication. **0:** This user is not required to use two-factor authentication.
username	string	The username the user last used to authenticate to BeyondTrust. Not necessarily unique.

User Session Policy Fields

These fields apply to the **user_session_policy_added** and **user_session_policy_removed** events.

Field	Value	Explanation
session_policy:name	string	The name of the session policy associated with this user.
user:id	string	The unique identifier of the user with whom the session policy is associated.
user:username	string	The username of the user with whom the session policy is associated.

Vault Account Password Rotation Fields

These fields apply to the **vault_account_password_rotation** event.

Field	Value	Explanation
reason	string	The reason for the rotation.
status	success failure	Whether the rotation attempt succeeded or failed.
account	string	The account username rotated.

Windows Service Fields

These fields apply to the **windows_service_removed** and **windows_service_changed** events.

Field	Value	Explanation
account_id	number	The unique identifier of the account.
display_name	string	The display name of the Windows service.
endpoint_id	number	The unique identifier of the endpoint.
name	string	The name of the Windows service.
restart_on_rotation	**1** or **0**	**1:** Enables the automatic rotation for this account. **0:** Disables the automatic rotation for this account.