OSIRIUM PAM CEF SPECIFICATION VERSION 8.0.19±G205D2C34

This document details a list of events that Osirium PAM can emit in Common Event Format (CEF) over the syslog protocol (see RFC3164). CEF is a standard in security event management that aids the interoperability of infrastructure devices by aggregating the logging output of different network devices and applications. As such, processing and analysing logged data can be streamlined, providing efficient access to semantically structured event data using a SIEM (Security Information and Event Management) approach.

---

account_updated

An account configuration has been updated on Osirium PAM

deviceAction — Always

The update action performed on the account

destinationUserName — Always

The account on the target device to which the event relates

authenticationServiceName *(as deviceCustomString4)* — When Available

The name of the authentication service associated with the account

sourceUserName — When Available

The username of the platform user who initiated the action

sourceUserDisplayName *(as deviceCustomString2)* — When Available

The human-readable name of the platform user who initiated the action

destinationHostName — When Available

The address of the device relating to the event

oldState *(as deviceCustomString6)* — When Available

The previous state of the account

destinationName *(as deviceCustomString1)* — When Available

The name of the device relating to the event

newState *(as deviceCustomString5)* — When Available

The new state of the account

---

cluster_health

Osirium PAM cluster health status

eventOutcome — Always

message — When Available

Full cluster health report in JSON format

device_account_created

New account created on device

destinationHostName — Always
The address of the device relating to the event

destinationUserName — Always
The account on the target device to which the event relates

destinationName *(as deviceCustomString1)* — Always
The name of the device relating to the event

---

device_account_deleted

Account deleted on device

destinationHostName — Always
The address of the device relating to the event

destinationUserName — Always
The account on the target device to which the event relates

destinationName *(as deviceCustomString1)* — Always
The name of the device relating to the event

---

device_account_discovered

Discovered new unapproved account on device

destinationHostName — Always
The address of the device relating to the event

destinationUserName — Always
The account on the target device to which the event relates

destinationName *(as deviceCustomString1)* — Always
The name of the device relating to the event

---

device_fingerprint_added

Added device fingerprint

port *(as deviceCustomString1)* — Always
Device port

fingerprint *(as deviceCustomString2)* — Always
Fingerprint

destinationHostName — Always
Device address

applicationProtocol — Always
The protocol used to communicate with the device

isApproved *(as deviceCustomString3)* — Always
State of fingerprint approval

---

device_fingerprint_removed

Removed device fingerprint

port *(as deviceCustomString1)* — Always

Device port

applicationProtocol — Always

The protocol used to communicate with the device

destinationHostName — Always

Device address

---

device_parameter_changed

Changed device parameter

toValue *(as deviceCustomString6)* — Always

The new value of the parameter

destinationName *(as deviceCustomString1)* — Always

The name of the device relating to the event

destinationHostName — Always

The address of the device relating to the event

parameterName *(as deviceCustomString4)* — Always

The name of the parameter that was changed

fromValue *(as deviceCustomString5)* — When Available

The old value of the parameter

---

disk_capacity

Disk capacity checked.

disk_display_name *(as deviceCustomString1)* — Always

The human-readable name of the disk which was checked

capacity *(as deviceCustomNumber1)* — Always

The percentage of the disk which is used

---

error

An error has occured

message — Always

A message describing the error

sourceUserName — When Available

The username of the platform user who initiated the action

sourceUserDisplayName *(as deviceCustomString2)* — When Available

The human-readable name of the platform user who initiated the action

---

failed_to_generate_fingerprint

Could not generate fingerprint

port *(as deviceCustomString1)* — Always
Device port

destinationHostName — Always
Device address

applicationProtocol — Always
The protocol used to communicate with the device

reason *(as deviceCustomString2)* — Always
Reason

aborting *(as deviceCustomString3)* — Always
Aborting

---

failed_to_generate_fingerprint_log_only

Could not generate fingerprint but behaviour is log only

port *(as deviceCustomString1)* — Always
Device port

destinationHostName — Always
Device address

applicationProtocol — Always
The protocol used to communicate with the device

reason *(as deviceCustomString2)* — Always
Reason

aborting *(as deviceCustomString3)* — Always
Aborting

---

failed_to_generate_fingerprint_non_default_tool

Could not generate fingerprint but non-default tool for device

port *(as deviceCustomString1)* — Always
Device port

destinationHostName — Always
Device address

applicationProtocol — Always
The protocol used to communicate with the device

reason *(as deviceCustomString2)* — Always
Reason

aborting *(as deviceCustomString3)* — Always
Aborting

fingerprint_verification_failure

Blocking connection. Fingerprint verification failed

port *(as deviceCustomString1)* Always
Device port

fingerprint *(as deviceCustomString2)* Always
Fingerprint

connecting *(as deviceCustomString3)* Always
Connecting

destinationHostName Always
Device address

applicationProtocol Always
The protocol used to communicate with the device

---

fingerprint_verification_failure_log_only

Allowing connection. Fingerprint verification failed but behaviour is log only

port *(as deviceCustomString1)* Always
Device port

fingerprint *(as deviceCustomString2)* Always
Fingerprint

connecting *(as deviceCustomString3)* Always
Connecting

destinationHostName Always
Device address

applicationProtocol Always
The protocol used to communicate with the device

---

fingerprint_verification_success

Allowing connection. Fingerprint verification succeeded

port *(as deviceCustomString1)* Always
Device port

fingerprint *(as deviceCustomString2)* Always
Fingerprint

connecting *(as deviceCustomString3)* Always
Connecting

destinationHostName Always
Device address

applicationProtocol Always
The protocol used to communicate with the device

long_running_connection_to_device

A user has been connected to a device for a long time

roleName *(as deviceCustomString5)* — Always
The name of the role in which the user connected to the device

applicationProtocol — Always
The protocol used to communicate with the device

sourceUserName — Always
The username of the platform user who initiated the action

changeTicketNames *(as deviceCustomString6)* — Always
The names of any change tickets associated with the connection

destinationUserName — Always
The account on the target device to which the event relates

channelToken *(as deviceCustomString4)* — Always
An arbitrary identifier useful for correlating events pertaining to this connection

destinationName *(as deviceCustomString1)* — Always
The name of the device relating to the event

duration *(as deviceCustomString3)* — Always
The length of time the user has been connected that is now considered to be "long"

sourceAddress — Always
The address from which the user connected to the device

destinationHostName — When Available
The address of the device relating to the event

MAPToolName *(as deviceCustomString2)* — When Available
The name of the MAP tool used

---

password_viewed_on_console

A password was revealed on the break-glass console

destinationHostName — Always
The address of the device relating to the event

destinationUserName — Always
The account on the target device to which the event relates

destinationName *(as deviceCustomString1)* — Always
The name of the device relating to the event

---

session_terminated_by_cluster

An administrator terminated a session

sessionID *(as deviceCustomString1)* — Always
The session which was terminated

nodeID *(as deviceCustomString3)* — Always
The node name on which the event triggering the termination originated

---

session_terminated_locally

An administrator terminated a session

sourceUserName — Always

The username of the platform user who initiated the action

sessionID *(as deviceCustomString1)* — Always

The session which was terminated

sourceUserDisplayName *(as deviceCustomString2)* — Always

The human-readable name of the platform user who initiated the action

---

task_finished

An automated task was completed

sourceUserName — Always

The username of the platform user who initiated the action

destinationName *(as deviceCustomString1)* — Always

The name of the device relating to the event

sourceUserDisplayName *(as deviceCustomString2)* — Always

The human-readable name of the platform user who initiated the action

destinationHostName — Always

The address of the device relating to the event

eventOutcome — Always

The success/failure status of the action

taskName *(as deviceCustomString6)* — When Available

The name assigned to the task that completed

task_queued

A task was queued to run

destinationHostName — Always
The address of the device relating to the event

destinationName *(as deviceCustomString1)* — Always
The name of the device relating to the event

taskName *(as deviceCustomString6)* — Always
The name assigned to the queued task

sourceUserName — When Available
The username of the platform user who initiated the action

sourceUserDisplayName *(as deviceCustomString2)* — When Available
The human-readable name of the platform user who initiated the action

destinationUserName — When Available
A argument required for logging when a "ad_account_password_changed" task is ran

domain *(as deviceCustomString3)* — When Available
A argument required for logging when a "ad_account_password_changed" task is ran

---

user_acquired_change_ticket

A user acquired a change ticket

destinationUserName — Always
The user who has been associated with the change ticket

sourceUserName — Always
The username of the platform user who initiated the action

changeTicketName *(as deviceCustomString6)* — Always
The name of the change ticket acquired by the user

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

---

user_associated_change_ticket_with_connection

A user associated a change ticket with a connection

externalId — Always
The arbitrary identifier of the connection associated with the change ticket

sourceUserName — Always
The username of the platform user who initiated the action

changeTicketName *(as deviceCustomString6)* — Always
The name of the change ticket associated with the connection

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

user_cloned_user

A user created new user by copying portions of an existing user

clonedUserName *(as deviceCustomString2)* — Always

The username of the user from which the new user was derived

sourceUserName — Always

The username of the platform user who initiated the action

destinationUserName — Always

The username of the new user

enabled *(as deviceCustomString5)* — When Available

Whether the new user is enabled

emailAddress *(as deviceCustomString3)* — When Available

The email address of the new user

authenticationType *(as deviceCustomString6)* — When Available

The authentication type of the new user

expiresAt *(as deviceCustomString4)* — When Available

When the new user account is set to expire

---

user_commented_on_change_ticket

A user commented on a change ticket

changeTicketName *(as deviceCustomString6)* — Always

The name of the change ticket on which the user commented

sourceUserName — Always

The username of the platform user who initiated the action

sourceUserDisplayName *(as deviceCustomString2)* — Always

The human-readable name of the platform user who initiated the action

comment *(as deviceCustomString1)* — When Available

The comment the user made on the change ticket

user_connected_to_device

A user connected to a device using Osirium PAM

roleName *(as deviceCustomString5)* — Always

The name of the role in which the user connected to the device

applicationProtocol — Always

The protocol used to communicate with the device

sourceUserName — Always

The username of the platform user who initiated the action

changeTicketNames *(as deviceCustomString6)* — Always

The names of any change tickets associated with the connection

destinationUserName — Always

The account on the target device to which the event relates

channelToken *(as deviceCustomString4)* — Always

An arbitrary identifier useful for correlating events pertaining to this connection

destinationName *(as deviceCustomString1)* — Always

The name of the device relating to the event

sourceAddress — Always

The address from which the user connected to the device

destinationHostName — When Available

The address of the device relating to the event

MAPToolName *(as deviceCustomString2)* — When Available

The name of the MAP tool used

---

user_created_access_request

A user created a new device access request

sourceUserName — Always

The username of the user who made the request

from *(as deviceCustomDate1)* — Always

Human-readable date string that denotes when the access request is valid from

destinationHostName — Always

The address of the device relating to the event

destinationName *(as deviceCustomString1)* — Always

The name of the device relating to the event

until *(as deviceCustomDate2)* — Always

Human-readable date string that denotes when the access request is valid until

toolName *(as deviceCustomString3)* — When Available

The human-readable name of the tool relating to the event

taskName *(as deviceProcessName)* — When Available

The name of the task the user wants to run

message — When Available

The reason for requesting access

destinationUserName — When Available

The account on the target device to which the event relates

---

user_created_account_mapping_pattern

A user created a new account mapping pattern

name *(as deviceCustomString5)* — Always

The newly created account mapping name

sourceUserName — Always

The username of the platform user who initiated the action

pattern *(as deviceCustomString6)* — Always

The newly created account mapping pattern

sourceUserDisplayName *(as deviceCustomString2)* — Always

The human-readable name of the platform user who initiated the action

---

user_created_auth_service

A user created an authentication service

authenticationServiceName *(as deviceCustomString6)* — Always

The name of the authentication service

sourceUserName — Always

The username of the platform user who initiated the action

sourceUserDisplayName *(as deviceCustomString2)* — Always

The human-readable name of the platform user who initiated the action

---

user_created_file

A user created a file stored on Osirium PAM

sourceUserName — Always

The username of the platform user who initiated the action

sourceUserDisplayName *(as deviceCustomString2)* — Always

The human-readable name of the platform user who initiated the action

destinationHostName — When Available

The address of the device relating to the event

destinationName *(as deviceCustomString1)* — When Available

The name of the device relating to the event

user_created_user

A user created a new user on Osirium PAM

destinationUserName — Always
The username of the new user

sourceUserName — Always
The username of the platform user who initiated the action

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

emailAddress *(as deviceCustomString3)* — When Available
The email address of the new user

expiresAt *(as deviceCustomString4)* — When Available
When the new user account is set to expire

enabled *(as deviceCustomString5)* — When Available
Whether the new user is enabled

authenticationType *(as deviceCustomString6)* — When Available
The authentication type of the new user

---

user_created_user_group

A user created a new user group

sourceUserName — Always
The username of the platform user who initiated the action

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

userGroupName *(as deviceCustomString6)* — Always
The name of the new user group

userNames *(as deviceCustomString5)* — Always
The usernames of the users in the new user group

---

user_delete_fingerprint_failed

A user failed to delete a fingerprint

sourceUserName — Always
The username of the platform user who initiated the action

fingerprintId *(as deviceCustomString4)* — Always
Fingerprint id

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

user_deleted_account_mapping_pattern

A user deleted an account mapping pattern

name *(as deviceCustomString5)* — Always
The account mapping name that was deleted

sourceUserName — Always
The username of the platform user who initiated the action

pattern *(as deviceCustomString6)* — Always
The account mapping pattern that was deleted

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

---

user_deleted_auth_service

A user deleted an authentication service

authenticationServiceName *(as deviceCustomString6)* — Always
The name of the authentication service

sourceUserName — Always
The username of the platform user who initiated the action

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

---

user_deleted_file

A user deleted a file stored on Osirium PAM

filePath — Always
The full path of the file that was deleted, including the file name

sourceUserName — Always
The username of the platform user who initiated the action

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

destinationHostName — When Available
The address of the device relating to the event

destinationName *(as deviceCustomString1)* — When Available
The name of the device relating to the event

user_deleted_fingerprint

A user deleted a fingerprint

fingerprint *(as deviceCustomString5)* — Always

Deleted fingerprint

sourceUserName — Always

The username of the platform user who initiated the action

fingerprintId *(as deviceCustomString4)* — Always

Fingerprint id

toolName *(as deviceCustomString3)* — Always

The human-readable name of the tool relating to the event

---

user_deleted_user

A user deleted a user from Osirium PAM

destinationUserName — Always

The username of the user that was deleted

sourceUserName — Always

The username of the platform user who initiated the action

sourceUserDisplayName *(as deviceCustomString2)* — Always

The human-readable name of the platform user who initiated the action

---

user_deleted_user_group

A user deleted a user group

userGroupName *(as deviceCustomString6)* — Always

The name of the deleted user group

sourceUserName — Always

The username of the platform user who initiated the action

sourceUserDisplayName *(as deviceCustomString2)* — Always

The human-readable name of the platform user who initiated the action

user_disconnected_from_device

A user disconnected from a device

roleName *(as deviceCustomString5)* — Always
The name of the role in which the user connected to the device

applicationProtocol — Always
The protocol used to communicate with the device

sourceUserName — Always
The username of the platform user who initiated the action

changeTicketNames *(as deviceCustomString6)* — Always
The names of any change tickets associated with the connection

destinationUserName — Always
The account on the target device to which the event relates

channelToken *(as deviceCustomString4)* — Always
An arbitrary identifier useful for correlating events pertaining to this connection

destinationName *(as deviceCustomString1)* — Always
The name of the device relating to the event

sourceAddress — Always
The address from which the user connected to the device

destinationHostName — When Available
The address of the device relating to the event

MAPToolName *(as deviceCustomString2)* — When Available
The name of the MAP tool used

duration *(as deviceCustomString3)* — When Available
The length of time that the user was connected

---

user_downloaded_breakglass_document

A user downloaded the breakglass document

sourceUserName — Always
The username of the platform user who initiated the action

---

user_executed_troubleshooting_script

A user executed a troubleshooting script on the PAM Server Console

sourceUserName — Always
The username of the platform user who initiated the action

scriptArguments *(as deviceCustomString6)* — Always
The arguments passed to the script

filename — Always
The name of the script that was executed on the console

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

---

user_failed_login_odc

A user failed to log in to Osirium PAM

destinationName *(as deviceCustomString1)* — Always
The name of the device relating to the event

sourceUserName — Always
The username of the platform user who initiated the action

destinationUserName — Always
The account on the target device to which the event relates

destinationHostName — Always
The address of the device relating to the event

sourceAddress — Always
The address from which the client attempted to connect

message — When Available
An error message about why the login attempt failed

---

user_failed_to_update_device_password

A user failed to update the password on a device

sourceUserName — Always
The username of the platform user who initiated the action

destinationName *(as deviceCustomString1)* — Always
The name of the device relating to the event

destinationUserName — Always
The account on the target device to which the event relates

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

destinationHostName — Always
The address of the device relating to the event

Reason — Always
The reason the password update did not proceed

user_forced_secrets_refresh

A user forced a password refresh for an account

sourceUserName — Always
The username of the platform user who initiated the action

destinationUserName — Always
The account on the target device to which the event relates

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

destinationHostName — When Available
The address of the device relating to the event

authenticationServiceName *(as deviceCustomString6)* — When Available
The authentication service to which the account belongs

destinationName *(as deviceCustomString1)* — When Available
The name of the device relating to the event

---

user_locked_device_account

A user locked an account on a device

sourceUserName — Always
The username of the platform user who initiated the action

destinationUserName — Always
The account on the target device to which the event relates

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

---

user_logged_in_odc

A user logged in to Osirium PAM

destinationName *(as deviceCustomString1)* — Always
The name of the device relating to the event

sourceUserName — Always
The username of the platform user who initiated the action

destinationUserName — Always
The account on the target device to which the event relates

destinationHostName — Always
The address of the device relating to the event

sourceAddress — Always
The address from which the client connected

user_logged_out_odc

A user logged out from Osirium PAM

sourceAddress — Always

The address from which the client was connected

sourceUserName — Always

The username of the platform user who initiated the action

destinationName *(as deviceCustomString1)* — Always

The name of the device relating to the event

destinationUserName — Always

The account on the target device to which the event relates

sourceUserDisplayName *(as deviceCustomString2)* — Always

The human-readable name of the platform user who initiated the action

destinationHostName — Always

The address of the device relating to the event

---

user_login_response_required

A user must respond to log in to Osirium PAM

destinationName *(as deviceCustomString1)* — Always

The name of the device relating to the event

sourceUserName — Always

The username of the platform user who initiated the action

destinationUserName — Always

The account on the target device to which the event relates

destinationHostName — Always

The address of the device relating to the event

sourceAddress — Always

The address from which the client connected

user_migrated_device_to_new_template

A user migrated a device to use a new template

newTemplateName *(as deviceCustomString4)* — Always

The name of the device template that will now be used to handle the device configuration and interactions

sourceUserName — Always

The username of the platform user who initiated the action

destinationHostName — Always

The address of the device relating to the event

oldTemplateName *(as deviceCustomString2)* — Always

The name of the device template that was used to handle the device configuration and interactions

templateVendor *(as deviceCustomString6)* — Always

The vendor of the device that the template is targetting

destinationName *(as deviceCustomString1)* — Always

The name of the device relating to the event

newTemplateVersion *(as deviceCustomString5)* — Always

The version of the device templated that will now be used to handle the device configuration and interactions

oldTemplateVersion *(as deviceCustomString3)* — Always

The version of the device templated that was used to handle the device configuration and interactions

---

user_provisioned_device

A user provisioned a device

sourceUserName — Always

The username of the platform user who initiated the action

templateName *(as deviceCustomString4)* — Always

The name of the device template used to handle the device configuration and interactions

sourceUserDisplayName *(as deviceCustomString2)* — Always

The human-readable name of the platform user who initiated the action

destinationHostName — Always

The address of the device relating to the event

templateVersion *(as deviceCustomString5)* — Always

The version of the device templated used to handle the device configuration and interactions

templateVendor *(as deviceCustomString6)* — Always

The vendor of the device that the template is targetting

destinationName *(as deviceCustomString1)* — Always

The name of the device relating to the event

authServiceName *(as deviceCustomString3)* — When Available

The human-readable name of the auth service the device was provisioned with

user_read_device_file

A user read the contents of a file on a device

filePath — Always
The full path on the device of the file that was read

sourceUserName — Always
The username of the platform user who initiated the action

destinationName *(as deviceCustomString1)* — Always
The name of the device relating to the event

destinationUserName — Always
The account on the target device to which the event relates

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

destinationHostName — Always
The address of the device relating to the event

---

user_released_change_ticket

A user released a change ticket

changeTicketName *(as deviceCustomString6)* — Always
The name of the change ticket released by the user

sourceUserName — Always
The username of the platform user who initiated the action

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

destinationUserName — When Available
The username of the user who was associated with the change ticket

---

user_requested_profile_deletion

A user requested the deletion of a profile

sourceUserName — Always
The username of the platform user who initiated the action

profileName *(as deviceCustomString6)* — Always
The name of the profile to be deleted

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

user_responded_to_access_request

A user responded to a device access request

sourceUserName — Always
The username of the platform user who initiated the action

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

destinationHostName — Always
The address of the device relating to the event

from *(as deviceCustomDate1)* — Always
Human-readable date string that denotes when the access request is valid from

requesterUserDisplayName *(as deviceCustomString3)* — Always
The display name of the user who made the request

requesterUserName *(as deviceCustomString4)* — Always
The username of the user who made the request

response *(as deviceCustomString6)* — Always
The response the user gave to the access request

destinationName *(as deviceCustomString1)* — Always
The name of the device relating to the event

until *(as deviceCustomDate2)* — Always
Human-readable date string that denotes when the access request is valid until

destinationUserName — When Available
The account on the target device to which the event relates

taskName *(as deviceProcessName)* — When Available
The name of the task the user wants to run

toolName *(as deviceCustomString5)* — When Available
The human-readable name of the tool relating to the event

---

user_revealed_secrets

A user revealed the secrets for an account

sourceUserName — Always
The username of the platform user who initiated the action

destinationUserName — Always
The account on the target device to which the event relates

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

destinationHostName — When Available
The address of the device relating to the event

authenticationServiceName *(as deviceCustomString6)* — When Available
The authentication service to which the account belongs

destinationName *(as deviceCustomString1)* — When Available
The name of the device relating to the event

user_revealed_secrets_history

A user revealed the secrets history for an account

sourceUserName — Always
The username of the platform user who initiated the action

numberRevealed *(as deviceCustomNumber1)* — Always
The number of historical secrets that were revealed

destinationUserName — Always
The account on the target device to which the event relates

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

destinationHostName — When Available
The address of the device relating to the event

authenticationServiceName *(as deviceCustomString6)* — When Available
The authentication service to which the account belongs

destinationName *(as deviceCustomString1)* — When Available
The name of the device relating to the event

---

user_rolled_back_device_passwords

A user rolled back the passwords on a device

sourceUserName — Always
The username of the platform user who initiated the action

destinationName *(as deviceCustomString1)* — Always
The name of the device relating to the event

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

destinationHostName — Always
The address of the device relating to the event

---

user_started_deleting_auth_service

A user triggered the deletion and cleanup of an authentication service

forced *(as deviceCustomString5)* — Always
Whether the deletion was forced

sourceUserName — Always
The username of the platform user who initiated the action

authenticationServiceName *(as deviceCustomString6)* — Always
The name of the authentication service being deleted

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

user_started_deleting_user

A user initiated the deletion of another user on Osirium PAM

destinationUserName — Always

The name of the user being deleted

sourceUserName — Always

The username of the platform user who initiated the action

droppedActiveConnetions *(as deviceCustomString6)* — Always

Whether Osirium PAM dropped active connections from the user in order to initiate the deletion

sourceUserDisplayName *(as deviceCustomString2)* — Always

The human-readable name of the platform user who initiated the action

---

user_unlocked_device_account

A user unlocked an account on a device

sourceUserName — Always

The username of the platform user who initiated the action

destinationUserName — Always

The account on the target device to which the event relates

sourceUserDisplayName *(as deviceCustomString2)* — Always

The human-readable name of the platform user who initiated the action

---

user_unprovisioned_device

A user unprovisioned a device

sourceUserName — Always

The username of the platform user who initiated the action

destinationName *(as deviceCustomString1)* — Always

The name of the device relating to the event

sourceUserDisplayName *(as deviceCustomString2)* — Always

The human-readable name of the platform user who initiated the action

destinationHostName — Always

The address of the device relating to the event

forced *(as deviceCustomString6)* — Always

Whether the device was forcibly unprovisioned

user_update_fingerprint_failed

A user failed to update a connection fingerprint

newIsApproved *(as deviceCustomString4)* — Always
New state of fingerprint approval

fingerprintId *(as deviceCustomString5)* — Always
Fingerprint id

sourceUserName — Always
The username of the platform user who initiated the action

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

---

user_updated_account_mapping_pattern

A user updated an account mapping pattern

name *(as deviceCustomString5)* — Always
The account mapping name that was updated

pattern *(as deviceCustomString6)* — Always
The account mapping pattern that was updated

sourceUserName — Always
The username of the platform user who initiated the action

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

---

user_updated_device_file

A user performed an action that changed a file on a device

sourceUserName — Always
The username of the platform user who initiated the action

destinationUserName — Always
The account on the target device to which the event relates

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

destinationHostName — Always
The address of the device relating to the event

filePath — Always
The full path on the device of the file that was updated

deviceAction — Always
The action (append, overwrite, delete) that was taken by the user

destinationName *(as deviceCustomString1)* — Always
The name of the device relating to the event

user_updated_device_secret

A user updated device credentials

sourceUserName — Always
The username of the platform user who initiated the action

destinationName *(as deviceCustomString1)* — Always
The name of the device relating to the event

destinationUserName — Always
The account on the target device to which the event relates

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

destinationHostName — Always
The address of the device relating to the event

---

user_updated_fingerprint

A user updated a connection fingerprint

fingerprint *(as deviceCustomString5)* — Always
Fingerprint

sourceUserName — Always
The username of the platform user who initiated the action

newIsApproved *(as deviceCustomString4)* — Always
New state of fingerprint approval

oldIsApproved *(as deviceCustomString3)* — Always
Old state of fingerprint approval

---

user_updated_personal_secrets

A user updated the secrets record for a personal account

sourceUserName — Always
The username of the platform user who initiated the action

destinationUserName — Always
The account on the target device to which the event relates

sourceUserDisplayName *(as deviceCustomString2)* — Always
The human-readable name of the platform user who initiated the action

destinationHostName — When Available
The address of the device relating to the event

authenticationServiceName *(as deviceCustomString6)* — When Available
The authentication service to which the account belongs

destinationName *(as deviceCustomString1)* — When Available
The name of the device relating to the event

user_updated_profile_memberships

A user updated the memberships of a profile

sourceUserName — Always

The username of the platform user who initiated the action

sourceUserDisplayName *(as deviceCustomString2)* — Always

The human-readable name of the platform user who initiated the action

profileName *(as deviceCustomString6)* — Always

The name of the profile for which the users were changed

entityType *(as deviceCustomString5)* — Always

The type of entity (user, user_group, approver, approver_group, device, tool, task) added to or removed from the profile

removedEntityNames *(as deviceCustomString3)* — When Available

The names of the entities of the sepcified type removed from the profile

addedEntityNames *(as deviceCustomString4)* — When Available

The names of the entities of the specified type added to the profile

---

user_updated_user_group

A user updated a user group

userGroupName *(as deviceCustomString6)* — Always

The name of the updated user group

sourceUserName — Always

The username of the platform user who initiated the action

removedUserNames *(as deviceCustomString2)* — When Available

The names of the users who were removed from the group

enabled_status *(as deviceCustomString1)* — When Available

Whether the user group is now enabled

oldUserGroupName *(as deviceCustomString5)* — When Available

The previous name of the user group if it has been changed

addedUserNames *(as deviceCustomString3)* — When Available

The names of the users who were added to the group