

OSIRIUM PAM CEF SPECIFICATION

VERSION 9.0.12±GA9816029



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

destinationUserName Always

The account on the target device to which the event relates

deviceAction Always

The update action performed on the account

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

sourceUserDisplayName (*as deviceCustomString2*) When Available

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

authenticationServiceName (*as deviceCustomString4*) When Available

The name of the authentication service associated with the account

newState (*as deviceCustomString5*) When Available

The new state of the account

oldState (*as deviceCustomString6*) When Available

The previous state of the account

sourceUserName When Available

The username of the platform user who initiated the action

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

applicationProtocol Always

The protocol used to communicate with the device

destinationHostName Always

Device address

port (as deviceCustomString1) Always

Device port

fingerprint (as deviceCustomString2) Always

Fingerprint

isApproved (as deviceCustomString3) Always

State of fingerprint approval

device_fingerprint_removed

Removed device fingerprint

applicationProtocol Always

The protocol used to communicate with the device

destinationHostName Always

Device address

port (as deviceCustomString1) Always

Device port

device_parameter_changed

Changed device parameter

destinationHostName	Always
The address of the device relating to the event	
destinationName (<i>as deviceCustomString1</i>)	Always
The name of the device relating to the event	
parameterName (<i>as deviceCustomString4</i>)	Always
The name of the parameter that was changed	
toValue (<i>as deviceCustomString6</i>)	Always
The new value of the parameter	
fromValue (<i>as deviceCustomString5</i>)	When Available
The old value of the parameter	

disk_capacity

Disk capacity checked.

capacity (<i>as deviceCustomNumber1</i>)	Always
The percentage of the disk which is used	
disk_display_name (<i>as deviceCustomString1</i>)	Always
The human-readable name of the disk which was checked	

error

An error has occurred

message	Always
A message describing the error	
sourceUserDisplayName (<i>as deviceCustomString2</i>)	When Available
The human-readable name of the platform user who initiated the action	
sourceUserName	When Available
The username of the platform user who initiated the action	

failed_to_generate_fingerprint

Could not generate fingerprint

applicationProtocol Always

The protocol used to communicate with the device

destinationHostName Always

Device address

port (*as deviceCustomString1*) Always

Device port

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

applicationProtocol Always

The protocol used to communicate with the device

destinationHostName Always

Device address

port (*as deviceCustomString1*) Always

Device port

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

applicationProtocol Always

The protocol used to communicate with the device

destinationHostName Always

Device address

port (*as deviceCustomString1*) Always

Device port

reason (*as deviceCustomString2*) Always

Reason

aborting (*as deviceCustomString3*) Always

Aborting

file_store_mount

The file store mount status was checked	
disk (<i>as deviceCustomString1</i>)	Always
The type of file store that was checked	
eventOutcome	Always
The outcome of the check: success if mounted, failure otherwise	

fingerprint_verification_failure

Blocking connection. Fingerprint verification failed	
applicationProtocol	Always
The protocol used to communicate with the device	
destinationHostName	Always
Device address	
port (<i>as deviceCustomString1</i>)	Always
Device port	
fingerprint (<i>as deviceCustomString2</i>)	Always
Fingerprint	
connecting (<i>as deviceCustomString3</i>)	Always
Connecting	

fingerprint_verification_failure_log_only

Allowing connection. Fingerprint verification failed but behaviour is log only	
applicationProtocol	Always
The protocol used to communicate with the device	
destinationHostName	Always
Device address	
port (<i>as deviceCustomString1</i>)	Always
Device port	
fingerprint (<i>as deviceCustomString2</i>)	Always
Fingerprint	
connecting (<i>as deviceCustomString3</i>)	Always
Connecting	

fingerprint_verification_success

Allowing connection. Fingerprint verification succeeded	
applicationProtocol The protocol used to communicate with the device	Always
destinationHostName Device address	Always
port (<i>as deviceCustomString1</i>) Device port	Always
fingerprint (<i>as deviceCustomString2</i>) Fingerprint	Always
connecting (<i>as deviceCustomString3</i>) Connecting	Always

long_running_connection_to_device

A user has been connected to a device for a long time	
applicationProtocol The protocol used to communicate with the device	Always
destinationUserName The account on the target device to which the event relates	Always
destinationName (<i>as deviceCustomString1</i>) The name of the device relating to the event	Always
duration (<i>as deviceCustomString3</i>) The length of time the user has been connected that is now considered to be "long"	Always
channelToken (<i>as deviceCustomString4</i>) An arbitrary identifier useful for correlating events pertaining to this connection	Always
roleName (<i>as deviceCustomString5</i>) The name of the role in which the user connected to the device	Always
sourceAddress The address from which the user connected to the device	Always
sourceUserName The username of the platform user who initiated the action	Always
destinationHostName The address of the device relating to the event	When Available
MAPToolName (<i>as deviceCustomString2</i>) The name of the MAP tool used	When Available
changeTicketName (<i>as deviceCustomString6</i>) The reference of the change ticket associated with the connection to the device	When Available

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_locally

An administrator terminated a session

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

sourceUserName Always

The username of the platform user who initiated the action

task_finished

An automated task was completed

destinationHostName Always

The address of the device relating to the event

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

taskName (as deviceCustomString6) Always

The name assigned to the task that completed

eventOutcome Always

The success/failure status of the action

sourceUserName Always

The username of the platform user who initiated the action

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

destinationUserName When Available

A argument required for logging when a "ad_account_password_changed" task is ran

sourceUserDisplayName (as deviceCustomString2) When Available

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

domain (as deviceCustomString3) When Available

A argument required for logging when a "ad_account_password_changed" task is ran

sourceUserName When Available

The username of the platform user who initiated the action

user_acquired_change_ticket

A user acquired a change ticket

destinationUserName Always

The user who has been associated with the change ticket

sourceUserDisplayName (as deviceCustomString2) Always

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

changeTicketName (as deviceCustomString6) Always

The name of the change ticket acquired by the user

sourceUserName Always

The username of the platform user who initiated the action

user_associated_change_ticket_with_connection

A user associated a change ticket with a connection

sourceUserDisplayName (as deviceCustomString2) Always

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

channelToken (as deviceCustomString4) Always

The arbitrary identifier of the connection associated with the change ticket

changeTicketName (as deviceCustomString6) Always

The name of the change ticket associated with the connection

sourceUserName Always

The username of the platform user who initiated the action

user_cloned_user

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

destinationUserName Always

The username of the new 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

emailAddress (as deviceCustomString3) When Available

The email address of the new user

enabled (as deviceCustomString5) When Available

Whether the new user is enabled

authenticationType (as deviceCustomString6) When Available

The authentication type of the new user

endTime When Available

When the new user account is set to expire

user_commented_on_change_ticket

A user commented on a change ticket

sourceUserDisplayName (as deviceCustomString2) Always

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

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

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 applicationProtocol	Always
The protocol used to communicate with the device	
destinationUserName	Always
The account on the target device to which the event relates	
destinationName (<i>as deviceCustomString1</i>)	Always
The name of the device relating to the event	
channelToken (<i>as deviceCustomString4</i>)	Always
An arbitrary identifier useful for correlating events pertaining to this connection	
roleName (<i>as deviceCustomString5</i>)	Always
The name of the role in which the user connected to the device	
sourceAddress	Always
The address from which the user connected to the device	
sourceUserName	Always
The username of the platform user who initiated the action	
destinationHostName	When Available
The address of the device relating to the event	
MAPToolName (<i>as deviceCustomString2</i>)	When Available
The name of the MAP tool used	
changeTicketReference (<i>as deviceCustomString6</i>)	When Available
The reference of the change ticket associated with the connection to the device	

user_created_access_request

A user created a new device access request	
destinationHostName	Always
The address of the device relating to the event	
destinationName (<i>as deviceCustomString1</i>)	Always
The name of the device relating to the event	
endTime	Always
Human-readable date string that denotes when the access request is valid until	
sourceUserName	Always
The username of the user who made the request	
startTime	Always
Human-readable date string that denotes when the access request is valid from	
destinationUserName	When Available
The account on the target device to which the event relates	
toolName (<i>as deviceCustomString3</i>)	When Available
The human-readable name of the tool relating to the event	
taskName (<i>as deviceProcessName</i>)	When Available
The name of the task the user wants to run	
message	When Available
The reason for requesting access	

user_created_account_mapping_pattern

A user created a new account mapping pattern

sourceUserDisplayName (*as deviceCustomString2*) Always

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

name (*as deviceCustomString5*) Always

The newly created account mapping name

pattern (*as deviceCustomString6*) Always

The newly created account mapping pattern

sourceUserName Always

The username of the platform user who initiated the action

user_created_auth_service

A user created an authentication service

sourceUserDisplayName (*as deviceCustomString2*) Always

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

authenticationServiceName (*as deviceCustomString6*) Always

The name of the authentication service

sourceUserName Always

The username of the platform user who initiated the action

user_created_file

A user created a file stored on Osirium PAM

sourceUserDisplayName (*as deviceCustomString2*) Always

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

sourceUserName Always

The username 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	
sourceUserDisplayName (<i>as deviceCustomString2</i>)	Always
The human-readable name of the platform user who initiated the action	
sourceUserName	Always
The username of the platform user who initiated the action	
emailAddress (<i>as deviceCustomString3</i>)	When Available
The email address of the new user	
enabled (<i>as deviceCustomString5</i>)	When Available
Whether the new user is enabled	
authenticationType (<i>as deviceCustomString6</i>)	When Available
The authentication type of the new user	
endTime	When Available
When the new user account is set to expire	

user_created_user_group

A user created a new user group

sourceUserDisplayName (<i>as deviceCustomString2</i>)	Always
The human-readable name of the platform user who initiated the action	
userNames (<i>as deviceCustomString5</i>)	Always
The usernames of the users in the new user group	
userGroupName (<i>as deviceCustomString6</i>)	Always
The name of the new user group	
sourceUserName	Always
The username of the platform user who initiated the action	

user_delete_fingerprint_failed

A user failed to delete a fingerprint

sourceUserDisplayName (<i>as deviceCustomString2</i>)	Always
The human-readable name of the platform user who initiated the action	
fingerprintId (<i>as deviceCustomString4</i>)	Always
Fingerprint id	
sourceUserName	Always
The username of the platform user who initiated the action	

user_deleted_account_mapping_pattern

A user deleted an account mapping pattern

sourceUserDisplayName (*as deviceCustomString2*) Always

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

name (*as deviceCustomString5*) Always

The account mapping name that was deleted

pattern (*as deviceCustomString6*) Always

The account mapping pattern that was deleted

sourceUserName Always

The username of the platform user who initiated the action

user_deleted_auth_service

A user deleted an authentication service

sourceUserDisplayName (*as deviceCustomString2*) Always

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

authenticationServiceName (*as deviceCustomString6*) Always

The name of the authentication service

sourceUserName Always

The username of the platform user who initiated the action

user_deleted_file

A user deleted a file stored on Osirium PAM

sourceUserDisplayName (*as deviceCustomString2*) Always

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

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

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

toolName (*as deviceCustomString3*) Always

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

fingerprintId (*as deviceCustomString4*) Always

Fingerprint id

fingerprint (*as deviceCustomString5*) Always

Deleted fingerprint

sourceUserName Always

The username of the platform user who initiated the action

user_deleted_user

A user deleted a user from Osirium PAM

destinationUserName Always

The username of the user that was deleted

sourceUserDisplayName (*as deviceCustomString2*) Always

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

sourceUserName Always

The username of the platform user who initiated the action

user_deleted_user_group

A user deleted a user group

sourceUserDisplayName (*as deviceCustomString2*) Always

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

userGroupName (*as deviceCustomString6*) Always

The name of the deleted user group

sourceUserName Always

The username of the platform user who initiated the action

user_disconnected_from_device

A user disconnected from a device

applicationProtocol	Always
The protocol used to communicate with the device	
destinationUserName	Always
The account on the target device to which the event relates	
destinationName <i>(as deviceCustomString1)</i>	Always
The name of the device relating to the event	
channelToken <i>(as deviceCustomString4)</i>	Always
An arbitrary identifier useful for correlating events pertaining to this connection	
roleName <i>(as deviceCustomString5)</i>	Always
The name of the role in which the user connected to the device	
sourceAddress	Always
The address from which the user connected to the device	
sourceUserName	Always
The username of the platform user who initiated the action	
destinationHostName	When Available
The address of the device relating to the event	
MAPToolName <i>(as deviceCustomString2)</i>	When Available
The name of the MAP tool used	
duration <i>(as deviceCustomString3)</i>	When Available
The length of time that the user was connected	
changeTicketName <i>(as deviceCustomString6)</i>	When Available
The reference of the change ticket associated with the connection to the device	

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

sourceUserDisplayName <i>(as deviceCustomString2)</i>	Always
The human-readable name of the platform user who initiated the action	
scriptArguments <i>(as deviceCustomString6)</i>	Always
The arguments passed to the script	
filename	Always
The name of the script that was executed on the console	
sourceUserName	Always
The username of the platform user who initiated the action	

user_failed_login_odc

A user failed to log in to Osirium PAM

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 (<i>as deviceCustomString1</i>)	Always
The name of the device relating to the event	
sourceAddress	Always
The address from which the client attempted to connect	
sourceUserName	Always
The username of the platform user who initiated the action	
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

Reason	Always
The reason the password update did not proceed	
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 (<i>as deviceCustomString1</i>)	Always
The name of the device relating to the event	
sourceUserDisplayName (<i>as deviceCustomString2</i>)	Always
The human-readable name of the platform user who initiated the action	
sourceUserName	Always
The username of the platform user who initiated the action	

user_forced_secrets_refresh

A user forced a password refresh for an account

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

sourceUserName Always

The username 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

authenticationServiceName (*as deviceCustomString6*) When AvailableThe authentication service to which the account belongs

user_logged_in_odc

A user logged in to Osirium PAM

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

sourceAddress Always

The address from which the client connected

sourceUserName Always

The username of the platform user who initiated the action

user_logged_out_odc

A user logged out from Osirium PAM

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 (<i>as deviceCustomString1</i>)	Always
The name of the device relating to the event	
sourceUserDisplayName (<i>as deviceCustomString2</i>)	Always
The human-readable name of the platform user who initiated the action	
sourceAddress	Always
The address from which the client was connected	
sourceUserName	Always
The username of the platform user who initiated the action	

user_login_response_required

A user must respond to log in to Osirium PAM

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 (<i>as deviceCustomString1</i>)	Always
The name of the device relating to the event	
sourceAddress	Always
The address from which the client connected	
sourceUserName	Always
The username of the platform user who initiated the action	

user_migrated_device_to_new_template

A user migrated a device to use a new template

destinationHostName Always

The address of the device relating to the event

destinationName (as deviceCustomString1) Always

The name 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

oldTemplateVersion (as deviceCustomString3) Always

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

newTemplateName (as deviceCustomString4) Always

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

newTemplateVersion (as deviceCustomString5) Always

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

templateVendor (as deviceCustomString6) Always

The vendor of the device that the template is targetting

sourceUserName Always

The username of the platform user who initiated the action

user_provisioned_device

A user provisioned a device

destinationHostName Always

The address of the device relating to the event

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

templateName (as deviceCustomString4) Always

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

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

sourceUserName Always

The username of the platform user who initiated the action

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

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

sourceUserDisplayName (as deviceCustomString2) Always

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

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

user_released_change_ticket

A user released a change ticket

sourceUserDisplayName (as deviceCustomString2) Always

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

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

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

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 to be deleted

sourceUserName Always

The username of the platform user who initiated the action

user_responded_to_access_request

A user responded to a device access request

destinationHostName	Always
The address of the device relating to the event	
destinationName <i>(as deviceCustomString1)</i>	Always
The name of the device relating to the event	
sourceUserDisplayName <i>(as deviceCustomString2)</i>	Always
The human-readable name of the platform user who initiated the action	
requesterUserDisplayName <i>(as deviceCustomString3)</i>	Always
The display name of the user who made the request	
requesterUserName <i>(as deviceCustomString4)</i>	Always
The username of the user who made the request	
response <i>(as deviceCustomString6)</i>	Always
The response the user gave to the access request	
endTime	Always
Human-readable date string that denotes when the access request is valid until	
sourceUserName	Always
The username of the platform user who initiated the action	
startTime	Always
Human-readable date string that denotes when the access request is valid from	
destinationUserName	When Available
The account on the target device to which the event relates	
toolName <i>(as deviceCustomString5)</i>	When Available
The human-readable name of the tool relating to the event	
taskName <i>(as deviceProcessName)</i>	When Available
The name of the task the user wants to run	

user_revealed_secrets

A user revealed the secrets for an account

destinationUserName	Always
The account on the target device to which the event relates	
sourceUserDisplayName <i>(as deviceCustomString2)</i>	Always
The human-readable name of the platform user who initiated the action	
sourceUserName	Always
The username of the platform user who initiated the action	
destinationHostName	When Available
The address of the device relating to the event	
destinationName <i>(as deviceCustomString1)</i>	When Available
The name of the device relating to the event	
authenticationServiceName <i>(as deviceCustomString6)</i>	When Available
The authentication service to which the account belongs	

user_revealed_secrets_history

A user revealed the secrets history for an account

destinationUserName Always

The account on the target device to which the event relates

numberRevealed (*as deviceCustomNumber1*) Always

The number of historical secrets that were revealed

sourceUserDisplayName (*as deviceCustomString2*) Always

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

sourceUserName Always

The username 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

authenticationServiceName (*as deviceCustomString6*) When Available

The authentication service to which the account belongs

user_rolled_back_device_passwords

A user rolled back the passwords on a device

destinationHostName Always

The address of the device relating to the event

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

sourceUserName Always

The username of the platform user who initiated the action

user_started_deleting_auth_service

A user triggered the deletion and cleanup of an authentication service

sourceUserDisplayName (*as deviceCustomString2*) Always

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

forced (*as deviceCustomString5*) Always

Whether the deletion was forced

authenticationServiceName (*as deviceCustomString6*) Always

The name of the authentication service being deleted

sourceUserName Always

The username 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

sourceUserDisplayName (as deviceCustomString2) Always

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

droppedActiveConnections (as deviceCustomString6) Always

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

sourceUserName AlwaysThe username of the platform user who initiated the action

user_unprovisioned_device

A user unprovisioned a device

destinationHostName Always

The address of the device relating to the event

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

forced (as deviceCustomString6) Always

Whether the device was forcibly unprovisioned

sourceUserName AlwaysThe username of the platform user who initiated the action

user_update_fingerprint_failed

A user failed to update a connection fingerprint

sourceUserDisplayName (as deviceCustomString2) Always

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

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

user_updated_account_mapping_pattern

A user updated an account mapping pattern

sourceUserDisplayName (*as deviceCustomString2*) Always

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

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

user_updated_device_file

A user performed an action that changed a file on a 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

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

sourceUserDisplayName (*as deviceCustomString2*) Always

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

filePath Always

The full path on the device of the file that was updated

sourceUserName Always

The username of the platform user who initiated the action

user_updated_device_secret

A user updated device credentials

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

sourceUserDisplayName (*as deviceCustomString2*) Always

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

sourceUserName Always

The username of the platform user who initiated the action

user_updated_fingerprint

A user updated a connection fingerprint

oldIsApproved (*as deviceCustomString3*) Always

Old state of fingerprint approval

newIsApproved (*as deviceCustomString4*) Always

New state of fingerprint approval

fingerprint (*as deviceCustomString5*) Always

Fingerprint

sourceUserName Always

The username of the platform user who initiated the action

user_updated_personal_secrets

A user updated the secrets record for a personal account

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

sourceUserName Always

The username 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

authenticationServiceName (*as deviceCustomString6*) When Available

The authentication service to which the account belongs

user_updated_profile_memberships

A user updated the memberships of a profile

sourceUserDisplayName (*as deviceCustomString2*) **Always**

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

entityType (*as deviceCustomString5*) **Always**

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

profileName (*as deviceCustomString6*) **Always**

The name of the profile for which the users were changed

sourceUserName **Always**

The username of the platform user who initiated the action

removedEntityNames (*as deviceCustomString3*) **When Available**

The names of the entities of the specified 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

enabled_status (*as deviceCustomString1*) **When Available**

Whether the user group is now enabled

removedUserNames (*as deviceCustomString2*) **When Available**

The names of the users who were removed from the group

addedUserNames (*as deviceCustomString3*) **When Available**

The names of the users who were added to the group

oldUserGroupName (*as deviceCustomString5*) **When Available**

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