

Article Number: 464 |
 Last Updated: Mon, Apr
 23, 2018 12:55 PM

This article provides complete information which will help you understating and auditing the log reports available in the Netop Portal. The generated log report will contain the following details (columns):

Report column	Description
Source	The module generating the log event. Currently, the possible values are portal and HOST .
Session	If Source is "portal", a unique identifier of the user session, useful to group log events by user session, or empty if the action is not in the context of a user session. If Source is "HOST", a unique identifier of the remote session, if the action is in the context of a Guest-Host connection, otherwise.
User Id	If Source is "portal", the internal ID of the logged in Portal user. If the action is performed in Portal rather than the actual user, the logged value is SYSTEM. If Source is "HOST", the Portal user, if Portal authentication was used for a remote session operation, or an empty value if another authentication method was used.
User Name	If Source is "portal", the username of the logged in Portal user. If the action is performed in Portal rather than the actual user, there will be no logged value in this column. If Source is "HOST", the username of the currently logged in Windows user (if the action is not in the context of a Guest-Host connection) the username that the Guest used for authenticating to the Host (depending on the Host's access settings). If the Host is set up to request a simple password (no username), this field will be empty.
Account Id	The internal ID of the account that the logged in Portal user belongs to.
Entity Type	The type of the entity involved in the current log event. For the complete list of entity types, see the next section of this article.
Action	The action executed by the entity. For the complete list of actions each entity can perform, see the next section of this article.
Entity Id	The internal ID of the entity involved in the current log event.
Entity Name	The name of the entity involved in the current log event.
Result Code	Indicates whether the action performed by the entity was successful or not. Normally, 0 means the action has been successful, anything greater than 0 means that an error has occurred.

Data	<p>Contains different data based on the action performed by the entity, as follows: If the current action is CREATE, UPDATE or DELETE, it will contain raw data with the entity updates. If the current action is LOGIN, it will contain raw data of the authenticated user, the public IP of the user performing the action and the User Agent. If the current action is PORTAL_CONNECTION_STARTED or PORTAL_CONNECTION_STOPPED, it will contain general information about the Host; if the current action is NRC_SESSION_STARTED or NRC_SESSION_STOPPED, it will also contain general information about the Guest that initiated the connection. If the current action is FILE_SENT, FILE_RECEIVED, RUN_PROGRAM, EXECUTE_COMMAND, HELP_REQUEST_SENT, GATEWAY LOGIN, GUEST_ACCESS_METHOD_CHANGED, LOGIN_FAILED, WEB_UPDATE_DOWNLOAD, WEB_UPDATE_FAILED or WEB_UPDATE_CHECK, it will contain action specific information. For more details, please refer to the table below. In all the other cases, it will contain raw data for the corresponding action.</p>
------	---

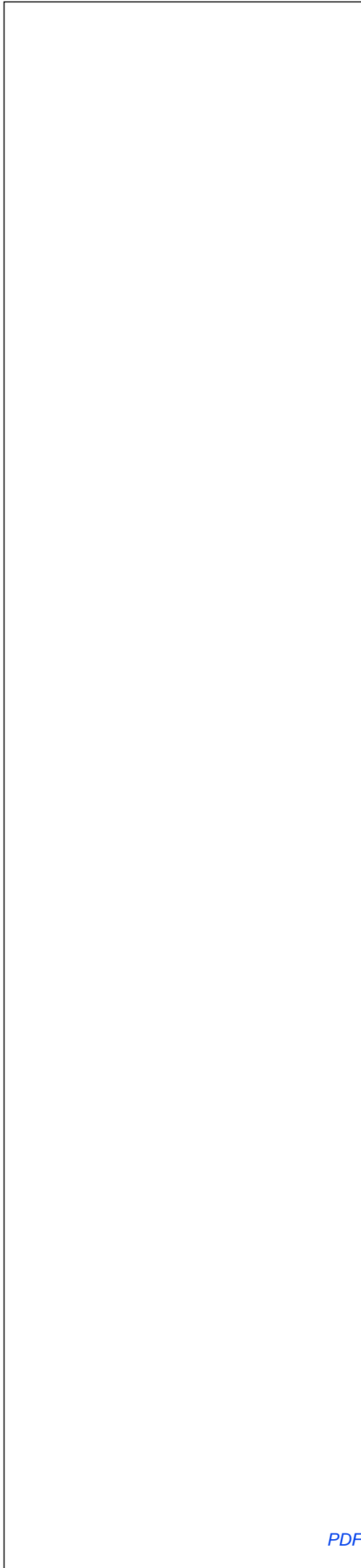
Below is the complete list of actions that can be performed on the Portal entity types and the description of the events logged in the audit trails.

Note: The Host events will be logged in the Portal only when a Netop Portal profile exists on the Host, is active (connected to the Portal), and Portal Logging is enabled for the account the Host belongs to. In case the Portal profile goes temporarily offline (after having been connected before), events will be retained by the Host until the Portal profile goes back online, or until the Host is closed. When the Portal profile goes back online, if logging is still enabled in the Portal for the Host's account, all retained events will be logged. If logging has meanwhile been disabled for the account, or the Host is closed before the Portal profile re-establishes the connection, all retained events will be discarded. In case no Portal profile is defined or active, no events will be logged.

Entity Type	Action	Event Description
ACCOUNT	CREATE	An event is logged when the first event is logged
	UPDATE	An event is logged in when owner updates the account, admin updates the account, or user updates the account.
ACCOUNT_AUTH_METHOD	CREATE	An event is logged when the first event is logged
	UPDATE	An event is logged when the account has been updated.
	DELETE	An event is logged when the account has been deleted.
	BROWSE_GROUPS	An event is logged when the user browses the Portal.
DEVICE	CREATE	An event is logged when the enrollment process begins or above or when registration is complete.
	UPDATE	An event is logged in when details are updated in the device status (going online/offline), or when the device is enrolled.
	ATTACH_TO_GROUP	An event is logged when the device is attached to a group.
	DETACH_FROM_GROUP	An event is logged when the device is detached from a group.
	DELETE	An event is logged when the device is deleted.
	REVOKE	An event is logged when the device is revoked from the Portal and subsequent events are not logged.
	CONNECT	An event is logged when the device connects to the Browser-based Setup.
	AUTHORIZE	An event is logged when the device is authorized for permissions for a specific group.
	REGISTER	An event is logged when the device registers (online/offline), having completed the enrollment process.
	ENROLL	An event is logged when the device is enrolled.
	RE_ENROLL	An event is logged when the device re-enrolls due to a conflict (e.g., the Hostname on device identity conflict).
	GET_ACCESS	An event is logged when the device attempts to access the Portal.
	UPGRADE	An event is logged when the device is upgraded from a user/password configuration to a configuration.
DEVICE_CONFLICTS	CREATE	An event is logged after the device is created with another online Hostname and workarounds, see Netop Hostname Conflicts .
	UPDATE	An event is logged as a device is updated with a conflicting Netop Hostname and workarounds, see Netop Hostname Conflicts .

DEPLOYMENT_PACKAGE	CREATE	An event is logged when a package is created in the Portal.
	UPDATE	An event is logged when a package is updated in the Portal. Host is deleted from the Portal.
	DELETE	An event is logged when a package is deleted from the Portal.
	REVOKE	An event is logged when a package is revoked from the Portal.
	GET_DOWNLOAD_URL	An event is logged when an online installer is downloaded from the Portal.
	GET_PUBLIC_DOWNLOAD_URL	An event is logged when an online installer is downloaded following an event from the Portal.
	UPLOAD_MSI	An event is logged when a specific deployment package is uploaded to the Portal.
	UPLOAD_MST	An event is logged when a specific deployment package is uploaded to the Portal.
	DOWNLOAD_EXE	An event is logged when an online installer is downloaded from the Portal.
	PUBLIC_DOWNLOAD_EXE	An event is logged when an online installer is downloaded following an event from the Portal.
	DOWNLOAD_MSI	An event is logged when the needed MSI file is downloaded from the Portal.
DOWNLOAD_MST	An event is logged when the needed MST file is downloaded from the Portal.	
USER_GROUP	CREATE	An event is logged when a user group is created in the Portal.
	UPDATE	An event is logged when a user group is updated in the Portal.
	DELETE	An event is logged when a user group is deleted from the Portal.
DEVICE_GROUP	CREATE	An event is logged when a device group is created in the Portal.
	UPDATE	An event is logged when a device group is updated in the Portal.
	DELETE	An event is logged when a device group is deleted from the Portal.
GUEST	GET_DOWNLOAD_URL	An event is logged when an online installer is downloaded from the Portal.
LDAP_GROUP	CREATE	An event is logged when an LDAP group is created in the Portal.
	UPDATE	An event is logged when an LDAP group is updated in the Portal.
	DELETE	An event is logged when an LDAP group is deleted from the Portal.
LOG_REPORT	CREATE	An event is logged when a log report is created. Usually, this log event happens when the log report is successfully generated.
	UPDATE	An event is logged when a log report is updated. Usually, this log event happens when the log report is successfully generated.
	DELETE	An event is logged when a log report is deleted.

ROLE_ASSIGNMENT	CREATE	An event is logged when a user is created in the Portal.
	UPDATE	An event is logged when a user is updated in the Portal.
	DELETE	An event is logged when a user is deleted in the Portal.
USER	CREATE	An event is logged when a user is created in the Portal.
	UPDATE	An event is logged when a user is updated in the Portal.
	DELETE	An event is logged when a user is deleted in the Portal.
	UPSERT	An event is logged when a user is created/updated in the Portal.
	START_RESET_PASSWORD	An event is logged when a user starts the password reset mechanism in the Portal.
	RESET_PASSWORD	An event is logged when a user receives password reset instructions in the Portal.
	CANCEL_RESET_PASSWORD	An event is logged when a user cancels a password reset request in the Portal.
	ATTACH_TO_GROUP	An event is logged when a user attaches to a group by clicking the Attach button in the Portal.
	DETACH_FROM_GROUP	An event is logged when a user detaches from a group in the Portal.
	GENERATE_MFA_OTC	An event is logged when a user generates Multi-Factor Authentication codes in the Portal.
	VERIFY_EMAIL	An event is logged when a user verifies their email address during the creation of a trial account in the Portal.
	LOGIN	An event is logged when a user logs in to the Portal.
	MFA_EMAIL_LOGIN	An event is logged when a user logs in to the Portal using a Multi Factor token received via email.
	MFA_OTC_LOGIN	An event is logged when a user logs in to the Portal using a one-time Multi-Factor Authentication code.
LOGOUT	An event is logged when a user logs out of the Portal.	



HOST

<p>PORTAL_CONNECTION_STARTED</p>	<p>An event is logged when a user successfully connects to the Host machine. guest_access_method are logged in the event. The username of the Windows user who is logged in on the Host machine. guest_access_method defined in the Host security policy. The name of the Host machine. private_ip. The private IP of the Host machine. operating_system. The operating system of the Host machine. nrc_version. The Host build number. nrc_buildnumber.</p>
<p>PORTAL_CONNECTION_STOPPED</p>	<p>An event is logged when a user successfully connects to the Host machine. The following Host parameters are logged in the event: logged_on_windows currently logged in on the Host machine. The Guest access method. Host ID. computer_name. public_ip. The public IP of the Host machine. private_ip. The private IP of the Host machine. operating_system. The operating system of the Host machine. nrc_buildnumber. The Host build number.</p>
<p>NRC_SESSION_STARTED</p>	<p>An event is logged when a user successfully connects to the Host machine. The following Host parameters are logged in the event: logged_on_windows currently logged in on the Host machine. The Guest access method. Host ID. computer_name. public_ip. The public IP of the Host machine. private_ip. The private IP of the Host machine. operating_system. The operating system of the Host machine. nrc_buildnumber. The Host build number. logged_on_windows currently logged in on the Host machine. username that the Guest user is logged in on the Host machine depending on the Host security policy. nrc_id. The Guest ID. public_ip. The public IP of the Host machine. private_ip. The private IP of the Host machine. reasons_for_authentication_failure. The reasons for an empty connection/authentication failure. private_ip. The private IP of the Host machine. nrc_buildnumber. The build number of the Host machine.</p>
<p>NRC_SESSION_STOPPED</p>	<p>An event is logged when a user successfully connects to the Host machine.</p>

REMOTECTRL_SESSION_STARTED	An event is logged wh
REMOTECTRL_SESSION_STOPPED	An event is logged wh
FILETRANSFER_SESSION_STARTED	An event is logged wh
FILETRANSFER_SESSION_STOPPED	An event is logged wh
CHAT_SESSION_STARTED	An event is logged wh
CHAT_SESSION_STOPPED	An event is logged wh
AUDIO_TRANSFER_STARTED	An event is logged wh
AUDIO_TRANSFER_STOPPED	An event is logged wh
KBDMOUSE_TRANSFER_STARTED	An event is logged wh technician takes over remote-controlled dev
KBDMOUSE_TRANSFER_STOPPED	An event is logged wh technician's control ov remote-controlled dev
REMOTEMGMT_SESSION_STARTED	An event is logged wh
REMOTEMGMT_SESSION_STOPPED	An event is logged wh
FILE_SENT	An event is logged wh sent from the Host to in the event log: file_n
FILE_RECEIVED	An event is logged wh received by the Host. log: file_name (the pa
RUN_PROGRAM	An event is logged wh following parameter is of the program or con
EXECUTE_COMMAND	An event is logged wh remote-accessed dev event log: file_name
INVENTORY_SENT	An event is logged wh
MESSAGE_RECEIVED	An event is logged wh
CLIPBOARD_SENT	An event is logged wh Host computer clipbo clipboard.
CLIPBOARD_RECEIVED	An event is logged wh Guest computer clipb clipboard.
KEYBOARD_LOCKED	An event is logged wh keyboard of the Host not available on this e
KEYBOARD_UNLOCKED	An event is logged wh keyboard of the Host not available on this e
SCREEN_BLANKED	An event is logged wh Host screen is blanke
SCREEN_UNBLANKED	An event is logged wh Host screen is unblan

HELP_REQUEST_SENT	An event is logged when a help request is sent. The parameters are logged in the event log. The description of the problem is logged before sending the help request. The description of the problem is logged in the event log.
HELP_REQUEST_CANCELLED	An event is logged when a help request is cancelled.
GATEWAY_LOGIN	An event is logged when a user logs in through the gateway that requires authentication. The user is logged in the event log. The access method defined in the configuration file is used by the user. The username used by the user is logged in the event log. The gateway authentication method is gateway_login_domain . Gateway authentication is successful. The following parameters are logged: 0: password wrong, maximum attempts.
GUEST_ACCESS_METHOD_CHANGED	An event is logged when the guest access method is changed. The host is changed. The old guest access method is logged in the event log: old_guest_access_method.
LOGIN_FAILED	An event is logged when a user fails to log in. The following Guest parameters are logged: logged_on_windows (boolean), currently logged in on Windows. username (string), the username that the user entered. Depending on the host configuration, the host name is logged. simple_password_authentication (boolean), whether simple password authentication is used. nrc_id (string), the Guest ID. public_ip (string), the public IP address of the machine. private_ip (string), the private IP address of the machine. reasons (array), reasons for an empty connection/authentication. private_ip (string), the private IP address of the machine. build_number (string), the build number of the software.
CONFIRM_ACCESS_GRANTED	An event is logged when a user confirms access and it is granted.
CONFIRM_ACCESS_DENIED	An event is logged when a user confirms access and it is denied.
ILLEGAL_PASSWORD_LIMIT_REACHED	An event is logged when a user enters an illegal password. The Guest exceeds the maximum number of illegal password attempts.
TIMEOUT_LIMIT_EXCEEDED_AUTHENTICATION	An event is logged when a user's authentication on the host exceeds the timeout limit.
TIMEOUT_LIMIT_EXCEEDED_CONFIRM_ACCESS	An event is logged when a user's confirmation of access exceeds the timeout limit.
TIMEOUT_LIMIT_EXCEEDED_INACTIVITY	An event is logged when a user's inactivity exceeds the timeout limit.

WEB_UPDATE_DOWNLOAD	An event is logged when a file is downloaded. The following parameters are logged: file_name, file_size, file_type, and error_message. The error_message parameter is empty. file_name is required.
WEB_UPDATE_INSTALL	An event is logged when a file is installed. The following parameters are logged: file_name, file_size, file_type, and error_message. The error_message parameter is empty. file_name is required.
WEB_UPDATE_FAILED	An event is logged when a file fails to download or install. The following parameters are logged: file_name, file_size, file_type, and error_message. The error_message parameter is empty. file_name is required.
WEB_UPDATE_CHECK	An event is logged when a file is checked for updates. The following parameters are logged: file_name, file_size, file_type, and error_message. The error_message parameter is empty. file_name is required.

>

Posted - Wed, Oct 18, 2017 2:07 PM.

Online URL: <https://kb.netop.com/article/netop-portal-audit-logging-events-464.html>