# Understand Window Events/EventIDs Read by A Connector

## Contents



## Introduction

This document describes which window events/eventIDs are read by a connector by default.

## Overview

The Umbrella Virtual Appliance (VA) technically only has visibility of which source IP address it receives a DNS query from. In order for a user to be associated with the DNS request, the VA works in conjunction with the connector which results in a user-to-IP mapping taking place.

The connector reads events with specific event IDs from the Security Event Logs on your Domain Controllers. These events are then parsed and the username and source IP address are sent to the VA, which then creates a mapping between that source IP and user.

If these events are not being audited by your domain controllers, the VAs mapping process can not take place properly. This article outlines exactly which type of event IDs the connector watches for by default.

| EventID | Description |
|---|---|
| **4624** | Event 4624 documents each and every successful attempt to logon to the local computer regardless of logon type, location of the user or type of account. |
| **528** | Event 528 is logged whenever an account logs on to the local computer, except for in the event of network logons. Event 528 is logged whether the account used for logon is a local SAM account or a domain account. |
| **540** | Event 540 gets logged when a user elsewhere on the network connects to a resource (such as a shared folder) provided by the Server service on this computer. |
| **4768** | This event is logged on domain controllers only and both success and failure instances of this event are logged. |
| **4769** | Windows uses this event ID for both successful and failed service ticket requests. |

If your connector is unable to read events directly from the Security Event Logs of the domain controller,

you can raise a support ticket with Umbrella asking for this to be changed to WMI subscription. In the case of WMI subscriptions, the connector subscribes to all the events listed above. In addition, the connector also subscribes to logoff events with EventIDs as mentioned below. Note that by default, the connector does not read these logoff events from the Security Event Logs.

| EventID | Description |
|---|---|
| **538** | Event 538 is logged whenever a user logs off, whether from a network connection, interactive logon, or other logon type (see event 528 for a chart of logon types). |
| **4647** | This event signals the end of a logon session and can be correlated back to the logon event 4624 using the Logon ID. |
| **4634** | This event also signals the end of a logon session and can be correlated back to the logon event 4624 using the Logon ID. |