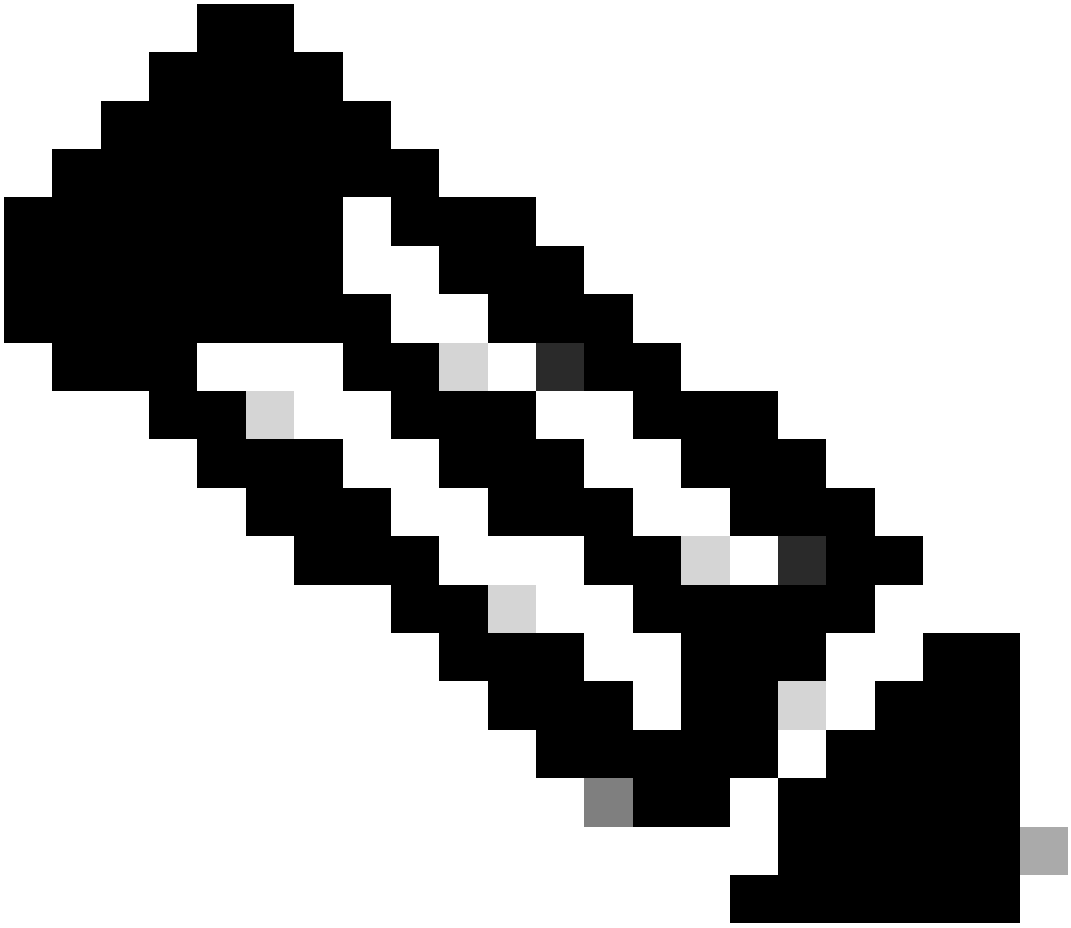
# Troubleshoot EventID 4662 (Windows 2008) or EventID 566 (Windows 2003) - Type: Failure Audit

## Contents



## Introduction

This document describes Security Event ID 566 and Security Event ID 4662, and what action can be taken when encountering them. These events could be expected to occur on Domain Controllers or a member server running as part of the Umbrella Insights deployment.



**Note**: These events are to be expected and are normal. The preferred and supported action is to do nothing and ignore these events.

---

```
Event ID: 566
Source: Security
Category: Directory Service Access
Type: Failure Audit
Description:
Object Operation:
Object Server:  DS
Operation Type: Object Access
Object Type:    user
Object Name:   CN=USER1,OU=MyOU,DC=domain,DC=net
Handle ID:        -
Primary User Name:     DC1$
Primary Domain:           DOMAIN1
Primary Logon ID:        (0x0,0x3E7)
Client User Name:        COMPUTER1$
Client Domain:  DOMAIN1
Client Logon ID:           (0x0,0x19540114)
```

```
Accesses:         Control Access
Properties:

Private Information

msPKIRoamingTimeStamp
msPKIDPAPIMasterKeys
msPKIAccountCredentials
msPKI-CredentialRoamingTokens
Default property set
unixUserPassword

user
Additional Info:
Additional Info2:
Access Mask:   0x100
```

Or you receive this Windows 2008 Event Security ID 4662.

```
Event ID: 4662
Type: Audit Failure
Category: Directory Service Access

Description:

An operation was performed on an object.

Subject :

Security ID:     DOMAIN1\COMPUTER1$
Account Name:     COMPUTER1$
Account Domain:     DOMAIN1

Logon ID:     0x3a26176b

Object:

Object Server:     DS
Object Type:     user
Object Name:     CN=USER1,OU=MyOU,DC=domain,DC=net

Handle ID:     0x0

Operation:

Operation Type:     Object Access
Accesses:     Control Access
Access Mask:     0x100

Properties:     ---

{91e647de-d96f-4b70-9557-d63ff4f3ccd8}
{6617e4ac-a2f1-43ab-b60c-11fbd1facf05}
{b3f93023-9239-4f7c-b99c-6745d87adbc2}
{b8dfa744-31dc-4ef1-ac7c-84baf7ef9da7}
{b7ff5a38-0818-42b0-8110-d3d154c97f24}
{bf967aba-0de6-11d0-a285-00aa003049e2}
```

# Cause

Windows 2008 introduced a new property set called **Private Information** that includes the **msPKI*** properties. By design, these properties are secured in such a manner that only the SELF object can access them. You can use the **DSACLS** command to verify the permissions on the object as needed.

Cursory investigation may lead you to believe this audit event is being caused by an attempt to write to these restricted properties. This is evident by the fact these events occur under the default Microsoft audit policy that only audits changes (writes), and does not audit attempts to read information from Active Directory.

However, this is not the case, the audit event clearly lists the permission being requested as **Control Access** (0x100). Unfortunately, you can not grant the **CA** (**Control Access**) permission to the **Private Information** property set.

# Solution

You can safely ignore these messages. This is by design.

It is not recommended that you take any action to prevent these events from appearing. However, these are presented as options if you choose to implement them. Neither workaround is recommended: use at your own risk.

# Workarounds

## Method 1

Disable all auditing in Active Directory by disabling the **Directory Service** auditing setting in the default Domain Controller policy.

## Method 2

The underlying process that manages the **Control Access** permission utilizes the **searchFlags** attribute that is assigned to each property (ie: msPKIRoamingTimeStamp). **searchFlags** is a 10 bit access mask. It uses bit 8 (counting from 0 to 7 in a binary access mask = 10000000 = 128 decimal) to implement the concept of **Confidential Access**. You can manually modify this attribute in the AD Schema and disable the **Confidential Access** of these properties. This then prevents the failure audit logs from being generated.

To disable Confidential Access for any property in AD use **ADSI Edit** to attach to the Schema naming context on the DC holding the Schema Master Role. Find the appropriate properties to modify, their name may be slightly different than what is shown in Event ID 566 or 4662.

To determine the correct value to enter subtract 128 from the current **searchFlags** value, and enter the result as the new value of **searchFlags**, thus 640-128 = 512. If the current value of **searchFlags** is < 128 do nothing, you may have the wrong property or **Confidential Access** is not causing the audit event.

Do this for each property listed in the Event ID 566 or 4662 description.

Force replication of the Schema Master to the other domain controllers, then check for new Events.

Modify the domain audit policy not to audit failures on these properties:

The downside to this method is performance may be degraded due to the high number of audit entries that need to be added.

# More Information:

Translating GUID to objects names is easy using google or another search engine.  Here is an example of how to search using google.

Example: **site:microsoft.com 91e647de-d96f-4b70-9557-d63ff4f3ccd8**

{91e647de-d96f-4b70-9557-d63ff4f3ccd8} = Private Information Property Set
{6617e4ac-a2f1-43ab-b60c-11fbd1facf05} = ms-PKI-RoamingTimeStamp Attribute