We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking "Manage Cookies" at the bottom of the page. Privacy Statement Third-Party Cookies

Accept Reject Manage cookies

We're no longer updating this content regularly. Check the Microsoft Product Lifecycle for information about how this product, service, technology, or API is supported.

Return to main site

Filter by title

- Security auditing
  - Security auditing
  - Basic security audit policies
  - Advanced security audit policies
    - Advanced security audit policies
    - Planning and deploying advanced security audit policies
    - Advanced security auditing FAQ
      - Advanced security auditing FAQ

4794(S, F): An attempt was made to set the Directory Services Restore Mode administrator password.

Article • 09/07/2021 • 1 contributor

Subcategory: Audit User Account Management

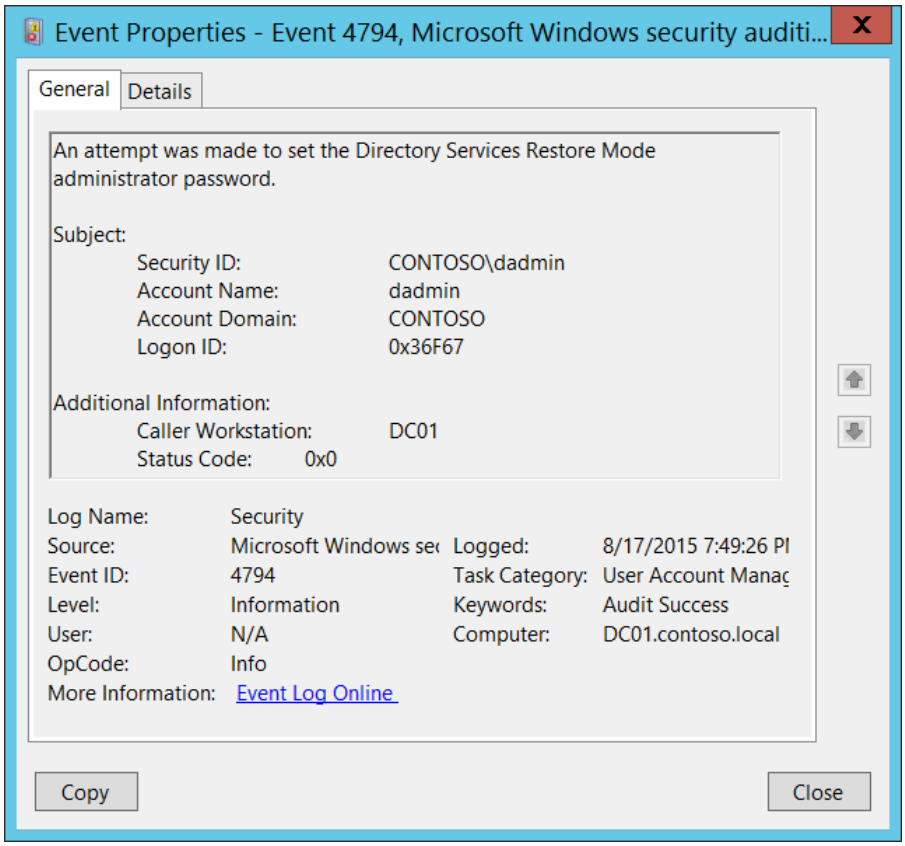
Event Description:

This event generates every time Directory Services Restore Mode (DSRM) administrator password is changed.

Which editions of Windows support advanced audit policy configuration

How to list XML elements in \<EventData>

› Using advanced security auditing options to



This event generates only on domain controllers.

Note For recommendations, see Security Monitoring Recommendations for this event.

Event XML:

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/eve
- <System>
 <Provider Name="Microsoft-Windows-Security-Auditing" Guid='
 <EventID>4794</EventID>
 <Version>0</Version>
 <Level>0</Level>
 <Task>13824</Task>
 <Opcode>0</Opcode>
 <Keywords>0x8020000000000000</Keywords>
 <TimeCreated SystemTime="2015-08-18T02:49:26.087748900Z" />
 <EventRecordID>172348</EventRecordID>
 <Correlation />
```

```
 <Execution ProcessID="520" ThreadID="2964" />
 <Channel>Security</Channel>
 <Computer>DC01.contoso.local</Computer>
 <Security />
 </System>
- <EventData>
 <Data Name="SubjectUserSid">S-1-5-21-3457937927-2839227994-
 <Data Name="SubjectUserName">dadmin</Data>
 <Data Name="SubjectDomainName">CONTOSO</Data>
 <Data Name="SubjectLogonId">0x36f67</Data>
 <Data Name="Workstation">DC01</Data>
 <Data Name="Status">0x0</Data>
 </EventData>
 </Event>
```

Required Server Roles: Active Directory domain controller.

Minimum OS Version: Windows Server 2008.

Event Versions: 0.

Field Descriptions:

Subject:

- **Security ID** [Type = SID]**:** SID of account that made an attempt to set Directory Services Restore Mode administrator password. Event Viewer automatically tries to resolve SIDs and show the account name. If the SID cannot be resolved, you will see the source data in the event.

> **Note** A **security identifier (SID)** is a unique value of variable length used to identify a trustee (security principal). Each account has a unique SID that is issued by an authority, such as an Active Directory domain controller, and stored in a security database. Each time a user logs on, the system retrieves the SID for that user from the database and places it in the access token for that user. The system uses the SID in the access token to identify the user in all subsequent interactions with Windows security. When a SID has been used as the unique identifier for a user or group, it cannot

> ever be used again to identify another user or group. For more information about SIDs, see Security identifiers.

- **Account Name** [Type = UnicodeString]: the name of the account that made an attempt to set Directory Services Restore Mode administrator password.
- **Account Domain** [Type = UnicodeString]: subject's domain or computer name. Formats vary, and include the following:
  - Domain NETBIOS name example: CONTOSO
  - Lowercase full domain name: contoso.local
  - Uppercase full domain name: CONTOSO.LOCAL
  - For some well-known security principals, such as LOCAL SERVICE or ANONYMOUS LOGON, the value of this field is "NT AUTHORITY".
  - For local user accounts, this field will contain the name of the computer or device that this account belongs to, for example: "Win81".
- **Logon ID** [Type = HexInt64]: hexadecimal value that can help you correlate this event with recent events that might contain the same Logon ID, for example, "4624: An account was successfully logged on."

Additional Information:

- **Caller Workstation** [Type = UnicodeString]: the name of computer account from which Directory Services Restore Mode (DSRM) administrator password change request was received. For example: "**DC01**". If the change request was sent locally (from the same server) this field will have the same name as the computer account.

- **Status Code** [Type = HexInt32]: for Success events it has "**0x0**" value.

Security Monitoring Recommendations

For 4794(S, F): An attempt was made to set the Directory Services Restore Mode administrator password.

- Always monitor 4794 events and trigger alerts when they occur.

English (United States) Your Privacy Choices Theme

Manage cookies Previous Versions Blog Contribute Privacy Terms of Use Trademarks

© Microsoft 2024