



Start free trial

Contact Sales

Platform Solutions Customers Resources Pricing Docs

IMPORTANT: No additional bug fixes or documentation updates will be released for this version. For the latest information, see the [current release documentation](#).

[Elastic Docs](#) › [Elastic Security Solution \[8.4\]](#) › [Detections and alerts](#) › [Prebuilt rule reference](#)

Potential Shadow Credentials added to AD Object

Identify the modification of the msDS-KeyCredentialLink attribute in an Active Directory Computer or User Object. Attackers can abuse control over the object and create a key pair, append to raw public key in the attribute, and obtain persistent and stealthy access to the target user or computer object.

Rule type: query

Rule indices:

- winlogbeat-*
- logs-system.*

Severity: high

Risk score: 73

Runs every: 5 minutes

Searches indices from: now-9m ([Date Math format](#), see also [Additional look-back time](#))

Maximum alerts per execution: 100

References:

- <https://posts.specterops.io/shadow-credentials-abusing-key-trust-account-mapping-for-takeover-8ee1a53566ab>
- <https://www.thehacker.recipes/ad/movement/kerberos/shadow-credentials>
- <https://github.com/OTRF/Set-AuditRule>

Tags:

- Elastic
- Host
- Windows
- Threat Detection
- Credential Access
- Active Directory

Version: 4 ([version history](#))

Added (Elastic Stack release): 8.1.0

Last modified (Elastic Stack release): 8.4.0

Rule authors: Elastic

Rule license: Elastic License v2

Potential false positives

Modifications in the msDS-KeyCredentialLink attribute can be done legitimately by the Azure AD Connect synchronization account or the ADFS service account. These accounts can be added as Exceptions.

Investigation guide



Rule query

```
event.action:"Directory Service Changes" and event.type:"winlog.event_data.AttributeLDAPDisplayName:"msDS-Key
```

Threat mapping

Framework: MITRE ATT&CK™

- Tactic:
 - Name: Credential Access
 - ID: TA0006
 - Reference URL:
<https://attack.mitre.org/tactics/TA0006/>
- Technique:
 - Name: Modify Authentication Process
 - ID: T1556
 - Reference URL:
<https://attack.mitre.org/techniques/T1556/>

Rule version history

Version 4 (8.4.0 release)

- Formatting only

Version 2 (8.2.0 release)

- Formatting only

[« Potential Secure File Deletion via SDelete Utility](#)

[Potential SharpRDP Behavior »](#)

ElasticON events are back!

Learn about the Elastic Search AI Platform from the experts at our live events.

[Learn more](#)

Was this helpful?



The Search AI Company

Follow us



About us

[About Elastic](#)

Partners

[Find a partner](#)

Leadership

DE&I

Blog

Newsroom

Join us

Careers

Career portal

Partner login

Request access

Become a partner

Trust & Security

Trust center

EthicsPoint portal

ECCN report

Ethics email

Investor relations

Investor resources

Governance

Financials

Stock

EXCELLENCE AWARDS

Previous winners

ElasticON Tour

Become a sponsor

All events

[Trademarks](#) [Terms of Use](#) [Privacy](#) [Sitemap](#)

© 2024. Elasticsearch B.V. All Rights Reserved

Elastic, Elasticsearch and other related marks are trademarks, logos or registered trademarks of Elasticsearch B.V. in the United States and other countries.

Apache, Apache Lucene, Apache Hadoop, Hadoop, HDFS and the yellow elephant logo are trademarks of the Apache Software Foundation in the United States and/or other countries. All other brand names, product names, or trademarks belong to their respective owners.