

NIST CSF 2.0-PR.AA-01-Ex2

PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used Identity Management, Authentication, and Access Control (PR.AA)

Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access

PR.AA-01

Identities and credentials for authorized users, services, and hardware are managed by the organization

Ex2

Issue, manage, and revoke cryptographic certificates and identity tokens, cryptographic keys (i.e., key management), and other credentials

Compliance Framework References:

CCMv4.0: CEK-01

CCMv4.0: CEK-10

CCMv4.0: CEK-11

CCMv4.0: CEK-12

CCMv4.0: CEK-13

CCMv4.0: CEK-14

CCMv4.0: CEK-15

CCMv4.0: CEK-16

CCMv4.0: CEK-17

CCMv4.0: CEK-18

CCMv4.0: CEK-19

CCMv4.0: CEK-20

CCMv4.0: CEK-21

CCMv4.0: DCS-08

CCMv4.0: IAM-01

CCMv4.0: IAM-03

CCMv4.0: IAM-06

CCMv4.0: IAM-07

CCMv4.0: IAM-09

CCMv4.0: IAM-13

CCMv4.0: IAM-14

CCMv4.0: IAM-15

CCMv4.0: IAM-16

CCMv4.0: UEM-14

CIS Controls v8.0: 5.1

CIS Controls v8.0: 6.7

CRI Profile v2.0: PR.AA-01

CRI Profile v2.0: PR.AA-01.01

CRI Profile v2.0: PR.AA-01.02

CSF v1.1: PR.AC-1

SP 800-53 Rev 5.1.1: AC-01

SP 800-53 Rev 5.1.1: AC-02

SP 800-53 Rev 5.1.1: AC-14

SP 800-53 Rev 5.1.1: IA-01

SP 800-53 Rev 5.1.1: IA-02

SP 800-53 Rev 5.1.1: IA-03

SP 800-53 Rev 5.1.1: IA-04

SP 800-53 Rev 5.1.1: IA-05

SP 800-53 Rev 5.1.1: IA-06

SP 800-53 Rev 5.1.1: IA-07

SP 800-53 Rev 5.1.1: IA-08

SP 800-53 Rev 5.1.1: IA-09

SP 800-53 Rev 5.1.1: IA-10

SP 800-53 Rev 5.1.1: IA-11

Vendor: Microsoft Azure

Comments: Evidence of these actions should be discoverable in the logs. However, it will take research to determine which logs would be appropriate.

UDM Search Query:

```
$e.additional.fields["targetResources.modifiedProperties.newValue    0"]    =
/KeyIdentifier.*/
$e.additional.fields["targetResources.modifiedProperties.oldValue    0"]    =
/KeyIdentifier.*/
$e.metadata.log_type = "AZURE_AD_AUDIT"
$e.metadata.product_event_type = "Update application - Certificates and
secrets management "

$date = timestamp.get_date($e.metadata.event_timestamp.seconds)

match:
    $date

outcome:
    $user_id = array_distinct($e.principal.user.userid)
                                $old_key                                =
array_distinct($e.additional.fields["targetResources.modifiedProperties.oldV
alue 0"])
                                $new_key                                =
array_distinct($e.additional.fields["targetResources.modifiedProperties.newV
alue 0"])

order:
    $date

limit: 25
```

10-20-2024

| hostname | destip | count |
|-------------------|----------------|-------|
| calm-orion-8112 | 207.3.50.185 | 7088 |
| loud-blaze-4706 | 37.198.57.90 | 875 |
| eager-glyph-3607 | 41.249.102.22 | 3152 |
| tough-zephyr-6801 | 162.195.41.129 | 8183 |
| keen-bear-2972 | 18.240.44.191 | 9823 |
| warm-fox-0927 | 42.28.42.216 | 9220 |
| lively-lion-7689 | 191.95.195.233 | 5858 |
| calm-glyph-5246 | 178.93.96.212 | 8215 |
| nifty-meteor-5590 | 112.40.225.248 | 4566 |
| rich-ember-2213 | 129.112.53.246 | 1836 |

09-20-2024

| hostname | destip | count |
|-------------------|----------------|-------|
| calm-orion-8112 | 207.3.50.185 | 7088 |
| loud-blaze-4706 | 37.198.57.90 | 875 |
| eager-glyph-3607 | 41.249.102.22 | 3152 |
| tough-zephyr-6801 | 162.195.41.129 | 8183 |
| keen-bear-2972 | 18.240.44.191 | 9823 |
| warm-fox-0927 | 42.28.42.216 | 9220 |
| lively-lion-7689 | 191.95.195.233 | 5858 |
| calm-glyph-5246 | 178.93.96.212 | 8215 |
| nifty-meteor-5590 | 112.40.225.248 | 4566 |
| rich-ember-2213 | 129.112.53.246 | 1836 |

08-20-2024

| hostname | destip | count |
|-------------------|----------------|-------|
| calm-orion-8112 | 207.3.50.185 | 7088 |
| loud-blaze-4706 | 37.198.57.90 | 875 |
| eager-glyph-3607 | 41.249.102.22 | 3152 |
| tough-zephyr-6801 | 162.195.41.129 | 8183 |
| keen-bear-2972 | 18.240.44.191 | 9823 |
| warm-fox-0927 | 42.28.42.216 | 9220 |
| lively-lion-7689 | 191.95.195.233 | 5858 |
| calm-glyph-5246 | 178.93.96.212 | 8215 |
| nifty-meteor-5590 | 112.40.225.248 | 4566 |
| rich-ember-2213 | 129.112.53.246 | 1836 |