User Account Management, Mitigation M1018 - Enterprise

Archived: 2026-04-02 10:47:40 UTC

Enterprise T1548 Abuse Elevation Control Mechanism

Limit the privileges of cloud accounts to assume, create, or impersonate additional roles, policies, and permissions to only those required. Where just-in-time access is enabled, consider requiring manual approval for temporary elevation of privileges.

.005 Temporary Elevated Cloud Access

Limit the privileges of cloud accounts to assume, create, or impersonate additional roles, policies, and permissions to only those required. Where just-in-time access is enabled, consider requiring manual approval for temporary elevation of privileges.

Enterprise T1134 Access Token Manipulation

An adversary must already have administrator level access on the local system to make full use of this technique; be sure to restrict users and accounts to the least privileges they require.

.001 Token Impersonation/Theft

An adversary must already have administrator level access on the local system to make full use of this technique; be sure to restrict users and accounts to the least privileges they require.

.002 Create Process with Token

An adversary must already have administrator level access on the local system to make full use of this technique; be sure to restrict users and accounts to the least privileges they require.

.003 Make and Impersonate Token

An adversary must already have administrator level access on the local system to make full use of this technique; be sure to restrict users and accounts to the least privileges they require.

Enterprise T1087 Account Discovery

Manage the creation, modification, use, and permissions associated to user accounts.

.004 Cloud Account

Limit permissions to discover cloud accounts in accordance with least privilege. Organizations should limit the number of users within the organization with an IAM role that has administrative privileges, strive to reduce all permanent privileged role assignments, and conduct periodic entitlement reviews on IAM users, roles and policies.

Enterprise T1098 Account Manipulation

Ensure that low-privileged user accounts do not have permissions to modify accounts or account-related policies.

.001 Additional Cloud Credentials

Ensure that low-privileged user accounts do not have permission to add access keys to accounts. In AWS environments, prohibit users from calling the `sts:GetFederationToken` API unless explicitly required.[1]

.003 Additional Cloud Roles

Ensure that low-privileged user accounts do not have permissions to add permissions to accounts or update IAM policies.

.004 SSH Authorized Keys

In cloud environments, ensure that only users who explicitly require the permissions to update instance metadata or configurations can do so.

.006 Additional Container Cluster Roles

Ensure that low-privileged accounts do not have permissions to add permissions to accounts or to update container cluster roles.

Enterprise T1020 .001 Automated Exfiltration: Traffic Duplication

In cloud environments, ensure that users are not granted permissions to create or modify traffic mirrors unless this is explicitly required.

Enterprise T1197 BITS Jobs

Consider limiting access to the BITS interface to specific users or groups.[2]

Enterprise T1547 .004 Boot or Logon Autostart Execution: Winlogon Helper DLL

Limit the privileges of user accounts so that only authorized administrators can perform Winlogon helper changes.

.006 Boot or Logon Autostart Execution: Kernel Modules and Extensions

Use MDM to disable user's ability to install or approve kernel extensions, and ensure all approved kernel extensions are in alignment with policies specified in `com.apple.syspolicy.kernel-extension-policy`.[3][4]

.009 Boot or Logon Autostart Execution: Shortcut Modification

Limit Privileges for Shortcut Creation: While the SeCreateSymbolicLinkPrivilege is not directly related to .lnk file creation, you should still enforce least privilege principles by limiting user rights to create and modify shortcuts, especially in system-critical locations. This can be done through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Create symbolic links. [5]

Regular User Permissions Review: Regularly review and audit user permissions to ensure that only necessary accounts have write access to startup folders and critical system directories.

.012 Boot or Logon Autostart Execution: Print Processors

Limit user accounts that can load or unload device drivers by disabling `SeLoadDriverPrivilege`.

.013 Boot or Logon Autostart Execution: XDG Autostart Entries

Limit privileges of user accounts so only authorized privileged users can create and modify XDG autostart entries.

Enterprise T1185 Browser Session Hijacking

Since browser pivoting requires a high integrity process to launch from, restricting user permissions and addressing Privilege Escalation and Bypass User Account Control opportunities can limit the exposure to this technique.

Enterprise T1110 Brute Force

Proactively reset accounts that are known to be part of breached credentials either immediately, or after detecting bruteforce attempts.

.004 Credential Stuffing

Proactively reset accounts that are known to be part of breached credentials either immediately, or after detecting bruteforce attempts.

Enterprise T1580 Cloud Infrastructure Discovery

Limit permissions to discover cloud infrastructure in accordance with least privilege. Organizations should limit the number of users within the organization with an IAM role that has administrative privileges, strive to reduce all permanent privileged role assignments, and conduct periodic entitlement reviews on IAM users, roles and policies.

Enterprise T1538 Cloud Service Dashboard

Enforce the principle of least-privilege by limiting dashboard visibility to only the resources required. This may limit the discovery value of the dashboard in the event of a compromised account.

Enterprise T1619 Cloud Storage Object Discovery

Restrict granting of permissions related to listing objects in cloud storage to necessary accounts.

Enterprise T1059 .008 Command and Scripting Interpreter: Network Device CLI

Use of Authentication, Authorization, and Accounting (AAA) systems will limit actions users can perform and provide a history of user actions to detect unauthorized use and abuse. Ensure least privilege principles are applied to user accounts and groups so that only authorized users can perform configuration changes. [6]

Enterprise T1609 Container Administration Command

Enforce authentication and role-based access control on the container service to restrict users to the least privileges required.[7] When using Kubernetes, avoid giving users wildcard permissions or adding users to the `system:masters` group, and use `RoleBindings` rather than `ClusterRoleBindings` to limit user privileges to specific namespaces.[8]

Enterprise T1613 Container and Resource Discovery

Enforce the principle of least privilege by limiting dashboard visibility to only the required users. When using Kubernetes, avoid giving users wildcard permissions or adding users to the `system:masters` group, and use `RoleBindings` rather than `ClusterRoleBindings` to limit user privileges to specific namespaces.[8]

Enterprise T1543 Create or Modify System Process

Limit privileges of user accounts and groups so that only authorized administrators can interact with system-level process changes and service configurations.

.002 Systemd Service

Limit user access to system utilities such as `systemctl` to only users who have a legitimate need.

.003 Windows Service

Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service configurations.

.004 Launch Daemon

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create new Launch Daemons.

.005 Container Service

Limit access to utilities such as docker to only users who have a legitimate need, especially if using docker in rootful mode. In Kubernetes environments, only grant privileges to deploy pods to users that require it.

Enterprise T1555 .003 Credentials from Password Stores: Credentials from Web Browsers

Implement strict user account management policies to prevent unnecessary accounts from accessing sensitive systems. Regularly audit user accounts to identify and disable inactive accounts that may be targeted by attackers to extract credentials or gain unauthorized access.

.005 Credentials from Password Stores: Password Managers

Implement strict user account management policies to prevent unnecessary accounts from accessing sensitive systems. Regularly audit user accounts to identify and disable inactive accounts that may be targeted by attackers to extract credentials or gain unauthorized access.

Enterprise T1485 Data Destruction

In cloud environments, limit permissions to modify cloud bucket lifecycle policies (e.g., `PutLifecycleConfiguration` in AWS) to only those accounts that require it. In AWS environments, consider using Service Control policies to limit the use of the `PutBucketLifecycle` API call.

.001 Lifecycle-Triggered Deletion

In cloud environments, limit permissions to modify cloud bucket lifecycle policies (e.g., `PutLifecycleConfiguration` in AWS) to only those accounts that require it. In AWS environments, consider using Service Control policies to limit the use of the `PutBucketLifecycle` API call.

Enterprise T1530 Data from Cloud Storage

Configure user permissions groups and roles for access to cloud storage.[9] Implement strict Identity and Access Management (IAM) controls to prevent access to storage solutions except for the applications, users, and services that require access.[10] Ensure that temporary access tokens are issued rather than permanent credentials, especially when access is being granted to entities outside of the internal security boundary.[11]

Enterprise T1213 Data from Information Repositories

Enforce the principle of least-privilege. Consider implementing access control mechanisms that include both authentication and authorization.

.001 Confluence

Enforce the principle of least-privilege. Consider implementing access control mechanisms that include both authentication and authorization.

.002 Sharepoint

Enforce the principle of least-privilege. Consider implementing access control mechanisms that include both authentication and authorization.

.003 Code Repositories

Enforce the principle of least-privilege. Consider implementing access control mechanisms that include both authentication and authorization for code repositories.

.004 Customer Relationship Management Software

Enforce the principle of least-privilege. Consider implementing access control mechanisms that include both authentication and authorization.

.006 Databases

Enforce the principle of least-privilege. Consider implementing access control mechanisms that include both authentication and authorization.

Enterprise T1610 Deploy Container

Enforce the principle of least privilege by limiting container dashboard access to only the necessary users. When using Kubernetes, avoid giving users wildcard permissions or adding users to the `system:masters` group, and use `RoleBindings` rather than `ClusterRoleBindings` to limit user privileges to specific namespaces.[8]

Enterprise T1006 Direct Volume Access

Ensure only accounts required to configure and manage backups have the privileges to do so. Monitor these accounts for unauthorized backup activity.

Enterprise T1484 Domain or Tenant Policy Modification

Consider implementing WMI and security filtering to further tailor which users and computers a GPO will apply to.[12][13][14]

.001 Group Policy Modification

Consider implementing WMI and security filtering to further tailor which users and computers a GPO will apply to.[12][13][14]

.002 Trust Modification

In cloud environments, limit permissions to create new identity providers to only those accounts that require them. In AWS environments, consider using Service Control policies to limit the use of API calls such as `CreateSAMLProvider` or `CreateOpenIDConnectProvider`.

Enterprise T1675 ESXi Administration Command

If not required, restrict the permissions of users to perform Guest Operations on ESXi-hosted VMs.[15]

Enterprise T1546 .003 Event Triggered Execution: Windows Management Instrumentation Event Subscription

By default, only administrators are allowed to connect remotely using WMI; restrict other users that are allowed to connect, or disallow all users from connecting remotely to WMI.

Enterprise T1048 Exfiltration Over Alternative Protocol

Configure user permissions groups and roles for access to cloud storage.[9] Implement strict Identity and Access Management (IAM) controls to prevent access to storage solutions except for the applications, users, and services that require access.[10] Ensure that temporary access tokens are issued rather than permanent credentials, especially when access is being granted to entities outside of the internal security boundary.[11]

Enterprise T1657 Financial Theft

Limit access/authority to execute sensitive transactions, and switch to systems and procedures designed to authenticate/approve payments and purchase requests outside of insecure communication lines such as email.

Enterprise T1606 Forge Web Credentials

Ensure that user accounts with administrative rights follow best practices, including use of privileged access workstations, Just in Time/Just Enough Administration (JIT/JEA), and strong authentication. Reduce the number of users that are members of highly privileged Directory Roles.[16] In AWS environments, prohibit users from calling the `sts:GetFederationToken` API unless explicitly required.[1]

.002 SAML Tokens

Ensure that user accounts with administrative rights follow best practices, including use of privileged access workstations, Just in Time/Just Enough Administration (JIT/JEA), and strong authentication. Reduce the number of users that are members of highly privileged Directory Roles.[16]

Enterprise T1574 Hijack Execution Flow

Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service binary target path locations. Deny execution from user directories such as file download directories and temp directories where able.

Ensure that proper permissions and directory access control are set to deny users the ability to write files to the top-level directory `C:` and system directories, such as `C:\Windows\` , to reduce places where malicious files could be placed for execution.

.005 Executable Installer File Permissions Weakness

Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service binary target path locations. Deny execution from user directories such as file download directories and temp directories where able.

.010 Services File Permissions Weakness

Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service binary target path locations. Deny execution from user directories such as file download directories and temp directories where able.

.012 COR_PROFILER

Limit the privileges of user accounts so that only authorized administrators can edit system environment variables.

Enterprise T1562 Impair Defenses

Ensure proper user permissions are in place to prevent adversaries from disabling or interfering with security/logging services.

.001 Disable or Modify Tools

Ensure proper user permissions are in place to prevent adversaries from disabling or interfering with security services.

.002 Disable Windows Event Logging

Ensure proper user permissions are in place to prevent adversaries from disabling or interfering with logging.

.004 Disable or Modify System Firewall

Ensure proper user permissions are in place to prevent adversaries from disabling or modifying firewall settings.

.006 Indicator Blocking

Ensure event tracers/forwarders [17], firewall policies, and other associated mechanisms are secured with appropriate permissions and access controls and cannot be manipulated by user accounts.

.007 Disable or Modify Cloud Firewall

Ensure least privilege principles are applied to Identity and Access Management (IAM) security policies.[18]

.008 Disable or Modify Cloud Logs

Configure default account policy to enable logging. Manage policies to ensure only necessary users have permissions to make changes to logging policies.

.012 Disable or Modify Linux Audit System

An adversary must already have root level access on the local system to make full use of this technique; be sure to restrict users and accounts to the least privileges they require.

.013 Disable or Modify Network Device Firewall

Ensure proper user permissions are in place to prevent adversaries from disabling or modifying firewall settings.

Enterprise T1490 Inhibit System Recovery

Limit the user accounts that have access to backups to only those required. In AWS environments, consider using Service Control Policies to restrict API calls to delete backups, snapshots, and images.

Enterprise T1654 Log Enumeration

Limit the ability to access and export sensitive logs to privileged accounts where possible.

Enterprise T1036 Masquerading

Consider defining and enforcing a naming convention for user accounts to more easily spot generic account names that do not fit the typical schema.

.010 Masquerade Account Name

Consider defining and enforcing a naming convention for user accounts to more easily spot generic account names that do not fit the typical schema.

Enterprise T1556 Modify Authentication Process

Ensure that proper policies are implemented to dictate the the secure enrollment and deactivation of authentication mechanisms, such as MFA, for user accounts.

.006 Multi-Factor Authentication

Ensure that proper policies are implemented to dictate the secure enrollment and deactivation of MFA for user accounts.

.009 Conditional Access Policies

Limit permissions to modify conditional access policies to only those required.

Enterprise T1578 Modify Cloud Compute Infrastructure

Limit permissions for creating, deleting, and otherwise altering compute components in accordance with least privilege. Organizations should limit the number of users within the organization with an IAM role that has administrative privileges, strive to reduce all permanent privileged role assignments, and conduct periodic entitlement reviews on IAM users, roles and policies.[19]

.001 Create Snapshot

Limit permissions for creating snapshots or backups in accordance with least privilege. Organizations should limit the number of users within the organization with an IAM role that has administrative privileges, strive to reduce all permanent privileged role assignments, and conduct periodic entitlement reviews on IAM users, roles and policies.[19]

.002 Create Cloud Instance

Limit permissions for creating new instances in accordance with least privilege. Organizations should limit the number of users within the organization with an IAM role that has administrative privileges, strive to reduce all permanent privileged role assignments, and conduct periodic entitlement reviews on IAM users, roles and policies.[19]

.003 Delete Cloud Instance

Limit permissions for deleting new instances in accordance with least privilege. Organizations should limit the number of users within the organization with an IAM role that has administrative privileges, strive to reduce all permanent privileged role assignments, and conduct periodic entitlement reviews on IAM users, roles and policies.[19]

.005 Modify Cloud Compute Configurations

Limit permissions to request quotas adjustments or modify tenant-level compute setting to only those required.

Enterprise T1666 Modify Cloud Resource Hierarchy

Limit permissions to add, delete, or modify resource groups to only those required.

Enterprise T1040 Network Sniffing

In cloud environments, ensure that users are not granted permissions to create or modify traffic mirrors unless this is explicitly required.

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Apply user account management principles to limit permissions for accounts interacting with email attachments, ensuring that only necessary accounts have the ability to open or execute files. Restricting account privileges reduces the potential impact of malicious attachments by preventing unauthorized execution or spread of malware within the environment.

.002 Phishing: Spearphishing Link

Azure AD Administrators apply limitations upon the ability for users to grant consent to unfamiliar or unverified third-party applications.

.003 Phishing: Spearphishing via Service

Enforce strict user account management policies on third-party service accounts to control access and limit privileges. Configure accounts with the minimum permissions necessary to perform their roles and regularly review access levels. This minimizes the risk of adversaries exploiting service accounts to execute spearphishing attacks or gain unauthorized access to sensitive resources.

Enterprise T1677 Poisoned Pipeline Execution

Ensure that CI/CD pipelines only have permissions they require to complete their operations. Additionally, limit the number of users who have write access to internal repositories to only those necessary.

Enterprise T1563 Remote Service Session Hijacking

Limit remote user permissions if remote access is necessary.

.002 RDP Hijacking

Limit remote user permissions if remote access is necessary.

Enterprise T1021 Remote Services

Limit the accounts that may use remote services. Limit the permissions for accounts that are at higher risk of compromise; for example, configure SSH so users can only run specific programs.

.001 Remote Desktop Protocol

Limit remote user permissions if remote access is necessary.

.004 SSH

Limit which user accounts are allowed to login via SSH.

.008 Direct Cloud VM Connections

Limit which users are allowed to access compute infrastructure via cloud native methods.

Enterprise T1053 Scheduled Task/Job

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create scheduled tasks on remote systems.

.002 At

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create scheduled tasks on remote systems. In Linux environments, users account-level access to `at` can be managed using `at.allow` and `at.deny` files. Users listed in the at.allow are enabled to schedule actions using at, whereas users listed in at.deny file disabled from the utility.

.003 Cron

`cron` permissions are controlled by `/etc/cron.allow and /etc/cron.deny`. If there is a `cron.allow` file, then the user or users that need to use `cron` will need to be listed in the file. `cron.deny` is used to explicitly disallow users from using cron. If neither files exist, then only the super user is allowed to run cron.

.005 Scheduled Task

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create scheduled tasks on remote systems.

.006 Systemd Timers

Limit user access to system utilities such as 'systemctl' or 'systemd-run' to users who have a legitimate need.

.007 Container Orchestration Job

Limit privileges of user accounts and remediate privilege escalation vectors so only authorized administrators can create container orchestration jobs.

Enterprise T1505 Server Software Component

Enforce the principle of least privilege by limiting privileges of user accounts so only authorized accounts can modify and/or add server software components.[20]

.003 Web Shell

Enforce the principle of least privilege by limiting privileges of user accounts so only authorized accounts can modify the web directory.[20]

Enterprise T1648 Serverless Execution

Remove permissions to create, modify, or run serverless resources from users that do not explicitly require them.

Enterprise T1489 Service Stop

Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service configurations.

Enterprise T1072 Software Deployment Tools

Ensure that any accounts used by third-party providers to access these systems are traceable to the third-party and are not used throughout the network or used by other third-party providers in the same environment. Ensure there are regular reviews of accounts provisioned to these systems to verify continued business need, and ensure there is governance to trace de-provisioning of access that is no longer required. Ensure proper system and access isolation for critical network systems through use of account privilege separation.

Enterprise T1528 Steal Application Access Token

Enforce role-based access control to limit accounts to the least privileges they require. A Cloud Access Security Broker (CASB) can be used to set usage policies and manage user permissions on cloud applications to prevent access to application access tokens. In Kubernetes applications, set "automountServiceAccountToken: false" in the YAML specification of pods that do not require access to service account tokens.[7]

Enterprise T1195 Supply Chain Compromise

Implement robust user account management practices to limit permissions associated with software execution. Ensure that software runs with the lowest necessary privileges, avoiding the use of root or administrator accounts when possible. By restricting permissions, you can minimize the risk of propagation and unauthorized actions in the event of a supply chain compromise, reducing the attack surface for adversaries to exploit within compromised systems.

Enterprise T1569 System Services

Prevent users from installing their own launch agents or launch daemons.

.001 Launchctl

Prevent users from installing their own launch agents or launch daemons.

.003 Systemctl

Limit user access to `systemctl` to only users who have a legitimate need.

Enterprise T1537 Transfer Data to Cloud Account

Limit user account and IAM policies to the least privileges required.

Enterprise T1199 Trusted Relationship

Properly manage accounts and permissions used by parties in trusted relationships to minimize potential abuse by the party and if the party is compromised by an adversary. In Office 365 environments, partner relationships and roles can be viewed under the "Partner Relationships" page.[21]

Enterprise T1552 .007 Unsecured Credentials: Container API

Enforce authentication and role-based access control on the container API to restrict users to the least privileges required.[7] When using Kubernetes, avoid giving users wildcard permissions or adding users to the `system:masters` group, and use `RoleBindings` rather than `ClusterRoleBindings` to limit user privileges to specific namespaces.[8]

Enterprise T1550 Use Alternate Authentication Material

Enforce the principle of least-privilege. Do not allow a domain user to be in the local administrator group on multiple systems.

.002 Pass the Hash

Do not allow a domain user to be in the local administrator group on multiple systems.

.003 Pass the Ticket

Do not allow a user to be a local administrator for multiple systems.

Enterprise T1078 Valid Accounts

Regularly audit user accounts for activity and deactivate or remove any that are no longer needed.

.002 Domain Accounts

Regularly review and manage domain accounts to ensure that only active, necessary accounts exist. Remove or disable inactive and unnecessary accounts to reduce the risk of adversaries abusing these accounts to gain unauthorized access or move laterally within the network.

.003 Local Accounts

Enforce user account management practices for local accounts to limit access and remove inactive or unused accounts. By doing so, you reduce the attack surface available to adversaries and prevent unauthorized access to local systems.

.004 Cloud Accounts

Periodically review user accounts and remove those that are inactive or unnecessary. Limit the ability for user accounts to create additional accounts.

Enterprise T1047 Windows Management Instrumentation

By default, only administrators are allowed to connect remotely using WMI. Restrict other users who are allowed to connect, or disallow all users to connect remotely to WMI.

Source: https://attack.mitre.org/mitigations/M1018