Active Directory Configuration, Mitigation M1015 - Enterprise

Archived: 2026-04-02 12:41:52 UTC

Enterprise T1134 .005 Access Token Manipulation: SID-History Injection

Clean up SID-History attributes after legitimate account migration is complete.

Consider applying SID Filtering to interforest trusts, such as forest trusts and external trusts, to exclude SID-History from requests to access domain resources. SID Filtering ensures that any authentication requests over a trust only contain SIDs of security principals from the trusted domain (i.e preventing the trusted domain from claiming a user has membership in groups outside of the domain).

SID Filtering of forest trusts is enabled by default, but may have been disabled in some cases to allow a child domain to transitively access forest trusts. SID Filtering of external trusts is automatically enabled on all created external trusts using Server 2003 or later domain controllers. [1] [2] However note that SID Filtering is not automatically applied to legacy trusts or may have been deliberately disabled to allow inter-domain access to resources.

SID Filtering can be applied by: [3]

- Disabling SIDHistory on forest trusts using the netdom tool (`netdom trust /domain: /EnableSIDHistory:no` on the domain controller)
- Applying SID Filter Quarantining to external trusts using the netdom tool (`netdom trust /domain: /quarantine:yes` on the domain controller)
- Applying SID Filtering to domain trusts within a single forest is not recommended as it is an unsupported configuration and can cause breaking changes. [3] [4] If a domain within a forest is untrustworthy then it should not be a member of the forest. In this situation it is necessary to first split the trusted and untrusted domains into separate forests where SID Filtering can be applied to an interforest trust

Enterprise T1606 .002 Forge Web Credentials: SAML Tokens

For containing the impact of a previously forged SAML token, rotate the token-signing AD FS certificate in rapid succession twice, which will invalidate any tokens generated using the previous certificate.[5]

Enterprise T1003 OS Credential Dumping

Manage the access control list for "Replicating Directory Changes All" and other permissions associated with domain controller replication. [6] [7] Consider adding users to the "Protected Users" Active Directory security group. This can help limit the caching of users' plaintext credentials.[8]

.005 Cached Domain Credentials

Consider adding users to the "Protected Users" Active Directory security group. This can help limit the caching of users' plaintext credentials.[8]

.006 DCSync

Manage the access control list for "Replicating Directory Changes" and other permissions associated with domain controller replication.[9][7]

Enterprise T1072 Software Deployment Tools

Ensure proper system and access isolation for critical network systems through use of group policy.

Enterprise T1649 Steal or Forge Authentication Certificates

Ensure certificate authorities (CA) are properly secured, including treating CA servers (and other resources hosting CA certificates) as tier 0 assets. Harden abusable CA settings and attributes.

For example, consider disabling the usage of AD CS certificate SANs within relevant authentication protocol settings to enforce strict user mappings and prevent certificates from authenticating as other identifies.[10] Also consider enforcing CA Certificate Manager approval for the templates that include SAN as an issuance requirement.

Enterprise T1558 Steal or Forge Kerberos Tickets

For containing the impact of a previously generated golden ticket, reset the built-in KRBTGT account password twice, which will invalidate any existing golden tickets that have been created with the KRBTGT hash and other Kerberos tickets derived from it. For each domain, change the KRBTGT account password once, force replication, and then change the password a second time. Consider rotating the KRBTGT account password every 180 days.[11]

.001 Golden Ticket

For containing the impact of a previously generated golden ticket, reset the built-in KRBTGT account password twice, which will invalidate any existing golden tickets that have been created with the KRBTGT hash and other Kerberos tickets derived from it. For each domain, change the KRBTGT account password once, force replication, and then change the password a second time. Consider rotating the KRBTGT account password every 180 days.[11]

Enterprise T1552 Unsecured Credentials

Remove vulnerable Group Policy Preferences.[12]

.006 Group Policy Preferences

Remove vulnerable Group Policy Preferences.[12]

Enterprise T1550 Use Alternate Authentication Material

Configure Active Directory to prevent use of certain techniques; use SID Filtering, etc.

.003 Pass the Ticket

To contain the impact of a previously generated golden ticket, reset the built-in KRBTGT account password twice, which will invalidate any existing golden tickets that have been created with the KRBTGT hash and other Kerberos tickets derived from it.[13] For each domain, change the KRBTGT account password once, force replication, and then change the password a second time. Consider rotating the KRBTGT account password every 180 days.[11]

Enterprise T1078 Valid Accounts

Disable legacy authentication, which does not support MFA, and require the use of modern authentication protocols instead.

.004 Cloud Accounts

Disable legacy authentication, which does not support MFA, and require the use of modern authentication protocols instead.
