MANDIANT
NOW PART OF Google Cloud

MANDIANT CONSULTING
WHITE PAPER

Step By Step Through Enterprise Password Resets

The content in this document was originally published in The Defender's Advantage Cyber Snapshot Issue 2.

Incident remediation is comprised of four phases: posturing, containment, eradication and longer-term security enhancements. During an active incident, the most crucial phase is eradication, which encompasses the actions taken to completely eliminate an attacker's access to regain control of an environment. Based on observations during Mandiant Incident Response engagements, eradication commonly includes the coordinated completion of an enterprise password reset.

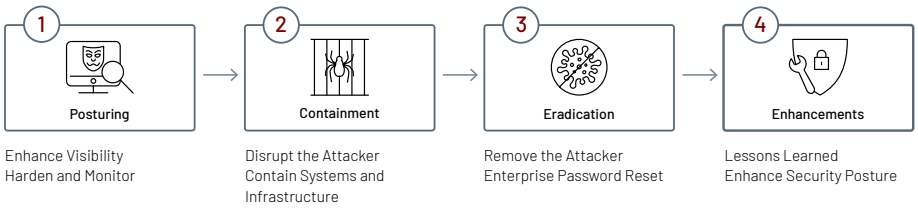


Figure 1. Phases of incident remediation.

Resetting passwords for all accounts in an environment is often a significant undertaking—particularly during an incident response engagement with an active attacker. A well-planned enterprise password reset can be performed with minimal impact. For best results, organizations need to understand what comprises an enterprise password reset event, as well as when, why and how should it be performed.

What an enterprise password reset comprises

An enterprise password reset involves the coordinated resetting of passwords for all accounts in an environment. The goal is to remove an attacker's ability to reuse stolen or compromised credentials. Depending on the scope of an incident, a successful enterprise password reset can include resetting passwords for:

- Domain-based privileged, user and service accounts
- Local accounts
- Application or technology-specific accounts
- API keys/secrets maintained within configuration files
- Cloud-based synchronization accounts
- Accounts that provide binding and integration with cloud-based/SaaS/ third-party components

Given its scale, this activity requires a coordinated effort of collaborative and synchronized teams across an organization. Aside from the security investigative team, stakeholders may include:

- System administrators and engineers
- Help and service desk personnel
- Endpoint and server administrators
- Cloud operations personnel
- Security operations personnel
- Application developers
- Corporate communications
- Internal counsel
- Executive leadership

When and why an enterprise password reset is required

From an attacker's perspective, compromising and maintaining persistence in an environment is vital to completing their objectives. They usually achieve this by compromising as many accounts as possible (including user, service, machine or application-specific accounts). During investigations, Mandiant often identifies evidence where an attacker has accessed or exfiltrated large sets of credentials or password hashes.

One common attack technique that always necessitates an enterprise password reset is the dumping of the NTDS.dit database from an Active Directory domain controller (DC). This file stores information about all domain-based accounts (user service or endpoints), groups and group membership – providing a potential avenue for complete domain-based credential compromise. Once an attacker has escalated privileges and is able to dump the NTDS.dit file, hashes can be extracted to perform pass-the-hash attacks or crack the passwords offline. In addition to NTDS dumping, many other Active Directory attacks, such as those involving DCSync, DCShadow, or Kerberoasting require this reponse.

Mandiant has also observed attackers accessing plaintext files of passwords or secrets stored locally on workstations, file shares, code repositories, local password vaults, cloud storage or other locations.

While these scenarios provide a clear indication that an enterprise password reset should be initiated, there are many scenarios where attackers compromise privileged accounts in an environment. In such scenarios, even without direct evidence of mass credential access, an enterprise password reset is still recommended because an attacker's scope of privileged access may have inferred access to a larger scope of accounts.

Resetting the passwords for only known-compromised accounts leaves open the possibility for an attacker to return using an account not previously identified as compromised during the investigation.

The decision to initiate an enterprise password reset should involve collaboration between the incident investigation and security teams. Once approved by the organization's leadership, the reset planning should be aligned within the overall remediation plan and coordinated with the aforementioned teams.

An enterprise password reset is often the most complex remediation task. Planning for password resets can take time (especially for service and application accounts). Mandiant recommends organizations include plans for conducting mass password resets as part of incident response playbooks and tabletop exercises.

Processes for enterprise password reset

There are several actions that organizations can take to prepare for an enterprise password reset, many of which can be integrated into existing projects relating to asset management, authentication and identity and access management. Dedicated workstreams may need to be established to complete each task.

First, organizations should be sure they understand and have documented all existing authentication mechanisms used to store account and password information, such as Active Directory, SQL databases, cloud identity providers and third-party applications. This inventory will be required to properly scope a coordinated password reset process. This is also a good time to ensure that strong authentication (such as multifactor) and password policies for each identified account type are aligned to best practices and include specific password requirements for standard users, privileged users and service accounts.

When planning an enterprise password reset, it can be difficult to identify and inventory all accounts in the environment, especially privileged and service accounts. Having this information mapped can save valuable time during an active incident. The documentation should include explicit information on the scope of privileged accounts and data required to identify legacy, dormant and stale accounts.

According to NIST, a privileged account/user is one "that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform."[1] Some examples of privileged user accounts may include but are not limited to:

- Accounts within Active Directory domain-based privileged groups including Domain Admins, Enterprise Admins, Schema Admins and Account Operators
- Accounts with the ability to access or manage identities, passwords and security attributes
- Accounts with the ability to modify security configuration settings on endpoints
- Accounts with SSH keys on one or more systems
- Access keys and/or secrets associates with privileged users/accounts
- Accounts that have administrative access to databases, storage repositories or applications that house data deemed sensitive by the organization

1. NIST. Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations.

Service accounts are typically the most challenging to fully correlate and assess the potential impact of a password change. To help assess impact, record the following information and attributes:

- Account name
- Account function/description
- System(s) where the account is used
- Operating system (such as Windows, Linux, Unix, Mac) where the service account is leveraged
- Log-on type performed by the account on identified systems (such as interactive, network, service, batch)
- Level of permissions or scope of access required (such as domain-level, local-level, application-specific permissions)
- Business owner of the account
- Technical owner or custodian of the account
- Manual or automated process for changing the password
  - If manual, note the specific technical process for changing the account password (including updating relevant documentation and configuration settings to reflect the new password)

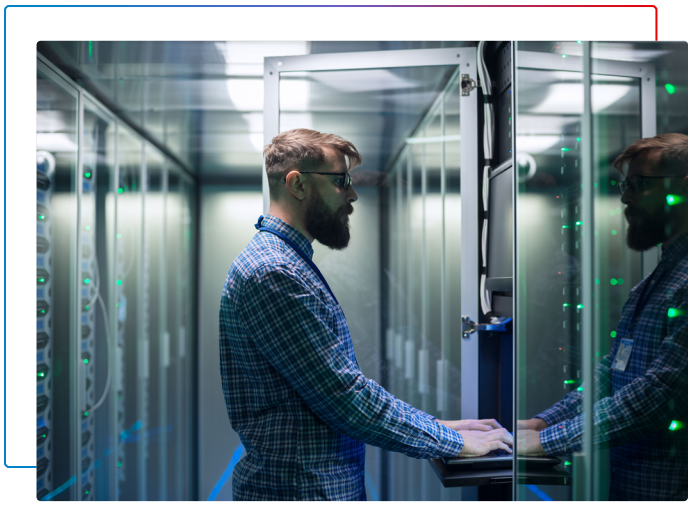
While organizations can perform password reset actions using an automated process, a manual reset for specific accounts may be required. These specific accounts should be tracked and documented to ensure manual resets occur within the same timeframe as the enterprise password reset. Enforcing unique and randomized passwords for local administrative accounts on endpoints will also help ease the burden of an enterprise password reset.

Communication and project management

A dedicated project leader should be designated to coordinate all stakeholders and drive the enterprise password reset to completion. Prior to the enforcement of a password reset, the impacted user base must be notified in a secure manner. When identifying who needs to be contacted before performing an enterprise password reset, organizations should coordinate with external and internal counsel and agree on the language to be included in the communications.

The planning process should also include guardrails for the password reset process, including:

- How new password/multifactor authentication (MFA) onboarding requirements will be communicated to all employees
- How and where users can change their passwords (on-premises, on VPN, only from trusted IP ranges, and other options)



- If MFA onboarding will be part of the password reset process, how secure onboarding of MFA devices/tokens will be conducted
- How long users will have to reset their passwords before their account is disabled
- The process for helpdesk/service desk staff to securely verify users that need assistance with resetting their password/unlocking their account(s)

Checklist items for enterprise password reset (partial)

Every organization should have a checklist of the accounts, secrets and keys that need to be reset. The following components are often in scope for an enterprise password reset:

- **KRBTGT.** This Active Directory account is responsible for encrypting and signing all Kerberos tickets for the domain. When resetting the password for this account, it should be conducted at least twice per domain (ten hours apart) and be performed first within the overall enterprise password reset process.
- **Privileged, User, Service and Local Accounts.** This password reset workstream should be performed across each account in the domain, using the inventory from preparation. Priority should be given to any compromised accounts identified during the investigation, followed by all privileged accounts. Any local accounts on systems accessed by the attacker should be reset.
- **Directory Services Restore Mode (DSRM) Account.** The DSRM account is a break glass local administrator account on every domain controller and requires a manual reset to ensure positive control of Active Directory. Mandiant recommends having a unique DSRM password per domain controller and storing these credentials in a secured privileged account management database or offline vault.

- **Domain Trust Keys.** Trust keys are stored on domain controllers and facilitate the trust relationship between domains in an Active Directory Forest. Resetting the trust key passwords is vital to prevent lateral movement to trusted domains. Depending on the trust type, organizations may need to reset the trust keys on both the trusting and trusted domains.
- **Active Directory Federated Services (AD FS) Service Account.** For a service account used for AD FS, a manual password reset may be required. Mandiant recommends using Group Managed Service Accounts (gMSAs) for the AD FS service account, to ensure automated password rotation occurs repeatedly and on a regular basis. Mandiant also recommends "rolling" the AD FS Token-Signing and Token-Decrypting certificate twice. Our whitepaper, **Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452,**[2] contains details of how to achieve this. If another platform is used to federate identities, then the service account associated with that Identity Provider (IdP) should be reset as well.
- **AZUREADSSOACC Account:** If seamless single sign-on (SSO) is utilized with Azure Active Directory Connect, the "AZUREADSSOACC" computer account is an on-premises account synchronized with Azure AD. To prevent vertical movement between on-premises and cloud services, the Kerberos decryption key for this account should be changed.
- **Azure AD Connect Sync Accounts:** If Azure AD Connect is used, the passwords for the various cloud connector and sync accounts should be changed. This includes the:
  - Azure AD Connector Account
  - Azure AD DS Account
  - ADSync Service Account
- **Rotate Secrets and Keys**: Organizations should prioritize the rotation of compromised secrets and access keys that may have been accessible to an attacker. Mandiant recommends proactively rotating keys and secrets across all platforms and services, even if they have not been identified as compromised during an investigation.

Successful eradication and remediation of an attacker depends on an organization's ability to conduct a timely, well-coordinated enterprise password reset. Mandiant recommendations enable organizations to drastically minimize operational loss and ensure an attacker's access has been eradicated post-incident.

2. Mandiant. Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452.

Read more articles from **The Defender's Advantage Cyber Snapshot.**

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.

MANDIANT
NOW PART OF Google Cloud