Mitigating Pass-the-Hash and Other Credential Theft, version 2

Trustworthy Computing

Microsoft

Legal disclaimer

Acknowledgments

Writers

Patrick Jungles
Mark Simos
Ben Godard
Joe Bialek
Matthew Bucher
Cal Waits
William Peteroy
Thomas Garnier

Contributors

Aaron Margosis
Aaron Tebrink
Adam Stasiniewicz
Al Tieman
Andrea Piazza
Andrew Idell
Arden White
Bill Talbot
Chris Betz
Chris Hale
Chris Jeuell
Cristin Goodwin
Cynthia Sandvick
Danielle Alyias
Dario Brambilla
David Cross
Dirk-Jan van der Vecht
Eric Leonard
Eric Mitchell
Eugene Siu
Georgeo Pulikkathara
Glenn Pittaway
Graham Calladine
Hasnat Naveed
James Noyce
Joe Corey
John Rodriguez
John Wall
Joshua Talbot
Keith Proctor
Lesley Kipling
Mark McIntyre
Mark McRoy
Mark Russinovich
Michael Howard
Michael Poole
Michael Scovetta
Michiko Short
Nate Morin
Nathan Ide
Nicholas DiCola
Patrick Arnold
Paul Cullimore
Roger Grimes
Ted Daley
Tom Stolk
Tony Rice
Tony Ureche
Troy Arwine
William Dixon
Yashar Bahman

Contents

Executive summary

Assume breach: two words that should change the way defenders think about compromise within their organizations. Microsoft investigations of attacks on customers all-too-often reveal success in compromising user and administrator account credentials including domain and enterprise administrator credentials. Technical features and capabilities alone are not enough. The most effective solution requires a planned approach as part of a comprehensive security architecture program.

Credential theft attacks like Pass-the-Hash, are attacks that use a technique in which an attacker captures account logon credentials from a compromised computer, and then uses those captured credentials to authenticate to other computers on the network.

Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques recommended simple, practical, and widely applicable mitigations for every organization to implement. This white paper builds on those recommendations by providing key strategies and mitigations designed to help organizations limit the impact of intrusions that will inevitably occur. It is critical to make proactive investments in the identification of high-value assets, detection, response, and recovery processes.

Along with providing strategic planning recommendations, this paper also summarizes the recent security mitigation features in Windows and Windows Server. Customers are strongly advised to upgrade computers to Windows 8.1 or Windows Server 2012 R2 to benefit from the latest available features and security enhancements. If immediate upgrade is not possible, customers should consider ensuring that important hosts, servers, and domain controllers are upgraded at minimum. Upgrading domain controllers is required to ensure that some mitigations are available.

Although credential theft attacks cannot be solved using a single strategy or mitigation, investments in the identification, detection, response, and recovery processes described in this paper should enable environments to become significantly more resilient to attacks and full compromises. In summary, a preventative attack strategy is not enough, assuming breach and preparing for internal attackers will provide the best level of defense to organizations.

Microsoft is committed to creating guidance and enhancing the Windows platform to help customers ensure the ongoing security of their infrastructure against evolving threats.

Matt Thomlinson

Vice President
Microsoft Security

Introduction

This white paper describes strategies and mitigations that are available with the release of features in Windows 8.1 / Windows Server 2012 R2 to address Pass-the-Hash (PtH) attacks. Prior knowledge of PtH attacks and the previously published mitigations are expected. Additional background information is provided in Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques.

The primary audience for this paper includes system administrators, security architects, and executives who understand IT security concepts and risk management. Its purpose is to enable organizations to create a comprehensive defense plan using the recommended strategies and latest updates to the Windows platform.

The paper begins by providing strategies and considerations to help prevent attacks and overcome challenges related to identification, protection, detection, response, and post–compromise recovery scenarios. In order to gain a more resilient defense, it is important for organizations to protect, detect, respond, and recover in a continuous ongoing effort.

The second half of the paper provides more information about the available technical mitigations that support these strategies, including a brief overview of the previous paper, key points about what has changed since its publication, and features introduced with the release of Windows 8.1 and Windows Server 2012 R2 that help mitigate credential theft. In the "Sample scenarios" section, the reader will find example cases, including helpdesk and administrative support, to understand risks and what mitigations can be used.

Assume breach

Traditional security approaches focus on hardening the outermost network perimeter in an effort to protect against a breach. But even the most stringent perimeter protections can be bypassed by a legitimate user account that has inadvertently been compromised or authorized personnel purposefully acting in a malicious capacity. In the pervasive threat environment that exists today, organizations need to assume this perimeter can be breached and protect key assets against internal as well as external threats.

Assuming breach requires a shift in mindset from prevention alone to containment after breach.

Assuming breach requires a shift in mindset from prevention alone to containment after breach. One reason for this is that shared long-term secrets (for example, privileged account passwords) are frequently used to access anything from the lowest print server to the domain controller. This represents a risk that transcends the technique or protocol being currently used. To achieve the containment of attackers, rapid detection and remediation of initial breaches is required. This level of organizational responsiveness can only be attained through preparation.

This level of organizational responsiveness can only be attained through preparation.

In addition, most threat modeling efforts stop at the point where the attacker gains administrative access, in effect declaring "game over." In reality, organizations must continue to do business, respond to the attack, and plan

to recover from security compromises. According to the New York Times, an often repeated adage among security experts is "*There are two types of companies today, those that have been hacked and those that don't know they've been hacked*." Assumption of breach represents a maturing of defenses to meet this reality and shifts the focus from "if" to "when" an attacker gets inside an organization's network.

Problem Solved?

Effective mitigations require a holistic approach addressing people, processes, and technology.

Although Microsoft continues to improve strategies for detection and provide new features that enable customers to protect against these types of attacks, the problem cannot be solved by implementing a single strategy or deploying a single feature. Credential theft attacks often leverage operational practices or user credential exposure, so effective mitigations require a holistic approach that addresses people, processes, and technology. Also, these attacks rely on stealing credentials after a system compromise to expand or persist access, so organizations need to ensure that breaches are contained rapidly by implementing strategies that prevent attackers from moving freely and undetected in a compromised network. Realistically, mitigations increase the effort that a determined attacker needs to apply to remain inconspicuous. When an effective program is implemented, attackers may find too many barriers and trigger detection mechanisms that could help organizations stop the attack.

Most organizations have unique deployments and specific requirements, so the strategies in this document must be tailored to their needs. When implemented correctly, these strategies and mitigations will ultimately move the bar even higher on the credential theft problem, but attackers may still be able to capture credentials after gaining access to an organization's network. Even in a very restricted environment, a weak link could exist that a determined adversary could take advantage of. In such a case, containment may be possible only if there are several layers of obstacles that restrict an attacker's ability to achieve their goal. The strategies and mitigations described in this paper are meant to enable the deployment of such obstacles, although they may often require a trade-off.

Plan for compromise

Technical features and capabilities alone will not prevent PtH and other credential theft attacks because the attack surface is primarily shaped by operational practices. Therefore, Microsoft encourages its customers to create a comprehensive plan using the security strategies and Windows features prior to deploying a security architecture program. To create resilience to PtH and related attacks, identify and investigate possible threats, and recover from a compromise, customers are encouraged to consider the following specific stages during architecture planning efforts. These stages map to the functions in the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity.

Figure 1: Security stages

- **Identify all high-value assets**
  During planning and prioritizing for security investments, organizations should identify their most valuable resources. Although assets critical to each organization will vary, assets in control of domain or forest consistently have direct influence over all business assets. This makes securing these resources a top priority for any organization. Once these assets are taken into account, the next priority should be to identify which IT assets host the most important business or mission-critical information or service, including proprietary intellectual property and sensitive communications. Identifying accounts that provide access to all these systems is a key exercise during this stage. The more detailed and accurate the identification process, the more effective other strategies will be.

- **Protect against known and unknown threats**
  To protect against these attacks, organizations must undergo a planning exercise in which they closely examine how they currently protect their infrastructure and business assets. Planning for protection is a critical task prior to deploying mitigations, and it requires organizations to understand how users and administrators are authenticated to perform daily tasks. Understanding these requirements will aid in developing a containment strategy that mitigates risk to the organization.

- **Detect PtH and related attacks**
  Detective controls are a critical part of any complete security strategy. Features introduced with Windows 8.1 and Windows Server 2012 R2 provide the ability to detect attacks by defining authorized scope, which creates cases of unauthorized use that can be monitored and alerted. Although detection can be challenging, the mitigations and strategies described in this paper can help detect some anomalies if an attacker attempts to use an account that has constrained scope.

- **Respond to suspicious activity**
  Creating a response strategy will prepare defenders to appropriately respond when suspicious events and activity occurs. If detection mechanisms are triggered, it is possible that a breach has occurred and an attacker may be attempting to move laterally or escalate privileges. False positives will help update the configuration of detection mechanisms to prevent reoccurrence. Updating plans after analyzing attacker behavior, compromised account, and scope of attack may prevent future attacks.

- **Recover from a breach**
  Recovery from credential theft attacks is not trivial in many cases. Although credentials and secrets can be updated with new passwords or new certificates, attackers may have installed rootkits or other malware on the affected computers during the compromise. If so, they may be able to regain access and compromise these accounts again. Detection plays an important role in efficient recovery because it may define the scope of an attack.

The next section examines each of these stages to help with planning and design, prior to deploying mitigations. We recommend here only an approach, along with considerations for these areas that we believe are important.

Strategies

Identify all high-value assets

It is challenging to protect what is not known or understood. A critical first step should be to identify and prioritize high-value IT and business assets. These may be assets that provide access to multiple computers with or without administrative rights, or access to sensitive data or resources, and may allow attackers to perform lateral movement or privilege escalation. See "Prioritize high-value accounts and computers" for examples.

Consider the attacker mindset

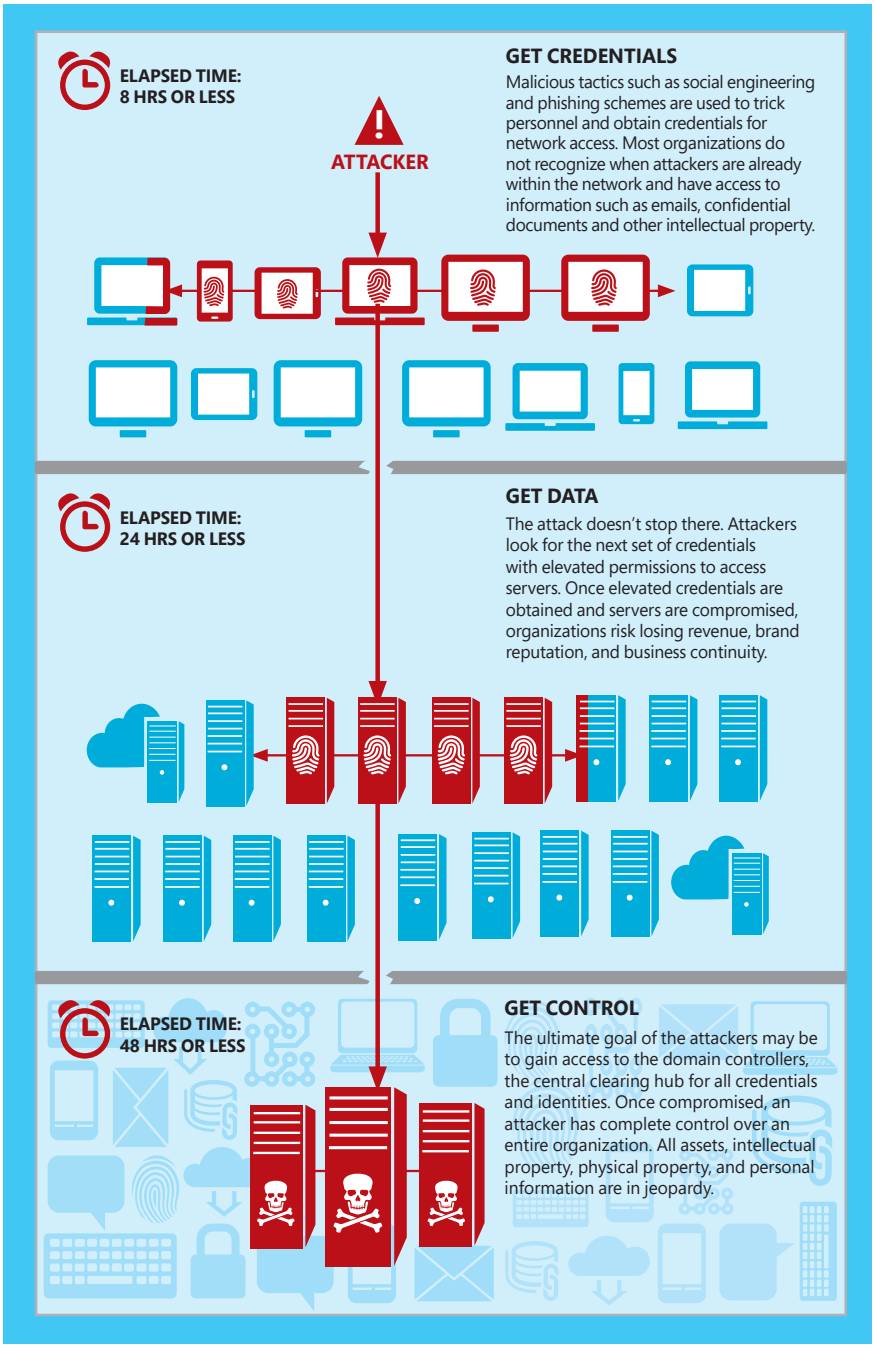
It is important for defenders to understand their network from the attackers' perspective, especially during identification and planning. When attackers gain a foothold on a new network, they ask:

- What are the assets we want access to (domain controller, certificate authority, mail server, file server)?
- Who has access to those assets (who are the administrators on these servers)?
- Where can we get access to those credentials (what servers can we compromise to capture the credentials of a target user or administrator)?

Attackers will see a network as a graph of dependencies between computers and accounts. Their goal is to identify a path between a compromised computer and a target computer, account, or group.

They will start gathering as many credentials as possible, each stolen credential grows the graph and helps them get closer to their goal. This process is repeated multiple times until the target can be reached.

Figure 2:
Attack graph



In many cases, an attack graph will look different from normal usage patterns. This is because the attacker may not care about the legitimate access pattern, only what can be accessed by using a compromised account or resource.

Since the attacker's first step is to understand the target, so too must defenders take a similar approach. By identifying both legitimate and possible unauthorized access patterns, organizations are better able to effectively tailor the strategies described in this paper.

Prioritize high-value accounts and computers

A good place to start when identifying high-value assets is with the accounts and hosts used in the administration of IT assets because these will be targeted by attackers to escalate privileges. Other hosts and services may be targeted for sensitive information or persons of interest. Some examples of targeted high-value accounts and hosts include:

- Domain administrator and domain administrator-equivalent account members of the following security groups:
  - Domain Administrators
  - Enterprise Administrators
  - Schema Administrators
  - Account Operators
  - Backup Operators
  - BUILTIN\Administrators
- Accounts that are used to manage domain controllers. For example, if System Center Operations Manager or System Center Configuration Manager runs on domain controllers or any server that a domain administrator-equivalent account logs on to, then Operations/Configuration Manager administrators are effectively domain administrators.
- When a server that contains domain administrator-equivalent credentials runs on a hypervisor, the hypervisor server administrators are domain administrator equivalents.
- When a server that contains domain administrator-equivalent credentials is connected to an out-of-band management device (such as baseboard management controller or, BMC) that gives physical equivalent access to a domain controller, the administrators of the device are domain administrator equivalents.
- Other accounts that have elevated permissions on numerous systems:
  - Service accounts used for software installation or updates
  - Service accounts used for security scans
  - Service accounts for backup
  - Shared local administrator accounts

For more information...

about locally stored credentials, see Cached and Stored Credentials Technical Overview on Microsoft TechNet. Although this document does not provide extensive background information on these general recommendations, you can find more details on pages 16 through 24 of the Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques white paper.

- Accounts that have access to high-value business assets
  - Email systems
  - File shares
  - Content management systems (such as SharePoint)
  - Other important infrastructure
  - Executives and directors
  - Researchers
  - Administrative assistants
- Hosts that are expected to use high-value accounts
  - Computers used for administration
  - Computers used for support such as helpdesk
  - Patch management servers
  - Security scanners

Identify normal behavior

In order to properly implement mitigations and enable detective controls later, it is also important to identify the current state of existing administrative practices and how other high-value accounts are being used. This may include identifying:

- Who has access to what resource
- How resources are being accessed
- Which applications should be run on high-value hosts

Understanding how these high-value accounts and computers should behave will allow organizations to define cases of unauthorized use. Normal behavior can be monitored for deviation and protected through mitigations.

Protect against known and unknown threats

Organizations need to consider protection holistically to mitigate against credential theft. The focus should be on attacker containment while ensuring that mitigations are deployed in a meaningful and usable manner. To achieve this, it is important to create a containment model and reshape credential use and administrative practices. The following subsection discusses general practices and considerations for architecting a credential theft defense to support this approach, prior to implementing and deploying mitigations.

Architect a credential theft defense

To create environments that are resilient to credential theft, defenders must consider all aspects of credential use and storage. Organizations should limit the availability of credentials throughout the following lifecycle as they are used or stored, and ensure they are transmitted securely.

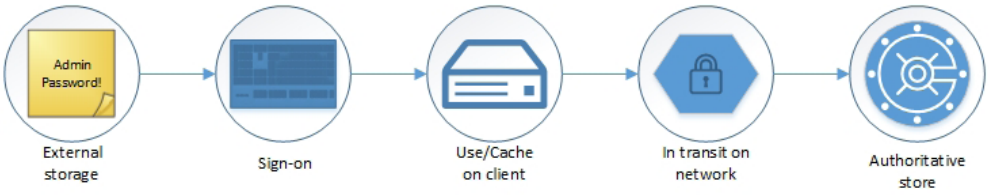


Figure 3: Credentials use and storage lifecycle

- Credentials stored outside of Windows (on sticky notes, in plaintext files, in a credential vault, and so on)
- Credentials used during Windows authentication (for example, on keyboards and in smartcard readers)
- Credentials being used or cached for later use (on clients or servers)
- Credentials in transit over network connections
- Credentials stored on authoritative stores such as domain controllers and local account databases on local computers

> **Note:** Consideration should also be given to any storage systems and devices where copies of the operating systems are stored such as storage of virtual hard drives and backups.

Because the focus of this white paper assumes a certain degree of account compromise, the remainder of this section focuses on containment, administrative practices, and supplemental general recommendations.

The value of containment

Today, large ships are designed with compartments to ensure that any one leak doesn't sink the whole ship. IT environments should similarly be designed so that the compromise of any one or several assets is contained and doesn't lead to a direct loss of confidentiality, integrity, or availability of all assets in the environment.

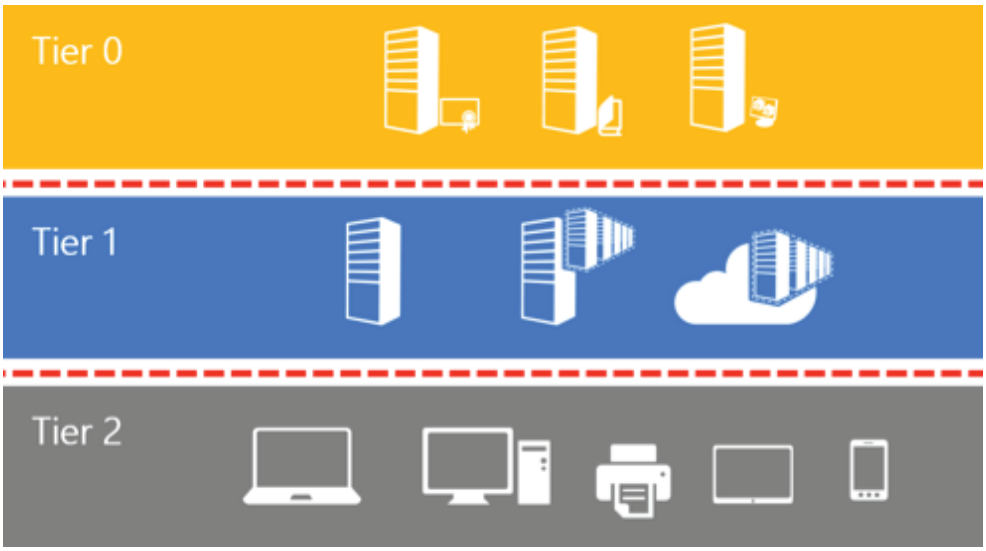
Because Internet-facing and internal hosts may be compromised at any given time, it is critical that organizations design an architecture that will prevent initial compromises and is adept at containing internal lateral movement and privilege escalations. Establishing a strategy to contain such risk can be accomplished using segmentation. Segmentation will limit the privileges, access, and exposed credentials that an attacker may gain by compromising a single or multiple resources.

Segmentation of accounts and networks also enables easier detection of an attacker who tries to remain inconspicuous with captured credentials. This document discusses account segmentation and containment in detail but does not cover network segmentation in depth. For more information on network segmentation, see the Appendix section of this document.

Establish a containment model for account privileges

The following figure provides a simple model for quickly classifying existing resources and setting up zones to limit account usage. This model adapts Biba and Bell-LaPadula hierarchical models to administrative control and is represented by three tiers of administrative privilege. Specific business needs may require other tiers or additional segmentation, but this model can be used as a starting point.

Figure 4: Tier Model



Tier 0 – Forest admins: Direct or indirect administrative control of the Active Directory forest, domains, or domain controllers

Tier 1 – Server admins: Direct or indirect administrative control over a single or multiple servers

Tier 2 – Workstation Admins: Direct or indirect administrative control over a single or multiple devices

Tier definition

The model is intended to prevent an escalation of privilege path for an attacker using stolen credentials and is defined by the following rules:

- Each administrative resource (group, account, servers, workstation, Active Directory object, or application) will be classified as only one tier.
- Personnel with responsibilities at multiple tiers will have separate administrative accounts created for each required tier. Any account that

currently logs on to multiple tiers will be split into multiple accounts, each of which fits within only one tier definition. These accounts will also be required to have different passwords.

- Administrative accounts may not control higher-tier resources through administrative access such as access control lists (ACLs), application agents, or control of service accounts. Accounts that control a higher tier may not log on to lower-tier computers because logging on to such a computer may expose and inadvertently grant control of the account credentials and privileges assigned to that account. Under some specific exceptions, a feature that supports Remote Desktop (RDP) with restricted admin mode could be used without exposing credentials (for example, see "Helpdesk" described in the "Sample scenarios" section of this document).
- Administrative accounts may control lower-tier resources as required by their role, but only through management interfaces that are at the higher tier and that do not expose credentials—for example, domain admin accounts (tier 0) managing server admin Active Directory account objects (tier 1) through Active Directory management consoles on a domain controller (tier 0).

Figure 5 visually depicts the logon restrictions for the tier model.

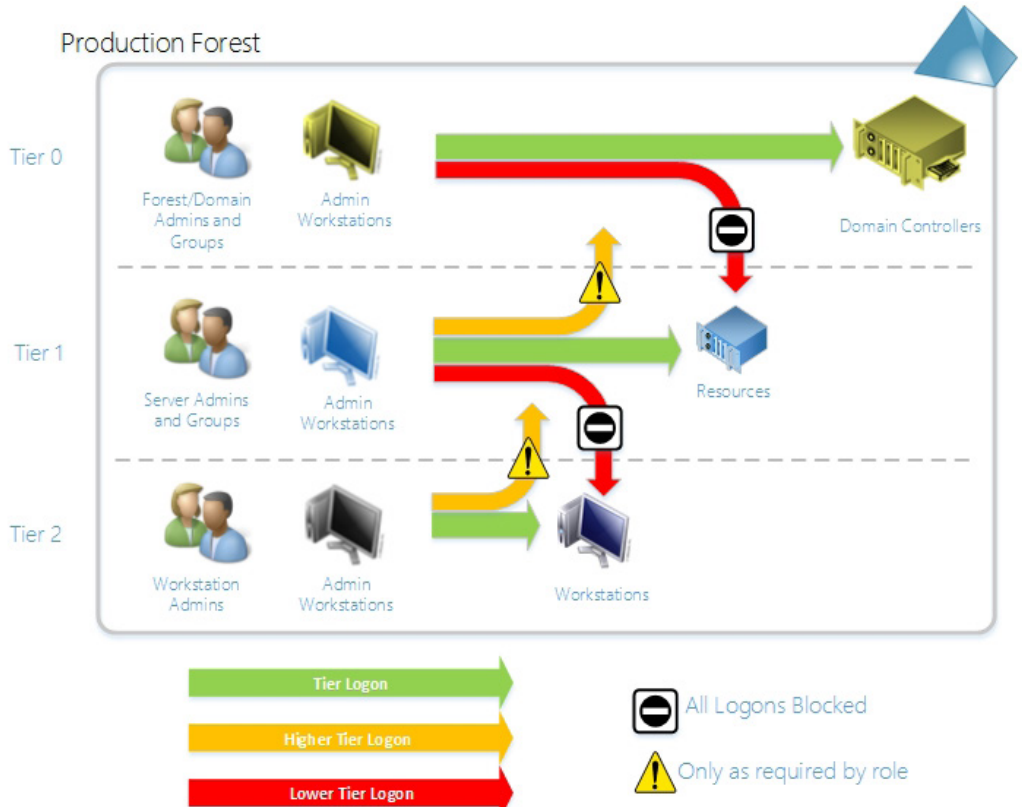


Figure 5: Tier Model-Administrative logon restrictions

Implement administrative practices

Containing credential theft risk for administrative accounts typically requires reshaping administrative practices to limit exposure to attackers. As a first step, organizations are recommended to:

- Limit the number of hosts on which administrative credentials are exposed.
- Limit role privileges to the minimum required.
- Ensure administrative tasks are not performed on hosts used for standard user activities (for example, email and web browsing).

The next step is to implement logon restrictions and enable processes and practices to adhere to the tier model requirements. Ideally, credential exposure should also be reduced to the least privilege required for the role within each tier (that is, isolation of business groups).

Logon restrictions should be enforced to ensure that

- Domain admins (tier 0) cannot log on to enterprise servers (tier 1) and standard user workstations (tier 2).
- Server administrators (tier 1) cannot log on to standard user workstations (tier 2).

  Note: Server administrators should not be added to the domain admin group. Personnel with responsibilities for managing both domain controllers and enterprise servers should be given separate accounts.

Logon restrictions can be enforced with:

- Group Policy Logon Rights Restrictions
  - Deny access to this computer from the network
  - Deny logon as a batch job
  - Deny logon as a service
  - Deny logon locally
  - Deny logon through Remote Desktop
- Authentication policies and silos (described in the "Mitigations" section)
- Selective authentication (if account is in another domain, such as a dedicated admin forest)

In addition, other enterprise solutions should also be considered to manage accounts and restrict access to applications, hosts, and servers:

- Implement temporary admin privileges and passwords.
- Implement mechanisms to rotate password or just-in-time access.
- Implement a dedicated administrative forest.

For more information...

about these policy settings, see User Rights Assignment and Authentication Policies and Authentication Policy Silos on Microsoft TechNet. For more information about dedicated admin forest, or selective authentication, see the Appendix section of this document.

- Implement network segmentation for client, server and domain isolation.
- Implement a physically separated multi-factor authentication solution. See Azure Multi-Factor Authentication for more information.

Harden and restrict hosts for administrative purposes

Any hosts on which administrators enter credentials or perform administrative tasks are entrusted with the privileges associated with the account that is used, even if temporarily. The act of physically typing a password, smartcard PIN, or other verifier, or connecting a physical authentication device grants the credentials' permissions to that computer. The risk of a system should be measured by the highest risk activity that is performed on it, such as Internet browsing, sending and receiving email, or the use of other applications that process unknown or untrusted content.

Administrative hosts include:

- Admin desktop on which credentials are physically typed or entered.
- Administrative "jump servers" on which administrative sessions and tools are run.
- Servers that host applications that need to be administered and are not accessed using RDP with Restricted Admin Mode or Windows PowerShell remoting. See Enable-PSRemoting for more information on Windows PowerShell remoting.
- All hosts on which administrative actions are performed, including those that use a standard user desktop running an RDP client to remotely administer servers and applications.

Create hardened and restricted administrative hosts

Although inconvenient, separate hardened workstations dedicated to users with high-impact administrative credentials may be required to provide a host with a level of security that is equal to or greater than the level of the privileges entrusted to the credentials. Maintaining security against a determined and talented adversary may require additional measures, such as:

Verification of all media in build as clean to mitigate against malware installed in a master image or injected into an installation file during download or storage.

Security Baselines should be used as starting configurations.

- Customers can use the Microsoft Security Compliance Manager (SCM) for configuring the baselines on the administrative hosts.

Secure Boot to mitigate against attackers or malware attempting to load unsigned code into the boot process.

- This feature was introduced in Windows 8 to leverage the Unified Extensible Firmware Interface (UEFI). See UEFI Firmware for more information.

Software restriction to ensure that only authorized administrative software is executed on the administrative hosts.

For more information...

see the "Other Enterprise Security Solution" section in the Appendix

- Customers can use AppLocker for this task to help prevent malicious software and unsupported applications from executing. Additional information is available in the AppLocker Design Guide. For updated information, see the AppLocker Policies Design Guide on TechNet.

Full volume encryption to mitigate against physical loss of computers, such as administrative laptops used remotely. See BitLocker for more information.

USB restrictions to protect against physical infection vectors. See Control Read or Write Access to Removable Devices or Media for more information.

Network isolation to protect against network attacks and inadvertent admin actions. Host firewalls should block all incoming connections except those explicitly required and block all outbound Internet access.

Antimalware to protect against known threats and malware.

Exploit mitigations to mitigate against unknown threats and exploits. See the Enhanced Mitigation Experience Toolkit (EMET).

Attack surface analysis to prevent introduction of new attack vectors to Windows during installation of new software.

- Use of tools such as the Attack Surface Analyzer (ASA) will help assess configuration settings on a host and identify attack vectors introduced by software or configuration changes.

Some of these measures might seem extreme, but public revelations in recent years have illustrated the significant capabilities that skilled adversaries possess to compromise targets.

Considerations for securing forests and domains

A domain or enterprise administrator account has the technical ability to exercise control over all resources on a domain, regardless of whether it operates with malicious or benign intent. This control includes the ability to create accounts; read, write, or delete data; install or alter applications; and erase operating systems. If any administrative host that is used to manage a domain is known to be compromised, the entire domain and forest should also be considered compromised.

Recommended credential management practices

General recommendations provided in this section should be implemented to ensure administrative staff is trained, administrative tasks and actions are visible to security personnel, and administrative operations are usable.

Ensure that users, especially administrators, are well trained

Organizations should design administrative use processes that are effective and secure, then educate administrators on the threats to their accounts and privileges as well as how to use these processes to avoid risk. Comprehensive security practices need to be applied consistently to be effective. Informing and training personnel appropriately increases the chances that they will execute appropriately rather than working around the controls.

Ensure visibility and accountability of administrative practices

Administrative account usage is logged in Windows, but an organization may wish to increase the visibility and control of how these accounts and privileges are used. An organization can use an identity management tool such as Microsoft Forefront Identity Manager (or Identity Manager) to provide managed access to privileged groups through workflows. An organization may also use third-party tools to control and review access to privileged accounts, several of which are described in the Best Practices for Securing Active Directory white paper.

Increasing visibility and control of administrative practices allows organizations to hold individuals accountable and to spot anomalous activity that may indicate compromise.

Establish security configurations

To ensure that a weak security configuration doesn't undermine the credential theft mitigation architecture, recommended security configurations from manufacturers and security vendors should be followed and regularly verified.

Ensure that security configurations are implemented

Windows hosts can use the Microsoft Security Compliance Manager (SCM) for host and domain baselines. Ensure exceptions only as required and after reviewing risks in the tool. Document reasons and review regularly.

Usability as a security feature

Usability is critical to security, processes, and technology. Administrative and maintenance tasks should be designed to be both secure and usable. All systems, processes, and configurations will degrade over time. Systems that are difficult to use will accelerate this degradation process significantly because they create incentives for administrators to find easier ways to accomplish daily tasks, with little or no regard for security.

To establish usability as a security feature

- Watch and follow a sample set of users in their daily tasks to identify their important and frequent duties, what aspects are security sensitive, and how to align security and usability.
- When designing systems, make it a priority to consider usability.
- Measure how many steps it takes to accomplish a task, and automate or eliminate steps.
- Perform user acceptance testing of administrative and security systems with administrators and security personnel.

Detect PtH and related attacks

Detection is an important part of a security strategy because it provides an alert that suspicious activity is happening and the data for investigating and evaluating that activity. Detective controls are a key dependency for proper response and remediation because data is needed to understand what attackers are targeting and the extent of their network reach.

Pass-the-Hash and other credential theft attacks typically consist of two steps: the attacker steals the credentials and then uses them to obtain unauthorized access to resources and extend control over the network. The attacker may also leverage a compromised user (non-administrative) session to obtain access to a resource for which the user has administrative rights and escalate privileges.

Detective controls are more effective on credential use because credential theft detection relies on retrieving events from a compromised computer. An attacker using stolen credentials may trigger suspicious events in a network while accessing resources. Detecting this illicit credential use is possible, but requires separating attacker activity from high volumes of legitimate events.

In most scenarios it is important to prioritize deploying detection for high-value accounts or computers that are more likely to be targeted by an attacker. Note that each network environment is different and high-value accounts are not necessarily just domain privileged accounts; non-privileged domain accounts may also have access to sensitive information.

Detect use of stolen credentials

Attackers who navigate networks with stolen credentials are impersonating valid users, making detection on complex networks difficult. However, they will use these stolen credentials for unauthorized access, which may provide an opportunity for detection.

Detection is most efficient when performed on well-structured networks in which high-value account usage is clearly defined. Every activity that is outside the previously observed or approved usage of a high-value account should be reported for analysis and possible correction of the detection pattern. Detection can also complement mitigations by ensuring they are correctly applied.

Indicators for detecting anomalous activity:

- Where the account was used (source or destination).
- When the authentication was performed (such as when a user is on leave or vacation or outside of working hours).
- Unusual or unexpected account creation (for example, domain accounts created outside of provisioning system or local accounts created on a server).
- Unusual activity performed with the account (for example, settings changed and authentication policy failures).
- Known and unknown malicious executables detected.
- Multiple unrelated high-value accounts used from the same host (for example, domain admin credentials and service accounts used from same host).
- Multiple accounts from different owners authenticating in a short period of time from the same computer in the same session.

- Modification of sensitive objects (for example, a change to the membership of Domain Admins).
- Mismatch between an account used for perimeter access, such as a virtual private network (VPN), and the account used to access resources.

Collect computer events

This section provides a recommended list of events worth collecting from computers for detecting credential theft. Many events are available on different versions of Windows, and it is important to assess which events should be collected for specific environments to enable detection as well as to make response and remediation easier.

Data collection

Events to collect include the following:

Application execution events (on any monitored computer)

Event ID 4688 - A new process has been created.
Key fields: Account Name, New Process Name

Authentication events (on any monitored computer)

Event ID 4648 - A logon was attempted using explicit credentials.
Key fields: Account Name (Subject), Account Name (account whose credentials were used), Process Name

Event ID 4624 - An account was successfully logged on.
Key fields: Account Name, Logon type

Kerberos events on domain controllers

Event ID 4769 - A Kerberos service ticket was requested.
Key fields: Account Name, Service Name, Client Address

Event ID 4768 - A Kerberos authentication ticket (TGT) was requested.
Key fields: Account Name, Service Name, Client Address

Event ID 4776 - The domain controller attempted to validate the credentials for an account.
Key fields: Logon Account, Source Workstation

Authentication policies and authentication policies silos events on domain controllers

In Applications and Services logs at Microsoft\Windows\Authentication.

Under **ProtectedUserFailures-DomainController**
Events generated when an account that is a member of the Protected Users security group tries to use blocked authentication options.

- **Event ID 100** – NLTM usage attempted.
- **Event ID 104** – DES or RC4 attempted for Kerberos Authentication.

Under **AuthenticationPolicyFailures-DomainController**
Events that are generated when an account is used outside of the allowed authentication policy silos.

- **Event ID 101** – NTLM usage attempted.
- **Event ID 105** – Kerberos authentication from a particular device was not permitted.
- **Event ID 106** – The user or device was not allowed to authenticate to the server.
- **Event ID 305** – Kerberos TGT request did not meet access control restrictions.
- **Event ID 306** – User, device or both do not meet the access control restrictions.

Detect LSA plug-ins and drivers that fail to run as a protected process

If audit mode is enabled for the Local Security Authority Subsystem (LSASS), an event will be generated when Lsass.exe attempts to load an unauthorized driver. See Configuring Additional LSA Protection on TechNet for details.

In Applications and Services Logs\Microsoft\Windows\CodeIntegrity

- **Event ID 3065**: Code integrity check determined that a process attempted to load a particular driver that did not meet the security requirements for Shared Sections. However, due to the system policy that is set, the image was allowed to load.
- **Event ID 3066**: This event records a code integrity check that determined that a process (usually lsass.exe) attempted to load a particular driver that did not meet the Microsoft signing level requirements. However, due to the system policy that is set, the image was allowed to load.

Other events

Systems running applications to restrict software, monitor system changes, antimalware, or other applications that may provide relevant information on PtH and related attacks should also be collected and observed. Access logs for supporting infrastructure, such as firewalls and VPNs, should be monitored. Organizations should evaluate what other software and infrastructure events are relevant when implementing a detection strategy. This information will be invaluable when investigating attacks and successful breaches.

Organizations using Azure Active Directory (AAD) can also benefit from machine learning and other geo-location detection of malicious activities for AAD cloud accounts. See Azure Active Directory Identity and Access Management for the Cloud for more information.

Manage event collection and alerts

Multiple options exist for centralized event log collection and management, including the following.

- Windows Event Collector
- Audit Collection Services (ACS)

Third-party solutions such as security information and event management (SIEM) solutions may provide agents for collection and alerting for specific events. See the Appendix for more information.

Log collections should be enabled for as many computers as possible and configured to push the events from these computers quickly. For example, the Windows Event Collector could be configured with a latency time of 0 to ensure that events are sent as soon as possible to the collector.

Respond to suspicious activity

A key element of a comprehensive security strategy is the ability to respond to suspicious activity and ensure that the right resources are rapidly engaged to evaluate, prioritize, investigate, and act on events. Some alerts may warrant immediate response, while others may be prioritized at a lower level to ensure that resources are reserved for the most important events.

Microsoft recommends integrating the following elements in an incident response process:

- Regularly update protection and detection mechanisms to limit false positive alerts from reoccurring.
- After each significant security event or compromise, update protection and detection mechanisms to prevent future attacks from reoccurring.
- After a compromise, continue with close observation of affected hosts and accounts to ensure that the attacker is not able to regain access.
- If a compromise has occurred, proceed to recovery plans and ensure that attack vectors are properly addressed.
- Consider delaying recovery efforts to track attacker behavior and uncover the intent or attack details. This information could lead to a better recovery strategy.

Investigate attacks

The most important part of developing an investigation strategy is to obtain enough details about an attack to determine the scope of a breach. Adversaries typically obtain a keychain of valid domain credentials in an attack and any individual credential compromise could be a sign of a larger problem.

Attackers typically need to periodically reacquire credentials as their keychain of stolen credentials will naturally degrade over time due to password changes and resets. Because of this, attackers frequently maintain a foothold by installing backdoors and maintaining credentials from a number of computers in the environment. This supports both the re-acquisition of credentials and other functions like remote access. Tracing the access chain backwards may lead to the discovery of other computers involved in the breach. Sometimes an attacker's presence is limited to a single compromised host. Other times it is a large number of compromised hosts harvesting credentials and a smaller number of hosts "managing" these compromised hosts.

When investigating activity on compromised hosts, customers may want to use a feature introduced with Windows 8.1 and Windows Server 2012 R2 to enable command-line auditing. Command-line auditing may provide further insight into what an attacker is doing in each host. This feature provides command-line information for every process logged in plain text in the security event log as part of the Audit Process Creation event 4688, A new process has been created, on the workstations and servers on which this policy setting is applied.

Note: For security and privacy reasons, Microsoft does not recommend enabling this feature permanently. When this policy setting is enabled, any user with read access to security events will be able to read the command-line arguments for any successfully created process. Command-line arguments can contain sensitive or private information, such as passwords or user data.

This feature can be enabled for the machine or user by setting Software\Microsoft\Windows\CurrentVersion\Policies\System\Audit\ProcessCreationIncludeCmdLine_Enabled to 1 or through a policy change.

For more information...

See Command Line Auditing onMicrosoft TechNet.

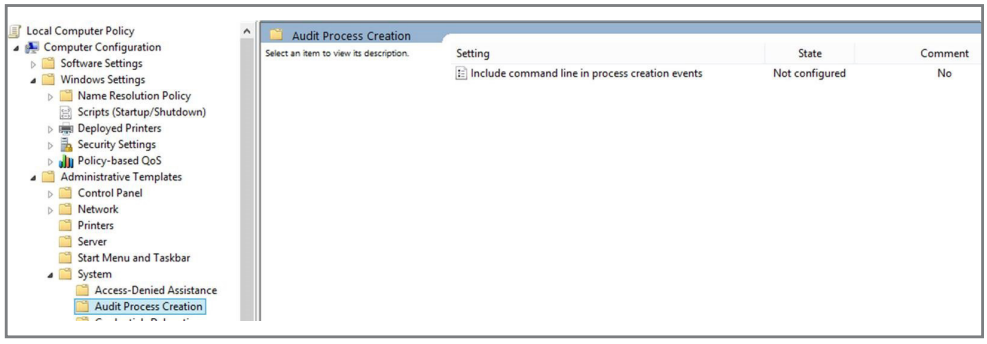


Figure 6: Include command line in process creation events.

Recover from a breach

After a successful PtH attack, the highest priority should be to recover control over the compromised assets. Unfortunately, the traditional disaster recovery approach of restoring from a recent backup is often ineffective, because attacks are not typically detected immediately. This section provides considerations for recovering accounts and domain integrity when restoring from backup is not viable.

This paper does not discuss post-incident recovery or host recovery in depth.

Recover accounts

In the event of a compromise, action must be taken to recover the control of compromised accounts. These practices are only effective if an organization has high confidence that the domain has not been compromised.

The following recovery practices have limitations and should be carefully evaluated before they are executed. It is also imperative that the root cause of a breach be identified in order for the following recommendations to be effective and prevent attackers from regaining access.

Changed compromised account passwords. The idea is straightforward: the adversary has user and computer credentials, so changing the affected accounts' passwords reclaims control of these accounts.

Methods:

- Set passwords to require change at next logon. One benefit of this action is that other types of credentials such as smartcards will be unusable until passwords are reset.
- Manually change passwords in Active Directory Domain Services (ADDS). Additional use of the previously compromised credentials will result in failed logon attempts.
- Consider resetting computer account credentials if a computer has been compromised.

  Note: Computer account passwords are used to prove the computer and the domain controller identity to each other. These secrets may be used on attacks that restrict access based on the machine account (for example authentication policies). For more information, see Reset a Computer Account.

- Reset NT hashes for smartcard-enforced accounts by disabling and re-enabling the account attribute Smart card is required for interactive logon.

For more information, see Settings for default local accounts in Active Directory.

Considerations:

- This is only effective against future authentications. Resources such as shares and named pipes that were accessed with the compromised credentials will remain available until the logon session that granted access is terminated.
- If the host is offline during this practice, cached logon password verifiers can still be used locally.

- This action will likely inform the attacker that a breach has been detected.
- The attacker can persist on a compromised host by using keystroke logger or other malware, and may be able to steal the new password.
- The attacker can persist in the context of the user by using malware installed in the user's profile.

Disable an account and remove group memberships. The idea is to restrict or remove the privileges associated with the compromised account.

Methods:

- Disable the account in Active Directory Domain Services.
- Remove the account from Active Directory security groups and any local security groups.

Considerations:

- This is only effective against future authentications.
- When the security token is created, the group membership is hard-coded in the token. Therefore, any process that is already running with that token will run with the original permissions of the account even after the account is removed from the security group.
- This action will likely inform the attacker that a breach has been detected.

Restore the integrity of the domain and forest

Because many existing implementations of Active Directory Domain Services have been operating for years at risk of credential theft, organizations should assume breach and consider the very real possibility that they may have an undetected compromise of domain or enterprise administrator credentials. An organization that suspects domain compromise should consider the use of professional incident response services.

Recovering the integrity of a large and complex IT environment is a particularly challenging undertaking because it is a complex system composed of many individual nodes that are each complex and difficult to assess or clean quickly. An organization that is planning any full recovery will need to address several requirements, including the following:

Disrupt an adversary's current operation. Removing the elements of control that an adversary can implant with domain administrator access is a daunting task that requires some incident details. In some scenarios a customer might not want to immediately disable an attacker's account so that they can better understand the attacker's actions or intent. In other scenarios, a customer might want to immediately block a compromised account to observe the use of another account or stop the current attack to prevent further damages.

> **Note:** If a domain controller has been compromised, it is possible that the KRBTGT password hash has been stolen and is now being used by an attacker to obtain access. In this case, it may be required to plan and execute a reset of the key stored in the password hash for the KRBTGT account. This action

requires planning because it can disrupt all authentication. See "Reset the KRBTGT account" at the end of this section for more information

Prevent the same attack from working again. Adversaries typically use techniques that were successful in the past and then move to other available techniques. The use of backdoors and other attacks may also allow an attacker to regain access.

Ultimately, there are two valid approaches to achieve meaningful recovery of accounts in large, complex environments:

Tactical recovery. A short-term operation designed to disrupt a known adversary operation currently present in an environment. This approach does not guarantee recovery, but can be effective at breaking an adversary's link to controlling an environment and preventing additional operations in a compromised state. A tactical operation relies on the following factors to be successful:

- Useful intelligence on the adversary presence. Disrupting an adversary operation requires an understanding of how the adversary operation is configured. Missing or overlooking an element of redundant adversary control can negate the effect of the operation. A tactical recovery typically requires the involvement of an experienced investigative team.
- A stealth operation that the adversary is unaware of. Adversaries frequently monitor email and other communications and are likely to modify their presence on a network to defeat a cleanup operation.
- A properly scoped defender operation. The scope has to be comprehensive enough to be effective and small enough to be executed in a short period of time, which is a difficult balance to achieve.

Strategic recovery. A long-term plan that consists of multiple operations focused on recovering integrity at a high assurance level, often for a large number of assets. Strategic recoveries can take months to plan and fully execute. A strategic recovery plan will need to address the following factors:

- Risk of migration. An organization should carefully conduct migrations to avoid transitioning adversary malware implants and compromised accounts to a new clean environment during the migration of legitimate users. The organization should also assess the way that migration tools and processes are designed and operated to help ensure that an adversary cannot traverse into the new organization by exploiting those tools or processes.
- Risk of coexistence. Organizations that are moving resources to a new environment will frequently need the ability for users to connect with the compromised environment to perform some job tasks until all resources and users are fully migrated. Organizations must take care to ensure that any credentials that are exposed to the old environment cannot be used to gain access to the new environment.
- Planned end State. Organizations should consider the relative cost and benefit of the options for the strategic recovery end state. These range from only recovering only the current forest to separating business critical functions into a separate forest to creating and migrating to a new forest (and many other variations). Organizations will have to consider their options in light of many factors including the business value

of assets in the forest, available budget, ability to separate business critical resources from lower value resources, and their ability to detect and respond to incidents.

Reset the KRBTGT account

The KRBTGT account stores a secret that is used by the Kerberos service to issue and validate ticket granting tickets (TGTs) in a domain. In a compromised domain, an attacker may use publicly available tools to steal this secret stored in the KRBTGT account and generate arbitrary valid TGTs. This technique allows an attacker to obtain long-term access to the infrastructure as any user, including domain administrators, if organizations do not reset the KRBTGT account after compromise. Initiating a password reset for the KRBTGT account will instruct the system to generate a new random key for this value. This action will invalidate the currently issued Kerberos TGTs but can also cause authentication errors throughout the domain and forest, so a planned approach is advised. For more information see KRBTGT account.

Mitigations

This section discusses previously recommended mitigations, platform enhancements, and features introduced since Windows 8.1 and 2012 R2. Readers are advised to review this entire section prior to implementing mitigations.

Updates

The previously referenced white paper, Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques, provides some simple, practical, yet effective mitigations that most customers could implement without any major changes to their infrastructure.

The previously recommended mitigations were ranked by priority. The first mitigation advises customers to protect high-privileged domain accounts, the second to protect the local administrator account, and the last to use the local Windows Firewall to restrict inbound access from unauthorized computers or applications. Improvements in Windows 8.1 and Windows Server 2012 R2 support these mitigations through the use of new functionality.

The three mitigation categories are shown in the following tables.

Mitigation 1: Restrict and protect high-privileged domain accounts

Objective	How	Outcome
This mitigation reduces the risk of administrators inadvertently exposing privileged credentials to higher risk computers.	Restrict domain and enterprise admin accounts from authenticating to less-trusted computers. Provide admins with accounts to perform administrative duties. Assign dedicated workstations for administrative tasks. Mark privileged accounts as "sensitive and cannot be delegated." Do not configure services or schedule tasks to use privileged domain accounts on lower trust computers.	An attacker cannot steal credentials for an account if the credentials are never used on the compromised computer.

Prior to Windows Server 2012 R2, this mitigation could not technically be enforced at domain controllers. Restricting privileged accounts from authenticating to less-trusted computers can now be accomplished through authentication policies and silos. This mitigation requires domain controllers to be upgraded because this functionality cannot be backported to previous versions of Windows Server. This mitigation employs Kerberos policies and requires administrators to use the Protected Users group that allows only Kerberos authentication and provides added security to the accounts it contains. See "Authentication policies and silos" for more information, considerations, and feature limitations.

Mitigation 2: Restrict and protect local accounts with administrative privileges

Objective	How	Outcome
This mitigation restricts the ability of attackers to use local administrator accounts or their equivalents for lateral movement PtH attacks.	Enforce the restrictions available in Windows Vista and later versions to prevent local accounts from being used for remote administration. Explicitly deny network and Remote Desktop logon rights for all administrative local accounts. Create unique passwords for local accounts with administrative privileges.	An attacker who successfully obtains local account credentials from a compromised computer will not be able to use those credentials to perform lateral movement on the organization's network.

The release of Windows 8.1 introduced two security identifiers (SIDs) to help identify the local administrator accounts and local accounts that are members of the local administrators group. This functionality allows administrators to use Group Policy to easily deny network and Remote Desktop logon rights for these accounts without knowing the corresponding account names. This feature has also been released for Windows 7, Windows 8, Windows Server 2008 R2 and Windows Server 2012.

Mitigation 3: Restrict inbound traffic using Windows Firewall

Objective	How	Outcome
This mitigation restricts the ability of attackers to initiate lateral movement from a compromised workstation by blocking inbound connections.	Restrict all inbound connections to all workstations except for those with expected traffic originating from trusted sources, such as helpdesk workstations, security compliance scanners and servers.	An attacker who successfully obtains any type of account credentials will not be able to connect to other workstations.

Although no recent features have updated this mitigation, Microsoft strongly recommends that customers implement network isolation, which may reduce the need for managing local firewall rules. This information does not replace or change the previously recommended mitigation because certain devices, such as mobile computers, may not always be in an organization's protected environment. We continue to strongly encourage the use of Windows Firewall to restrict inbound access to trusted hosts, services and applications.

Windows features

Windows 8.1 and Windows Server 2012 R2 include a number of features that customers can use to restrict and control exposure of credentials. Some of the features described here can only be used effectively in fully upgraded environments, some are available in mixed environments with domain controllers running Windows Server 2012 R2, and a few are available in legacy environments running earlier versions of Windows. The "Applicability summary for mitigations" section explains these options in detail. These features are natively available on Windows 8.1 and Windows Server 2012 R2 and are available through Windows update for other versions. For more information, see the Microsoft Security Advisory 2871997: Update to Improve Credentials Protection and Management.

These features and platform enhancements are designed to help prevent an attacker from stealing or using stolen credentials.

FEATURE	THEFT	USE
Logon restrictions with new well-known security identifiers (SIDs)		✓
Enforce credential removal after logoff	✓	
Remove LAN Manager (LM) hashes from LSASS	✓	
Remove plaintext credentials from LSASS for domain accounts	✓	
Restricted Admin mode for Remote Desktop	✓	
Protected Users security group	✓	
Authentication Policies and Silos	✓	✓
LSA protection-theft	✓	
Disable Automatic Restart Sign-on (ARSO) Routine	✓	

Logon restrictions with new well-known security identifiers (SIDs)

Available on:
Windows 7, Windows 8, Windows 8.1, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2

Domain requirements:
None

Security identifiers (SIDs) uniquely identify individual users, groups, and other security principals for access control and management purposes. This feature adds two new well-known SIDs that can be used to select local accounts:

S-1-5-113 – Local account

S-1-5-114 – Local account and member of Administrators group

With earlier versions of Windows, customers had to select local accounts explicitly when applying network logon restrictions, which often meant deploying scripts or other tools to identify local accounts and groups. Organizations can use the new SIDs to block network logon for local users and groups by account type, regardless of what the local accounts are actually named (for example, deny access to the computer from the network in Mitigation 2). This feature helps prevent an attacker from using stolen local account credentials.

Feature limitations

This feature does not help discover local account or groups created on computers. It is only meant to mark such accounts to enable the use of Group Policy Objects (GPOs) to control the capabilities of local accounts).

Enforce credential removal after logoff

Available on:
Windows 7, Windows 8, Windows 8.1, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2

Domain requirements:
None

Previous Windows releases were susceptible to session leaks that allowed credentials to remain in LSASS after users signed out. This susceptibility was particularly a problem when applications impersonated another account and failed to terminate the session after closing, which allowed credentials to remain in memory after users had initiated the logoff process. New mechanisms have been implemented to eliminate session leaks in LSASS, thereby preventing credentials from remaining in memory. This feature helps prevent credential theft.

Feature limitations

This feature does not attempt to clean up all credentials stored locally after a user logs off—only credentials stored in LSASS memory. There are still several of other application and user credentials that an attacker could obtain from a compromised computer. Microsoft encourages and supports secure development of applications (see Security Development Lifecycle), but attack vectors will depend on how applications handle or cache access credentials.

Remove LAN Manager (LM) hashes from LSASS

Available on:
Windows 7, Windows 8, Windows 8.1, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2

Domain requirements:
None

Earlier versions of Windows stored LAN Manager (LM) hashes in LSASS for passwords that were compatible with LM (up to 15 characters long containing only ASCII characters), even if the Group Policy setting Network Security: Do not store LAN Manager hash value on next password change prevented LM hashes from being stored in the local Security Accounts Manager (SAM) database or Active Directory Domain Services (AD DS) database. LM hashes can be easily brute-forced to obtain a plaintext password if an attacker manages to obtain these hashes from LSASS during a session. These legacy hashes are no longer stored in LSASS. This feature helps prevent credential theft.

Feature limitations

Although LM hashes have been removed from the platform by default, this change does not prevent an attacker from obtaining plaintext passwords through other means such as keystroke logging or brute-forcing a captured NT hash. Although NT hashes are significantly more secure, they can still be brute-forced in a matter of hours if the corresponding password is weak.

Remove plaintext credentials from LSASS for domain accounts

Available on:
Windows 7, Windows 8, Windows 8.1, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2

Domain requirements:
None

By default, versions of Windows prior to Windows 8.1 or Windows Server 2012 R2 stored plaintext credentials in LSASS for domain users while they were logged on. Attackers found ways to extract the plaintext credentials from LSASS memory. This platform enhancement removed plaintext credentials for domain accounts from LSASS after logon. This feature helps prevent credential theft.

The following diagram summarizes these changes.

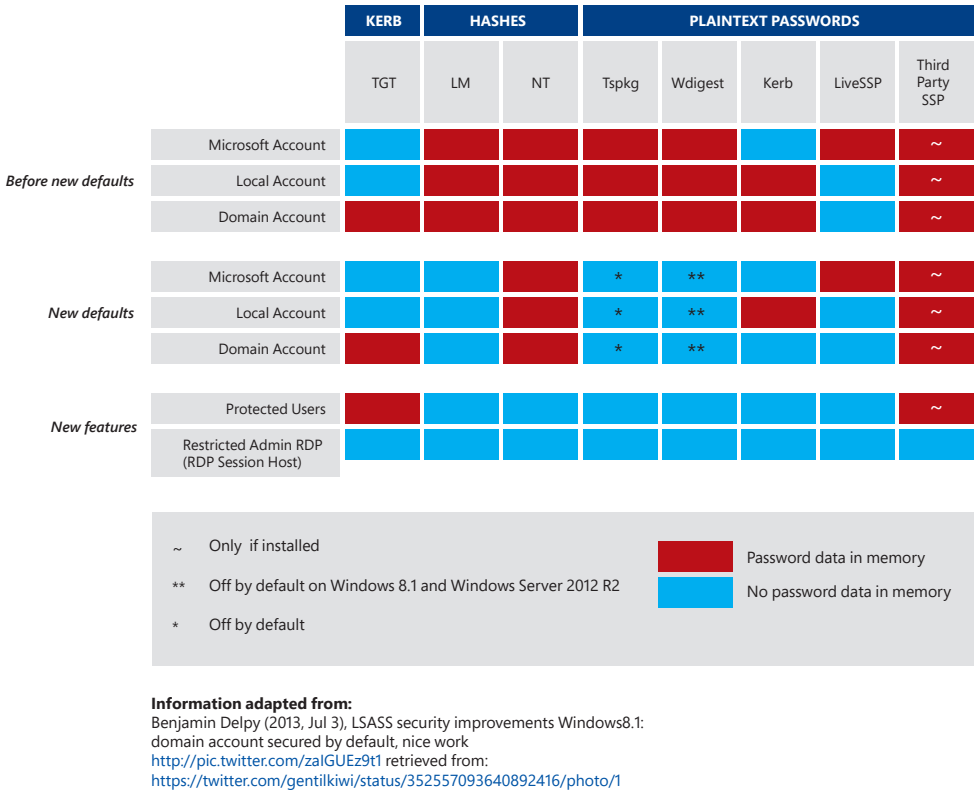


Figure 7: Remove plaintext credentials from LSASS for domain accounts

Information adapted from:
Benjamin Delpy (2013, Jul 3), LSASS security improvements Windows8.1: domain account secured by default, nice work
http://pic.twitter.com/zaIGUEz9t1 retrieved from:
https://twitter.com/gentilkiwi/status/352557093640892416/photo/1

Feature limitations

Microsoft ID security support provider (LiveSSP) and third-party security support providers (SSPs) may still require the storage of plaintext passwords. If the Terminal Services Package (Tspkg) or Windows Digest Authentication (Wdigest) are enabled on the computer, plaintext credentials for these services will also be required in LSASS. Updates to support this functionality for Windows 7, Windows 8, Windows Server 2008 R2, and Windows Server 2012 were released with the Microsoft Security Advisory 2871997. This update allows users to disable Wdigest, but it does not disable it by default. A "Fix it for me" package can be used to change the UseLogonCredentials registry key to disable WDigest.

In addition, Kerberos requires plaintext credentials to request a TGT, so the plaintext password may still be kept in LSASS during Kerberos pre-authentication until a TGT is acquired. If Kerberos encounters problems during TGT negotiation, plaintext credentials will remain in LSASS after user logon so the computer can continue its request for a TGT. This scenario occurs when a user logs on while disconnected from the network and is authenticated with a cached logon password verifier (CLPV) instead of a live domain controller. Hashes and TGTs remain in memory and could be used by an attacker.

Restricted Admin mode for Remote Desktop Connection

Available on:
Remote Desktop Client support for Restricted Admin mode is available on Windows 7, Windows 8, Windows 8.1, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. Remote Desktop service (RDP Session Host) support for this feature is only available on Windows 8.1 and Windows Server 2012 R2.

Domain requirements:
None

System administrators and helpdesk personnel often use Remote Desktop Protocol (RDP) to provide remote assistance to computer users. If a computer has been compromised by an attacker, connecting to the compromised computer remotely with RDP creates a risk that the attacker can obtain the remote user's credentials and use them to access other systems. To mitigate this risk, RDP has been updated to support authentication without providing credentials to the RDP Session Host. This feature is limited to accounts that have administrative rights on the remote host and supports both NT LAN Manager (NTLM) and Kerberos protocols for authentication. This feature helps prevent credential theft on the remote host.

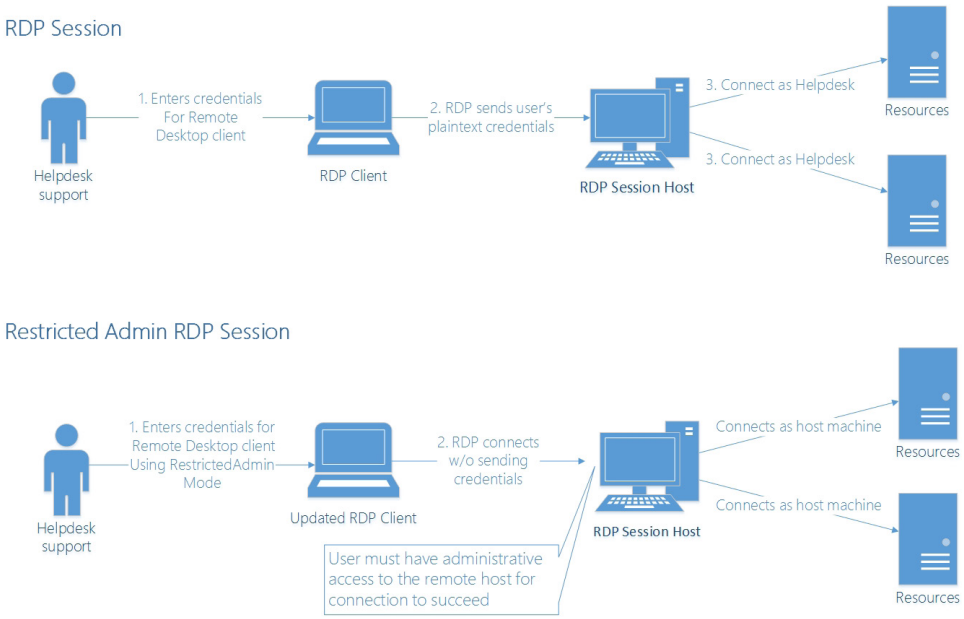


Figure 8: Remote Desktop Restricted Admin

After applying the Windows updates 2973351 and 2975625, this feature is disabled by default and can be enabled through a GPO. Customers can enable and configure Restricted Admin mode by creating registry key settings in HKLM\System\CurrentControlSet\Control\Lsa\:

- The DisableRestrictedAdmin value (REG_DWORD) can be used to enable RDP with Restricted Admin mode.
  - Setting this value to 0 will enable the Restricted Admin mode functionality for remote clients connecting to this computer.
  - Setting this value to 1 can be used to explicitly disable this functionality.
- DisableRestrictedAdminOutboundCreds value (DWORD) is used to disable the ability of a user in a Restricted Admin mode RDP session from automatically authenticating to remote resources using the local machine account. If Restricted Admin mode is enabled, this functionality is enabled by default.
  - Creating this value and setting it to 1 will disable the use of the machine account credentials for outbound connections in this mode.

To use Restricted Admin mode, a parameter to the Remote Desktop client application must be supplied on the command line (mstsc.exe / RestrictedAdmin) or by applying a Group Policy setting to the client to enforce it on all RDP connections from this computer:

Computer Configuration\Administrative Templates\System\Credentials Delegation\Restrict delegation of credentials to remote servers

Restricted Admin Mode causes the client application to perform a Kerberos authentication using a service ticket to the remote host or a network logon

For more information...

see What's New on Remote Desktop Services in Windows Server

challenge-response with the NTOWF function (NT Hash). After authentication, the remote session for the helpdesk support staff (administrator) will not have respective account credentials in LSASS because they were not supplied to the remote host during the logon process. Because the administrator's own credentials are not supplied to the remote host during authentication, any attacker who has compromised the host will not have access to them (unless entered manually by the administrator during the session).

Any actions the administrator performs in this mode will use the host's computer account by default, so the administrator will only have access to network resources that the computer account is allowed to access. Network resources required while using this feature (for example, file shares) need appropriate permissions assigned to the computer accounts or groups that contain them. This feature helps protect against credential theft by allowing management of computers without exposing credentials.

If the target host does not support this feature, administrators will get the following message: "The remote PC doesn't support Restricted Administration mode."

Feature limitations

Because Restricted Admin Mode accepts standard Kerberos or NTLM authentication on the remote host instead of requiring plaintext credentials, enabling this feature can create additional risk in an environment in which security best practices are not being followed. An attacker could use a modified Remote Desktop client to gain access to a host using this feature, provided that the attacker has network connectivity and credentials (TGT or account name with associated NT hash) for an account with administrative permissions on the host.

Following security best practices such as those described in this paper and the previously referenced white paper Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques can help mitigate these limitations and significantly reduce the risk that attackers can gain access to administrative credentials. Nevertheless, administrators should be aware of the potential risk that Restricted Admin Mode might introduce if used in an environment without best practices and other mitigations that limits the availability of credentials to attackers.

Protected Users security group

Client side protection available on: Windows 7, Windows 8, Windows 8.1, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2.

Available on:
Windows 8.1, Windows Server 2008 R2

Domain requirements:
Windows Server 2012 R2 Domain Functional Level (DFL), which requires all domain controllers to be upgraded to Windows Server 2012 R2.

The new Protected Users security group enables administrators to restrict authentication to only the Kerberos protocol through group membership.

Members of the Protected Users group cannot authenticate using NTLM, Digest Authentication, or CredSSP. Users joined to this group will not use cached logon password verifiers causing a logon event on the domain controller for every interactive authentication. For more information on using events for detection, see "Detect PtH and related attacks."

Members of this group are also restricted to strong encryption types during the Kerberos pre-authentication process and cannot use the weaker DES and RC4 encryption types. In addition, members of this group cannot be delegated using constrained or unconstrained delegation of authentication.

The ticket lifetime for Protected Users is set by default to four hours, but authentication policies can increase or decrease this lifetime. After the TGT lifetime expires, users need to authenticate to renew the TGT.

Customers can use the Protected Users group to identify NTLM dependencies in their networks when considering a move to a Kerberos-authentication-only environment. Although retiring NTLM is currently only possible in very specific environments and is not advised for most customers, this feature could assist the transition for customers exploring this approach. This feature helps prevent credential theft.

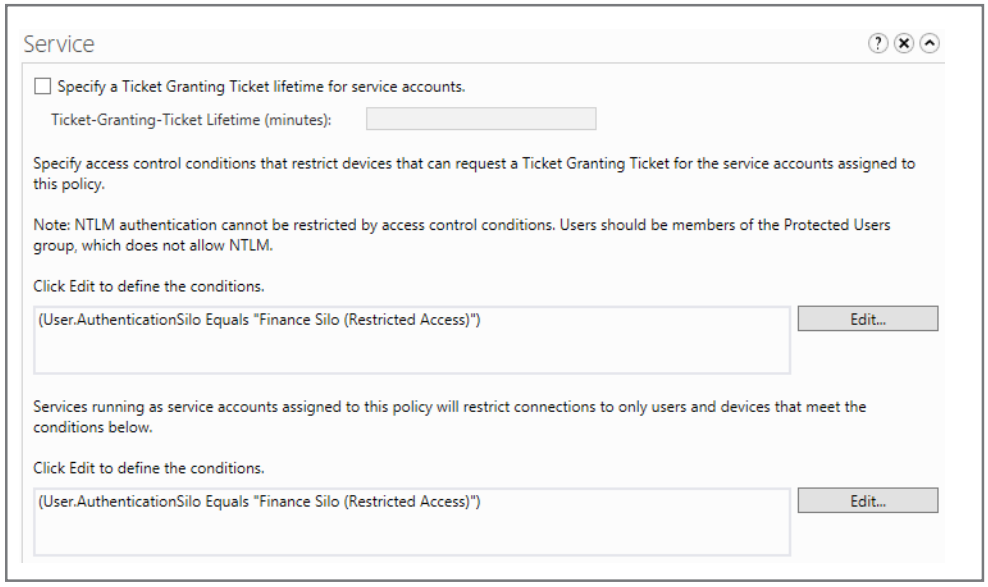


Figure 9: Creating authentication policies and silos

For more information...

see Protected Users Security Group. More information on retiring NTLM can be found in the Auditing and restricting NTLM usage guide on Microsoft TechNet.

Feature limitations

This feature will not protect users from interactive sign-on to a compromised host. Protected users cannot authenticate if Kerberos is not working appropriately. All protected user accounts must be able to function in a Kerberos-only configuration without falling back on NTLM authentication. Accounts that require delegation should not be added to the protected users group, because delegation is not supported for members of this group.

For more information...

about these authentication policies, see Authentication Policies and Authentication Policy Silos on TechNet.

Authentication policies and silos

Available on:
Windows 8.1 and Windows Server 2012 R2

Domain requirements:
Windows Server 2012 R2 Domain Functional Level (DFL), which requires all domain controllers to be upgraded to Windows Server 2012 R2

These Kerberos policies were introduced to provide specificity in controlling authentication. Authentication policies provide the ability to restrict:

- The hosts from which an account may authenticate
- Which accounts may get a service ticket to a resource

The configuration access control conditions for authentication are enforced by domain controllers, which allow isolation of accounts that have constrained network scope.

Administrators can apply authentication configuration to the following new account classes:

- User
- Computer
- Managed Service Account
- Group Managed Service Account

Support for both User Managed Service Account and Group Managed Service Account are referred to as Services in the user interface. These authentication policies are meant to be used in combination with Protected User accounts.

This feature helps prevent credential theft and use of stolen credentials by limiting where accounts may log on. Accounts may be restricted to logging on to designated computers, limiting the usefulness of the credentials to access other resources if stolen.

Note that this requires GPOs to enable both KDC (Key Distribution Center) and Kerberos Client support for claims, compound authentication, and Kerberos armoring.

Feature limitations

Authentication policies and silos require Kerberos and the Protected Users group to ensure that restrictions are effective and not circumvented with NTLM authentication. Authentication policies and silos should not include domain controllers, because doing so could result in all other accounts being unable to authenticate to the domain controller. See "Sample scenarios" for guidance on domain administration.

LSA protection

Available on:
Windows 8.1 and Windows Server 2012 R2

Domain requirements:
None

Windows 8.1 allows the LSASS process to be turned into a protected process. This feature prevents other processes (including processes running as SYSTEM\Administrator) that are not signed by Microsoft from an approved certification authority (CA) from tampering with the LSASS process. This approach means that some attack tools, even when running as SYSTEM, will be unable to steal credentials from the LSASS process. This feature helps prevent credential theft.

Feature limitations

Protected process for LSASS is not a security boundary and should not be used as a comprehensive mitigation; it is designed to make credential harvesting harder but not impossible. This feature currently can be defeated through a number of known means. Additionally, credentials may be stored outside of LSASS in applications or Credential Manager and could be obtained by an attacker. Ultimately, the only current way to prevent an attacker from stealing privileged credentials from a system is to ensure that the system never receives privileged credentials in the first place.

Disable Automatic Restart Sign-On (ARSO) routine

Available on:
Windows 8.1, Windows Server 2012 R2 (disabled by default)

Domain requirements:
None

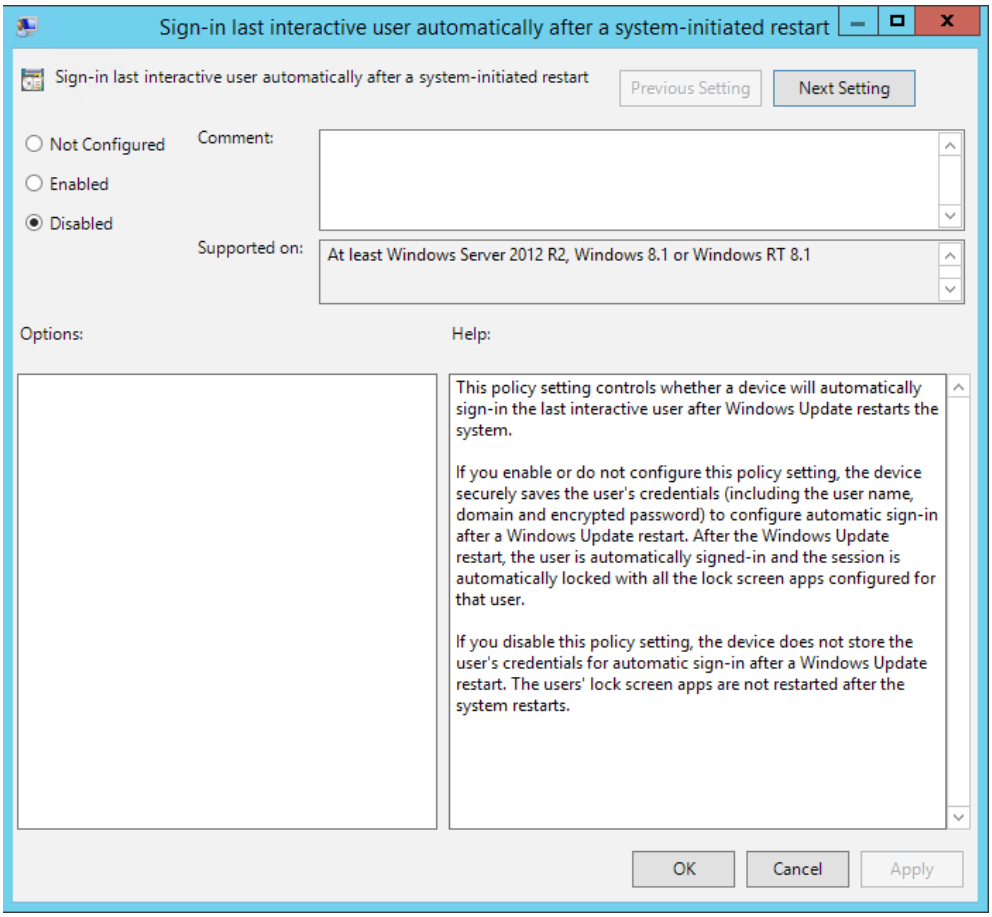
Although most of the changes in Windows 8.1 discussed in this paper are designed to help administrators mitigate the risk of credential theft, the Automatic Restart Sign-On (ARSO) feature introduced in Windows 8.1 creates a new attack vector for credential theft if enabled. The ARSO routine is designed to allow Windows lock screen notification (for example, an alarm clock or calendar notifications that appear on the device's lock screen) to continue functioning when the device automatically installs updates and reboots in the user's absence. To achieve this experience, Windows must temporarily store the logged-on user's encrypted credentials to local storage while the device restarts, and then use them to log the user back on and lock the device. This approach makes any important notifications immediately visible to users when they return to the device. However, an attacker may be able to gain access to the credentials during the period when they are stored.

For more information...

on how to turn the LSASS process into a protected process, see Configuring Additional LSA Protection on TechNet. Microsoft encourages vendors to have their LSA plug-ins signed. For more on this program, see LSA plug-in signing.

This feature is enabled by default on Windows 8.1 when BitLocker is enabled, but it can be disabled using Group Policy Editor. Windows Server 2012 R2 disables this feature by default. Microsoft encourages customers who are concerned about the availability of plaintext domain account passwords to disable the ARSO feature by setting the policy Sign in last interactive user automatically after a system-initiated restart (located in Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Logon Option) to Disabled.

Figure 10: Automatic restart sign-in



For more information...

about ARSO, see Winlogon Automatic Restart Sign-On (ARSO) on Microsoft TechNet.

Applicability summary for mitigations

MITIGATION	DESCRIPTION	WINDOWS 7 AND WINDOWS SERVER 2008 R2	WINDOWS 8 AND WINDOWS SERVER 2012	WINDOWS 8.1 AND WINDOWS SERVER 2012 R2	REQUIRES DOMAIN UPDATE
Logon restrictions with new well-known security identifiers (SIDs)	Use the new SIDs to block network logon for local users and groups by account type, regardless of what the local accounts are named	✓	✓	✓	
Enforce credential removal after logoff	New mechanisms have been implemented to eliminate session leaks in LSASS, thereby preventing credentials from remaining in memory	✓	✓	✓	
Remove LAN Manager (LM) hashes from LSASS	LAN Manager legacy hashes are no longer stored in LSASS	✓	✓	✓	
Remove plaintext credentials from LSASS for domain accounts	LAN Manager legacy hashes are no longer stored in LSASS	✓	✓	✓	
Restricted Admin mode for Remote Desktop Connection*	The Remote Desktop application and service have been updated to support authentication without providing credentials to the remote host	✓	✓	✓	
Protected Users security group client-side protections	The types of credentials available are reduced for Members of the Protected Users group	✓	✓	✓	
Protected Users security group	The new Protected Users security group enables administrators to restrict authentication to the Kerberos protocol only for group members within a domain	✓	✓	✓	✓
Authentication Policy and Authentication Policy Silos	New Authentication policies provide the ability to restrict account authentication to specific hosts and resources			✓	✓
LSA protection	Allows the LSASS process to be turned into a Protected Process preventing other processes (including processes running as SYSTEM\Administrator) that are not signed by Microsoft from tampering with the LSASS process			✓	

*Remote Desktop service (RDP Session Host) support for this feature is only available on Windows 8.1 and Windows Server 2012 R2.

All Windows 8.1 and Windows Server 2012 R2

Newly built environments running Windows 8.1 and Windows Server 2012 R2 can benefit from all the features described in this paper. Customers deploying all new upgraded Windows clients and servers are advised to understand and deploy all recommendations and features described in this paper to help ensure that their environments are more resilient to such attacks at time of deployment.

Mixed environments: Upgraded domain level functionality

Customers are strongly advised to upgrade their domain controllers even if all clients and servers cannot also be upgraded at this time. Doing so will result in a mixed environment of new and legacy computers that will greatly benefit from the updates to the platform, and will provide the quickest return on investment for customers who want to use these new features on an established network. Upgrading domain controllers will allow customers to gradually upgrade their environments while deploying configurations to enable the new Protected User accounts and authentication policies and silos features described in this paper. Microsoft recommend that each organization plan and test per their standard procedures to avoid issues.

Legacy environments: Legacy domain level functionality

Microsoft strongly advises customers to upgrade their domain environments to benefit from the latest security available on the Windows platform. For cases where domain controllers cannot be upgraded immediately, added functionality will be limited to features that were backported to supported versions of Windows. Legacy environments will not benefit from enhancements that require domain controller upgrade, including the ability to use Protected User accounts and authentication policies and silos.

Sample scenarios

This section describes common IT scenarios, strategies, and recommendations to reduce the risk of credential theft. For some scenarios, it also recommends when to implement mitigations such as RDP with Restricted Admin mode, authentication policies and silos, and the Protected Users group. General considerations are provided for Business group isolation and bring your own device (BYOD) scenarios.

The following scenarios are discussed:

Helpdesk

Domain administration

Operations and service management

Service accounts

Business group isolation (for example, Finance and HR)

Bring your own device (BYOD)

Helpdesk

Helpdesk support accounts are high-value accounts and an attractive target for adversaries. These accounts typically have administrative access on most or all user workstations to resolve support issues.

Risks: This scenario could result in an attacker gaining access to credentials with more privileges than the credentials that are typically available on the target computer. When planning support processes and technology, customers should consider the following risk factors:

- The user is not malicious, but the computer has been compromised by an attacker.
- The user is malicious, and is inducing the support staffer to authenticate to the compromised host to gain access to their domain credentials.
- The helpdesk account has more user rights than it needs.
- The support staffer is logging on remotely from a computer that has not been designated as a helpdesk computer.

When the user is malicious or the computer has been compromised, exposing credentials to the computer could enable an attacker to obtain credentials that could be used to authenticate to other computers and escalate privileges. Using accounts with unnecessary user rights or from a non-designated workstation increases the risk.

Recommendations: When possible, implement the following mitigations to reduce the likelihood of credentials being captured or maliciously used:

Separate administrative accounts from user accounts. Ensure helpdesk staff administrator accounts are separate from their user accounts and have limited access. Provide accounts that have access that is limited to the organization's support needs by role. Consider separating user support by business requirements according to the organization layout to ensure that if one helpdesk account is compromised, an attacker could still be constrained.

Use hardened and restricted hosts. Enable helpdesk administrators to perform their work from hardened workstations that are constantly monitored for security events. Ensure these recommended security practices are enforced on these workstations.

- Ensure that local firewalls are in place to restrict incoming connections to designated helpdesk computers and required services and applications only.
- Ensure that the password for the local administrator account for these workstations are each unique.
- If possible, limit the administrative accounts from accessing the Internet while allowing the nonprivileged user accounts to have Internet access.

Limit exposure of administrative credentials. For remote control sessions where the helpdesk support personnel require administrative access, ensure that RDP connections are only performed using the /RestrictedAdmin switch to ensure that credentials are not exposed to compromised hosts.

Add accounts to Protected Users security group. If Kerberos is supported and domain controllers have been upgraded, add helpdesk administrator accounts to the Protected Users group to increase security for these accounts.

Create authentication policies and silos. If the organization can use the Protected Users security group, they can create authentication policies and silos to constrain the helpdesk administrator accounts to obtain Kerberos TGTs only on the hardened workstations. Doing so will help limit exposure of these accounts and ensure that any compromised helpdesk accounts cannot be used outside this defined scope.

This approach would still allow the use of Remote Desktop with Restricted Admin mode to manage user workstations outside of the silo, because only Kerberos service tickets are required to connect to a remote host. If combined with monitoring, this approach could also flag potential misuse.

Domain administration

Organizations generally require certain administrators to have privileged access to domain controllers to maintain the organization's computing infrastructure. While organizations are advised to delegate other functions of domain administrator (DA) and enterprise administrator (EA) groups, Microsoft recognizes that the use of these privileges is frequently unconstrained. Accounts with these privileges are often used to administer Active Directory accounts and other objects in the forest.

Risks: DA or equivalent accounts are high-value targets because they can enable an attacker to compromise an organization's entire Active Directory environment. Customers should consider these risk factors:

- Administrators log on with DA accounts to computers that are more likely to be compromised such as workstations or web servers.
- Administrators perform risky activities while logged on with privileged accounts such as browsing the web, reading email, or opening or executing downloaded files on domain controllers.
- The organization does not monitor DA accounts for anomalous behavior or usage.
- These accounts are assigned to vendors and other support staff outside the organization, without ensuring third-party compliance with best practices.
- The organization has not implemented or maintained an account lifecycle for these accounts.

Recommendations: When possible, implement the following mitigations to reduce the likelihood of DA credentials being captured and maliciously used:

Reduce privileges and privilege use. We strongly discourage customers from conducting any activity with DA and EA accounts other than administering domain controllers and delegating privileges. Most Active Directory data administration functions can be delegated to roles that don't need service administration privileges of the domain or forest.

Use hardened and restricted hosts. Require that DA and equivalent accounts perform their work only from hardened workstations that are consistently monitored, and ensure that security best practices are enforced in the use of these workstations. See the "Create hardened and restricted administrative hosts" section for more details. Also ensure that the password for the local administrator account for these workstations is unique.

Strengthen authentication assurance. Deploy multifactor authentication as well as privileged password management, just-in-time, or another mechanism to strengthen authentication assurance and enforce consistent password rotation and limit the lifetime of DA accounts.

Implement security monitoring Monitor the usage of these privileges carefully and investigate anomalous behavior rapidly. Monitoring and investigation can be accomplished with a combination of processes and tools that enforce just-in-time access, access hours, and automatic account monitoring or similar mechanisms.

If it is absolutely necessary that third-party vendors be assigned the use of DA credentials, ensure that contractual obligations are in place to restrict, review, and monitor vendor(s) practices of managing these credentials.

Add accounts to Protected Users security group. If Kerberos is fully supported for their tasks and domain controllers have been upgraded, add all these DA accounts to the Protected Users group to ensure added security for these accounts.

> **IMPORTANT:** If this measure is implemented, Microsoft strongly recommends that customers have a backup plan in place if Kerberos fails. This can be a closely monitored domain administrator account that is not in the Protected Users group.

Create authentication policies and silos. Create authentication policies and silos to define constraints on the use of DA accounts. Doing so will help ensure that if accounts are compromised, they cannot be used outside their defined scope (authenticate from a designated administrative workstation to a domain controller). If combined with monitoring, this approach could flag potential misuse. For more information about how to do this, see How to Configure Protected Accounts on TechNet.

Operations and service management

Every organization has one or more administrative staffers who are responsible for operations and management of services. These tasks require the use of privileged accounts with administrative access to various services, servers, and applications (typically Tier 1 resources).

Risks: Much like DA accounts, accounts that are used for operations management are highly sought after by attackers because they provide significant access to an organization's data, systems, infrastructure, and services. The risks are very similar to domain administrators, with exception of the scope of impact.

Recommendations: When possible, implement the same mitigations as for domain administrators to reduce the likelihood of privileged account credentials being captured and maliciously used.

Service accounts

A service account is an account that is not assigned to an individual and is typically associated with a specific application or service. Service accounts are commonly used to run a Windows service or used by an application to perform actions on remote hosts and devices on a network.

The usage requirement for accounts used to run a Windows service are typically consistent. Windows Server 2008 R2 introduced the concept of the managed service accounts, which are accounts that are tied to a specific computer and are automatically set up and maintained with a complex password updated every 30 days by default. Managed service accounts are exempt from domain password policies and cannot be used to log on interactively.

The usage requirements for service accounts used by an application to perform actions and tasks on remote hosts and devices will vary significantly by the application and its functionality.

Risks: Attackers frequently target service accounts for credential theft. The specific risks associated with any given service account are directly related to:

- What privileges are granted to the account
- How closely the account activity is monitored for anomalies
- Whether there are any restrictions on the account(s)
- Where the authentication credentials are stored
- Where the account logs on and how the credentials are used

Service accounts are often granted administrative privileges on a single computer or a group of computers, frequently spanning multiple tiers of privilege. The manner in which such privileges are granted can have significant implications for the overall security level of the domain. For example, service accounts in the Domain Admins or Enterprise Admins groups can create risk to the integrity of the entire forest, all the domains in it, and all computers joined to those domains if the credentials are stolen. If attackers manage to capture these credentials, they could use the credentials to rapidly gain administrative access to most or all assets in the entire enterprise.

Another common risk with using domain unmanaged service accounts is that passwords will not be automatically generated or managed, which often results in weak passwords, password reuse, and passwords that are valid for months or years. Changing the password for a service account can frequently incur the risk of service downtime, which increases the chances that service account passwords are not changed frequently.

Recommendations: When possible, implement the following mitigations to reduce the likelihood of service account credentials being captured and maliciously used:

Grant the least privilege. For all service accounts, grant the least privilege to the accounts that is required by the application. Accounts should start with standard user privileges and only be granted privileges on hosts and in Active Directory Domain Services as required by the application. This privilege level will vary by application, but several general rules should be followed:

- Service accounts should never be granted membership in Domain Admins, Enterprise Admins, Schema Admins, Account Operators, or BUILTIN\Administrators. In rare cases, exceptions can be made for applications that manage Active Directory Domain Services, but these groups should never be used to grant local administrative privileges on hosts. Features such as restricted groups and Group Policy preferences should be used to grant access to multiple hosts instead. For more information, see Local Users and Groups Extension.

- For accounts that can be configured to use Network Service or Local Service, use one of these accounts rather than Local System. For more information see Service User Accounts.

Use managed service accounts. Whenever possible, use managed service accounts so that passwords for the accounts are set and managed automatically. This mitigation is appropriate for accounts that run Windows services, but is not applicable for accounts that applications use to perform tasks (which require the application to store the account password). Create and use managed service accounts with the default managed service account container. For more information, see Managed Service Accounts (documentation for Windows 7 and Windows Server 2008 R2) or Group Managed Service Accounts Overview on TechNet.

Change passwords regularly. For service accounts whose passwords are not automatically managed with a tool or by the managed service account process, organizations should design a process to regularly change these passwords and follow these procedures.

Monitor service account activity. Monitoring should also be in place if such accounts are used in an enterprise to ensure that they do not move from one assigned area of the network into another (which suggests that they have been compromised by an attacker).

Contain credential exposure. Ensure that the service accounts are compliant with the tiered model described earlier in this paper. For unmanaged service accounts, organizations can create authentication policies and silos to define network constraints in their use. Doing so will ensure that if accounts are compromised, they cannot be used outside their defined scope. If combined with monitoring, this approach could flag potential misuse. Service accounts should be limited to the required hosts and accounts used for a particular service or application. For more information about how to accomplish this configuration, see How to Configure Protected Accounts on TechNet.

> **Note:** Do not add service accounts used to run Windows services to the protected users group. Services and hosts need to access long-term keys to decrypt service tickets from clients. Protected users discard keys so all inbound connections would fail to these services and hosts. Service accounts used exclusively for outbound authentication, such as those used by an application to perform actions on remote hosts are potentially good candidates for this protection.

Business groups and isolation

Organizations typically have multiple business groups that could benefit from an account isolation strategy to protect critical business assets. Just like for administrative accounts, credentials for high value business accounts may be stolen and used for unauthorized access to sensitive business data.

This section contains only general considerations for business group isolation as it relates to credential theft.

Considerations:

- Ensure that use cases for users, applications, and accounts are well defined.
- Configure hosts in the department or workgroup to adhere to an assurance standard that includes elements described in the "Create hardened and restricted administrative hosts" section.
- Restrict users that have access to sensitive data from logging on to computers outside their department. Consider implementing restrictions based on the Tier Model described in the "Protect against known and unknown threats"section.
- Consider blocking Internet access from the hosts and providing Internet browsing through a separate computer, such as a server hosting the browser in Remote Desktop Protocol (RDP) sessions.
- Ensure that business groups do not share accounts or passwords outside the isolated business group.
- Ensure that the local administrative passwords on workstations and servers are different from that of other hosts.

Bring your own device (BYOD)

Many organizations now allow employees to connect their personal devices to the corporate network and access resources. These devices are often unmanaged and do not follow the organization's security standards and best practices. In addition, these devices spend their lifetimes transitioning between public and corporate networks, so they are at greater risk of being compromised and introducing attackers to internal networks and resources.

This section contains guidelines and considerations for the BYOD scenario related to credential theft. This section is not comprehensive for all BYOD design considerations and Microsoft advises customers to perform extensive planning and testing for this scenario.

The risks related to allowing BYOD devices to connect to resources varies depending on the strategy adopted by the organization and the type of device. Because organizations do not have exclusive control over the policy and configuration of these devices, they should be considered high-risk.

Considerations:

- Ensure that the use cases and policies for BYOD are well defined.
- Ensure that the risks of allowing BYOD devices to access and store corporate data are fully understood and accepted by stakeholders.
- Ensure that BYOD devices are not used for administrative tasks and administrative users don't log on to BYOD devices.

- Ensure that high business impact (HBI) data is not being stored on these devices, and that accounts with access to HBI data are not used on them.
- Ensure that users don't use the same password between corporate and personal accounts on the devices.
- Ensure that privileged service accounts with administrative access to corporate resources are not exposed to the BYOD devices.
- Deploy policies to enforce a minimum level of security on mobile devices. Some devices, such as Windows Phones, allow the deployment of certain policies when connecting to services using corporate accounts, such as encryption standard enforcement and the use of lock screens and PINs. If possible, deploy a remote wipe policy that also allows users and administrators to remotely erase a device if it is lost or stolen. Mobile Device Management (MDM) solutions can allow organizations to deploy policies to multiple platforms. For more information, see Exchange ActiveSync Policy Engine Overview, Windows Selective Wipe for Device Data Management, and Windows Intune.
- Isolate network access to these devices and monitor activity.
- Create a strategy to remediate compromised devices and user accounts.

Conclusion

It is important to understand that technology alone cannot solve the problem of credential theft, and that people and processes are critical elements in the defense plan. The strategies and mitigations described in this paper and its predecessor are designed to help promote best practices and behaviors that encourage restricted use of privileged credentials. This is especially important for credential theft attacks, since the attack surface is primarily shaped by operational practices.

Organizations need to adopt and enforce processes as well as people-readiness programs to ensure a complete approach to defending against these attacks. This is even more significant in a time where determined adversaries and targeted attacks actively seek seams they can exploit, which can include gaps between design and operation as well as misalignment of identity management and security practices.

The determined adversaries who conduct targeted attacks will continue to evolve rapidly, as will the threat landscape. Determined adversaries will adapt to the defenses of targeted organizations and seek out new ways of exploiting systems and the people who operate and maintain them. It is crucial to recognize that a comprehensive defense approach is needed and that organizations should be prepared to defend against these threats.

References

References made in this paper include the following:

Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques
http://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating%20Pass-the-Hash%20(PtH)%20Attacks%20and%20Other%20Credential%20Theft%20Techniques_English.pdf

Auditing and restricting NTLM usage guide
http://technet.microsoft.com/en-us/library/jj865674(v=ws.10).aspx

Authentication Policies and Authentication Policy Silos
http://technet.microsoft.com/en-us/library/dn486813.aspx

Configuring Additional LSA Protection
http://technet.microsoft.com/en-us/library/dn408187.aspx

Winlogon Automatic Restart Sign-On (ARSO)
http://technet.microsoft.com/en-us/library/dn535772.aspx

Cached and Stored Credentials Technical Overview
http://technet.microsoft.com/en-us/library/hh994565.aspx

User Rights Assignment
http://technet.microsoft.com/en-us/library/dn221963.aspx

Authentication Policies and Authentication Policy Silos
http://technet.microsoft.com/en-us/library/dn486813.aspx

AppLocker Design Guide
http://www.microsoft.com/en-us/download/details.aspx?id=40330

AppLocker Policies Design Guide
http://technet.microsoft.com/en-us/library/ee449480.aspx

Enhanced Mitigation Experience Toolkit (EMET)
http://technet.microsoft.com/en-us/security/jj653751

Attack Surface Analyzer
http://www.microsoft.com/en-us/download/details.aspx?id=24487

Best Practices for Securing Active Directory
http://www.microsoft.com/en-us/download/details.aspx?id=38785

Microsoft Security Compliance Manager
http://technet.microsoft.com/en-us/library/cc677002.aspx

Configuring Additional LSA Protection
http://technet.microsoft.com/en-us/library/dn408187.aspx

Windows Event Collector
http://msdn.microsoft.com/en-us/library/windows/desktop/bb427443(v=vs.85).aspx

Audit Collection Services
http://technet.microsoft.com/en-us/library/bb381258.aspx
http://technet.microsoft.com/en-us/library/hh212908.aspx

How to Configure Protected Accounts
http://technet.microsoft.com/en-us/library/dn518179.aspx

Managed Service Accounts
http://technet.microsoft.com/en-us/library/ff641731(v=ws.10).aspx

Group Managed Service Accounts Overview
http://technet.microsoft.com/en-us/library/hh831782.aspx

Exchange ActiveSync Policy Engine Overview
http://technet.microsoft.com/library/dn282287.aspx

Windows Selective Wipe for Device Data Management
http://technet.microsoft.com/en-us/library/dn486874.aspx

Networking and Access Technologies: IPsec
http://technet.microsoft.com/en-us/network/bb531150.aspx

Forefront Identity Manager
http://www.microsoft.com/en-us/server-cloud/products/forefront-identity-manager/#fbid=hXztqFJXe-Y

Command line process auditing
http://technet.microsoft.com/en-us/library/dn535776.aspx

Active Directory Security Groups
http://technet.microsoft.com/en-us/library/dn579255.aspx

Configuring Selective Authentication Settings
http://technet.microsoft.com/en-us/library/cc755844(v=ws.10).aspx

What's New in Remote Desktop Services in Windows Server
http://technet.microsoft.com/en-us/library/dn283323.aspx

How to change the default permissions on GPOs in Windows Server 2008 R2, Windows Server 2008, Windows Server 2003, and Windows 2000 Server
http://support.microsoft.com/kb/321476

Deploy Remote Server Administration Tools
http://technet.microsoft.com/en-us/library/hh831501.aspx

Approving Updates
http://technet.microsoft.com/en-us/library/cc708458(v=ws.10).aspx

Security Development Lifecycle
http://www.microsoft.com/sdl

Reset a Computer Account
http://technet.microsoft.com/en-us/library/cc753596.aspx

LSA plug-in signing
http://msdn.microsoft.com/en-us/library/windows/hardware/dn629520.aspx

KRBTGT account
http://technet.microsoft.com/en-us/library/dn745899.aspx#Sec_KRBTGT

New York Times: The Year in Hacking, by the Numbers
http://bits.blogs.nytimes.com/2013/04/22/the-year-in-hacking-by-the-numbers/?_php=true&_type=blogs&_php=true&_type=blogs&_php=true&_type=blogs&_r=4&

Azure Active Directory Identity and Access Management for the Cloud
http://azure.microsoft.com/en-us/services/active-directory/

Monitoring.pdf Settings for default local accounts in Active Directory
http://technet.microsoft.com/en-us/library/dn745899.aspx#Sec_Account_Settings

Other references that may be of interest include:

Windows 8.1 and Windows 8
http://technet.microsoft.com/en-us/library/hh832030.aspx

Windows Server 2012 R2 and Windows Server 2012
http://technet.microsoft.com/en-us/library/hh801901.aspx

Credentials Protection and Management
http://technet.microsoft.com/en-us/library/dn408190.aspx

Reducing the Effectiveness of Pass-the-Hash
http://www.nsa.gov/ia/_files/app/Reducing_the_Effectiveness_of_Pass-the-Hash.pdf

Local Users and Groups Extension
http://technet.microsoft.com/en-us/library/cc731972.aspx

Service User Accounts
http://msdn.microsoft.com/en-us/library/windows/desktop/ms686005(v=vs.85).aspx

The NIST Cybersecurity Framework: A Significant Milestone towards Critical Infrastructure Resiliency
http://blogs.technet.com/b/security/archive/2014/02/13/the-nist-cybersecurity-framework-a-significant-milestone-towards-critical-infrastructure-resiliency.aspx

Windows PowerShell Remoting (Enable-PSRemoting)
http://technet.microsoft.com/en-us/library/hh849694.aspx

BitLocker
http://technet.microsoft.com/en-us/library/dn641993.aspx

Defending Against Pass-the-Hash Attacks
http://www.microsoft.com/security/sir/strategy/default.aspx#!password_hashes

Appendix

Other enterprise security solutions

Network segmentation requires:

- Network isolation between resources that do not share a similar risk level and administrative model. Examples may include combining all workstations and all financial systems into separate groups and isolating network traffic between them. Other examples could include control hardware, such as supervisory control and data acquisition (SCADA) systems and heating, ventilation, and air conditioning (HVAC) systems).
- Allowing authorized and expected activity for authentication and network traffic between each zone and denying unauthorized or anomalous activity. For example, some inbound connections to an administrative network zone may be considered anomalous.

Several enterprise solutions exist that facilitate host isolation and credential management; other solutions can facilitate the handling of security events.

Internet protocol security (IPsec) allows not only isolation but also network-level peer authentication, data origin authentication, data integrity, and data confidentiality through encryption and replay protection.

  - **Pros:** Hard isolation boundary protects against network-based attacks.
  - **Cons:** Difficult to set up, requires maintenance if IP addressing changes.

- **Temporary admin privileges, password management, and security policy enforcement** can be done with a number of tools, including Forefront Identity Manager.

  - **Pros:** Self-service privilege assignment, group membership, password reset, and identity lifecycle management.
  - **Cons:** Some solutions do not provide password rotation or vaulting.

Just-in-time access and automatic password rotation solutions allow for approved workflow and check-in, check-out account management. There are no Microsoft solutions currently available to support this requirement, but third-party tools are available.

  - **Pros:** Restricts the lifetime when an administrator can obtain access. Centralized password storage through a password vault and automatic rotation of passwords, which prevents password reuse, ensures complex passwords, and enforces unique passwords for accounts.
  - **Cons:** Some accounts cannot be rotated frequently. Centralized service needs to be secured appropriately because it may have the same trust level as a domain controller (Tier 0).

For more information...

on deploying IPsec is available in Networking and Access Technologies: IPsec on TechNet.

Security information and event management (SIEM) solutions allow organizations to automatically detect threats. By processing high log volumes, classifying events and indexing, these tools can enable watchdogs on specific events that could enable organizations to detect specific threats. There are no Microsoft solutions currently available to support this requirement, but many third-party tools are available.

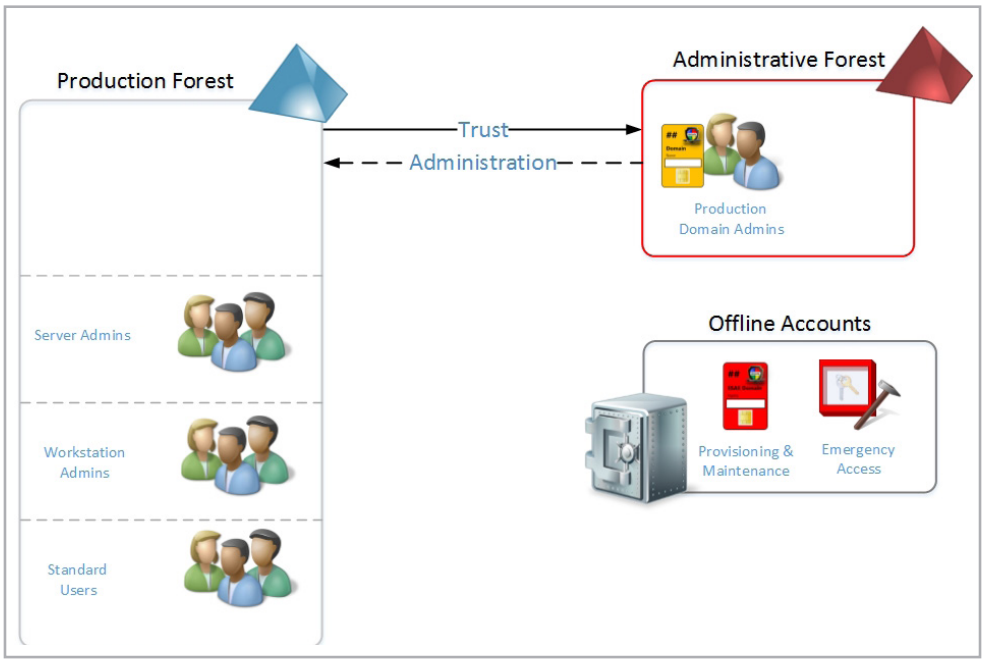
- **Pros:** Allow high-volume collection and processing of logs, which enables automatic event detection.
- **Cons:** There are limitations on events that can currently be monitored for credential theft. Customers are advised to implement mitigations and strategies to restrict scope and create watchdogs on deviation. Another important consideration is that some devices are not real-time devices and have capacity limitations. Check with third-party manufacturers for tool specifications.

Dedicated administrative forests allow organizations to host administrative accounts, workstations, and groups in an environment that has stronger security controls than the production environment.

- **Pros:** This architecture enables a number of controls that aren't possible or easily configured in a single forest architecture. This approach allows the provisioning of accounts as standard non-privileged users in the administrative forest that are highly privileged in the production environment, enabling greater technical enforcement of governance. This architecture also enables the use of the selective authentication feature of a trust as a means to restrict logons (and credential exposure) to only authorized hosts. In situations in which a greater level of assurance is desired for the production forest without incurring the cost and complexity of a complete rebuild, an administrative forest can provide an environment that increases the assurance level of the production environment.
- **Cons:** This approach adds cost and complexity to an Active Directory environment. While this approach is suitable for administering Active Directory, many applications aren't compatible with being administered with accounts from an external forest over a trust.

Designing an admin forest

Figure 11: Admin forest



A dedicated administrative forest is a standard single domain Active Directory forest dedicated to the function of Active Directory management. Administrative forests and domains may be hardened more stringently than production forests because of the limited use cases.

An administrative forest design should include the following considerations:

- **Limited scope**–The value of an admin forest is the high level of security assurance and reduced attack surface resulting in lower residual risk. The forest can be used to house additional management functions and applications, but each increase in scope will increase the attack surface of the forest and its resources. The objective is to limit the functions of the forest and admin users inside to keep the attack surface minimal, so each scope increase should be considered carefully.
- **Trust configurations**–Configure trust from managed forests(s) or domain(s) to the administrative forest
  - A one-way trust is required from production environment to the admin forest. This can be a domain trust or a forest trust. The admin forest/domain does not need to trust the managed domains/forests to manage Active Directory, though additional applications may require a two-way trust relationship, security validation, and testing.

- Selective authentication should be used to restrict accounts in the admin forest to only logging on to the appropriate production hosts. For maintaining domain controllers and delegating rights in Active Directory, this typically requires granting the "Allowed to logon" right for domain controllers to designated Tier 0 admin accounts in the admin forest. See Configuring Selective Authentication Settings for more information.

- **Privileges and domain hardening**–The administrative forest should be configured to least privilege based on the requirements for Active Directory administration.

  - Granting rights to administer domain controllers and delegate permissions requires adding admin forest accounts to the BUILTIN\Administrators domain local group. This is because the Domain Admins global group cannot have members from an external domain.

    One caveat to using this group to grant rights is that they won't have administrative access to new group policy objects by default. This can be changed by following the procedure in this knowledge base article to change the schema default permissions: http://support.microsoft.com/kb/321476

  - Accounts in the admin forest that are used to administer the production environment should not be granted administrative privileges to the admin forest, domains in it, or workstations in it.

  - Administrative privileges over the admin forest should be tightly controlled by an offline process to reduce the opportunity for an attacker or malicious insider to erase audit logs. This also helps ensure that personnel with production admin accounts cannot relax the restrictions on their accounts and increase risk to the organization.

  - The administrative forest should follow the Microsoft Security Compliance Manager (SCM) configurations for the domain, including strong configurations for authentication protocols.

- **Host hardening**–For all domain controllers, servers, and workstations in the administrative forest:

  - The administrative forest hosts should have the latest operating systems installed, even if this is not feasible in production.

  - The administrative workstations and server hosts should follow all guidance in the "Create hardened and restricted administrative hosts" section

  - The applications required for performing administration should be pre-installed on workstations so that accounts using them don't need to be in the local administrators group to install them. Domain Controller maintenance can typically be performed with RDP and Remote Server Administration Tools.

For more information...

see Deploy Remote Server Administration Tools

- Admin forest hosts should be automatically updated with security updates. While this may create risk of interrupting domain controller maintenance operations, it provides a significant mitigation of security risk of unpatched vulnerabilities.

  Windows Server Update Services can be configured to automatically approve updates. For more information, see the "Automatically Approve Updates for Installation" section in Approving Updates.

- **Account hardening**

  - Multi-factor authentication should be configured for all accounts in the admin forest, except one account. At least one administrative account should be password based to ensure access will work in case the multi-factor authentication process breaks. This account should be protected by a stringent physical control process.
  - Accounts configured for multi-factor authentication should be configured to set a new NTLM hash on accounts regularly. This can be accomplished by disabling and enabling the account attribute Smart card is required for interactive logon.

Note: This can interrupt operations in progress that are using this account, so this process should be initiated only when administrators won't be using the account, such as at night or on weekends.

- **Detective controls**

  - Detective controls for the administrative forest should be designed to alert on anomalies in the admin forest. The limited number of authorized scenarios and activities can help tune these controls more accurately than the production environment.

For more information...

see Settings for default local accounts in Active Directory.


Microsoft