Microsoft

Best Practices for Securing Active Directory

Microsoft IT

Information Security and Risk Management

Published: April, 2013

For the latest information, please see

http://aka.ms/bpsad

Contents

Foreword

In today's information rich environment, senior executives are faced with the challenge of harnessing information technology to help their business:

- Execute its strategy
- Improve its operations
- Enhance the perceived value of its own products and services

In support of these challenges, consumer-centric computing models that leverage highly scalable platforms (the cloud) and a plethora of devices are being utilized. The new business paradigm is obsessed with speed, agility, and execution. The evolution of these models requires even more comprehensive and agile security and risk management programs to ensure success.

This document provides a practitioner's perspective and contains a set of practical techniques to help IT executives protect an enterprise Active Directory® environment. Active Directory plays a critical role in the IT infrastructure, and ensures the harmony and security of different network resources in a global, interconnected environment. The methods discussed are based largely on the Microsoft® Information Security and Risk Management (ISRM) organization's experience, which is accountable for protecting the assets of Microsoft IT and other Microsoft Business Divisions, in addition to advising a selected number of Microsoft Global 500 customers.

Key tenets of this paper are understanding the avenues for establishing a healthy Active Directory, implementing monitoring systems, actions to reduce the attack surface, and managing a resilient environment. This risk-based approach assumes that the corporate infrastructure, and more specifically the Active Directory, is a critical target. With this mindset, resiliency and recovery become critical components of an Active Directory protection program

This document encompasses experience from several hundred Active Directory Security Assessments, critical incident responses, and recovery engagements, and proven techniques for mitigating IT risks. Based on numerous requests from Microsoft customers and partners, this document reflects a comprehensive guide, and it contains best practices for protecting Active Directory. Information security and risk management executives will find the techniques explained in this document to be a significant contribution to their understanding of best practices, in addition to practical implementation programs for their Active Directory environments.

Bret Arsenault
Microsoft Chief Information Security Officer

Acknowledgements

Authors

Laura A. Robinson, Lead Author

Khurram Chaudhary

Roger Grimes

Eric Leonard

Contributors

Ahmad Mahdi

Ashish Popli

Dan Kaufman

Jenn LeMond

Joost van Haaren

Rob Labbé

Reviewers

Alan von Weltin

Andrew Idell

Bret Arsenault

David Shaw

Dean Wells

Fernando Cima

Georgeo Pulikkathara

Joost van Haaren

Joseph Lindstrom

Laura Hunter

Lesley Kipling

Mark Simos

Michiko Short

Neil Carpenter

Patrick Jungles

Paul Rich

Rob Labbé

Sean Finnegan

Tim Rains

Todd Thompson

Executive Summary

No organization with an information technology (IT) infrastructure is immune from attack, but if appropriate policies, processes, and controls are implemented to protect key segments of an organization's computing infrastructure, it might be possible to prevent a breach event from growing to a wholesale compromise of the computing environment.

This executive summary is intended to be useful as a standalone document summarizing the content of the document, which contains recommendations that will assist organizations in enhancing the security of their Active Directory installations. By implementing these recommendations, organizations will be able to identify and prioritize security activities, protect key segments of their organization's computing infrastructure, and create controls that significantly decrease the likelihood of successful attacks against critical components of the IT environment.

Although this document discusses the most common attacks against Active Directory and countermeasures to reduce the attack surface, it also contains recommendations for recovery in the event of complete compromise. The only sure way to recover in the event of a complete compromise of Active Directory is to be prepared for the compromise before it happens.

The major sections of this document are:

- Avenues to Compromise
- Reducing the Active Directory Attack Surface
- Monitoring Active Directory for Signs of Compromise
- Planning for Compromise

Avenues to Compromise

This section provides information about some of the most commonly leveraged vulnerabilities used by attackers to compromise customers' infrastructures. It contains general categories of vulnerabilities and how they're used to initially penetrate customers' infrastructures, propagate compromise across additional systems, and eventually target Active Directory and domain controllers to obtain complete control of the organizations' forests. It does not provide detailed recommendations about addressing each type of vulnerability, particularly in the areas in which the vulnerabilities are not used to directly target Active Directory.

However, for each type of vulnerability, we have provided links to additional information to use to develop countermeasures and reduce the organization's attack surface.

Included are the following subjects:

- **Initial breach targets** - Most information security breaches start with the compromise of small pieces of an organization's infrastructure—often one or two systems at a time. These initial events, or entry points into the network, often exploit vulnerabilities that could have been fixed, but weren't. Commonly seen vulnerabilities are:
    - Gaps in antivirus and antimalware deployments
    - Incomplete patching
    - Outdated applications and operating systems
    - Misconfiguration
    - Lack of secure application development practices
- **Attractive Accounts for Credential Theft** - Credential theft attacks are those in which an attacker initially gains privileged access to a computer on a network and then uses freely available tooling to extract credentials from the sessions of other logged-on accounts.

  Included in this section are the following:
    - **Activities that Increase the Likelihood of Compromise** - Because the target of credential theft is usually highly privileged domain accounts and "very important person" (VIP) accounts, it is important for administrators to be conscious of activities that increase the likelihood of a success of a credential-theft attack. These activities are:
        - Logging on to unsecured computers with privileged accounts
        - Browsing the Internet with a highly privileged account
        - Configuring local privileged accounts with the same credentials across systems
        - Overpopulation and overuse of privileged domain groups
        - Insufficient management of the security of domain controllers.
    - **Privilege Elevation and Propagation** - Specific accounts, servers, and infrastructure components are usually the primary targets of attacks against Active Directory. These accounts are:
        - Permanently privileged accounts
        - VIP accounts
        - "Privilege-Attached" Active Directory accounts

- Domain controllers
- Other infrastructure services that affect identity, access, and configuration management, such as public key infrastructure (PKI) servers and systems management servers

Reducing the Active Directory Attack Surface

This section focuses on technical controls to reduce the attack surface of an Active Directory installation. Included in this section are the following subjects:

- The **Privileged Accounts and Groups in Active Directory** section discusses the highest privileged accounts and groups in Active Directory and the mechanisms by which privileged accounts are protected. Within Active Directory, three built-in groups are the highest privilege groups in the directory (Enterprise Admins, Domain Admins, and Administrators), although a number of additional groups and accounts should also be protected.

- The **Implementing Least-Privilege Administrative Models** section focuses on identifying the risk that the use of highly privileged accounts for day-to-day administration presents, in addition to providing recommendations to reduce that risk.

  Excessive privilege isn't only found in Active Directory in compromised environments. When an organization has developed the habit of granting more privilege than is required, it is typically found throughout the infrastructure:

  - In Active Directory
  - On member servers
  - On workstations
  - In applications
  - In data repositories

- The **Implementing Secure Administrative Hosts** section describes secure administrative hosts, which are computers that are configured to support administration of Active Directory and connected systems. These hosts are dedicated to administrative functionality and do not run software such as email applications, web browsers, or productivity software (such as Microsoft Office).

  Included in this section are the following:

  - **Principles for Creating Secure Administrative Hosts** - The general principles to keep in mind are:

        - Never administer a trusted system from a less-trusted host.
        - Do not rely on a single authentication factor when performing privileged activities.
        - Do not forget physical security when designing and implementing secure administrative hosts.

- **Securing Domain Controllers Against Attack** - If a malicious user obtains privileged access to a domain controller, that user can modify, corrupt, and destroy the Active Directory database, and by extension, all of the systems and accounts that are managed by Active Directory.
  Included in this section are the following subjects:

    - **Physical Security for Domain Controllers** – Contains recommendations for providing physical security for domain controllers in datacenters, branch offices, and remote locations.
    - **Domain Controller Operating Systems** – Contains recommendations for securing the domain controller operating systems.
    - **Secure Configuration of Domain Controllers** – Native and freely available configuration tools and settings can be used to create security configuration baselines for domain controllers that can subsequently be enforced by Group Policy Objects (GPOs).

Monitoring Active Directory for Signs of Compromise

This section provides information about legacy audit categories and audit policy subcategories (which were introduced in Windows Vista and Windows Server® 2008), and Advanced Audit Policy (which was introduced in Windows Server 2008 R2). Also provided is information about events and objects to monitor that can indicate attempts to compromise the environment and some additional references that can be used to construct a comprehensive audit policy for Active Directory.

Included in this section are the following subjects:

- **Windows Audit Policy** – Windows security event logs have categories and subcategories that determine which security events are tracked and recorded.
- **Audit Policy Recommendations** - This section describes the Windows default audit policy settings, audit policy settings that are recommended by Microsoft, and more aggressive recommendations for organizations to use to audit critical servers and workstations.

Planning for Compromise

This section contains recommendations that will help organizations prepare for a compromise before it happens, implement controls that can detect a compromise event before a full breach has occurred, and provide response and recovery guidelines for cases in which a complete compromise of the directory is achieved by attackers. Included in this section are the following subjects:

- **Rethinking the Approach** - Contains principles and guidelines to create secure environments into which an organization can place their most critical assets. These guidelines are as follows:
    - Identifying principles for segregating and securing critical assets
    - Defining a limited, risk-based migration plan
    - Leveraging “nonmigratory” migrations where necessary
    - Implementing “creative destruction”
    - Isolating legacy systems and applications
    - Simplifying security for end users
- **Maintaining a More Secure Environment** – Contains high-level recommendations meant to be used as guidelines to use in developing not only effective security, but effective lifecycle management. Included in this section are the following subjects:
    - **Creating Business-Centric Security Practices for Active Directory** - To effectively manage the lifecycle of the users, data, applications and systems managed by Active Directory, follow these principles.
        - **Assign a Business Ownership to Active Directory Data** - Assign ownership of infrastructure components to IT; for data that is added to Active Directory Domain Services (AD DS) to support the business, for example, new employees, new applications, and new information repositories, a designated business unit or user should be associated with the data.
        - **Implement Business-Driven Lifecycle Management** - Lifecycle management should be implemented for data in Active Directory.
        - **Classify all Active Directory Data** - Business owners should provide classification for data in Active Directory. Within the data classification model, classification for the following Active Directory data should be included:
            - **Systems** - Classify server populations, their operating system their role, the applications running on them, and the IT and business owners of record.
            - **Applications** - Classify applications by functionality, user base, and their operating system.

- **Users** - The accounts in the Active Directory installations that are most likely to be targeted by attackers should be tagged and monitored.

Summary of Best Practices for Securing Active Directory Domain Services

The following table provides a summary of the recommendations provided in this document for securing an AD DS installation. Some best practices are strategic in nature and require comprehensive planning and implementation projects; others are tactical and focused on specific components of Active Directory and related infrastructure.

Practices are listed in approximate order of priority, that is., lower numbers indicate higher priority. Where applicable, best practices are identified as preventative or detective in nature. All of these recommendations should be thoroughly tested and modified as needed for your organization's characteristics and requirements.

Best Practice		Tactical or Strategic	Preventative or Detective
1	Patch applications.	Tactical	Preventative
2	Patch operating systems.	Tactical	Preventative
3	Deploy and promptly update antivirus and antimalware software across all systems and monitor for attempts to remove or disable it.	Tactical	Both
4	Monitor sensitive Active Directory objects for modification attempts and Windows for events that may indicate attempted compromise.	Tactical	Detective
5	Protect and monitor accounts for users who have access to sensitive data	Tactical	Both
6	Prevent powerful accounts from being used on unauthorized systems.	Tactical	Preventative
7	Eliminate permanent membership in highly privileged groups.	Tactical	Preventative
8	Implement controls to grant temporary membership in privileged groups when needed.	Tactical	Preventative
9	Implement secure administrative hosts.	Tactical	Preventative
10	Use application whitelisting on domain controllers, administrative hosts, and other sensitive systems.	Tactical	Preventative

Best Practice		Tactical or Strategic	Preventative or Detective
11	Identify critical assets, and prioritize their security and monitoring.	Tactical	Both
12	Implement least-privilege, role-based access controls for administration of the directory, its supporting infrastructure, and domain-joined systems.	Strategic	Preventative
13	Isolate legacy systems and applications.	Tactical	Preventative
14	Decommission legacy systems and applications.	Strategic	Preventative
15	Implement secure development lifecycle programs for custom applications.	Strategic	Preventative
16	Implement configuration management, review compliance regularly, and evaluate settings with each new hardware or software version.	Strategic	Preventative
17	Migrate critical assets to pristine forests with stringent security and monitoring requirements.	Strategic	Both
18	Simplify security for end users.	Strategic	Preventative
19	Use host-based firewalls to control and secure communications.	Tactical	Preventative
20	Patch devices.	Tactical	Preventative
21	Implement business-centric lifecycle management for IT assets.	Strategic	N/A
22	Create or update incident recovery plans.	Strategic	N/A

Introduction

Attacks against computing infrastructures, whether simple or complex, have existed as long as computers have. However, within the past decade, increasing numbers of organizations of all sizes, in all parts of the world have been attacked and compromised in ways that have significantly changed the threat landscape. Cyber-warfare and cybercrime have increased at record rates. “Hacktivism,” in which attacks are motivated by activist positions, has been claimed as the motivation for a number of breaches intended to expose organizations’ secret information, to create denials-of-service, or even to destroy infrastructure. Attacks against public and private institutions with the goal of exfiltrating the organizations’ intellectual property (IP) have become ubiquitous.

No organization with an information technology (IT) infrastructure is immune from attack, but if appropriate policies, processes, and controls are implemented to protect key segments of an organization’s computing infrastructure, escalation of attacks from penetration to complete compromise might be preventable. Because the number and scale of attacks originating from outside an organization has eclipsed insider threat in recent years, this document often discusses external attackers rather than misuse of the environment by authorized users. Nonetheless, the principles and recommendations provided in this document are intended to help secure your environment against external attackers and misguided or malicious insiders.

The information and recommendations provided in this document are drawn from a number of sources and derived from practices designed to protect Active Directory installations against compromise. Although it is not possible to prevent attacks, it is possible to reduce the Active Directory attack surface and to implement controls that make compromise of the directory much more difficult for attackers. This document presents the most common types of vulnerabilities we have observed in compromised environments and the most common recommendations we have made to customers to improve the security of their Active Directory installations.

Account and Group Naming Conventions

The following table provides a guide to the naming conventions used in this document for the groups and accounts referenced throughout the document. Included in the table is the location of each account/group, its name, and how these accounts/groups are referenced in this document.

Account/Group Location	Name of Account/Group	How It is Referenced in this Document
Active Directory - each domain	Administrator	Built-in Administrator account
Active Directory - each domain	Administrators	Built-in Administrators (BA) group
Active Directory - each domain	Domain Admins	Domain Admins (DA) group

Account/Group Location	Name of Account/Group	How It is Referenced in this Document
Active Directory - forest root domain	Enterprise Admins	Enterprise Admins (EA) group
Local computer security accounts manager (SAM) database on computers running Windows Server and workstations that are not domain controllers	Administrator	Local Administrator account
Local computer security accounts manager (SAM) database on computers running Windows Server and workstations that are not domain controllers	Administrators	Local Administrators group

About this Document

The Microsoft Information Security and Risk Management (ISRM) organization, which is part of Microsoft Information Technology (MSIT), works with internal business units, external customers, and industry peers to gather, disseminate, and define policies, practices, and controls. This information can be used by Microsoft and our customers to increase the security and reduce the attack surface of their IT infrastructures. The recommendations provided in this document are based on a number of information sources and practices used within MSIT and ISRM. The following sections present more information about the origins of this document.

Microsoft IT and ISRM

A number of practices and controls have been developed within MSIT and ISRM to secure the Microsoft AD DS forests and domains. Where these controls are broadly applicable, they have been integrated into this document. SAFE-T (Solution Accelerators for Emerging Technologies) is a team within ISRM whose charter is to identify emerging technologies, and to define security requirements and controls to accelerate their adoption.

Active Directory Security Assessments

Within Microsoft ISRM, the Assessment, Consulting, and Engineering (ACE) Team works with internal Microsoft business units and external customers to assess application and infrastructure security and to provide tactical and strategic guidance to increase the organization’s security posture. One ACE service offering is the Active Directory Security Assessment (ADSA), which is a holistic assessment of an organization’s AD DS environment that assesses people, process, and technology and produces customer-specific recommendations. Customers are provided with recommendations that are based on the organization’s unique characteristics,

practices, and risk appetite. ADSAs have been performed for Active Directory installations at Microsoft in addition to those of our customers. Over time, a number of recommendations have been found to be applicable across customers of varying sizes and industries.

Content Origin and Organization

Much of the content of this document is derived from the ADSA and other ACE Team assessments performed for compromised customers and customers who have not experienced significant compromise. Although individual customer data was not used to create this document, we have collected the most commonly exploited vulnerabilities we have identified in our assessments and the recommendations we have made to customers to improve the security of their AD DS installations. Not all vulnerabilities are applicable to all environments, nor are all recommendations feasible to implement in every organization.

This document is organized as follows:

Executive Summary

The Executive Summary, which can be read as a standalone document or in combination with the full document, provides a high-level summary of this document. Included in the Executive Summary are the most common attack vectors we have observed used to compromise customer environments, summary recommendations for securing Active Directory installations, and basic objectives for customers who plan to deploy new AD DS forests now or in the future.

Introduction

This is the section you are reading now.

Avenues to Compromise

This section provides information about some of the most commonly leveraged vulnerabilities we have found to be used by attackers to compromise customers' infrastructures. This section begins with general categories of vulnerabilities and how they are leveraged to initially penetrate customers' infrastructures, propagate compromise across additional systems, and eventually target AD DS and domain controllers to obtain complete control of organizations' forests.

This section does not provide detailed recommendations about addressing each type of vulnerability, particularly in the areas in which the vulnerabilities are not used to directly target Active Directory. However, for each type of vulnerability, we have provided links to additional information that you can use to develop countermeasures and reduce your organization's attack surface.

Reducing the Active Directory Attack Surface

This section begins by providing background information about privileged accounts and groups in Active Directory to provide the information that helps clarify the reasons for the subsequent recommendations for securing and managing privileged groups and accounts. We then discuss approaches to reduce the need to use highly privileged accounts for day-to-day administration, which does not require the level of privilege that is granted to groups such as the Enterprise Admins (EA), Domain

Admins (DA), and Built-in Administrators (BA) groups in Active Directory. Next, we provide guidance for securing the privileged groups and accounts and for implementing secure administrative practices and systems.

Although this section provides detailed information about these configuration settings, we have also included appendices for each recommendation that provide step-by-step configuration instructions that can be used “as is” or can be modified for the organization’s needs. This section finishes by providing information to securely deploy and manage domain controllers, which should be among the most stringently secured systems in the infrastructure.

Monitoring Active Directory for Signs of Compromise

Whether you have implemented robust security information and event monitoring (SIEM) in your environment or are using other mechanisms to monitor the security of the infrastructure, this section provides information that can be used to identify events on Windows systems that may indicate that an organization is being attacked. We discuss traditional and advanced audit policies, including effective configuration of audit subcategories in the Windows 7 and Windows Vista operating systems. This section includes comprehensive lists of objects and systems to audit, and an associated appendix lists events for which you should monitor if the goal is to detect compromise attempts.

Planning for Compromise

This section begins by “stepping back” from technical detail to focus on principles and processes that can be implemented to identify the users, applications, and systems that are most critical not only to the IT infrastructure, but to the business. After identifying what is most critical to the stability and operations of your organization, you can focus on segregating and securing these assets, whether they are intellectual property, people, or systems. In some cases, segregating and securing assets may be performed in your existing AD DS environment, while in other cases, you should consider implementing small, separate “cells” that allow you to establish a secure boundary around critical assets and monitor those assets more stringently than less-critical components. A concept called “creative destruction,” which is a mechanism by which legacy applications and systems can be eliminated by creating new solutions is discussed, and the section ends with recommendations that can help to maintain a more secure environment by combining business and IT information to construct a detailed picture of what is a normal operational state. By knowing what is normal for an organization, abnormalities that may indicate attacks and compromises can be more easily identified.

Summary of Best Practice Recommendations

This section provides a table that summarizes the recommendations made in this document and orders them by relative priority, in addition to providing links to where more information about each recommendation can be found in the document and its appendices.

Appendices

Appendices are included in this document to augment the information contained in the body of the document. The list of appendices and a brief description of each is included the following table.

Appendix	Description
A: Patch and Vulnerability Management Software	Contains a list of companies that produce patch and vulnerability management software.
B: Privileged Accounts and Groups in Active Directory	Provides background information that helps you to identify the users and groups that are granted elevated privileges in Active Directory and on domain-joined systems. These accounts typically present the greatest risk because they can be leveraged by attackers to compromise and even destroy your Active Directory installation.
C: Protected Accounts and Groups in Active Directory	Contains information about protected groups in Active Directory.
D: Securing Built-in Administrator Accounts in Active Directory	Provides guidelines to secure the built-in Administrator account in each domain in a forest.
E: Securing Enterprise Admins Group in Active Directory	Provides step-by-step instructions to help secure the Enterprise Admins group in an Active Directory forest.
F: Securing Domain Admins Groups in Active Directory	Provides step-by-step instructions to help secure the Domain Admins group in each domain in a forest.
G: Securing Administrator Groups in Active Directory	Provides step-by-step instructions to help secure the built-in Administrators group in each domain in a forest.
H: Securing Local Administrator Accounts and Groups	Provides step-by-step instructions to help secure local Administrator accounts and groups on domain-joined systems.
I: Creating Management Accounts for Protected Accounts and Groups in Active Directory	Provides information and steps to create accounts that have limited privileges and can be stringently controlled, but can be used to populate privileged groups in Active Directory when temporary elevation is required.
J: Third-Party RBAC Vendors	Contains a list of third-party, role-based access control (RBAC) software vendors and their solutions.
K: Third-Party PIM Vendors	Contains a list of third-party privileged identity management (PIM) software vendors and their offerings.
L: Events to Monitor	Lists events for which you should monitor in your environment.

Appendix	Description
M: Document Links and Recommended Reading	Contains a list of recommended reading. Also contains a list of links to external documents and their URLs so that readers of hard copies of this document can access this information.

Avenues to Compromise

Law Number Seven: The most secure network is a well-administered one. – 10 Immutable Laws of Security Administration

In organizations that have experienced catastrophic compromise events, assessments usually reveal that the organizations have limited visibility into the actual state of their IT infrastructures, which may differ significantly from their "as documented" states. These variances introduce vulnerabilities that expose the environment to compromise, often with little risk of discovery until the compromise has progressed to the point at which the attackers effectively "own" the environment.

Detailed assessments of these organizations' AD DS configuration, public key infrastructures (PKIs), servers, workstations, applications, access control lists (ACLs), and other technologies reveal misconfigurations and vulnerabilities that, if remediated, could have prevented the initial compromise.

Analysis of IT documentation, processes, and procedures identifies vulnerabilities introduced by gaps in administrative practices that were leveraged by attackers to eventually obtain privileges that were used to fully compromise the Active Directory forest. A fully compromised forest is one in which attackers compromise not only individual systems, applications, or user accounts, but escalate their access to obtain a level of privilege in which they can modify or destroy all aspects of the forest. When an Active Directory installation has been compromised to that degree, attackers can make changes that allow them to maintain a presence throughout the environment, or worse, to destroy the directory and the systems and accounts it manages.

Although a number of the commonly exploited vulnerabilities in the descriptions that follow are not attacks against Active Directory, they allow attackers to establish a foothold in an environment that can be used to run privilege escalation (also called privilege elevation) attacks and to eventually target and compromise AD DS.

This section of this document focuses on describing the mechanisms that attackers typically use to gain access to the infrastructure and eventually to launch privilege elevation attacks. Also see the following sections:

- Reducing the Active Directory Attack Surface Detailed recommendations for the secure configuration of Active Directory.
- Monitoring Active Directory for Signs of Compromise Recommendations to help detect compromise
- Planning for Compromise High-level approaches to help prepare for attacks against the infrastructure from IT and business perspectives

> **Note**
>
> Although this document focuses on Active Directory and Windows systems that are part of an AD DS domain, attackers rarely focus solely on Active Directory and Windows. In environments with a mixture of operating systems, directories, applications, and data repositories, it is common to find that non-Windows systems have also been compromised. This is particularly true if the systems provide a "bridge" between Windows and non-Windows environments, such as file servers accessed by Windows and UNIX or Linux clients, directories that provide authentication services to multiple operating systems, or metadirectories that synchronize data across disparate directories.
>
> AD DS is targeted because of the centralized access and configuration management capabilities it provides not only to Windows systems, but to other clients. Any other directory or application that provides authentication and configuration management services can, and will be targeted by determined attackers. Although this document is focused on protections that can reduce the likelihood of a compromise of Active Directory installations, every organization that includes non-Windows computers, directories, applications, or data repositories should also prepare for attacks against those systems.

Initial Breach Targets

Nobody intentionally builds an IT infrastructure that exposes the organization to compromise. When an Active Directory forest is first constructed, it is usually pristine and current. As years pass and new operating systems and applications are acquired, they're added to the forest. As the manageability benefits that Active Directory provides are recognized, more and more content is added to the directory, more people integrate their computers or applications with AD DS, and domains are upgraded to support new functionality offered by the most current versions of the Windows operating system. What also happens over time, however, is that even as a new infrastructure is being added, other parts of the infrastructure might not be maintained as well as they initially were, systems and applications are functioning properly and therefore are not receiving attention, and organizations begin to forget that they have not eliminated their legacy infrastructure. Based on what we see in assessing compromised infrastructures, the older, larger, and more complex the environment, the more likely it is that there are numerous instances of commonly exploited vulnerabilities.

Regardless of the motivation of the attacker, most information security breaches start with the compromise of one or two systems at a time. These initial events, or entry points into the network, often leverage vulnerabilities that could have been fixed, but were not. The 2012 Data Breach Investigations Report (DBIR), which is an annual study produced by the Verizon RISK Team in cooperation with a number of national security agencies and other companies, states that 96 percent of attacks were "not highly difficult," and that "97 percent of breaches were avoidable through simple or

intermediate controls.” These findings may be a direct consequence of the commonly exploited vulnerabilities that follow.

Gaps in Antivirus and Antimalware Deployments

Law Number Eight: An out-of-date malware scanner is only marginally better than no scanner at all. - Ten Immutable Laws of Security (Version 2.0)

Analysis of organizations’ antivirus and antimalware deployments often reveals an environment in which most workstations are configured with antivirus and antimalware software that is enabled and current. Exceptions are usually workstations that connect infrequently to the corporate environment or employee devices for which antivirus and antimalware software can be difficult to deploy, configure, and update.

Server populations, however, tend to be less consistently protected in many compromised environments. As reported in the 2012 Data Breach Investigations Report, 94 percent of all data compromises involved servers, which represents an 18 percent increase over the previous year, and 69 percent of attacks incorporated malware. In server populations, it is not uncommon to find that antivirus and antimalware installations are inconsistently configured, outdated, misconfigured, or even disabled. In some cases, the antivirus and antimalware software is disabled by administrative staff, but in other cases, attackers disable the software after compromising a server via other vulnerabilities. When the antivirus and antimalware software is disabled, the attackers then plant malware on the server and focus on propagating compromise across the server population.

It is important not only to ensure that your systems are protected with current, comprehensive malware protection, but also to monitor systems for disabling or removal of antivirus and antimalware software and to automatically restart protection when it is manually disabled. Although no antivirus and antimalware software can guarantee prevention and detection of all infections, a properly configured and deployed antivirus and antimalware implementation can reduce the likelihood of infection.

Incomplete Patching

Law Number Three: If you don’t keep up with security fixes, your network won’t be yours for long. – 10 Immutable Laws of Security Administration

Microsoft releases security bulletins on the second Tuesday of each month, although on rare occasions security updates are released between the monthly security updates (these are also known as “out-of-band” updates) when the vulnerability is determined to pose an urgent risk to customer systems. Whether a small business configures its Windows computers to use Windows Update to manage system and application patching or a large organization uses management software such as System Center Configuration Manager (SCCM) to deploy patches according to detailed, hierarchical plans, many customers patch their Windows infrastructures in a relatively timely manner.

However, few infrastructures include only Windows computers and Microsoft applications, and in compromised environments, it is common to find that the organization’s patch management strategy contains gaps. Windows systems in these environments are inconsistently patched. Non-Windows operating systems are patched

sporadically, if at all. Commercial off-the-shelf (COTS) applications contain vulnerabilities for which patches exist, but have not been applied. Networking devices are often configured with factory-default credentials and no firmware updates years after their installation. Applications and operating systems that are no longer supported by their vendors are often kept running, despite the fact that they can no longer be patched against vulnerabilities. Each of these unpatched systems represents another potential entry point for attackers.

The consumerization of IT has introduced additional challenges in that employee owned devices are being used to access corporate owned data, and the organization may have little to no control over the patching and configuration of employees' personal devices. Enterprise-class hardware typically ships with enterprise-ready configuration options and management capabilities, at the cost of less choice in individual customization and device selection. Employee-focused hardware offers a broader range of manufacturers, vendors, hardware security features, software security features, management capabilities and configuration options, and many enterprise features may be absent altogether.

Patch and Vulnerability Management Software

If an effective patch management system is in place for the Windows systems and Microsoft applications, part of the attack surface that unpatched vulnerabilities create has been addressed. However, unless the non-Windows systems, non-Microsoft applications, network infrastructure, and employee devices are also kept up-to-date on patches and other fixes, the infrastructure remains vulnerable. In some cases, an application's vendor may offer automatic update capabilities; in others, there may be a need to devise an approach to regularly retrieve and apply patches and other fixes. Although specific product recommendations cannot be made here, Appendix A: Patch and Vulnerability Management Software includes information about commercially available patch and vulnerability management software provided by Microsoft Partners.

Outdated Applications and Operating Systems

"You can't expect a six-year-old operating system to protect you against a six-month-old attack." – Information Security Professional with 10 years of experience securing enterprise installations

Although "get current, stay current" may sound like a marketing phrase, outdated operating systems and applications create risk in many organizations' IT infrastructures. An operating system that was released in 2003 might still be supported by the vendor and provided with updates to address vulnerabilities, but that operating system might not contain security features added in newer versions of the operating system. Outdated systems can even require weakening of certain AD DS security configuration to support the lesser capabilities of those computers.

Applications that were written to use legacy authentication protocols by vendors who are no longer supporting the application usually cannot be retooled to support stronger authentication mechanisms. However, an organization's Active Directory domain may still be configured to store LAN Manager hashes or reversibly encrypted passwords to support such applications. Applications written prior to the introduction of newer operating systems may not function well or at all on current operating systems, requiring organizations to maintain older and older systems, and in some cases, completely unsupported hardware and software.

Even in cases in which organizations have updated their domain controllers to Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008, it is typical to find significant portions of the member server population to be running Windows Server 2003 (which is no longer in mainstream support), or even Windows 2000 Server or Windows NT Server 4.0 (which are completely unsupported). The longer an organization maintains aging systems, the more the disparity between feature sets grows, and the more likely it becomes that production systems will be unsupported. Additionally, the longer an Active Directory forest is maintained, the more we observe that legacy systems and applications are missed in upgrade plans. This can mean that a single computer running a single application can introduce domain- or forest-wide vulnerabilities because Active Directory is configured to support its legacy protocols and authentication mechanisms.

To eliminate legacy systems and applications, you should first focus on identifying and cataloging them, then on determining whether to upgrade or replace the application or host. Although it can be difficult to find replacements for highly specialized applications for which there is neither support nor an upgrade path, you may be able to leverage a concept called “creative destruction” to replace the legacy application with a new application that provides the necessary functionality. Creative destruction is described in more depth in Planning for Compromise later in this document.

Misconfiguration

Law Number Four: It doesn’t do much good to install security fixes on a computer that was never secured to begin with. – 10 Immutable Laws of Security Administration

Even in environments where systems are generally kept current and patched, we commonly identify gaps or misconfigurations in the operating system, applications running on computers, and Active Directory. Some misconfigurations expose only the local computer to compromise, but after a computer is “owned,” attackers usually focus on further propagating the compromise across other systems and eventually to Active Directory. Following are some of the common areas in which we identify configurations that introduce risk.

In Active Directory

The accounts in Active Directory that are most commonly targeted by attackers are those that are members of the most-highly privileged groups, such as members of the Domain Admins (DA), Enterprise Admins (EA), or built-in Administrators (BA) groups in Active Directory. The membership of these groups should be reduced to the smallest number of accounts possible so that the attack surface of these groups is limited. It is even possible to eliminate “permanent” membership in these privileged groups; that is, you can implement settings that allow you to temporarily populate these groups only when their domain- and forest-wide privileges are needed. When highly privileged accounts are used, they should be used only on designated, secure systems such as domain controllers or secure administrative hosts. Detailed information to help implement all of these configurations is provided in Reducing the Active Directory Attack Surface later in this document.

When we evaluate the membership of the highest privileged groups in Active Directory, we commonly find excessive membership in all three of the most-

privileged groups. In some cases, organizations have dozens, even hundreds of accounts in DA groups. In other cases, organizations place accounts directly into built-in Administrators groups, thinking that that group is “less privileged” than the DAs group. It is not. We often find a handful of permanent members of the EA group in the forest root domain, despite the fact that EA privileges are rarely and temporarily required. Finding an IT user’s day-to-day administrative account in all three groups is also common, even though this is an effectively redundant configuration. As described in Privileged Accounts and Groups in Active Directory in this document, whether an account is a permanent member of one of these groups or all of them, the account can be used to compromise, and even destroy the AD DS environment and the systems and accounts managed by it. Recommendations for the secure configuration and use of privileged accounts in Active Directory are provided in Implementing Least-Privilege Administrative Models.

On Domain Controllers

When we assess domain controllers, we find often find them configured and managed no differently than member servers. Domain controllers sometimes run the same applications and utilities installed on member servers, not because they’re needed on the domain controllers, but because the applications are part of a standard build. These applications may provide minimal functionality on the domain controllers but add significantly to its attack surface by requiring configuration setting that open ports, create highly privileged service accounts, or grant access to the system by users who should not connect to a domain controller for any purpose other than authentication and Group Policy application. In some breaches, attackers have used tools that were already installed on domain controllers not only to gain access to the domain controllers, but to modify or damage the AD DS database.

When we extract the Internet Explorer® configuration settings on domain controllers, we find that users have logged on with accounts that have high levels of privilege in Active Directory and have used the accounts to access the Internet and intranet from the domain controllers. In some cases, the accounts have configured Internet Explorer settings on the domain controllers to allow download of Internet content, and freeware utilities have been downloaded from Internet sites and installed on the domain controllers. Internet Explorer Enhanced Security Configuration is enabled for Users and Administrators by default, yet we often observe that is has been disabled for Administrators. When a highly privileged account accesses the Internet and downloads content to any computer, that computer is put at severe risk. When the computer is a domain controller, the entire AD DS installation is put at risk.

Protecting Domain Controllers

Domain controllers should be treated as critical infrastructure components, secured more stringently and configured more rigidly than file, print, and application servers. Domain controllers should not run any software that is not required for the domain controller to function or doesn’t protect the domain controller against attacks. Domain controllers should not be permitted to access the Internet, and security settings should be configured and enforced by Group Policy Objects (GPOs). Detailed recommendations for the secure installation, configuration, and management of domain controllers are provided in the Securing Domain Controllers Against Attack section of this document.

Within the Operating System

Law Number Two: If a bad guy can alter the operating system on your computer, it's not your computer anymore. – Ten Immutable Laws of Security (Version 2.0)

Although some organizations create baseline configurations for servers of different types and allow limited customization of the operating system after it's installed, analysis of compromised environments often uncovers large numbers of servers deployed in an ad hoc fashion, and configured manually and independently. Configurations between two servers performing the same function may be completely different, where neither server is configured securely. Conversely, server configuration baselines may be consistently enforced, but also consistently misconfigured; that is, servers are configured in a manner that creates the same vulnerability on all servers of a given type. Misconfiguration includes practices such as disabling of security features, granting excessive rights and permissions to accounts (particularly service accounts), use of identical local credentials across systems, and permitting installation of unauthorized applications and utilities that create vulnerabilities of their own.

Disabling Security Features

Organizations sometimes disable Windows Firewall with Advanced Security (WFAS) out of a belief that WFAS is difficult to configure or requires work-intensive configuration. However, beginning with Windows Server 2008, when any role or feature is installed on a server, it is configured by default with the least privileges required for the role or feature to function, and the Windows Firewall is automatically configured to support the role or feature. By disabling WFAS (and not using another host-based firewall in its place), organizations increase the attack surface of the entire Windows environment. Perimeter firewalls provide some protection against attacks that directly target an environment from the Internet, but they provide no protection against attacks that exploit other attack vectors such as drive-by download attacks, or attacks that originate from other compromised systems on the intranet.

User Account Control (UAC) settings are sometimes disabled on servers because administrative staff find the prompts intrusive. Although Microsoft Support article 2526083 describes scenarios in which UAC may be disabled on Windows Server, unless you are running a server core installation (where UAC is disabled by design), you should not disable UAC on servers without careful consideration and research.

In other cases, server settings are configured to less-secure values because organizations apply outdated server configuration settings to new operating systems, such as applying Windows Server 2003 baselines to computers running Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008, without changing the baselines to reflect the changes in the operating system. Rather than carrying old server baselines to new operating systems, when deploying a new operating system, review security changes and configuration settings to ensure that the settings implemented are applicable and appropriate for the new operating system.

Granting Excessive Privilege

In nearly every environment we have assessed, excessive privilege is granted to local and domain-based accounts on Windows systems. Users are granted local Administrator rights on their workstations, member servers run services that are

configured with rights beyond what they need to function, and local Administrators groups across the server population contain dozens or even hundreds of local and domain accounts. Compromise of only one privileged account on a computer allows attackers to compromise the accounts of every user and service that logs on to the computer, and to harvest and leverage credentials to propagate the compromise to other systems.

Although pass-the-hash (PTH) and other credential theft attacks are ubiquitous today, it is because there is freely available tooling that makes it simple and easy to extract the credentials of other privileged accounts when an attacker has gained Administrator- or SYSTEM-level access to a computer. Even without tooling that allows harvesting of credentials from logon sessions, an attacker with privileged access to a computer can just as easily install keystroke loggers that capture keystrokes, screenshots, and clipboard contents. An attacker with privileged access to a computer can disable antimalware software, install rootkits, modify protected files, or install malware on the computer that automates attacks or turns a server into a drive-by download host.

The tactics used to extend a breach beyond a single computer vary, but the key to propagating compromise is the acquisition of highly privileged access to additional systems. By reducing the number of accounts with privileged access to any system, you reduce the attack surface not only of that computer, but the likelihood of an attacker harvesting valuable credentials from the computer.

Standardizing Local Administrator Credentials

There has long been debate among security specialists as to whether there is value in renaming local Administrator accounts on Windows computers. What is actually important about local Administrator accounts is whether they are configured with the same user name and password across multiple computers.

If the local Administrator account is named to the same value across servers and the password assigned to the account is also configured to the same value, attackers can extract the account's credentials on one computer on which Administrator or SYSTEM-level access has been obtained. The attacker does not have to initially compromise the Administrator account; they need only compromise the account of a user who is a member of the local Administrators group, or of a service account that is configured to run as LocalSystem or with Administrator privileges. The attacker can then extract the credentials for the Administrator account and replay those credentials in network logons to other computers on the network.

As long as another computer has a local account with the same user name and password (or password hash) as the account credentials that are being presented, the logon attempt succeeds and the attacker obtains privileged access to the targeted computer. In current versions of Windows, the built-in Administrator account is disabled by default, but in legacy operating systems, the account is enabled by default.

> **Note**
>
> Some organizations have intentionally configured local Administrator accounts to be enabled in the belief that this provides a “failsafe” in case all other privileged accounts are locked out of a system. However, even if the local Administrator account is disabled and there are no other accounts available that can enable the account or log on to the system with Administrator privileges, the system can be booted into safe mode and the built-in local Administrator account can be re-enabled, as described in Microsoft Support article 814777. Additionally, if the system still successfully applies GPOs, a GPO can be modified to (temporarily) re-enable the Administrator account, or Restricted Groups can be configured to add a domain-based account to the local Administrators group. Repairs can be performed and the Administrator account can again be disabled. To effectively prevent a lateral compromise that uses built-in local Administrator account credentials, unique user names and passwords must be configured for local Administrator accounts. To deploy unique passwords for local Administrator accounts via a GPO, see Solution for management of built-in Administrator account's password via GPO on the MSDN website.

Permitting Installation of Unauthorized Applications

Law Number One: If a bad guy can persuade you to run his program on your computer, it’s not solely your computer anymore. – Ten Immutable Laws of Security (Version 2.0)

Whether an organization deploys consistent baseline settings across servers, the installation of applications that are not part of a server’s defined role should not be permitted. By allowing software to be installed that is not part of a server’s designated functionality, servers are exposed to inadvertent or malicious installation of software that increases the server’s attack surface, introduces application vulnerabilities, or causes system instability.

Applications

As described earlier, applications are often installed and configured to use accounts that are granted more privilege than the application actually requires. In some cases, the application’s documentation specifies that service accounts must be members of a server’s local Administrators group or must be configured to run in the context of the LocalSystem. This is often not because the application requires those rights, but because determining what rights and permissions an application’s service accounts need requires investment in additional time and effort. If an application does not install with the minimum privileges required for the application and its configured features to function, the system is exposed to attacks that leverage application privileges without any attack against the operating system itself.

Lack of Secure Application Development Practices

Infrastructure exists to support business workloads. Where these workloads are implemented in custom applications, it is critical to ensure that the applications are developed using secure best practices. Root-cause analysis of enterprise-wide

incidents often reveals that an initial compromise is effected through custom applications–particularly those that are Internet facing. Most of these compromises are accomplished via compromise of well-known attacks such as SQL injection (SQLi) and cross-site scripting (XSS) attacks.

SQL Injection is an application vulnerability that allows user-defined input to modify a SQL statement that is passed to the database for execution. This input can be provided via a field in the application, a parameter (such as the query string or a cookie), or other methods. The result of this injection is that the SQL statement provided to the database is fundamentally different than what the developer intended. Take, for example, a common query used in the evaluation of a user name/password combination:

SELECT userID FROM users WHERE username = ‘sUserName’ AND password = ‘sPassword’

When this is received by the database server, it instructs the server to look through the users table and return any userID record where the user name and password match those provided by the user (presumably via a login form of some kind). Naturally the intent of the developer in this case is to only return a valid record if a correct user name and password can be provided by the user. If either is incorrect, the database server will be unable to find a matching record and return an empty result.

The issue occurs when an attacker does something unexpected such as providing their own SQL in place of valid data. Because SQL is interpreted on-the-fly by the database server, the injected code would be processed as if the developer had put it in himself. For example, if the attacker entered **“administrator”** for the user ID and **“xyz”** OR **“1=1”** as the password, the resulting statement processed by the database would be:

SELECT userID FROM users WHERE username = ‘administrator’ AND password = ‘xyz’ OR 1=1

When this query is processed by the database server, all rows in the table will be returned in the query because 1=1 will always evaluate to True, thus it doesn’t matter if the correct username and password is known or provided. The net result in most cases is that the user will be logged on as the first user in the user’s database; in most cases, this will be the administrative user.

In addition to simply logging on, malformed SQL statements such as this can be used to add, delete, or change data, or even drop (delete) entire tables from a database. In the most extreme cases where SQLi is combined with excessive privilege, operating system commands can be run to enable the creation of new users, to download attack tools, or to take any other actions of the attackers choosing.

In cross-site scripting, the vulnerability is introduced in the application’s output. An attack begins with an attacker providing malformed data to the application, but in this case the malformed data is in the form of scripting code (such as JavaScript) that will be run by the victim’s browser. Exploit of an XSS vulnerability can allow an attacker to run any functions of the target application in the context of the user who launched the browser. XSS attacks are typically initiated by a phishing email

encouraging the user to click a link that connects to the application and runs the attack code.

XSS is often exploited in online banking and e-commerce scenarios where an attacker can make purchases or transfer money in the context of the exploited user. In the case of a targeted attack on a custom web-based identity management application, it can allow an attacker to create their own identities, modify permissions and rights, and lead to a systemic compromise.

Although a full discussion of cross-site scripting and SQL injection is outside the scope of this document, the Open Web Application Security Project (OWASP) publishes a top 10 list with in-depth discussion of the vulnerabilities and countermeasures.

Regardless of the investment in infrastructure security, if poorly designed and written applications are deployed within that infrastructure, the environment is made vulnerable to attacks. Even well-secured infrastructures often cannot provide effective countermeasures to these application attacks. Compounding the problem, poorly designed applications may require that service accounts be granted excessive permissions for the application to function.

The Microsoft Security Development Lifecycle (SDL) is a set of structural process controls that work to improve security beginning early in requirements gathering and extending through the lifecycle of the application until it is decommissioned. This integration of effective security controls is not only critical from a security perspective, it is critical to ensure that application security is cost and schedule effective. Assessing an application for security issues when it is effectively code complete requires organizations to make decisions about application security only before or even after the application has been deployed. An organization can choose to address the application flaws before deploying the application in production, incurring costs and delays, or the application can be deployed in production with known security flaws, exposing the organization to compromise.

Some organizations place the full cost of fixing a security issue in production code above $10,000 per issue, and applications developed without an effective SDL can average more than ten high-severity issues per 100,000 lines of code. In large applications, the costs escalate quickly. By contrast, many companies set a benchmark of less than one issue per 100,000 lines of code at the final code review stage of the SDL, and aim for zero issues in high-risk applications in production.

Implementing the SDL improves security by including security requirements early in requirements gathering and design of an application provides threat modeling for high-risk applications; requires effective training and monitoring of developers; and requires clear, consistent code standards and practices. The net effect of an SDL is significant improvements in application security while reducing the cost to develop, deploy, maintain, and decommission an application. Although a detailed discussion of the design and implementation of SDL is beyond the scope of this document, refer to the Microsoft Security Development Lifecycle for detailed guidance and information.

Attractive Accounts for Credential Theft

Credential theft attacks are those in which an attacker initially gains highest-privilege (root, Administrator, or SYSTEM, depending on the operating system in

use) access to a computer on a network and then uses freely available tooling to extract credentials from the sessions of other logged-on accounts. Depending on the system configuration, these credentials can be extracted in the form of hashes, tickets, or even plaintext passwords. If any of the harvested credentials are for local accounts that are likely to exist on other computers on the network (for example, Administrator accounts in Windows, or root accounts in OSX, UNIX, or Linux), the attacker presents the credentials to other computers on the network to propagate compromise to additional computers and to try to obtain the credentials of two specific types of accounts:

1. Privileged domain accounts with both broad and deep privileges (that is, accounts that have administrator-level privileges on many computers and in Active Directory). These accounts may not be members of any of the highest-privilege groups in Active Directory, but they may have been granted Administrator-level privilege across many servers and workstations in the domain or forest, which makes them effectively as powerful as members of privileged groups in Active Directory. In most cases, accounts that have been granted high levels of privilege across broad swaths of the Windows infrastructure are service accounts, so service accounts should always be assessed for breadth and depth of privilege.
2. “Very Important Person” (VIP) domain accounts. In the context of this document, a VIP account is any account that has access to information an attacker wants (intellectual property and other sensitive information), or any account that can be used to grant the attacker access to that information. Examples of these user accounts include:
    a. Executives whose accounts have access to sensitive corporate information
    b. Accounts for Help Desk staff who are responsible for maintaining the computers and applications used by executives
    c. Accounts for legal staff who have access to an organization’s bid and contract documents, whether the documents are for their own organization or client organizations
    d. Product planners who have access to plans and specifications for products in an company’s development pipeline, regardless of the types of products the company makes
    e. Researchers whose accounts are used to access study data, product formulations, or any other research of interest to an attacker

Because highly privileged accounts in Active Directory can be used to propagate compromise and to manipulate VIP accounts or the data that they can access, the most useful accounts for credential theft attacks are accounts that are members of Enterprise Admins, Domain Admins, and Administrators groups in Active Directory.

Because domain controllers are the repositories for the AD DS database and domain controllers have full access to all of the data in Active Directory, domain controllers are also targeted for compromise, whether in parallel with credential theft attacks, or after one or more highly privileged Active Directory accounts have been compromised. Although numerous publications (and many attackers) focus on the Domain Admins group memberships when describing pass-the-hash and other credential theft attacks (as is described in Privileged Accounts and Groups in Active Directory later in this

document), an account that is a member of any of the groups listed here can be used to compromise the entire AD DS installation.

> **Note**
>
> For comprehensive information about pass-the-hash and other credential theft attacks, please see the Mitigating Pass-the-Hash (PTH) Attacks and Other Credential Theft Techniques whitepaper listed in Appendix M: Document Links and Recommended Reading. For more information about attacks by determined adversaries, which are sometimes referred to as “advanced persistent threats” (APTs), please see Determined Adversaries and Targeted Attacks.

Activities that Increase the Likelihood of Compromise

Because the target of credential theft is usually highly privileged domain accounts and VIP accounts, it is important for administrators to be conscious of activities that increase the likelihood of success of a credential-theft attack. Although attackers also target VIP accounts, if VIPs are not given high levels of privilege on systems or in the domain, theft of their credentials requires other types of attacks, such as socially engineering the VIP to provide secret information. Or the attacker must first obtain privileged access to a system on which VIP credentials are cached. Because of this, activities that increase the likelihood of credential theft described here are focused primarily on preventing the acquisition of highly privileged administrative credentials. These activities are common mechanisms by which attackers are able to compromise systems to obtain privileged credentials.

Logging on to Unsecured Computers with Privileged Accounts

The core vulnerability that allows credential theft attacks to succeed is the act of logging on to computers that are not secure with accounts that are broadly and deeply privileged throughout the environment. These logons can be the result of various misconfigurations described here.

Not Maintaining Separate Administrative Credentials

Although this is relatively uncommon, in assessing various AD DS installations, we have found IT employees using a single account for all of their work. The account is a member of at least one of the most highly privileged groups in Active Directory and is the same account that the employees use to log on to their workstations in the morning, check their email, browse Internet sites, and download content to their computers. When users run with accounts that are granted local Administrator rights and permissions, they expose the local computer to complete compromise. When those accounts are also members of the most privileged groups in Active Directory, they expose the entire forest to compromise, making it trivially easy for an attacker to gain complete control of the Active Directory and Windows environment.

Similarly, in some environments, we’ve found that the same user names and passwords are used for root accounts on non-Windows computers as are used in the Windows environment, which allows attackers to extend compromise from UNIX or Linux systems to Windows systems and vice versa.

Logons to Compromised Workstations or Member Servers with Privileged Accounts

When a highly privileged domain account is used to log on interactively to a compromised workstation or member server, that compromised computer may harvest credentials from any account that logs on to the system.

Unsecured Administrative Workstations

In many organizations, IT staff use multiple accounts. One account is used for logon to the employee's workstation, and because these are IT staff, they often have local Administrator rights on their workstations. In some cases, UAC is left enabled so that the user at least receives a split access token at logon and must elevate when privileges are required. When these users are performing maintenance activities, they typically use locally installed management tools and provide the credentials for their domain-privileged accounts, by selecting the **Run as Administrator** option or by providing the credentials when prompted. Although this configuration may seem appropriate, it exposes the environment to compromise because:

- The "regular" user account that the employee uses to log on to their workstation has local Administrator rights, the computer is vulnerable to drive-by download attacks in which the user is convinced to install malware.
- The malware is installed in the context of an administrative account, the computer can now be used to capture keystrokes, clipboard contents, screenshots, and memory-resident credentials, any of which can result in exposure of the credentials of a powerful domain account.

The problems in this scenario are twofold. First, although separate accounts are used for local and domain administration, the computer is unsecured and does not protect the accounts against theft. Second, the regular user account and the administrative account have been granted excessive rights and permissions.

Browsing the Internet with a Highly Privileged Account

Users who log on to computers with accounts that are members of the local Administrators group on the computer, or members of privileged groups in Active Directory, and who then browse the Internet (or a compromised intranet) expose the local computer and the directory to compromise.

Accessing a maliciously crafted website with a browser running with administrative privileges can allow an attacker to deposit malicious code on the local computer in the context of the privileged user. If the user has local Administrator rights on the computer, attackers may deceive the user into downloading malicious code or opening email attachments that leverage application vulnerabilities and leverage the user's privileges to extract locally cached credentials for all active users on the computer. If the user has administrative rights in the directory by membership in the Enterprise Admins, Domain Admins, or Administrators groups in Active Directory, the attacker can extract the domain credentials and use them to compromise the entire AD DS domain or forest, without needing to compromise any other computer in the forest.

Configuring Local Privileged Accounts with the Same Credentials across Systems

Configuring the same local Administrator account name and password on many or all computers enables credentials stolen from the SAM database on one computer to be used to compromise all other computers that use the same credentials. At a minimum, you should use different passwords for local Administrator accounts across each domain-joined system. Local Administrator accounts may also be uniquely named, but using different passwords for each system's privileged local accounts is sufficient to ensure that credentials cannot be used on other systems.

Overpopulation and Overuse of Privileged Domain Groups

Granting membership in the EA, DA, or BA groups in a domain creates a target for attackers. The greater the number of members of these groups, the greater the likelihood that a privileged user may inadvertently misuse the credentials and expose them to credential theft attacks. Every workstation or server to which a privileged domain user logs on presents a possible mechanism by which the privileged user's credentials may be harvested and used to compromise the AD DS domain and forest.

Poorly Secured Domain Controllers

Domain controllers house a replica of a domain's AD DS database. In the case of read-only domain controllers, the local replica of the database contains the credentials for only a subset of the accounts in the directory, none of which are privileged domain accounts by default. On read-write domain controllers, each domain controller maintains a full replica of the AD DS database, including credentials not only for privileged users like Domain Admins, but privileged accounts such as domain controller accounts or the domain's Krbtgt account, which is the account that is associated with the KDC service on domain controllers. If additional applications that are not necessary for domain controller functionality are installed on domain controllers, or if domain controllers are not stringently patched and secured, attackers may compromise them via unpatched vulnerabilities, or they may leverage other attack vectors to install malicious software directly on them.

Privilege Elevation and Propagation

Regardless of the attack methods used, Active Directory is always targeted when a Windows environment is attacked, because it ultimately controls access to whatever the attackers want. This does not mean that the entire directory is targeted, however. Specific accounts, servers, and infrastructure components are usually the primary targets of attacks against Active Directory. These accounts are described as follows.

Permanent Privileged Accounts

Because the introduction of Active Directory, it has been possible to use highly privileged accounts to build the Active Directory forest and then to delegate rights and permissions required to perform day-to-day administration to less-privileged accounts. Membership in the Enterprise Admins, Domain Admins, or Administrators groups in Active Directory is required only temporarily and infrequently in an environment that implements least-privilege approaches to daily administration.

Permanent privileged accounts are accounts that have been placed in privileged groups and left there from day to day. If your organization places five accounts into the Domain Admins group for a domain, those five accounts can be targeted 24-hours a day, seven days a week. However, the actual need to use accounts with Domain Admins privileges is typically only for specific domain-wide configuration, and for short periods of time.

VIP Accounts

An often overlooked target in Active Directory breaches is the accounts of "very important persons" (or VIPs) in an organization. Privileged accounts are targeted because those accounts can grant access to attackers, which allows them to compromise or even destroy targeted systems, as described earlier in this section.

"Privilege-Attached" Active Directory Accounts

"Privilege-attached" Active Directory accounts are domain accounts that have not been made members of any of the groups that have the highest levels of privilege in Active Directory, but have instead been granted high levels of privilege on many servers and workstations in the environment. These accounts are most often domain-based accounts that are configured to run services on domain-joined systems, typically for

applications running on large sections of the infrastructure. Although these accounts have no privileges in Active Directory, if they are granted high privilege on large numbers of systems, they can be used to compromise or even destroy large segments of the infrastructure, achieving the same effect as compromise of a privileged Active Directory account.

Reducing the Active Directory Attack Surface

This section focuses on technical controls to implement to reduce the attack surface of the Active Directory installation. The section contains the following information:

- Privileged Accounts and Groups in Active Directory discusses the highest-privileged accounts and groups and the mechanisms to protect privileged accounts in Active Directory.
- Implementing Least-Privilege Administrative Models focuses on identifying the risk that the use of highly privileged accounts for day-to-day administration presents, in addition to providing recommendations to implement to reduce the risk that privileged accounts present.
- Implementing Secure Administrative Hosts describes principles for deployment of dedicated, secure administrative systems, in addition to some sample approaches to a secure administrative host deployment.
- Securing Domain Controllers Against Attack discusses policies and settings that, although similar to the recommendations for the implementation of secure administrative hosts, contain some domain controller-specific recommendations to help ensure that the domain controllers and the systems used to manage them are well-secured.

Privileged Accounts and Groups in Active Directory

This section provides background information about privileged accounts and groups in Active Directory intended to explain the commonalities and differences between privileged accounts and groups in Active Directory. By understanding these distinctions, whether you implement the recommendations in Implementing Least-Privilege Administrative Models verbatim or choose to customize them for your organization, you have the tools you need to secure each group and account appropriately.

Built-in Privileged Accounts and Groups

Active Directory facilitates delegation of administration and supports the principle of least privilege in assigning rights and permissions. “Regular” users who have accounts in a domain are, by default, able to read much of what is stored in the directory, but are able to change only a very limited set of data in the directory. Users who require additional privilege can be granted membership in various “privileged” groups that are built into the directory so that they may perform specific tasks related to their roles, but cannot perform tasks that are not relevant to their duties. Organizations can also create groups that are tailored to specific job responsibilities and are granted granular rights and permissions that allow IT staff to perform day-to-day administrative functions without granting rights and permissions that exceed what is required for those functions.

Within Active Directory, three built-in groups are the highest privilege groups in the directory: Enterprise Admins, Domain Admins, and Administrators. The default

configuration and capabilities of each of these groups are described in the following sections:

Highest Privilege Groups in Active Directory

Enterprise Admins

Enterprise Admins (EA) is a group that exists only in the forest root domain, and by default, it is a member of the Administrators group in all domains in the forest. The built-in Administrator account in the forest root domain is the only default member of the EA group. EAs are granted rights and permissions that allow them to implement forest-wide changes (that is, changes that affect all domains in the forest), such as adding or removing domains, establishing forest trusts, or raising forest functional levels. In a properly designed and implemented delegation model, EA membership is required only when first constructing the forest or when making certain forest-wide changes such as establishing an outbound forest trust. Most of the rights and permissions granted to the EA group can be delegated to lesser-privileged users and groups.

Domain Admins

Each domain in a forest has its own Domain Admins (DA) group, which is a member of that domain's Administrators group and a member of the local Administrators group on every computer that is joined to the domain. The only default member of the DA group for a domain is the built-in Administrator account for that domain. DAs are "all-powerful" within their domains, while EAs have forest-wide privilege. In a properly designed and implemented delegation model, Domain Admins membership should be required only in "break glass" scenarios (such as situations in which an account with high levels of privilege on every computer in the domain is needed). Although native Active Directory delegation mechanisms allow delegation to the extent that it is possible to use DA accounts only in emergency scenarios, constructing an effective delegation model can be time consuming, and many organizations leverage third-party tools to expedite the process.

Administrators

The third group is the built-in domain local Administrators (BA) group into which DAs and EAs are nested. This group is granted many of the direct rights and permissions in the directory and on domain controllers. However, the Administrators group for a domain has no privileges on member servers or on workstations. It is via membership in the computers' local Administrators group that local privilege is granted.

> **Note**
>
> Although these are the default configurations of these privileged groups, a member of any of the three groups can manipulate the directory to gain membership in any of the other groups. In some cases, it is trivial to obtain membership in the other groups, while in others it is more difficult, but from the perspective of potential privilege, all three groups should be considered effectively equivalent.

Schema Admins

A fourth privileged group, Schema Admins (SA), exists only in the forest root domain and has only that domain's built-in Administrator account as a default member, similar to the Enterprise Admins group. The Schema Admins group is intended to be populated only temporarily and occasionally (when modification of the AD DS schema is required).

Although the SA group is the only group that can modify the Active Directory schema (that is., the directory's underlying data structures such as objects and attributes), the scope of the SA group's rights and permissions is more limited than the previously described groups. It is also common to find that organizations have developed appropriate practices for the management of the membership of the SA group because membership in the group is typically infrequently needed, and only for short periods of time. This is technically true of the EA, DA, and BA groups in Active Directory, as well, but it is far less common to find that organizations have implemented similar practices for these groups as for the SA group.

Protected Accounts and Groups in Active Directory

Within Active Directory, a default set of privileged accounts and groups called "protected" accounts and groups are secured differently than other objects in the directory. Any account that has direct or transitive membership in any protected group (regardless of whether the membership is derived from security or distribution groups) inherits this restricted security.

For example, if a user is a member of a distribution group that is, in turn, a member of a protected group in Active Directory, that user object is flagged as a protected account. When an account is flagged as a protected account, the value of the adminCount attribute on the object is set to **1**.

> **Note**
>
> Although transitive membership in a protected group includes nested distribution and nested security groups, accounts that are members of nested distribution groups will not receive the protected group's SID in their access tokens. However, distribution groups can be converted to security groups in Active Directory, which is why distribution groups are included in protected group member enumeration. Should a protected nested distribution group ever be converted to a security group, the accounts that are members of the former distribution group will subsequently receive the parent protected group's SID in their access tokens at the next logon.

The following table lists the default protected accounts and groups in Active Directory by operating system version and service pack level.

Default Protected Accounts and Groups in Active Directory by Operating System and Service Pack (SP) Version

Windows 2000 <SP4	Windows 2000 SP4 – Windows Server 2003	Windows Server 2003 SP1+	Windows Server 2008 – Windows Server 2012
Administrators	Account Operators	Account Operators	Account Operators
	Administrator	Administrator	Administrator
	Administrators	Administrators	Administrators
Domain Admins	Backup Operators	Backup Operators	Backup Operators
	Cert Publishers		
	Domain Admins	Domain Admins	Domain Admins
Enterprise Admins	Domain Controllers	Domain Controllers	Domain Controllers
	Enterprise Admins	Enterprise Admins	Enterprise Admins
	Krbtgt	Krbtgt	Krbtgt
	Print Operators	Print Operators	Print Operators
			Read-only Domain Controllers
	Replicator	Replicator	Replicator
Schema Admins	Schema Admins		Schema Admins

AdminSDHolder and SDProp

In the System container of every Active Directory domain, an object called AdminSDHolder is automatically created. The purpose of the AdminSDHolder object is to ensure that the permissions on protected accounts and groups are consistently enforced, regardless of where the protected groups and accounts are located in the domain.

Every 60 minutes (by default), a process known as Security Descriptor Propagator (SDProp) runs on the domain controller that holds the domain's PDC Emulator role. SDProp compares the permissions on the domain's AdminSDHolder object with the permissions on the protected accounts and groups in the domain. If the permissions on any of the protected accounts and groups do not match the permissions on the AdminSDHolder object, the permissions on the protected accounts and groups are reset to match those of the domain's AdminSDHolder object.

Permissions inheritance is disabled on protected groups and accounts, which means that even if the accounts or groups are moved to different locations in the directory, they do not inherit permissions from their new parent objects. Inheritance is also disabled on the AdminSDHolder object so that permissions changes to the parent objects do not change the permissions of AdminSDHolder.

> **Note**
>
> When an account is removed from a protected group, it is no longer considered a protected account, but its adminCount attribute remains set to **1** if it is not manually changed. The result of this configuration is that the object's ACLs are no longer updated by SDProp, but the object still does not inherit permissions from its parent object. Therefore, the object may reside in an organizational unit (OU) to which permissions have been delegated, but the formerly protected object will not inherit these delegated permissions. A script to locate and reset formerly protected objects in the domain can be found in the Microsoft Support article 817433.

AdminSDHolder Ownership

Most objects in Active Directory are owned by the domain's BA group. However, the AdminSDHolder object is, by default, owned by the domain's DA group. (This is a circumstance in which DAs do not derive their rights and permissions via membership in the Administrators group for the domain.)

In versions of Windows earlier than Windows Server 2008, owners of an object can change permissions of the object, including granting themselves permissions that they did not originally have. Therefore, the default permissions on a domain's AdminSDHolder object prevent users who are members of BA or EA groups from changing the permissions for a domain's AdminSDHolder object. However, members of the Administrators group for the domain can take ownership of the object and grant themselves additional permissions, which means that this protection is rudimentary and only protects the object against accidental modification by users who are not members of the DA group in the domain. Additionally, the BA and EA (where applicable) groups have permission to change the attributes of the AdminSDHolder object in the local domain (root domain for EA).

> **Note**
>
> An attribute on the AdminSDHolder object, dSHeuristics, allows limited customization (removal) of groups that are considered protected groups and are affected by AdminSDHolder and SDProp. This customization should be carefully considered if it is implemented, although there are valid circumstances in which modification of dSHeuristics on AdminSDHolder is useful. More information about modification of the dSHeuristics attribute on an AdminSDHolder object can be found in the Microsoft Support articles 817433 and 973840, and in Appendix C: Protected Accounts and Groups in Active Directory.

Although the most privileged groups in Active Directory are described here, there are a number of other groups that have been granted elevated levels of privilege. For more information about all of the default and built-in groups in Active Directory and the user rights assigned to each, see Appendix B: Privileged Accounts and Groups in Active Directory.

Implementing Least-Privilege Administrative Models

The following excerpt is from The Administrator Accounts Security Planning Guide, first published on April 1, 1999:

> Most security-related training courses and documentation discuss the implementation of a principle of least privilege, yet organizations rarely follow it. The principle is simple, and the impact of applying it correctly greatly increases your security and reduces your risk. The principle states that all users should log on with a user account that has the absolute minimum permissions necessary to complete the current task and nothing more. Doing so provides protection against malicious code, among other attacks. This principle applies to computers and the users of those computers.
>
> One reason this principle works so well is that it forces you to do some internal research. For example, you must determine the access privileges that a computer or user really needs, and then implement them. For many organizations, this task might initially seem like a great deal of work; however, it is an essential step to successfully secure your network environment.
>
> You should grant all domain administrator users their domain privileges under the concept of least privilege. For example, if an administrator logs on with a privileged account and inadvertently runs a virus program, the virus has administrative access to the local computer and to the entire domain. If the administrator had instead logged on with a nonprivileged (nonadministrative) account, the virus's scope of damage would only be the local computer because it runs as a local computer user.
>
> In another example, accounts to which you grant domain-level administrator rights must not have elevated rights in another forest, even if there is a trust relationship between the forests. This tactic helps prevent widespread damage if an attacker manages to compromise one managed forest. Organizations should regularly audit their network to protect against unauthorized escalation of privilege.

The following excerpt is from the Microsoft Windows Security Resource Kit, first published in 2005:

> Always think of security in terms of granting the least amount of privileges required to carry out the task. If an application that has too many privileges should be compromised, the attacker might be able to expand the attack beyond what it would if the application had been under the least amount of privileges possible. For example, examine the consequences of a network administrator unwittingly opening an email attachment that launches a virus. If the administrator is logged on using the domain Administrator account, the virus will have Administrator privileges on all computers in the domain and thus unrestricted access to nearly all data on the network. If the

administrator is logged on using a local Administrator account, the virus will have Administrator privileges on the local computer and thus would be able to access any data on the computer and install malicious software such as key-stroke logging software on the computer. If the administrator is logged on using a normal user account, the virus will have access only to the administrator's data and will not be able to install malicious software. By using the least privileges necessary to read email, in this example, the potential scope of the compromise is greatly reduced.

The Privilege Problem

The principles described in the preceding excerpts have not changed, but in assessing Active Directory installations, we invariably find excessive numbers of accounts that have been granted rights and permissions far beyond those required to perform day-to-day work. The size of the environment affects the raw numbers of overly privileged accounts, but not the proportion—midsized directories may have dozens of accounts in the most highly privileged groups, while large installations may have hundreds or even thousands. With few exceptions, regardless of the sophistication of an attacker's skills and arsenal, attackers typically follow the path of least resistance. They increase the complexity of their tooling and approach only if and when simpler mechanisms fail or are thwarted by defenders.

Unfortunately, the path of least resistance in many environments has proven to be the overuse of accounts with broad and deep privilege. Broad privileges are rights and permissions that allow an account to perform specific activities across a large cross-section of the environment- for example, Help Desk staff may be granted permissions that allow them to reset the passwords on many user accounts.

Deep privileges are powerful privileges that are applied to a narrow segment of the population, such giving an engineer Administrator rights on a server so that they can perform repairs. Neither broad privilege nor deep privilege is necessarily dangerous, but when many accounts in the domain are permanently granted broad and deep privilege, if only one of the accounts is compromised, it can quickly be used to reconfigure the environment to the attacker's purposes or even to destroy large segments of the infrastructure.

Pass-the-hash attacks, which are a type of credential theft attack, are ubiquitous because the tooling to perform them is freely available and easy-to-use, and because many environments are vulnerable to the attacks. Pass-the-hash attacks, however, are not the real problem. The crux of the problem is twofold:

1. It is usually easy for an attacker to obtain deep privilege on a single computer and then propagate that privilege broadly to other computers.
2. There are usually too many permanent accounts with high levels of privilege across the computing landscape.

Even if pass-the-hash attacks are eliminated, attackers would simply use different tactics, not a different strategy. Rather than planting malware that contains credential theft tooling, they might plant malware that logs keystrokes, or leverage any number of other approaches to capture credentials that are powerful across the environment. Regardless of the tactics, the targets remain the same: accounts with broad and deep privilege.

Granting of excessive privilege isn't only found in Active Directory in compromised environments. When an organization has developed the habit of granting more privilege than is required, it is typically found throughout the infrastructure as discussed in the following sections.

In Active Directory

In Active Directory, it is common to find that the EA, DA and BA groups contain excessive numbers of accounts. Most commonly, an organization's EA group contains the fewest members, DA groups usually contain a multiplier of the number of users in the EA group, and Administrators groups usually contain more members than the populations of the other groups combined. This is often due to a belief that Administrators are somehow "less privileged" than DAs or EAs. As the Background portion of this section explains, while the rights and permissions granted to each of these groups differ, they should be effectively considered equally powerful groups because a member of one can make himself or herself a member of the other two.

On Member Servers

When we retrieve the membership of local Administrators groups on member servers in many environments, we find membership ranging from a handful of local and domain accounts, to dozens of nested groups that, when expanded, reveal hundreds, even thousands, of accounts with local Administrator privilege on the servers. In many cases, domain groups with large memberships are nested in member servers' local Administrators groups, without consideration to the fact that any user who can modify the memberships of those groups in the domain can gain administrative control of all systems on which the group has been nested in a local Administrators group.

On Workstations

Although workstations typically have significantly fewer members in their local Administrators groups than member servers do, in many environments, users are granted membership in the local Administrators group on their personal computers. When this occurs, even if UAC is enabled, those users present an elevated risk to the integrity of their workstations.

> **Important**
>
> You should consider carefully whether users require administrative rights on their workstations, and if they do, a better approach may be to create a separate local account on the computer that is a member of the Administrators group. When users require elevation, they can present the credentials of that local account for elevation, but because the account is local, it cannot be used to compromise other computers or access domain resources. As with any local accounts, however, the credentials for the local privileged account should be unique; if you create a local account with the same credentials on multiple workstations, you expose the computers to pass-the-hash attacks.

In Applications

In attacks in which the target is an organization's intellectual property, accounts that have been granted powerful privileges within applications can be targeted to allow exfiltration of data. Although the accounts that have access to sensitive data may have been granted no elevated privileges in the domain or the operating system, accounts that can manipulate the configuration of an application or access to the information the application provides present risk.

In Data Repositories

As is the case with other targets, attackers seeking access to intellectual property in the form of documents and other files can target the accounts that control access to the file stores, accounts that have direct access to the files, or even groups or roles that have access to the files. For example, if a file server is used to store contract documents and access is granted to the documents by the use of an Active Directory group, an attacker who can modify the membership of the group can add compromised accounts to the group and access the contract documents. In cases in which access to documents is provided by applications such as SharePoint, attackers can target the applications as described earlier.

Reducing Privilege

The larger and more complex an environment, the more difficult it is to manage and secure. In small organizations, reviewing and reducing privilege may be a relatively simple proposition, but each additional server, workstation, user account, and application in use in an organization adds another object that must be secured. Because it can be difficult or even impossible to properly secure every aspect of an organization's IT infrastructure, you should focus efforts first on the accounts whose privilege create the greatest risk, which are typically the built-in privileged accounts and groups in Active Directory, and privileged local accounts on workstations and member servers.

Securing Local Administrator Accounts on Workstations and Member Servers

Although this document focuses on securing Active Directory, as has been previously discussed, most attacks against the directory begin as attacks against individual hosts. Full guidelines for securing local groups on member systems cannot be provided, but the following recommendations can be used to help you secure the local Administrator accounts on workstations and member servers.

Securing Local Administrator Accounts

On all versions of Windows currently in mainstream support, the local Administrator account is disabled by default, which makes the account unusable for pass-the-hash and other credential theft attacks. However, in domains containing legacy operating systems or in which local Administrator accounts have been enabled, these accounts can be used as previously described to propagate compromise across member servers and workstations. For this reason, the following controls are recommended for all local Administrator accounts on domain-joined systems.

Detailed instructions for implementing these controls are provided in Appendix H: Securing Local Administrator Accounts and Groups. Before implementing these settings, however, ensure that local Administrator accounts are not currently used in the environment to run services on computers or perform other activities for which these

accounts should not be used. Test these settings thoroughly before implementing them in a production environment.

Controls for Local Administrator Accounts

Built-in Administrator accounts should never be used as service accounts on member servers, nor should they be used to log on to local computers (except in Safe Mode, which is permitted even if the account is disabled). The goal of implementing the settings described here is to prevent each computer's local Administrator account from being usable unless protective controls are first reversed. By implementing these controls and monitoring Administrator accounts for changes, you can significantly reduce the likelihood of success of an attack that targets local Administrator accounts.

Configuring GPOs to Restrict Administrator Accounts on Domain-Joined Systems

In one or more GPOs that you create and link to workstation and member server OUs in each domain, add the Administrator account to the following user rights in **Computer Configuration\Policies\Windows Settings\Security Settings\Local Settings\User Rights Assignments**:

- Deny access to this computer from the network
- Deny log on as a batch job
- Deny log on as a service
- Deny log on through Remote Desktop Services

When you add Administrator accounts to these user rights, specify whether you are adding the local Administrator account or the domain's Administrator account by the way that you label the account. For example, to add the NWTRADERS domain's Administrator account to these deny rights, you would type the account as **NWTRADERS\Administrator**, or browse to the Administrator account for the NWTRADERS domain. To ensure that you restrict the local Administrator account, type **Administrator** in these user rights settings in the Group Policy Object Editor.

> **Note**
>
> Even if local Administrator accounts are renamed, the policies will still apply.

These settings will ensure that a computer's Administrator account cannot be used to connect to the other computers, even if it is inadvertently or maliciously enabled. Local logons using the local Administrator account cannot be completely disabled, nor should you attempt to do so, because a computer's local Administrator account is designed to be used in disaster recovery scenarios.

Should a member server or workstation become disjoined from the domain with no other local accounts granted administrative privileges, the computer can be booted into safe mode, the Administrator account can be enabled, and the account can then be used to effect repairs on the computer. When repairs are completed, the Administrator account should again be disabled.

Securing Local Privileged Accounts and Groups in Active Directory

Law Number Six: A computer is only as secure as the administrator is trustworthy. – Ten Immutable Laws of Security (Version 2.0)

The information provided here is intended to give general guidelines for securing the highest privilege built-in accounts and groups in Active Directory. Detailed step-by-step instructions are also provided in Appendix D: Securing Built-in Administrator Accounts in Active Directory, Appendix E: Securing Enterprise Admins Groups in Active Directory, Appendix F: Securing Domain Admins Groups in Active Directory and in Appendix G: Securing Administrators Groups in Active Directory.

Before you implement any of these settings, however, review the Role-Based Access Controls (RBAC) for Active Directory and Privileged Identity Management sections of this document. You should also test all settings thoroughly to determine if they are appropriate for your environment. Not all organizations will be able to implement these settings.

Securing Built-in Administrator Accounts in Active Directory

In each domain in Active Directory, an Administrator account is created as part of the creation of the domain. This account is by default a member of the Domain Admins and Administrator groups in the domain, and if the domain is the forest root domain, the account is also a member of the Enterprise Admins group. Use of a domain's local Administrator account should be reserved only for initial build activities and, possibly, disaster-recovery scenarios. To ensure that a built-in Administrator account can be used to effect repairs in the event that no other accounts can be used, you should not change the default membership of the Administrator account in any domain in the forest. Instead, you should following guidelines to help secure the Administrator account in each domain in the forest. Detailed instructions for implementing these controls are provided in Appendix D: Securing Built-in Administrator Accounts in Active Directory.

Controls for Built-in Administrator Accounts

The goal of implementing the settings described here is to prevent each domain's Administrator *account* (not a group) from being usable unless a number of controls are reversed. By implementing these controls and monitoring the Administrator accounts for changes, you can significantly reduce the likelihood of a successful attack by leveraging a domain's Administrator account. For the Administrator account in each domain in your forest, you should configure the following settings.

Enable the "Account is sensitive and cannot be delegated" flag on the account

By default, all accounts in Active Directory can be *delegated*. Delegation allows a computer or service to present the credentials for an account that has authenticated to the computer or service to other computers to obtain services on behalf of the account. When you enable the **Account is sensitive and cannot be delegated** attribute on a domain-based account, the account's credentials cannot be presented to other computers or services on the network, which limits attacks that leverage delegation to use the account's credentials on other systems.

Enable the "Smart card is required for interactive logon" flag on the account

When you enable the **Smart card is required for interactive logon** attribute on an account, Windows resets the account's password to a 120-character random

value. By setting this flag on built-in Administrator accounts, you ensure that the password for the account is not only long and complex, but is not known to any user. It is not technically necessary to create smart cards for the accounts before enabling this attribute, but if possible, smart cards should be created for each Administrator account prior to configuring the account restrictions and the smart cards should be stored in secure locations.

Although setting the **Smart card is required for interactive logon** flag resets the account's password, it does not prevent a user with rights to reset the account's password from setting the account to a known value and using the account's name and new password to access resources on the network. Because of this, you should implement the following additional controls on the account.

Disable the Account

If the Administrator account is not already disabled, disable it when you have completed configuration of the account's properties. This prevents the account from being used for any purpose unless it is first enabled. In a disaster recovery scenario in which no accounts are available to perform repairs of the AD DS environment, you can boot a domain controller into Directory Services Restore Mode (DSRM), log on by using the DSRM Administrator account, and enable the domain's Administrator account if necessary.

Configuring GPOs to Restrict Domains' Administrator Accounts on Domain-Joined Systems

Although disabling the Administrator account in a domain makes the account effectively unusable, you should implement additional restrictions on the account in case the account is inadvertently or maliciously enabled. Although these controls can ultimately be reversed by the Administrator account, the goal is to create controls that slow an attacker's progress and limit the damage the account can inflict.

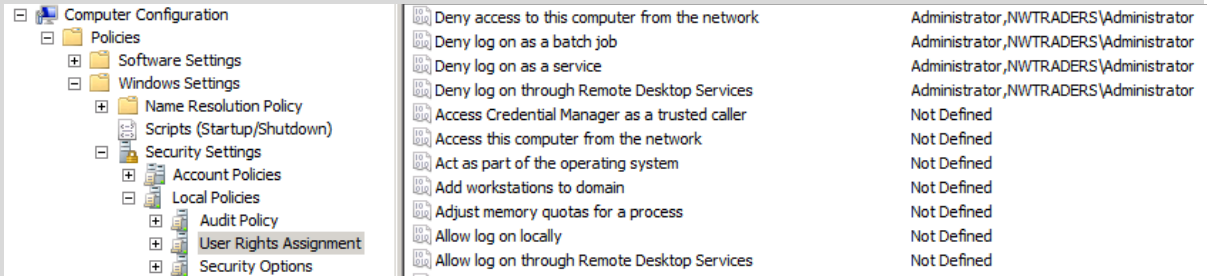
In one or more GPOs that you create and link to workstation and member server OUs in each domain, add each domain's Administrator account to the following user rights in **Computer Configuration\Policies\Windows Settings\Security Settings\Local Settings\User Rights Assignments**:

- Deny access to this computer from the network
- Deny log on as a batch job
- Deny log on as a service
- Deny log on through Remote Desktop Services

Note

When you add local Administrator accounts to this setting, you must specify whether you are configuring local Administrator accounts or domain Administrator accounts. For example, to add the NWTRADERS domain's local Administrator account to these deny rights, you must either type the account as **NWTRADERS\Administrator,** or browse to the local Administrator account for the NWTRADERS domain. If you type **Administrator** in these user rights settings in the Group Policy Object Editor, you will restrict the local Administrator account on each computer to which the GPO is applied.

We recommend restricting local Administrator accounts on member servers and workstations in the same manner as domain-based Administrator accounts. Therefore, you should generally add the Administrator account for each domain in the forest and the Administrator account for the local computers to these user rights settings. The following screenshot shows an example of configuring these user rights to block local Administrator accounts and a domain's Administrator account from performing logons that should not be needed for these accounts.



Configuring GPOs to Restrict Administrator Accounts on Domain Controllers

In each domain in the forest, the Default Domain Controllers policy or a policy linked to the Domain Controllers OU should be modified to add each domain's Administrator account to the following user rights in **Computer Configuration\Policies\Windows Settings\Security Settings\Local Settings\User Rights Assignments**:

- Deny access to this computer from the network
- Deny log on as a batch job
- Deny log on as a service
- Deny log on through Remote Desktop Services

Note

These settings will ensure that the local Administrator account cannot be used to connect to a domain controller, although the account, if enabled, can log on locally to domain controllers. Because this account should only be enabled and used in disaster-recovery scenarios, it is anticipated that physical access to at

> least one domain controller will be available, or that other accounts with permissions to access domain controllers remotely can be used.

Configure Auditing of Built-in Administrator Accounts

When you have secured each domain's Administrator account and disabled it, you should configure auditing to monitor for changes to the account. If the account is enabled, its password is reset, or any other modifications are made to the account, alerts should be sent to the users or teams responsible for administration of AD DS, in addition to incident response teams in your organization.

Securing Administrators, Domain Admins and Enterprise Admins Groups

Securing Enterprise Admin Groups

The Enterprise Admins group, which is housed in the forest root domain, should contain no users on a day-to-day basis, with the possible exception of the domain's local Administrator account, provided it is secured as described earlier and in Appendix D: Securing Built-In Administrator Accounts in Active Directory.

When EA access is required, the users whose accounts require EA rights and permissions should be temporarily placed into the Enterprise Admins group. Although users are using the highly privileged accounts, their activities should be audited and preferably performed with one user performing the changes and another user observing the changes to minimize the likelihood of inadvertent misuse or misconfiguration. When the activities have been completed, the accounts should be removed from the EA group. This can be achieved via manual procedures and documented processes, third-party privileged identity/access management (PIM/PAM) software, or a combination of both. Guidelines for creating accounts that can be used to control the membership of privileged groups in Active Directory are provided in Privilege Elevation and Propagation and detailed instructions are provided in Appendix I: Creating Management Accounts for Protected Accounts and Groups in Active Directory.

Enterprise Admins are, by default, members of the built-in Administrators group in each domain in the forest. Removing the Enterprise Admins group from the Administrators groups in each domain is an inappropriate modification because in the event of a forest disaster-recovery scenario, EA rights will likely be required. If the Enterprise Admins group has been removed from Administrators groups in a forest, it should be added to the Administrators group in each domain and the following additional controls should be implemented:

- As described earlier, the Enterprise Admins group should contain no users on a day-to-day basis, with the possible exception of the forest root domain's Administrator account, which should be secured as described in Appendix D: Securing Built-In Administrator Accounts in Active Directory.
- In GPOs linked to OUs containing member servers and workstations in each domain, the EA group should be added to the following user rights:
    - Deny access to this computer from the network
    - Deny log on as a batch job
    - Deny log on as a service

- Deny log on locally
- Deny log on through Remote Desktop Services.

This will prevent members of the EA group from logging on to member servers and workstations. If jump servers are used to administer domain controllers and Active Directory, ensure that jump servers are located in an OU to which the restrictive GPOs are not linked. For more information about the use of jump servers, see the Implementing Secure Administrative Workstations and Jump Servers section.

- Auditing should be configured to send alerts if any modifications are made to the properties or membership of the EA group. These alerts should be sent, at a minimum, to users or teams responsible for Active Directory administration and incident response. You should also define processes and procedures for temporarily populating the EA group, including notification procedures when legitimate population of the group is performed.

Securing Domain Admins Groups

As is the case with the Enterprise Admins group, membership in Domain Admins groups should be required only in build or disaster-recovery scenarios. There should be no day-to-day user accounts in the DA group with the exception of the local Administrator account for the domain, if it has been secured as described in Appendix D: Securing Built-In Administrator Accounts in Active Directory.

When DA access is required, the accounts needing this level of access should be temporarily placed in the DA group for the domain in question. Although the users are using the highly privileged accounts, activities should be audited and preferably performed with one user performing the changes and another user observing the changes to minimize the likelihood of inadvertent misuse or misconfiguration. When the activities have been completed, the accounts should be removed from the Domain Admins group. This can be achieved via manual procedures and documented processes, via third-party privileged identity/access management (PIM/PAM) software, or a combination of both. Guidelines for creating accounts that can be used to control the membership of privileged groups in Active Directory are provided in Appendix I: Creating Management Accounts for Protected Accounts and Groups in Active Directory.

Domain Admins are, by default, members of the local Administrators groups on all member servers and workstations in their respective domains. This default nesting should not be modified because it affects supportability and disaster recovery options. If Domain Admins groups have been removed from the local Administrators groups on the member servers, they should be added to the Administrators group on each member server and workstation in the domain via restricted group settings in linked GPOs. The following general controls, which are described in depth in Appendix F: Securing Domain Admins Groups in Active Directory should also be implemented.

For the Domain Admins group in each domain in the forest:

1. Remove all members from the DA group, with the possible exception of the built-in Administrator account for the domain, provided it has been secured

as described in Appendix D: Securing Built-In Administrator Accounts in Active Directory.

2. In GPOs linked to OUs containing member servers and workstations in each domain, the DA group should be added to the following user rights:
    - Deny access to this computer from the network
    - Deny log on as a batch job
    - Deny log on as a service
    - Deny log on locally
    - Deny log on through Remote Desktop Services

    This will prevent members of the DA group from logging on to member servers and workstations. If jump servers are used to administer domain controllers and Active Directory, ensure that jump servers are located in an OU to which the restrictive GPOs are not linked.
3. Auditing should be configured to send alerts if any modifications are made to the properties or membership of the DA group. These alerts should be sent, at a minimum, to users or teams responsible for AD DS administration and incident response. You should also define processes and procedures for temporarily populating the DA group, including notification procedures when legitimate population of the group is performed.

Securing Administrators Groups in Active Directory

As is the case with the EA and DA groups, membership in the Administrators (BA) group should be required only in build or disaster-recovery scenarios. There should be no day-to-day user accounts in the Administrators group with the exception of the local Administrator account for the domain, if it has been secured as described in Appendix D: Securing Built-In Administrator Accounts in Active Directory.

When Administrators access is required, the accounts needing this level of access should be temporarily placed in the Administrators group for the domain in question. Although the users are using the highly privileged accounts, activities should be audited and, preferably, performed with a user performing the changes and another user observing the changes to minimize the likelihood of inadvertent misuse or misconfiguration. When the activities have been completed, the accounts should immediately be removed from the Administrators group. This can be achieved via manual procedures and documented processes, via third-party privileged identity/access management (PIM/PAM) software, or a combination of both.

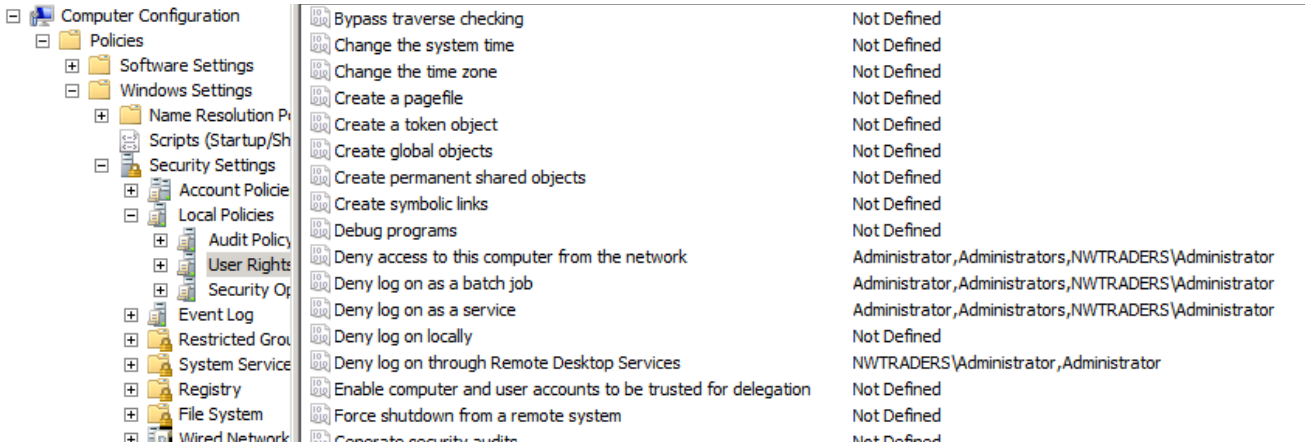
Administrators are, by default, the owners of most of the AD DS objects in their respective domains. Membership in this group may be required in build and disaster recovery scenarios in which ownership or the ability to take ownership of objects is required. Additionally, DAs and EAs inherit a number of their rights and permissions by virtue of their default membership in the Administrators group. Default group nesting for privileged groups in Active Directory should not be modified, and each domain’s Administrators group should be secured as described in Appendix G: Securing Administrators Groups in Active Directory, and in the general instructions below.

1. Remove all members from the Administrators group, with the possible exception of the local Administrator account for the domain, provided it has been secured as described in Appendix D: Securing Built-In Administrator Accounts in Active Directory.
2. Members of the domain's Administrators group should never need to log on to member servers or workstations. In one or more GPOs linked to workstation and member server OUs in each domain, the Administrators group should be added to the following user rights:
    - Deny access to this computer from the network
    - Deny log on as a batch job,
    - Deny log on as a service

    This will prevent members of the Administrators group from being used to log on or connect to member servers or workstations (unless multiple controls are first breached), where their credentials could be cached and thereby compromised. A privileged account should never be used to log on to a less-privileged system, and enforcing these controls affords protection against a number of attacks.
3. At the domain controllers OU in each domain in the forest, the Administrators group should be granted the following user rights (if they do not already have these rights), which will allow the members of the Administrators group to perform functions necessary for a forest-wide disaster recovery scenario:
    - Access this computer from the network
    - Allow log on locally
    - Allow log on through Remote Desktop Services
4. Auditing should be configured to send alerts if any modifications are made to the properties or membership of the Administrators group. These alerts should be sent, at a minimum, to members of the team responsible for AD DS administration. Alerts should also be sent to members of the security team, and procedures should be defined for modifying the membership of the Administrators group. Specifically, these processes should include a procedure by which the security team is notified when the Administrators group is going to be modified so that when alerts are sent, they are expected and an alarm is not raised. Additionally, processes to notify the security team when the use of the Administrators group has been completed and the accounts used have been removed from the group should be implemented.

    > **Note**
    >
    > When you implement restrictions on the Administrators group in GPOs, Windows applies the settings to members of a computer's local Administrators group in addition to the domain's Administrators group. Therefore, you should use caution when implementing restrictions on the Administrators group. Although prohibiting network, batch and service logons for members of the Administrators group is advised wherever it is feasible to implement, do not restrict local logons or logons through Remote

> Desktop Services. Blocking these logon types can block legitimate administration of a computer by members of the local Administrators group. The following screenshot shows configuration settings that block misuse of built-in local and domain Administrator accounts, in addition to misuse of built-in local or domain Administrators groups. Note that the **Deny log on through Remote Desktop Services** user right does not include the Administrators group, because including it in this setting would also block these logons for accounts that are members of the local computer's Administrators group. If services on computers are configured to run in the context of any of the privileged groups described in this section, implementing these settings can cause services and applications to fail. Therefore, as with all of the recommendations in this section, you should thoroughly test settings for applicability in your environment.



Role-Based Access Controls (RBAC) for Active Directory

Generally speaking, role-based access controls (RBAC) are a mechanism for grouping users and providing access to resources based on business rules. In the case of Active Directory, implementing RBAC for AD DS is the process of creating roles to which rights and permissions are delegated to allow members of the role to perform day-to-day administrative tasks without granting them excessive privilege. RBAC for Active Directory can be designed and implemented via native tooling and interfaces, by leveraging software you may already own, by purchasing third-party products, or any combination of these approaches. This section does not provide step-by-step instructions to implement RBAC for Active Directory, but instead discusses factors you should consider in choosing an approach to implementing RBAC in your AD DS installations.

Native Approaches to RBAC for Active Directory

In the simplest RBAC implementation, you can implement roles as AD DS groups and delegate rights and permissions to the groups that allow them to perform daily administration within the designated scope of the role.

In some cases, existing security groups in Active Directory can be used to grant rights and permissions appropriate to a job function. For example, if specific

employees in your IT organization are responsible for the management and maintenance of DNS zones and records, delegating those responsibilities can be as simple as creating an account for each DNS administrator and adding it to the DNS Admins group in Active Directory. The DNS Admins group, unlike more highly privileged groups, has few powerful rights across Active Directory, although members of this group have been delegated permissions that allow them to administer DNS.

In other cases, you may need to create security groups and delegate rights and permissions to Active Directory objects, file system objects, and registry objects to allow members of the groups to perform designated administrative tasks. For example, if your Help Desk operators are responsible for resetting forgotten passwords, assisting users with connectivity problems, and troubleshooting application settings, you may need to combine delegation settings on user objects in Active Directory with privileges that allow Help Desk users to connect remotely to users' computers to view or modify the users' configuration settings. For each role you define, you should identify:

1. Which tasks members of the role perform on a day-to-day basis and which tasks are less frequently performed.
2. On which systems and in which applications members of a role should be granted rights and permissions.
3. Which users should be granted membership in a role.
4. How management of role memberships will be performed.

In many environments, manually creating role-based access controls for administration of an Active Directory environment can be challenging to implement and maintain. If you have clearly defined roles and responsibilities for administration of your IT infrastructure, you may want to leverage additional tooling to assist you in creating a manageable native RBAC deployment. For example, if Forefront Identity Manager (FIM) is in use in your environment, you can use FIM to automate the creation and population of administrative roles, which can ease ongoing administration. If you use System Center Configuration Manager (SCCM) and System Center Operations Manager (SCOM), you can use application-specific roles to delegate management and monitoring functions, and also enforce consistent configuration and auditing across systems in the domain. If you have implemented a public key infrastructure (PKI), you can issue and require smart cards for IT staff responsible for administering the environment. With FIM Credential Management (FIM CM), you can even combine management of roles and credentials for your administrative staff.

In other cases, it may be preferable for an organization to consider deploying third-party RBAC software that provides "out-of-box" functionality. Commercial, off-the-shelf (COTS) solutions for RBAC for Active Directory, Windows, and non-Windows directories and operating systems are offered by a number of vendors. A list of third-party RBAC solutions is provided in Appendix J: Third-Party RBAC Vendors. When choosing between native solutions and third-party products, you should consider the following factors:

1. Budget: By investing in development of RBAC using software and tools you may already own, you can reduce the software costs involved in deploying a

solution. However, unless you have staff who are experienced in creating and deploying native RBAC solutions, you may need to engage consulting resources to develop your solution. You should carefully weigh the anticipated costs for a custom-developed solution with the costs to deploy an “out-of-box” solution, particularly if your budget is limited.

2. Composition of the IT environment: If your environment is comprised primarily of Windows systems, or if you are already leveraging Active Directory for management of non-Windows systems and accounts, custom native solutions may provide the optimal solution for your needs. If your infrastructure contains many systems that are not running Windows and are not managed by Active Directory, you may need to consider options for management of non-Windows systems separately from the Active Directory environment.
3. Privilege model in the solution: If a product relies on placement of its service accounts into highly privileged groups in Active Directory and does not offer options that do not require excessive privilege be granted to the RBAC software, you have not really reduced your Active Directory attack surface—you’ve only changed the composition of the most privileged groups in the directory. Unless an application vendor can provide controls for service accounts that minimize the probability of the accounts being compromised and maliciously used, you may want to consider other options.

Privileged Identity Management

Privileged identity management (PIM), sometimes referred to as privileged account management (PAM) or privileged credential management (PCM) is the design, construction, and implementation of approaches to managing privileged accounts in your infrastructure. Generally speaking, PIM provides mechanisms by which accounts are granted temporary rights and permissions required to perform build-or-break fix functions, rather than leaving privileges permanently attached to accounts. Whether PIM functionality is manually created or is implemented via the deployment of third-party software (see Appendix K: Third-Party PIM Vendors), one or more of the following features may be available:

- Credential “vaults,” where passwords for privileged accounts are “checked out” and assigned an initial password, then “checked in” when activities have been completed, at which time passwords are again reset on the accounts.
- Time-bound restrictions on the use of privileged credentials
- One-time-use credentials
- Workflow-generated granting of privilege with monitoring and reporting of activities performed and automatic removal of privilege when activities are completed or allotted time has expired
- Replacement of hard-coded credentials such as user names and passwords in scripts with application programming interfaces (APIs) that allow credentials to be retrieved from vaults as needed
- Automatic management of service account credentials

Creating Unprivileged Accounts to Manage Privileged Accounts

One of the challenges in managing privileged accounts is that, by default, the accounts that can manage privileged and protected accounts and groups are privileged and protected accounts. If you implement appropriate RBAC and PIM solutions for your Active Directory installation, the solutions may include approaches that allow you to effectively depopulate the membership of the most privileged groups in the directory, populating the groups only temporarily and when needed.

If you implement native RBAC and PIM, however, you should consider creating accounts that have no privilege and with the only function of populating and depopulating privileged groups in Active Directory when needed. Appendix I: Creating Management Accounts for Protected Accounts and Groups in Active Directory provides step-by-step instructions that you can use to create accounts for this purpose.

Implementing Robust Authentication Controls

Law Number Six: There really is someone out there trying to guess your passwords. – 10 Immutable Laws of Security Administration

Pass-the-hash and other credential theft attacks are not specific to Windows operating systems, nor are they new. The first pass-the-hash attack was created in 1997. Historically, however, these attacks required customized tools, were hit-or-miss in their success, and required attackers to have a relatively high degree of skill. The introduction of freely available, easy-to-use tooling that natively extracts credentials has resulted in an exponential increase in the number and success of credential theft attacks in recent years. However, credential theft attacks are by no means the only mechanisms by which credentials are targeted and compromised.

Although you should implement controls to help protect you against credential theft attacks, you should also identify the accounts in your environment that are most likely to be targeted by attackers, and implement robust authentication controls for those accounts. If your most privileged accounts are using single factor authentication such as user names and passwords (both are “something you know,” which is one authentication factor), those accounts are weakly protected. All that an attacker needs is knowledge of the user name and knowledge of the password associated with the account, and pass-the-hash attacks are not required—the attacker can authenticate as the user to any systems that accept single factor credentials.

Although implementing multifactor authentication does not protect you against pass-the-hash attacks, implementing multifactor authentication in combination with protected systems can. More information about implementing protected systems is provided in Implementing Secure Administrative Hosts later in this document, and authentication options are discussed in the following sections.

General Authentication Controls

If you have not already implemented multifactor authentication such as smart cards, consider doing so. Smart cards implement hardware-enforced protection of private keys in a public-private key pair, preventing a user's private key from being accessed or used unless the user presents the proper PIN, passcode, or biometric identifier to the smart card. Even if a user's PIN or passcode is intercepted by a keystroke logger on a compromised computer, for an attacker to reuse the PIN or passcode, the card must also be physically present.

In cases in which long, complex passwords have proven difficult to implement because of user resistance, smart cards provide a mechanism by which users may implement relatively simple PINs or passcodes without the credentials being susceptible to brute force or rainbow table attacks. Smart card PINs are not stored in Active Directory or in local SAM databases, although credential hashes may still be stored in LSASS protected memory on computers on which smart cards have been used for authentication.

Additional Controls for VIP Accounts

Another benefit of implementing smart cards or other certificate-based authentication mechanisms is the ability to leverage Authentication Mechanism Assurance to protect sensitive data that is accessible to VIP users. Authentication Mechanism Assurance is available in domains in which the functional level is set to Windows Server 2012 or Windows Server 2008 R2. When it is enabled, Authentication Mechanism Assurance adds an administrator-designated global group membership to a user's Kerberos token when the user's credentials are authenticated during logon using a certificate-based logon method.

This makes it possible for resource administrators to control access to resources, such as files, folders, and printers, based on whether the user logs on using a certificate-based logon method, in addition to the type of certificate used. For example, when a user logs on by using a smart card, the user's access to resources on the network can be specified as different from what the access is when the user does not use a smart card (that is, when the user logs on by entering a user name and password). For more information about Authentication Mechanism Assurance, see the Authentication Mechanism Assurance for AD DS in Windows Server 2008 R2 Step-by-Step Guide.

Configuring Privileged Account Authentication

In Active Directory for all administrative accounts, enable the **Require smart card for interactive logon** attribute, and audit for changes to (at a minimum), any of the attributes on the **Account** tab for the account (for example, cn, name, sAMAccountName, userPrincipalName, and userAccountControl) administrative user objects.

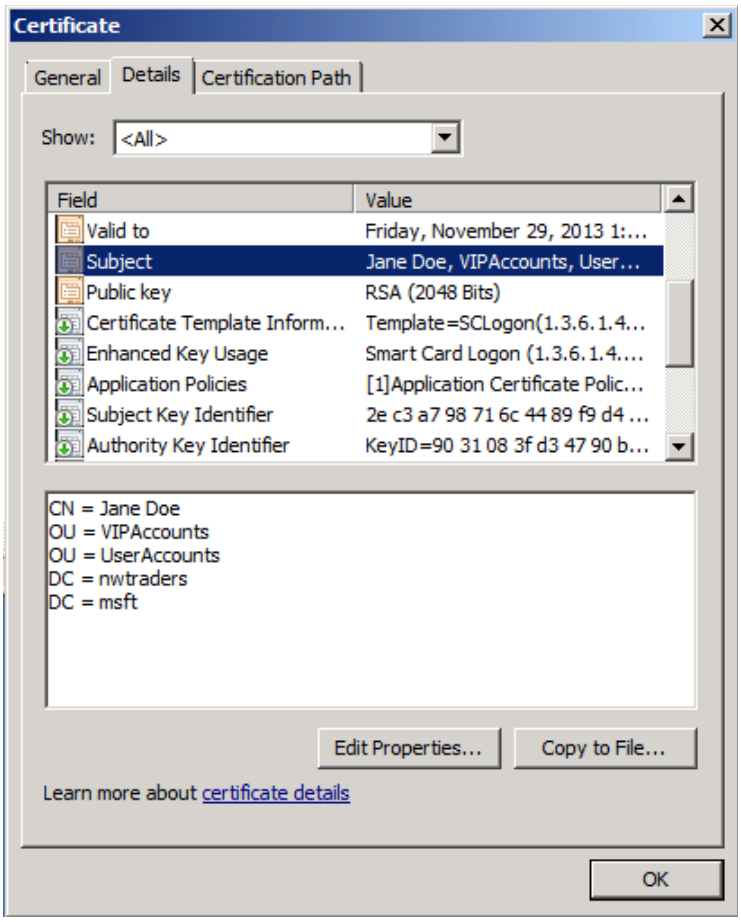
Although setting the **Require smart card for interactive logon** on accounts resets the account's password to a 120-character random value and requires smart cards for interactive logons, the attribute can still be overwritten by users with permissions that allow them to change passwords on the accounts, and the accounts can then be used to establish noninteractive logons with only user name and password.

In other cases, depending on the configuration of accounts in Active Directory and certificate settings in Active Directory Certificate Services (AD CS) or a third-party PKI, User Principal Name (UPN) attributes for administrative or VIP accounts can be targeted for a specific kind of attack, as described here.

UPN Hijacking for Certificate Spoofing

Although a thorough discussion of attacks against public key infrastructures (PKIs) is outside the scope of this document, attacks against public and private PKIs have increased exponentially since 2008. Breaches of public PKIs have been broadly publicized, but attacks against an organization's internal PKI are perhaps even more prolific. One such attack leverages Active Directory and certificates to allow an attacker to spoof the credentials of other accounts in a manner that can be difficult to detect.

When a certificate is presented for authentication to a domain-joined system, the contents of the Subject or the Subject Alternative Name (SAN) attribute in the certificate are used to map the certificate to a user object in Active Directory. Depending on the type of certificate and how it is constructed, the Subject attribute in a certificate typically contains a user's common name (CN), as shown in the following screenshot.



By default, Active Directory constructs a user's CN by concatenating the account's first name + " "+ last name. However, CN components of user objects in Active Directory are not required or guaranteed to be unique, and moving a user account to a different location in the directory changes the account's distinguished name (DN), which is the full path to the object in the directory, as shown in the bottom pane of the previous screenshot.

Because certificate subject names are not guaranteed to be static or unique, the contents of the Subject Alternative Name are often used to locate the user object in Active Directory. The SAN attribute for certificates issued to users from enterprise certification authorities (Active Directory integrated CAs) typically contains the user's UPN or email address. Because UPNs are guaranteed to be unique in an AD DS forest, locating a user object by UPN is commonly performed as part of authentication, with or without certificates involved in the authentication process.

The use of UPNs in SAN attributes in authentication certificates can be leveraged by attackers to obtain fraudulent certificates. If an attacker has compromised an account that has the ability to read and write UPNs on user objects, the attack is implemented as follows:

The UPN attribute on a user object (such as a VIP user) is temporarily changed to a different value. The SAM account name attribute and CN can also be changed at this time, although this is usually not necessary for the reasons described earlier.

When the UPN attribute on the target account has been changed, a stale, enabled user account or a freshly created user account's UPN attribute is changed to the value that was originally assigned to the target account. Stale, enabled user accounts are accounts that have not logged on for long periods of time, but have not been disabled. They are targeted by attackers who intend to "hide in plain sight" for the following reasons:

1. Because the account is enabled, but hasn't been used recently, using the account is unlikely to trigger alerts the way that enabling a disabled user account might.
2. Use of an existing account doesn't require the creation of a new user account that might be noticed by administrative staff.
3. Stale user accounts that are still enabled are usually members of various security groups and are granted access to resources on the network, simplifying access and "blending in" to an existing user population.

The user account on which the target UPN has now been configured is used to request one or more certificates from Active Directory Certificate Services.

When certificates have been obtained for the attacker's account, the UPNs on the "new" account and the target account are returned to their original values.

The attacker now has one or more certificates that can be presented for authentication to resources and applications as if the user is the VIP user whose account was temporarily modified. Although a full discussion of all of the ways in which certificates and PKI can be targeted by attackers is outside the scope of this document, this attack mechanism is provided to illustrate why you should monitor privileged and VIP accounts in AD DS for changes, particularly for changes to any of the attributes on the **Account** tab for the account (for example, cn, name, sAMAccountName, userPrincipalName, and userAccountControl). In addition to monitoring the accounts, you should restrict who can modify the accounts to as small a set of administrative users as possible. Likewise, the accounts of administrative users should be protected and monitored for unauthorized changes.

Implementing Secure Administrative Hosts

Secure administrative hosts are workstations or servers that have been configured specifically for the purposes of creating secure platforms from which privileged accounts can perform administrative tasks in Active Directory or on domain controllers, domain-joined systems, and applications running on domain-joined systems. In this case, "privileged accounts" refers not only to accounts that are members of the most privileged groups in Active Directory, but to any accounts that have been delegated rights and permissions that allow administrative tasks to be performed.

These accounts may be Help Desk accounts that have the ability to reset passwords for most of the users in a domain, accounts that are used to administer DNS records and zones, or accounts that are used for configuration management. Secure administrative

hosts are dedicated to administrative functionality, and they do not run software such as email applications, web browsers, or productivity software such as Microsoft Office.

Although the “most privileged” accounts and groups should accordingly be the most stringently protected, this does not eliminate the need to protect any accounts and groups to which privileges above those of standard user accounts have been granted.

A secure administrative host can be a dedicated workstation that is used only for administrative tasks, a member server that runs the Remote Desktop Gateway server role and to which IT users connect to perform administration of destination hosts, or a server that runs the Hyper-V® role and provides a unique virtual machine for each IT user to use for their administrative tasks. In many environments, combinations of all three approaches may be implemented.

Implementing secure administrative hosts requires planning and configuration that is consistent with your organization’s size, administrative practices, risk appetite, and budget. Considerations and options for implementing secure administrative hosts are provided here for you to use in developing an administrative strategy suitable for your organization.

Principles for Creating Secure Administrative Hosts

To effectively secure systems against attacks, a few general principles should be kept in mind:

1. You should never administer a trusted system (that is, a secure server such as a domain controller) from a less-trusted host (that is, a workstation that is not secured to the same degree as the systems it manages).
2. You should not rely on a single authentication factor when performing privileged activities; that is, user name and password combinations should not be considered acceptable authentication because only a single factor (something you know) is represented. You should consider where credentials are generated and cached or stored in administrative scenarios.
3. Although most attacks in the current threat landscape leverage malware and malicious hacking, do not omit physical security when designing and implementing secure administrative hosts.

Account Configuration

Even if your organization does not currently use smart cards, you should consider implementing them for privileged accounts and secure administrative hosts. Administrative hosts should be configured to require smart card logon for all accounts by modifying the following setting in a GPO that is linked to the OUs containing administrative hosts:

Computer Configuration\Policies\Windows Settings\Local Policies\Security Options\Interactive logon: Require smart card

This setting will require all interactive logons to use a smart card, regardless of the configuration on an individual account in Active Directory.

You should also configure secure administrative hosts to permit logons only by authorized accounts, which can be configured in:

Computer Configuration\Policies\Windows Settings\Local Policies\Security Settings\Local Policies\User Rights Assignment

This grants interactive (and, where appropriate, Remote Desktop Services) logon rights only to authorized users of the secure administrative host.

Physical Security

For administrative hosts to be considered trustworthy, they must be configured and protected to the same degree as the systems they manage. Most of the recommendations provided in the Securing Domain Controllers Against Attack section of this document are also applicable to the hosts that are used to administer domain controllers and the AD DS database. One of the challenges of implementing secure administrative systems in most environments is that physical security can be more difficult to implement because these computers often reside in areas that are not as secure as servers hosted in datacenters, such as administrative users' desktops.

Physical security includes controlling physical access to administrative hosts. In a small organization, this may mean that you maintain a dedicated administrative workstation that is kept locked in an office or a desk drawer when not in use. Or it may mean that when you need to perform administration of Active Directory or your domain controllers, you log on to the domain controller directly.

In medium-sized organizations, you may consider implementing secure administrative "jump servers" that are located in a secured location in an office and are used when management of Active Directory or domain controllers is required. You may also implement administrative workstations that are locked in secure locations when not in use, with or without jump servers.

In large organizations, you can deploy datacenter-housed jump servers that provide strictly controlled access to Active Directory; domain controllers; and file, print, or application servers. Implementation of a jump server architecture is most likely to include a combination of secure workstations and servers in large environments.

Regardless of the size of your organization and the design of your administrative hosts, you should secure physical computers against unauthorized access or theft, and should use BitLocker® Drive Encryption to encrypt and protect the drives on administrative hosts. By implementing BitLocker on administrative hosts, even if a host is stolen or its disks are removed, you can ensure that the data on the drive is inaccessible to unauthorized users.

Operating System Versions and Configuration

All administrative hosts, whether servers or workstations, should run the newest operating system in use in your organization for the reasons described earlier in this document. By running current operating systems, your administrative staff benefits from new security features, full vendor support, and additional functionality introduced in the operating system. Moreover, when you are evaluating a new operating system, by deploying it first to administrative hosts, you will need to familiarize yourself with the new features, settings and management mechanisms it offers, which can subsequently be leveraged in planning broader deployment of the operating system. By then, the most sophisticated users in your organization will

also be the users who are familiar with the new operating system and best positioned to support it.

Microsoft Security Configuration Wizard

If you implement jump servers as part of your administrative host strategy, you should use the built-in Security Configuration Wizard to configure service, registry, audit, and firewall settings to reduce the server's attack surface. When the Security Configuration Wizard configuration settings have been collected and configured, the settings can be converted to a GPO that is used to enforce a consistent baseline configuration on all jump servers. You can further edit the GPO to implement security settings specific to jump servers, and can combine all of the settings with additional baseline settings extracted from the Microsoft Security Compliance Manager.

Microsoft Security Compliance Manager

The Microsoft Security Compliance Manager is a freely available tool that integrates security configurations that are recommended by Microsoft, based on operating system version and role configuration, and collects them in a single tool and UI that can be used to create and configure baseline security settings for domain controllers. Microsoft Security Compliance Manager templates can be combined with Security Configuration Wizard settings to produce comprehensive configuration baselines for jump servers that are deployed and enforced by GPOs deployed at the OUs in which jump servers are located in Active Directory.

> **Note**
>
> As of this writing, the Microsoft Security Compliance Manager does not include settings specific to jump servers or other secure administrative hosts, but Security Compliance Manager (SCM) can still be used to create initial baselines for your administrative hosts. To properly secure the hosts, however, you should apply additional security settings appropriate to highly secured workstations and servers.

AppLocker

Administrative hosts and virtual machinesshould be configured with script, tool, and application whitelists via AppLocker or a third-party application restriction software. Any administrative applications or utilities that do not adhere to secure settings should be upgraded or replaced with tooling that adheres to secure development and administrative practices. When new or additional tooling is needed on an administrative host, applications and utilities should be thoroughly tested, and if the tooling is suitable for deployment on administrative hosts, it can be added to the systems' whitelists.

RDP Restrictions

Although the specific configuration will vary depending on the architecture of your administrative systems, you should include restrictions on which accounts and computers can be used to establish Remote Desktop Protocol (RDP) connections to managed systems, such as using Remote Desktop Gateway (RD Gateway) jump

servers to control access to domain controllers and other managed systems from authorized users and systems. More information about using RD Gateway to help secure administrative hosts is provided in Sample Approaches to Implementing Secure Administrative Hosts later in this document.

You should allow interactive logons by authorized users and should remove or even block other logon types that are not needed for server access.

Patch and Configuration Management

Smaller organizations may rely on offerings such as Windows Update or Windows Server Update Services (WSUS) to manage deployment of updates to Windows systems, while larger organizations may implement enterprise patch and configuration management software such as System Center Configuration Manager. Regardless of the mechanisms you use to deploy updates to your general server and workstation population, you should consider separate deployments for highly secure systems such as domain controllers, certification authorities, and administrative hosts. By segregating these systems from the general management infrastructure, if your management software or service accounts are compromised, the compromise cannot be easily extended to the most secure systems in your infrastructure.

Although you should not implement manual update processes for secure systems, you should configure a separate infrastructure for updating secure systems. Even in very large organizations, this infrastructure can usually be implemented via dedicated WSUS servers and GPOs for secured systems.

Blocking Internet Access

Administrative hosts should not be permitted to access the Internet, nor should they be able to browse an organization’s intranet. Web browsers and similar applications should not be permitted on administrative hosts. You can block Internet access for secure hosts via a combination of perimeter firewall settings, WFAS configuration, and “black hole” proxy configuration on secure hosts. You can also use application whitelisting to prevent web browsers from being used on administrative hosts.

Virtualization

Where possible, consider implementing virtual machines as administrative hosts. Using virtualization, you can create per-user administrative systems that are centrally stored and managed, and which can be easily shut down when not in use, ensuring that credentials are not left active on the administrative systems. You can also require that virtual administrative hosts are reset to an initial snapshot after each use, ensuring that the virtual machines remain pristine. More information about options for virtualization of administrative hosts is provided in the following section.

Sample Approaches to Implementing Secure Administrative Hosts

Regardless of how you design and deploy your administrative host infrastructure, you should keep in mind the guidelines provided in Principles for Creating Secure Administrative Hosts. Each of the approaches described here provides general

information about how you can separate “administrative” and “productivity” systems used by your IT staff. Productivity systems are computers that IT administrators employ to check email, browse the Internet, and to use general productivity software such as Microsoft Office. Administrative systems are computers that are hardened and dedicated to use for day-to-day administration of an IT environment.

The simplest way to implement secure administrative hosts is to provide your IT staff with secured workstations from which they can perform administrative tasks. In a workstation-only implementation, each administrative workstation is used to launch management tools and RDP connections to manage servers and other infrastructure. Workstation-only implementations can be effective in smaller organizations, although larger, more complex infrastructures may benefit from a distributed design for administrative hosts in which dedicated administrative servers and workstations are used, as described in Implementing Secure Administrative Workstations and Jump Servers.

Implementing Separate Physical Workstations

One way that you can implement administrative hosts is to issue each IT user two workstations. One workstation is used with a “regular” user account to perform activities such as checking email and using productivity applications, while the second workstation is dedicated strictly to administrative functions.

For the productivity workstation, the IT staff can be given regular user accounts rather than using privileged accounts to log on to unsecured computers. The administrative workstation should be configured with a stringently controlled configuration and the IT staff should use a different account to log on to the administrative workstation.

If you have implemented smart cards, administrative workstations should be configured to require smart card logons, and IT staff should be given separate accounts for administrative use, also configured to require smart cards for interactive logon. The administrative host should be hardened as previously described, and only designated IT users should be allowed to log on locally to the administrative workstation.

Pros

By implementing separate physical systems, you can ensure that each computer is configured appropriately for its role and that IT users cannot inadvertently expose administrative systems to risk.

Cons

- Implementing separate physical computers increases hardware costs.
- Logging on to a physical computer with credentials that are used to administer remote systems caches the credentials in memory.

- If administrative workstations are not stored securely, they may be vulnerable to compromise via mechanisms such as physical hardware key loggers or other physical attacks.

Implementing a Secure Physical Workstation with a Virtualized Productivity Workstation

In this approach, IT users are given a secured administrative workstation from which they can perform day-to-day administrative functions, using Remote Server Administration Tools (RSAT) or RDP connections to servers within their scope of responsibility. When IT users need to perform productivity tasks, they can connect via RDP to a remote productivity workstation running as a virtual machine. Separate credentials should be used for each workstation, and controls such as smart cards should be implemented.

Pros

- Administrative workstations and productivity workstations are separated.
- IT staff using secure workstations to connect to productivity workstations can use separate credentials and smart cards, and privileged credentials are not deposited on the less-secure computer.

Cons

- Implementing the solution requires design and implementation work and robust virtualization options.
- If the physical workstations are not stored securely, they may be vulnerable to physical attacks that compromise the hardware or the operating system and make them susceptible to communications interception.

Implementing a Single Secure Workstation with Connections to Separate “Productivity” and “Administrative” Virtual Machines

In this approach, you can issue IT users a single physical workstation that is locked down as previously described, and on which IT users do not have privileged access. You can provide Remote Desktop Services connections to virtual machines hosted on dedicated servers, providing IT staff with one virtual machine that runs email and other productivity applications, and a second virtual machine that is configured as the user’s dedicated administrative host.

You should require smart card or other multifactor logon for the virtual machines, using separate accounts other than the account that is used to log on to the physical computer. After an IT user logs on to a physical computer, they can use their productivity smart card to connect to their remote productivity computer and a separate account and smart card to connect to their remote administrative computer.

Pros

- IT users can use a single physical workstation.
- By requiring separate accounts for the virtual hosts and using Remote Desktop Services connections to the virtual machines, IT users' credentials are not cached in memory on the local computer.
- The physical host can be secured to the same degree as administrative hosts, reducing the likelihood of compromise of the local computer.
- In cases in which an IT user's productivity virtual machine or their administrative virtual machine may have been compromised, the virtual machine can easily be reset to a "known good" state.
- If the physical computer is compromised, no privileged credentials will be cached in memory, and the use of smart cards can prevent compromise of credentials by keystroke loggers.

Cons

- Implementing the solution requires design and implementation work and robust virtualization options.
- If the physical workstations are not stored securely, they may be vulnerable to physical attacks that compromise the hardware or the operating system and make them susceptible to communications interception.

Implementing Secure Administrative Workstations and Jump Servers

As an alternative to secure administrative workstations, or in combination with them, you can implement secure jump servers, and administrative users can connect to the jump servers using RDP and smart cards to perform administrative tasks.

Jump servers should be configured to run the Remote Desktop Gateway role to allow you to implement restrictions on connections to the jump server and to destination servers that will be managed from it. If possible, you should also install the Hyper-V role and create Personal Virtual Desktops or other per-user virtual machines for administrative users to use for their tasks on the jump servers.

By giving the administrative users per-user virtual machines on the jump server, you provide physical security for the administrative workstations, and administrative users can reset or shut down their virtual machines when not in use. If you prefer not to install the Hyper-V role and the Remote Desktop Gateway role on the same administrative host, you can install them on separate computers.

Wherever possible, remote administration tools should be used to manage servers. The Remote Server Administration Tools (RSAT) feature should be installed on the users' virtual machines (or the jump server if you are not implementing per-user virtual machines for administration), and administrative staff should connect via RDP to their virtual machines to perform administrative tasks.

In cases when an administrative user must connect via RDP to a destination server to manage it directly, RD Gateway should be configured to allow the connection to be made only if the appropriate user and computer are used to establish the connection to the destination server. Execution of RSAT (or similar) tools should be prohibited on systems that are not designated management systems, such as general-use workstations and member servers that are not jump servers.

Pros

- Creating jump servers allows you to map specific servers to “zones” (collections of systems with similar configuration, connection, and security requirements) in your network and to require that the administration of each zone is achieved by administrative staff connecting from secure administrative hosts to a designated “zone” server.
- By mapping jump servers to zones, you can implement granular controls for connection properties and configuration requirements, and can easily identify attempts to connect from unauthorized systems.
- By implementing per-administrator virtual machines on jump servers, you enforce shutdown and resetting of the virtual machines to a known clean state when administrative tasks are completed. By enforcing shutdown (or restart) of the virtual machines when administrative tasks are completed, the virtual machines cannot be targeted by attackers, nor are credential theft attacks feasible because memory-cached credentials do not persist beyond a reboot.

Cons

- Dedicated servers are required for jump servers, whether physical or virtual.
- Implementing designated jump servers and administrative workstations requires careful planning and configuration that maps to any security zones configured in the environment.

Securing Domain Controllers Against Attack

Law Number Three: If a bad guy has unrestricted physical access to your computer, it’s not your computer anymore. – Ten Immutable Laws of Security (Version 2.0)

Domain controllers provide the physical storage for the AD DS database, in addition to providing the services and data that allow enterprises to effectively manage their servers, workstations, users, and applications. If privileged access to a domain controller is obtained by a malicious user, that user can modify, corrupt, or destroy the AD DS database and, by extension, all of the systems and accounts that are managed by Active Directory.

Because domain controllers can read from and write to anything in the AD DS database, compromise of a domain controller means that your Active Directory forest can never be considered trustworthy again unless you are able to recover

using a known good backup and to close the gaps that allowed the compromise in the process.

Depending on an attacker’s preparation, tooling, and skill, modification or even irreparable damage to the AD DS database can be completed in minutes to hours, not days or weeks. What matters isn’t how long an attacker has privileged access to Active Directory, but how much the attacker has planned for the moment when privileged access is obtained. Compromising a domain controller can provide the most expedient path to wide scale propagation of access, or the most direct path to destruction of member servers, workstations, and Active Directory. Because of this, domain controllers should be secured separately and more stringently than the general Windows infrastructure.

Physical Security for Domain Controllers

This section provides information about physically securing domain controllers, whether the domain controllers are physical or virtual machines, in datacenter locations, branch offices, and even remote locations with only basic infrastructure controls.

Datacenter Domain Controllers

Physical Domain Controllers

In datacenters, physical domain controllers should be installed in dedicated secure racks or cages that are separate from the general server population. When possible, domain controllers should be configured with Trusted Platform Module (TPM) chips and all volumes in the domain controller servers should be protected via BitLocker Drive Encryption. BitLocker generally adds performance overhead in single-digit percentages, but protects the directory against compromise even if disks are removed from the server. BitLocker can also help protect systems against attacks such as rootkits because the modification of boot files will cause the server to boot into recovery mode so that the original binaries can be loaded. If a domain controller is configured to use software RAID, serial-attached SCSI, SAN/NAS storage, or dynamic volumes, BitLocker cannot be implemented, so locally attached storage (with or without hardware RAID) should be used in domain controllers whenever possible.

Virtual Domain Controllers

If you implement virtual domain controllers, you should ensure that domain controllers run on separate physical hosts than other virtual machines in the environment. Even if you use a third-party virtualization platform, consider deploying virtual domain controllers on Hyper-V Server in Windows Server 2012 or Windows Server 2008 R2, which provides a minimal attack surface and can be managed with the domain controllers it hosts rather than being managed with the rest of the virtualization hosts. If you implement System Center Virtual Machine Manager (SCVMM) for management of your virtualization infrastructure, you can delegate administration for the physical hosts on which domain controller virtual machines reside and the domain controllers themselves to authorized administrators. You should also consider separating the storage of virtual domain

controllers to prevent storage administrators from accessing the virtual machine files.

Branch Locations

Physical Domain Controllers

In locations in which multiple servers reside but are not physically secured to the degree that datacenter servers are secured, physical domain controllers should be configured with TPM chips and BitLocker Drive Encryption for all server volumes. If a domain controller cannot be stored in a locked room in branch locations, you should consider deploying RODCs in those locations.

Virtual Domain Controllers

Whenever possible, you should run virtual domain controllers in branch offices on separate physical hosts than the other virtual machines in the site. In branch offices in which virtual domain controllers cannot run on separate physical hosts from the rest of the virtual server population, you should implement TPM chips and BitLocker Drive Encryption on hosts on which virtual domain controllers run at minimum, and all hosts if possible. Depending on the size of the branch office and the security of the physical hosts, you should consider deploying RODCs in branch locations.

Remote Locations with Limited Space and Security

If your infrastructure includes locations in which only a single physical server can be installed, a server capable of running virtualization workloads should be installed in the remote location, and BitLocker Drive Encryption should be configured to protect all volumes in the server. One virtual machine on the server should run an RODC, with other servers running as separate virtual machines on the host. Information about planning for deployment of RODC is provided in the Read-Only Domain Controller Planning and Deployment Guide. For more information about deploying and securing virtualized domain controllers, see Running Domain Controllers in Hyper-V on the TechNet website. For more detailed guidance for hardening Hyper-V, delegating virtual machine management, and protecting virtual machines, see the Hyper-V Security Guide Solution Accelerator on the Microsoft website.

Domain Controller Operating Systems

You should run all domain controllers on the newest version of Windows Server that is supported within your organization and prioritize decommissioning of legacy operating systems in the domain controller population. By keeping your domain controllers current and eliminating legacy domain controllers, you can often take advantage of new functionality and security that may not be available in domains or forests with domain controllers running legacy operating system. Domain controllers should be freshly installed and promoted rather than upgraded from previous operating systems or server roles; that is, do not perform in-place upgrades of domain controllers or run the AD DS Installation Wizard on servers on which the operating system is not freshly installed. By implementing freshly installed domain controllers, you ensure that legacy files and settings are not inadvertently left on domain controllers, and you simplify the enforcement of consistent, secure domain controller configuration.

Secure Configuration of Domain Controllers

A number of freely available tools, some of which are installed by default in Windows, can be used to create an initial security configuration baseline for domain controllers that can subsequently be enforced by GPOs. These tools are described here.

Security Configuration Wizard

All domain controllers should be locked down upon initial build. This can be achieved using the Security Configuration Wizard that ships natively in Windows Server to configure service, registry, system, and WFAS settings on a “base build” domain controller. Settings can be saved and exported to a GPO that can be linked to the Domain Controllers OU in each domain in the forest to enforce consistent configuration of domain controllers. If your domain contains multiple versions of Windows operating systems, you can configure Windows Management Instrumentation (WMI) filters to apply GPOs only to the domain controllers running the corresponding version of the operating system.

Microsoft Security Compliance Manager

Microsoft Security Compliance Manager domain controller settings can be combined with Security Configuration Wizard settings to produce comprehensive configuration baselines for domain controllers that are deployed and enforced by GPOs deployed at the Domain Controllers OU in Active Directory.

AppLocker

AppLocker or a third-party application whitelisting tool should be used to configure services and applications that are permitted to run on domain controllers, and these permitted applications and services should be comprised only of what is required for the computer to host AD DS and possibly DNS, plus any system security software such as antivirus software. By whitelisting permitted applications on domain controllers, an additional layer of security is added so that even if an unauthorized application is installed on a domain controller, the application cannot run.

RDP Restrictions

Group Policy Objects that link to all domain controllers OUs in a forest should be configured to allow RDP connections only from authorized users and systems—that is, jump servers. This can be achieved through a combination of user rights settings and WFAS configuration and should be implemented in GPOs so that the policy is consistently applied. If it is bypassed, the next Group Policy refresh returns the system to its proper configuration.

Patch and Configuration Management for Domain Controllers

Although it may seem counterintuitive, you should consider patching domain controllers and other critical infrastructure components separately from your general Windows infrastructure. If you leverage enterprise configuration management software for all computers in your infrastructure, compromise of the systems management software can be used to compromise or destroy all infrastructure components managed by that software. By separating patch and

systems management for domain controllers from the general population, you can reduce the amount of software installed on domain controllers, in addition to tightly controlling their management.

Blocking Internet Access for Domain Controllers

One of the checks that is performed as part of an Active Directory Security Assessment is the use and configuration of Internet Explorer on domain controllers. Internet Explorer (or any other web browser) should not be used on domain controllers, but analysis of thousands of domain controllers has revealed numerous cases in which privileged users used Internet Explorer to browse the organization's intranet or the Internet.

As previously described in the Misconfiguration section of Initial Breach Targets, browsing the Internet (or an infected intranet) from one of the most powerful computers in a Windows infrastructure using a highly privileged account (which are the only accounts permitted to log on locally to domain controllers by default) presents an extraordinary risk to an organization's security. Whether via a drive by download or by download of malware-infected "utilities," attackers can gain access to everything they need to completely compromise or destroy the Active Directory environment.

Although Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, and current versions of Internet Explorer offer a number of protections against malicious downloads, in most cases in which domain controllers and privileged accounts had been used to browse the Internet, the domain controllers were running Windows Server 2003, or protections offered by newer operating systems and browsers had been intentionally disabled.

Launching web browsers on domain controllers should be prohibited not only by policy, but by technical controls, and domain controllers should not be permitted to access the Internet. If your domain controllers need to replicate across sites, you should implement secure connections between the sites. Although detailed configuration instructions are outside the scope of this document, you can implement a number of controls to restrict the ability of domain controllers to be misused or misconfigured and subsequently compromised.

Perimeter Firewall Restrictions

Perimeter firewalls should be configured to block outbound connections from domain controllers to the Internet. Although domain controllers may need to communicate across site boundaries, perimeter firewalls can be configured to allow intersite communication by following the guidelines provided in How to configure a firewall for domains and trusts on the Microsoft Support website.

DC Firewall Configurations

As described earlier, you should use the Security Configuration Wizard to capture configuration settings for the Windows Firewall with Advanced Security on domain controllers. You should review the output of Security Configuration Wizard to ensure that the firewall configuration settings meet your organization's requirements, and then use GPOs to enforce configuration settings.

Preventing Web Browsing from Domain Controllers

You can use a combination of AppLocker configuration, “black hole” proxy configuration, and WFAS configuration to prevent domain controllers from accessing the Internet and to prevent the use of web browsers on domain controllers.

Monitoring Active Directory for Signs of Compromise

Law Number Five: Eternal vigilance is the price of security. – 10 Immutable Laws of Security

A solid event log monitoring system is a crucial part of any secure Active Directory design. Many computer security compromises could be discovered early in the event if the victims enacted appropriate event log monitoring and alerting. Independent reports have long supported this conclusion. For example, the 2009 Verizon Data Breach Report states:

> “The apparent ineffectiveness of event monitoring and log analysis continues to be somewhat of an enigma. The opportunity for detection is there; investigators noted that 66 percent of victims had sufficient evidence available within their logs to discover the breach had they been more diligent in analyzing such resources.”

This lack of monitoring active event logs remains a consistent weakness in many companies’ security defense plans. The 2012 Verizon Data Breach report found that even though 85 percent of breaches took several weeks to be noticed, 84 percent of victims had evidence of the breach in their event logs.

Windows Audit Policy

The following are links to the Microsoft official enterprise support blog. The content of these blogs provides advice, guidance, and recommendations about auditing that will assist you in enhancing the security of your Active Directory infrastructure and are a valuable resource when designing an audit policy.

- Global Object Access Auditing is Magic – describes a control mechanism called Advanced Audit Policy Configuration that was added to Windows® 7 and Windows Server 2008 R2 that lets you set what types of data you wanted to audit easily and not juggle scripts and auditpol.exe.
- Introducing Auditing Changes in Windows 2008 – introduces the auditing changes made in Windows Server 2008.
- Cool Auditing Tricks in Vista and 2008 – explains interesting auditing features of Windows Vista and Windows Server 2008 that can be used for troubleshooting problems or seeing what is happening in your environment.
- One-Stop Shop for Auditing in Windows Server 2008 and Windows Vista – contains a compilation of auditing features and information contained in Windows Server 2008 and Windows Vista.

The following links provide information about improvements to Windows auditing in Windows 8 and Windows Server 2012, and information about AD DS auditing in Windows Server 2008.

- What's New in Security Auditing – provides an overview of new security auditing features in Windows 8 and Windows Server 2012.
- AD DS Auditing Step-by-Step Guide – describes the new Active Directory Domain Services (AD DS) auditing feature in Windows Server 2008. It also provides procedures to implement this new feature.

Windows Audit Categories

Prior to Windows Vista and Windows Server 2008, Windows had only nine event log audit policy categories:

- Account Logon Events
- Account Management
- Directory Service Access
- Logon Events
- Object Access
- Policy Change
- Privilege Use
- Process Tracking
- System Events

These nine traditional audit categories comprise an audit policy. Each audit policy category can be enabled for Success, Failure, or Success and Failure events. Their descriptions are included in the next section.

Audit Policy Category Descriptions

The audit policy categories enable the following event log message types.

Audit Account Logon Events

Reports each instance of a security principal (for example, user, computer, or service account) that is logging on to or logging off from one computer in which another computer is used to validate the account. Account logon events are generated when a domain security principal account is authenticated on a domain controller. Authentication of a local user on a local computer generates a logon event that is logged in the local security log. No account logoff events are logged.

This category generates a lot of "noise" because Windows is constantly having accounts logging on to and off of the local and remote computers during the normal course of business. Still, any security plan should include the success and failure of this audit category.

Audit Account Management

This audit setting determines whether to track management of users and groups. For example, users and groups should be tracked when a user or computer account, a security group, or a distribution group is created, changed, or deleted; when a user or computer account is renamed, disabled, or enabled; or when a user or computer password is changed. An event can be generated for users or groups that are added to or removed from other groups.

Audit Directory Service Access

This policy setting determines whether to audit security principal access to an Active Directory object that has its own specified system access control list (SACL). In general, this category should only be enabled on domain controllers. When enabled, this setting generates a lot of “noise.”

Audit Logon Events

Logon events are generated when a local security principal is authenticated on a local computer. Logon Events records domain logons that occur on the local computer. Account logoff events are not generated. When enabled, Logon Events generates a lot of “noise,” but they should be enabled by default in any security auditing plan.

Audit Object Access

Object Access can generate events when subsequently defined objects with auditing enabled are accessed (for example, Opened, Read, Renamed, Deleted, or Closed). After the main auditing category is enabled, the administrator must individually define which objects will have auditing enabled. Many Windows system objects come with auditing enabled, so enabling this category will usually begin to generate events before the administrator has defined any.

This category is very “noisy” and will generate five to ten events for each object access. It can be difficult for administrators new to object auditing to gain useful information. It should only be enabled when needed.

Auditing Policy Change

This policy setting determines whether to audit every incidence of a change to user rights assignment policies, Windows Firewall policies, Trust policies, or changes to the audit policy. This category should be enabled on all computers. It generates very little noise.

Audit Privilege Use

There are dozens of user rights and permissions in Windows (for example, Logon as a Batch Job and Act as Part of the Operating System). This policy setting determines whether to audit each instance of a security principal by exercising a user right or privilege. Enabling this category results in a lot of “noise,” but it can be helpful in tracking security principal accounts using elevated privileges.

Audit Process Tracking

This policy setting determines whether to audit detailed process tracking information for events such as program activation, process exit, handle duplication,

and indirect object access. It is useful for tracking malicious users and the programs they use.

Enabling Audit Process Tracking generates a large number of events, so typically it is set to **No Auditing**. However, this setting can provide a great benefit during an incident response from the detailed log of the processes started and the time they were launched. For domain controllers and other single-role infrastructure servers, this category can be safely turned on all the time. Single role servers do not generate much process tracking traffic during the normal course of their duties. As such, they can be enabled to capture unauthorized events if they occur.

System Events Audit

System Events is almost a generic catch-all category, registering various events that impact the computer, its system security, or the security log. It includes events for computer shutdowns and restarts, power failures, system time changes, authentication package initializations, audit log clearings, impersonation issues, and a host of other general events. In general, enabling this audit category generates a lot of "noise," but it generates enough very useful events that it is difficult to ever recommend not enabling it.

Advanced Audit Policies

Starting with Windows Vista and Windows Server 2008, Microsoft improved the way event log category selections can be made by creating subcategories under each main audit category. Subcategories allow auditing to be far more granular than it could otherwise by using the main categories. By using subcategories, you can enable only portions of a particular main category, and skip generating events for which you have no use. Each audit policy subcategory can be enabled for Success, Failure, or Success and Failure events.

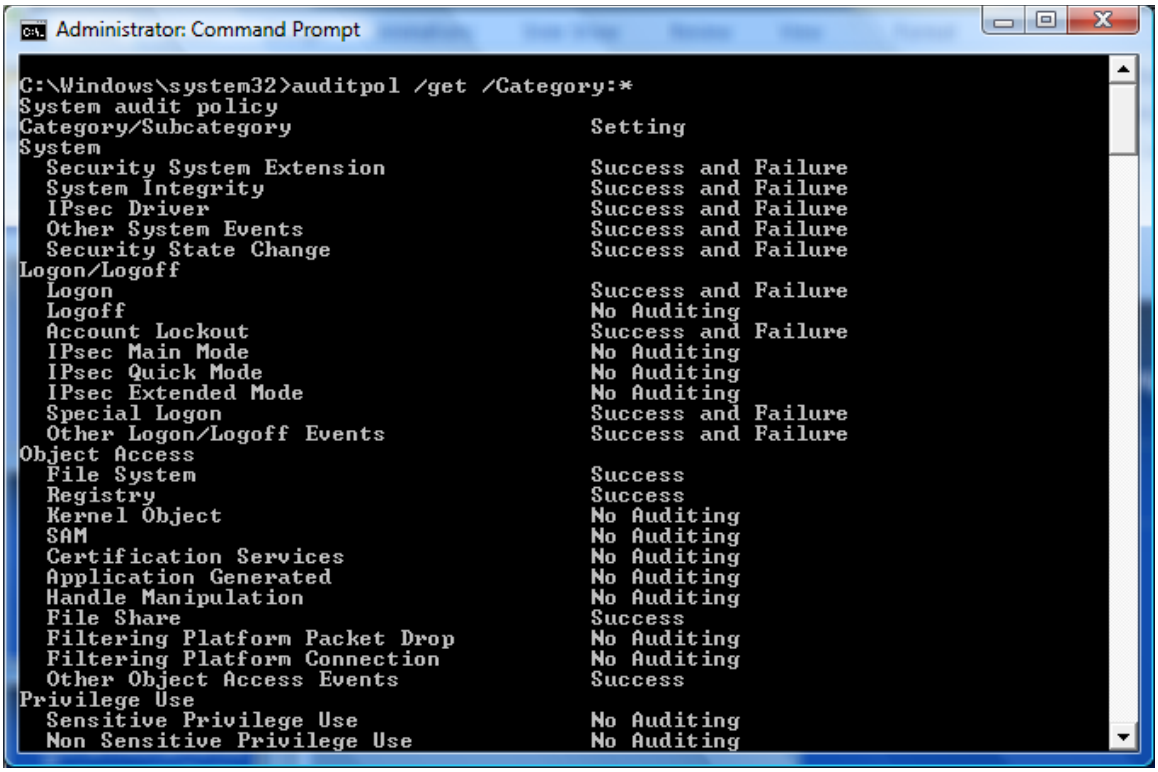
To list all the available auditing subcategories, review the Advanced Audit Policy container in a Group Policy Object, or type the following at a command prompt on any computer running Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008, Windows 8, Windows 7, or Windows Vista:

auditpol /list /subcategory:*

To get a list of currently configured auditing subcategories on a computer running Windows Server 2012, Windows Server 2008 R2, or Windows 2008, type the following:

auditpol /get /category:*

The following screenshot shows an example of auditpol.exe listing the current audit policy.



> **Note**
>
> Group Policy does not always accurately report the status of all enabled auditing policies, whereas auditpol.exe does. See [Getting the Effective Audit Policy in Windows 7 and 2008 R2] for more details.

Each main category has multiple subcategories. Below is a list of categories, their subcategories, and a description of their functions.

Auditing Subcategories Descriptions

Audit policy subcategories enable the following event log message types:

Account Logon

Credential Validation

This subcategory reports the results of validation tests on credentials submitted for a user account logon request. These events occur on the computer that is authoritative for the credentials. For domain accounts, the domain controller is authoritative, whereas for local accounts, the local computer is authoritative.

In domain environments, most of the account logon events are logged in the security log of the domain controllers that are authoritative for the domain accounts. However, these events can occur on other computers in the organization when local accounts are used to log on.

Kerberos Service Ticket Operations

This subcategory reports events generated by Kerberos ticket request processes on the domain controller that is authoritative for the domain account.

Kerberos Authentication Service

This subcategory reports events generated by the Kerberos authentication service. These events occur on the computer that is authoritative for the credentials.

Other Account Logon Events

This subcategory reports the events that occur in response to credentials submitted for a user account logon request that do not relate to credential validation or Kerberos tickets. These events occur on the computer that is authoritative for the credentials. For domain accounts, the domain controller is authoritative, whereas for local accounts, the local computer is authoritative.

In domain environments, most account logon events are logged in the security log of the domain controllers that are authoritative for the domain accounts. However, these events can occur on other computers in the organization when local accounts are used to log on. Examples can include the following:

- Remote Desktop Services session disconnections
- New Remote Desktop Services sessions
- Locking and unlocking a workstation
- Invoking a screen saver
- Dismissing a screen saver
- Detection of a Kerberos replay attack, in which a Kerberos request with identical information is received twice
- Access to a wireless network granted to a user or computer account
- Access to a wired 802.1x network granted to a user or computer account

Account Management

User Account Management

This subcategory reports each event of user account management, such as when a user account is created, changed, or deleted; a user account is renamed, disabled, or enabled; or a password is set or changed. If this audit policy setting is enabled, administrators can track events to detect malicious, accidental, and authorized creation of user accounts.

Computer Account Management

This subcategory reports each event of computer account management, such as when a computer account is created, changed, deleted, renamed, disabled, or enabled.

Security Group Management

This subcategory reports each event of security group management, such as when a security group is created, changed, or deleted or when a member is added to or removed from a security group. If this audit policy setting is enabled, administrators

can track events to detect malicious, accidental, and authorized creation of security group accounts.

Distribution Group Management

This subcategory reports each event of distribution group management, such as when a distribution group is created, changed, or deleted or when a member is added to or removed from a distribution group. If this audit policy setting is enabled, administrators can track events to detect malicious, accidental, and authorized creation of group accounts.

Application Group Management

This subcategory reports each event of application group management on a computer, such as when an application group is created, changed, or deleted or when a member is added to or removed from an application group. If this audit policy setting is enabled, administrators can track events to detect malicious, accidental, and authorized creation of application group accounts.

Other Account Management Events

This subcategory reports other account management events.

Detailed Process Tracking

Process Creation

This subcategory reports the creation of a process and the name of the user or program that created it.

Process Termination

This subcategory reports when a process terminates.

DPAPI Activity

This subcategory reports encrypt or decrypt calls into the data protection application programming interface (DPAPI). DPAPI is used to protect secret information such as stored password and key information.

RPC Events

This subcategory reports remote procedure call (RPC) connection events.

Directory Service Access

Directory Service Access

This subcategory reports when an AD DS object is accessed. Only objects with configured SACLs cause audit events to be generated, and only when they are accessed in a manner that matches the SACL entries. These events are similar to the directory service access events in earlier versions of Windows Server. This subcategory applies only to domain controllers.

Directory Service Changes

This subcategory reports changes to objects in AD DS. The types of changes that are reported are create, modify, move, and undelete operations that are performed on an object. Directory service change auditing, where appropriate, indicates the old and new values of the changed properties of the objects that were changed.

Only objects with SACLs cause audit events to be generated, and only when they are accessed in a manner that matches their SACL entries. Some objects and properties do not cause audit events to be generated due to settings on the object class in the schema. This subcategory applies only to domain controllers.

Directory Service Replication

This subcategory reports when replication between two domain controllers begins and ends.

Detailed Directory Service Replication

This subcategory reports detailed information about the information replicated between domain controllers. These events can be very high in volume.

Logon/Logoff

Logon

This subcategory reports when a user attempts to log on to the system. These events occur on the accessed computer. For interactive logons, the generation of these events occurs on the computer that is logged on to. If a network logon takes place to access a share, these events generate on the computer that hosts the accessed resource. If this setting is configured to **No auditing**, it is difficult or impossible to determine which user has accessed or attempted to access organization computers.

Network Policy Server

This subcategory reports events generated by RADIUS (IAS) and Network Access Protection (NAP) user access requests. These requests can be **Grant**, **Deny**, **Discard**, **Quarantine**, **Lock**, and **Unlock**. Auditing this setting will result in a medium or high volume of records on NPS and IAS servers.

IPsec Main Mode

This subcategory reports the results of Internet Key Exchange (IKE) protocol and Authenticated Internet Protocol (AuthIP) during Main Mode negotiations.

IPsec Extended Mode

This subcategory reports the results of AuthIP during Extended Mode negotiations.

Other Logon/Logoff Events

This subcategory reports other logon and logoff-related events, such as Remote Desktop Services session disconnects and reconnects, using RunAs to run processes under a different account, and locking and unlocking a workstation.

Logoff

This subcategory reports when a user logs off the system. These events occur on the accessed computer. For interactive logons, the generation of these events occurs on the computer that is logged on to. If a network logon takes place to access a share, these events generate on the computer that hosts the accessed resource. If this setting is configured to **No auditing**, it is difficult or impossible to determine which user has accessed or attempted to access organization computers.

Account Lockout

This subcategory reports when a user’s account is locked out as a result of too many failed logon attempts.

IPsec Quick Mode

This subcategory reports the results of IKE protocol and AuthIP during Quick Mode negotiations.

Special Logon

This subcategory reports when a special logon is used. A special logon is a logon that has administrator equivalent privileges and can be used to elevate a process to a higher level.

Policy Change

Audit Policy Change

This subcategory reports changes in audit policy including SACL changes.

Authentication Policy Change

This subcategory reports changes in authentication policy.

Authorization Policy Change

This subcategory reports changes in authorization policy including permissions (DACL) changes.

MPSSVC Rule-Level Policy Change

This subcategory reports changes in policy rules used by the Microsoft Protection Service (MPSSVC.exe). This service is used by Windows Firewall.

Filtering Platform Policy Change

This subcategory reports the addition and removal of objects from WFP, including startup filters. These events can be very high in volume.

Other Policy Change Events

This subcategory reports other types of security policy changes such as configuration of the Trusted Platform Module (TPM) or cryptographic providers.

Privilege Use

Sensitive Privilege Use

This subcategory reports when a user account or service uses a sensitive privilege. A sensitive privilege includes the following user rights: act as part of the operating system, back up files and directories, create a token object, debug programs, enable computer and user accounts to be trusted for delegation, generate security audits, impersonate a client after authentication, load and unload device drivers, manage auditing and security log, modify firmware environment values, replace a process-level token, restore files and directories, and take ownership of files or other objects. Auditing this subcategory will create a high volume of events.

Nonsensitive Privilege Use

This subcategory reports when a user account or service uses a nonsensitive privilege. A nonsensitive privilege includes the following user rights: access

Credential Manager as a trusted caller, access this computer from the network, add workstations to domain, adjust memory quotas for a process, allow log on locally, allow log on through Remote Desktop Services, bypass traverse checking, change the system time, create a pagefile, create global objects, create permanent shared objects, create symbolic links, deny access this computer from the network, deny log on as a batch job, deny log on as a service, deny log on locally, deny log on through Remote Desktop Services, force shutdown from a remote system, increase a process working set, increase scheduling priority, lock pages in memory, log on as a batch job, log on as a service, modify an object label, perform volume maintenance tasks, profile single process, profile system performance, remove computer from docking station, shut down the system, and synchronize directory service data. Auditing this subcategory will create a very high volume of events.

Other Privilege Use Events

This security policy setting is not currently used.

Object Access

File System

This subcategory reports when file system objects are accessed. Only file system objects with SACLs cause audit events to be generated, and only when they are accessed in a manner matching their SACL entries. By itself, this policy setting will not cause auditing of any events. It determines whether to audit the event of a user who accesses a file system object that has a specified system access control list (SACL), effectively enabling auditing to take place.

If the audit object access setting is configured to **Success**, an audit entry is generated each time that a user successfully accesses an object with a specified SACL. If this policy setting is configured to **Failure,** an audit entry is generated each time that a user fails in an attempt to access an object with a specified SACL.

Registry

This subcategory reports when registry objects are accessed. Only registry objects with SACLs cause audit events to be generated, and only when they are accessed in a manner matching their SACL entries. By itself, this policy setting will not cause auditing of any events.

Kernel Object

This subcategory reports when kernel objects such as processes and mutexes are accessed. Only kernel objects with SACLs cause audit events to be generated, and only when they are accessed in a manner matching their SACL entries. Typically kernel objects are only given SACLs if the AuditBaseObjects or AuditBaseDirectories auditing options are enabled.

SAM

This subcategory reports when local Security Accounts Manager (SAM) authentication database objects are accessed.

Certification Services

This subcategory reports when Certification Services operations are performed.

Application Generated

This subcategory reports when applications attempt to generate audit events by using the Windows auditing application programming interfaces (APIs).

Handle Manipulation

This subcategory reports when a handle to an object is opened or closed. Only objects with SACLs cause these events to be generated, and only if the attempted handle operation matches the SACL entries. Handle Manipulation events are only generated for object types where the corresponding object access subcategory is enabled (for example, file system or registry).

File Share

This subcategory reports when a file share is accessed. By itself, this policy setting will not cause auditing of any events. It determines whether to audit the event of a user who accesses a file share object that has a specified system access control list (SACL), effectively enabling auditing to take place.

Filtering Platform Packet Drop

This subcategory reports when packets are dropped by Windows Filtering Platform (WFP). These events can be very high in volume.

Filtering Platform Connection

This subcategory reports when connections are allowed or blocked by WFP. These events can be high in volume.

Other Object Access Events

This subcategory reports other object access-related events such as Task Scheduler jobs and COM+ objects.

System

Security State Change

This subcategory reports changes in security state of the system, such as when the security subsystem starts and stops.

Security System Extension

This subcategory reports the loading of extension code such as authentication packages by the security subsystem.

System Integrity

This subcategory reports on violations of integrity of the security subsystem.

IPsec Driver

This subcategory reports on the activities of the Internet Protocol security (IPsec) driver.

Other System Events

This subcategory reports on other system events.

For more information about the subcategory descriptions, refer to the Microsoft Security Compliance Manager tool.

Each organization should review the previous covered categories and subcategories and enable the ones which best fit their environment. Changes to audit policy should always be tested prior to deployment in a production environment.

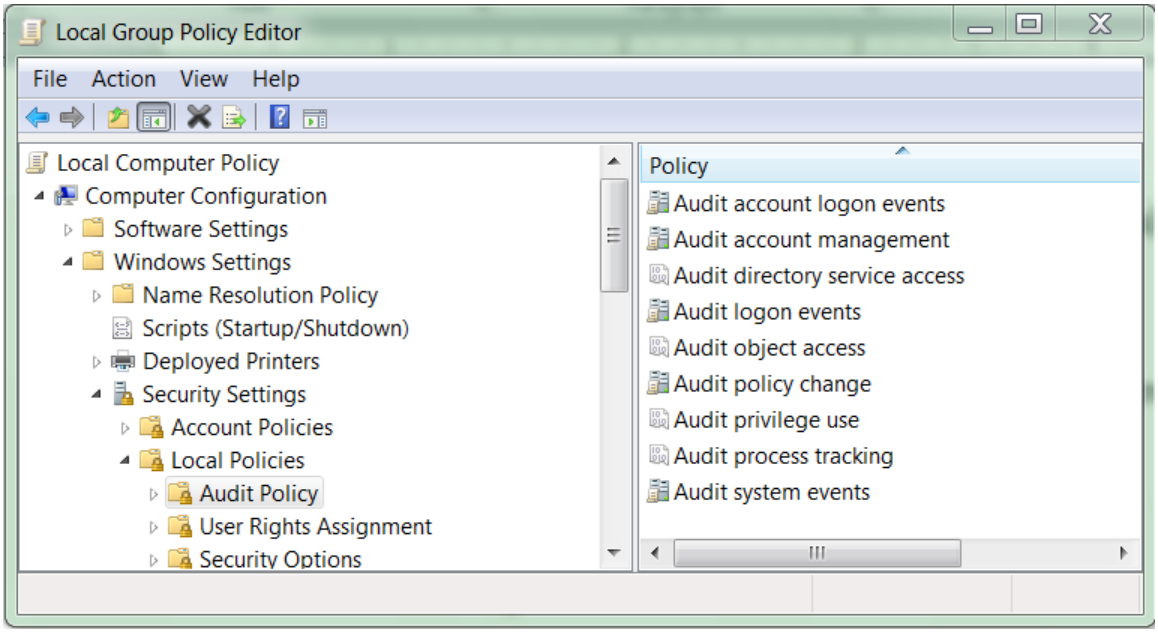
Configuring Windows Audit Policy

Windows audit policy can be set using group policies, auditpol.exe, APIs, or registry edits. The recommended methods for configuring audit policy for most companies are Group Policy or auditpol.exe. Setting a system's audit policy requires administrator-level account permissions or the appropriate delegated permissions.

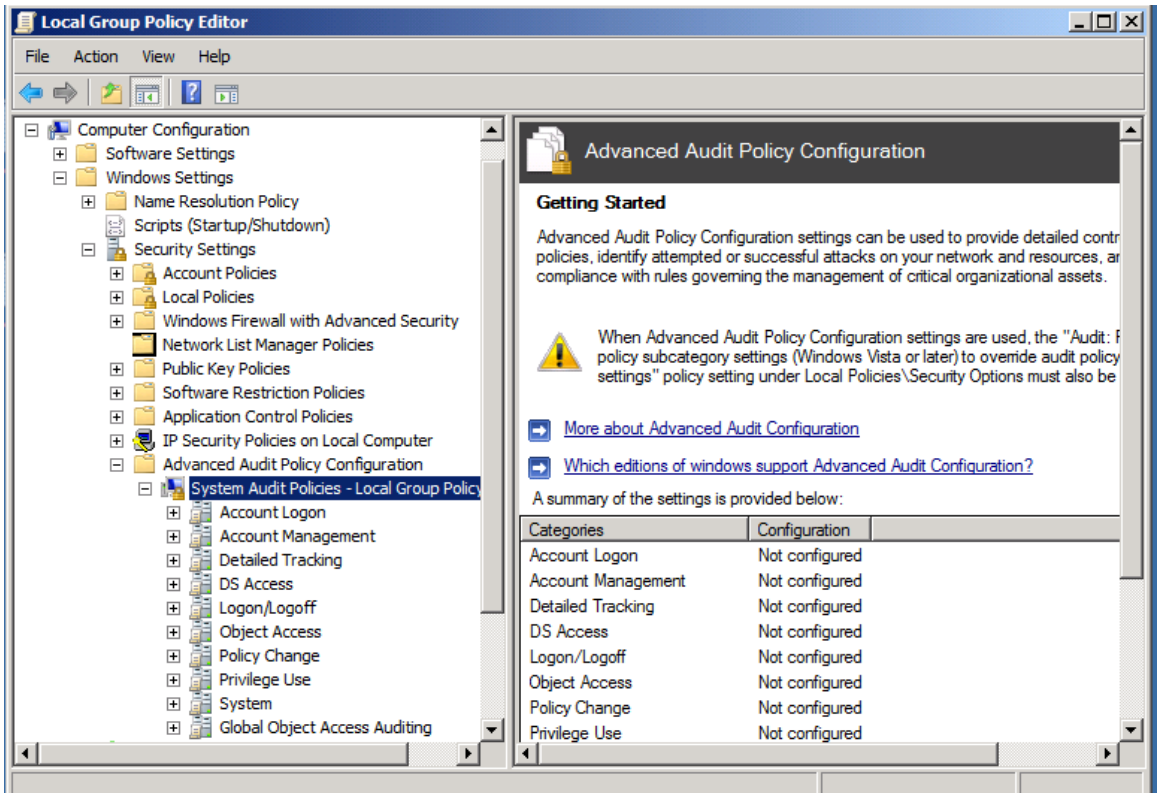
> **Note**
>
> The **Manage auditing and security log** privilege must be given to security principals (Administrators have it by default) to allow the modification of object access auditing options of individual resources, such as files, Active Directory objects, and registry keys.

Setting Windows Audit Policy by Using Group Policy

To set audit policy using group policies, configure the appropriate audit categories located under **Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy** (see the following screenshot for an example from the Local Group Policy Editor (gpedit.msc)). Each audit policy category can be enabled for **Success**, **Failure**, or **Success** and **Failure** events.



Advanced Audit Policy can be set by using Active Directory or local group policies. To set Advanced Audit Policy, configure the appropriate subcategories located under **Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy** (see the following screenshot for an example from the Local Group Policy Editor (gpedit.msc)). Each audit policy subcategory can be enabled for **Success**, **Failure**, or **Success** and **Failure** events.



Setting Windows Audit Policy Using Auditpol.exe

Auditpol.exe (for setting Windows audit policy) was introduced in Windows Server 2008 and Windows Vista. Initially, only auditpol.exe could be used to set Advanced Audit Policy, but Group Policy can be used in Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008, Windows 8, and Windows 7.

Auditpol.exe is a command-line utility. The syntax is as follows:

auditpol /set /<Category|Subcategory>:<audit category> /<success|failure:> /<enable|disable>

Auditpol.exe syntax examples:

auditpol /set /subcategory:”user account management” /success:enable /failure:enable

auditpol /set /subcategory:”logon” /success:enable /failure:enable

auditpol /set /subcategory:”IPSEC Main Mode” /failure:enable

> **Note**
>
> Auditpol.exe sets Advanced Audit Policy locally. If local policy conflicts with Active Directory or local Group Policy, Group Policy settings usually prevail over auditpol.exe settings. When multiple group or local policy conflicts exist, only one policy will prevail (that is, replace). Audit policies will not merge.

Scripting Auditpol

Microsoft provides a sample script for administrators who want to set Advanced Audit Policy by using a script instead of manually typing in each auditpol.exe command.

> **Note**
>
> Group Policy does not always accurately report the status of all enabled auditing policies, whereas auditpol.exe does. See Getting the Effective Audit Policy in Windows 7 and Windows 2008 R2 for more details.

Other Auditpol Commands

Auditpol.exe can be used to save and restore a local audit policy, and to view other auditing related commands. Here are the other **auditpol** commands.

auditpol /clear - Used to clear and reset local audit policies

auditpol /backup /file:<filename> - Used to back up a current local audit policy to a binary file

auditpol /restore /file:<filename> - Used to import a previously saved audit policy file to a local audit policy

auditpol /<get/set> /option:<CrashOnAuditFail> /<enable/disable> - If this audit policy setting is enabled, it causes the system to immediately stop (with STOP: C0000244 {Audit Failed} message) if a security audit cannot be logged for any reason. Typically, an event fails to be logged when the security audit log is full and the retention method specified for the security log is **Do Not Overwrite Event**s or **Overwrite Events by Days**. Typically it is only enabled by environments that need higher assurance that the security log is logging. If enabled, administrators must closely watch security log size and rotate logs as required. It can also be set with Group Policy by modifying the security option **Audit: Shut down system immediately if unable to log security audits** (default=disabled).

Auditpol /<get/set> /option:<AuditBaseObjects> /<enable/disable> - This audit policy setting determines whether to audit the access of global system objects. If this policy is enabled, it causes system objects, such as mutexes, events, semaphores, and DOS devices to be created with a default system access control list (SACL). Most administrators consider auditing global system objects to be too “noisy,” and they will only enable it if malicious hacking is suspected. Only named objects are given a SACL. If the audit object access audit policy (or Kernel Object audit subcategory) is also enabled, access to these

system objects is audited. When configuring this security setting, changes will not take effect until you restart Windows. This policy can also be set with Group Policy by modifying the security option **Audit the access of global system objects** (default=disabled).

auditpol /<get/set> /option:<AuditBaseDirectories> /<enable/disable> - This audit policy setting specifies that named kernel objects (such as mutexes and semaphores) are to be given SACLs when they are created. AuditBaseDirectories affects container objects while AuditBaseObjects affects objects that cannot contain other objects.

Auditpol /<get/set> /option:<FullPrivilegeAuditing> /<enable/disable> -

This audit policy setting specifies whether the client generates an event when one or more of these privileges are assigned to a user security token: AssignPrimaryTokenPrivilege, AuditPrivilege, BackupPrivilege, CreateTokenPrivilege, DebugPrivilege, EnableDelegationPrivilege, ImpersonatePrivilege, LoadDriverPrivilege, RestorePrivilege, SecurityPrivilege, SystemEnvironmentPrivilege, TakeOwnershipPrivilege, and TcbPrivilege. If this option is not enabled (default=Disabled), the BackupPrivilege and RestorePrivilege privileges are not recorded. Enabling this option can make the security log extremely noisy (sometimes hundreds of events a second) during a backup operation. This policy can also be set with Group Policy by modifying the security option **Audit: Audit the use of Backup and Restore privilege.**

Note Some information provided here was taken from the Microsoft Audit Option Type and the Microsoft SCM tool.

Enforcing Traditional Auditing or Advanced Auditing

In Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows 8, Windows 7, and Windows Vista, administrators can choose to enable the nine traditional categories or to use the subcategories. It’s a binary choice that must be made in each Windows system. Either the main categories can be enabled or the subcategories—it cannot be both.

To prevent the legacy traditional category policy from overwriting audit policy subcategories, you must enable the **Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings** policy setting located under **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options.**

We recommend that the subcategories be enabled and configured instead of the nine main categories. This requires that a Group Policy setting be enabled (to allow subcategories to override the auditing categories) along with configuring the different subcategories that support auditing policies.

Auditing subcategories can be configured by using several methods, including Group Policy and the command-line program, auditpol.exe.

For more information about Windows auditing, see the following articles:

- Advanced Security Auditing in Windows 7 and Windows Server 2008 R2
- Auditing and Compliance in Windows Server 2008
- How to use Group Policy to configure detailed security auditing settings for Windows Vista-based and Windows Server 2008-based computers in a Windows Server 2008 domain, in a Windows Server 2003 domain, or in a Windows 2000 domain
- Advanced Security Audit Policy Step-by-Step Guide

Audit Policy Recommendations

This section addresses the Windows default audit policy settings, baseline recommended audit policy settings, and the more aggressive recommendations from Microsoft, for workstation and server products.

The SCM baseline recommendations shown here, along with the settings we recommend to help detect compromise, are intended only to be a starting baseline guide to administrators. Each organization must make its own decisions regarding the threats they face, their acceptable risk tolerances, and what audit policy categories or subcategories they should enable. For further information about threats, refer to the Threats and Countermeasures Guide. Administrators without a thoughtful audit policy in place are encouraged to start with the settings recommended here, and then to modify and test, prior to implementing in their production environment.

The recommendations are for enterprise-class computers, which Microsoft defines as computers that have average security requirements and require a high level of operational functionality. Entities needing higher security requirements should consider more aggressive audit policies.

> **Note**
>
> Microsoft Windows defaults and baseline recommendations were taken from the Microsoft Security Compliance Manager tool.

The following baseline audit policy settings are recommended for normal security computers that are not known to be under active, successful attack by determined adversaries or malware.

Recommended Audit Policies by Operating System

This section contains tables that list the audit setting recommendations that apply to the following operating systems:

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2008
- Windows 8
- Windows 7

These tables contain the Windows default setting, the baseline recommendations, and the stronger recommendations for these operating systems.

Audit Policy Tables Legend	
Notation	**Recommendation**
YES	Enable in general scenarios
NO	Do **not** enable in general scenarios
IF	Enable if needed for a specific scenario, or if a role or feature for which auditing is desired is installed on the machine
DC	Enable on domain controllers
[Blank]	No recommendation

Windows 8 and Windows 7 Audit Settings Recommendations

Audit Policy						
Audit Policy Category or Subcategory	**Windows Default**		**Baseline Recommendation**		**Stronger Recommendation**	
	Success	**Failure**	**Success**	**Failure**	**Success**	**Failure**
Account Logon						
Audit Credential Validation	NO	NO	YES	NO	YES	YES
Audit Kerberos Authentication Service					YES	YES
Audit Kerberos Service Ticket Operations					YES	YES
Audit Other Account Logon Events					YES	YES

Audit Policy						
Audit Policy Category or Subcategor	Windows Default		Baseline Recommendation		Stronger Recommendation	
	Success	Failure	Success	Failure	Success	Failure
Account Management						
Audit Application Group Management						
Audit Computer Account Management			YES	NO	YES	YES
Audit Distribution Group Management						
Audit Other Account Management Events			YES	NO	YES	YES
Audit Security Group Management			YES	NO	YES	YES
Audit User Account Management	YES	NO	YES	NO	YES	YES
Detailed Tracking						
Audit DPAPI Activity					YES	YES
Audit Process Creation			YES	NO	YES	YES
Audit Process Termination						
Audit RPC Events						

Audit Policy						
Audit Policy Category or Subcategor	Windows Default		Baseline Recommendation		Stronger Recommendation	
	Success	Failure	Success	Failure	Success	Failure
DS Access						
Audit Detailed Directory Service Replication						
Audit Directory Service Access						
Audit Directory Service Changes						
Audit Directory Service Replication						
Logon and Logoff						
Audit Account Lockout	YES	NO			YES	NO
Audit User/Device Claims						
Audit IPsec Extended Mode						
Audit IPsec Main Mode					IF	IF
Audit IPsec Quick Mode						
Audit Logoff	YES	NO	YES	NO	YES	NO
Audit Logon	YES	NO	YES	NO	YES	YES
Audit Network Policy Server	YES	YES				
Audit Other Logon/Logoff Events					YES	YES

Audit Policy						
Audit Policy Category or Subcategor	Windows Default		Baseline Recommendation		Stronger Recommendation	
	Success	Failure	Success	Failure	Success	Failure
Audit Special Logon	YES	NO	YES	NO	YES	YES
Object Access						
Audit Application Generated						
Audit Certification Services						
Audit Detailed File Share						
Audit File Share						
Audit File System						
Audit Filtering Platform Connection						
Audit Filtering Platform Packet Drop						
Audit Handle Manipulation						
Audit Kernel Object						
Audit Other Object Access Events						
Audit Registry						
Audit Removable Storage						
Audit SAM						

Audit Policy						
Audit Policy Category or Subcategor	Windows Default		Baseline Recommendation		Stronger Recommendation	
	Success	Failure	Success	Failure	Success	Failure
Audit Central Access Policy Staging						
Policy Change						
Audit Audit Policy Change	YES	NO	YES	YES	YES	YES
Audit Authentication Policy Change	YES	NO	YES	NO	YES	YES
Audit Authorization Policy Change						
Audit Filtering Platform Policy Change						
Audit MPSSVC Rule-Level Policy Change					YES	
Audit Other Policy Change Events						
Privilege Use						
Audit Non Sensitive Privilege Use						
Audit Other Privilege Use Events						
Audit Sensitive Privilege Use						

Audit Policy						
Audit Policy Category or Subcategor	Windows Default		Baseline Recommendation		Stronger Recommendation	
	Success	Failure	Success	Failure	Success	Failure
System						
Audit IPsec Driver			YES	YES	YES	YES
Audit Other System Events	YES	YES				
Audit Security State Change	YES	NO	YES	YES	YES	YES
Audit Security System Extension			YES	YES	YES	YES
Audit System Integrity	YES	YES	YES	YES	YES	YES
Global Object Access Auditing						
Audit IPsec Driver						
Audit Other System Events						
Audit Security State Change						
Audit Security System Extension						
Audit System Integrity						

Windows Server 2012, Windows Server 2008 R2, and Windows Server 2008

Audit Settings Recommendations

Audit Policy						
Audit Policy Category or Subcategory	Windows Default		Baseline Recommendation		Stronger Recommendation	
	Success	Failure	Success	Failure	Success	Failure
Account Logon						
Audit Credential Validation	NO	NO	YES	YES	YES	YES
Audit Kerberos Authentication Service					YES	YES
Audit Kerberos Service Ticket Operations					YES	YES
Audit Other Account Logon Events					YES	YES
Account Management						
Audit Application Group Management						
Audit Computer Account Management			YES	DC	YES	YES
Audit Distribution Group Management						
Audit Other Account Management Events			YES	YES	YES	YES
Audit			YES	YES	YES	YES

Audit Policy						
Audit Policy Category or Subcategor	Windows Default		Baseline Recommendation		Stronger Recommendation	
	Success	Failure	Success	Failure	Success	Failure
Security Group Management						
Audit User Account Management	YES	NO	YES	YES	YES	YES
Detailed Tracking						
Audit DPAPI Activity					YES	YES
Audit Process Creation			YES	NO	YES	YES
Audit Process Termination						
Audit RPC Events						
DS Access						
Audit Detailed Directory Service Replication						
Audit Directory Service Access			DC	DC	DC	DC
Audit Directory Service Changes			DC	DC	DC	DC
Audit Directory Service Replication						
Logon and Logoff						
Audit Account Lockout	YES	NO			YES	NO
Audit User/Device						

Audit Policy						
Audit Policy Category or Subcategor	Windows Default		Baseline Recommendation		Stronger Recommendation	
	Success	Failure	Success	Failure	Success	Failure
Claims						
Audit IPsec Extended Mode						
Audit IPsec Main Mode					IF	IF
Audit IPsec Quick Mode						
Audit Logoff	YES	NO	YES	NO	YES	NO
Audit Logon	YES	NO	YES	YES	YES	YES
Audit Network Policy Server	YES	YES				
Audit Other Logon/Logoff Events					YES	YES
Audit Special Logon	YES	NO	YES	NO	YES	YES
Object Access						
Audit Application Generated						
Audit Certification Services						
Audit Detailed File Share						
Audit File Share						
Audit File System						
Audit Filtering Platform Connection						
Audit Filtering Platform Packet Drop						
Audit						

Audit Policy						
Audit Policy Category or Subcategor	Windows Default		Baseline Recommendation		Stronger Recommendation	
	Success	Failure	Success	Failure	Success	Failure
Handle Manipulation						
Audit Kernel Object						
Audit Other Object Access Events						
Audit Registry						
Audit Removable Storage						
Audit SAM						
Audit Central Access Policy Staging						
Policy Change						
Audit Audit Policy Change	YES	NO	YES	YES	YES	YES
Audit Authentication Policy Change	YES	NO	YES	NO	YES	YES
Audit Authorization Policy Change						
Audit Filtering Platform Policy Change						
Audit MPSSVC Rule-Level Policy Change					YES	
Audit Other Policy						

Audit Policy						
Audit Policy Category or Subcategor	Windows Default		Baseline Recommendation		Stronger Recommendation	
	Success	Failure	Success	Failure	Success	Failure
Change Events						
Privilege Use						
Audit Non-Sensitive Privilege Use						
Audit Other Privilege Use Events						
Audit Sensitive Privilege Use			YES	YES	YES	YES
System						
Audit IPsec Driver			YES	YES	YES	YES
Audit Other System Events	YES	YES				
Audit Security State Change	YES	NO	YES	YES	YES	YES
Audit Security System Extension			YES	YES	YES	YES
Audit System Integrity	YES	YES	YES	YES	YES	YES
Global Object Access Auditing						
Audit IPsec Driver						
Audit Other System Events						
Audit Security State Change						
Audit Security						

Audit Policy						
Audit Policy Category or Subcategor	Windows Default		Baseline Recommendation		Stronger Recommendation	
	Success	Failure	Success	Failure	Success	Failure
System Extension						
Audit System Integrity						

Set Audit Policy on Workstations and Servers

All event log management plans should monitor workstations and servers. A common mistake is to only monitor servers or domain controllers. Because malicious hacking often initially occurs on workstations, not monitoring workstations is ignoring the best and earliest source of information.

Administrators should thoughtfully review and test any audit policy prior to implementation in their production environment.

Events to Monitor

A perfect event ID to generate a security alert should contain the following attributes:

- High likelihood that occurrence indicates unauthorized activity
- Low number of false positives
- Occurrence should result in an investigative/forensics response

Two types of events should be monitored and alerted:

1. Those events in which even a single occurrence indicates unauthorized activity
2. An accumulation of events above an expected and accepted baseline

An example of the first event is:

If Domain Admins (DAs) are forbidden from logging on to computers that are not domain controllers, a single occurrence of a DA member logging on to an end-user workstation should generate an alert and be investigated. This type of alert is easy to generate by using the Audit Special Logon event 4964 (Special groups have been assigned to a new logon). Other examples of single instance alerts include:

- If Server A should never connect to Server B, alert when they connect to each other.
- Alert if a normal end-user account is unexpectedly added to a sensitive security group.
- If employees in factory location A never work at night, alert when a user logs on at midnight.
- Alert if an unauthorized service is installed on a domain controller.

- Investigate if a regular end-user attempts to directly log on to a SQL Server for which they have no clear reason for doing so.
- If you have no members in your DA group, and someone adds themselves there, check it immediately.

An example of the second event is:

An aberrant number of failed logons could indicate a password guessing attack. For an enterprise to provide an alert for an unusually high number of failed logons, they must first understand the normal levels of failed logons within their environment prior to a malicious security event.

For a comprehensive list of events that you should include when you monitor for signs of compromise, please see Appendix L: Events to Monitor.

Active Directory Objects and Attributes to Monitor

The following are the accounts, groups, and attributes that you should monitor to help you detect attempts to compromise your Active Directory Domain Services installation.

- Systems for disabling or removal of antivirus and antimalware software (automatically restart protection when it is manually disabled)
- Administrator accounts for unauthorized changes
- Activities that are performed by using privileged accounts (automatically remove account when suspicious activities are completed or allotted time has expired)
- Privileged and VIP accounts in AD DS. Monitor for changes, particularly changes to attributes on the Account tab (for example, cn, name, sAMAccountName, userPrincipalName, or userAccountControl). In addition to monitoring the accounts, restrict who can modify the accounts to as small a set of administrative users as possible.

  Refer to Appendix L: Events to Monitor for a list of recommended events to monitor, their criticality ratings, and an event message summary.
- Group servers by the classification of their workloads, which allows you to quickly identify the servers that should be the most closely monitored and most stringently configured
- Changes to the properties and membership of following AD DS groups: Enterprise Admins (EA), Domain Admins (DA), Administrators (BA), and Schema Admins (SA)
- Disabled privileged accounts (such as built-in Administrator accounts in Active Directory and on member systems) for enabling the accounts
- Management accounts to log all writes to the account

- Built-in Security Configuration Wizard to configure service, registry, audit, and firewall settings to reduce the server's attack surface. Use this wizard if you implement jump servers as part of your administrative host strategy.

Additional Information for Monitoring Active Directory Domain Services

Review the following links for additional information about monitoring AD DS:

- Global Object Access Auditing is Magic – Provides information about configuring and using Advanced Audit Policy Configuration that was added to Windows 7 and Windows Server 2008 R2.
- Introducing Auditing Changes in Windows 2008 – Introduces the auditing changes made in Windows 2008.
- Cool Auditing Tricks in Vista and 2008 – Explains interesting new features of auditing in Windows Vista and Windows Server 2008 that can be used for troubleshooting problems or seeing what's happening in your environment.
- One-Stop Shop for Auditing in Windows Server 2008 and Windows Vista – Contains a compilation of auditing features and information contained in Windows Server 2008 and Windows Vista.
- AD DS Auditing Step-by-Step Guide – Describes the new Active Directory Domain Services (AD DS) auditing feature in Windows Server 2008. It also provides procedures to implement this new feature.

General List of Security Event ID Recommendation Criticalities

All Event ID recommendations are accompanied by a criticality rating as follows:

High: Event IDs with a high criticality rating should always and immediately be alerted and investigated.

Medium : An Event ID with a medium criticality rating could indicate malicious activity, but it must be accompanied by some other abnormality (for example, an unusual number occurring in a particular time period, unexpected occurrences, or occurrences on a computer that normally would not be expected to log the event.). A medium-criticality event may also r be collected as a metric and compared over time.

Low: And Event ID with a low criticality events should not garner attention or cause alerts, unless correlated with medium or high criticality events.

These recommendations are meant to provide a baseline guide for the administrator. All recommendations should be thoroughly reviewed prior to implementation in a production environment.

Refer to Appendix L: Events to Monitor for a list of the recommended events to monitor, their criticality ratings, and an event message summary.

Planning For Compromise

Law Number One: Nobody believes anything bad can happen to them, until it does. – 10 Immutable Laws of Security Administration

Disaster recovery plans in many organizations focus on recovering from regional disasters or failures that result in loss of computing services. However, when working with compromised customers, we often find that recovering from intentional compromise is absent in their disaster recovery plans. This is particularly true when the compromise results in theft of intellectual property or intentional destruction that leverages logical boundaries (such as destruction of all Active Directory domains or all servers) rather than physical boundaries (such as destruction of a datacenter). Although an organization may have incident response plans that define initial activities to take when a compromise is discovered, these plans often omit steps to recover from a compromise that affects the entire computing infrastructure.

Because Active Directory provides rich identity and access management capabilities for users, servers, workstations, and applications, it is invariably targeted by attackers. If an attacker gains highly privileged access to an Active Directory domain or domain controller, that access can be leveraged to access, control, or even destroy the entire Active Directory forest.

This document has discussed some of the most common attacks against Windows and Active Directory and countermeasures you can implement to reduce your attack surface, but the only sure way to recover in the event of a complete compromise of Active Directory is to be prepared for the compromise before it happens. This section focuses less on technical implementation details than previous sections of this document, and more on high-level recommendations that you can use to create a holistic, comprehensive approach to secure and manage your organization’s critical business and IT assets.

Whether your infrastructure has never been attacked, has resisted attempted breaches, or has succumbed to attacks and been fully compromised, you should plan for the inevitable reality that you will be attacked again and again. It is not possible to prevent attacks, but it may indeed be possible to prevent significant breaches or wholesale compromise. Every organization should closely evaluate their existing risk management programs, and make necessary adjustments to help reduce their overall level of vulnerability by making balanced investments in prevention, detection, containment, and recovery.

To create effective defenses while still providing services to the users and businesses that depend on your infrastructure and applications, you may need to consider novel ways to prevent, detect, and contain compromise in your environment, and then recover from the compromise. The approaches and recommendations in this document may not help you repair a compromised Active Directory installation, but can help you secure your next one.

Recommendations for recovering an Active Directory forest are presented in Windows Server 2008: Planning for Active Directory Forest Recovery. You may be able to prevent your new environment from being completely compromised, but even if you can't, you will have tools to recover and regain control of your environment.

Rethinking the Approach

Law Number Eight: The difficulty of defending a network is directly proportional to its complexity. – 10 Immutable Laws of Security Administration

It is generally well-accepted that if an attacker has obtained SYSTEM, Administrator, root, or equivalent access to a computer, regardless of operating system, that computer can no longer be considered trustworthy, no matter how many efforts are made to "clean" the system. Active Directory is no different. If an attacker has obtained privileged access to a domain controller or a highly privileged account in Active Directory, unless you have a record of every modification the attacker makes or a known good backup, you can never restore the directory to a completely trustworthy state.

When a member server or a workstation is compromised and altered by an attacker, the computer is no longer trustworthy, but neighboring uncompromised servers and workstations are—compromise of one computer does not imply that all computers are compromised.

However, in an Active Directory domain, all domain controllers host replicas of the same AD DS database. If a single domain controller is compromised and an attacker modifies the AD DS database, those modifications replicate to every other domain controller in the domain, and depending on the partition in which the modifications are made, the forest. Even if you reinstall every domain controller in the forest, you are simply reinstalling the hosts on which the AD DS database resides. Malicious modifications to Active Directory will replicate to freshly installed domain controllers as easily as they will replicate to domain controllers that have been running for years.

In assessing compromised environments, we commonly find that what was believed to be the first breach "event" was actually triggered after weeks, months, or even years after attackers had initially compromised the environment. Attackers usually obtained the credentials for highly privileged accounts long before a breach was detected, and they leveraged those accounts to compromise the directory, domain controllers, member servers, workstations, and even connected non-Windows systems.

These findings are consistent with several findings in Verizon's 2012 Data Breach Investigations Report, which states that:

- 98 percent of data breaches stemmed from external agents
- 85 percent of data breaches took weeks or more to discover
- 92 percent of incidents were discovered by a third party, and

- 97 percent of breaches were avoidable though simple or intermediate controls.

A compromise to the degree described earlier is effectively irreparable, and the standard advice to “flatten and rebuild” every compromised system is simply not feasible or even possible if Active Directory has been compromised or destroyed. Even restoring to a known good state does not eliminate the flaws that allowed the environment to be compromised in the first place.

Although you must defend every facet of your infrastructure, an attacker only needs to find enough flaws in your defenses to get to their desired goal. If your environment is relatively simple and pristine, and historically well-managed, then implementing the recommendations provided earlier in this document may be a straightforward proposition.

However, we have found that the older, larger, and more complex the environment, the more likely it is that the recommendations in this document will be infeasible or even impossible to implement. It is much harder to secure an infrastructure after the fact than it is to start fresh and to construct an environment that is resistant to attack and compromise. But as previously noted, it is no small undertaking to rebuild an entire Active Directory forest. For these reasons, we recommend a more focused, targeted approach to secure your Active Directory forests.

Rather than focusing on and trying to fix all of the things that are “broken,” consider an approach in which you prioritize based on what is most important to your business and in your infrastructure. Instead of trying to remediate an environment filled with outdated, misconfigured systems and applications, consider creating a new small, secure environment into which you can safely port the users, systems, and information that are most critical to your business.

In this section, we describe an approach by which you can create a pristine AD DS forest that serves as a “life boat” or “secure cell” for your core business infrastructure. A pristine forest is simply a newly installed Active Directory forest that is typically limited in size and scope, and which is built by using current operating systems, applications, and with the principles described in Reducing the Active Directory Attack Surface earlier in this document.

By implementing the recommended configuration settings in a newly built forest, you can create an AD DS installation that is built from the ground up with secure settings and practices, and you can reduce the challenges that accompany supporting legacy systems and applications. While detailed instructions for the design and implementation of a pristine AD DS installation are outside the scope of this document, you should follow some general principles and guidelines to create a “secure cell” into which you can house your most critical assets. These guidelines are as follows:

1. Identify principles for segregating and securing critical assets.
2. Define a limited, risk-based migration plan.
3. Leverage “nonmigratory” migrations where necessary.
4. Implement “creative destruction.”
5. Isolate legacy systems and applications.

6. Simplify security for end users.

Identifying Principles for Segregating and Securing Critical Assets

The characteristics of the pristine environment that you create to house critical assets can vary widely. For example, you may choose to create a pristine forest into which you migrate only VIP users and sensitive data that only those users can access. You may create a pristine forest in which you migrate not only VIP users, but which you implement as an administrative forest, implementing the principles described in Reducing the Active Directory Attack Surface to create secure administrative accounts and hosts that can be used to manage your legacy forests from the pristine forest. You might implement a "purpose-built" forest that houses VIP accounts, privileged accounts, and systems requiring additional security such as servers running Active Directory Certificate Services (AD CS) with the sole goal of segregating them from less-secure forests. Finally, you might implement a pristine forest that becomes the de facto location for all new users, systems, applications and data, allowing you to eventually decommission your legacy forest via attrition.

Regardless of whether your pristine forest contains a handful of users and systems or it forms the basis for a more aggressive migration, you should follow these principles in your planning:

1. Assume that your legacy forests have been compromised.
2. Do not configure a pristine environment to trust a legacy forest, although you can configure a legacy environment to trust a pristine forest.
3. Do not migrate user accounts or groups from a legacy forest to a pristine environment if there is a possibility that the accounts' group memberships, SID history, or other attributes may have been maliciously modified. Instead, use "nonmigratory" approaches to populate a pristine forest. (Nonmigratory approaches are described later in this section.)
4. Do not migrate computers from legacy forests to pristine forests. Implement freshly installed servers in the pristine forest, install applications on the freshly installed servers, and migrate application data to the newly installed systems. For file servers, copy data to freshly installed servers, set ACLs by using users and groups in the new forest, and then create print servers in a similar fashion.
5. Do not permit the installation of legacy operating systems or applications in the pristine forest. If an application cannot be updated and freshly installed, leave it in the legacy forest and consider creative destruction to replace the application's functionality. (Creative destruction is described later in this document.)

Defining a Limited, Risk-Based Migration Plan

Creating a limited, risk-based migration plan simply means that when deciding which users, applications, and data to migrate into your pristine forest, you should identify migration targets based on the degree of risk to which your organization is exposed if one of the users or systems is compromised. VIP users whose accounts are most likely to be targeted by attackers should be housed in the pristine forest.

Applications that provide vital business functions should be installed on freshly built servers in the pristine forest, and highly sensitive data should be moved to secured servers in the pristine forest.

If you do not already have a clear picture of the most business-critical users, systems, applications, and data in your Active Directory environment, work with business units to identify them. Any application required for the business to operate should be identified, as should any servers on which critical applications run or critical data is stored. By identifying the users and resources that are required for your organization to continue to function, you create a naturally prioritized collection of assets on which to focus your efforts.

Leveraging “Nonmigratory” Migrations

Whether you know that your environment has been compromised, suspect that it has been compromised, or simply prefer not to migrate legacy data and objects from a legacy Active Directory installation to a new one, consider migration approaches that do not technically “migrate” objects.

User Accounts

In a traditional Active Directory migration from one forest to another, the SIDHistory (SID history) attribute on user objects is used to store users’ SID and the SIDs of groups that users were members of in the legacy forest. If users accounts are migrated to a new forest, and they access resources in the legacy forest, the SIDs in the SID history are used to create an access token that allows the users to access resources to which they had access before the accounts were migrated.

Maintaining SID history, however, has proven problematic in some environments because populating users’ access tokens with current and historical SIDs can result in token bloat. Token bloat is an issue in which the number of SIDs that must be stored in a user’s access token uses or exceeds the amount of space available in the token.

Although token sizes can be increased to a limited extent, the ultimate solution to token bloat is to reduce the number of SIDs associated with user accounts, whether by rationalizing group memberships, eliminating SID history, or a combination of both. For more information about token bloat, see MaxTokenSize and Kerberos Token Bloat.

Rather than migrating users from a legacy environment (particularly one in which group memberships and SID histories may be compromised) by using SID history, consider leveraging metadirectory applications to “migrate” users, without carrying SID histories into the new forest. When user accounts are created in the new forest, you can use a metadirectory application to map the accounts to their corresponding accounts in the legacy forest.

To provide the new user accounts access to resources in the legacy forest, you can use the metadirectory tooling to identify resource groups into which the users' legacy accounts were granted access, and then add the users' new accounts to those groups. Depending on your group strategy in the legacy forest, you may need to create domain local groups for resource access or convert existing groups to domain local groups to allow the new accounts to be added to resource groups. By focusing first on the most critical applications and data and migrating them to the new environment (with or without SID history), you can limit the amount of effort expended in the legacy environment.

> **Note**
>
> Some of the applications listed in Appendix J: Third-Party RBAC Vendors and Appendix K: Third-Party PIM Vendors provide mechanisms to perform "nonmigratory" migrations, as does Microsoft Forefront Identity Manager.

Servers and Workstations

In a traditional migration from one Active Directory forest to another, migrating computers is often relatively simple compared to migrating users, groups, and applications. Depending on the computer role, migrating to a new forest can be as simple as disjoining an old domain and joining a new one. However, migrating computer accounts intact into a pristine forest defeats the purpose of creating a fresh environment. Rather than migrating (potentially compromised, misconfigured, or outdated) computer accounts to a new forest, you should freshly install servers and workstations in the new environment. You can migrate data from systems in the legacy forest to systems in the pristine forest, but not the systems that house the data.

Applications

Applications can present the most significant challenge in any migration from one forest to another, but in the case of a "nonmigratory" migration, one of the most basic principles you should apply is that applications in the pristine forest should be current, supported, and freshly installed. Data can be migrated from application instances in the old forest where possible. In situations in which an application cannot be "recreated" in the pristine forest, you should consider approaches such as creative destruction or isolation of legacy applications as described in the following section.

Implementing Creative Destruction

Creative destruction is an economics term that describes economic development created by the destruction of a prior order. In recent years, the term has been applied to information technology. It typically refers to mechanisms by which old infrastructure is eliminated, not by upgrading it, but by replacing it with something altogether new. The 2011 Gartner Symposium IT[XPO] for CIOs and senior IT executives presented creative destruction as one of its key themes for cost reduction and increases in efficiency. Improvements in security are possible as a natural outgrowth of the process.

For example, an organization may be composed of multiple business units that use a different application that performs similar functionality, with varying degrees of modernity and vendor support. Historically, IT might be responsible for maintaining each business unit's application separately, and consolidation efforts would consist of attempting to figure out which application offered the best functionality and then migrating data into that application from the others.

In creative destruction, rather than maintaining outdated or redundant applications, you implement entirely new applications to replace the old, migrate data into the new applications, and decommission the old applications and the systems on which they run. In some cases, you can implement creative destruction of legacy applications by deploying a new application in your own infrastructure, but wherever possible, you should consider porting the application to a cloud-based solution instead.

By deploying cloud-based applications to replace legacy in-house applications, you not only reduce maintenance efforts and costs, but you reduce your organization's attack surface by eliminating legacy systems and applications that present vulnerabilities for attackers to leverage. This approach provides a faster way for an organization to obtain desired functionality while simultaneously eliminating legacy targets in the infrastructure. Although the principle of creative destruction does not apply to all IT assets, it provides an often viable option to eliminating legacy systems and applications while simultaneously deploying robust, secure, cloud-based applications.

Isolating Legacy Systems and Applications

A natural outgrowth of migrating your business-critical users and systems to a pristine, secure environment is that your legacy forest will be contain less valuable information and systems. Although the legacy systems and applications that remain in the less secure environment may present elevated risk of compromise, they also represent a reduced severity of compromise. By rehoming and modernizing your critical business assets, you can focus on deploying effective management and monitoring while not needing to accommodate legacy settings and protocols.

When you have rehomed your critical data to a pristine forest, you can evaluate options to further isolating legacy systems and applications in your "main" AD DS forest. Although you might implement creative destruction to replace one application and the servers on which it runs, in other cases you might consider additional isolation of the least secure systems and applications. For example, an application that is used by a handful of users, but which requires legacy credentials like LAN Manager hashes can be migrated to a small domain you create to support systems for which you have no replacement options.

By removing these systems from domains where they forced implementation of legacy settings, you can subsequently increase the security of the domains by configuring them to support only current operating systems and applications. Although, it is preferable to decommission legacy systems and applications whenever possible. If decommissioning is simply not feasible for a small segment of your legacy population, segregating it into a separate domain (or forest) allows you to perform incremental improvements in the rest of the legacy installation.

Simplifying Security for End Users

In most organizations, users who have access to the most sensitive information due to the nature of their roles in the organization often have the least amount of time to devote to learning complex access restrictions and controls. Although you should have a comprehensive security education program for all users in your organization, you should also focus on making security as simple to use as possible by implementing controls that are transparent and simplifying principles to which users adhere.

For example, you may define a policy in which executives and other VIPs are required to use secure workstations to access sensitive data and systems, allowing them to use their other devices to access less sensitive data. This is a simple principle for users to remember, but you can implement a number of backend controls to help to enforce the approach.

You can use Authentication Mechanism Assurance to permit the users to access sensitive data only if they've logged on to their secure systems using their smart cards, and can use IPsec and user rights restrictions to control the systems from which they can connect to sensitive data repositories. You can use the Microsoft Data Classification Toolkit to build a robust file classification infrastructure, and you can implement Dynamic Access Control to restrict access to data based on characteristics of an access attempt, translating business rules into technical controls.

From the perspective of the user, accessing sensitive data from a secured system "just works," and attempting to do so from an unsecured system "just doesn't." However, from the perspective of monitoring and managing your environment, you're helping to create identifiable patterns in how users access sensitive data and systems, making it easier for you to detect anomalous access attempts.

In environments in which user resistance to long, complex passwords has resulted in insufficient password policies, particularly for VIP users, consider alternate approaches to authentication, whether via smart cards (which come in a number of form factors and with additional features to strengthen authentication), biometric controls such as finger-swipe readers, or even authentication data that is secured by trusted platform module (TPM) chips in users' computers. Although multifactor authentication does not prevent credential theft attacks if a computer is already compromised, by giving your users easy-to-use authentication controls, you can assign more robust passwords to the accounts of users for whom traditional user name and password controls are unwieldy.

Maintaining a More Secure Environment

Law Number Ten: Technology is not a panacea. – 10 Immutable Laws of Security Administration

When you have created a manageable, secure environment for your critical business assets, your focus should shift to ensuring that it is maintained securely.

Although you've been given specific technical controls to increase the security of your AD DS installations, technology alone will not protect an environment in which IT does not work in partnership with the business to maintain a secure, usable infrastructure. The high level recommendations in this section are meant to be used as guidelines that you can use to develop not only effective security, but effective lifecycle management.

In some cases, your IT organization might already have a close working relationship with business units, which will ease implementing these recommendations. In organizations in which IT and business units are not closely tied, you might need to first obtain executive sponsorship for efforts to forge a closer relationship between IT and business units. The Executive Summary in this document is intended to be useful as a standalone document for executive review, and it can be disseminated to decision makers in your organization.

Creating Business-Centric Security Practices for Active Directory

In the past, information technology within many organizations was viewed as a support structure and a cost center. IT departments were often largely segregated from business users, and interactions limited to a request-response model in which the business requested resources and IT responded.

As technology has evolved and proliferated, the vision of "a computer on every desktop" has effectively come to pass for much of the world, and even been eclipsed by the broad range of easily accessible technologies available today. Information technology is no longer a support function, it is a core business function. If your organization could not continue to function if all IT services were unavailable, your organization's business is, at least in part, information technology.

To create effective compromise recovery plans, IT services must work closely with business units in your organization to identify not only the most critical components of the IT landscape, but the critical functions required by the business. By identifying what is important to your organization as a whole, you can focus on securing the components that have the most value. This is not a recommendation to shirk the security of low value systems and data. Rather, like you define levels of service for system uptime, you should consider defining levels of security control and monitoring based on criticality of asset.

When you have invested in creating a current, secure, manageable environment, you can shift focus to managing it effectively and ensuring that you have effective lifecycle management processes that aren't determined only by IT, but by the business. To achieve this, you need not only to partner with the business, but to invest the business in "ownership" of data and systems in Active Directory.

When data and systems are introduced into Active Directory without designated owners, business owners and IT owners, there is no clear chain of responsibility for the provisioning, management, monitoring, updating, and eventually decommissioning the system. This results in infrastructures in which systems expose the organization to risk but cannot be decommissioned because ownership is unclear. To effectively manage the lifecycle of the users, data, applications, and systems managed by your Active Directory installation, you should follow the principles described in this section.

Assign a Business Owner to Active Directory Data

Data in Active Directory should have an identified business owner, that is, a specified department or user who is the point of contact for decisions about the lifecycle of the asset. In some cases, the business owner of a component of Active Directory will be an IT department or user. Infrastructure components such as domain controllers, DHCP and DNS servers, and Active Directory will most likely be "owned" by IT. For data that is added to AD DS to support the business (for example, new employees, new applications, and new information repositories), a designated business unit or user should be associated with the data.

Whether you use Active Directory to record ownership of data in the directory, or whether you implement a separate database for tracking IT assets, no user account should be created, no server or workstation should be installed, and no application should be deployed without a designated owner of record. Trying to establish ownership of systems after they've been deployed in production can be challenging at best, and impossible in some cases. Therefore, ownership should be established at the time the data is introduced into Active Directory.

Implement Business-Driven Lifecycle Management

Lifecycle management should be implemented for all data in Active Directory. For example, when a new application is introduced into an Active Directory domain, the application's business owner should, at regular intervals, be expected to attest to the continued use of the application. When a new version of an application is released, the application's business owner should be informed and should decide if and when the new version will be implemented.

If a business owner chooses not to approve deployment of a new version of an application, that business owner should also be notified of the date when the current version will no longer be supported and should be responsible for determining whether the application will be decommissioned or replaced. Keeping legacy applications running and unsupported should not be an option.

When user accounts are created in Active Directory, their managers of record should be notified at object creation and required to attest to the validity of the account at regular intervals. By implementing a business driven lifecycle and regular attestation of the validity of the data, the people who are best equipped to identify anomalies in the data are the people who review the data.

For example, attackers might create user accounts that appear to be valid accounts, following your organization's naming conventions and object placement. To detect these account creations, you might implement a daily task that returns all user objects without a designated business owner so that you can investigate the accounts. If attackers create accounts and assign a business owner, by implementing a task that reports new object creation to the designated business owner, the business owner can quickly identify whether the account is legitimate.

You should implement similar approaches to security and distribution groups. Although some groups may be functional groups created by IT, by creating every group with a designated owner, you can retrieve all groups owned by a designated user and require the user to attest to the validity of their memberships. Similar to the approach taken with user account creation, you can trigger reporting group modifications to the designated business owner. The more routine it becomes for a business owner to attest to the validity or invalidity of data in Active Directory, the

more equipped you are to identify anomalies that can indicate process failures or actual compromise.

Classify all Active Directory Data

In addition to recording a business owner for all Active Directory data at the time it is added to the directory, you should also require business owners to provide classification for the data. For example, if an application stores business-critical data, the business owner should label the application as such, in accordance with your organization's classification infrastructure.

Some organizations implement data classification policies that label data according to the damage that exposure of the data would incur if it were stolen or exposed. Other organizations implement data classification that labels data by criticality, by access requirements, and by retention. Regardless of the data classification model in use in your organization, you should ensure that you are able to apply classification to Active Directory data, not only to "file" data. If a user's account is a VIP account, it should be identified in your asset classification database (whether you implement this via the use of attributes on the objects in AD DS, or whether you deploy separate asset classification databases).

Within your data classification model, you should include classification for AD DS data such as the following.

Systems

You should not only classify data, but also their server populations. For each server, you should know what operating system is installed, what general roles the server provides, what applications are running on the server, the IT owner of record, and the business owner of record, where applicable. For all data or applications running on the server, you should require classification, and the server should be secured according to the requirements for the workloads it supports and the classifications applied to the system and data. You can also group servers by the classification of their workloads, which allows you to quickly identify the servers that should be the most closely monitored and most stringently configured.

Applications

You should classify applications by functionality (what they do), user base (who uses the applications), and the operating system on which they run. You should maintain records that contain version information, patch status, and any other pertinent information. You should also classify applications by the types of data they handle, as previously described.

Users

Whether you call them "VIP" users, critical accounts, or use a different label, the accounts in your Active Directory installations that are most likely to be targeted by attackers should be tagged and monitored. In most organizations, it is simply not feasible to monitor all of the activities of all users. However, if you are able to identify the critical accounts in your Active Directory installation, you can monitor those accounts for changes as described earlier in this document.

You can also begin to build a database of “expected behaviors” for these accounts as you audit the accounts. For example, if you find that a given executive uses his secured workstation to access business-critical data from his office and from his home, but rarely from other locations, if you see attempts to access data by using his account from an unauthorized computer or a location halfway around the planet where you know the executive is not currently located, you can more quickly identify and investigate this anomalous behavior.

By integrating business information with your infrastructure, you can use that business information to help you identify false positives. For example, if executive travel is recorded in a calendar that is accessible to IT staff responsible for monitoring the environment, you can correlate connection attempts with the executives’ known locations.

Let’s say Executive A is normally located in Chicago and uses a secured workstation to access business-critical data from his desk, and an event is triggered by a failed attempt to access the data from an unsecured workstation located in Atlanta. If you are able to verify that the executive is currently in Atlanta, you can resolve the event by contacting the executive or the executive’s assistant to determine if the access failure was the result of the executive forgetting to use the secured workstation to access the data. By constructing a program that uses the approaches described in Simplifying Security for End Users, you can begin to build a database of expected behaviors for the most “important” accounts in your Active Directory installation that can potentially help you more quickly discover and respond to attacks.

Summary of Best Practices

The following table contains a summary of the best practices for securing Active Directory as described in this document, with hyperlinks to the sections in which the recommendations are detailed. Practices and controls that are described as tactical in nature may be implemented more quickly and with less effort than those that are described as strategic or are applicable to discrete components in the larger infrastructure.

Some of the best practices described here are not specific to Active Directory, but are designed to help you implement solutions that can reduce the most commonly exploited vulnerabilities that are used to gain an initial foothold in an organization's infrastructure, which may then be used to launch attacks directly against Active Directory.

Other recommendations are specific to Active Directory and may be implemented in existing AD DS installations, or implemented as fundamental principles in a new Active Directory installation, whether that installation is an enterprise deployment (housing corporate users, servers, workstations, and applications), or whether the installation is "purpose-built" (designed to house critical accounts and assets that should be separated from other AD DS forests and secured more stringently).

Another version of this table, which provides information about whether each best practice is tactical or strategic in nature, and whether its implementation provides preventative or detective controls can be found in the Executive Summary section of this document. The following table provides each recommended best practice in general order of priority, and links to more information about each.

Best Practice		More Information
1	Patch applications.	Initial Breach Targets Appendix A: Patch and Vulnerability Management Software
2	Patch operating systems.	Initial Breach Targets Appendix A: Patch and Vulnerability Management Software Principles for Creating Secure Administrative Hosts Secure Configuration of Domain Controllers
3	Deploy and promptly update antivirus and antimalware software across all systems and monitor for attempts to remove or disable it.	Initial Breach Targets Appendix A: Patch and Vulnerability Management Software
4	Monitor sensitive Active Directory objects for modification attempts and Windows for events that may indicate attempted compromise.	Monitoring Active Directory for Signs of Compromise Active Directory Objects and Attributes to Monitor Appendix L: Events to Monitor

Best Practice		More Information
5	Protect and monitor accounts for users who have access to sensitive data.	VIP Accounts Implementing Robust Authentication Controls Identifying Principles for Segregating and Securing Critical Assets Simplify Security for End Users Active Directory Objects and Attributes to Monitor
6	Prevent powerful accounts from being used on unauthorized systems.	Implementing Least-Privilege Administrative Models Implementing Secure Administrative Hosts Securing Domain Controllers Against Attack
7	Eliminate permanent membership in highly privileged groups.	Appendix B: Privileged Accounts and Groups in Active Directory Appendix C: Protected Accounts and Groups in Active Directory Appendix D: Securing Built-in Administrator Accounts in Active Directory Appendix E: Securing Enterprise Admins Groups in Active Directory Appendix F: Securing Domain Admins Groups in Active Directory Appendix G: Securing Administrators Groups in Active Directory Appendix H: Securing Local Administrator Accounts and Groups Appendix J: Third-Party RBAC Vendors
8	Implement controls to grant temporary membership in privileged groups when needed.	Appendix I: Creating Management Accounts for Protected Accounts and Groups in Active Directory Appendix K: Third-Party PIM Vendors
9	Implement secure administrative hosts.	Implementing Secure Administrative Hosts
10	Use application whitelisting on domain controllers, administrative hosts, and other sensitive systems.	Implementing Secure Administrative Hosts Securing Domain Controllers Against Attack
11	Identify critical assets, and prioritize their security and monitoring.	Planning for Compromise
12	Implement least-privilege, role-based access controls to administer the directory, its supporting infrastructure, and domain-joined systems.	Role-Based Access Controls (RBAC) for Active Directory Appendix J: Third-Party RBAC Vendors
13	Isolate legacy systems and applications.	Isolating Legacy Systems and Applications

Best Practice		More Information
14	Decommission legacy systems and applications.	Implementing Creative Destruction
15	Implement secure development lifecycle programs for custom applications.	Lack of Secure Application Development Practices
16	Implement configuration management, review compliance regularly, and evaluate settings with each new hardware or software version.	Maintaining a More Secure Environment
17	Migrate critical assets to pristine forests with stringent security and monitoring requirements.	Planning for Compromise
18	Simplify security for end users.	Simplifying Security for End Users
19	Use host-based firewalls to control and secure communications.	Principles for Creating Secure Administrative Hosts Secure Configuration of Domain Controllers
20	Patch devices.	Contact your device vendors Appendix A: Patch and Vulnerability Management Software
21	Implement business-centric lifecycle management for IT assets.	Creating Business-Centric Security Practices for Active Directory
22	Create or update incident recovery plans.	Planning for Compromise

Appendices

Appendices are included in this document to augment the information contained in the body of the document. The list of appendices and a brief description of each in included the following table.

Appendix	Description
A - Patch and Vulnerability Management Software	Contains a list of companies that produce patch and vulnerability management software.
B - Privileged Accounts and Groups in Active Directory	Provides background information that helps you to identify the users and groups you should focus on securing because they can be leveraged by attackers to compromise and even destroy your Active Directory installation.
C – Protected Accounts and Groups in Active	Contains information about protected groups in Active Directory. It also contains information for

Appendix	Description
Directory	limited customization (removal) of groups that are considered protected groups and are affected by AdminSDHolder and SDProp.
D – Securing Built-in Administrator Accounts in Active Directory	Contains guidelines to help secure the Administrator account in each domain in the forest.
E – Securing Enterprise Admins Groups in Active Directory	Contains guidelines to help secure the Enterprise Admins group in the forest.
F – Securing Domain Admins Groups in Active Directory	Contains guidelines to help secure the Domain Admins group in each domain in the forest.
G – Securing Administrator Groups in Active Directory	Contains guidelines to help secure the Built-in Administrators group in each domain in the forest.
H – Securing Local Administrator Accounts and Groups	Contains guidelines to help secure local Administrator accounts and Administrators groups on domain-joined servers and workstations.
I – Creating Management Accounts for Protected Accounts and Groups in Active Directory	Provides information to create accounts that have limited privileges and can be stringently controlled, but can be used to populate privileged groups in Active Directory when temporary elevation is required.
J – Third-Party RBAC Vendors	Contains a list of third-party RBAC vendors and the RBAC solutions they offer.
K – Third-Party PIM Vendors	Contains a list of third-party PIM vendors and the PIM solutions they offer.
L – Events to Monitor	Lists events for which you should monitor in your environment.
M – Document Links and Recommended Reading	Contains a list of recommended reading. Also contains a list of links to external documents and their URLs so that readers of hard copies of this document can access this information.

Appendix A: Patch and Vulnerability Management Software

The following companies produce patch and vulnerability management software that you can use to help keep third-party applications and non-Windows operating systems up to date if you do not already have a comprehensive patch management plan. This list is not intended to serve as a recommendation, only as reference

material that you can use to devise a patch management methodology for your environment.

Vendor	Offerings
Absolute Software	Absolute Manage, Absolute Manage MDM
SolarWinds	EminentWare WSUS Extension Pack, EminentWare System Center Configuration Manager Extension Pack
GFI Software	GFI LanGuard
Secunia	Secunia Corporate Software Inspector (CSI), Vulnerability Intelligence Manager
eEye Digital Security	Retina CS Management
Lumension	Lumension Vulnerability Management

Appendix B: Privileged Accounts and Groups in Active Directory

“Privileged” accounts and groups in Active Directory are those to which powerful rights, privileges, and permissions are granted that allow them to perform nearly any action in Active Directory and on domain-joined systems. This appendix begins by discussing rights, privileges, and permissions, followed by information about the “highest privilege” accounts and groups in Active Directory,that is, the most powerful accounts and groups.

Information is also provided about built-in and default accounts and groups in Active Directory, in addition to their rights. Although specific configuration recommendations for securing the highest privilege accounts and groups are provided as separate appendices, this appendix provides background information that helps you identify the users and groups you should focus on securing. You should do so because they can be leveraged by attackers to compromise and even destroy your Active Directory installation.

Rights, Privileges, and Permissions in Active Directory

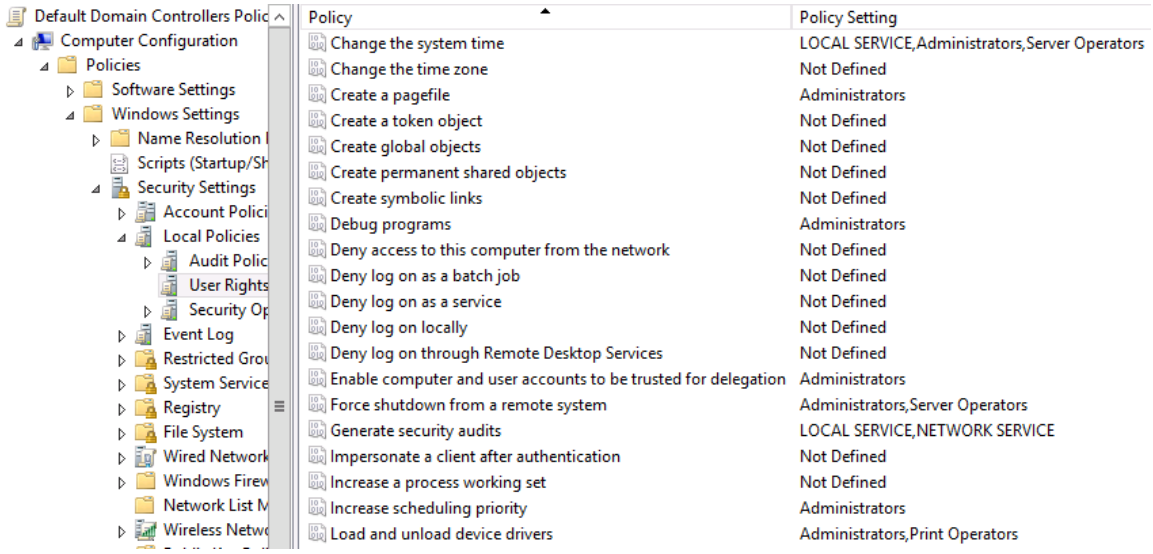
The differences between rights, permissions, and privileges can be confusing and contradictory, even within documentation from Microsoft. This section describes some of the characteristics of each as they are used in this document. These descriptions should not be considered authoritative for other Microsoft documentation, because it may use these terms differently.

Rights and Privileges

Rights and privileges are effectively the same thing—system-wide capabilities that are granted to security principals such as users, services, computers, or groups. In

interfaces typically used by IT professionals, these are usually referred to as “rights” or “user rights,” and they are often assigned by Group Policy Objects. The following screenshot shows some of the most common user rights that can be assigned to security principals (it represents the Default Domain Controllers GPO in a Windows Server 2012 domain). Some of these rights apply to Active Directory, such as the **Enable computer and user accounts to be trusted for delegation** user right, while other rights apply to the Windows operating system, such as **Change the system time**.

User Rights in Active Directory and Windows



In interfaces such as the Group Policy Object Editor, all of these assignable capabilities are referred to broadly as user rights. In reality however, some user rights are programmatically referred to as rights, while others are programmatically referred to as privileges. Table B-1: User Rights and Privileges provides some of the most common assignable user rights and their programmatic constants. Although Group Policy and other interfaces refer to all of these as user rights, some are programmatically identified as rights, while others are defined as privileges.

For more information about each of the user rights listed in the following table, use the links in the table or see Threats and Countermeasures Guide: User Rights in the Threats and Vulnerabilities Mitigation guide for Windows Server 2008 R2 on the Microsoft TechNet site. For information applicable to Windows Server 2008, please see User Rights in the Threats and Vulnerabilities Mitigation documentation on the Microsoft TechNet site. As of the writing of this document, corresponding documentation for Windows Server 2012 is not yet published.

> **Note**
>
> For the purposes of this document, the terms “rights” and “user rights” are used to identify rights and privileges unless otherwise specified.

Table B-1: User Rights and Privileges

User Right in Group Policy	Name of Constant
Access Credential Manager as a trusted caller	SeTrustedCredManAccessPrivilege
Access this computer from the network	SeNetworkLogonRight
Act as part of the operating system	SeTcbPrivilege
Add workstations to domain	SeMachineAccountPrivilege
Adjust memory quotas for a process	SeIncreaseQuotaPrivilege
Allow log on locally	SeInteractiveLogonRight
Allow log on through Remote Desktop Services	SeRemoteInteractiveLogonRight
Back up files and directories	SeBackupPrivilege
Bypass traverse checking	SeChangeNotifyPrivilege
Change the system time	SeSystemtimePrivilege
Change the time zone	SeTimeZonePrivilege
Create a pagefile	SeCreatePagefilePrivilege
Create a token object	SeCreateTokenPrivilege
Create global objects	SeCreateGlobalPrivilege
Create permanent shared objects	SeCreatePermanentPrivilege
Create symbolic links	SeCreateSymbolicLinkPrivilege
Debug programs	SeDebugPrivilege
Deny access to this computer from the network	SeDenyNetworkLogonRight
Deny log on as a batch job	SeDenyBatchLogonRight
Deny log on as a service	SeDenyServiceLogonRight
Deny log on locally	SeDenyInteractiveLogonRight
Deny log on through Remote	SeDenyRemoteInteractiveLogonRight

User Right in Group Policy	Name of Constant
Desktop Services	
Enable computer and user accounts to be trusted for delegation	SeEnableDelegationPrivilege
Force shutdown from a remote system	SeRemoteShutdownPrivilege
Generate security audits	SeAuditPrivilege
Impersonate a client after authentication	SeImpersonatePrivilege
Increase a process working set	SeIncreaseWorkingSetPrivilege
Increase scheduling priority	SeIncreaseBasePriorityPrivilege
Load and unload device drivers	SeLoadDriverPrivilege
Lock pages in memory	SeLockMemoryPrivilege
Log on as a batch job	SeBatchLogonRight
Log on as a service	SeServiceLogonRight
Manage auditing and security log	SeSecurityPrivilege
Modify an object label	SeRelabelPrivilege
Modify firmware environment values	SeSystemEnvironmentPrivilege
Perform volume maintenance tasks	SeManageVolumePrivilege
Profile single process	SeProfileSingleProcessPrivilege
Profile system performance	SeSystemProfilePrivilege
Remove computer from docking station	SeUndockPrivilege
Replace a process level token	SeAssignPrimaryTokenPrivilege
Restore files and directories	SeRestorePrivilege
Shut down the system	SeShutdownPrivilege
Synchronize directory service data	SeSyncAgentPrivilege
Take ownership of files or other objects	SeTakeOwnershipPrivilege

Permissions

Permissions are access controls that are applied to securable objects such as the file system, registry, service, and Active Directory objects. Each securable object has an

associated access control list (ACL), which contains access control entries (ACEs) that grant or deny security principals (users, services, computers, or groups) the ability to perform various operations on the object. For example, the ACLs for many objects in Active Directory contain ACEs that allow Authenticated Users to read general information about the objects, but do not grant them the ability to read sensitive information or to change the objects.

With the exception of each domain's built-in Guest account, every security principal that logs on and is authenticated by a domain controller in an Active Directory forest or a trusted forest has the Authenticated Users Security Identifier (SID) added to its access token by default. Therefore, whether a user, service, or computer account attempts to read general properties on user objects in a domain, the read operation is successful.

If a security principal attempts to access an object for which no ACEs are defined and that contain a SID that is present in the principal's access token, the principal cannot access the object. Moreover, if an ACE in an object's ACL contains a deny entry for a SID that matches the user's access token, the "deny" ACE will generally override a conflicting "allow" ACE. For more information about access control in Windows, see Access Control on the MSDN website.

Within this document, permissions refers to capabilities that are granted or denied to security principals on securable objects. Whenever there is a conflict between a user right and a permission, the user right generally takes precedence. For example, if an object in Active Directory has been configured with an ACL that denies Administrators all read and write access to an object, a user who is a member of the domain's Administrators group will be unable to view much information about the object. However, because the Administrators group is granted the user right "Take ownership of files or other objects," the user can simply take ownership of the object in question, then rewrite the object's ACL to grant Administrators full control of the object.

It is for this reason that this document encourages you to avoid using powerful accounts and groups for day-to-day administration, rather than trying to restrict the capabilities of the accounts and groups. It is not effectively possible to stop a determined user who has access to powerful credentials from using those credentials to gain access to any securable resource.

Built-in Privileged Accounts and Groups

Active Directory is intended to facilitate delegation of administration and the principle of least privilege in assigning rights and permissions. "Regular" users who have accounts in an Active Directory domain are, by default, able to read much of what is stored in the directory, but are able to change only a very limited set of data in the directory. Users who require additional privilege can be granted membership in various privileged groups that are built into the directory so that they may

perform specific tasks related to their roles, but cannot perform tasks that are not relevant to their duties.

Within Active Directory, there are three built-in groups that comprise the highest privilege groups in the directory: the Enterprise Admins (EA) group, the Domain Admins (DA) group, and the built-in Administrators (BA) group.

A fourth group, the Schema Admins (SA) group, has privileges that, if abused, can damage or destroy an entire Active Directory forest, but this group is more restricted in its capabilities than the EA, DA, and BA groups.

In addition to these four groups, there are a number of additional built-in and default accounts and groups in Active Directory, each of which is granted rights and permissions that allow specific administrative tasks to be performed. Although this appendix does not provide a thorough discussion of every built-in or default group in Active Directory, it does provide a table of the groups and accounts that you're most likely to see in your installations.

For example, if you install Microsoft Exchange Server into an Active Directory forest, additional accounts and groups may be created in the Built-in and Users containers in your domains. This appendix describes only the groups and accounts that are created in the Built-in and Users containers in Active Directory, based on native roles and features. Accounts and groups that are created by the installation of enterprise software are not included.

Enterprise Admins

The Enterprise Admins (EA) group is located in the forest root domain, and by default, it is a member of the built-in Administrators group in every domain in the forest. The Built-in Administrator account in the forest root domain is the only default member of the EA group. EAs are granted rights and permissions that allow them to affect forest-wide changes. These are changes that affect all domains in the forest, such as adding or removing domains, establishing forest trusts, or raising forest functional levels. In a properly designed and implemented delegation model, EA membership is required only when first constructing the forest or when making certain forest-wide changes such as establishing an outbound forest trust.

The EA group is located by default in the Users container in the forest root domain, and it is a universal security group, unless the forest root domain is running in Windows 2000 Server mixed mode, in which case the group is a global security group. Although some rights are granted directly to the EA group, many of this group's rights are actually inherited by the EA group because it is a member of the Administrators group in each domain in the forest. Enterprise Admins have no default rights on workstations or member servers.

Domain Admins

Each domain in a forest has its own Domain Admins (DA) group, which is a member of that domain's built-in Administrators (BA) group in addition to a member of the local Administrators group on every computer that is joined to the domain. The only default member of the DA group for a domain is the Built-in Administrator account for that domain.

DAs are all-powerful within their domains, while EAs have forest-wide privilege. In a properly designed and implemented delegation model, DA membership should be required only in "break glass" scenarios, which are situations in which an account with high levels of privilege on every computer in the domain is needed, or when certain domain wide changes must be made. Although native Active Directory delegation mechanisms do allow delegation to the extent that it is possible to use DA accounts only in emergency scenarios, constructing an effective delegation model can be time consuming, and many organizations use third-party applications to expedite the process.

The DA group is a global security group located in the Users container for the domain. There is one DA group for each domain in the forest, and the only default member of a DA group is the domain's Built-in Administrator account. Because a domain's DA group is nested in the domain's BA group and every domain-joined system's local Administrators group, DAs not only have permissions that are specifically granted to Domain Admins, but they also inherit all rights and permissions granted to the domain's Administrators group and the local Administrators group on all systems joined to the domain.

Administrators

The built-in Administrators (BA) group is a domain local group in a domain's Built-in container into which DAs and EAs are nested, and it is this group that is granted many of the direct rights and permissions in the directory and on domain controllers. However, the Administrators group for a domain does not have any privileges on member servers or on workstations. Membership in domain-joined computers' local Administrators group is where local privilege is granted; and of the groups discussed, only DAs are members of all domain-joined computers' local Administrators groups by default.

The Administrators group is a domain-local group in the domain's Built-in container. By default, every domain's BA group contains the local domain's Built-in Administrator account, the local domain's DA group, and the forest root domain's EA group. Many user rights in Active Directory and on domain controllers are granted specifically to the Administrators group, not to EAs or DAs. A domain's BA group is granted full control permissions on most directory objects, and can take ownership of directory objects. Although EA and DA groups are granted certain object-specific permissions in the forest and domains, much of the power of groups is actually "inherited" from their membership in BA groups.

> **Note**
>
> Although these are the default configurations of these privileged groups, a member of any one of the three groups can manipulate the directory to gain membership in any of the other groups. In some cases, it is trivial to achieve, while in others it is more difficult, but from the perspective of potential privilege, all three groups should be considered effectively equivalent.

Schema Admins

The Schema Admins (SA) group is a universal group in the forest root domain and has only that domain's Built-in Administrator account as a default member, similar to the EA group. Although membership in the SA group can allow an attacker to compromise the Active Directory schema, which is the framework for the entire Active Directory forest, SAs have few default rights and permissions beyond the schema.

You should carefully manage and monitor membership in the SA group, but in some respects, this group is "less privileged" than the three highest privileged groups described earlier because the scope of its privilege is very narrow; that is, SAs have no administrative rights anywhere other than the schema.

Additional Built-in and Default Groups in Active Directory

To facilitate delegating administration in the directory, Active Directory ships with various built-in and default groups that have been granted specific rights and permissions. These groups are described briefly in the following table.

The following table lists the built-in and default groups in Active Directory. Both sets of groups exist by default; however, built-in groups are located (by default) in the Built-in container in Active Directory, while default groups are located (by default) in the Users container in Active Directory. Groups in the Built-in container are all Domain Local groups, while groups in the Users container are a mixture of Domain Local, Global, and Universal groups, in addition to three individual user accounts (Administrator, Guest, and Krbtgt).

In addition to the highest privileged groups described earlier in this appendix, some built-in and default accounts and groups are granted elevated privileges and should also be protected and used only on secure administrative hosts. These groups and accounts can be found in the shaded rows in Table B-1: Built-in and Default Groups and Accounts in Active Directory. Because some of these groups and accounts are granted rights and permissions that can be misused to compromise Active Directory or domain controllers, they are afforded additional protections as described in Appendix C: Protected Accounts and Groups in Active Directory.

Table B-1: Built-in and Default Accounts and Groups in Active Directory

Account or Group	Default Container, Group Scope and Type	Description and Default User Rights
Access Control Assistance Operators (Active Directory in Windows Server 2012)	Built-in container Domain-local security group	Members of this group can remotely query authorization attributes and permissions for resources on this computer. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Account Operators	Built-in container Domain-local security group	Members can administer domain user and group accounts. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set

Account or Group	Default Container, Group Scope and Type	Description and Default User Rights
Administrator account	Users container Not a group	Built-in account for administering the domain. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Adjust memory quotas for a process Allow log on locally Allow log on through Remote Desktop Services Back up files and directories Bypass traverse checking Change the system time Change the time zone Create a pagefile Create global objects Create symbolic links Debug programs Enable computer and user accounts to be trusted for delegation Force shutdown from a remote system Impersonate a client after authentication Increase a process working set Increase scheduling priority Load and unload device drivers Log on as a batch job Manage auditing and security log Modify firmware environment values Perform volume maintenance tasks Profile single process Profile system performance Remove computer from docking station Restore files and directories Shut down the system Take ownership of files or other objects

Account or Group	Default Container, Group Scope and Type	Description and Default User Rights
Administrators group	Built-in container Domain-local security group	Administrators have complete and unrestricted access to the domain. **Direct user rights**: Access this computer from the network Adjust memory quotas for a process Allow log on locally Allow log on through Remote Desktop Services Back up files and directories Bypass traverse checking Change the system time Change the time zone Create a pagefile Create global objects Create symbolic links Debug programs Enable computer and user accounts to be trusted for delegation Force shutdown from a remote system Impersonate a client after authentication Increase scheduling priority Load and unload device drivers Log on as a batch job Manage auditing and security log Modify firmware environment values Perform volume maintenance tasks Profile single process Profile system performance Remove computer from docking station Restore files and directories Shut down the system Take ownership of files or other objects **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Allowed RODC Password Replication Group	Users container Domain-local security group	Members in this group can have their passwords replicated to all read-only domain controllers in the domain. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set

Account or Group	Default Container, Group Scope and Type	Description and Default User Rights
Backup Operators	Built-in container Domain-local security group	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files. **Direct user rights:** Allow log on locally Back up files and directories Log on as a batch job Restore files and directories Shut down the system **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Cert Publishers	Users container Domain-local security group	Members of this group are permitted to publish certificates to the directory. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Certificate Service DCOM Access	Built-in container Domain-local security group	If Certificate Services is installed on a domain controller (not recommended), this group grants DCOM enrollment access to Domain Users and Domain Computers. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Cloneable Domain Controllers (AD DS in Windows Server 2012A D DS)	Users container Global security group	Members of this group that are domain controllers may be cloned. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set

Account or Group	Default Container, Group Scope and Type	Description and Default User Rights
Cryptographic Operators	Built-in container Domain-local security group	Members are authorized to perform cryptographic operations. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Debugger Users	This is neither a default nor a built-in group, but when present in AD DS, is cause for further investigation.	The presence of a Debugger Users group indicates that debugging tools have been installed on the system at some point, whether via Visual Studio, SQL, Office, or other applications that require and support a debugging environment. This group allows remote debugging access to computers. When this group exists at the domain level, it indicates that a debugger or an application that contains a debugger has been installed on a domain controller.
Denied RODC Password Replication Group	Users container Domain-local security group	Members in this group cannot have their passwords replicated to any read-only domain controllers in the domain. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
DHCP Administrators	Users container Domain-local security group	Members of this group have administrative access to the DHCP Server service. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
DHCP Users	Users container Domain-local security group	Members of this group have view-only access to the DHCP Server service. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set

Account or Group	Default Container, Group Scope and Type	Description and Default User Rights
Distributed COM Users	Built-in container Domain-local security group	Members of this group are allowed to launch, activate, and use distributed COM objects on this computer. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
DnsAdmins	Users container Domain-local security group	Members of this group have administrative access to the DNS Server service. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
DnsUpdateProxy	Users container Global security group	Members of this group are DNS clients who are permitted to perform dynamic updates on behalf of clients that cannot themselves perform dynamic updates. Members of this group are typically DHCP servers. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set

Account or Group	Default Container, Group Scope and Type	Description and Default User Rights
Domain Admins	Users container Global security group	Designated administrators of the domain; Domain Admins is a member of every domain-joined computer's local Administrators group and receives rights and permissions granted to the local Administrators group, in addition to the domain's Administrators group. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Adjust memory quotas for a process Allow log on locally Allow log on through Remote Desktop Services Back up files and directories Bypass traverse checking Change the system time Change the time zone Create a pagefile Create global objects Create symbolic links Debug programs Enable computer and user accounts to be trusted for delegation Force shutdown from a remote system Impersonate a client after authentication Increase a process working set Increase scheduling priority Load and unload device drivers Log on as a batch job Manage auditing and security log Modify firmware environment values Perform volume maintenance tasks Profile single process Profile system performance Remove computer from docking station Restore files and directories Shut down the system Take ownership of files or other objects

Account or Group	Default Container, Group Scope and Type	Description and Default User Rights
Domain Computers	Users container Global security group	All workstations and servers that are joined to the domain are by default members of this group. **Default direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Domain Controllers	Users container Global security group	All domain controllers in the domain. Note: Domain controllers are not a member of the Domain Computers group. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Domain Guests	Users container Global security group	All guests in the domain **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Domain Users	Users container Global security group	All users in the domain **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set

Account or Group	Default Container, Group Scope and Type	Description and Default User Rights
Enterprise Admins (exists only in forest root domain)	Users container Universal security group	Enterprise Admins have permissions to change forest-wide configuration settings; Enterprise Admins is a member of every domain's Administrators group and receives rights and permissions granted to that group. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Adjust memory quotas for a process Allow log on locally Allow log on through Remote Desktop Services Back up files and directories Bypass traverse checking Change the system time Change the time zone Create a pagefile Create global objects Create symbolic links Debug programs Enable computer and user accounts to be trusted for delegation Force shutdown from a remote system Impersonate a client after authentication Increase a process working set Increase scheduling priority Load and unload device drivers Log on as a batch job Manage auditing and security log Modify firmware environment values Perform volume maintenance tasks Profile single process Profile system performance Remove computer from docking station Restore files and directories Shut down the system Take ownership of files or other objects

Account or Group	Default Container, Group Scope and Type	Description and Default User Rights
Enterprise Read-only Domain Controllers	Users container Universal security group	This group contains the accounts for all read-only domain controllers in the forest. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Event Log Readers	Built-in container Domain-local security group	Members of this group in can read the event logs on domain controllers. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Group Policy Creator Owners	Users container Global security group	Members of this group can create and modify Group Policy Objects in the domain. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Guest	Users container Not a group	This is the only account in an AD DS domain that does not have the Authenticated Users SID added to its access token. Therefore, any resources that are configured to grant access to the Authenticated Users group will not be accessible to this account. This behavior is not true of members of the Domain Guests and Guests groups, however- members of those groups *do* have the Authenticated Users SID added to their access tokens. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Bypass traverse checking Increase a process working set

Account or Group	Default Container, Group Scope and Type	Description and Default User Rights
Guests	Built-in container Domain-local security group	Guests have the same access as members of the Users group by default, except for the Guest account, which is further restricted as described earlier. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Hyper-V Administrators (Windows Server 2012)	Built-in container Domain-local security group	Members of this group have complete and unrestricted access to all features of Hyper-V. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
IIS_IUSRS	Built-in container Domain-local security group	Built-in group used by Internet Information Services. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Incoming Forest Trust Builders (exists only in forest root domain)	Built-in container Domain-local security group	Members of this group can create incoming, one-way trusts to this forest. (Creation of outbound forest trusts is reserved for Enterprise Admins.) **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Krbtgt	Users container Not a group	The Krbtgt account is the service account for the Kerberos Key Distribution Center in the domain. This account has access to all accounts' credentials stored in Active Directory. This account is disabled by default and should never be enabled **User rights:** N/A

Account or Group	Default Container, Group Scope and Type	Description and Default User Rights
Network Configuration Operators	Built-in container Domain-local security group	Members of this group are granted privileges that allow them to manage configuration of networking features. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Performance Log Users	Built-in container Domain-local security group	Members of this group can schedule logging of performance counters, enable trace providers, and collect event traces locally and via remote access to the computer. **Direct user rights:** Log on as a batch job **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Performance Monitor Users	Built-in container Domain-local security group	Members of this group can access performance counter data locally and remotely. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Pre-Windows 2000 Compatible Access	Built-in container Domain-local security group	This group exists for backward compatibility with operating systems prior to Windows 2000 Server, and it provides the ability for members to read user and group information in the domain. **Direct user rights:** Access this computer from the network Bypass traverse checking **Inherited user rights:** Add workstations to domain Increase a process working set

Account or Group	Default Container, Group Scope and Type	Description and Default User Rights
Print Operators	Built-in container Domain-local security group	Members of this group can administer domain printers. **Direct user rights:** Allow log on locally Load and unload device drivers Shut down the system **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
RAS and IAS Servers	Users container Domain-local security group	Servers in this group can read remote access properties on user accounts in the domain. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
RDS Endpoint Servers (Windows Server 2012)	Built-in container Domain-local security group	Servers in this group run virtual machines and host sessions where users RemoteApp programs and personal virtual desktops run. This group needs to be populated on servers running RD Connection Broker. RD Session Host servers and RD Virtualization Host servers used in the deployment need to be in this group. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set

Account or Group	Default Container, Group Scope and Type	Description and Default User Rights
RDS Management Servers (Windows Server 2012)	Built-in container Domain-local security group	Servers in this group can perform routine administrative actions on servers running Remote Desktop Services. This group needs to be populated on all servers in a Remote Desktop Services deployment. The servers running the RDS Central Management service must be included in this group. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
RDS Remote Access Servers (Windows Server 2012)	Built-in container Domain-local security group	Servers in this group enable users of RemoteApp programs and personal virtual desktops access to these resources. In Internet-facing deployments, these servers are typically deployed in an edge network. This group needs to be populated on servers running RD Connection Broker. RD Gateway servers and RD Web Access servers used in the deployment need to be in this group. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Read-only Domain Controllers	Users container Global security group	This group contains all read-only domain controllers in the domain. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Remote Desktop Services Users	Built-in container Domain-local security group	Members of this group are granted the right to log on remotely using RDP. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set

Account or Group	Default Container, Group Scope and Type	Description and Default User Rights
Remote Management Servers (Windows Server 2012)	Built-in container Domain-local security group	Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to WMI namespaces that grant access to the user. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Replicator	Built-in container Domain-local security group	Supports legacy file replication in a domain. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Schema Admins (exists only in forest root domain)	Users container Universal security group	Schema admins are the only users who can make modifications to the Active Directory schema, and only if the schema is write-enabled. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Server Operators	Built-in container Domain-local security group	Members of this group can administer domain servers. **Direct user rights:** Allow log on locally Back up files and directories Change the system time Change the time zone Force shutdown from a remote system Restore files and directories Shut down the system **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set

Account or Group	Default Container, Group Scope and Type	Description and Default User Rights
Terminal Server License Servers	Built-in container Domain-local security group	Members of this group can update user accounts in Active Directory with information about license issuance, for the purpose of tracking and reporting TS Per User CAL usage **Default direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
Users	Built-in container Domain-local security group	Users have permissions that allow them to read many objects and attributes in Active Directory, although they cannot change most. Users are prevented from making accidental or intentional system-wide changes and can run most applications. **Direct user rights:** Increase a process working set **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking
Windows Authorization Access Group	Built-in container Domain-local security group	Members of this group have access to the computed tokenGroupsGlobalAndUniversal attribute on User objects **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set
WinRMRemote WMIUsers_ (Windows Server 2012)	Users container Domain-local security group	Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to WMI namespaces that grant access to the user. **Direct user rights:** None **Inherited user rights:** Access this computer from the network Add workstations to domain Bypass traverse checking Increase a process working set

Within Active Directory, a default set of highly privileged accounts and groups are considered protected accounts and groups. With most objects in Active Directory, delegated administrators (users who have been delegated permissions to manage Active Directory objects) can change permissions on the objects, including changing permissions to allow themselves to change memberships of the groups, for example.

However, with protected accounts and groups, the objects' permissions are set and enforced via an automatic process that ensures the permissions on the objects remains consistent even if the objects are moved the directory. Even if somebody manually changes a protected object's permissions, this process ensures that permissions are returned to their defaults quickly.

Protected Groups

The following table contains the protected groups in Active Directory listed by domain controller operating system.

Protected Accounts and Groups in Active Directory by Operating System

Windows 2000 <SP4	Windows 2000 SP4 – Windows Server 2003 RTM	Windows Server 2003 SP1+	Windows Server 2012, Windows Server 2008 R2, Windows Server 2008
Administrators	Account Operators	Account Operators	Account Operators
	Administrator	Administrator	Administrator
	Administrators	Administrators	Administrators
	Backup Operators	Backup Operators	Backup Operators
	Cert Publishers		
Domain Admins	Domain Admins	Domain Admins	Domain Admins
	Domain Controllers	Domain Controllers	Domain Controllers
Enterprise Admins	Enterprise Admins	Enterprise Admins	Enterprise Admins
	Krbtgt	Krbtgt	Krbtgt
	Print Operators	Print Operators	Print Operators
			Read-only Domain Controllers
	Replicator	Replicator	Replicator
Schema Admins	Schema Admins	Schema Admins	Schema Admins
	Server Operators	Server Operators	Server Operators

AdminSDHolder

The purpose of the AdminSDHolder object is to provide "template" permissions for the protected accounts and groups in the domain. AdminSDHolder is automatically

created as an object in the System container of every Active Directory domain. Its path is:
CN=AdminSDHolder,CN=System,DC=<domain_component>,DC=<domain_component>….

Unlike most objects in the Active Directory domain, which are owned by the Administrators group, AdminSDHolder is owned by the Domain Admins group. By default, EAs can make changes to any domain's AdminSDHolder object, as can the domain's Domain Admins and Administrators groups. Additionally, although the default owner of AdminSDHolder is the domain's Domain Admins group, members of Administrators or Enterprise Admins can take ownership of the object.

SDProp

SDProp is a process that runs every 60 minutes (by default) on the domain controller that holds the domain's PDC Emulator (PDCE). SDProp compares the permissions on the domain's AdminSDHolder object with the permissions on the protected accounts and groups in the domain. If the permissions on any of the protected accounts and groups do not match the permissions on the AdminSDHolder object, the permissions on the protected accounts and groups are reset to match those of the domain's AdminSDHolder object.

Additionally, permissions inheritance is disabled on protected groups and accounts, which means that even if the accounts and groups are moved to different locations in the directory, they do not inherit permissions from their new parent objects. Inheritance is disabled on the AdminSDHolder object so that permission changes to the parent objects do not change the permissions of AdminSDHolder.

Changing SDProp Interval

Normally, you should not need to change the interval at which SDProp runs, except for testing purposes. If you need to change the SDProp interval, on the PDCE for the domain, use regedit to add or modify the AdminSDProtectFrequency DWORD value in HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters.

The range of values is in seconds from 60 to 7200 (one minute to two hours). To reverse the changes, delete AdminSDProtectFrequency key, which will cause SDProp to revert back to the 60 minute interval. You generally should not reduce this interval in production domains as it can increase LSASS processing overhead on the domain controller. The impact of this increase is dependent on the number of protected objects in the domain.

Running SDProp Manually

A better approach to testing AdminSDHolder changes is to run SDProp manually, which causes the task to run immediately but does not affect scheduled execution. Running SDProp manually is performed slightly differently on domain controllers running Windows Server 2008 and earlier than it is on domain controllers running Windows Server 2012 or Windows Server 2008 R2.

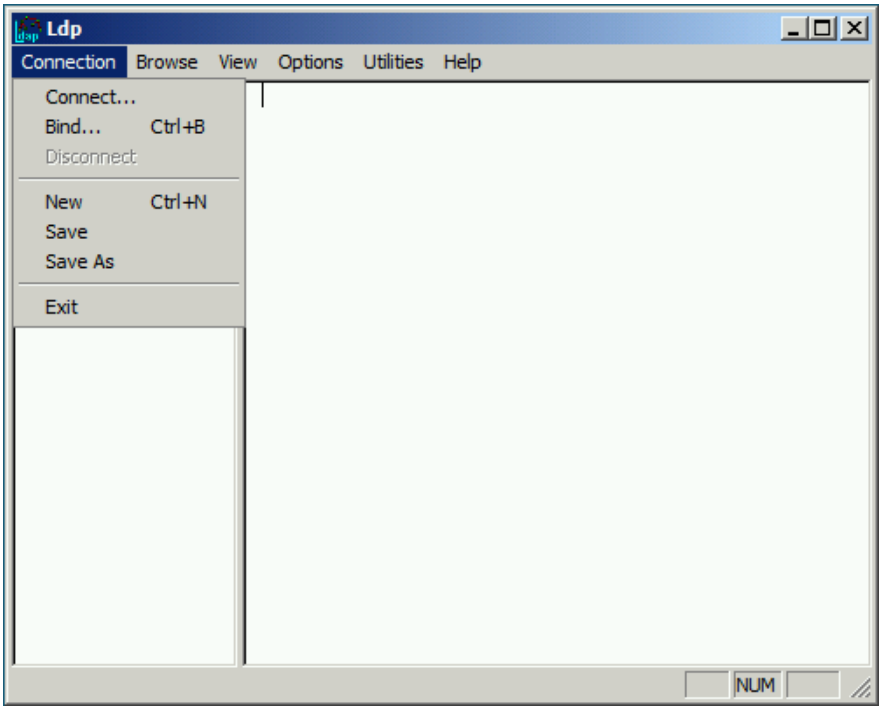
Procedures for running SDProp manually on older operating systems are provided in Microsoft Support article 251343, and following are step-by-step instructions for older and newer operating systems. In either case, you must connect to the rootDSE object in Active Directory and perform a modify operation with a null DN for the

rootDSE object, specifying the name of the operation as the attribute to modify. For more information about modifiable operations on the rootDSE object, see rootDSE Modify Operations on the MSDN website.

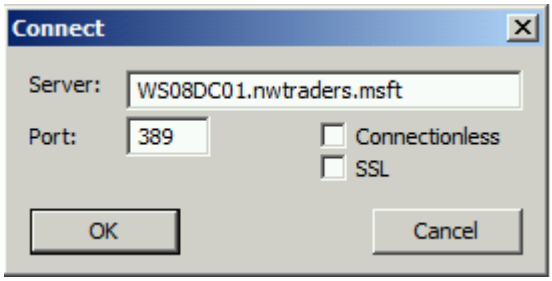
Running SDProp Manually in Windows Server 2008 or Earlier

You can force SDProp to run by using Ldp.exe or by running an LDAP modification script. To run SDProp using Ldp.exe, perform the following steps after you have made changes to the AdminSDHolder object in a domain:

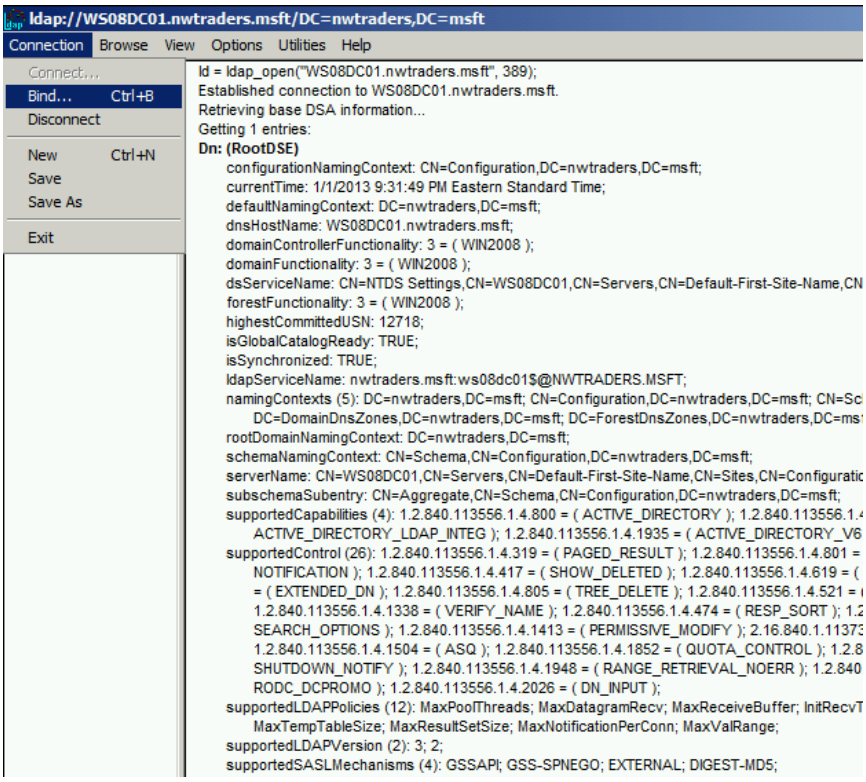
1. Launch **Ldp**.exe.
2. Click **Connection** on the Ldp dialog box, and click **Connect…**.



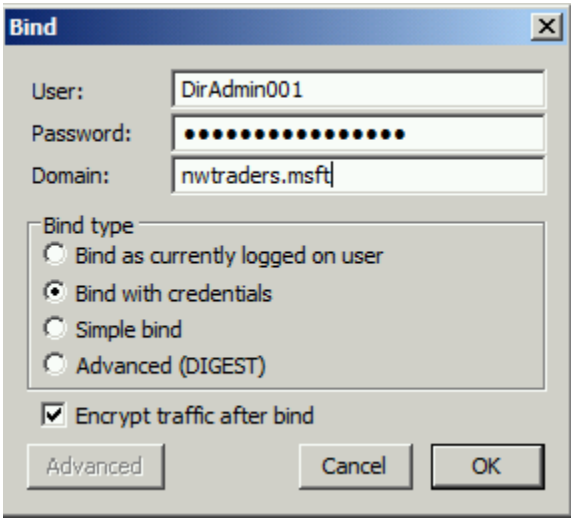
3. In the **Connect** dialog box, type the name of the domain controller for the domain that holds the PDC Emulator (PDCE) role and click **OK**.



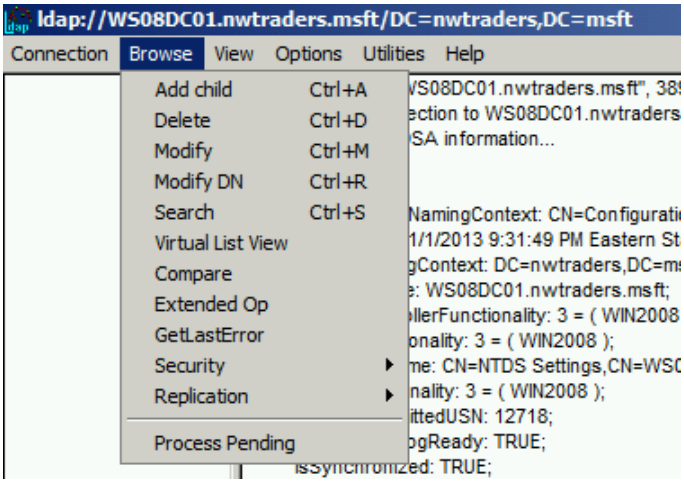
4. Verify that you have connected successfully, as indicated by **Dn: (RootDSE)** in the following screenshot, click **Connection** and click **Bind**.



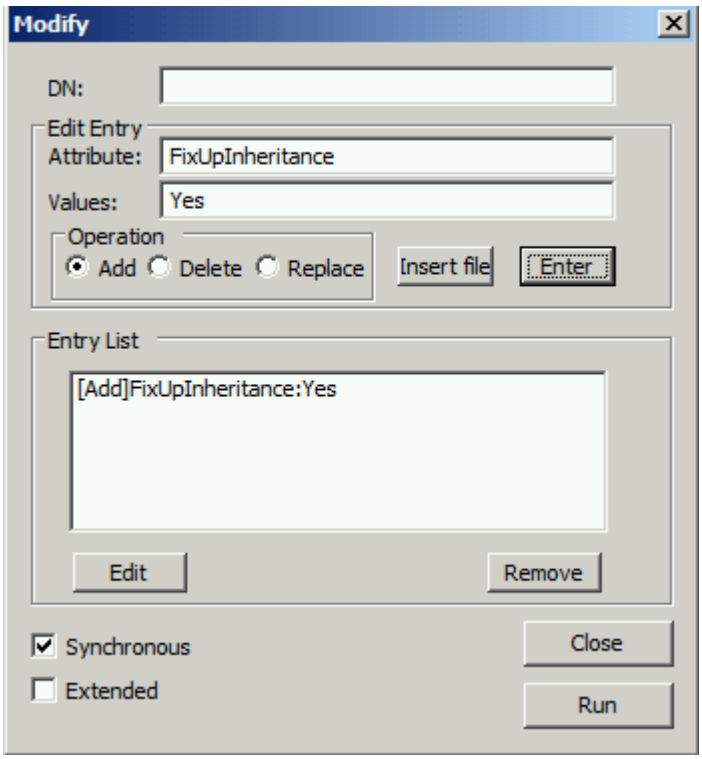
5. In the **Bind** dialog box, type the credentials of a user account that has permission to modify the rootDSE object. (If you are logged on as that user, you can select **Bind as currently logged on user**.) Click **OK**.



6. After you have completed the bind operation, click **Browse**, and click **Modify**.



7. In the **Modify** dialog box, leave the **DN** field blank. In the **Edit Entry Attribute** field, type **FixUpInheritance**, and in the **Values** field, type **Yes.** Click **Enter** to populate the **Entry List** as shown in the following screenshot.



8. In the populated **Modify** dialog box, click **Run**, and verify that the changes you made to the AdminSDHolder object have appeared on that object.

> **Note**
>
> For information about modifying AdminSDHolder to allow designated unprivileged accounts to modify the membership of protected groups, see Appendix I: Creating Management Accounts for Protected Accounts and Groups in Active Directory.

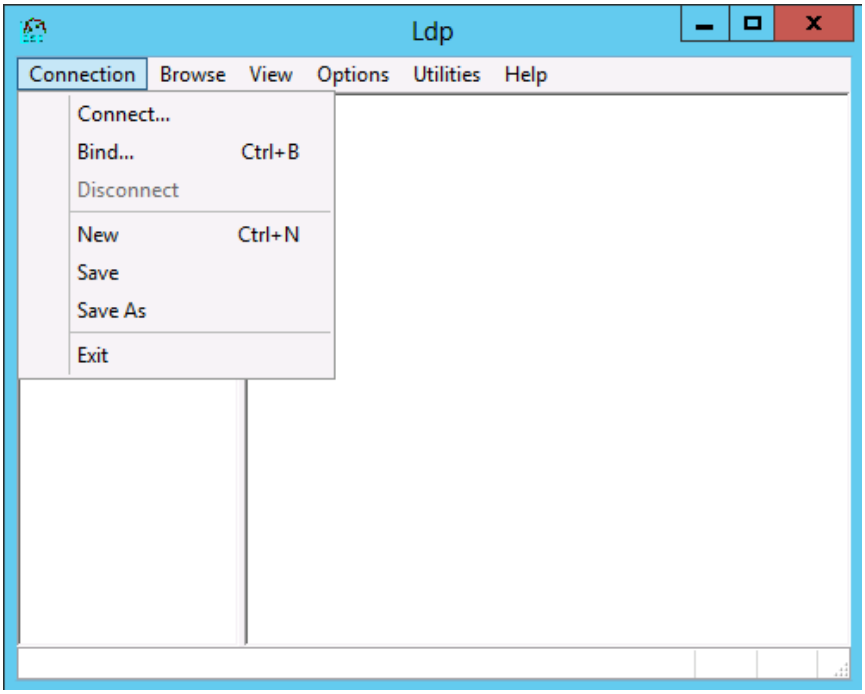
If you prefer to run SDProp manually via LDIFDE or a script, you can create a modify entry as shown here:

```
dn:
changetype: modify
add: FixUpInheritance
FixUpInheritance: yes
```

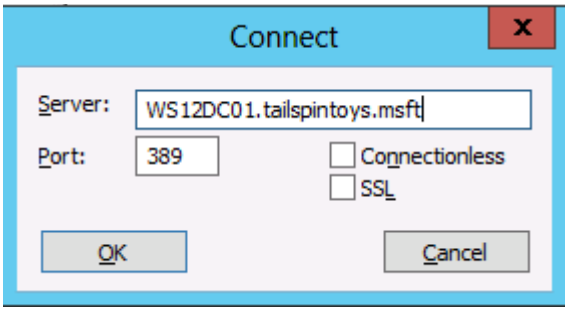
Running SDProp Manually in Windows Server 2012 or Windows Server 2008 R2

You can also force SDProp to run by using Ldp.exe or by running an LDAP modification script. To run SDProp using Ldp.exe, perform the following steps after you have made changes to the AdminSDHolder object in a domain:

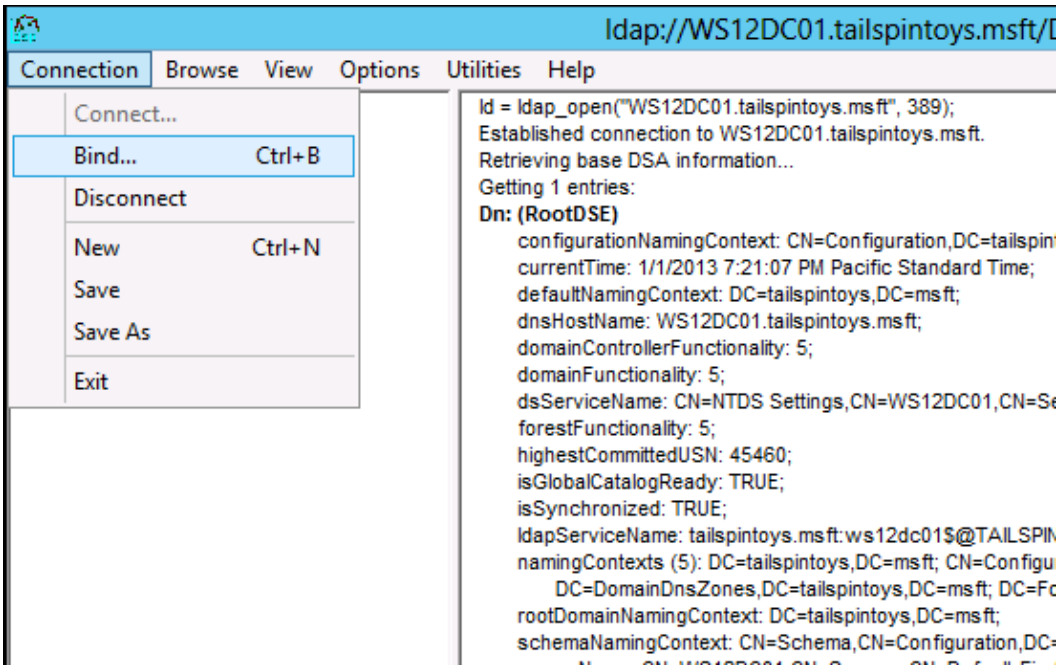
1. Launch **Ldp**.exe.
2. In the **Ldp** dialog box, click **Connection**, and click **Connect…**.



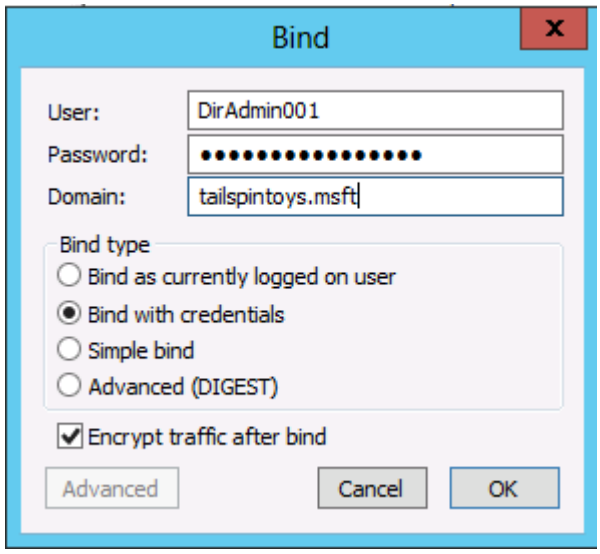
3. In the **Connect** dialog box, type the name of the domain controller for the domain that holds the PDC Emulator (PDCE) role and click **OK**.



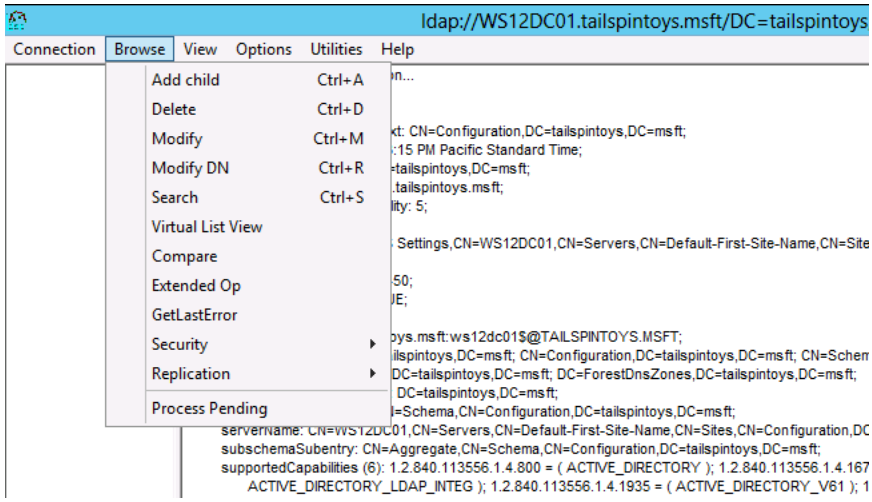
4. Verify that you have connected successfully, as indicated by **Dn: (RootDSE)** in the following screenshot, click **Connection** and click **Bind**.



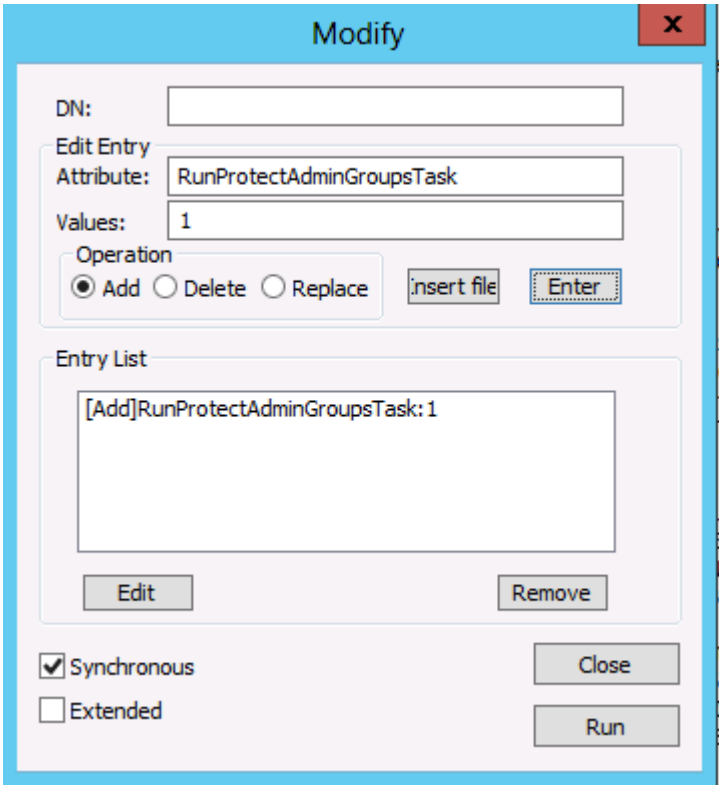
5. In the **Bind** dialog box, type the credentials of a user account that has permission to modify the rootDSE object. (If you are logged on as that user, you can select **Bind as currently logged on user**.) Click **OK**.



6. After you have completed the bind operation, click **Browse**, and click **Modify**.



7. In the **Modify** dialog box, leave the **DN** field blank. In the **Edit Entry Attribute** field, type **RunProtectAdminGroupsTask**, and in the **Values** field, type **1**. Click **Enter** to populate the entry list as shown here.



8. In the populated **Modify** dialog box, click **Run**, and verify that the changes you made to the AdminSDHolder object have appeared on that object.

If you prefer to run SDProp manually via LDIFDE or a script, you can create a modify entry as shown here:

```
dn:
changetype: modify
add: runProtectAdminGroupsTask
runProtectAdminGroupsTask: 1
```

In each domain in Active Directory, an Administrator account is created as part of the creation of the domain. This account is by default a member of the Domain Admins and Administrators groups in the domain, and if the domain is the forest root domain, the account is also a member of the Enterprise Admins group.

Use of a domain's Administrator account should be reserved only for initial build activities, and possibly, disaster-recovery scenarios. To ensure that an Administrator account can be used to effect repairs in the event that no other accounts can be used, you should not change the default membership of the Administrator account in any domain in the forest. Instead, you should secure the Administrator account in each domain in the forest as described in the following section and detailed in the step-by-step instructions that follow. For more information about each of the controls listed here, please see Securing Built-in Administrator Accounts in Active Directory in this document.

Controls for Built-in Administrator Accounts

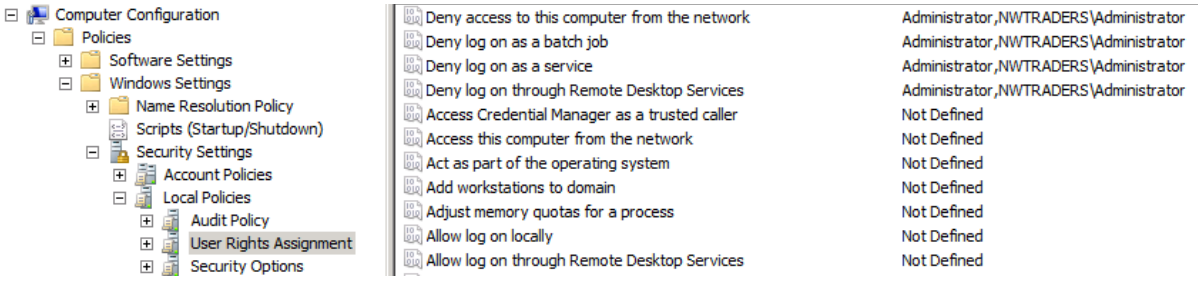
For the built-in Administrator account in each domain in your forest, you should configure the following settings:

- Enable the **Account is sensitive and cannot be delegated** flag on the account.
- Enable the **Smart card is required for interactive logon** flag on the account.
- Disable the account.
- Configure GPOs to restrict the Administrator account's use on domain-joined systems:
    - In one or more GPOs that you create and link to workstation and member server OUs in each domain, add each domain's Administrator account to the following user rights in **Computer Configuration\Policies\Windows Settings\Security Settings\Local Settings\User Rights Assignments**:
        - Deny access to this computer from the network
        - Deny log on as a batch job
        - Deny log on as a service
        - Deny log on through Remote Desktop Services

> **Note**
>
> When you add accounts to this setting, you must specify whether you are configuring local Administrator accounts or domain Administrator accounts. For example, to add the NWTRADERS domain's Administrator account to these deny rights, you must type the account as NWTRADERS\Administrator, or browse to the Administrator account for the NWTRADERS domain. If you type "Administrator" in these user rights settings in the Group Policy Object Editor,

you will restrict the local Administrator account on each computer to which the GPO is applied.

We recommend restricting local Administrator accounts on member servers and workstations in the same manner as domain-based Administrator accounts. Therefore you should generally add the Administrator account for each domain in the forest and the Administrator account for the local computers to these user rights settings. The following screenshot shows an example of configuring these user rights to block local Administrator accounts and a domain's Administrator account from performing logons that should not be needed for these accounts.



- Configure GPOs to restrict Administrator accounts on domain controllers
    - In each domain in the forest, the Default Domain Controllers GPO or a policy linked to the domain controllers OU should be modified to add each domain's Administrator account to the following user rights in **Computer Configuration\Policies\Windows Settings\Security Settings\Local Settings\User Rights Assignments**:
        - Deny access to this computer from the network
        - Deny log on as a batch job
        - Deny log on as a service
        - Deny log on through Remote Desktop Services

Note

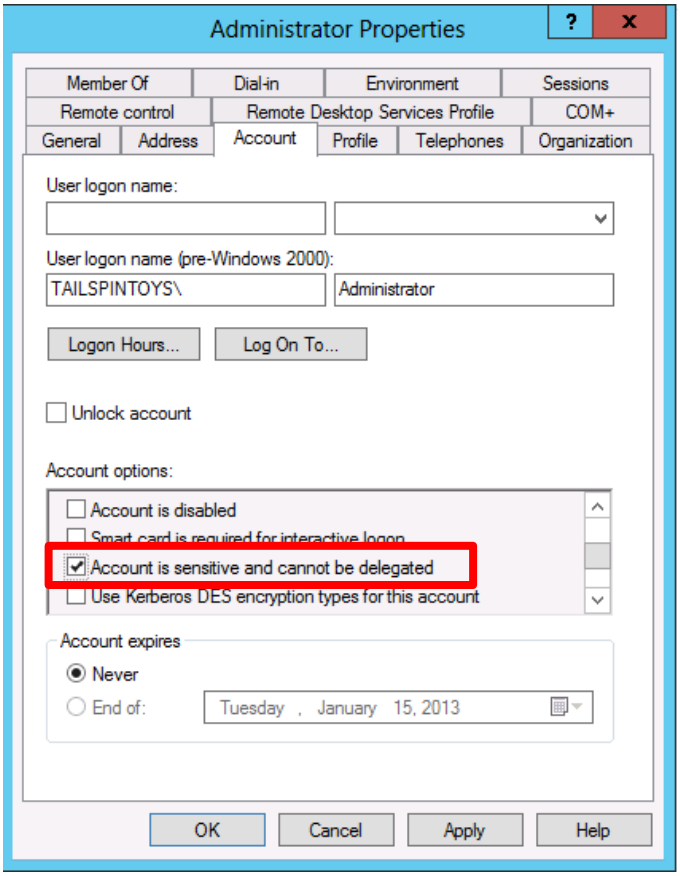
These settings will ensure that the domain's built-in Administrator account cannot be used to connect to a domain controller, although the account, if enabled, can log on locally to domain controllers. Because this account should only be enabled and used in disaster-recovery scenarios, it is anticipated that physical access to at least one domain controller will be available, or that other accounts with permissions to access domain controllers remotely can be used.

- Configure Auditing of Administrator Accounts

  When you have secured each domain's Administrator account and disabled it, you should configure auditing to monitor for changes to the account. If the account is enabled, its password is reset, or any other modifications are made to the account, alerts should be sent to the users or teams responsible for administration of Active Directory, in addition to incident response teams in your organization.

Step-by-Step Instructions to Secure Built-in Administrator Accounts in Active Directory

1. In **Server Manager**, click **Tools**, and click **Active Directory Users and Computers**.
2. To prevent attacks that leverage delegation to use the account's credentials on other systems, perform the following steps:
   a. Right-click the **Administrator** account and click **Properties**.
   b. Click the **Account** tab.
   c. Under **Account options**, select **Account is sensitive and cannot be delegated** flag as indicated in the following screenshot, and click **OK**.

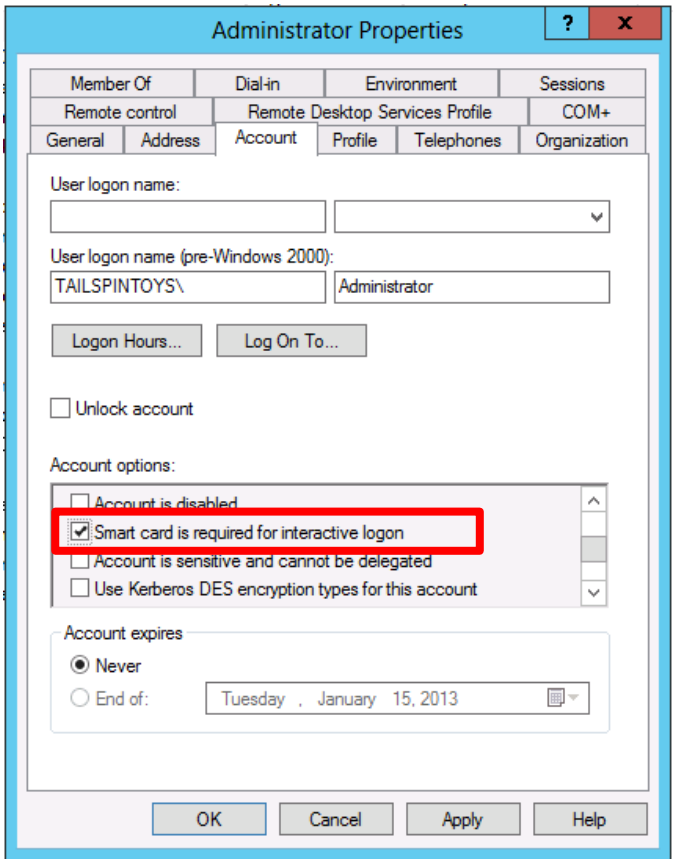


3. To enable the **Smart card is required for interactive logon** flag on the account, perform the following steps:

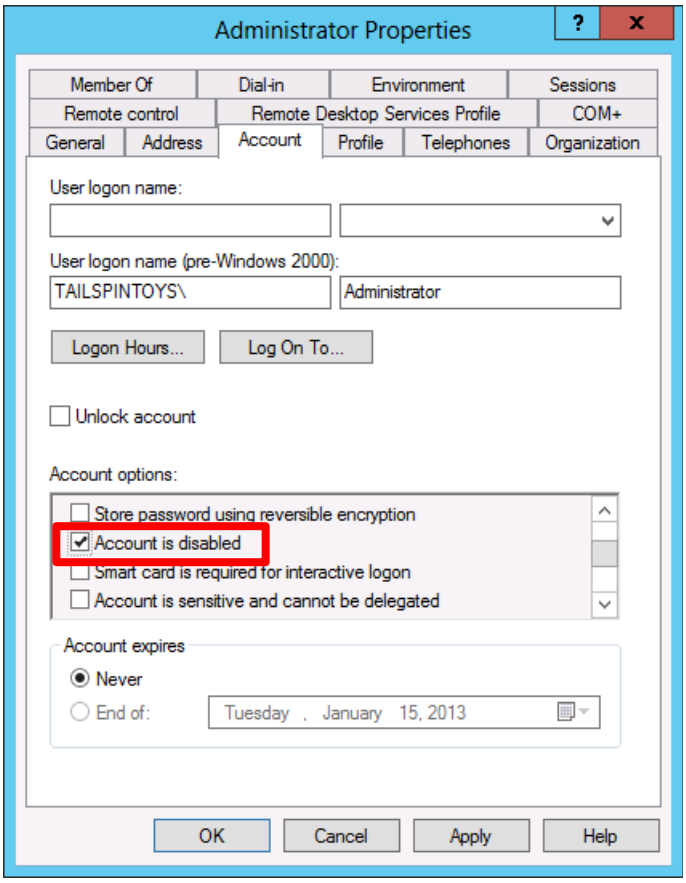
a. Right-click the **Administrator** account and select **Properties**.

b. Click the **Account** tab.

c. Under **Account options**, select the **Smart card is required for interactive logon** flag as indicated in the following screenshot, and click **OK**.



4. To disable the account, perform the following steps:
   a. Right-click the **Administrator** account and click **Properties**.
   b. Click the **Account** tab.
   c. In the **Account options** field, select the **Account is disabled** flag as indicated in the following screenshot, and click **OK**.

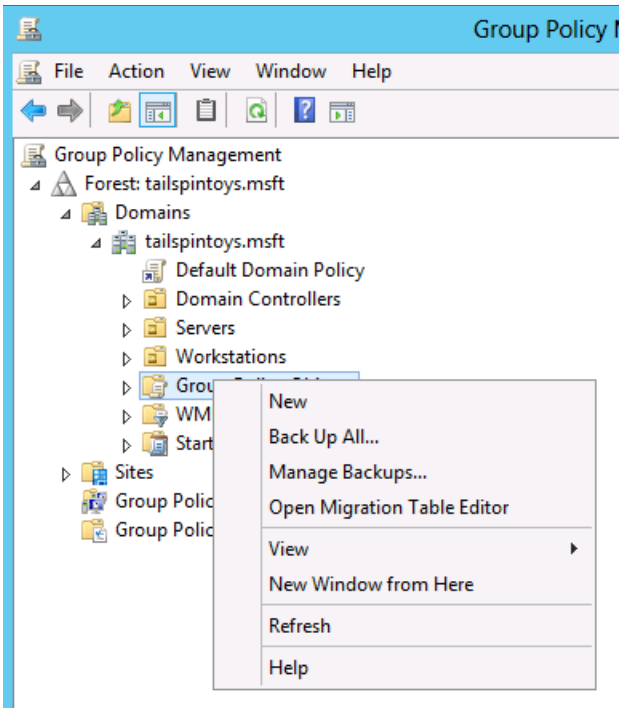


Configuring GPOs to Restrict Administrator Accounts at the Domain-Level

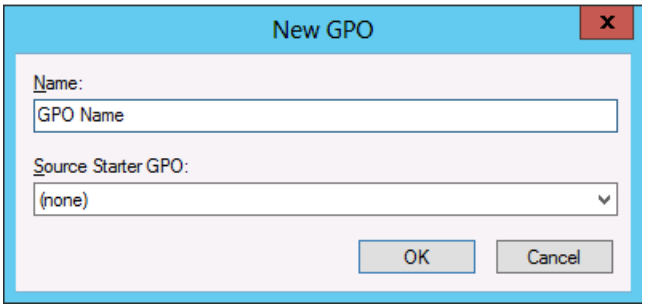
> **Warning**
>
> This GPO should never be linked at the domain-level because it can make the built-in Administrator account unusable, even in disaster recovery scenarios.

1. In **Server Manager**, click **Tools**, and click **Group Policy Management**.
2. In the console tree, expand <Forest>\Domains\<Domain>, and then **Group Policy Objects** (where <Forest> is the name of the forest and <Domain> is the name of the domain where you want to create the Group Policy).

3. In the console tree, right-click **Group Policy Objects**, and click **New**.

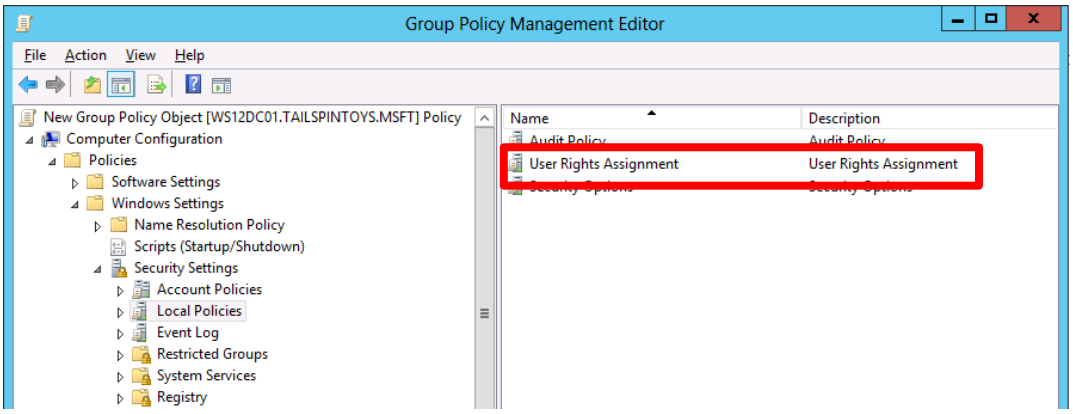


4. In the **New GPO** dialog box, type <GPO Name>, and click **OK** (where <GPO Name> is the name of this GPO) as indicated in the following screenshot.



5. In the details pane, right-click <GPO Name>, and click **Edit**.

6. Navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies**, and click **User Rights Assignment**.

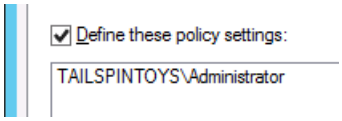


7. Configure the user rights to prevent the Administrator account from accessing members servers and workstations over the network by doing the following:

   a. Double-click **Deny access to this computer from the network** and select **Define these policy settings**.

   b. Click **Add User or Group…** and click **Browse …**.

   c. Type **Administrator**, click **Check Names**, and click **OK**. Verify that the account is displayed in <DomainName>\Username format as indicated in the following screenshot.



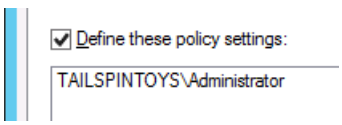
   d. Click **OK**, and **OK** again.

8. Configure the user rights to prevent the Administrator account from logging on as a batch job by doing the following:

   a. Double-click **Deny log on as a batch job** and select **Define these policy settings**.

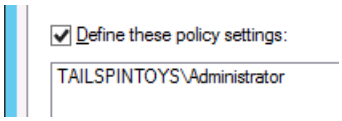
   b. Click **Add User or Group…** and click **Browse …**.

   c. Type **Administrator**, click **Check Names**, and click **OK**. Verify that the account is displayed in <DomainName>\Username format as indicated in the following screenshot.

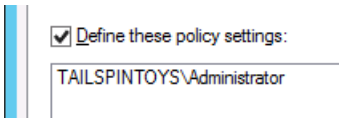


   d. Click **OK**, and **OK** again.

9. Configure the user rights to prevent the Administrator account from logging on as a service by doing the following:
   a. Double-click **Deny log on as a service** and select **Define these policy settings**.
   b. Click **Add User or Group…** and click **Browse …**.
   c. Type **Administrator**, click **Check Names**, and click **OK**. Verify that the account is displayed in <DomainName>\Username format as indicated in the following screenshot.



   d. Click **OK**, and **OK** again.
10. Configure the user rights to prevent the BA account from accessing member servers and workstations via Remote Desktop Services by doing the following:
   a. Double-click **Deny log on through Remote Desktop Services** and select **Define these policy settings**.
   b. Click **Add User or Group…** and click **Browse …**.
   c. Type **Administrator**, click **Check Names**, and click **OK**. Verify that the account is displayed in <DomainName>\Username format as indicated in the following screenshot.

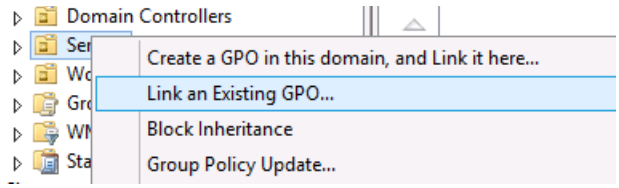


   d. Click **OK**, and **OK** again.
11. To exit **Group Policy Management Editor**, click **File**, and click **Exit**.

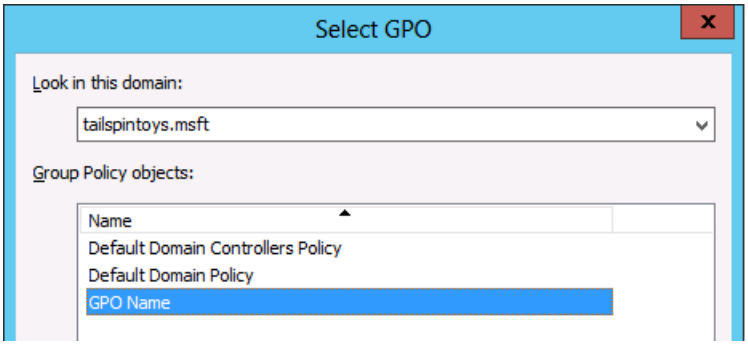
12. In **Group Policy Management**, link the GPO to the member server and workstation OUs by doing the following:

    a. Navigate to the <Forest>\Domains\<Domain> (where <Forest> is the name of the forest and <Domain> is the name of the domain where you want to set the Group Policy).

    b. Right-click the OU that the GPO will be applied to and click **Link an existing GPO…**.



    c. Select the GPO that you only created and click **OK**.



    d. Create links to all other OUs that contain workstations.

    e. Create links to all other OUs that contain member servers.

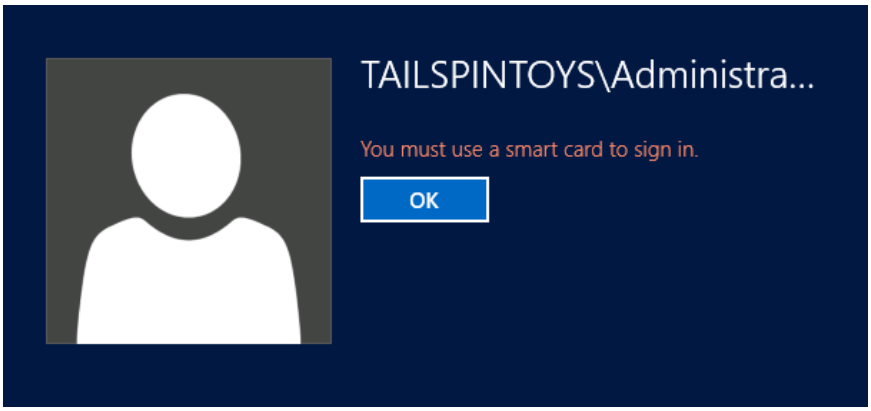
> **Important**
>
> When you add the Administrator account to these settings, you specify whether you are configuring a local Administrator account or a domain Administrator account by how you label the accounts. For example, to add the TAILSPINTOYS domain's Administrator account to these deny rights, you would browse to the Administrator account for the TAILSPINTOYS domain, which would appear as TAILSPINTOYS\Administrator. If you type "Administrator" in these user rights settings in the Group Policy Object Editor, you will restrict the local Administrator account on each computer to which the GPO is applied, as described earlier.

Verification Steps

The verification steps outlined here are specific to Windows 8 and Windows Server 2012.

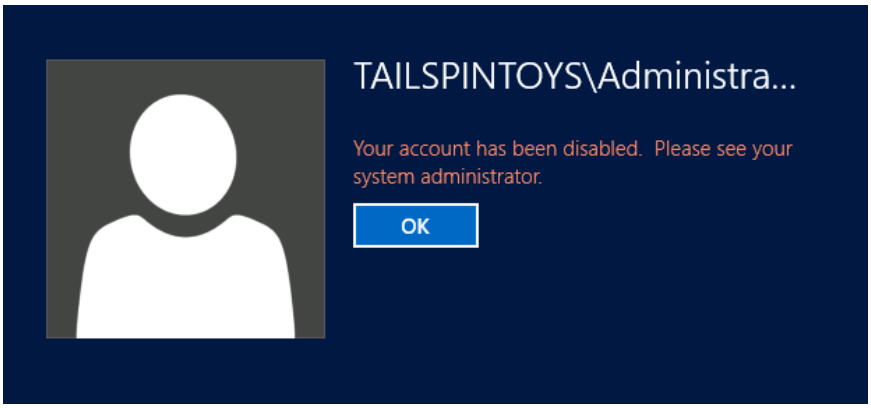
Verify “Smart card is required for interactive logon” Account Option

1. From any member server or workstation affected by the GPO changes, attempt to log on interactively to the domain by using the domain’s built-in Administrator account. After attempting to log on, a dialog box similar to the following should appear.



Verify “Account is disabled” Account Option

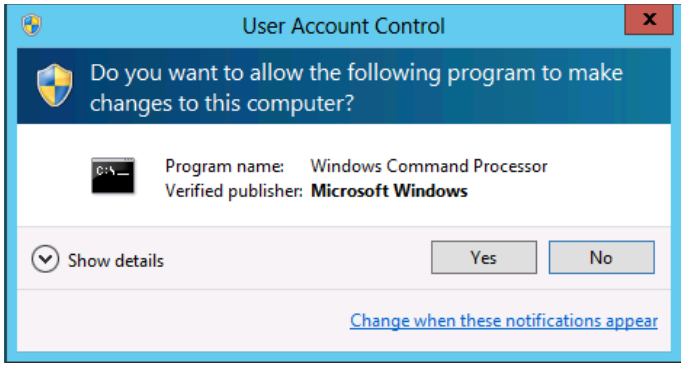
1. From any member server or workstation affected by the GPO changes, attempt to log on interactively to the domain by using the domain’s built-in Administrator account. After attempting to log on, a dialog box similar to the following should appear.



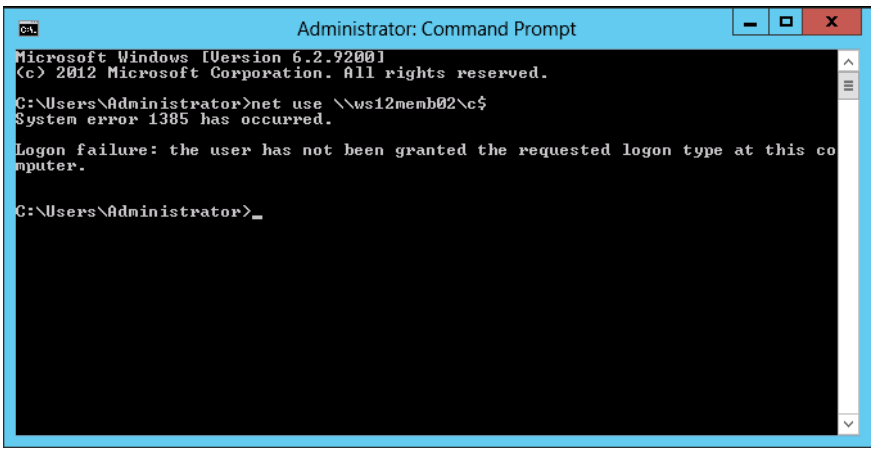
Verify “Deny access to this computer from the network” GPO Settings

From any member server or workstation that is not affected by the GPO changes (such as a jump server), attempt to access a member server or workstation over the network that is affected by the GPO changes. To verify the GPO settings, attempt to map the system drive by using the **NET USE** command by performing the following steps:

1. Log on to the domain using the domain's built-in Administrator account.
2. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
3. In the **Search** box, type **command prompt**, right-click **Command Prompt**, and then click **Run as administrator** to open an elevated command prompt.
4. When prompted to approve the elevation, click **Yes**.



5. In the **Command Prompt** window, type **net use \\<Server Name>\c$**, where <Server Name> is the name of the member server or workstation you are attempting to access over the network.
6. The following screenshot shows the error message that should appear.



Verify "Deny log on as a batch job" GPO Settings

1. From any member server or workstation affected by the GPO changes, log on locally.

Create a Batch File

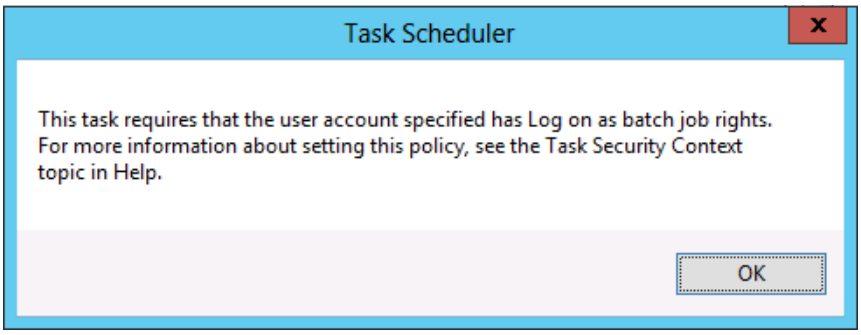
2. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
3. In the **Search** box, type **notepad**, and click **Notepad**.
4. In **Notepad,** type **dir c:**.
5. Click **File** and click **Save As…**.
6. In the **File name** field, type <Filename>.bat (where <Filename> is the name of the new batch file).

Schedule a Task

1. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
2. In the **Search** box, type **task scheduler**, and click **Task Scheduler**.

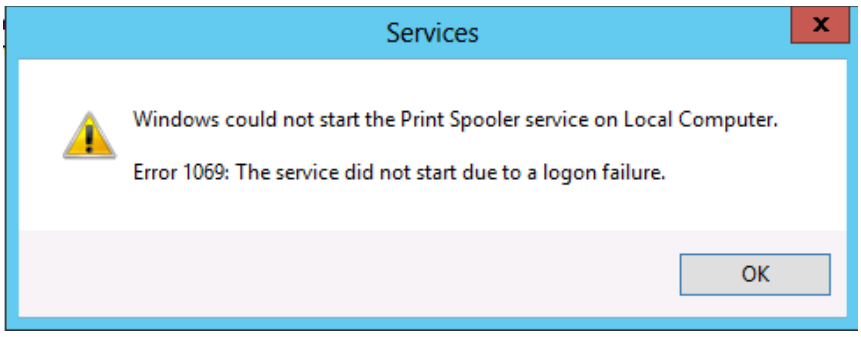
> **Note**
>
> On computers running Windows 8, in the **Search** box, type **schedule tasks**, and click **Schedule tasks**.

3. On **Task Scheduler**, click **Action**, and click **Create Task…**.
4. In the **Create Task** dialog box, type <Task Name> (where <Task Name> is the name of the new task).
5. Click the **Actions** tab, and click **New…**.
6. Under **Action:**, select **Start a program**.
7. Under **Program/script:**, click **Browse…**, locate and select the batch file created in the “Create a Batch File” section, and click **Open**.
8. Click **OK**.
9. Click the **General** tab.
10. Under **Security options**, click **Change User or Group…**.
11. Type the name of the BA account at the domain-level, click **Check Names**, and click **OK**.
12. Select **Run whether the user is logged on or not** and **Do not store password. The task will only have access to local computer resources**.
13. Click **OK**.
14. A dialog box should appear, requesting user account credentials to run the task.
15. After entering the credentials, click **OK**.
16. A dialog box similar to the following should appear.



Verify “Deny log on as a service” GPO Settings

1. From any member server or workstation affected by the GPO changes, log on locally.
2. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
3. In the **Search** box, type **services**, and click **Services**.
4. Locate and double-click **Print Spooler**.
5. Click the **Log On** tab.
6. Under **Log on as:**, select **This account**.
7. Click **Browse…**, type the name of the BA account at the domain-level, click **Check Names**, and click **OK**.
8. Under **Password:** and **Confirm password:**, type the Administrator account’s password, and click **OK**.
9. Click **OK** three more times.
10. Right-click the **Print Spooler** service and select **Restart**.
11. When the service is restarted, a dialog box similar to the following should appear.

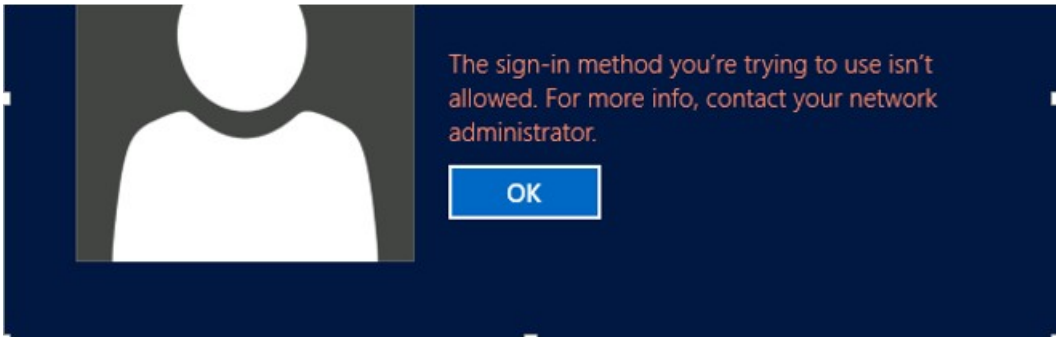


Revert Changes to the Printer Spooler Service

1. From any member server or workstation affected by the GPO changes, log on locally.
2. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
3. In the **Search** box, type **services**, and click **Services**.
4. Locate and double-click **Print Spooler**.
5. Click the **Log On** tab.
6. Under **Log on as:**, select the **Local System account**, and click **OK**.

Verify “Deny log on through Remote Desktop Services” GPO Settings

1. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
2. In the **Search** box, type **remote desktop connection**, and click **Remote Desktop Connection**.
3. In the **Computer** field, type the name of the computer that you want to connect to, and click **Connect**. (You can also type the IP address instead of the computer name.)
4. When prompted, provide credentials for the name of the BA account at the domain-level.
5. A dialog box similar to the following should appear.



Appendix E: Securing Enterprise Admins Groups in Active Directory

The Enterprise Admins (EA) group, which is housed in the forest root domain, should contain no users on a day-to-day basis, with the possible exception of the root domain's Administrator account, provided it is secured as described in Appendix D: Securing Built-In Administrator Accounts in Active Directory.

For detailed information about considerations for securing EA groups, see Securing Enterprise Admins in this document.

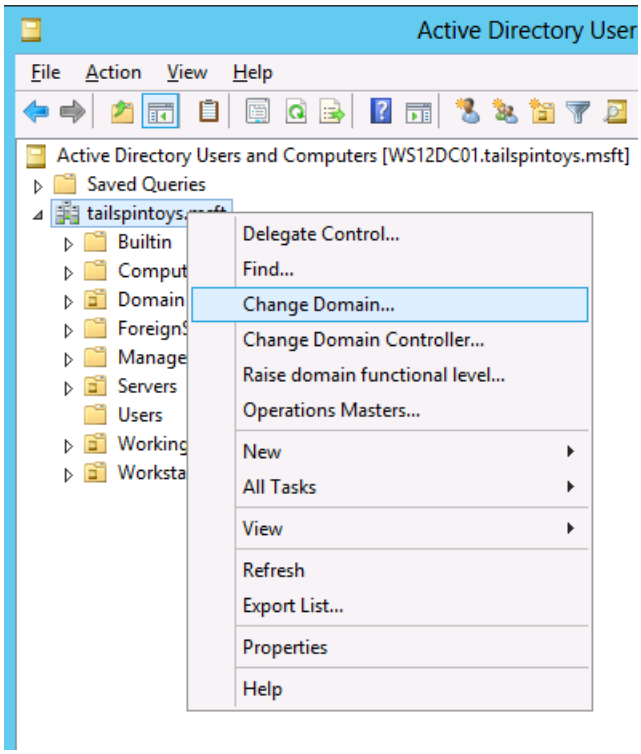
Enterprise Admins are, by default, members of the Administrators group in each domain in the forest. You should not remove the EA group from the Administrators groups in each domain because in the event of a forest disaster recovery scenario, EA rights will likely be required. The forest's Enterprise Admins group should be secured as detailed in the step-by-step instructions that follow.

For the Enterprise Admins group in the forest:

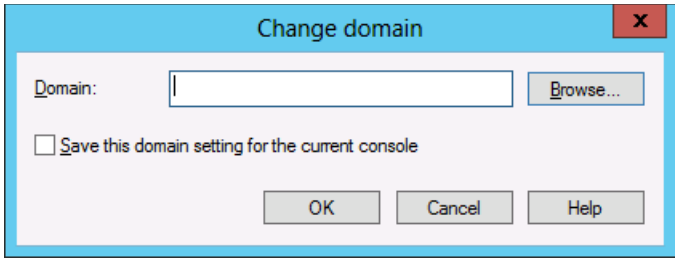
1. In GPOs linked to OUs containing member servers and workstations in each domain, the Enterprise Admins group should be added to the following user rights in **Computer Configuration\Policies\Windows Settings\Security Settings\Local Settings\User Rights Assignments**:
    - Deny access to this computer from the network
    - Deny log on as a batch job
    - Deny log on as a service
    - Deny log on locally
    - Deny log on through Remote Desktop Services
2. Configure auditing to send alerts if any modifications are made to the properties or membership of the Enterprise Admins group.

Step-by-Step Instructions for Removing All Members from the Enterprise Admins Group

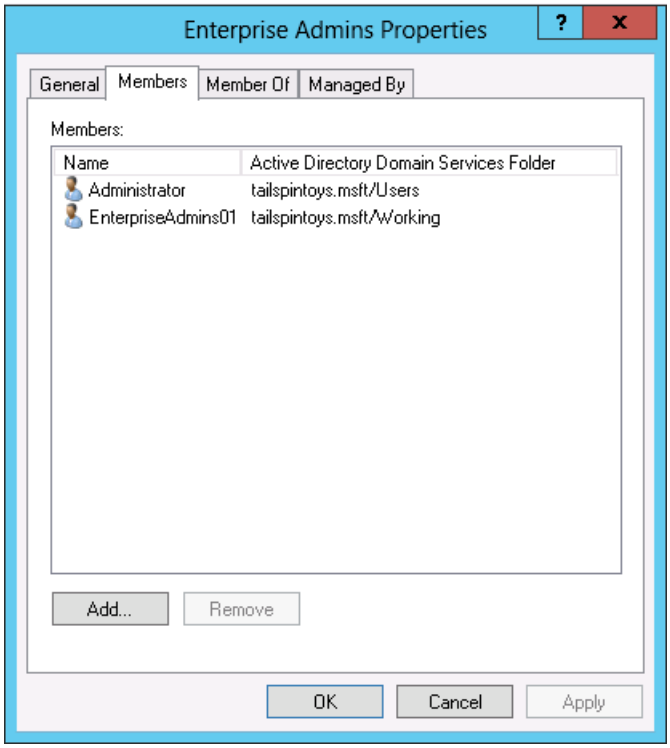
1. In **Server Manager**, click **Tools**, and click **Active Directory Users and Computers**.
2. If you are not managing the root domain for the forest, in the console tree, right-click <Domain>, and then click **Change Domain…** (where <Domain> is the name of the domain you're currently administering).



3. In the **Change domain** dialog box, click **Browse…**, select the root domain for the forest, and click **OK**.



4. To remove all members from the EA group:
   a. Double-click the **Enterprise Admins** group and then click the **Members** tab.



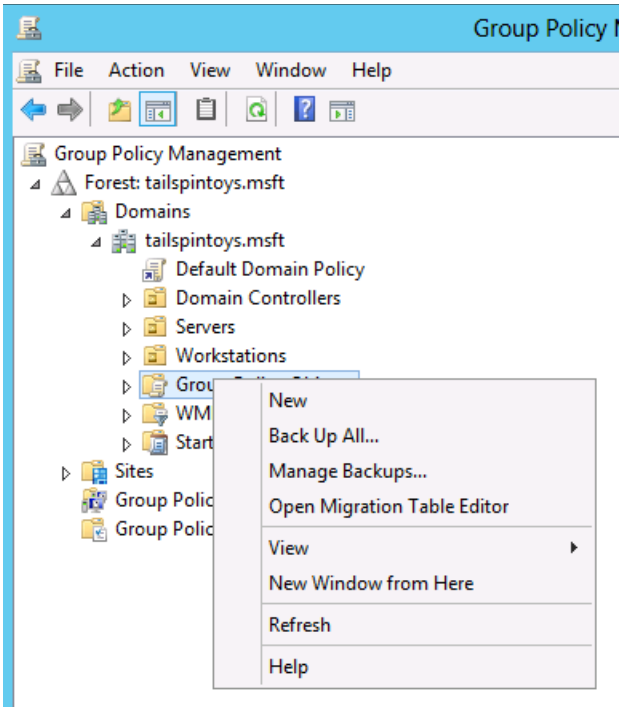
   b. Select a member of the group, click **Remove**, click **Yes**, and click **OK**.
5. Repeat step 2 until all members of the EA group have been removed.

Step-by-Step Instructions to Secure Enterprise Admins in Active Directory

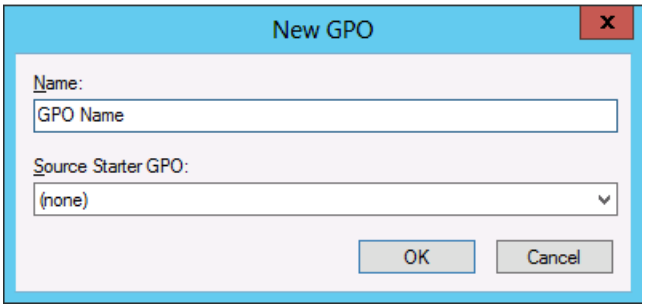
1. In **Server Manager**, click **Tools**, and click **Group Policy Management**.
2. In the console tree, expand <Forest>\Domains\<Domain>, and then **Group Policy Objects** (where <Forest> is the name of the forest and <Domain> is the name of the domain where you want to set the Group Policy).

> **Note**
>
> In a forest that contains multiple domains, a similar GPO should be created in each domain that requires that the Enterprise Admins group be secured.

3. In the console tree, right-click **Group Policy Objects**, and click **New**.

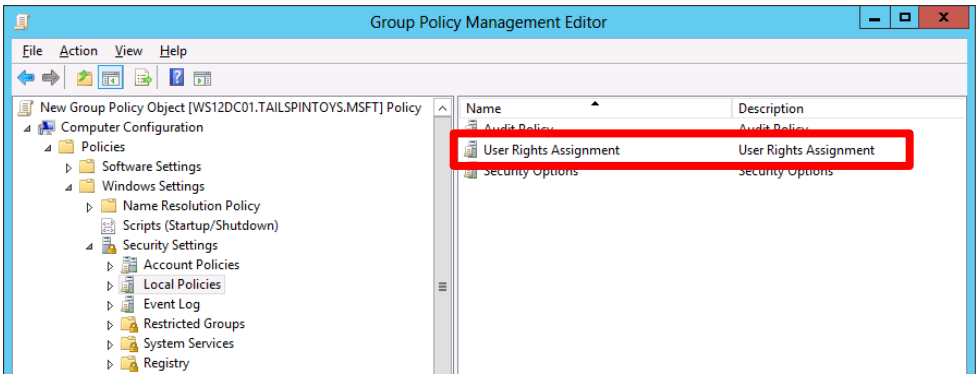


4. In the **New GPO** dialog box, type <GPO Name>, and click **OK** (where <GPO Name> is the name of this GPO).



5. In the details pane, right-click <GPO Name>, and click **Edit**.

6. Navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies**, and click **User Rights Assignment**.

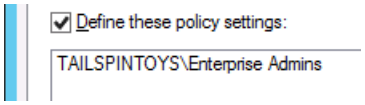


7. Configure the user rights to prevent members of the Enterprise Admins group from accessing member servers and workstations over the network by doing the following:

   a. Double-click **Deny access to this computer from the network** and select **Define these policy settings**.

   b. Click **Add User or Group…** and click **Browse …**.

   c. Type **Enterprise Admins**, click **Check Names**, and click **OK**.



   d. Click **OK**, and **OK** again.

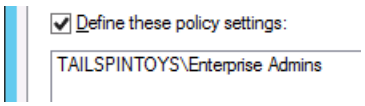
8. Configure the user rights to prevent members of the Enterprise Admins group from logging on as a batch job by doing the following:

   a. Double-click **Deny log on as a batch job** and select **Define these policy settings**.

   b. Click **Add User or Group…** and click **Browse …**.

> **Note**
>
> In a forest that contains multiple domains, click **Locations…** and select the root domain of the forest.

   c. Type **Enterprise Admins**, click **Check Names**, and click **OK**.



   d. Click **OK**, and **OK** again.

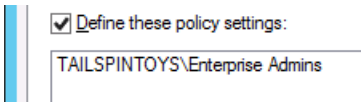
9. Configure the user rights to prevent members of the EA group from logging on as a service by doing the following:

a. Double-click **Deny log on as a service** and select **Define these policy settings**.

b. Click **Add User or Group…** and then click **Browse …**.

> **Note**
>
> In a forest that contains multiple domains, click **Locations…** and select the root domain of the forest.

c. Type **Enterprise Admins**, click **Check Names**, and click **OK**.



d. Click **OK**, and **OK** again.

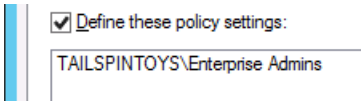
10. Configure user rights to prevent members of the Enterprise Admins group from logging on locally to member servers and workstations by doing the following:

a. Double-click **Deny log on locally** and select **Define these policy settings**.

b. Click **Add User or Group…** and click **Browse …**.

> **Note**
>
> In a forest that contains multiple domains, click **Locations…** and select the root domain of the forest.

c. Type **Enterprise Admins**, click **Check Names**, and click **OK**.



d. Click **OK**, and **OK** again.

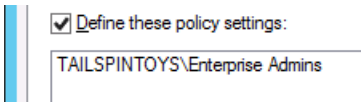
11. Configure the user rights to prevent members of the Enterprise Admins group from accessing member servers and workstations via Remote Desktop Services by doing the following:

a. Double-click **Deny log on through Remote Desktop Services** and select **Define these policy settings**.

b. Click **Add User or Group…** and click **Browse …**.

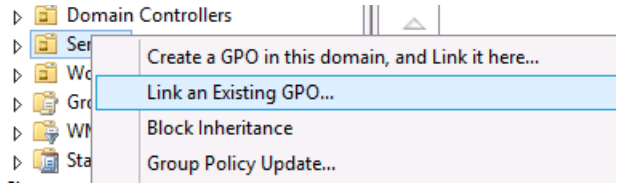
> **Note**
>
> In a forest that contains multiple domains, click **Locations…** and select the root domain of the forest.

c. Type **Enterprise Admins**, click **Check Names**, and click **OK**.

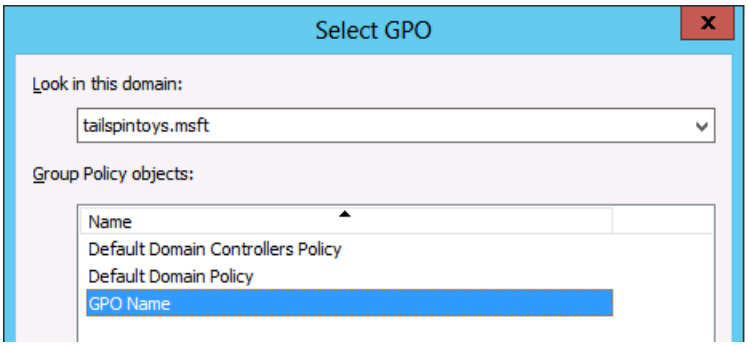


d. Click **OK**, and **OK** again.

12. To exit **Group Policy Management Editor**, click **File**, and click **Exit**.
13. In **Group Policy Management**, link the GPO to the member server and workstation OUs by doing the following:
    a. Navigate to the <Forest>\Domains\<Domain> (where <Forest> is the name of the forest and <Domain> is the name of the domain where you want to set the Group Policy).
    b. Right-click the OU that the GPO will be applied to and click **Link an existing GPO…**.



    c. Select the GPO that you just created and click **OK**.



    d. Create links to all other OUs that contain workstations.
    e. Create links to all other OUs that contain member servers.
    f. In a forest that contains multiple domains, a similar GPO should be created in each domain that requires that the Enterprise Admins group be secured.

> **Important**
>
> If jump servers are used to administer domain controllers and Active Directory, ensure that jump servers are located in an OU to which this GPOs is not linked.

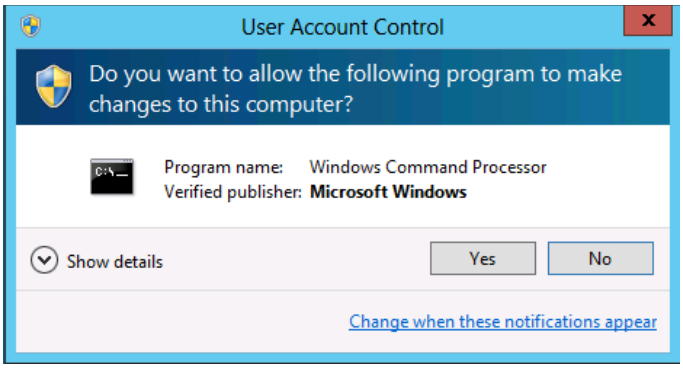
Verification Steps

Verify “Deny access to this computer from the network” GPO Settings

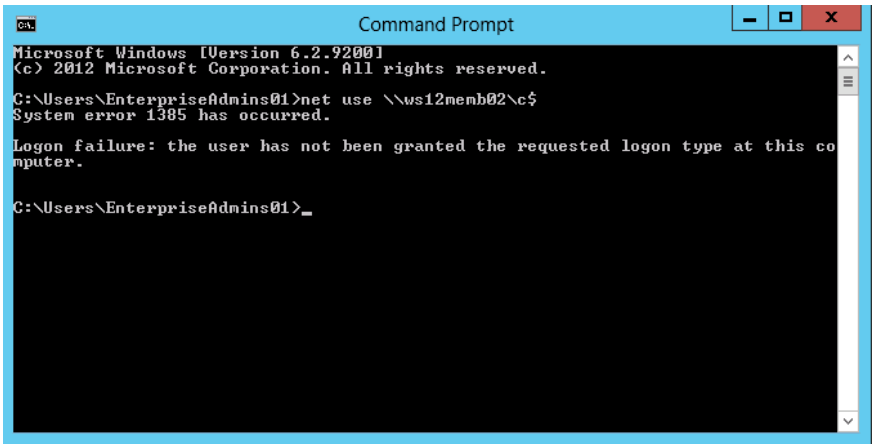
From any member server or workstation that is not affected by the GPO changes (such as a “jump server”), attempt to access a member server or workstation over the network that is affected by the GPO changes. To verify the GPO settings,

attempt to map the system drive by using the **NET USE** command by performing the following steps:

1. Log on locally using an account that is a member of the EA group.
2. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
3. In the **Search** box, type **command prompt**, right-click **Command Prompt**, and then click **Run as administrator** to open an elevated command prompt.
4. When prompted to approve the elevation, click **Yes**.



5. In the **Command Prompt** window, type **net use \\<Server Name>\c$**, where <Server Name> is the name of the member server or workstation you're attempting to access over the network.
6. The following screenshot shows the error message that should appear.



Verify "Deny log on as a batch job" GPO Settings

1. From any member server or workstation affected by the GPO changes, log on locally.

Create a Batch File

2. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
3. In the **Search** box, type **notepad**, and click **Notepad**.

4. In **Notepad,** type **dir c:**.
5. Click **File**, and click **Save As…**.
6. In the **File name** box, type <Filename>.bat (where <Filename> is the name of the new batch file).

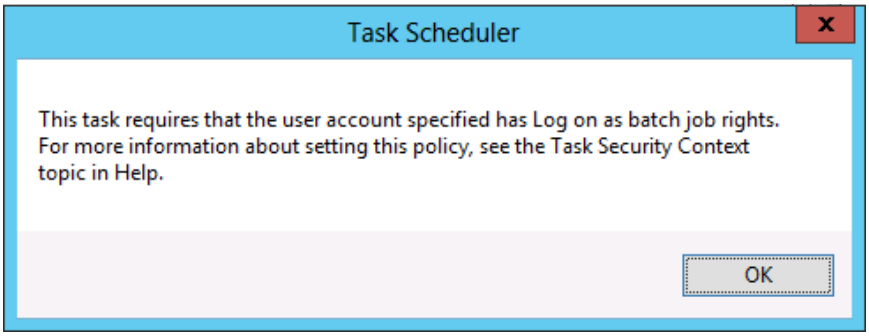
Schedule a Task

7. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
8. In the **Search** box, type **task scheduler**, and click **Task Scheduler**.

> **Note**
>
> On computers running Windows 8, in the **Search** box, type **schedule tasks**, and click **Schedule tasks**.

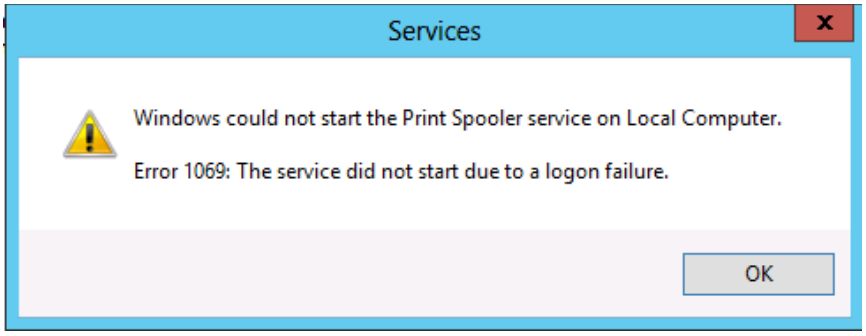
9. Click **Action**, and click **Create Task…**.
10. In the **Create Task** dialog box, type <Task Name> (where <Task Name> is the name of the new task).
11. Click the **Actions** tab, and click **New…**.
12. In the **Action:** field, select **Start a program**.
13. Under **Program/script:**, click **Browse…**, locate and select the batch file created in the **Create a Batch File** section, and click **Open**.
14. Click **OK**.
15. Click the **General** tab.
16. In the **Security options** field, click **Change User or Group…**.
17. Type the name of an account that is a member of the EAs group, click **Check Names**, and click **OK**.
18. Select **Run whether the user is logged on or not** and select **Do not store password. The task will only have access to local computer resources**.
19. Click **OK**.
20. A dialog box should appear, requesting user account credentials to run the task.
21. After entering the credentials, click **OK**.

22. A dialog box similar to the following should appear.



Verify “Deny log on as a service” GPO Settings

1. From any member server or workstation affected by the GPO changes, log on locally.
2. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
3. In the **Search** box, type **services**, and click **Services**.
4. Locate and double-click **Print Spooler**.
5. Click the **Log On** tab.
6. Under **Log on as:**, select **This account**.
7. Click **Browse…**, type the name of an account that is a member of the EAs group, click **Check Names**, and click **OK**.
8. Under **Password:** and **Confirm password:**, type the selected account’s password, and click **OK**.
9. Click **OK** three more times.
10. Right-click the **Print Spooler** service and select **Restart**.
11. When the service is restarted, a dialog box similar to the following should appear.

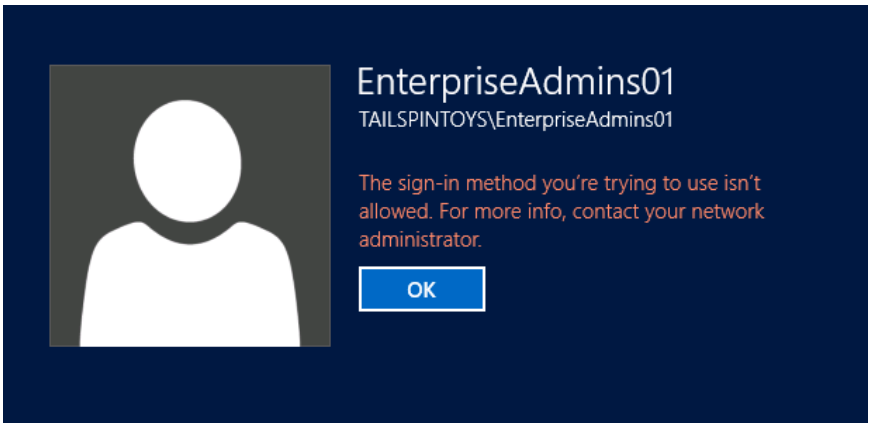


Revert Changes to the Printer Spooler Service

1. From any member server or workstation affected by the GPO changes, log on locally.
2. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
3. In the **Search** box, type **services**, and click **Services**.
4. Locate and double-click **Print Spooler**.
5. Click the **Log On** tab.
6. Under **Log on as:**, select the **Local System account**, and click **OK**.

Verify “Deny log on locally” GPO Settings

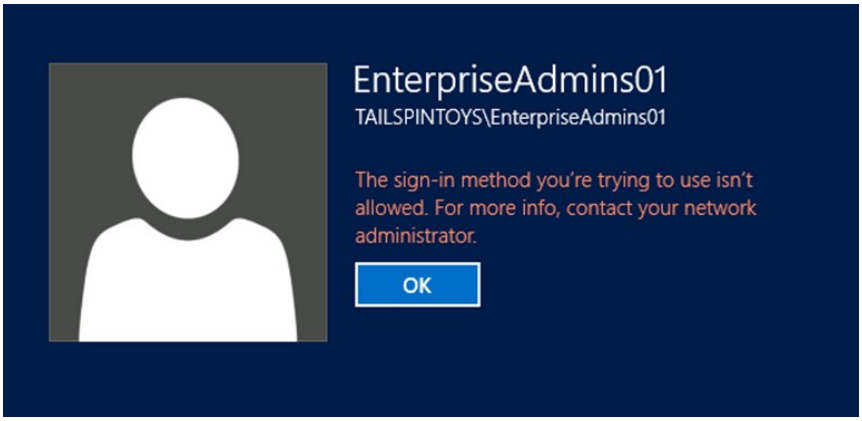
1. From any member server or workstation affected by the GPO changes, attempt to log on locally using an account that is a member of the EA group. A dialog box similar to the following should appear.



Verify “Deny log on through Remote Desktop Services” GPO Settings

1. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
2. In the **Search** box, type **remote desktop connection**, and then click **Remote Desktop Connection**.
3. In the **Computer** field, type the name of the computer that you want to connect to, and then click **Connect**. (You can also type the IP address instead of the computer name.)
4. When prompted, provide credentials for an account that is a member of the EA group.

5. A dialog box similar to the following should appear.



As is the case with the Enterprise Admins (EA) group, membership in the Domain Admins (DA) group should be required only in build or disaster recovery scenarios. There should be no day-to-day user accounts in the DA group with the exception of the built-in Administrator account for the domain, if it has been secured as described in Appendix D: Securing Built-In Administrator Accounts in Active Directory.

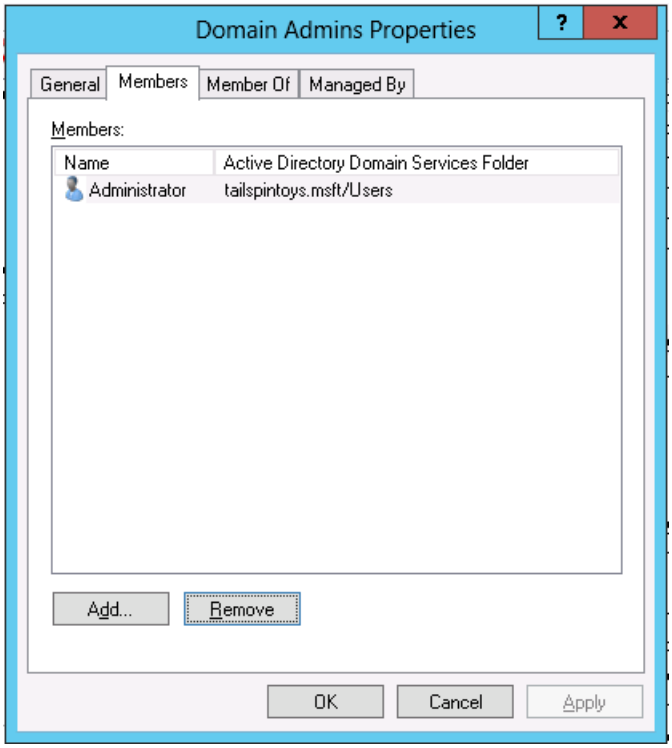
Domain Admins are, by default, members of the local Administrators groups on all member servers and workstations in their respective domains. This default nesting should not be modified for supportability and disaster recovery purposes. If Domain Admins have been removed from the local Administrators groups on the member servers, the group should be added to the Administrators group on each member server and workstation in the domain. Each domain's Domain Admins group should be secured as described in the step-by-step instructions that follow.

For the Domain Admins group in each domain in the forest:

1. Remove all members from the group, with the possible exception of the built-in Administrator account for the domain, provided it has been secured as described in Appendix D: Securing Built-In Administrator Accounts in Active Directory.
2. In GPOs linked to OUs containing member servers and workstations in each domain, the DA group should be added to the following user rights in **Computer Configuration\Policies\Windows Settings\Security Settings\Local Settings\User Rights Assignments**:
    - Deny access to this computer from the network
    - Deny log on as a batch job
    - Deny log on as a service
    - Deny log on locally
    - Deny log on through Remote Desktop Services user rights
3. Auditing should be configured to send alerts if any modifications are made to the properties or membership of the Domain Admins group.

Step-by-Step Instructions for Removing all Members from the Domain Admins Group

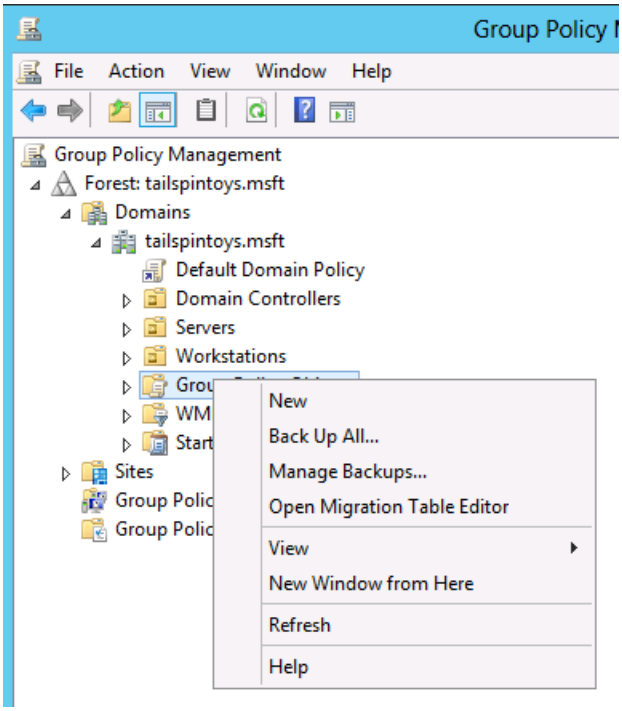
1. In **Server Manager**, click **Tools**, and click **Active Directory Users and Computers**.
2. To remove all members from the DA group, perform the following steps:
   a. Double-click the **Domain Admins** group and click the **Members** tab.



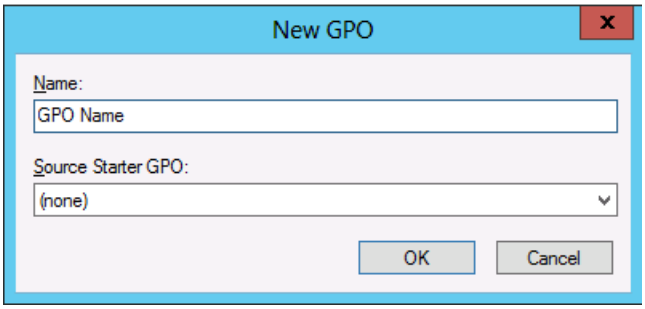
   b. Select a member of the group, click **Remove**, click **Yes**, and click **OK**.
3. Repeat step 2 until all members of the DA group have been removed.

Step-by-Step Instructions to Secure Domain Admins in Active Directory

1. In **Server Manager**, click **Tools**, and click **Group Policy Management**.
2. In the console tree, expand <Forest>\Domains\<Domain>, and then **Group Policy Objects** (where <Forest> is the name of the forest and <Domain> is the name of the domain where you want to set the Group Policy).
3. In the console tree, right-click **Group Policy Objects**, and click **New**.

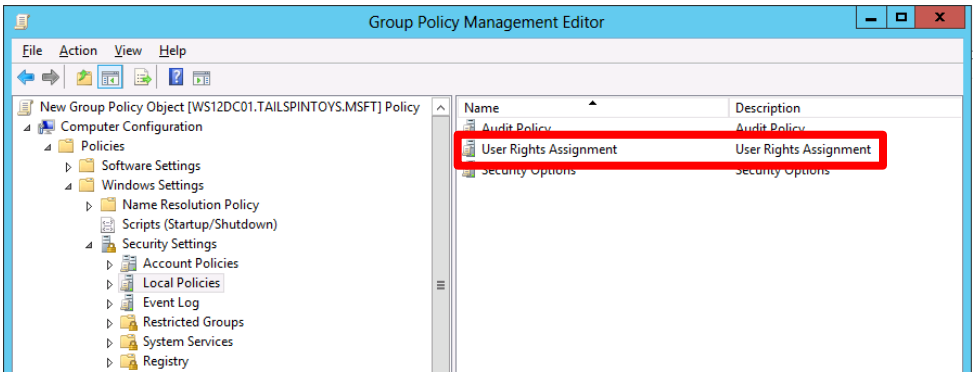


4. In the **New GPO** dialog box, type <GPO Name>, and click **OK** (where *GPO Name* is the name of this GPO).



5. In the details pane, right-click <GPO Name>, and click **Edit**.

6. Navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies**, and click **User Rights Assignment**.

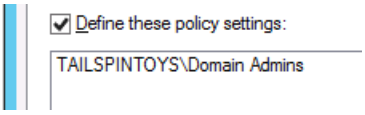


7. Configure the user rights to prevent members of the Domain Admins group from accessing members servers and workstations over the network by doing the following:

   a. Double-click **Deny access to this computer from the network** and select **Define these policy settings**.

   b. Click **Add User or Group…** and click **Browse …**.

   c. Type **Domain Admins**, click **Check Names**, and click **OK**.



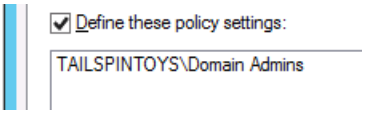
   d. Click **OK**, and **OK** again.

8. Configure the user rights to prevent members of the DA group from logging on as a batch job by doing the following:

   a. Double-click **Deny log on as a batch job** and select **Define these policy settings**.

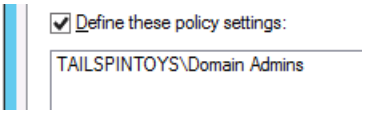
   b. Click **Add User or Group…** and click **Browse …**.

   c. Type **Domain Admins**, click **Check Names**, and click **OK**.

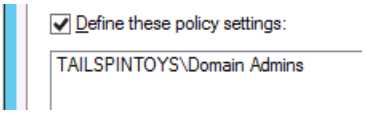


   d. Click **OK**, and **OK** again.

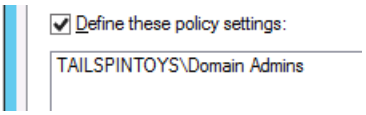
9. Configure the user rights to prevent members of the DA group from logging on as a service by doing the following:
   a. Double-click **Deny log on as a service** and select **Define these policy settings**.
   b. Click **Add User or Group…** and click **Browse …**.
   c. Type **Domain Admins**, click **Check Names**, and click **OK**.



   d. Click **OK**, and **OK** again.
10. Configure the user rights to prevent members of the Domain Admins group from logging on locally to member servers and workstations by doing the following:
   a. Double-click **Deny log on locally** and select **Define these policy settings**.
   b. Click **Add User or Group…** and click **Browse …**.
   c. Type **Domain Admins**, click **Check Names**, and click **OK**.



   d. Click **OK**, and **OK** again.
11. Configure the user rights to prevent members of the Domain Admins group from accessing member servers and workstations via Remote Desktop Services by doing the following:
   a. Double-click **Deny log on through Remote Desktop Services** and select **Define these policy settings**.
   b. Click **Add User or Group…** and click **Browse …**.
   c. Type **Domain Admins**, click **Check Names**, and click **OK**.

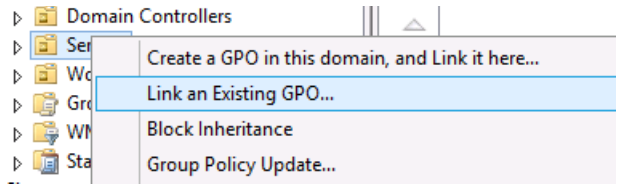


   d. Click **OK**, and **OK** again.
12. To exit **Group Policy Management Editor**, click **File**, and click **Exit**.

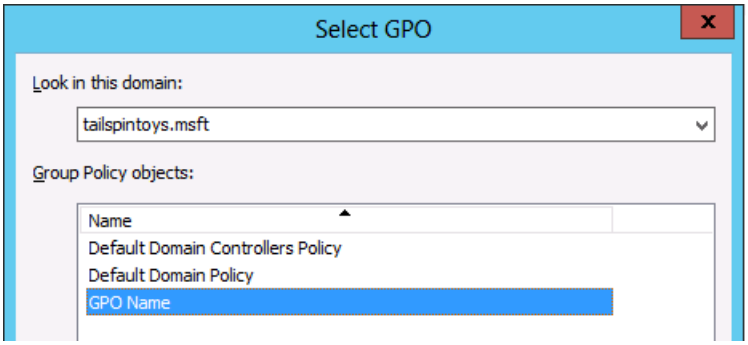
13. In **Group Policy Management**, link the GPO to the member server and workstation OUs by doing the following:

    a. Navigate to the <Forest>\Domains\<Domain> (where <Forest> is the name of the forest and <Domain> is the name of the domain where you want to set the Group Policy).

    b. Right-click the OU that the GPO will be applied to and click **Link an existing GPO…**.



    c. Select the GPO that you just created and click **OK**.



    d. Create links to all other OUs that contain workstations.

    e. Create links to all other OUs that contain member servers.

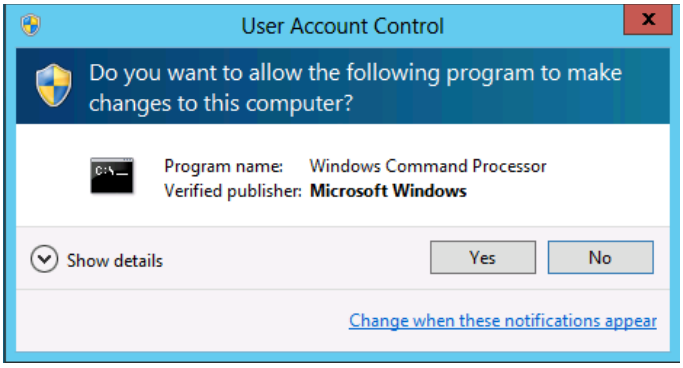
> **Important**
>
> If jump servers are used to administer domain controllers and Active Directory, ensure that jump servers are located in an OU to which this GPOs is not linked.

Verification Steps

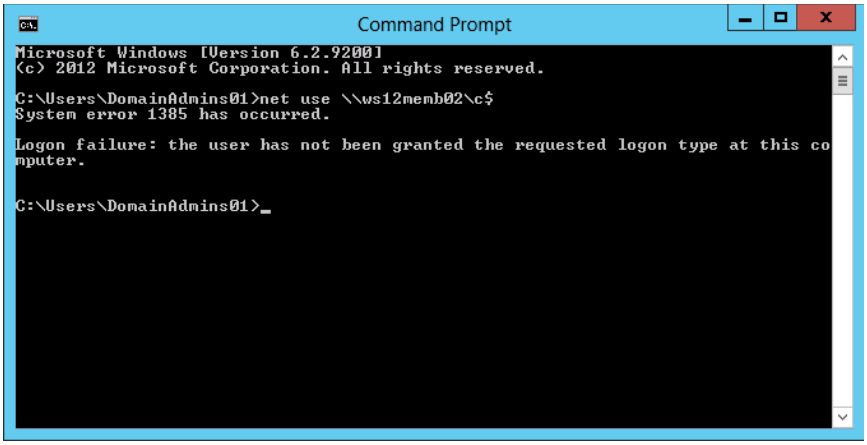
Verify “Deny access to this computer from the network” GPO Settings

From any member server or workstation that is not affected by the GPO changes (such as a “jump server”), attempt to access a member server or workstation over the network that is affected by the GPO changes. To verify the GPO settings, attempt to map the system drive by using the **NET USE** command.

1. Log on locally using an account that is a member of the Domain Admins group.
2. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
3. In the **Search** box, type **command prompt**, right-click **Command Prompt**, and then click **Run as administrator** to open an elevated command prompt.
4. When prompted to approve the elevation, click **Yes**.



5. In the **Command Prompt** window, type **net use \\<Server Name>\c$**, where <Server Name> is the name of the member server or workstation you’re attempting to access over the network.
6. The following screenshot shows the error message that should appear.



Verify “Deny log on as a batch job” GPO Settings

1. From any member server or workstation affected by the GPO changes, log on locally.

Create a Batch File

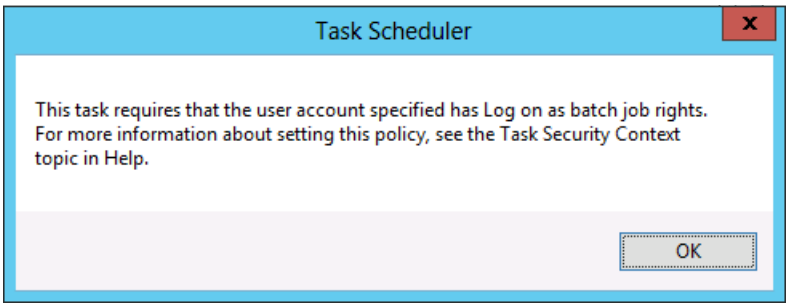
2. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
3. In the **Search** box, type **notepad**, and click **Notepad**.
4. In **Notepad,** type **dir c:**.
5. Click **File**, and click **Save As…**.
6. In the **File name** field, type <Filename>.bat (where <Filename> is the name of the new batch file).

Schedule a Task

7. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
8. In the **Search** box, type **task scheduler**, and click **Task Scheduler**.

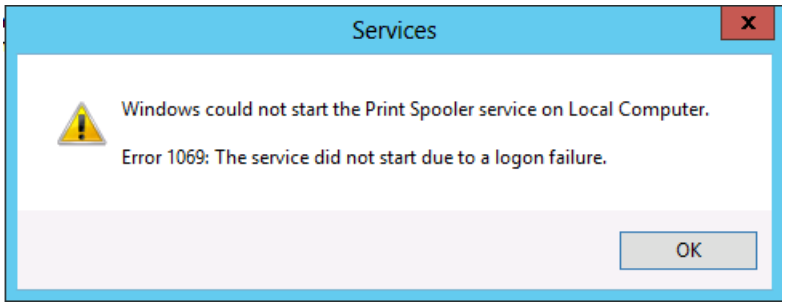
> **Note**
>
> On computers running Windows 8, in the **Search** box, type **schedule tasks**, and click **Schedule tasks**.

9. In the **Task Scheduler** menu bar, click **Action**, and click **Create Task…**.
10. In the **Create Task** dialog box, type <Task Name> (where <Task Name> is the name of the new task).
11. Click the **Actions** tab, and click **New…**.
12. In the **Action:** field, select **Start a program**.
13. Under **Program/script:**, click **Browse…**, locate and select the batch file created in the **Create a Batch File** section, and click **Open**.
14. Click **OK**.
15. Click the **General** tab.
16. Under **Security options**, click **Change User or Group…**.
17. Type the name of an account that is a member of the Domain Admins group, click **Check Names**, and click **OK**.
18. Select **Run whether the user is logged on or not** and select **Do not store password. The task will only have access to local computer resources**.
19. Click **OK**.
20. A dialog box should appear, requesting user account credentials to run the task.
21. After entering the credentials, click **OK**.
22. A dialog box similar to the following should appear.



Verify “Deny log on as a service” GPO Settings

1. From any member server or workstation affected by the GPO changes, log on locally.
2. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
3. In the **Search** box, type **services**, and click **Services**.
4. Locate and double-click **Print Spooler**.
5. Click the **Log On** tab.
6. Under **Log on as:**, select the **This account** option.
7. Click **Browse…**, type the name of an account that is a member of the Domain Admins group, click **Check Names**, and click **OK**.
8. Under **Password:** and **Confirm password:**, type the selected account’s password, and click **OK**.
9. Click **OK** three more times.
10. Right-click **Print Spooler** and click **Restart**.
11. When the service is restarted, a dialog box similar to the following should appear.



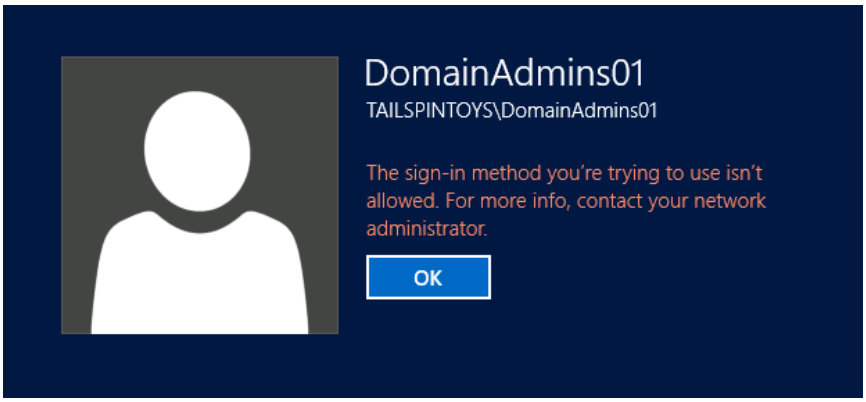
Revert Changes to the Printer Spooler Service

1. From any member server or workstation affected by the GPO changes, log on locally.
2. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
3. In the **Search** box, type **services**, and click **Services**.

4. Locate and double-click **Print Spooler**.
5. Click the **Log On** tab.
6. Under **Log on as:**, select the **Local System account**, and click **OK**.

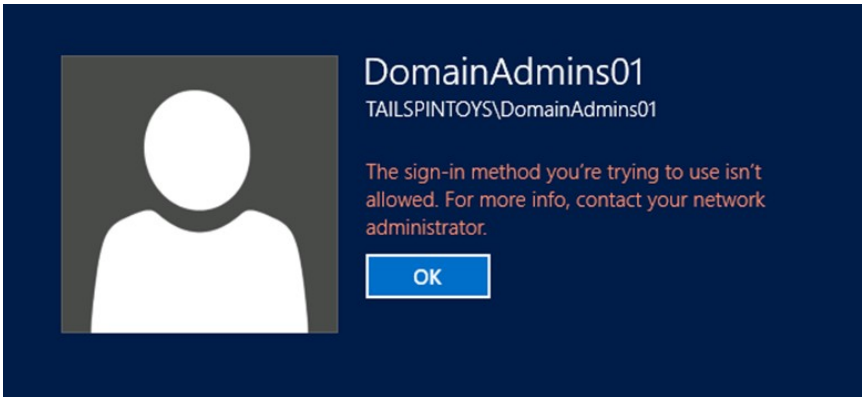
Verify “Deny log on locally” GPO Settings

1. From any member server or workstation affected by the GPO changes, attempt to log on locally using an account that is a member of the Domain Admins group. A dialog box similar to the following should appear.



Verify “Deny log on through Remote Desktop Services” GPO Settings

1. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
2. In the **Search** box, type **remote desktop connection**, and click **Remote Desktop Connection**.
3. In the **Computer** field, type the name of the computer that you want to connect to, and click **Connect**. (You can also type the IP address instead of the computer name.)
4. When prompted, provide credentials for an account that is a member of the Domain Admins group.
5. A dialog box similar to the following should appear.



Appendix G: Securing Administrators Groups in Active Directory

As is the case with the Enterprise Admins (EA) and Domain Admins (DA) groups, membership in the built-in Administrators (BA) group should be required only in build or disaster recovery scenarios. There should be no day-to-day user accounts in the Administrators group with the exception of the Built-in Administrator account for the domain, if it has been secured as described in Appendix D: Securing Built-in Administrator Accounts in Active Directory.

For detailed information about considerations in securing Domain Admins groups, see Securing Administrators Groups in Active Directory in this document.

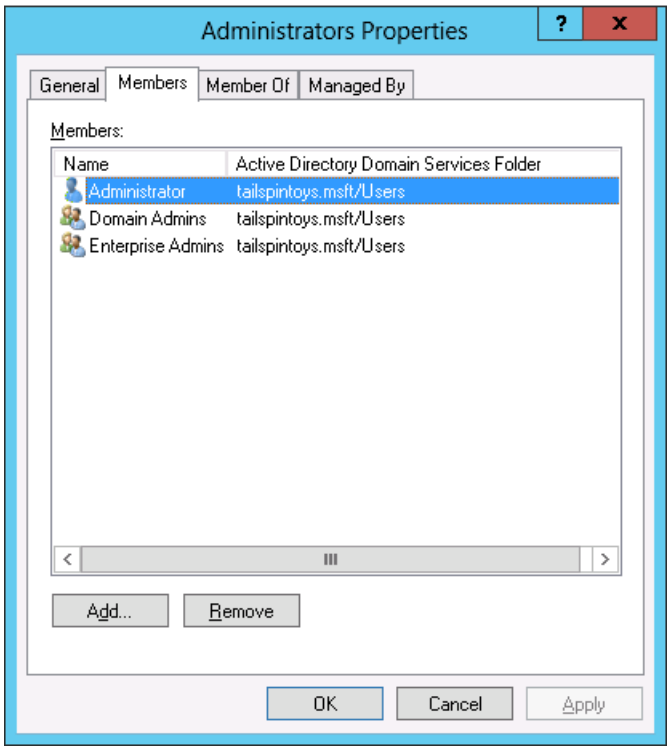
Administrators are, by default, the owners of most of the AD DS objects in their respective domains. Membership in this group may be required in build or disaster recovery scenarios in which ownership or the ability to take ownership of objects is required. Additionally, DAs and EAs inherit a number of their rights and permissions by virtue of their default membership in the Administrators group. Default group nesting for privileged groups in Active Directory should not be modified, and each domain's Administrators group should be secured as described in the step-by-step instructions that follow.

For the Administrators group in each domain in the forest:

1. Remove all members from the Administrators group, with the possible exception of the built-in Administrator account for the domain, provided it has been secured as described in Appendix D: Securing Built-In Administrator Accounts in Active Directory.
2. In GPOs linked to OUs containing member servers and workstations in each domain, the DA group should be added to the following user rights **in Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\ User Rights Assignment**:
    - Deny access to this computer from the network
    - Deny log on as a batch job
    - Deny log on as a service
3. At the domain controllers OU in each domain in the forest, the Administrators group should be granted the following user rights:
    - Access this computer from the network
    - Allow log on locally
    - Allow log on through Remote Desktop Services
4. Auditing should be configured to send alerts if any modifications are made to the properties or membership of the Administrators group.

Step-by-Step Instructions for Removing All Members from the Administrators Group

1. In **Server Manager**, click **Tools**, and click **Active Directory Users and Computers**.
2. To remove all members from the Administrators group, perform the following steps:
    a. Double-click the **Administrators** group and click the **Members** tab.

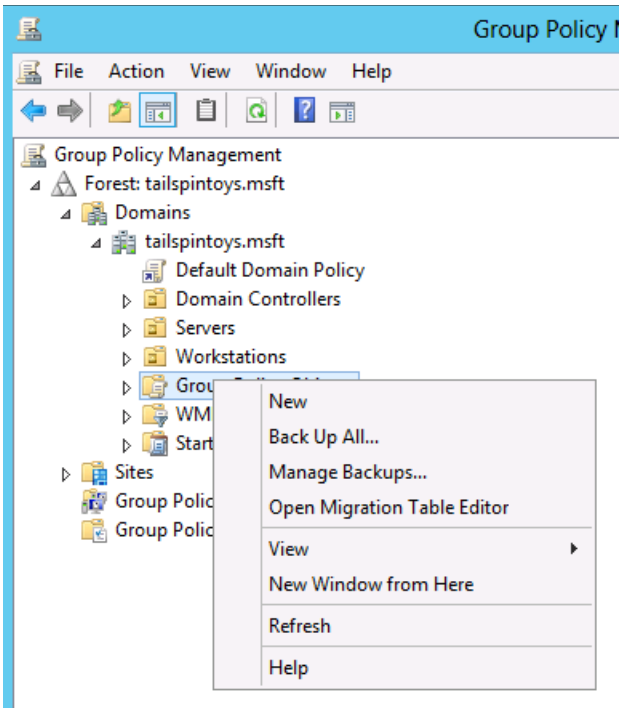


b. Select a member of the group, click **Remove**, click **Yes**, and click **OK**.

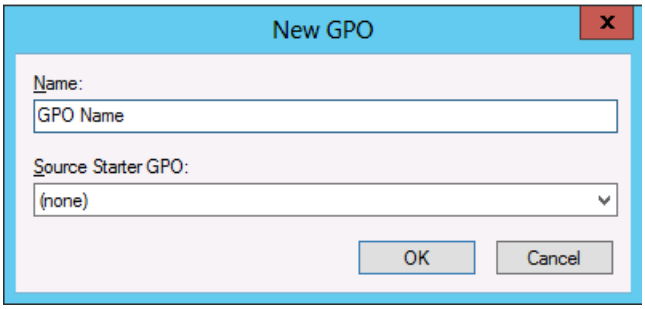
3. Repeat step 2 until all members of the Administrators group have been removed.

Step-by-Step Instructions to Secure Administrators Groups in Active Directory

1. In **Server Manager**, click **Tools**, and click **Group Policy Management**.
2. In the console tree, expand <Forest>\Domains\<Domain>, and then **Group Policy Objects** (where <Forest> is the name of the forest and <Domain> is the name of the domain where you want to set the Group Policy).
3. In the console tree, right-click **Group Policy Objects**, and click **New**.

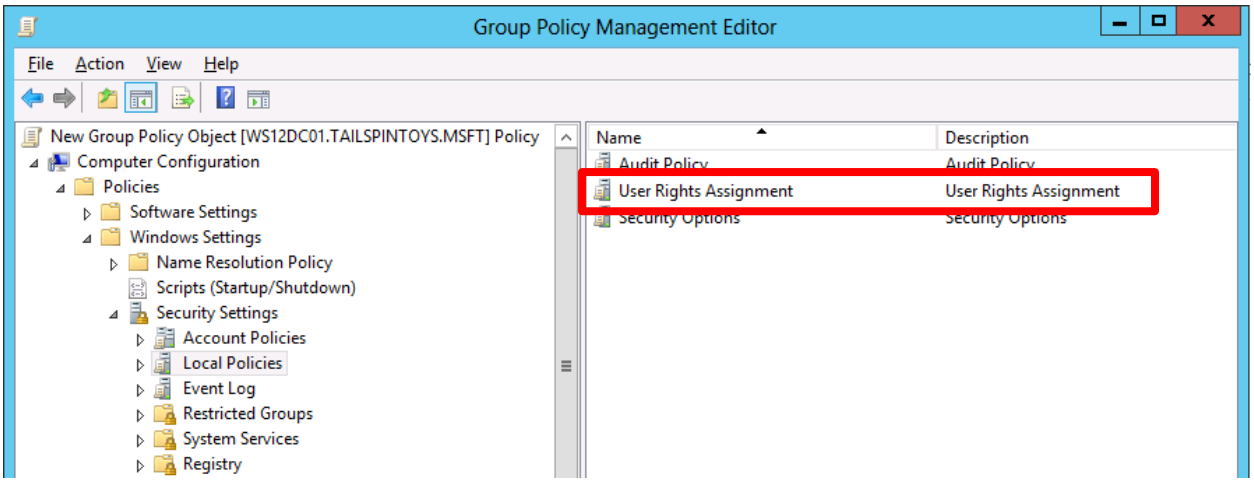


4. In the **New GPO** dialog box, type <GPO Name>, and click **OK** (where *GPO Name* is the name of this GPO).

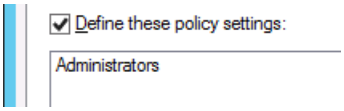


5. In the details pane, right-click <GPO Name>, and click **Edit**.

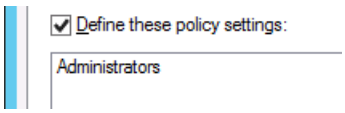
6. Navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies**, and click **User Rights Assignment**.



7. Configure the user rights to prevent members of the Administrators group from accessing members servers and workstations over the network by doing the following:
   a. Double-click **Deny access to this computer from the network** and select **Define these policy settings**.
   b. Click **Add User or Group…** and click **Browse …**.
   c. Type **Administrators**, click **Check Names**, and click **OK**.



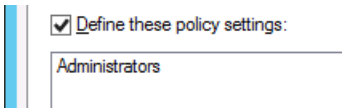
   d. Click **OK**, and **OK** again.
8. Configure the user rights to prevent members of the Administrators group from logging on as a batch job by doing the following:
   a. Double-click **Deny log on as a batch job** and select **Define these policy settings**.
   b. Click **Add User or Group…** and click **Browse …**.
   c. Type **Administrators**, click **Check Names**, and click **OK**.



   d. Click **OK**, and **OK** again.
9. Configure the user rights to prevent members of the Administrators group from logging on as a service by doing the following:
   a. Double-click **Deny log on as a service** and select **Define these policy settings**.

b. Click **Add User or Group…** and click **Browse …**.

c. Type **Administrators**, click **Check Names**, and click **OK**.



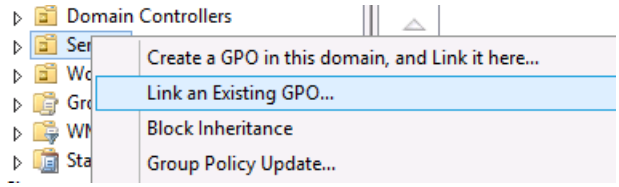
d. Click **OK**, and **OK** again.

10. To exit **Group Policy Management Editor**, click **File**, and click **Exit**.

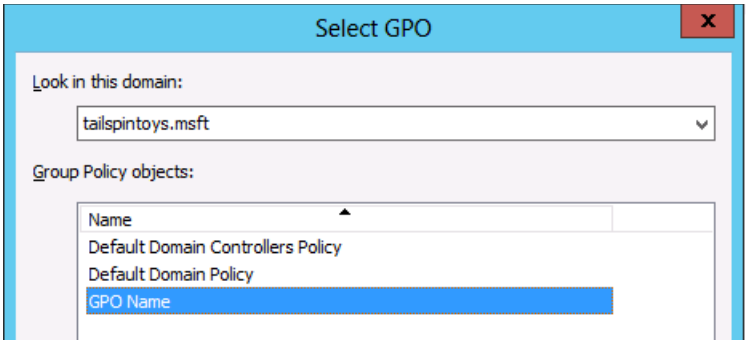
11. In **Group Policy Management**, link the GPO to the member server and workstation OUs by doing the following:

a. Navigate to the <Forest>\Domains\<Domain> (where <Forest> is the name of the forest and <Domain> is the name of the domain where you want to set the Group Policy).

b. Right-click the OU that the GPO will be applied to and click **Link an existing GPO…**.



c. Select the GPO that you just created and click **OK**.



d. Create links to all other OUs that contain workstations.

e. Create links to all other OUs that contain member servers.

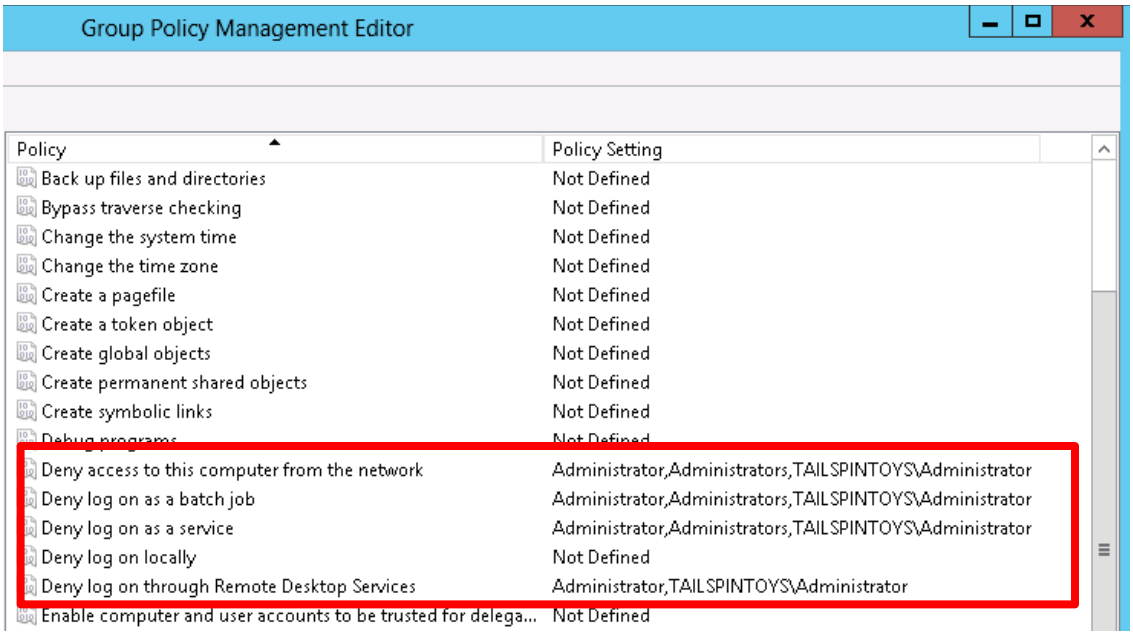
Important

If jump servers are used to administer domain controllers and Active Directory, ensure that jump servers are located in an OU to which this GPOs is not linked.

Note

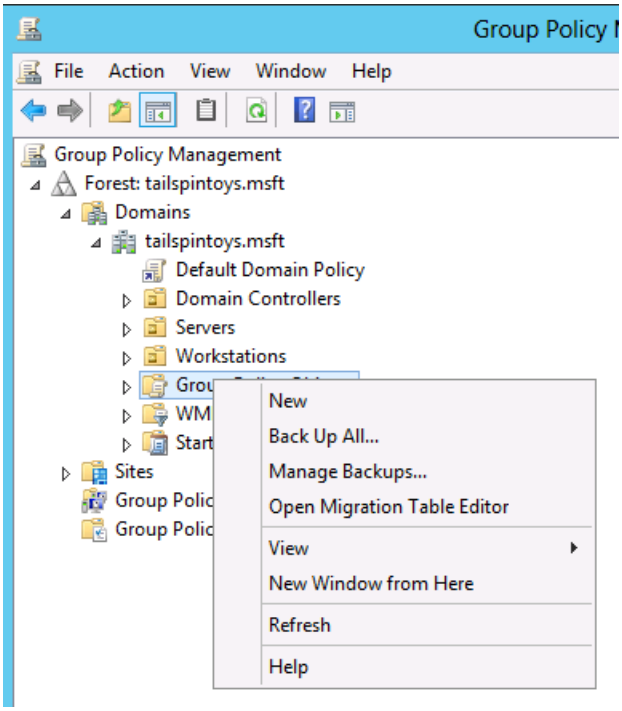
When you implement restrictions on the Administrators group in GPOs, Windows applies the settings to members of a computer's local Administrators group in addition to the domain's Administrators group. Therefore, you should use caution when implementing restrictions in the Administrators group. Although prohibiting network, batch, and service logons for members of the Administrators group is advised wherever it is feasible to implement, do not restrict local logons or logons through Remote Desktop Services. Blocking these logon types can block legitimate administration of a computer by members of the local Administrators group.

The following screenshot shows configuration settings that block misuse of built-in local and domain Administrator accounts, in addition to misuse of built-in local or domain Administrators groups. Note that the **Deny log on through Remote Desktop Services** user right does not include the Administrators group, because including it in this setting would also block these logons for accounts that are members of the local computer's Administrators group. If services on computers are configured to run in the context of any of the privileged groups described in this section, implementing these settings can cause services and applications to fail. Therefore, as with all of the recommendations in this section, you should thoroughly test settings for applicability in your environment.

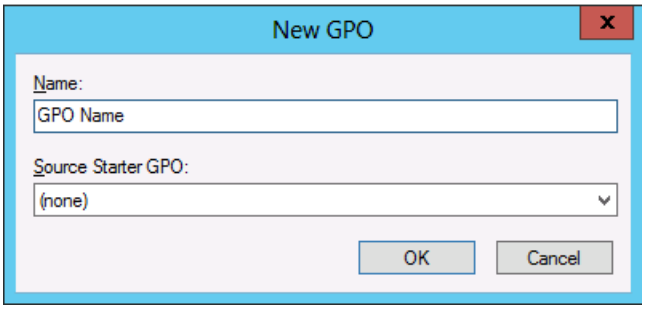


Step-by-Step Instructions to Grant User Rights to the Administrators Group

1. In **Server Manager**, click **Tools**, and click **Group Policy Management**.
2. In the console tree, expand <Forest>\Domains\<Domain>, and then **Group Policy Objects** (where <Forest> is the name of the forest and <Domain> is the name of the domain where you want to set the Group Policy).
3. In the console tree, right-click **Group Policy Objects**, and click **New**.

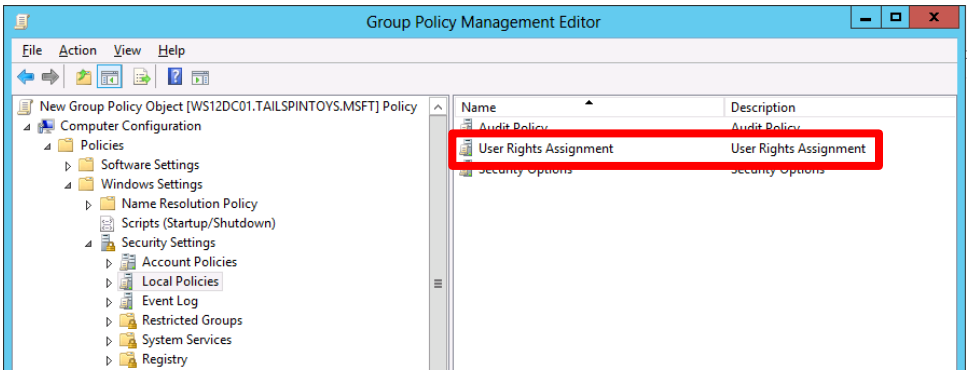


4. In the **New GPO** dialog box, type <GPO Name>, and click **OK** (where <GPO Name> is the name of this GPO).

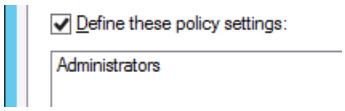


5. In the details pane, right-click <GPO Name>, and click **Edit**.

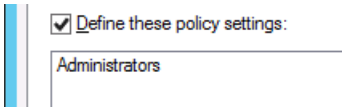
6. Navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies**, and click **User Rights Assignment**.



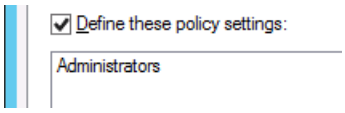
7. Configure the user rights to allow members of the Administrators group to access domain controllers over the network by doing the following:
   a. Double-click **Access to this computer from the network** and select **Define these policy settings**.
   b. Click **Add User or Group…** and click **Browse …**.
   c. Type **Administrators**, click **Check Names**, and click **OK**.



   d. Click **OK**, and **OK** again.
8. Configure the user rights to allow members of the Administrators group to log on locally by doing the following:
   a. Double-click **Allow log on locally** and select **Define these policy settings**.
   b. Click **Add User or Group…** and click **Browse …**.
   c. Type **Administrators**, click **Check Names**, and click **OK**.

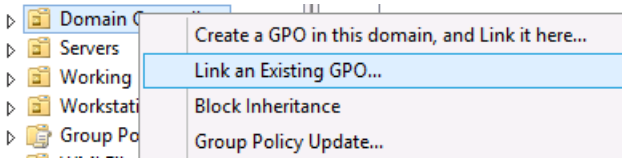


   d. Click **OK**, and **OK** again.
9. Configure the user rights to allow members of the Administrators group to log on through Remote Desktop Services by doing the following:
   a. Double-click **Allow log on through Remote Desktop Services** and select **Define these policy settings**.
   b. Click **Add User or Group…** and click **Browse …**.
   c. Type **Administrators**, click **Check Names**, and click **OK**.

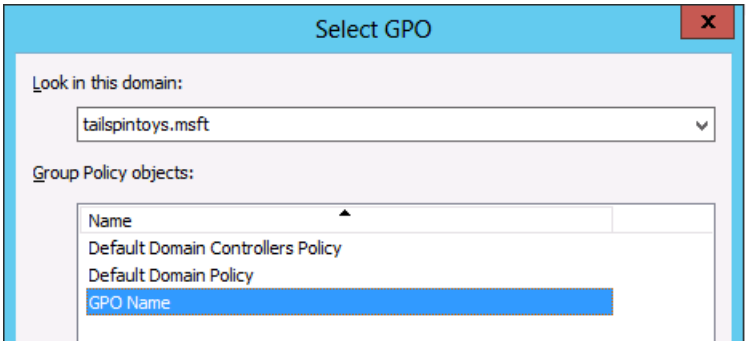


d. Click **OK**, and **OK** again.

10. To exit **Group Policy Management Editor**, click **File**, and click **Exit**.
11. In **Group Policy Management**, link the GPO to the domain controllers OU by doing the following:
    a. Navigate to the <Forest>\Domains\<Domain> (where <Forest> is the name of the forest and <Domain> is the name of the domain where you want to set the Group Policy).
    b. Right-click the domain controllers OU and click **Link an existing GPO…**.



    c. Select the GPO that you just created and click **OK**.

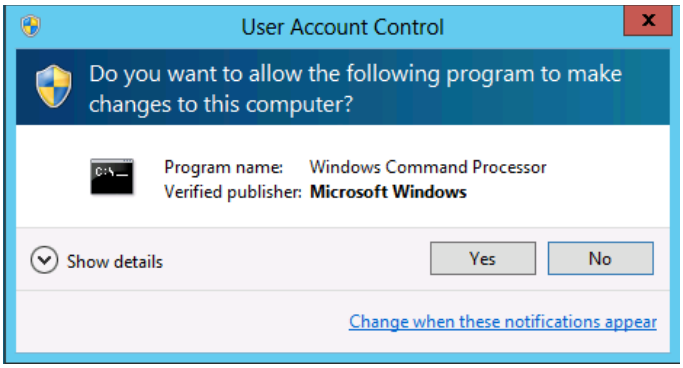


Verification Steps

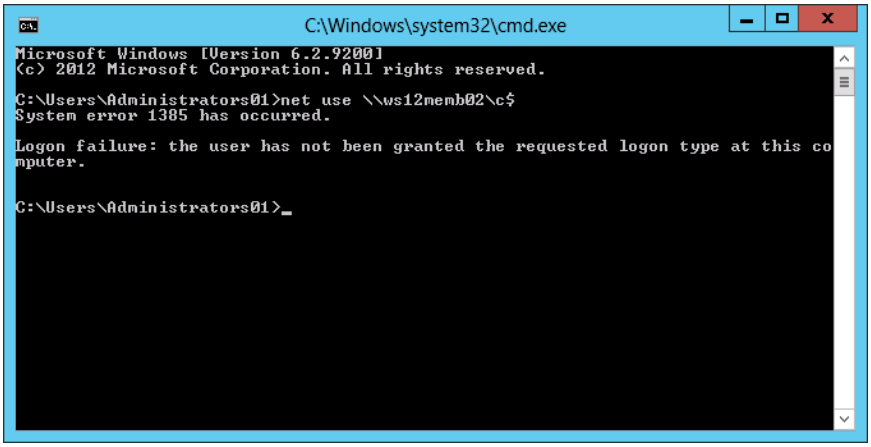
Verify “Deny access to this computer from the network” GPO Settings

From any member server or workstation that is not affected by the GPO changes (such as a “jump server”), attempt to access a member server or workstation over the network that is affected by the GPO changes. To verify the GPO settings, attempt to map the system drive by using the **NET USE** command.

1. Log on locally using an account that is a member of the Administrators group.
2. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
3. In the **Search** box, type **command prompt**, right-click **Command Prompt**, and then click **Run as administrator** to open an elevated command prompt.
4. When prompted to approve the elevation, click **Yes**.



5. In the **Command Prompt** window, type **net use \\<Server Name>\c$**, where <Server Name> is the name of the member server or workstation you're attempting to access over the network.
6. The following screenshot shows the error message that should appear.



Verify "Deny log on as a batch job" GPO Settings

1. From any member server or workstation affected by the GPO changes, log on locally.

Create a Batch File

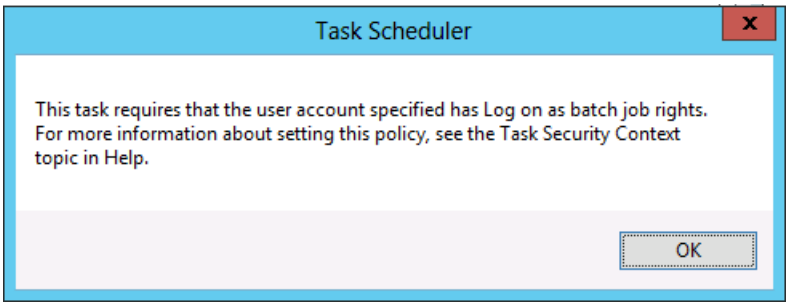
2. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
3. In the **Search** box, type **notepad**, and click **Notepad**.
4. In **Notepad,** type **dir c:**.
5. Click **File**, and click **Save As…**.
6. In the **File name** field, type <Filename>.bat (where <Filename> is the name of the new batch file).

Schedule a Task

7. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
8. In the **Search** box, type **task scheduler**, and click **Task Scheduler**.

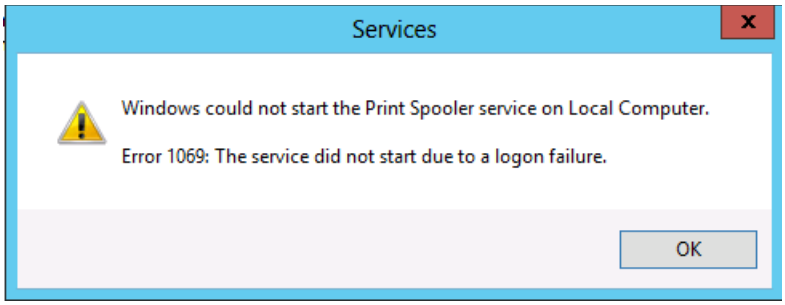
> **Note**
>
> On computers running Windows 8, in the **Search** box, type **schedule tasks**, and click **Schedule tasks**.

9. Click **Action**, and click **Create Task…**.
10. In the **Create Task** dialog box, type <Task Name> (where <Task Name> is the name of the new task).
11. Click the **Actions** tab, and click **New…**.
12. In the **Action:** field, select **Start a program**.
13. In the **Program/script:** field, click **Browse…**, locate and select the batch file created in the **Create a Batch File** section, and click **Open**.
14. Click **OK**.
15. Click the **General** tab.
16. In the **Security options** field, click **Change User or Group…**.
17. Type the name of an account that is a member of the Administrators group, click **Check Names**, and click **OK**.
18. Select **Run whether the user is logged on or not** and **Do not store password. The task will only have access to local computer resources**.
19. Click **OK**.
20. A dialog box should appear, requesting user account credentials to run the task.
21. After entering the password, click **OK**.
22. A dialog box similar to the following should appear.



Verify “Deny log on as a service” GPO Settings

1. From any member server or workstation affected by the GPO changes, log on locally.
2. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
3. In the **Search** box, type **services**, and click **Services**.
4. Locate and double-click **Print Spooler**.
5. Click the **Log On** tab.
6. In the **Log on as:** field, select **This account**.
7. Click **Browse…**, type the name of an account that is a member of the Administrators group, click **Check Names**, and click **OK**.
8. In the **Password:** and **Confirm password:** fields, type the selected account’s password, and click **OK**.
9. Click **OK** three more times.
10. Right-click **Print Spooler** and click **Restart**.
11. When the service is restarted, a dialog box similar to the following should appear.



Revert Changes to the Printer Spooler Service

1. From any member server or workstation affected by the GPO changes, log on locally.
2. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
3. In the **Search** box, type **services**, and click **Services**.
4. Locate and double-click **Print Spooler**.
5. Click the **Log On** tab.
6. In the **Log on as:** field, click **Local System account**, and click **OK**.

Appendix H: Securing Local Administrator Accounts and Groups

On all versions of Windows currently in mainstream support, the local Administrator account is disabled by default, which makes the account unusable for pass-the-hash and other credential theft attacks. However, in environments that contain legacy

operating systems or in which local Administrator accounts have been enabled, these accounts can be used as previously described to propagate compromise across member servers and workstations. Each local Administrator account and group should be secured as described in the step-by-step instructions that follow.

For detailed information about considerations in securing Built-in Administrator (BA) groups, see Securing Local Administrator Accounts in this document.

Controls for Local Administrator Accounts

For the local Administrator account in each domain in your forest, you should configure the following settings:

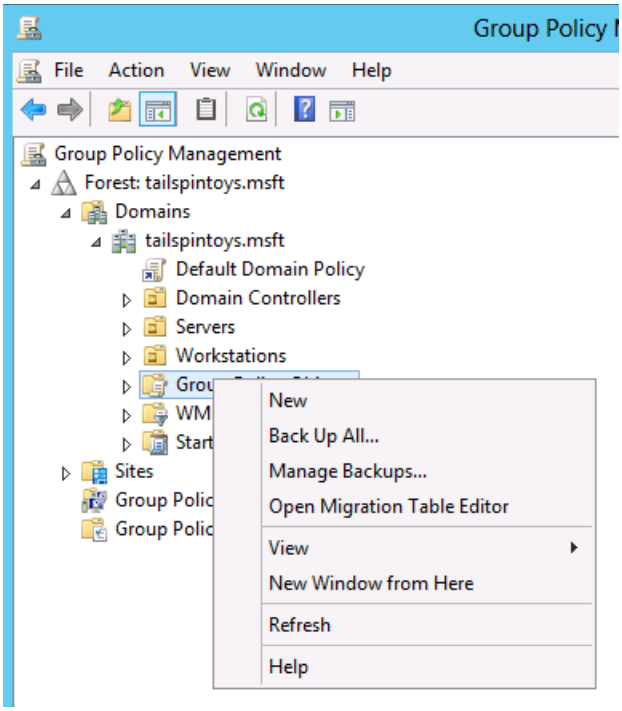
- Configure GPOs to restrict the domain's Administrator account's use on domain-joined systems
    - In one or more GPOs that you create and link to workstation and member server OUs in each domain, add the Administrator account to the following user rights in **Computer Configuration\Policies\Windows Settings\Security Settings\Local Settings\User Rights Assignments**:
        - Deny access to this computer from the network
        - Deny log on as a batch job
        - Deny log on as a service
        - Deny log on through Remote Desktop Services

Step-by-Step Instructions to Secure Local Administrators Groups

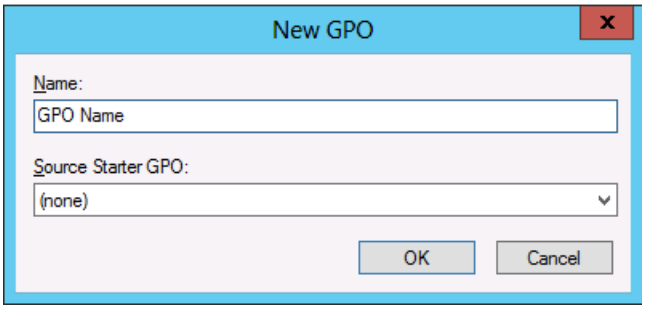
Configuring GPOs to Restrict Administrator Account on Domain-Joined Systems

1. In **Server Manager**, click **Tools**, and click **Group Policy Management**.
2. In the console tree, expand <Forest>\Domains\<Domain>, and then **Group Policy Objects** (where <Forest> is the name of the forest and <Domain> is the name of the domain where you want to set the Group Policy).

3. In the console tree, right-click **Group Policy Objects**, and click **New**.

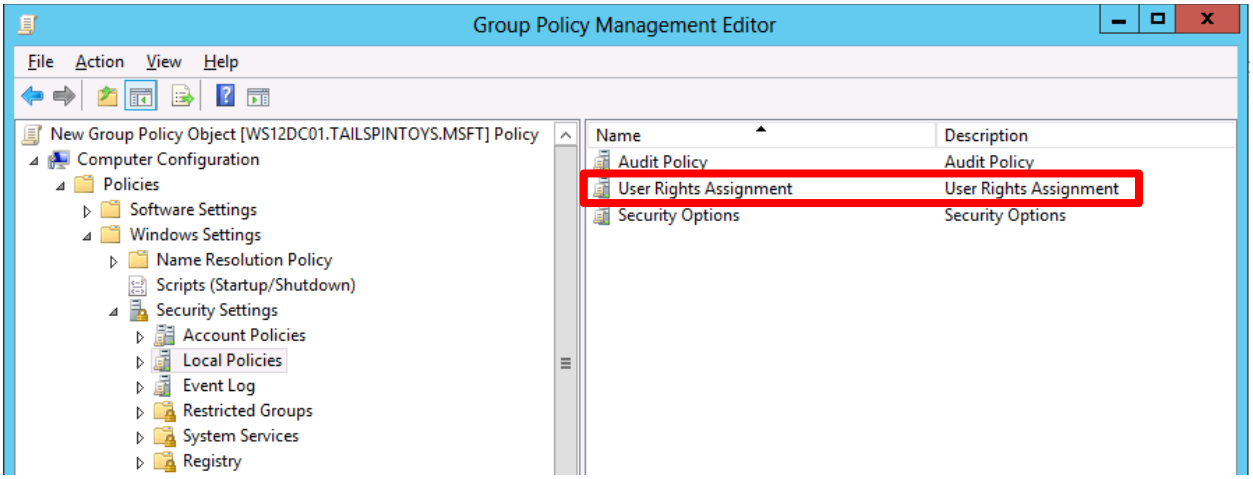


4. In the **New GPO** dialog box, type <GPO Name>, and click **OK** (where <GPO Name> is the name of this GPO).



5. In the details pane, right-click <GPO Name>, and click **Edit**.

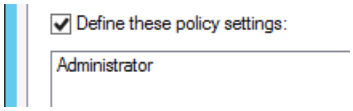
6. Navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies**, and click **User Rights Assignment**.



7. Configure the user rights to prevent the local Administrator account from accessing members servers and workstations over the network by doing the following:

    a. Double-click **Deny access to this computer from the network** and select **Define these policy settings**.

    b. Click **Add User or Group…**, type the user name of the local Administrator account, and click **OK**. This user name will be **Administrator**, the default when Windows is installed.



    c. Click **OK**.

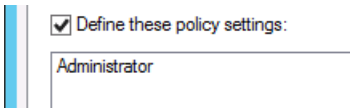
> **Important**
>
> When you add the Administrator account to these settings, you specify whether you are configuring a local Administrator account or a domain Administrator account by how you label the accounts. For example, to add the TAILSPINTOYS domain's Administrator account to these deny rights, you would browse to the Administrator account for the TAILSPINTOYS domain, which would appear as TAILSPINTOYS\Administrator. If you type **Administrator** in these user rights settings in the Group Policy Object Editor, you will restrict the local

> Administrator account on each computer to which the GPO is applied, as described earlier.

8. Configure the user rights to prevent the local Administrator account from logging on as a batch job by doing the following:

    a. Double-click **Deny log on as a batch job** and select **Define these policy settings**.

    b. Click **Add User or Group…**, type the user name of the local Administrator account, and click **OK**. This user name will be **Administrator**, the default when Windows is installed.

    c. Click **OK**.

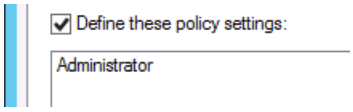
    Important

    When you add the Administrator account to these settings, you specify whether you are configuring local Administrator account or domain Administrator account by how you label the accounts. For example, to add the TAILSPINTOYS domain's Administrator account to these deny rights, you would browse to the Administrator account for the TAILSPINTOYS domain, which would appear as TAILSPINTOYS\Administrator. If you type **Administrator** in these user rights settings in the Group Policy Object Editor, you will restrict the local Administrator account on each computer to which the GPO is applied, as described earlier.

9. Configure the user rights to prevent the local Administrator account from logging on as a service by doing the following:

    a. Double-click **Deny log on as a service** and select **Define these policy settings**.

    b. Click **Add User or Group…**, type the user name of the local Administrator account, and click **OK**. This user name will be **Administrator**, the default when Windows is installed.

    c. Click **OK**.

    Important

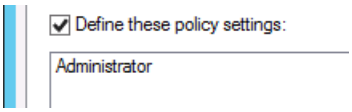
    When you add the Administrator account to these settings, you specify whether you are configuring local Administrator account or domain Administrator account by how you label the accounts. For example, to

> add the TAILSPINTOYS domain's Administrator account to these deny rights, you would browse to the Administrator account for the TAILSPINTOYS domain, which would appear as TAILSPINTOYS\Administrator. If you type **Administrator** in these user rights settings in the Group Policy Object Editor, you will restrict the local Administrator account on each computer to which the GPO is applied, as described earlier.

10. Configure the user rights to prevent the local Administrator account from accessing member servers and workstations via Remote Desktop Services by doing the following:

    a. Double-click **Deny log on through Remote Desktop Services** and select **Define these policy settings**.

    b. Click **Add User or Group…**, type the user name of the local Administrator account, and click **OK**. This user name will be **Administrator**, the default when Windows is installed.

    c. Click **OK**.

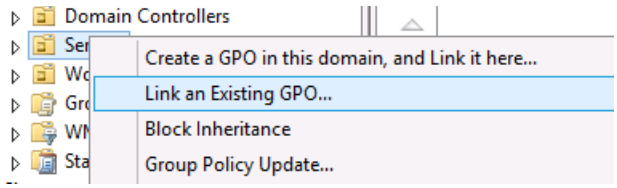
> **Important**
>
> When you add the Administrator account to these settings, you specify whether you are configuring local Administrator account or domain Administrator account by how you label the accounts. For example, to add the TAILSPINTOYS domain's Administrator account to these deny rights, you would browse to the Administrator account for the TAILSPINTOYS domain, which would appear as TAILSPINTOYS\Administrator. If you type **Administrator** in these user rights settings in the Group Policy Object Editor, you will restrict the local Administrator account on each computer to which the GPO is applied, as described earlier.

11. To exit **Group Policy Management Editor**, click **File**, and click **Exit**.

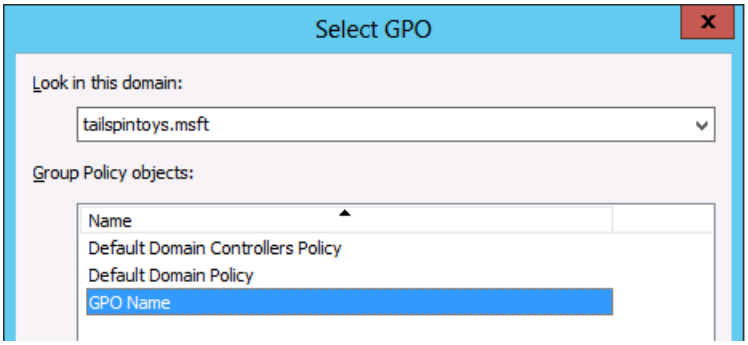
12. In **Group Policy Management**, link the GPO to the member server and workstation OUs by doing the following:

    a. Navigate to the <Forest>\Domains\<Domain> (where <Forest> is the name of the forest and <Domain> is the name of the domain where you want to set the Group Policy).

    b. Right-click the OU that the GPO will be applied to and click **Link an existing GPO…**.



c. Select the GPO that you only created and click **OK**.



d. Create links to all other OUs that contain workstations.

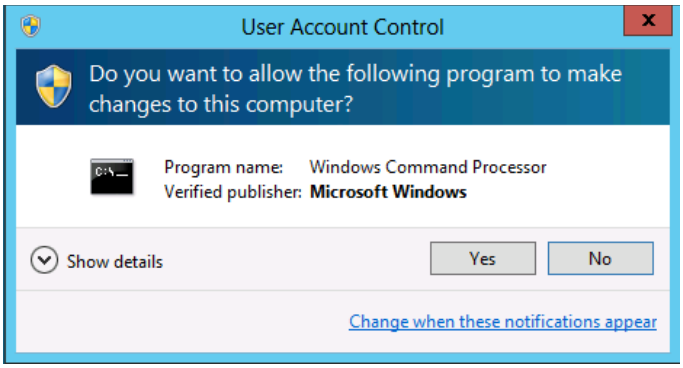
e. Create links to all other OUs that contain member servers.

Verification Steps

Verify “Deny access to this computer from the network” GPO Settings

From any member server or workstation that is not affected by the GPO changes (such as a jump server), attempt to access a member server or workstation over the network that is affected by the GPO changes. To verify the GPO settings, attempt to map the system drive by using the **NET USE** command.

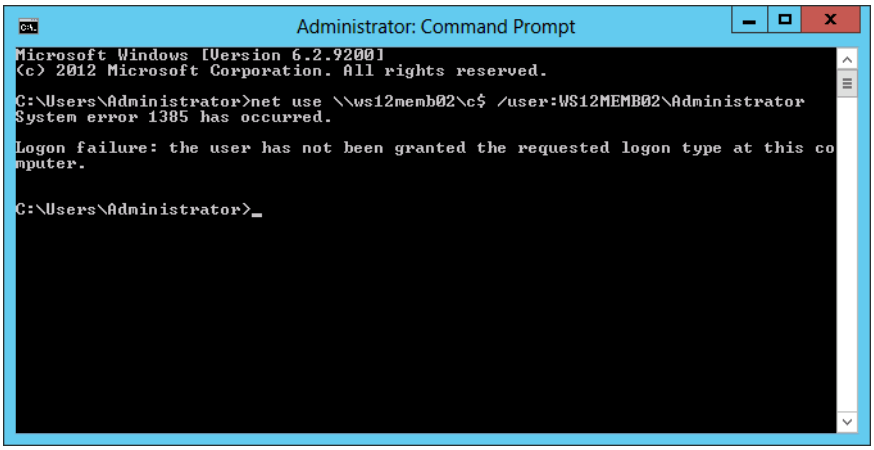
1. Log on locally to any member server or workstation that is not affected by the GPO changes.
2. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
3. In the **Search** box, type **command prompt**, right-click **Command Prompt**, and then click **Run as administrator** to open an elevated command prompt.
4. When prompted to approve the elevation, click **Yes**.



5. In the **Command Prompt** window, type **net use \\<Server Name>\c$ /user:<Server Name>\Administrator**, where <Server Name> is the name of the member server or workstation you're attempting to access over the network.

> **Note**
>
> The local Administrator credentials must be from the same system you're attempting to access over the network.

6. The following screenshot shows the error message that should appear.



Verify "Deny log on as a batch job" GPO Settings

1. From any member server or workstation affected by the GPO changes, log on locally.

Create a Batch File

2. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
3. In the **Search** box, type **notepad**, and click **Notepad**.
4. In **Notepad,** type **dir c:**.

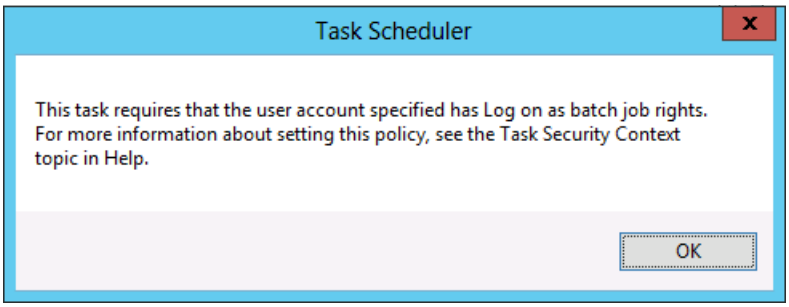
5. Click **File**, and click **Save As…**.
6. In the **File name** box, type <Filename>.bat (where <Filename> is the name of the new batch file).

Schedule a Task

7. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
8. In the **Search** box, type **task scheduler**, and click **Task Scheduler**.

> **Note**
>
> On computers running Windows 8, in the **Search** box, type **schedule tasks**, and click **Schedule tasks**.

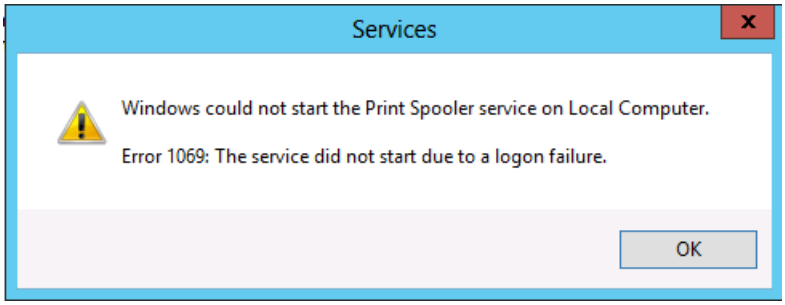
9. Click **Action**, and click **Create Task…**.
10. In the **Create Task** dialog box, type <Task Name> (where <Task Name> is the name of the new task).
11. Click the **Actions** tab, and click **New…**.
12. In the **Action:** field, click **Start a program**.
13. In the **Program/script:** field, click **Browse…**, locate and select the batch file created in the **Create a Batch File** section, and click **Open**.
14. Click **OK**.
15. Click the **General** tab.
16. In the **Security options** field, click **Change User or Group…**.
17. Type the name of the system's local Administrator account, click **Check Names**, and click **OK**.
18. Select **Run whether the user is logged on or not** and **Do not store password. The task will only have access to local computer resources**.
19. Click **OK**.
20. A dialog box should appear, requesting user account credentials to run the task.
21. After entering the credentials, click **OK**.
22. A dialog box similar to the following should appear.



Verify “Deny log on as a service” GPO Settings

1. From any member server or workstation affected by the GPO changes, log on locally.
2. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
3. In the **Search** box, type **services**, and click **Services**.
4. Locate and double-click **Print Spooler**.
5. Click the **Log On** tab.
6. In **Log on as:** field, click **This account**.
7. Click **Browse…**, type the system’s local Administrator account, click **Check Names**, and click **OK**.
8. In the **Password:** and **Confirm password:** fields, type the selected account’s password, and click **OK**.
9. Click **OK** three more times.
10. Right-click **Print Spooler** and click **Restart**.

11. When the service is restarted, a dialog box similar to the following should appear.

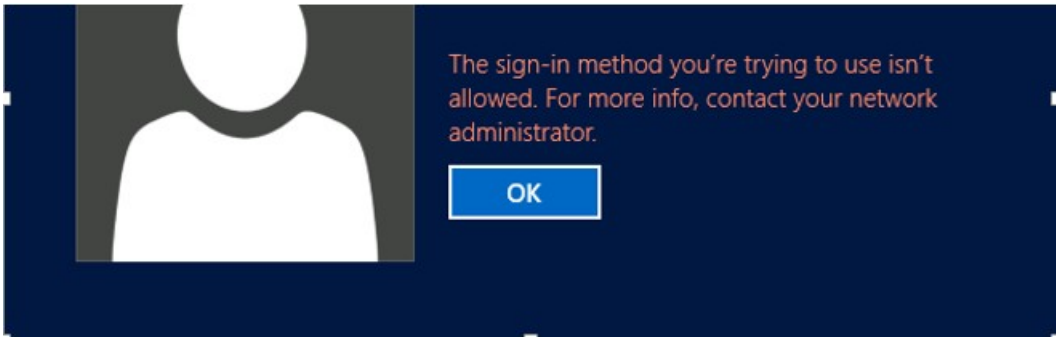


Revert Changes to the Printer Spooler Service

1. From any member server or workstation affected by the GPO changes, log on locally.
2. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
3. In the **Search** box, type **services**, and click **Services**.
4. Locate and double-click **Print Spooler**.
5. Click the **Log On** tab.
6. In the **Log on as:** field, select **Local System account**, and click **OK**.

Verify “Deny log on through Remote Desktop Services” GPO Settings

1. With the mouse, move the pointer into the upper-right or lower-right corner of the screen. When the **Charms** bar appears, click **Search**.
2. In the **Search** box, type **remote desktop connection**, and click **Remote Desktop Connection**.
3. In the **Computer** field, type the name of the computer that you want to connect to, and click **Connect**. (You can also type the IP address instead of the computer name.)
4. When prompted, provide credentials for the system's local Administrator account.
5. A dialog box similar to the following should appear.



Appendix I: Creating Management Accounts for Protected Accounts and Groups in Active Directory

One of the challenges in implementing an Active Directory model that does not rely on permanent membership in highly privileged groups is that there must be a mechanism to populate these groups when temporary membership in the groups is required. Some privileged identity management solutions require that the software's service accounts are granted permanent membership in groups such as DA or Administrators in each domain in the forest. However, it is technically not necessary for Privileged Identity Management (PIM) solutions to run their services in such highly privileged contexts.

This appendix provides information that you can use for natively implemented or third-party PIM solutions to create accounts that have limited privileges and can be stringently controlled, but can be used to populate privileged groups in Active Directory when temporary elevation is required. If you are implementing PIM as a native solution, these accounts may be used by administrative staff to perform the temporary group population, and if you're implementing PIM via third-party software, you might be able to adapt these accounts to function as service accounts.

> **Note**
>
> The procedures described in this appendix provide one approach to the management of highly privileged groups in Active Directory. You can adapt these procedures to suit your needs, add additional restrictions, or omit some of the restrictions that are described here.

Creating Management Accounts for Protected Accounts and Groups in Active Directory

Creating accounts that can be used to manage the membership of privileged groups without requiring the management accounts to be granted excessive rights and permissions consists of four general activities that are described in the step-by-step instructions that follow:

1. First, you should create a group that will manage the accounts, because these accounts should be managed by a limited set of trusted users. If you do not already have an OU structure that accommodates segregating privileged and protected accounts and systems from the general population in the domain, you should create one. Although specific instructions are not provided in this appendix, screenshots show an example of such an OU hierarchy.
2. Create the management accounts. These accounts should be created as "regular" user accounts and granted no user rights beyond those that are already granted to users by default.

3. Implement restrictions on the management accounts that make them usable only for the specialized purpose for which they were created, in addition to controlling who can enable and use the accounts (the group you created in the first step).
4. Configure permissions on the AdminSDHolder object in each domain to allow the management accounts to change the membership of the privileged groups in the domain.

You should thoroughly test all of these procedures and modify them as needed for your environment before implementing them in a production environment. You should also verify that all settings work as expected (some testing procedures are provided in this appendix), and you should test a disaster recovery scenario in which the management accounts are not available to be used to populate protected groups for recovery purposes. For more information about backing up and restoring Active Directory, see the AD DS Backup and Recovery Step-by-Step Guide.

> **Note**
>
> By implementing the steps described in this appendix, you will create accounts that will be able to manage the membership of all protected groups in each domain, not only the highest-privilege Active Directory groups like EAs, DAs and BAs. For more information about protected groups in Active Directory, see Appendix C: Protected Accounts and Groups in Active Directory.

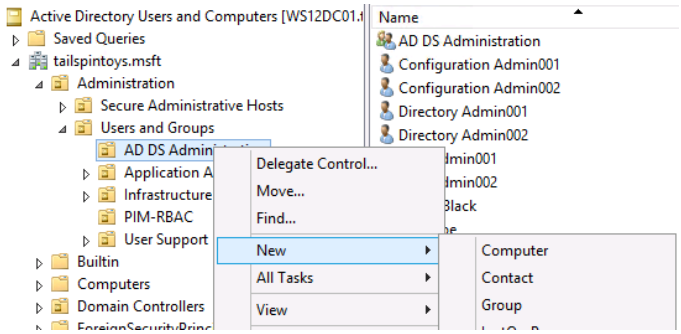
Step-by-Step Instructions for Creating Management Accounts for Protected Groups

Creating a Group to Enable and Disable Management Accounts

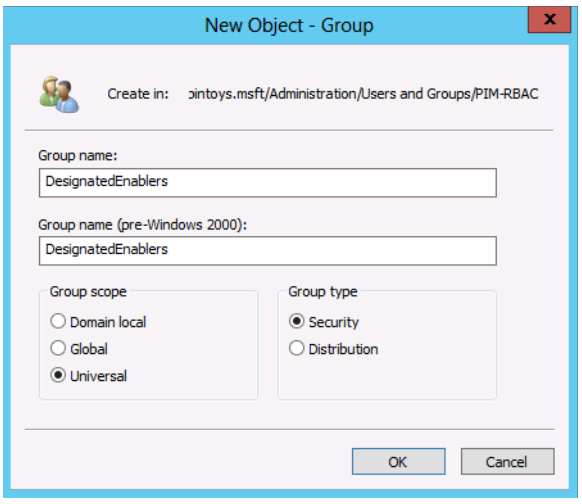
Management accounts should have their passwords reset at each use and should be disabled when activities requiring them are complete. Although you might also consider implementing smart card logon requirements for these accounts, it is an optional configuration and these instructions assume that the management accounts will be configured with a user name and long, complex password as minimum controls. In this step, you will create a group that has permissions to reset password on the management accounts and to enable and disable the accounts.

To create a group to enable and disable management accounts, perform the following steps:

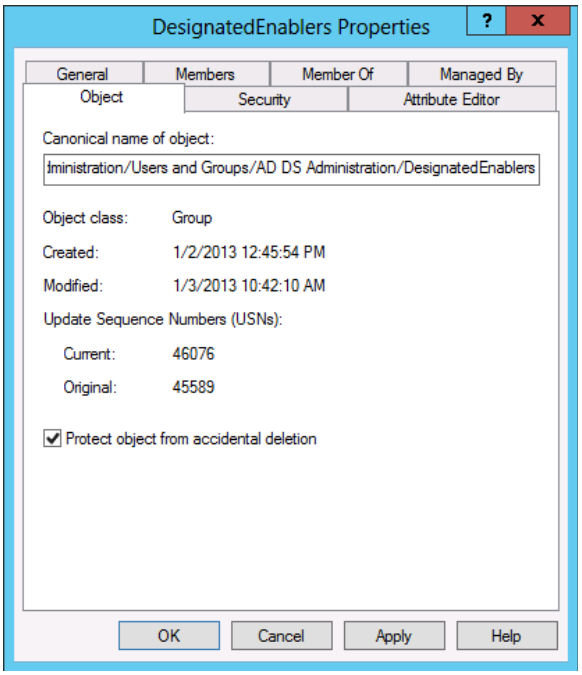
1. In the OU structure where you will be housing the management accounts, right-click the OU where you want to create the group, click **New** and click **Group**.



2. In the **New Object – Group** dialog box, enter a name for the group. If you plan to use this group to “activate” all management accounts in your forest, make it a universal security group. If you have a single-domain forest or if you plan to create a group in each domain, you can create a global security group. Click **OK** to create the group.

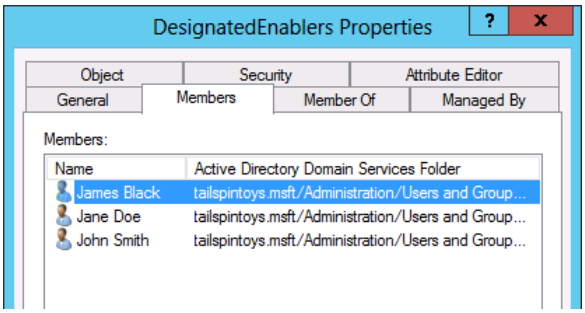


3. Right-click the group you just created, click **Properties**, and click the **Object** tab. In the group's **Object property** dialog box, select **Protect object from accidental deletion**, which will not only prevent otherwise-authorized users from deleting the group, but also from moving it to another OU unless the attribute is first deselected.

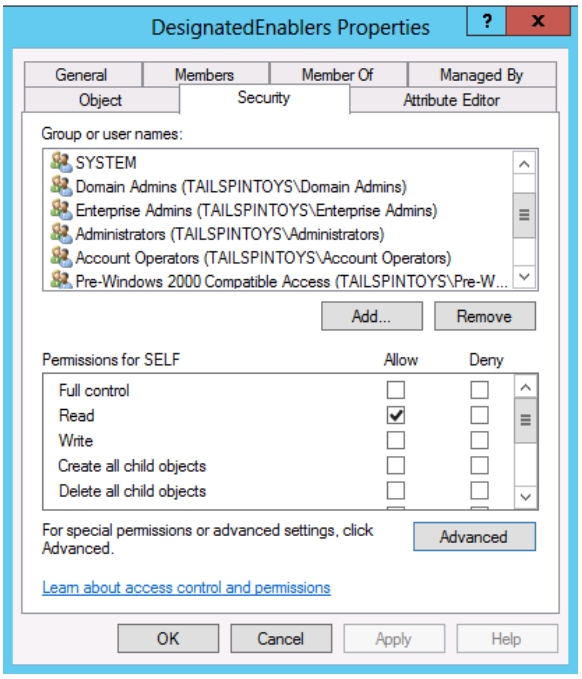


> **Note**
>
> If you have already configured permissions on the group's parent OUs to restrict administration to a limited set of users, you may not need to perform the following steps. They are provided here so that even if you have not yet implemented limited administrative control over the OU structure in which you've created this group, you can secure the group against modification by unauthorized users.

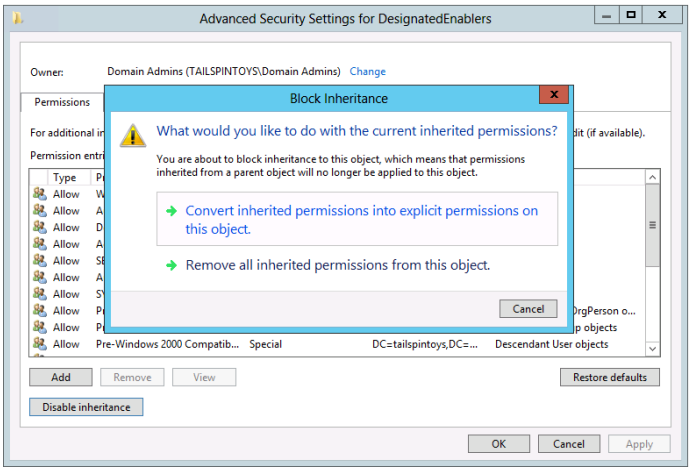
4. Click the **Members** tab, and add the accounts for members of your team who will be responsible for enabling management accounts or populating protected groups when necessary.



5. If you have not already done so, in the **Active Directory Users and Computers** console, click **View** and select **Advanced Features**. Right-click the group you just created, click **Properties**, and click the **Security** tab. On the security tab, click **Advanced**.



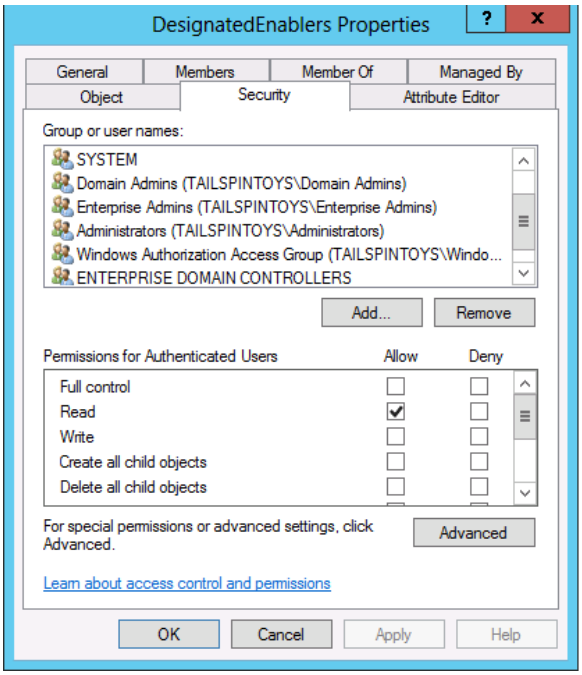
6. In the **Advanced Security Settings for [Group]** dialog box, click **Disable Inheritance**. When prompted, click **Convert inherited permissions into explicit permissions on this object**, and click **OK** to return to the group's Security dialog box.



7. On the **Security** tab, remove groups that should not be permitted to access this group. For example, if you do not want Authenticated Users to be able to read the group's name and general properties, you can remove that ACE. You can also remove ACEs, such as those for account operators and pre-Windows 2000 Server compatible access. You should, however, leave a minimum set of object permissions in place. Leave the following ACEs intact:

    - SELF
    - SYSTEM
    - Domain Admins
    - Enterprise Admins
    - Administrators
    - Windows Authorization Access Group (if applicable)
    - ENTERPRISE DOMAIN CONTROLLERS

    Although it may seem counterintuitive to allow the highest privileged groups in Active Directory to manage this group, your goal in implementing these settings is not to prevent members of those groups from making authorized changes. Rather, the goal is to ensure that when you have occasion to require very high levels of privilege, authorized changes will succeed. It is for this reason that changing default privileged group nesting, rights, and permissions are discouraged throughout this document. By leaving default structures intact and emptying the membership of the highest privilege groups in the directory, you can create a more secure environment that still functions as expected.



> **Note**
>
> If you have not already configured audit policies for the objects in the OU structure where you created this group, you should configure auditing to log changes this group.

8. You have completed configuration of the group that will be used to “check out” management accounts when they are needed and “check in” the accounts when their activities have been completed.

Creating the Management Accounts

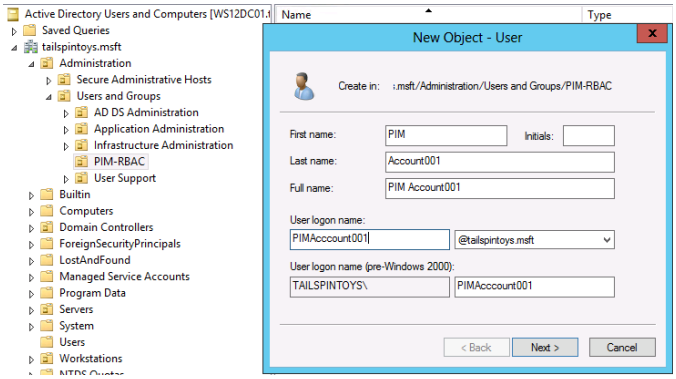
You should create at least one account that will be used to manage the membership of privileged groups in your Active Directory installation, and preferably a second account to serve as a backup. Whether you choose to create the management accounts in a single domain in the forest and grant them management capabilities for all domains’ protected groups, or whether you choose to implement management accounts in each domain in the forest, the procedures are effectively the same.

> **Note**
>
> The steps in this document assume that you have not yet implemented role-based access controls and privileged identity management for Active Directory. Therefore, some procedures must be performed by a user whose account is a member of the Domain Admins group for the domain in question.

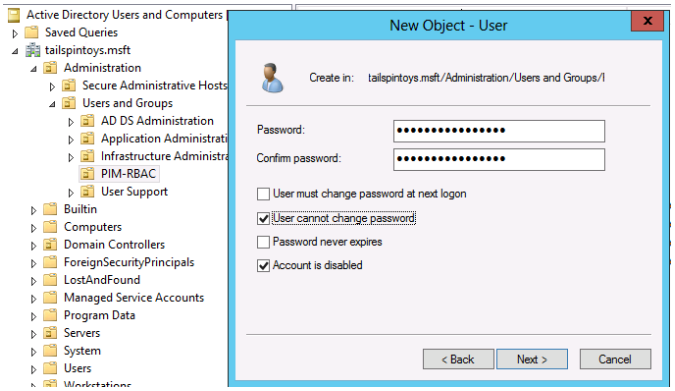
> When you are using an account with DA privileges, you can log on to a domain controller to perform the configuration activities. Steps that do not require DA privileges can be performed by less-privileged accounts that are logged on to administrative workstations. Screen shots that show dialog boxes bordered in the lighter blue color represent activities that can be performed on a domain controller. Screen shots that show dialog boxes in the darker blue color represent activities that can be performed on administrative workstations with accounts that have limited privileges.

To create the management accounts, perform the following steps:

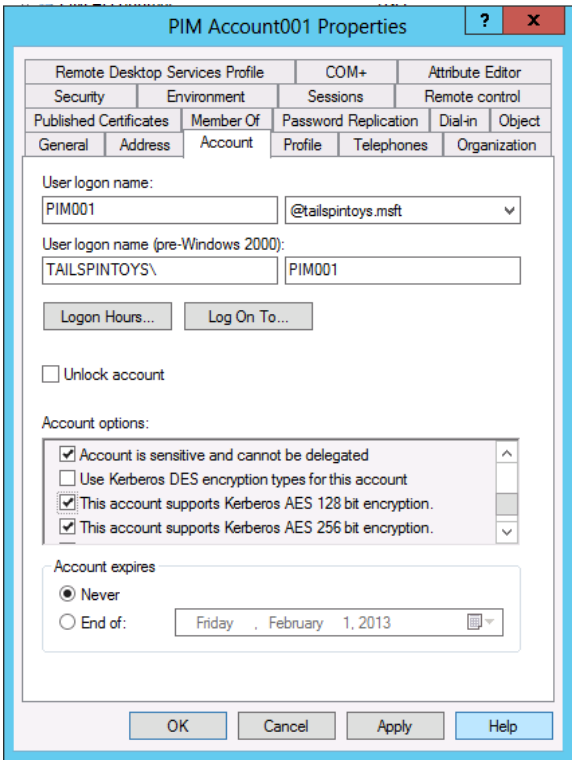
1. Log on to a domain controller with an account that is a member of the domain's DA group.
2. Launch **Active Directory Users and Computers** and navigate to the OU where you will be creating the management account.
3. Right-click the OU and click **New** and click **User**.
4. In the **New Object – User** dialog box, enter your desired naming information for the account and click **Next**.
5. Log on to a domain controller with an account that is a member of the domain's DA group.
6. Launch **Active Directory Users and Computers** and navigate to the OU where you will be creating the management account.
7. Right-click the OU and click **New** and click **User**.
8. In the **New Object – User** dialog box, enter your desired naming information for the account and click **Next**.



9. Provide an initial password for the user account, clear **User must change password at next logon**, select **User cannot change password** and **Account is disabled**, and click **Next**.



10. Verify that the account details are correct and click **Finish**.
11. Right-click the user object you just created and click **Properties**.
12. Click the **Account** tab.
13. In the **Account Options** field, select the **Account is sensitive and cannot be delegated** flag, select the **This account supports Kerberos AES 128 bit encryption** and/or the **This account supports Kerberos AES 256 encryption** flag, and click **OK**.



Note

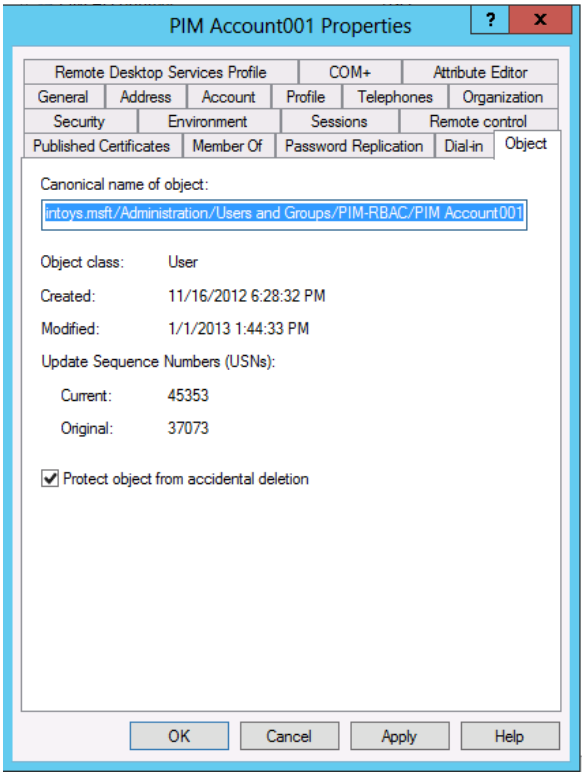
Because this account, like other accounts, will have a limited, but powerful function, the account should only be used on secure administrative hosts. For all secure administrative hosts in your environment, you should consider implementing the Group Policy setting **Network Security: Configure Encryption types allowed for Kerberos** to allow only the most secure encryption types you can implement for secure hosts.

Although implementing more secure encryption types for the hosts does not mitigate credential theft attacks, the appropriate use and configuration of the secure hosts does. Setting stronger encryption types for hosts that are only used by privileged accounts simply reduces the overall attack surface of the computers.

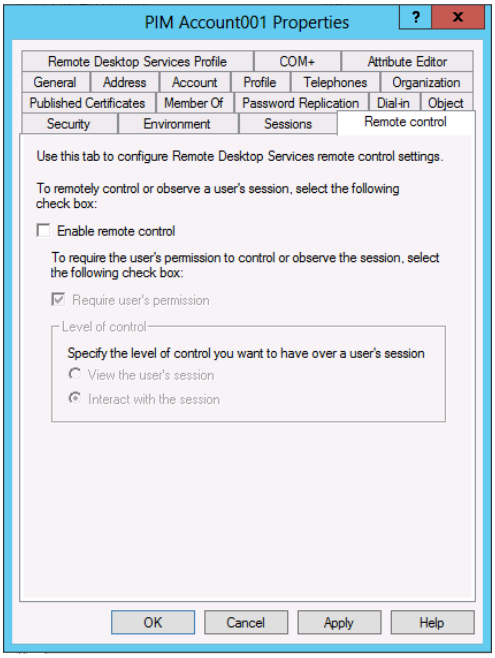
For more information about configuring encryption types on systems and accounts, see Windows Configurations for Kerberos Supported Encryption Type.

Note These settings are supported only on computers running Windows Server 2012, Windows Server 2008 R2, Windows 8, or Windows 7.

14. On the **Object** tab, select **Protect object from accidental deletion**. This will not only prevent the object from being deleted (even by authorized users), but will prevent it from being moved to a different OU in your AD DS hierarchy, unless the checkbox is first cleared by a user with permission to change the attribute.

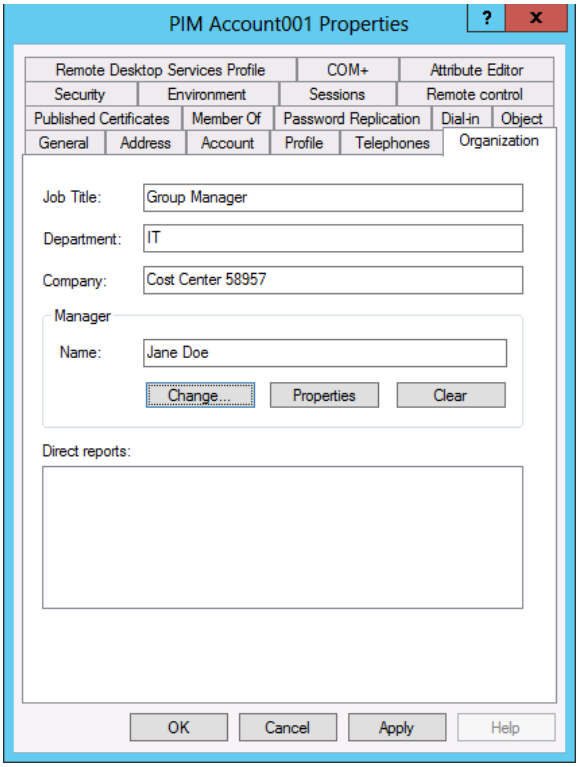


15. Click the Remote control tab.
16. Clear the **Enable remote control** flag. It should never be necessary for support staff to connect to this account's sessions to implement fixes.

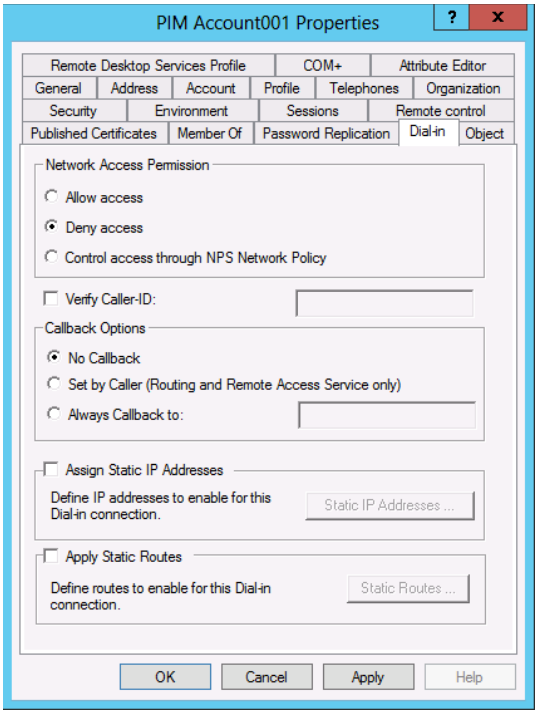


> **Note**
>
> Every object in Active Directory should have a designated IT owner and a designated business owner, as described in Creating Business-Centric Security Practices for Active Directory. If you are tracking ownership of AD DS objects in Active Directory (as opposed to an external database), you should enter appropriate ownership information in this object's properties.
>
> In this case, the business owner is most likely an IT division, andthere is no prohibition on business owners also being IT owners. The point of establishing ownership of objects is to allow you to identify contacts when changes need to be made to the objects, perhaps years from their initial creation.

17. Click on the **Organization** tab.
18. Enter any information that is required in your AD DS object standards.



19. Click on the **Dial-in** tab.
20. In the **Network Access Permission** field, select **Deny access**.This account should never need to connect over a remote connection.

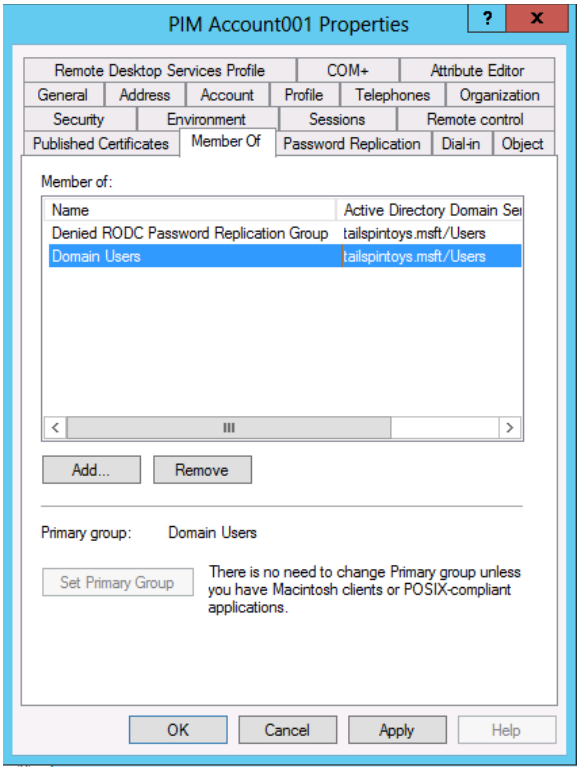


Note

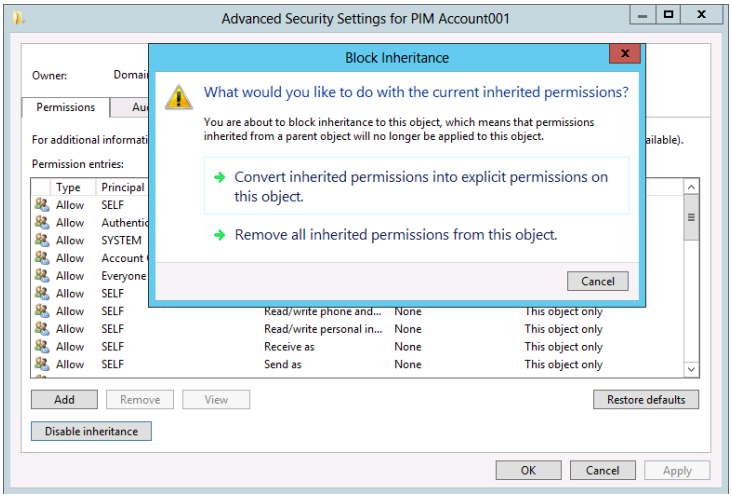
It is unlikely that this account will be used to log on to read-only domain controllers (RODCs) in your environment. However, should circumstance ever require the account to log on to an RODC, you should add this account to the Denied RODC Password Replication Group so that its password is not cached on the RODC.

Although the account's password should be reset after each use and the account should be disabled, implementing this setting does not have a deleterious effect on the account, and it might help in situations in which an administrator forgets to reset the account's password and disable it.

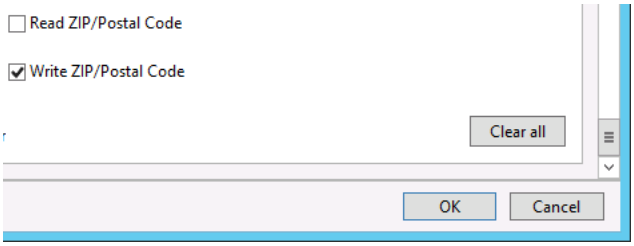
21. Click the **Member Of** tab.
22. Click **Add…**.
23. Type **Denied RODC Password Replication Group** in the **Select Users, Contacts, Computers…** dialog box and click **Check Names**. When the name of the group is underlined in the object picker, click **OK** and verify that the account is now a member of the two groups displayed in the following screenshot. Do not add the account to any protected groups.
24. Click **OK**.



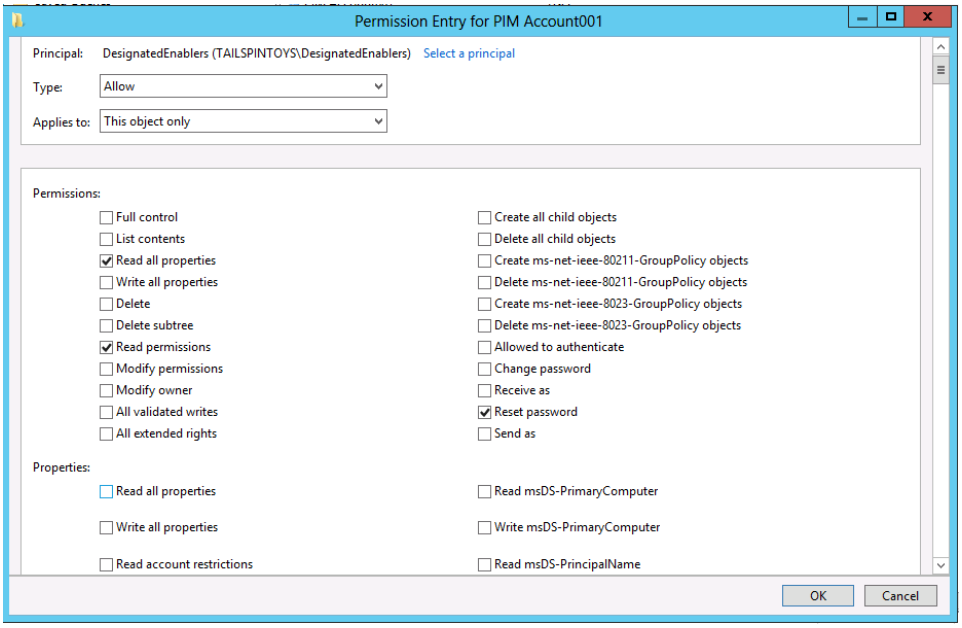
25. Click the **Security** tab and click **Advanced**.
26. In the **Advanced Security Settings** dialog box, click **Disable inheritance** and copy the inherited permissions as explicit permissions, and click **Add**.



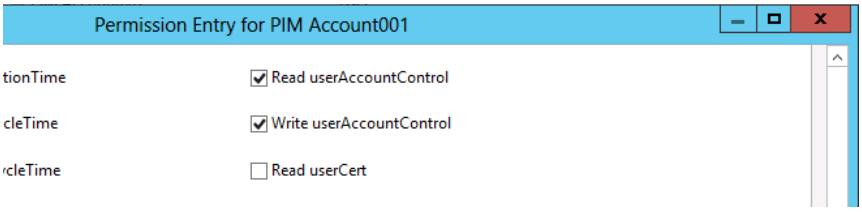
27. In the **Permission Entry for [Account]** dialog box, click **Select a principal** and add the group you created in the previous procedure. Scroll to the bottom of the dialog box and click **Clear all** to remove all default permissions.



28. Scroll to the top of the **Permission Entry** dialog box. Ensure that the **Type** drop-down list is set to **Allow**, and in the **Applies to** drop-down list, select **This object only**.
29. In the **Permissions** field, select **Read all properties**, **Read permissions**, and **Reset password**.

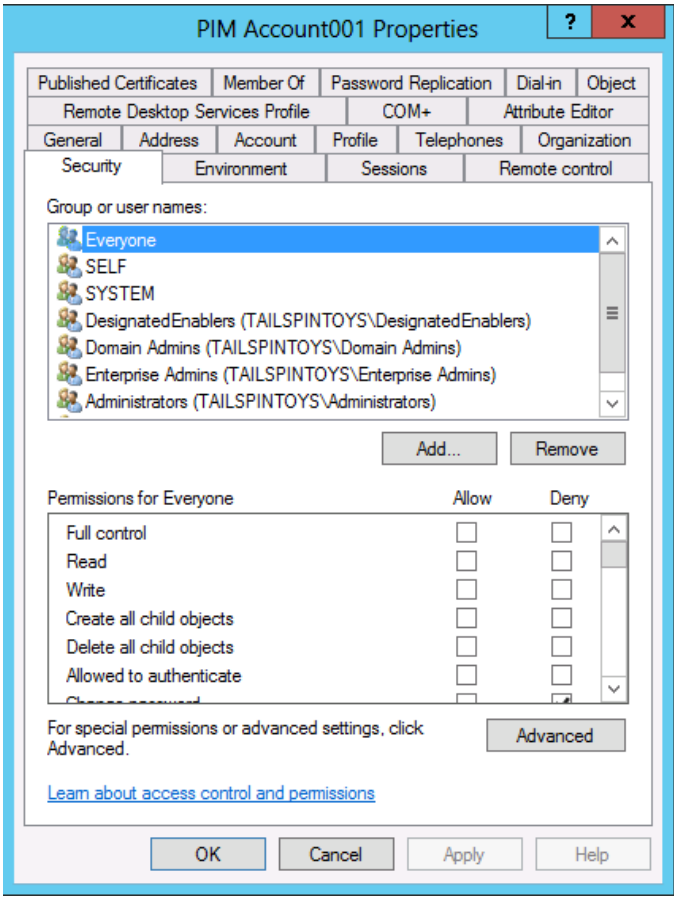


30. In the **Properties** field, select **Read userAccountControl** and **Write userAccountControl**.
31. Click **OK**, **OK** again in the **Advanced Security Settings** dialog box.

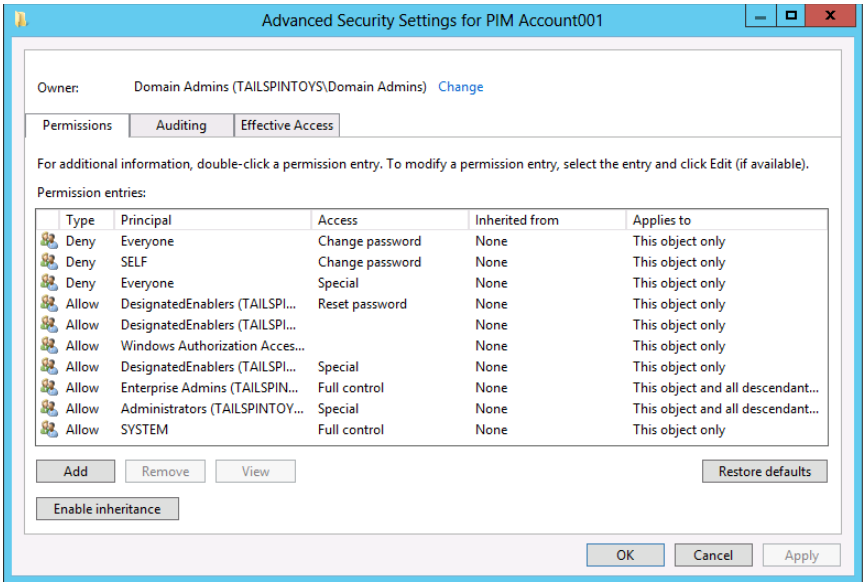


> **Note**
>
> The **userAccountControl** attribute controls multiple account configuration options. You cannot grant permission to change only some of the configuration options when you grant write permission to the attribute.

32. In the **Group or user names** field of the **Security** tab, remove any groups that should not be permitted to access or manage the account. Do not remove any groups that have been configured with Deny ACEs, such as the Everyone group and the SELF computed account (that ACE was set when the **user cannot change password** flag was enabled during creation of the account. Also do not remove the group you just added, the SYSTEM account, or groups such as EA, DA, BA, or the Windows Authorization Access Group.



33. Click **Advanced** and verify that the Advanced Security Settings dialog box looks similar to the following screenshot.
34. Click **OK**, and **OK** again to close the account's property dialog box.



35. Setup of the first management account is now complete. You will test the account in a later procedure.

Creating Additional Management Accounts

You can create additional management accounts by repeating the previous steps, by copying the account you just created, or by creating a script to create accounts with your desired configuration settings. Note, however, that if you copy the account you just created, many of the customized settings and ACLs will not be copied to the new account and you will have to repeat most of the configuration steps.

You can instead create a group to which you delegate rights to populate and unpopulate protected groups, but you will need to secure the group and the accounts you place in it. Because there should be very few accounts in your directory that are granted the ability to manage the membership of protected groups, creating individual accounts might be the simplest approach.

Regardless of how you choose to create a group into which you place the management accounts, you should ensure that each account is secured as described earlier. You should also consider implementing GPO restrictions similar to those described in Appendix D: Securing Built-in Administrator Accounts in Active Directory.

Auditing Management Accounts

You should configure auditing on the account to log, at minimum, all writes to the account. This will allow you to not only identify successful enabling of the account and resetting of its password during authorized uses, but to also identify attempts by unauthorized users to manipulate the account. Failed writes on the account should be captured in your Security Information and Event Monitoring (SIEM) system (if applicable), and should trigger alerts that provide notification to the staff responsible for investigating potential compromises.

SIEM solutions take event information from involved security sources (for example, event logs, application data, network streams, antimalware products, and intrusion detection sources), collate the data, and try to make intelligent views and proactive actions. There are many commercial SIEM solutions, and many enterprises create private implementations. A well designed and appropriately implemented SIEM can significantly enhance security monitoring and incident response capabilities. However, capabilities and accuracy vary tremendously between solutions. SIEMs are beyond the scope of this paper, but the specific event recommendations contained should be considered by any SIEM implementer.

For more information about recommended audit configuration settings for domain controllers, see Monitoring Active Directory for Signs of Compromise in this document. Domain controller-specific configuration settings are provided in Recommended Audit Policies by Operating System.

Enabling Management Accounts to Modify the Membership of Protected Groups

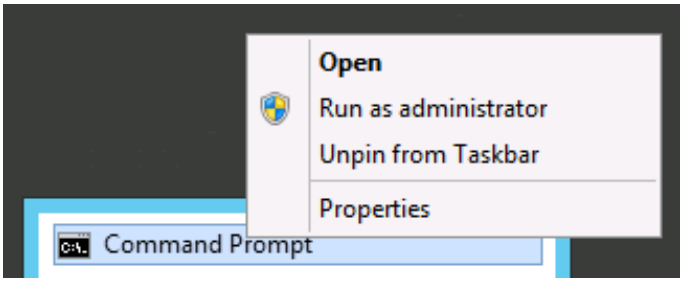
In this procedure, you will configure permissions on the domain's AdminSDHolder object to allow the newly created management accounts to modify the membership of protected groups in the domain. This procedure cannot be performed via a graphical user interface (GUI).

As discussed in Appendix C: Protected Accounts and Groups in Active Directory, the ACL on a domain's AdminSDHolder object is effectively "copied" to protected objects when the SDProp task runs. Protected groups and accounts do not inherit their permissions from the AdminSDHolder object; their permissions are explicitly set to match those on the AdminSDHolder object. Therefore, when you modify permissions on the AdminSDHolder object, you must modify them for attributes that are appropriate to the type of the protected object you are targeting.

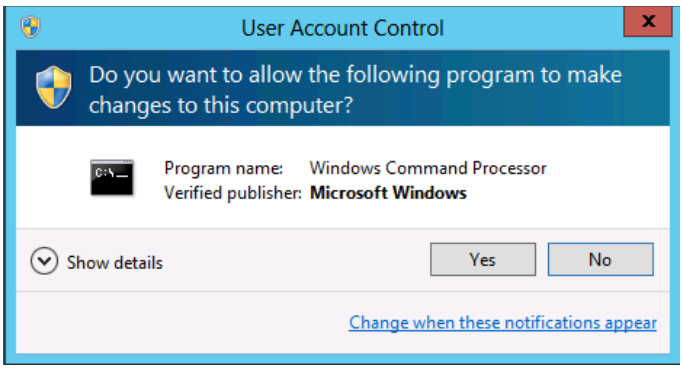
In this case, you will be granting the newly created management accounts to allow them to read and write the members attribute on group objects. However, the AdminSDHolder object is not a group object and group attributes are not exposed in the graphical ACL editor. It is for this reason that you will implement the permissions changes via the Dsacls command-line utility. To grant the (disabled) management accounts permissions to modify the membership of protected groups, perform the following steps:

1. Log on to a domain controller, preferably the domain controller holding the PDC Emulator (PDCE) role, with the credentials of a user account that has been made a member of the DA group in the domain.

2. Open an elevated command prompt by right-clicking **Command Prompt** and click **Run as administrator**.

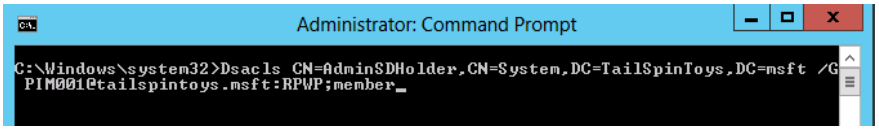


3. When prompted to approve the elevation, click **Yes**.



> **Note**
>
> For more information about elevation and user account control (UAC) in Windows, see UAC Processes and Interactions on the TechNet website.

4. At the Command Prompt, type (substituting your domain-specific information) **Dsacls [distinguished name of the AdminSDHolder object in your domain] /G [management account UPN]:RPWP;member**.



   The previous command (which is not case-sensitive) works as follows:

   - Dsacls sets or displays ACEs on directory objects
   - CN=AdminSDHolder,CN=System,DC=TailSpinToys,DC=msft identifies the object to be modified
   - /G indicates that a grant ACE is being configured
   - PIM001@tailspintoys.msft is the User Principal Name (UPN) of the security principal to which the ACEs will be granted
   - RPWP grants read property and write property permissions
   - Member is the name of the property (attribute) on which the permissions will be set

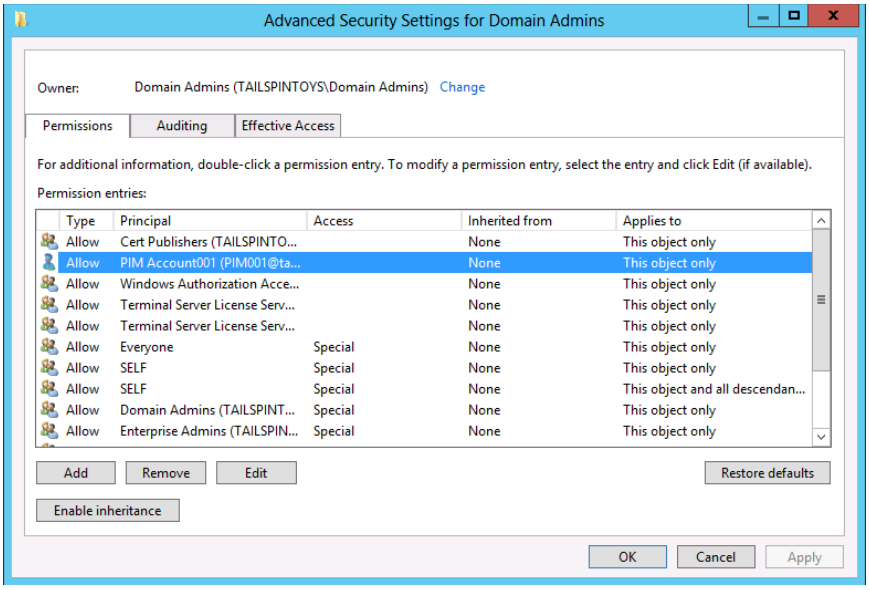
   For more information about use of Dsacls, type **Dsacls** without any parameters at a command prompt.

   If you have created multiple management accounts for the domain, you should run the Dsacls command for each account. When you have completed the ACL configuration on the AdminSDHolder object, you should force SDProp to run, or wait until its scheduled run completes. For information about forcing SDProp to run, see Running SDProp Manually in Appendix C: Protected Accounts and Groups in Active Directory.

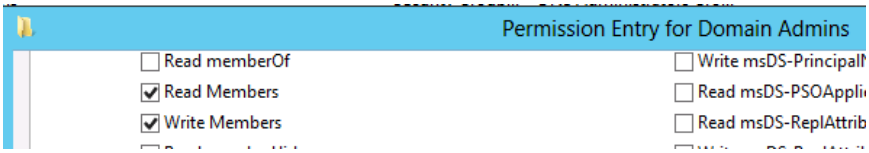
   When SDProp has run, you can verify that the changes you made to the AdminSDHolder object have been applied to protected groups in the domain. You cannot verify this by viewing the ACL on the AdminSDHolder object for the reasons previously described, but you can verify that the permissions have been applied by viewing the ACLs on protected groups.

5. In **Active Directory Users and Computers**, verify that you have enabled **Advanced Features.** To do so, click **View**, locate the **Domain Admins** group, right-click the group and click **Properties**.

6. Click the **Security** tab and click **Advanced** to open the **Advanced Security Settings for Domain Admins** dialog box.



7. Select **Allow ACE for the management account** and click **Edit**. Verify that the account has been granted only **Read Members** and **Write Members** permissions on the DA group, and click **OK**.
8. Click **OK** in the **Advanced Security Settings** dialog box, and click **OK** again to close the property dialog box for the DA group.



9. You can repeat the previous steps for other protected groups in the domain; the permissions should be the same for all protected groups. You have now completed creation and configuration of the management accounts for the protected groups in this domain.

> **Note**
>
> Any account that has permission to write membership of a group in Active Directory can also add itself to the group. This behavior is by design and cannot be disabled. For this reason, you should always keep management accounts disabled when not in use, and should closely monitor the accounts when they’re disabled and when they’re in use.

Verifying Group and Account Configuration Settings

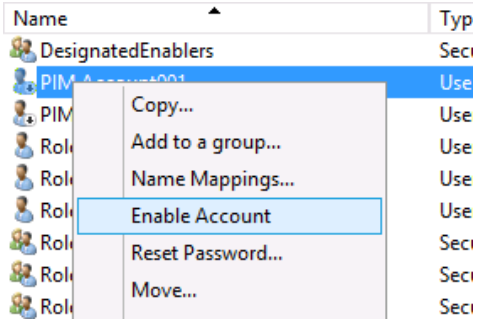
Now that you have created and configured management accounts that can modify the membership of protected groups in the domain (which includes the most highly privileged EA, DA, and BA groups), you should verify that the accounts and their management group have been created properly. Verification consists of these general tasks:

1. Test the group that can enable and disable management accounts to verify that members of the group can enable and disable the accounts and reset their passwords, but cannot perform other administrative activities on the management accounts.
2. Test the management accounts to verify that they can add and remove members to protected groups in the domain, but cannot change any other properties of protected accounts and groups.

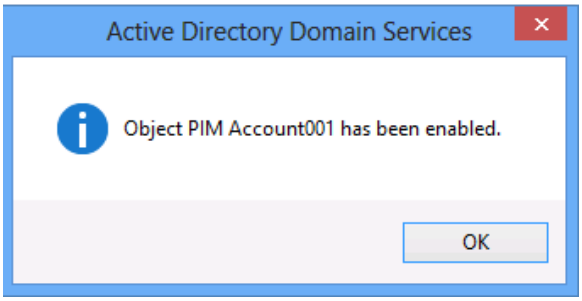
Test the Group that Will Enable and Disable Management Accounts

1. To test enabling a management account and resetting its password, log on to a secure administrative workstation with an account that is a member of the group you created in Creating a Group to Enable and Disable Management Accounts.

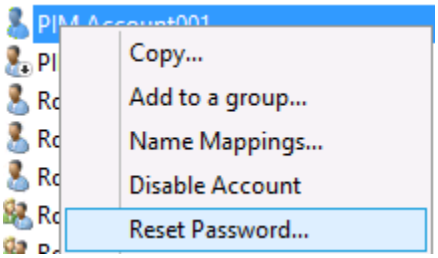
2. Open **Active Directory Users and Computers**, right-click the management account, and click **Enable Account**.



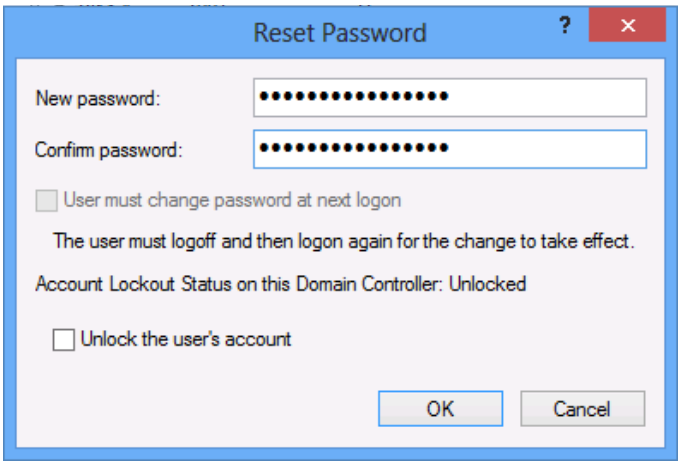
3. A dialog box should display, confirming that the account has been enabled.



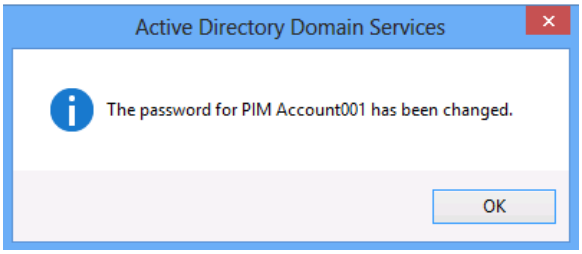
4. Next, reset the password on the management account. To do so, right-click the account again and click **Reset Password**.



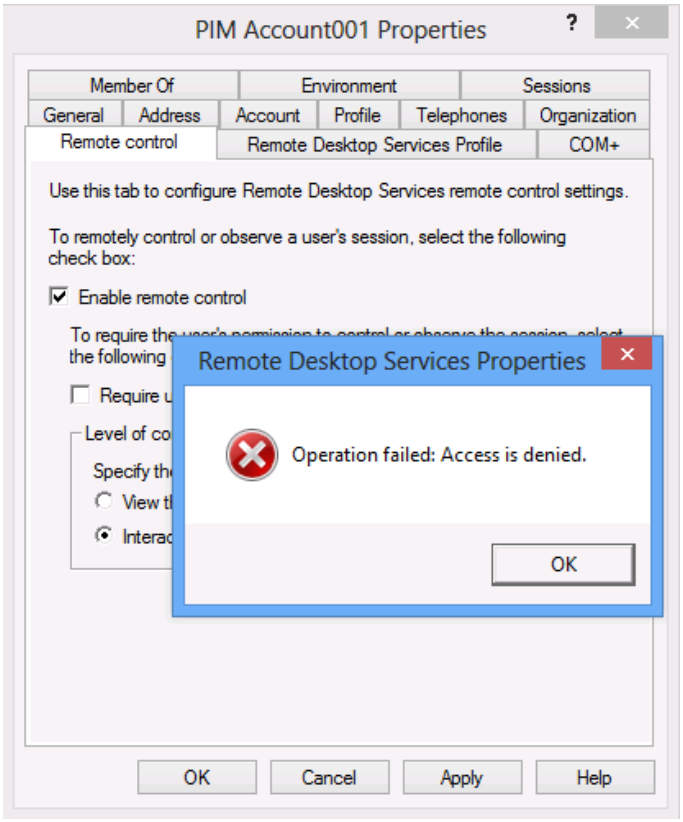
5. Type a new password for the account in the **New password** and **Confirm password** fields, and click **OK**.



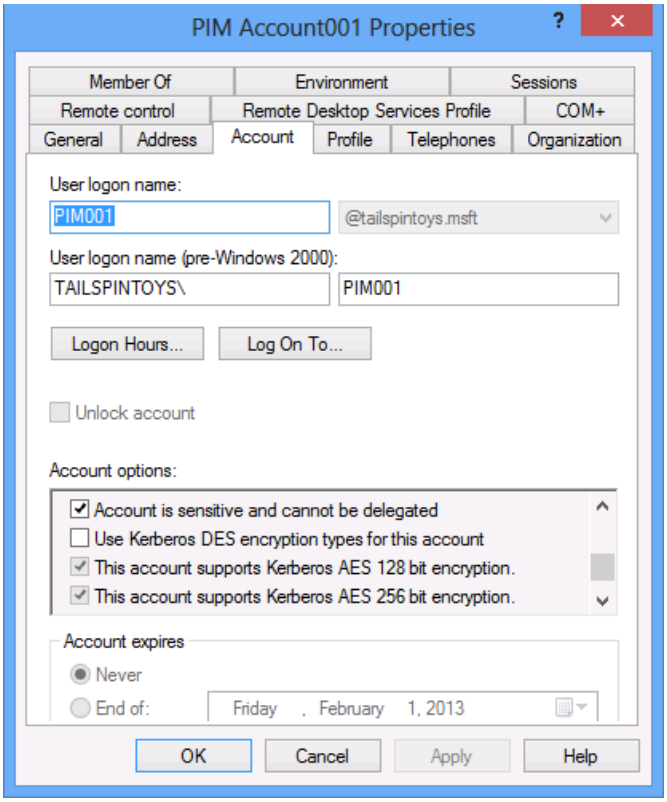
6. A dialog box should appear, confirming that the password for the account has been reset.



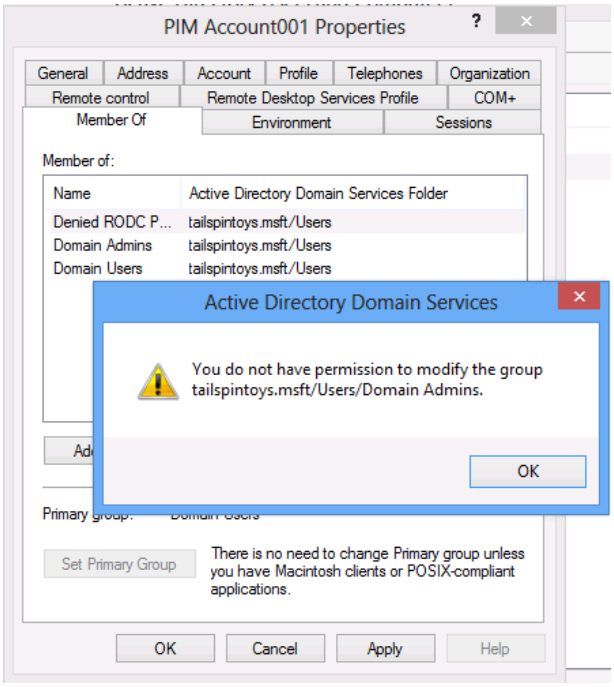
7. Now attempt to modify additional properties of the management account. Right-click the account and click **Properties**, and click the **Remote control** tab.
8. Select **Enable remote control** and click **Apply**. The operation should fail and an **Access Denied** error message should display.



9. Click the **Account** tab for the account and attempt to change the account's name, logon hours, or logon workstations. All should fail, and account options that are not controlled by the **userAccountControl** attribute should be grayed out and unavailable for modification.



10. Attempt to add the management group to a protected group such as the DA group. When you click **OK**, a message should appear, informing you that you do not have permissions to modify the group.



11. Perform additional tests as required to verify that you cannot configure anything on the management account except **userAccountControl** settings and password resets.

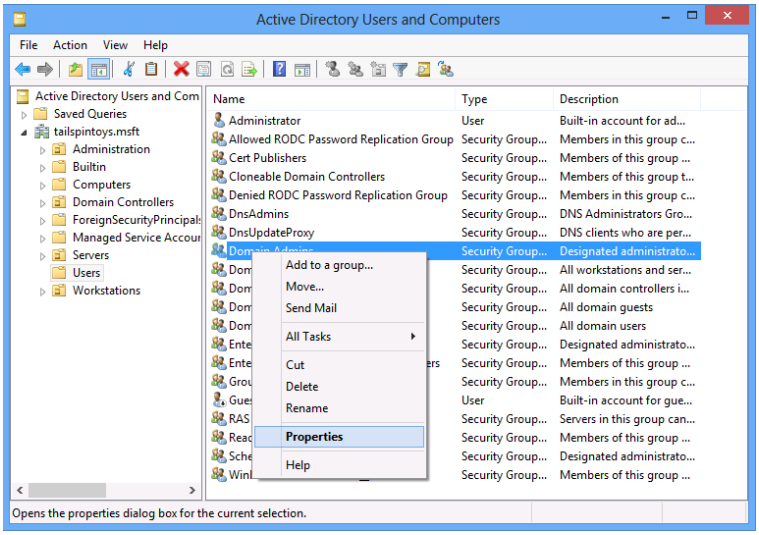
> **Note**
>
> The userAccountControl attribute controls multiple account configuration options. You cannot grant permission to change only some of the configuration options when you grant write permission to the attribute.

Test the Management Accounts

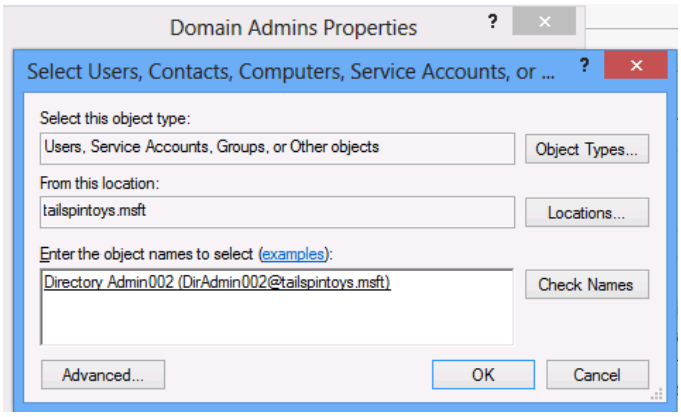
Now that you have enabled one or more accounts that can change the membership of protected groups, you can test the accounts to ensure that they can modify protected group membership, but cannot perform other modifications on protected accounts and groups.

1. Log on to a secure administrative host as the first management account.

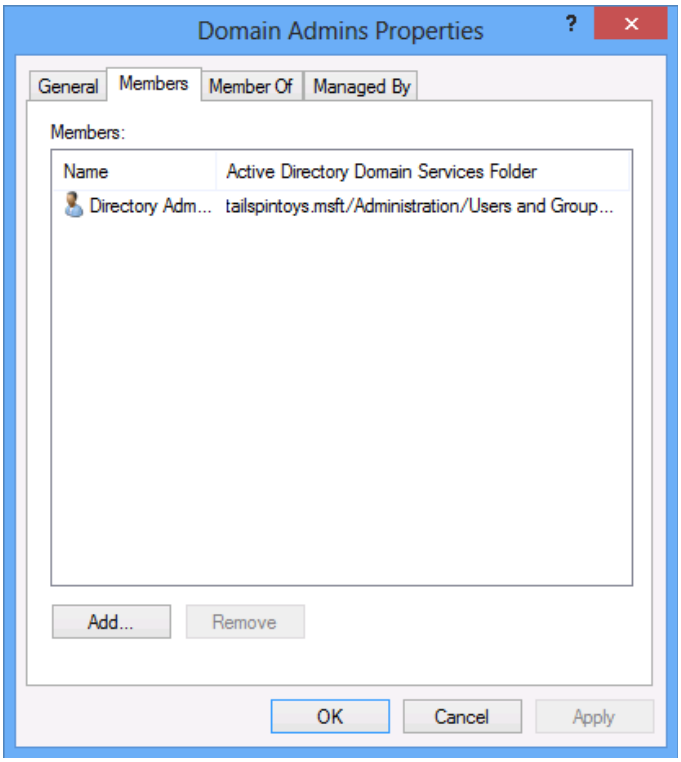
2. Launch **Active Directory Users and Computers** and locate the **Domain Admins** group.
3. Right-click the **Domain Admins group** and click **Properties**.



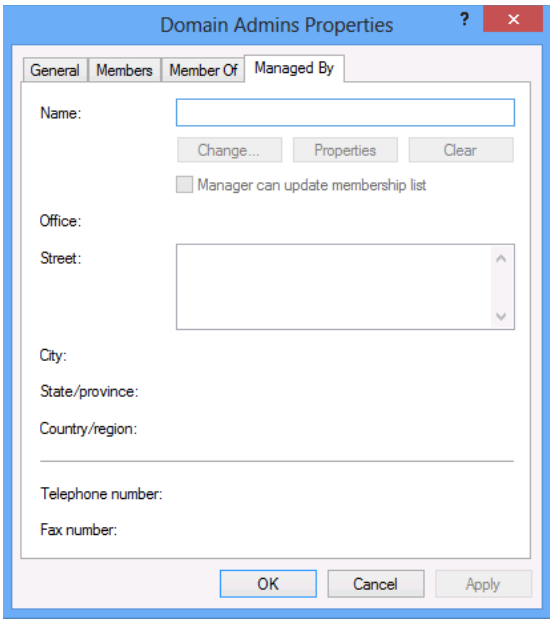
4. In the **Domain Admins Properties**, click the **Members** tab and click **Add**. Enter the name of an account that will be given temporary Domain Admins privileges and click **Check Names**. When the name of the account is underlined, click **OK** to return to the **Members** tab.



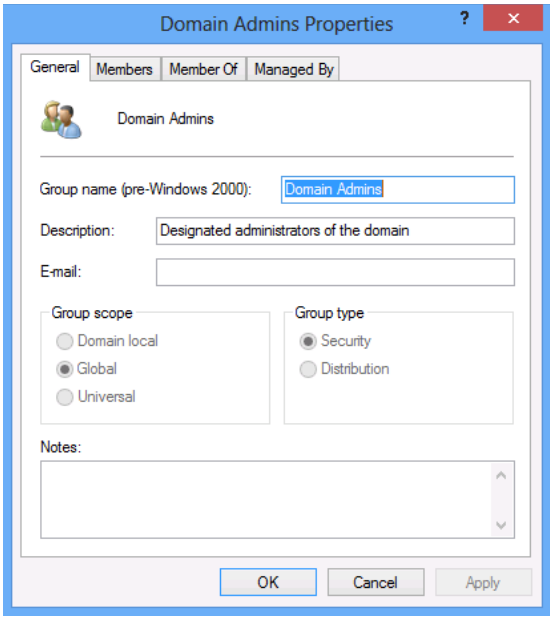
5. On the **Members** tab for the **Domain Admins Properties** dialog box, click **Apply**. After clicking **Apply**, the account should stay a member of the DA group and you should receive no error messages.



6. Click the **Managed By** tab in the **Domain Admins Properties** dialog box and verify that you cannot enter text in any fields and all buttons are grayed out.



7. Click the **General** tab in the **Domain Admins Properties** dialog box and verify that you cannot modify any of the information about that tab.



8. Repeat these steps for additional protected groups as needed. When you have finished, log on to a secure administrative host with an account that is a member of the group you created to enable and disable the management accounts. Then reset the password on the management account you just

tested and disable the account. You have completed setup of the management accounts and the group that will be responsible for enabling and disabling the accounts.

Appendix J: Third-Party RBAC Vendors

> **Note:**
>
> Descriptions of software described in this appendix were obtained from the respective vendors' websites. No endorsement of or preference for any solution is intended or implied.

The Dot Net Factory

EmpowerID includes an advanced authorization policy engine that allows organizations to define a user's access to a diverse set of corporate and cloud-hosted resources via flexible RBAC and ABAC rules. This "resultant access" information is then consumed or "pulled" by systems that support leveraging an external authorization engine to make access decisions or "pushed" down onto systems that don't.

Examples of systems supporting the "pull" model are applications that can leverage SAML or WS-Trust Identity and Claims Providers or applications supporting the Microsoft .NET Membership and Role Provider. These would include applications like Microsoft SharePoint 2010, SaaS applications, and internally developed corporate applications. EmpowerID falls into the category of a system supporting "pull" or external authorization.

Unfortunately, the majority of an enterprise's systems do not yet support external authorization. For these systems, access is defined and controlled within each application's security database or via ACLs. EmpowerID supports a "push" model for such cases in which the RBAC engine allows organizations to dynamically define who has access to these resources. The EmpowerID sync engine then enforces these policies by translating them into native system permissions or roles, pushing down the changes onto these systems. Additionally, the systems are monitored for permission changes so the EmpowerID engine can detect changes and roll them back when set up to do so. Examples of systems that require the "push" model are Windows Shared Folders, Group membership, Exchange mailboxes, custom database application roles and permissions, and directory ACLs.

Powerful RBAC policies leverage EmpowerID's multitiered model to pre-calculate access to all known enterprise applications and resources based on an organization's structure, a person's job function, and all directly assigned access. These rules allow information from authoritative systems to drive changes in application access and provisioning policies.

ABAC policies on the other hand, provide more fine-grained on-the-fly decisions regarding a user's access level and the actions they are authorized to perform. ABAC rules benefit from the ability to analyze contextual "in the moment" information to make decisions without the overhead and maintenance of an RBAC structure. However, ABAC rules are more limited in their use of an organization's structural information as they must real-time decisions and cannot wait for complex

analyses or pre-compilation of hierarchical information from multiple sources. The EmpowerID authorization engine is a hybrid of the RBAC and ABAC models, leveraging the best of each. It offers RBAC authorization to leverage diverse information sources for automating role-based access control and ABAC authorization, which further refines RBAC access with fine-grained controls.

Key Features and Benefits:

- Manages and enforces access control for applications that support external authorization and for enterprise systems that require permissions to be pushed down onto them
- A powerful security model supporting Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Separation of Duties enforcement (SoD)
- Reduces the time to market when developing new applications by eliminating the need to write complex security code into each application
- Supports enterprise compliance initiatives by centralizing authorization into an auditable system
- Reduces risk by reducing the number of places where security logic is maintained and can be modified
- Increases agility by reducing the impact of changes in infrastructure and application providers
- Standards-based support for SAML and WS-Trust applications such as Microsoft SharePoint 2010
- Unique Rights-Based Approval Routing (RBAR) technology automatically routes requests for approval based on delegations without hard-coded logic maintained inside workflows
- Fully programmable supporting integration with custom systems via connectors or a secure web services API

IBM

Domain RBAC

Role-based access control (RBAC), introduced in AIX 6.1, provides a mechanism to split the various functions of the super user root into roles, which can be delegated to other users on the system. RBAC provides the facility to delegate duties and improves the security of the system because the auditing and tracking of activities on the system is easier. RBAC provide delegation of responsibility to another user (referred as an authorized user), but it does not provide a mechanism to limit the administrative rights of an authorized user to specific resources of the system. For example, a user that has network administrative rights can manage every network interface on the system. You cannot restrict the authorized user to modify a set of interfaces.

The domain feature for RBAC is used to restrict access to authorized users. The users and resources of the system are labeled by attaching tags called domains, and the specific access rules determine access to resources by the users.

Oracle

Oracle Solaris RBAC Elements and Basic Concepts

The RBAC model in the Oracle Solaris Operating System introduces the following elements:

Authorization – A permission that enables a user or role to perform a class of actions that require additional rights. For example, security policy at installation gives regular users the solaris.device.cdrw authorization. This authorization enables users to read and write to a CD-ROM device.

Privilege – A discrete right that can be granted to a command, a user, a role, or a system. Privileges enable a process to succeed. For example, the proc_exec privilege allows a process to call execve(). Regular users have basic privileges.

Security attributes – An attribute that enables a process to perform an operation. In a typical UNIX environment, a security attribute enables a process to perform an operation that is otherwise forbidden to regular users. For example, setuid and setgid programs have security attributes. In the RBAC model, authorizations and privileges are security attributes in addition to setuid and setgid programs. These attributes can be assigned to a user. For example, a user with the solaris.device.allocate authorization can allocate a device for exclusive use. Privileges can be placed on a process. For example, a process with the file_flag_set privilege can set immutable, no-unlink, or append-only file attributes.

Privileged application – An application or command that can override system controls by checking for security attributes. In a typical UNIX environment and in the RBAC model, programs that use setuid and setgid are privileged applications. In the RBAC model, programs that require privileges or authorizations to succeed are also privileged applications.

Rights profile – A collection of administrative capabilities that can be assigned to a role or to a user. A rights profile can consist of authorizations, of commands with security attributes, and of other rights profiles. Rights profiles offer a convenient way to group security attributes.

Role – A special identity for running privileged applications. The special identity can be assumed by assigned users only. In a system that is run by roles, superuser is unnecessary. Superuser capabilities are distributed to different roles. For example, in a two-role system, security tasks would be handled by a security role. The second role would handle system administration tasks that are not security-related. Roles can be more fine-grained. For example, a system could include separate administrative roles for handling the cryptographic framework, printers, system time, file systems, and auditing.

Centrify

IT Security & Access Control

Strengthen IT security with Active Directory-centric access control and policy enforcement for UNIX, Linux and Mac systems and applications.

The Challenge

One of the most difficult questions asked of IT security managers in cross-platform environments is: Can you prove which users have access to a specific business-critical system or application?

For Linux and UNIX systems in particular, access controls might be stored in insecure legacy systems such as NIS or managed locally system by system. Passwords to superuser accounts may be shared among many individuals. Or a single user may have multiple identities across systems.

The Centrify Solution

Centrify addresses this challenge by giving organizations a global view of access controls and user permissions, tied to a single, centrally managed Active Directory identity. With the Centrify Suite, you can:

- Associate all access rights and permissions on audited systems to individual Active Directory accounts
- Define logical sets of systems that can have their own authorized users, administrators, and security policies, with centralized reporting of who has access to what systems
- Implement role-based access controls and limit superuser privileges to only the set of commands they need to perform their jobs
- Add additional layers of security by isolating and protecting systems holding sensitive information.
- Capture detailed logs of all user actions, and system responses, to monitor for suspicious activity
- Globally enforce consistent security and configuration policies (via Windows Group Policy) across a heterogeneous enterprise

> **Note:**
>
> Descriptions of software described in this appendix were obtained from the respective vendors' websites. No endorsement of or preference for any solution is intended or implied.

Cyber-Ark

Privileged accounts and passwords are extremely powerful, allowing a privileged user to log on anonymously and have complete control of the target system with full access to all of the information about that system. This vulnerability could potentially cause tremendous financial losses and reputational damage for businesses. For enterprises, privileged accounts are especially difficult to manage:

- The average enterprise has thousands of privileged identities, accounts, and passwords. Manually managing and updating these are a time-consuming, costly and repetitive process.
- Administrative and application accounts (hard-coded, embedded credentials) are found on virtually every piece of hardware, software, and application within an organization, including virtual environments.
- Administrative or application accounts are shared, which means that the system does not track WHO logged on as an Administrator, merely that a login occurred—a significant audit challenge.
- Unlike a personal identity, such as Jdoe, administrative or application accounts are nearly impossible to disable due to high potential for disruption to business.
- Administrative and application accounts are subject to regulations such as Sarbanes Oxley, PCI, and Basel II, requiring that companies prove exactly who logs in to sensitive systems and, increasingly, what they are doing.

What is the PIM Suite?

Cyber-Ark's Privileged Identity Management (PIM) Suite is an enterprise-class, unified policy-based solution that secures, manages and logs all privileged accounts and activities associated with datacenter management whether on-premise or in the cloud:

- Control access to privileged accounts based on pre-defined security policies
- Manage application and service credentials
- Grant granular control to the commands superusers can run

- Comply with audit and regulatory requirements
- Streamline policy management of privileged accounts
- Seamlessly integrate with enterprise systems

The PIM Suite allows organizations to manage, track and audit their most privileged identities, avert internal and external threats, and prevent the loss of sensitive information. It complements the Privileged Session Management Suite designed to isolate, protect and monitor all sensitive target systems in your datacenter including servers, network devices, databases and virtual environments and records all privileged sessions on these systems for better visibility, control and smoother audit processes.

The PIM Suite: features and components

The PIM Suite offers a robust set of system features and capabilities for consistent policy definition and enforcement, automated privileged password management, and centralized reporting for compliance audits. The PIM Suite comprises three well integrated core products which can also be purchased separately as needed:

- Enterprise Password Vault
- Application Identity Manager
- On-Demand Privileges Manager

Because they share a common server platform, an initial deployment of any individual solution can quickly and easily be expanded to address any additional audit or security challenges that may arise in the future.

With Cyber-Ark’s Privileged Identity Management suite you can:

- Approach Compliance with Confidence: Superior security that protects the ‘keys to your kingdom’ with a proven ability to meet regulatory requirements
- Minimize Internal or External Threats: Control who is accessing your most sensitive assets with out of the box best practices for defining and enforcing a unified policy for privileged identity management
- Do Business Better: Improve workforce productivity with a single access point for automatically managing privileged credentials

Quest

Privileged Account Management

Controlling and Auditing Superuser Access

Quest One helps you control and audit administrative access with privileged credentials through granular delegation and command control, keystroke logging and session audit, policy-based control, and secure and automated workflows. This approach enhances security and compliance while improving the efficiency of

administering superuser access. Administrators are granted only the rights they need—nothing more, nothing less—and all activity is tracked and audited.

- Enhance security by granting administrators only the access rights required for their jobs—nothing more, nothing less—and basing those rights on established and intelligently controlled policy. In addition, when full credentials must be used, secure the process of requesting, approving and issuing access to those accounts, including the critical application-to-application (A2A) and application-to-database (A2D) passwords that pose the greatest security risk.
- Achieve compliance through access control and separation of duties for privileged access that you can track through comprehensive audit capabilities that include policy, rights and activities performed through privileged access —even down to the keystroke level on many critical systems.
- Improve efficiency through granular, policy-driven delegation of elevated access privileges and execution of specific commands across a wide range of systems and platforms, with centralized management and comprehensive audit. Through automated workflows, your administrators gain sufficient rights to do their jobs eliminating the need for manual credential management. In addition, Quest One adds significant value to Sudo by centralizing management of Sudo policy and providing visibility into Sudo-related activities.

Lieberman Software

Privileged Identity Management

Privileged identities are accounts that hold elevated permission to access files, install and run programs, and change configuration settings. These keys to your IT kingdom exist on virtually every server and desktop operating system, business application, database, Web service, and network appliance in your organization.

Risks of Unsecured Privileged Identities

Privileged identities aren’t controlled by your identity access management (IAM) system, so in all likelihood:

- You do not know of all the privileged logins that exist on your network;
- You have no record of which privileged credentials are known to different individuals;
- You have no proof of who has used privileged logins to gain access to any of your IT resources, when, and for what purpose;

- There is no way to verify that each of your privileged account passwords are cryptographically strong, are sufficiently unique, and are changed often enough to be secure;
- You have no reliable list of privileged logins stored within your applications, and no way to know which in-house and vendor personnel can use these credentials to access sensitive information.

Controlling Privileged Account Access

Enterprise Random Password Manager (ERPM) from Lieberman Software can help your organization's privileged account management through a four-part I.D.E.A. process:

- Identify and document critical IT assets, their privileged accounts and their interdependencies.
- Delegate access to privileged credentials so that only appropriate personnel, using the least privilege required, can login to IT assets.
- Enforce rules for password complexity, diversity and change frequency, and synchronize changes across all dependencies.
- Audit and alert so that the requester, purpose, and duration of each privileged access request is documented.

ERPM continuously discovers, strengthens, monitors and recovers local, domain and process account passwords in the cross-platform enterprise. It identifies, secures and manages the privileged identities found throughout your IT infrastructure, including:

- Super-user login accounts utilized by individuals to change configuration settings, run programs and perform other administrative duties.
- Service accounts that require privileged login IDs and passwords to run.
- Application-to-application passwords used by web services, line-of-business applications, custom software, and other applications to connect to databases, middleware, and more.

Business Value of Privileged Identity Management

Taking control of privileged identities can help your organization:

- Reduce IT staff workloads by eliminating the manual steps required to secure privileged account credentials, access systems for maintenance, and document each access.

- Improve IT governance by automatically documenting which individuals have access to sensitive data and the ability to make changes that impact IT service delivery; at what times, and for what purpose.
- Lower cost and uncertainty of IT regulatory compliance audits by providing detailed reports that prove compliance with today's regulatory standards including SOX, PCI-DSS, HIPAA, CAG-8 and others.
- Mitigate risks whenever planned and unplanned changes happen in your IT environment or IT staff turnover occurs.

Novell

NetIQ Privileged User Manager

Secure access to UNIX, Linux and Windows systems

Do you have visibility into everything that privileged users are doing on your systems across your environment? Would you know if an unauthorized user gained access to sensitive information? The frequency and seriousness these breaches are increasing and compliance requirements for regulated information are forcing businesses to monitor of privileged user access.

NetIQ Privileged User Manager allows IT administrators to work on systems without exposing superuser (administrator or supervisor) passwords or root-account credentials to the administrator. It specifically targets managing, controlling and recording of all privileged administrator activities for UNIX, Linux and Windows environments.

Smart privileged user control features

- Secure cross-platform privileged user management Control and record "which privileged user have access to what." You centrally define the commands that privileged users are able to run on any UNIX, Linux or Windows platform.
- Simplified policy management with web-based console. Centrally manage security policies from a single point. The intuitive drag-and-drop interface makes it easy to create rules instead of relying on manual scripting.
- Detailed analysis with color-coded risk ratings Powerful risk-analysis tools record and play back user activity—down to the keystroke level. The unique risk-profiling capability points out any collected user input that poses a risk.
- Automatic data filtering for continuous compliance Prove compliance with permanent audit records 24x7x365, not only around compliance audits. Detailed logs of user activity help maintain your compliance posture.

CA

CA IdentityMinder

CA IdentityMinder™ helps improve the operational efficiency and effectiveness of IT organizations by providing a scalable and configurable identity management foundation that can organize your identity information within the context of your unique business roles and processes. It helps streamline the on-boarding and off-boarding of users, enables the business to manage access requests, and automates identity compliance processes.

Business Challenges

Whether applications reside in the enterprise or the cloud, managing the identities and access of users to key resources is a critical function for IT organizations that are under increasing pressure to cut operating costs while demonstrating continuous compliance. They must also deal with other challenges such as:

- Mitigating risks. Protect critical systems, applications, and information from unauthorized access and use.
- Reducing costs. Increase efficiency and productivity, without sacrificing security.
- Maintaining compliance. Efficiently prove compliance with internal policies, regulations, and best practices.
- Support business initiatives. Adopt new technologies easily (such as virtualization and cloud) that support business initiatives.

Organizations are seeking solutions that automate identity-related processes throughout the enterprise—from the mainframe to the cloud, across employees, contractors, partners, and customers. The result is a smarter, more efficiently managed infrastructure that helps IT save money, reduce risk, and deliver a more reliable service.

Solution Overview

CA IdentityMinder delivers a unified approach for managing users' identities throughout their entire lifecycle and providing them with timely, appropriate access to applications and data.

CA IdentityMinder can be used to organize identity information within the context of an organization's unique business roles and processes. It helps streamline the on-boarding and off-boarding of users, enables the business to manage access requests, and automates identity compliance processes. CA IdentityMinder contains a range of features for managing identities and access rights, and meeting identity compliance requirements.

CA IdentityMinder can increase operational efficiency and user productivity while decreasing Help Desk workload and costs. In addition, the CA Technologies approach to identity management and administration helps improve your overall security posture with a consistent, auditable method for managing identity-related activities and a platform to help maintain adherence to regulations.

Key features

- **User provisioning and deprovisioning.** Automates account provisioning, removal, and approval processes throughout the user's entire lifecycle. Customizable workflows support the unique way each organization approves, alerts, and schedules these activities.
- **User self-service.** Enables users to manage attributes of their own identities, reset
- Passwords and request access to resources, easing the IT and Help Desk burden.
- **Customization without custom code.** Powerful features such as ConfigXpress, PolicyXpress, and ConnectorXpress let you customize your identity management infrastructure without custom code.
- **Securing on-premise and cloud applications.** Provides centralized control of identities, users, roles and policies across on-premise and cloud applications.

Appendix L: Events to Monitor

The following table lists events that you should monitor in your environment, according to the recommendations provided in Monitoring Active Directory for Signs of Compromise. In the following table, the “Current Windows Event ID” column lists the event ID as it is implemented in versions of Windows and Windows Server that are currently in mainstream support.

The “Legacy Windows Event ID” column lists the corresponding event ID in legacy versions of Windows such as client computers running Windows XP or earlier and servers running Windows Server 2003 or earlier. The “Potential Criticality” column identifies whether the event should be considered of low, medium, or high criticality in detecting attacks, and the “Event Summary” column provides a brief description of the event.

A potential criticality of High means that one occurrence of the event should be investigated. Potential criticality of Medium or Low means that these events should only be investigated if they occur unexpectedly or in numbers that significantly exceed the expected baseline in a measured period of time. All organizations should test these recommendations in their environments before creating alerts that require mandatory investigative responses. Every environment is different, and some of the events ranked with a potential criticality of High may occur due to other harmless events.

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
4618	N/A	High	A monitored security event pattern has occurred.
4649	N/A	High	A replay attack was detected. May be a harmless false positive due to misconfiguration error.
4719	612	High	System audit policy was changed.
4765	N/A	High	SID History was added to an account.
4766	N/A	High	An attempt to add SID History to an account failed.
4794	N/A	High	An attempt was made to set the Directory Services Restore Mode.

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
4897	801	High	Role separation enabled:
4964	N/A	High	Special groups have been assigned to a new logon.
5124	N/A	High	A security setting was updated on the OCSP Responder Service
N/A	550	Medium to High	Possible denial-of-service (DoS) attack
1102	517	Medium to High	The audit log was cleared
4621	N/A	Medium	Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded.
4675	N/A	Medium	SIDs were filtered.
4692	N/A	Medium	Backup of data protection master key was attempted.
4693	N/A	Medium	Recovery of data protection master key was attempted.
4706	610	Medium	A new trust was created to a domain.
4713	617	Medium	Kerberos policy was changed.
4714	618	Medium	Encrypted data recovery policy was changed.
4715	N/A	Medium	The audit policy (SACL) on an object was changed.
4716	620	Medium	Trusted domain information was modified.
4724	628	Medium	An attempt was made to reset an account’s password.
4727	631	Medium	A security-enabled global group was created.

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
4735	639	Medium	A security-enabled local group was changed.
4737	641	Medium	A security-enabled global group was changed.
4739	643	Medium	Domain Policy was changed.
4754	658	Medium	A security-enabled universal group was created.
4755	659	Medium	A security-enabled universal group was changed.
4764	667	Medium	A security-disabled group was deleted
4764	668	Medium	A group’s type was changed.
4780	684	Medium	The ACL was set on accounts which are members of administrators groups.
4816	N/A	Medium	RPC detected an integrity violation while decrypting an incoming message.
4865	N/A	Medium	A trusted forest information entry was added.
4866	N/A	Medium	A trusted forest information entry was removed.
4867	N/A	Medium	A trusted forest information entry was modified.
4868	772	Medium	The certificate manager denied a pending certificate request.
4870	774	Medium	Certificate Services revoked a certificate.
4882	786	Medium	The security permissions for Certificate Services changed.
4885	789	Medium	The audit filter for Certificate Services changed.
4890	794	Medium	The certificate manager settings for Certificate

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
			Services changed.
4892	796	Medium	A property of Certificate Services changed.
4896	800	Medium	One or more rows have been deleted from the certificate database.
4906	N/A	Medium	The CrashOnAuditFail value has changed.
4907	N/A	Medium	Auditing settings on object were changed.
4908	N/A	Medium	Special Groups Logon table modified.
4912	807	Medium	Per User Audit Policy was changed.
4960	N/A	Medium	IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations.
4961	N/A	Medium	IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.
4962	N/A	Medium	IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay.

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
4963	N/A	Medium	IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt.
4965	N/A	Medium	IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored.
4976	N/A	Medium	During Main Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
4977	N/A	Medium	During Quick Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
4978	N/A	Medium	During Extended Mode negotiation, IPsec received an

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
			invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
4983	N/A	Medium	An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.
4984	N/A	Medium	An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.
5027	N/A	Medium	The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy.
5028	N/A	Medium	The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy.
5029	N/A	Medium	The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy.
5030	N/A	Medium	The Windows Firewall Service failed to start.
5035	N/A	Medium	The Windows Firewall Driver failed to start.
5037	N/A	Medium	The Windows Firewall Driver detected critical runtime error. Terminating.
5038	N/A	Medium	Code integrity determined that the image hash of a file is

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
			not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.
5120	N/A	Medium	OCSP Responder Service Started
5121	N/A	Medium	OCSP Responder Service Stopped
5122	N/A	Medium	A configuration entry changed in OCSP Responder Service
5123	N/A	Medium	A configuration entry changed in OCSP Responder Service
5376	N/A	Medium	Credential Manager credentials were backed up.
5377	N/A	Medium	Credential Manager credentials were restored from a backup.
5453	N/A	Medium	An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service is not started.
5480	N/A	Medium	IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.
5483	N/A	Medium	IPsec Services failed to initialize RPC server. IPsec Services could not be started.
5484	N/A	Medium	IPsec Services has experienced a critical failure and has been shut down. The

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
			shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.
5485	N/A	Medium	IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.
6145	N/A	Medium	One or more errors occurred while processing security policy in the Group Policy objects.
6273	N/A	Medium	Network Policy Server denied access to a user.
6274	N/A	Medium	Network Policy Server discarded the request for a user.
6275	N/A	Medium	Network Policy Server discarded the accounting request for a user.
6276	N/A	Medium	Network Policy Server quarantined a user.
6277	N/A	Medium	Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy.
6278	N/A	Medium	Network Policy Server granted full access to a user because the host met the defined health policy.

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
6279	N/A	Medium	Network Policy Server locked the user account due to repeated failed authentication attempts.
6280	N/A	Medium	Network Policy Server unlocked the user account.
-	640	Medium	General account database changed
-	619	Medium	Quality of Service Policy changed
24586	N/A	Medium	An error was encountered converting volume
24592	N/A	Medium	An attempt to automatically restart conversion on volume %2 failed.
24593	N/A	Medium	Metadata write: Volume %2 returning errors while trying to modify metadata. If failures continue, decrypt volume
24594	N/A	Medium	Metadata rebuild: An attempt to write a copy of metadata on volume %2 failed and may appear as disk corruption. If failures continue, decrypt volume.
4608	512	Low	Windows is starting up.
4609	513	Low	Windows is shutting down.
4610	514	Low	An authentication package has been loaded by the Local Security Authority.
4611	515	Low	A trusted logon process has been registered with the Local Security Authority.
4612	516	Low	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
4614	518	Low	A notification package has been loaded by the Security Account Manager.
4615	519	Low	Invalid use of LPC port.
4616	520	Low	The system time was changed.
4622	N/A	Low	A security package has been loaded by the Local Security Authority.
4624	528,540	Low	An account was successfully logged on.
4625	529-537,539	Low	An account failed to log on.
4634	538	Low	An account was logged off.
4646	N/A	Low	IKE DoS-prevention mode started.
4647	551	Low	User initiated logoff.
4648	552	Low	A logon was attempted using explicit credentials.
4650	N/A	Low	An IPsec Main Mode security association was established. Extended Mode was not enabled. Certificate authentication was not used.
4651	N/A	Low	An IPsec Main Mode security association was established. Extended Mode was not enabled. A certificate was used for authentication.
4652	N/A	Low	An IPsec Main Mode negotiation failed.
4653	N/A	Low	An IPsec Main Mode negotiation failed.
4654	N/A	Low	An IPsec Quick Mode negotiation failed.
4655	N/A	Low	An IPsec Main Mode security

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
			association ended.
4656	560	Low	A handle to an object was requested.
4657	567	Low	A registry value was modified.
4658	562	Low	The handle to an object was closed.
4659	N/A	Low	A handle to an object was requested with intent to delete.
4660	564	Low	An object was deleted.
4661	565	Low	A handle to an object was requested.
4662	566	Low	An operation was performed on an object.
4663	567	Low	An attempt was made to access an object.
4664	N/A	Low	An attempt was made to create a hard link.
4665	N/A	Low	An attempt was made to create an application client context.
4666	N/A	Low	An application attempted an operation:
4667	N/A	Low	An application client context was deleted.
4668	N/A	Low	An application was initialized.
4670	N/A	Low	Permissions on an object were changed.
4671	N/A	Low	An application attempted to access a blocked ordinal through the TBS.
4672	576	Low	Special privileges assigned to new logon.
4673	577	Low	A privileged service was called.

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
4674	578	Low	An operation was attempted on a privileged object.
4688	592	Low	A new process has been created.
4689	593	Low	A process has exited.
4690	594	Low	An attempt was made to duplicate a handle to an object.
4691	595	Low	Indirect access to an object was requested.
4694	N/A	Low	Protection of auditable protected data was attempted.
4695	N/A	Low	Unprotection of auditable protected data was attempted.
4696	600	Low	A primary token was assigned to process.
4697	601	Low	Attempt to install a service
4698	602	Low	A scheduled task was created.
4699	602	Low	A scheduled task was deleted.
4700	602	Low	A scheduled task was enabled.
4701	602	Low	A scheduled task was disabled.
4702	602	Low	A scheduled task was updated.
4704	608	Low	A user right was assigned.
4705	609	Low	A user right was removed.
4707	611	Low	A trust to a domain was removed.
4709	N/A	Low	IPsec Services was started.
4710	N/A	Low	IPsec Services was disabled.

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
4711	N/A	Low	May contain any one of the following: PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer. PAStore Engine applied Active Directory storage IPsec policy on the computer. PAStore Engine applied local registry storage IPsec policy on the computer. PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer. PAStore Engine failed to apply Active Directory storage IPsec policy on the computer. PAStore Engine failed to apply local registry storage IPsec policy on the computer. PAStore Engine failed to apply some rules of the active IPsec policy on the computer. PAStore Engine failed to load directory storage IPsec policy on the computer. PAStore Engine loaded directory storage IPsec policy on the computer. PAStore Engine failed to load local storage IPsec policy on the computer. PAStore Engine loaded local storage IPsec policy on the computer. PAStore Engine polled for changes to the active IPsec policy and detected no changes.
4712	N/A	Low	IPsec Services encountered a potentially serious failure.
4717	621	Low	System security access was granted to an account.

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
4718	622	Low	System security access was removed from an account.
4720	624	Low	A user account was created.
4722	626	Low	A user account was enabled.
4723	627	Low	An attempt was made to change an account’s password.
4725	629	Low	A user account was disabled.
4726	630	Low	A user account was deleted.
4728	632	Low	A member was added to a security-enabled global group.
4729	633	Low	A member was removed from a security-enabled global group.
4730	634	Low	A security-enabled global group was deleted.
4731	635	Low	A security-enabled local group was created.
4732	636	Low	A member was added to a security-enabled local group.
4733	637	Low	A member was removed from a security-enabled local group.
4734	638	Low	A security-enabled local group was deleted.
4738	642	Low	A user account was changed.
4740	644	Low	A user account was locked out.
4741	645	Low	A computer account was changed.
4742	646	Low	A computer account was changed.
4743	647	Low	A computer account was deleted.

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
4744	648	Low	A security-disabled local group was created.
4745	649	Low	A security-disabled local group was changed.
4746	650	Low	A member was added to a security-disabled local group.
4747	651	Low	A member was removed from a security-disabled local group.
4748	652	Low	A security-disabled local group was deleted.
4749	653	Low	A security-disabled global group was created.
4750	654	Low	A security-disabled global group was changed.
4751	655	Low	A member was added to a security-disabled global group.
4752	656	Low	A member was removed from a security-disabled global group.
4753	657	Low	A security-disabled global group was deleted.
4756	660	Low	A member was added to a security-enabled universal group.
4757	661	Low	A member was removed from a security-enabled universal group.
4758	662	Low	A security-enabled universal group was deleted.
4759	663	Low	A security-disabled universal group was created.
4760	664	Low	A security-disabled universal group was changed.
4761	665	Low	A member was added to a

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
			security-disabled universal group.
4762	666	Low	A member was removed from a security-disabled universal group.
4767	671	Low	A user account was unlocked.
4768	672,676	Low	A Kerberos authentication ticket (TGT) was requested.
4769	673	Low	A Kerberos service ticket was requested.
4770	674	Low	A Kerberos service ticket was renewed.
4771	675	Low	Kerberos pre-authentication failed.
4772	672	Low	A Kerberos authentication ticket request failed.
4774	678	Low	An account was mapped for logon.
4775	679	Low	An account could not be mapped for logon.
4776	680,681	Low	The domain controller attempted to validate the credentials for an account.
4777	N/A	Low	The domain controller failed to validate the credentials for an account.
4778	682	Low	A session was reconnected to a Window Station.
4779	683	Low	A session was disconnected from a Window Station.
4781	685	Low	The name of an account was changed:
4782	N/A	Low	The password hash an account was accessed.
4783	667	Low	A basic application group was

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
			created.
4784	N/A	Low	A basic application group was changed.
4785	689	Low	A member was added to a basic application group.
4786	690	Low	A member was removed from a basic application group.
4787	691	Low	A nonmember was added to a basic application group.
4788	692	Low	A nonmember was removed from a basic application group.
4789	693	Low	A basic application group was deleted.
4790	694	Low	An LDAP query group was created.
4793	N/A	Low	The Password Policy Checking API was called.
4800	N/A	Low	The workstation was locked.
4801	N/A	Low	The workstation was unlocked.
4802	N/A	Low	The screen saver was invoked.
4803	N/A	Low	The screen saver was dismissed.
4864	N/A	Low	A namespace collision was detected.
4869	773	Low	Certificate Services received a resubmitted certificate request.
4871	775	Low	Certificate Services received a request to publish the certificate revocation list (CRL).
4872	776	Low	Certificate Services published the certificate revocation list

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
			(CRL).
4873	777	Low	A certificate request extension changed.
4874	778	Low	One or more certificate request attributes changed.
4875	779	Low	Certificate Services received a request to shut down.
4876	780	Low	Certificate Services backup started.
4877	781	Low	Certificate Services backup completed.
4878	782	Low	Certificate Services restore started.
4879	783	Low	Certificate Services restore completed.
4880	784	Low	Certificate Services started.
4881	785	Low	Certificate Services stopped.
4883	787	Low	Certificate Services retrieved an archived key.
4884	788	Low	Certificate Services imported a certificate into its database.
4886	790	Low	Certificate Services received a certificate request.
4887	791	Low	Certificate Services approved a certificate request and issued a certificate.
4888	792	Low	Certificate Services denied a certificate request.
4889	793	Low	Certificate Services set the status of a certificate request to pending.
4891	795	Low	A configuration entry changed in Certificate Services.
4893	797	Low	Certificate Services archived a key.

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
4894	798	Low	Certificate Services imported and archived a key.
4895	799	Low	Certificate Services published the CA certificate to Active Directory Domain Services.
4898	802	Low	Certificate Services loaded a template.
4902	N/A	Low	The Per-user audit policy table was created.
4904	N/A	Low	An attempt was made to register a security event source.
4905	N/A	Low	An attempt was made to unregister a security event source.
4909	N/A	Low	The local policy settings for the TBS were changed.
4910	N/A	Low	The Group Policy settings for the TBS were changed.
4928	N/A	Low	An Active Directory replica source naming context was established.
4929	N/A	Low	An Active Directory replica source naming context was removed.
4930	N/A	Low	An Active Directory replica source naming context was modified.
4931	N/A	Low	An Active Directory replica destination naming context was modified.
4932	N/A	Low	Synchronization of a replica of an Active Directory naming context has begun.
4933	N/A	Low	Synchronization of a replica of an Active Directory naming context has ended.

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
4934	N/A	Low	Attributes of an Active Directory object were replicated.
4935	N/A	Low	Replication failure begins.
4936	N/A	Low	Replication failure ends.
4937	N/A	Low	A lingering object was removed from a replica.
4944	N/A	Low	The following policy was active when the Windows Firewall started.
4945	N/A	Low	A rule was listed when the Windows Firewall started.
4946	N/A	Low	A change has been made to Windows Firewall exception list. A rule was added.
4947	N/A	Low	A change has been made to Windows Firewall exception list. A rule was modified.
4948	N/A	Low	A change has been made to Windows Firewall exception list. A rule was deleted.
4949	N/A	Low	Windows Firewall settings were restored to the default values.
4950	N/A	Low	A Windows Firewall setting has changed.
4951	N/A	Low	A rule has been ignored because its major version number was not recognized by Windows Firewall.
4952	N/A	Low	Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced.
4953	N/A	Low	A rule has been ignored by

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
			Windows Firewall because it could not parse the rule.
4954	N/A	Low	Windows Firewall Group Policy settings have changed. The new settings have been applied.
4956	N/A	Low	Windows Firewall has changed the active profile.
4957	N/A	Low	Windows Firewall did not apply the following rule:
4958	N/A	Low	Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer:
4979	N/A	Low	IPsec Main Mode and Extended Mode security associations were established.
4980	N/A	Low	IPsec Main Mode and Extended Mode security associations were established.
4981	N/A	Low	IPsec Main Mode and Extended Mode security associations were established.
4982	N/A	Low	IPsec Main Mode and Extended Mode security associations were established.
4985	N/A	Low	The state of a transaction has changed.
5024	N/A	Low	The Windows Firewall Service has started successfully.
5025	N/A	Low	The Windows Firewall Service has been stopped.
5031	N/A	Low	The Windows Firewall Service blocked an application from accepting incoming connections on the network.

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
5032	N/A	Low	Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.
5033	N/A	Low	The Windows Firewall Driver has started successfully.
5034	N/A	Low	The Windows Firewall Driver has been stopped.
5039	N/A	Low	A registry key was virtualized.
5040	N/A	Low	A change has been made to IPsec settings. An Authentication Set was added.
5041	N/A	Low	A change has been made to IPsec settings. An Authentication Set was modified.
5042	N/A	Low	A change has been made to IPsec settings. An Authentication Set was deleted.
5043	N/A	Low	A change has been made to IPsec settings. A Connection Security Rule was added.
5044	N/A	Low	A change has been made to IPsec settings. A Connection Security Rule was modified.
5045	N/A	Low	A change has been made to IPsec settings. A Connection Security Rule was deleted.
5046	N/A	Low	A change has been made to IPsec settings. A Crypto Set was added.
5047	N/A	Low	A change has been made to IPsec settings. A Crypto Set was modified.
5048	N/A	Low	A change has been made to IPsec settings. A Crypto Set

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
			was deleted.
5050	N/A	Low	An attempt to programmatically disable the Windows Firewall using a call to InetFwProfile.FirewallEnabled(False)
5051	N/A	Low	A file was virtualized.
5056	N/A	Low	A cryptographic self test was performed.
5057	N/A	Low	A cryptographic primitive operation failed.
5058	N/A	Low	Key file operation.
5059	N/A	Low	Key migration operation.
5060	N/A	Low	Verification operation failed.
5061	N/A	Low	Cryptographic operation.
5062	N/A	Low	A kernel-mode cryptographic self test was performed.
5063	N/A	Low	A cryptographic provider operation was attempted.
5064	N/A	Low	A cryptographic context operation was attempted.
5065	N/A	Low	A cryptographic context modification was attempted.
5066	N/A	Low	A cryptographic function operation was attempted.
5067	N/A	Low	A cryptographic function modification was attempted.
5068	N/A	Low	A cryptographic function provider operation was attempted.
5069	N/A	Low	A cryptographic function property operation was attempted.
5070	N/A	Low	A cryptographic function

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
			property modification was attempted.
5125	N/A	Low	A request was submitted to the OCSP Responder Service
5126	N/A	Low	Signing Certificate was automatically updated by the OCSP Responder Service
5127	N/A	Low	The OCSP Revocation Provider successfully updated the revocation information
5136	566	Low	A directory service object was modified.
5137	566	Low	A directory service object was created.
5138	N/A	Low	A directory service object was undeleted.
5139	N/A	Low	A directory service object was moved.
5140	N/A	Low	A network share object was accessed.
5141	N/A	Low	A directory service object was deleted.
5152	N/A	Low	The Windows Filtering Platform blocked a packet.
5153	N/A	Low	A more restrictive Windows Filtering Platform filter has blocked a packet.
5154	N/A	Low	The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections.
5155	N/A	Low	The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections.

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
5156	N/A	Low	The Windows Filtering Platform has allowed a connection.
5157	N/A	Low	The Windows Filtering Platform has blocked a connection.
5158	N/A	Low	The Windows Filtering Platform has permitted a bind to a local port.
5159	N/A	Low	The Windows Filtering Platform has blocked a bind to a local port.
5378	N/A	Low	The requested credentials delegation was disallowed by policy.
5440	N/A	Low	The following callout was present when the Windows Filtering Platform Base Filtering Engine started.
5441	N/A	Low	The following filter was present when the Windows Filtering Platform Base Filtering Engine started.
5442	N/A	Low	The following provider was present when the Windows Filtering Platform Base Filtering Engine started.
5443	N/A	Low	The following provider context was present when the Windows Filtering Platform Base Filtering Engine started.
5444	N/A	Low	The following sublayer was present when the Windows Filtering Platform Base Filtering Engine started.
5446	N/A	Low	A Windows Filtering Platform callout has been changed.
5447	N/A	Low	A Windows Filtering Platform

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
			filter has been changed.
5448	N/A	Low	A Windows Filtering Platform provider has been changed.
5449	N/A	Low	A Windows Filtering Platform provider context has been changed.
5450	N/A	Low	A Windows Filtering Platform sublayer has been changed.
5451	N/A	Low	An IPsec Quick Mode security association was established.
5452	N/A	Low	An IPsec Quick Mode security association ended.
5456	N/A	Low	PAStore Engine applied Active Directory storage IPsec policy on the computer.
5457	N/A	Low	PAStore Engine failed to apply Active Directory storage IPsec policy on the computer.
5458	N/A	Low	PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer.
5459	N/A	Low	PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer.
5460	N/A	Low	PAStore Engine applied local registry storage IPsec policy on the computer.
5461	N/A	Low	PAStore Engine failed to apply local registry storage IPsec policy on the computer.
5462	N/A	Low	PAStore Engine failed to apply some rules of the active IPsec policy on the computer. Use the IP Security Monitor snap-in to diagnose the problem.

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
5463	N/A	Low	PAStore Engine polled for changes to the active IPsec policy and detected no changes.
5464	N/A	Low	PAStore Engine polled for changes to the active IPsec policy, detected changes, and applied them to IPsec Services.
5465	N/A	Low	PAStore Engine received a control for forced reloading of IPsec policy and processed the control successfully.
5466	N/A	Low	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory cannot be reached, and will use the cached copy of the Active Directory IPsec policy instead. Any changes made to the Active Directory IPsec policy since the last poll could not be applied.
5467	N/A	Low	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, and found no changes to the policy. The cached copy of the Active Directory IPsec policy is no longer being used.
5468	N/A	Low	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, found changes to the policy, and applied those changes. The cached copy of the Active Directory IPsec policy is no

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
			longer being used.
5471	N/A	Low	PAStore Engine loaded local storage IPsec policy on the computer.
5472	N/A	Low	PAStore Engine failed to load local storage IPsec policy on the computer.
5473	N/A	Low	PAStore Engine loaded directory storage IPsec policy on the computer.
5474	N/A	Low	PAStore Engine failed to load directory storage IPsec policy on the computer.
5477	N/A	Low	PAStore Engine failed to add quick mode filter.
5479	N/A	Low	IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.
5632	N/A	Low	A request was made to authenticate to a wireless network.
5633	N/A	Low	A request was made to authenticate to a wired network.
5712	N/A	Low	A Remote Procedure Call (RPC) was attempted.
5888	N/A	Low	An object in the COM+ Catalog was modified.
5889	N/A	Low	An object was deleted from the COM+ Catalog.
5890	N/A	Low	An object was added to the COM+ Catalog.
6008	N/A	Low	The previous system

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
			shutdown was unexpected
6144	N/A	Low	Security policy in the Group Policy objects has been applied successfully.
6272	N/A	Low	Network Policy Server granted access to a user.
N/A	561	Low	A handle to an object was requested.
N/A	563	Low	Object open for delete
N/A	625	Low	User Account Type Changed
N/A	613	Low	IPsec policy agent started
N/A	614	Low	IPsec policy agent disabled
N/A	615	Low	IPsec policy agent
N/A	616	Low	IPsec policy agent encountered a potential serious failure
24577	N/A	Low	Encryption of volume started
24578	N/A	Low	Encryption of volume stopped
24579	N/A	Low	Encryption of volume completed
24580	N/A	Low	Decryption of volume started
24581	N/A	Low	Decryption of volume stopped
24582	N/A	Low	Decryption of volume completed
24583	N/A	Low	Conversion worker thread for volume started
24584	N/A	Low	Conversion worker thread for volume temporarily stopped
24588	N/A	Low	The conversion operation on volume %2 encountered a bad sector error. Please validate the data on this volume
24595	N/A	Low	Volume %2 contains bad

Current Windows Event ID	Legacy Windows Event ID	Potential Criticality	Event Summary
			clusters. These clusters will be skipped during conversion.
24621	N/A	Low	Initial state check: Rolling volume conversion transaction on %2.
5049	N/A	Low	An IPsec Security Association was deleted.
5478	N/A	Low	IPsec Services has started successfully.

Notes

- Refer to Microsoft Support article 947226 for lists of many security event IDs and their meaning
- Run **wevtutil gp Microsoft-Windows-Security-Auditing /ge /gm:true** to get a very detailed listing of all security event IDs

For more information about Windows security event IDs and their meanings, see the Microsoft Support articles Description of security events in Windows Vista and in Windows Server 2008 and Description of security events in Windows 7 and in Windows Server 2008 R2. You can also download Security Audit Events for Windows 7 and Windows Server 2008 R2 and Windows 8 and Windows Server 2012 Security Event Details, which provide detailed event information for the referenced operating systems in spreadsheet format.

Appendix M: Document Links and Recommended Reading

Document Links

The following table contains a list of links to external documents and their URLs so that readers of hard copies of this document can access this information. The links are listed in the order they appear in the document.

Links	URLs
10 Immutable Laws of Security Administration	http://technet.microsoft.com/en-us/library/cc722488.aspx
Microsoft Security Compliance Manager	http://technet.microsoft.com/en-us/library/cc677002.aspx
Gartner Symposium ITXPO	http://www.gartner.com/technology/sym

Links	URLs
	posium/orlando/
2012 Data Breach Investigations Report (DBIR)	http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf
Ten Immutable Laws of Security (Version 2.0)	http://technet.microsoft.com/en-us/security/hh278941.aspx
Using Heuristic Scanning	http://technet.microsoft.com/en-us/library/bb418939.aspx
drive-by download	http://www.microsoft.com/security/sir/glossary/drive-by-download-sites.aspx
Microsoft Support article 2526083	http://support.microsoft.com/kb/2526083
Microsoft Support article 814777	http://support.microsoft.com/kb/814777
Open Web Application Security Project (OWASP)	https://www.owasp.org/index.php/Main_Page
Microsoft Security Development Lifecycle	http://www.microsoft.com/security/sdl/default.aspx
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 Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques_English.pdf
Determined Adversaries and Targeted Attacks	http://www.microsoft.com/en-us/download/details.aspx?id=34793
Solution for management of built-in Administrator account's password via GPO	http://code.msdn.microsoft.com/windowsdesktop/Solution-for-management-of-ae44e789
Microsoft Support article 817433	http://support.microsoft.com/?id=817433
Microsoft Support article 973840	http://support.microsoft.com/kb/973840
Administrator account is disabled by default	http://technet.microsoft.com/en-us/library/cc753450.aspx
The Administrator Accounts Security Planning Guide	http://technet.microsoft.com/en-us/library/cc162797.aspx
Microsoft Windows Security Resource Kit	http://www.microsoft.com/learning/en/us/book.aspx?ID=6815&locale=en-us

Links	URLs
Authentication Mechanism Assurance for AD DS in Windows Server 2008 R2 Step-by-Step Guide	http://technet.microsoft.com/en-us/library/dd378897(WS.10).aspx
Windows Server Update Services	http://technet.microsoft.com/en-us/windowsserver/bb332157
Personal Virtual Desktops	http://technet.microsoft.com/en-us/library/dd759174.aspx
Read-Only Domain Controller Planning and Deployment Guide	http://technet.microsoft.com/en-us/library/cc771744(WS.10).aspx
Running Domain Controllers in Hyper-V	http://technet.microsoft.com/en-us/library/dd363553(v=ws.10).aspx
Hyper-V Security Guide	http://www.microsoft.com/en-us/download/details.aspx?id=16650
Ask the Directory Services Team	http://blogs.technet.com/b/askds/archive/2011/09/12/managing-rid-pool-depletion.aspx
How to configure a firewall for domains and trusts	http://support.microsoft.com/kb/179442
2009 Verizon Data Breach Report	http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf
2012 Verizon Data Breach report	http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf
Introducing Auditing Changes in Windows 2008	http://blogs.technet.com/b/askds/archive/2007/10/19/introducing-auditing-changes-in-windows-2008.aspx
Cool Auditing Tricks in Vista and 2008	http://blogs.technet.com/b/askds/archive/2007/11/16/cool-auditing-tricks-in-vista-and-2008.aspx
Global Object Access Auditing is Magic	http://blogs.technet.com/b/askds/archive/2011/03/10/global-object-access-auditing-is-magic.aspx
One-Stop Shop for Auditing in Windows Server 2008 and Windows Vista	http://blogs.technet.com/b/askds/archive/2008/03/27/one-stop-shop-for-auditing-in-windows-server-2008-and-windows-vista.aspx

Links	URLs
AD DS Auditing Step-by-Step Guide	http://technet.microsoft.com/en-US/library/a9c25483-89e2-4202-881c-ea8e02b4b2a5.aspx
Getting the Effective Audit Policy in Windows 7 and 2008 R2	http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf
sample script	http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf
Audit Option Type	http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf
Advanced Security Auditing in Windows 7 and Windows Server 2008 R2	http://social.technet.microsoft.com/wiki/contents/articles/advanced-security-auditing-in-windows-7-and-windows-server-2008-r2.aspx
Auditing and Compliance in Windows Server 2008	http://technet.microsoft.com/en-us/magazine/2008.03.auditing.aspx
How to use Group Policy to configure detailed security auditing settings for Windows Vista-based and Windows Server 2008-based computers in a Windows Server 2008 domain, in a Windows Server 2003 domain, or in a Windows 2000 Server domain	http://support.microsoft.com/kb/921469
Advanced Security Audit Policy Step-by-Step Guide	http://technet.microsoft.com/en-us/library/dd408940(WS.10).aspx
Threats and Countermeasures Guide	http://technet.microsoft.com/en-us/library/hh125921(v=ws.10).aspx
MaxTokenSize and Kerberos Token Bloat	http://blogs.technet.com/b/shanecothran/archive/2010/07/16/maxtokensize-and-kerberos-token-bloat.aspx
Authentication Mechanism Assurance	http://technet.microsoft.com/en-us/library/dd391847(v=WS.10).aspx
Microsoft Data Classification Toolkit	http://technet.microsoft.com/en-us/library/hh204743.aspx

Links	URLs
Dynamic Access Control	http://blogs.technet.com/b/windowsserver/archive/2012/05/22/introduction-to-windows-server-2012-dynamic-access-control.aspx
Absolute Software	http://www.absolute.com/en/landing/Google/absolute-software-google/computrace-and-absolute-manage?gclid=CPPh5P6v3rMCFQtxQgodFEQAnA
Absolute Manage	http://www.absolute.com/landing/Google/absolute-manage-google/it-asset-management-software
Absolute Manage MDM	http://www.absolute.com/landing/Google/MDM-google/mobile-device-management
SolarWinds	http://www.solarwinds.com/eminentware-products.aspx
EminentWare WSUS Extension Pack	http://solarwinds-marketing.s3.amazonaws.com/solarwinds/Datasheets/EminentWare-WSUS-Extension-Pack-005-Datasheet2.pdf
EminentWare System Center Configuration Manager Extension Pack	http://solarwinds-marketing.s3.amazonaws.com/solarwinds/Datasheets/EminentWare-Extension-Pack-for-CM-Datasheet-006-Revised.pdf
GFI Software	http://www.gfi.com/?adv=952&loc=58&gclid=CLq9y5603rMCFal7QgodMFkAyA
GFI LanGuard	http://www.gfi.com/network-security-vulnerability-scanner/?adv=952&loc=60&gclid=CP2t-7i03rMCFQuCQgodNkAA7g
Secunia	http://secunia.com/
Secunia Corporate Software Inspector (CSI)	http://secunia.com/products/corporate/csi/
Vulnerability Intelligence Manager	http://secunia.com/vulnerability_intelligence/
eEye Digital Security	http://www.wideeyesecurity.com/?gclid=CK6b0sm13rMCFad_QgodhScAiw
Retina CS Management	http://www.wideeyesecurity.com/produc

Links	URLs
	ts.asp
Lumension	http://www.lumension.com/?rpLeadSourceId=5009&gclid=CKuai_e13rMCFal7QgodMFkAyA
Lumension Vulnerability Management	http://www.lumension.com/Solutions/Vulnerability-Management.aspx
Threats and Countermeasures Guide: User Rights	http://technet.microsoft.com/en-us/library/hh125917(v=ws.10).aspx
Threats and Vulnerabilities Mitigation	http://technet.microsoft.com/en-us/library/cc755181(v=ws.10).aspx
User Rights	http://technet.microsoft.com/en-us/library/dd349804(v=WS.10).aspx
Access Credential Manager as a trusted caller	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_2
Access this computer from the network	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_1
Act as part of the operating system	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_3
Add workstations to domain	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_4
Adjust memory quotas for a process	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_4
Allow log on locally	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_4
Allow log on through Remote Desktop Services	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_4
Back up files and directories	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_4
Bypass traverse checking	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_9

Links	URLs
Change the system time	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_10
Change the time zone	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_11
Create a pagefile	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_12
Create a token object	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_13
Create global objects	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_14
Create permanent shared objects	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_15
Create symbolic links	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_16
Debug programs	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_17
Deny access to this computer from the network	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_18
Deny log on as a batch job	http://technet.microsoft.com/en-us/library/hh125917(v=ws.10).aspx#BKMK_denybatch
Deny log on as a service	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_19
Deny log on locally	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_20
Deny log on through Remote Desktop Services	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_21
Enable computer and user	http://technet.microsoft.com/en-

Links	URLs
accounts to be trusted for delegation	us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_22
Force shutdown from a remote system	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_23
Generate security audits	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_24
Impersonate a client after authentication	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_25
Increase a process working set	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_26
Increase scheduling priority	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_26
Load and unload device drivers	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_28
Lock pages in memory	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_29
Log on as a batch job	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_30
Log on as a service	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_31
Manage auditing and security log	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_32
Modify an object label	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_33
Modify firmware environment values	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_34
Perform volume maintenance tasks	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-

Links	URLs
	e9845182f4b6(v=ws.10)#BKMK_35
Profile single process	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_36
Profile system performance	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_37
Remove computer from docking station	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_38
Replace a process level token	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_39
Restore files and directories	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_40
Shut down the system	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_41
Synchronize directory service data	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_42
Take ownership of files or other objects	http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_43
Access Control	http://msdn.microsoft.com/en-us/library/aa374860(v=VS.85).aspx
Microsoft Support article 251343	http://support.microsoft.com/kb/251343
rootDSE Modify Operations	http://msdn.microsoft.com/en-us/library/cc223297.aspx
AD DS Backup and Recovery Step-by-Step Guide	http://technet.microsoft.com/en-us/library/cc771290(v=ws.10).aspx
Windows Configurations for Kerberos Supported Encryption Type	http://blogs.msdn.com/b/openspecification/archive/2011/05/31/windows-configurations-for-kerberos-supported-encryption-type.aspx
UAC Processes and Interactions	http://technet.microsoft.com/en-us/library/dd835561(v=WS.10).aspx#1

Links	URLs
EmpowerID	http://www.empowerid.com/products/authorizationservices
Role-based access control (RBAC)	http://pic.dhe.ibm.com/infocenter/aix/v7r1/index.jsp?topic=%2Fcom.ibm.aix.security%2Fdoc%2Fsecurity%2Fdomain_rbac.htm
The RBAC model	http://docs.oracle.com/cd/E19082-01/819-3321/6n5i4b7ap/index.html
Active Directory-centric access control	http://www.centrify.com/solutions/it-security-access-control.asp
Cyber-Ark's Privileged Identity Management (PIM) Suite	http://www.cyber-ark.com/digital-vault-products/pim-suite/index.asp
Quest One	http://www.quest.com/landing/?id=7370&gclid=CJnNgNyr3rMCFYp_QgodXFwA3w
Enterprise Random Password Manager (ERPM)	http://www.liebsoft.com/Random_Password_Manager/
NetIQ Privileged User Manager	https://www.netiq.com/products/privileged-user-manager/
CA IdentityMinder™	http://awards.scmagazine.com/ca-technologies-ca-identity-manager
Description of security events in Windows Vista and in Windows Server 2008	http://support.microsoft.com/kb/947226
Description of security events in Windows 7 and in Windows Server 2008 R2	http://support.microsoft.com/kb/977519
Security Audit Events for Windows 7	http://www.microsoft.com/en-us/download/details.aspx?id=21561
Windows Server 2008 R2 and Windows 8 and Windows Server 2012 Security Event Details	http://www.microsoft.com/en-us/download/details.aspx?id=35753
Georgia Tech's Emerging Cyber Threats for 2013 report	http://www.gtsecuritysummit.com/report.html
Microsoft Security Intelligence Report	http://www.microsoft.com/security/sir/default.aspx
Australian Government	http://www.dsd.gov.au/infosec/top35miti

Links	URLs
Defense Signals Directory Top 35 Mitigation Strategies	gationstrategies.htm
Cloud Computing Security Benefits	http://www.microsoft.com/en-us/news/Press/2012/May12/05-14SMBSecuritySurveyPR.aspx
Applying the Principle of Least Privilege to User Accounts on Windows	http://www.microsoft.com/en-us/download/details.aspx?id=4868
The Administrator Accounts Security Planning Guide	http://www.microsoft.com/en-us/download/details.aspx?id=19406
Best Practice Guide for Securing Active Directory Installations for Windows Server 2003	http://www.microsoft.com/en-us/download/details.aspx?id=16755
Best Practices for Delegating Active Directory Administration for Windows Server 2003	http://www.microsoft.com/en-us/download/details.aspx?id=21678
Microsoft Support Lifecycle	http://support.microsoft.com/common/international.aspx?RDPATH=%2flifecycle%2fdefault.aspx
Active Directory Technical Specification	http://msdn.microsoft.com/en-us/library/cc223122(v=prot.20).aspx
Error message when nonadministrator users who have been delegated control try to join computers to a Windows Server 2003-based or a Windows Server 2008-based domain controller: “Access is denied”	http://support.microsoft.com/kb/932455
Authentication Mechanism Assurance for AD DS in Windows Server 2008 R2 Step-by-Step Guide	http://technet.microsoft.com/en-us/library/dd378897(WS.10).aspx
Strict KDC Validation	http://www.microsoft.com/en-us/download/details.aspx?id=6382

Recommended Reading

The following table contains a list of recommended reading that will assist you in enhancing the security of your Active Directory systems.

Recommended Reading
Georgia Tech's Emerging Cyber Threats for 2013 Report
Microsoft Security Intelligence Report
Mitigating Pass-the-Hash (PTH) Attacks and Other Credential Theft Techniques
Australian Government Defense Signals Directory Top 35 Mitigation Strategies
2012 Data Breach Investigations Report - (Verizon, US Secret Service)
2009 Data Breach Investigations Report
Cloud Computing Security Benefits
Applying the Principle of Least Privilege to User Accounts on Windows
The Administrator Accounts Security Planning Guide
Best Practice Guide for Securing Active Directory Installations for Windows Server 2003
Best Practices for Delegating Active Directory Administration for Windows Server 2003
Microsoft Support Lifecycle
Active Directory Technical Specification - dSHeuristics information
Error message when nonadministrator users who have been delegated control try to join computers to a Windows Server 2003-based or a Windows Server 2008-based domain controller: "Access is denied"
Best Practice Guide for Securing Active Directory Installations.doc
Hyper-V Security Guide
Authentication Mechanism Assurance for AD DS in Windows Server 2008 R2 Step-

Recommended Reading
by-Step Guide.
Strict KDC Validation

Copyright Information