

Information Technology

Assessment Document

Pace Domain Assessment

Table of Contents

[Team Members 3](#_Toc520446367)

[Revision History 3](#_Toc520446368)

[Approval Signatures 3](#_Toc520446369)

[1 Introduction 4](#_Toc520446370)

[2 Purpose 4](#_Toc520446371)

[3 Scope 4](#_Toc520446372)

[4 Pace Domain Assessment 4](#_Toc520446373)

[5 Pace Site Assessment 5](#_Toc520446374)

[6 Pace OU and Group Policy Assessment 6](#_Toc520446375)

[7 Next Steps 6](#_Toc520446376)

[7.1 Group Polices 6](#_Toc520446377)

[7.2 Hosts 6](#_Toc520446378)

[7.3 Networks 6](#_Toc520446379)

[7.4 Internet 7](#_Toc520446380)

[7.5 Remote Access 7](#_Toc520446381)

[8 Appendix 7](#_Toc520446382)

[8.1 Pace Group Policy Settings 7](#_Toc520446383)

[8.1.1 Group Policy: Automatic Updates 7](#_Toc520446384)

[8.1.2 Group Policy: No Updates 7](#_Toc520446385)

[8.1.3 Group Policy: Drives 7](#_Toc520446386)

[8.1.4 Group Policy: Redirect User Files (Disabled Policy) 8](#_Toc520446387)

[8.1.5 Group Policy: User File Redirection (Disabled Policy) 8](#_Toc520446388)

[8.1.6 Group Policy: WMI Enable 8](#_Toc520446389)

[8.1.1 Group Policy: Default Domain Policy 9](#_Toc520446390)

[8.1.2 Group Policy: LPI MW Default Group Policy 10](#_Toc520446391)

[8.1.3 Group Policy: Default Domain Controllers Policy 12](#_Toc520446392)

[8.2 Gates NA Domain versus Pace Domain 14](#_Toc520446393)

[8.2.1 Group Policy: Gates NA Default Domain Policy 14](#_Toc520446394)

[8.2.2 Group Policy: Pace Domain Default Domain Policy 14](#_Toc520446395)

[8.2.3 Group Policy Changes Suggested in Pace Domain 15](#_Toc520446396)

[8.3 Reference Default Domain Policies 15](#_Toc520446397)

[8.3.1 Group Policy: Gates NA Default Domain Policy 15](#_Toc520446398)

[8.3.2 Group Policy: Pace Domain Default Domain Policy 16](#_Toc520446399)

[8.4 Domain Scripts 17](#_Toc520446400)

[8.4.1 Startup Scripts 17](#_Toc520446401)

# Team Members

|  |  |  |  |
| --- | --- | --- | --- |
| Team Member Name | Location | Member Email | Member Telephone Number |
| Philip Robley | Denver, CO | [Phil.Robley@gates.com](mailto:Phil.Robley@gates.com) | 303-774-5878 |
| Ramesh | Denver, CO | [Ramesh.Thangamani@gates.com](mailto:Ramesh.Thangamani@gates.com) | 303-774-5156 |
| Ken Maybee | Denver, CO | [Ken.Maybee@gates.com](mailto:Ken.Maybee@gates.com) | 303-744-4764 |
|  |  |  |  |

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Document Version | Description of Change | Author of Change | Effective Date (MM/DD/YYYY) |
| 1.0 | Initial Draft | Philip Robley / Ramesh T | 7/13/2018 |
| 1.5 | Additional Information | Ken Maybee | 7/19/2018 |
| 2.0 | Group Policy updates | Ken Maybee | 7/27/2018 |
|  |  |  |  |

# Approval Signatures

|  |  |  |
| --- | --- | --- |
| Signature | Department | Date (MM/DD/YYYY) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Introduction

Gates Corporation has recently acquired a new business unit called Pace.

The process of integrating a newly acquired business unit could have a drastic impact on the security of Gates Corporation and or the Pace.

The network and security infrastructure of both companies may vary greatly. This document describes the infrastructure items that were reviewed during the domain assessment for the Pace.

The following individuals are potential users of information in this document, either directly or through other derived documentation:

* The Gates Corporation IT management team.
* The Gates Corporation IT Infrastructure team.
* Anyone interested in the architectural and technical details of the subject.

# Purpose

The purpose of this domain assessment is to establish responsibilities regarding the corporate acquisition, and define the minimum security and infrastructure requirements for the acquisition of the Pace. This assessment will provide a single source of information that will be useful in the structuring, development and executing the acquisition strategy.

# Scope

Preform an acquisition assessment to ensure that the Pace being acquired by Gates Corporation does not pose a security risk to corporate networks, internal systems, and/or confidential/sensitive information.

The Gates Corporation’s role is to detect and evaluate information security risk, develop a remediation plan with the affected parties for the identified risk, and work with the acquisitions team to implement solutions for any identified security risks, prior to allowing connectivity to Pace's networks.

# Pace Domain Assessment

The Pace domain is a single forest and single domain structure that has a PKI root installed. Upon initial the evaluation of the domain it appears to be a flat structure.

The Pace domain has two Domain Controllers one in each site.

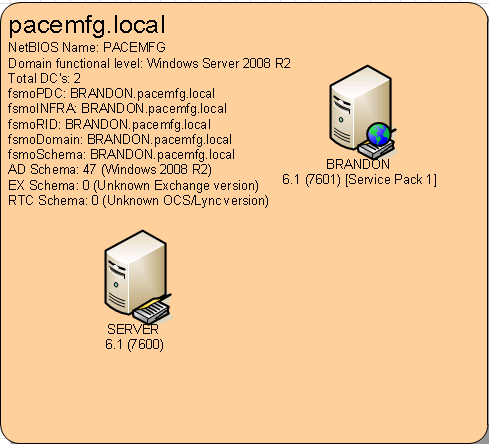
The FSMO roles are found on a single domain controller (BRANDON).

The domain functional level for Pace is Windows server 2008 R2.

The Pace has a total of eighty six (86) computers and one hundred and thirteen (113) total users.

Seventy two (72) users have passwords that never expire.

See below:



# Pace Site Assessment

The Pace’s site structure has only one site Brandon using the following subnets:

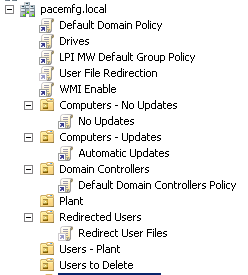
* 10.40.136.0/24
* 10.40.138.0/24
* 10.40.148.0/24
* 192.168.31.0/24

The Pace has the following computer objects that have been discovered:

|  |  |
| --- | --- |
| Operating System | Count |
| Windows Server 2008 R2 Standard | 2 |
| Windows XP Professional | 1 |
| Windows 7 Professional | 73 |
| Windows 8.1 Enterprise | 8 |
| Windows 10 Pro | 1 |
| Surface | 1 |

# Pace OU and Group Policy Assessment

The Pace has the following OU structure and GPO objects that have been discovered:



# Next Steps

Below are the minimum requirements that Pace should be met before being connected to the Gates Corporation network.

## Group Polices

The Pace Default Domain Policy needs changes to confirm to Gates Corporation stronger password policies security settings. Please see **section 8.2.3 Group Policy Changes Suggested in Pace Domain.**

**.**

## Hosts

All hosts (servers, desktops, laptops) will be replaced or re-imaged with a Gates Corporation standard image or will be required to adopt the minimum standards for end user devices.

Business critical production servers that cannot be replaced or re-imaged must be audited by Gates Corporation.

All PC based hosts will require Gates Corporation approved virus protection or audit Pace virus protection on all existing host before the PC connects to the network.

## Networks

All network devices will be replaced or re-imaged with a Gates Corporation standard image.

Wireless network access points will be configured to the Gates Corporation standard.

**Note:** LAN refresh has already happened. Gates standard Cisco gear is in place as well as standard Palo Alto firewall.

## Internet

All Internet connections will be terminated.

## Remote Access

All remote access connections will be terminated.

Remote access to the production network will be provided by Gates Corporation.

# Appendix

## Pace Group Policy Settings

### Group Policy: Automatic Updates

|  |  |  |
| --- | --- | --- |
| Group Policy: Automatic Updates | | |
| General policy settings | | |
| Links | **Applied to:** pacemfg.local/Computers – Updates OU. | |
| Security filtering | **Applied to:** Authenticated Users (All Computers ) | |
| Delegation | Domain and Enterprise Administrators | |
| User Configuration | | |
| Disabled |  | |
| Computer Configuration | | |
| Administrative Templates\Windows Components\Windows Update | | Auto download and schedule the install Every day at 01:00 |

### Group Policy: No Updates

|  |  |  |
| --- | --- | --- |
| Group Policy: No Updates | | |
| General policy settings | | |
| Links | **Applied to:** pacemfg.local/Computers – Updates OU. | |
| Security filtering | **Applied to:** All Computers | |
| Delegation | Domain and Enterprise Administrators | |
| User Configuration | | |
| Disabled | |  |
| Computer Configuration | | |
| Administrative Templates\Windows Components\Windows Update | | Auto download and schedule the install Every day at 01:00 |

### Group Policy: Drives

|  |  |  |
| --- | --- | --- |
| Group Policy: Drives | | |
| General policy settings | | |
| Links | **Applied to:** pacemfg.local (Domain Root) | |
| Security filtering | **Applied to:** Authenticated Users (All Computers and Computers) | |
| Delegation | Domain and Enterprise Administrators | |
| User Configuration | | |
| Preferences\Windows Settings\Drive Maps | | Map S: to \\brandon\shared |
| Computer Configuration | | |
| No settings deployed. | |  |

### Group Policy: Redirect User Files (Disabled Policy)

|  |  |  |  |
| --- | --- | --- | --- |
| Group Policy: Redirect User Files (Disabled Policy) | | | |
| General policy settings | | | |
| Links | **Applied to:** pacemfg.local/Redirected Users | | |
| Security filtering | **Applied to:** Authenticated Users (All Computers ) | | |
| Delegation | Domain and Enterprise Administrators | | |
| User Configuration | | | |
| Windows Settings\Folder Redirection\Desktop | | | Path: \\brandon\users\%username% |
| Windows Settings\Folder Redirection\AppData(Roaming) | | | Path: \\brandon\users\%username% |
| Computer Configuration | | | |
| No settings deployed | |  | |

### Group Policy: User File Redirection (Disabled Policy)

|  |  |  |  |
| --- | --- | --- | --- |
| Group Policy: User File Redirection (Disabled Policy) | | | |
| General policy settings | | | |
| Links | **Applied to:** pacemfg.local (Domain Root) | | |
| Security filtering | **Applied to:** PACEMFG\Users w\_ Server Folder Sync | | |
| Delegation | Domain and Enterprise Administrators | | |
| User Configuration | | | |
| Windows Settings\Folder Redirection\AppData(Roaming) | | Path: Redirect to local user profile path | |
| Windows Settings\Folder Redirection\Contacts | | Path: Redirect to local user profile path | |
| Windows Settings\Folder Redirection\Desktop | | Path: Redirect to local user profile path | |
| Windows Settings\Folder Redirection\Documents | | Path: Redirect to local user profile path | |
| Windows Settings\Folder Redirection\Downloads | | Path: Redirect to local user profile path | |
| Windows Settings\Folder Redirection\Favorites | | Path: Redirect to local user profile path | |
| Windows Settings\Folder Redirection\Links | | Path: Redirect to local user profile path | |
| Windows Settings\Folder Redirection\Music | | Setting: Follow the Documents Folder | |
| Windows Settings\Folder Redirection\Pictures | | Setting: Follow the Documents Folder | |
| Windows Settings\Folder Redirection\Start Menu | | Path: Redirect to local user profile path | |
| Windows Settings\Folder Redirection\Videos | | Setting: Follow the Documents Folder | |
| Computer Configuration | | | |
| Administrative Templates\Network\Offline Files\Default cache size | | | Enabled |

### Group Policy: WMI Enable

|  |  |  |
| --- | --- | --- |
| Group Policy: WMI Enable | | |
| General policy settings | | |
| Links | **Applied to:** pacemfg.local (Domain Root) | |
| Security filtering | **Applied to:** Authenticated Users (All Computers ) | |
| Delegation | Domain and Enterprise Administrators | |
| User Configuration | | |
| No settings deployed | |  |
| Computer Configuration | | |
| Windows Settings\Security Settings\Windows Firewall with Advanced Security\Global Settings | | Policy Version: 2.10 |
| Windows Settings\Security Settings\Windows Firewall with Advanced Security\Inbound Rules | | Windows Management Instrumentation (ASync-In)  Inbound rule to allow Asynchronous WMI traffic for remote Windows Management Instrumentation. [TCP] |
| Windows Settings\Security Settings\Windows Firewall with Advanced Security\Inbound Rules | | Windows Management Instrumentation (WMI-In)  Inbound rule to allow WMI traffic for remote Windows Management Instrumentation. [TCP] |
| Windows Settings\Security Settings\Windows Firewall with Advanced Security\Inbound Rules | | Windows Management Instrumentation (DCOM-In)  Inbound rule to allow DCOM traffic for remote Windows Management Instrumentation. [TCP 135] |

### Group Policy: Default Domain Policy

|  |  |  |
| --- | --- | --- |
| Group Policy: Default Domain Policy | | |
| General policy settings | | |
| Links | **Applied to:** pacemfg.local (Domain Root) | |
| Security filtering | **Applied to:** Authenticated Users (All Computers and Users) | |
| Delegation | Domain and Enterprise Administrators | |
| User Configuration | | |
| No settings deployed | |  |
| Computer Configuration | | |
| Windows Settings\Security Settings\Account Policies\Password Policy | | Minimum password length: 3 characters  Password must meet complexity requirements: Disabled  Store passwords using reversible encryption: Disabled |
| Windows Settings\Security Settings\Account Policies\Account Lockout Policy | | Account lockout threshold: 0 invalid logon attempts |
| Windows Settings\Security Settings\Account Policies\Kerberos Policy | | Enforce user logon restrictions: Enabled  Maximum lifetime for service ticket: 600 minutes  Maximum lifetime for user ticket: 10 hours  Maximum lifetime for user ticket renewal: 7 days  Maximum tolerance for computer clock synchronization: 5 minutes |
| Windows Settings\Security Settings\Local Policies\Security Options\Network Access | | Network access: Allow anonymous SID/Name translation: Disabled |
| Windows Settings\Security Settings\Local Policies\Security Options\Network Security | | Network security: Do not store LAN Manager hash value on next password change: Enabled  Network security: Force logoff when logon hours expire: Disabled |
| Windows Settings\Security Settings\ Wireless Network (802.11) Policies\ New  Wireless Network Policy | | Policy Name: New Wireless Network Policy  Policy Description: Sample Description  Policy Type: Windows Vista and Later Releases |
| Windows Settings\Security Settings\ Wireless Network (802.11) Policies\Global Settings | | Use Windows wireless LAN network services for clients: Enabled  Shared user credentials for network authentication: Enabled  Hosted networks: Enabled  Allow user to view denied networks: Enabled  Allow everyone to create all user profiles: Enabled  Only use Group Policy profiles for allowed networks: Disabled |
| Windows Settings\Security Settings\ Wireless Network (802.11) Policies\Network Filters | | Prevent connection to infrastructure networks: Disabled  Prevent connection to adhoc networks: Disabled |
| Windows Settings\Security Settings\ Public Key Policies\Encrypting File System\ Certificates | | Issued To: Administrator  Issued By: Administrator  Expiration Date: 5/1/2111 5:05:53 PM  Intended Purposes: File Recovery |
| Windows Settings\Security Settings\Public Key Policies\ Trusted Root Certification Authorities | | Allow users to select new root certification authorities (CAs) to trust: Enabled  Client computers can trust the following certificate stores:  Third-Party Root Certification Authorities and Enterprise Root Certification Authorities  To perform certificate-based authentication of users and computers, CAs must meet the following criteria:  Registered in Active Directory only |
| Administrative Templates\Windows Components\Windows Update | | Allow Automatic Updates immediate installation: Enabled  Configure Automatic Updates: Enabled  Auto download and notify for install Every day at 03:00 |

### Group Policy: LPI MW Default Group Policy

|  |  |  |  |
| --- | --- | --- | --- |
| Group Policy: LPI MW Default Group Policy | | | |
| General policy settings | | | |
| Links | **Applied to:** pacemfg.local (Domain Root) | | |
| Security filtering | **Applied to:** Authenticated Users (All Computers) | | |
| Delegation | Domain and Enterprise Administrators | | |
| User Configuration | | | |
| No settings deployed | | |  |
| Computer Configuration | | | |
| Windows Settings\Scripts\Startup | | Domain\_Sample\_Startup\_Script.vbs | |
| Security Settings\System Services\Background Intelligent Transfer Service (Startup Mode: Automatic) | | **Permissions:** No permissions specified  **Auditing:** No auditing specified | |
| Security Settings\System Services \Remote Registry (Startup Mode: Automatic) | | **Permissions:** No permissions specified  **Auditing:** No auditing specified | |
| Security Settings\System Services\Remote Procedure Call (RPC) (Startup Mode: Automatic) | | **Permissions:** No permissions specified  **Auditing:** No auditing specified | |
| Security Settings\System Services\Windows Management Instrumentation (Startup Mode: Automatic) | | **Permission**  Allow: NT AUTHORITY\SYSTEM: Full Control  Allow: BUILTIN\Administrators: Full Control  Allow: NT AUTHORITY\Authenticated Users: Read  Allow: NT AUTHORITY\INTERACTIVE: Read  **Auditing**  Failure: Everyone: Full Control | |
| Security Settings\System Services\Windows Remote Management (WS-Management) (Startup Mode: Automatic) | | **Permissions:** No permissions specified  **Auditing:** No auditing specified | |
| Security Settings\System Services\Windows Update (Startup Mode: Automatic) | | **Permissions:** No permissions specified  **Auditing:** No auditing specified | |
| Security Settings Windows Firewall with Advanced Security\ Global Settings | | Policy Version: 2.10 | |
| Windows Settings\Security Settings\Windows Firewall with Advanced Security\Inbound Rules | | Remote Event Log Management (RPC-EPMAP)  Inbound rule for the RPCSS service to allow RPC/TCP traffic for the local Event Log Service. | |
| Windows Settings\Security Settings\Windows Firewall with Advanced Security\Inbound Rules | | Remote Event Log Management (NP-In)  Inbound rule for the local Event Log service to be remotely managed over Named Pipes. | |
| Windows Settings\Security Settings\Windows Firewall with Advanced Security\Inbound Rules | | Remote Event Log Management (RPC)  Inbound rule for the local Event Log service to be remotely managed via RPC/TCP. | |
| Windows Settings\Security Settings\Windows Firewall with Advanced Security\Inbound Rules | | Windows Management Instrumentation (WMI-In)  Inbound rule to allow WMI traffic for remote Windows Management Instrumentation. [TCP] | |
| Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile\ Windows Firewall: Allow ICMP exceptions | | Allow outbound destination unreachable: Disabled  Allow outbound source quench: Disabled  Allow redirect: Disabled  Allow inbound echo request: **Enabled**  Allow inbound router request: Disabled  Allow outbound time exceeded: Disabled  Allow outbound parameter problem: Disabled  Allow inbound timestamp request: Disabled  Allow inbound mask request: Disabled  Allow outbound packet too big: Disabled | |
| Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile\Windows Firewall: Allow inbound file and printer sharing exception | | Enabled | |
| Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile\ Windows Firewall: Allow inbound remote administration exception | | Enabled | |
| Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile\ Windows Firewall: Allow inbound Remote Desktop exceptions | | Enabled | |
| Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile\ Windows Firewall: Define inbound port exceptions | | Enabled  Define port exceptions:  5985:TCP:192.168.31.10:enabled:WinRM | |
| Administrative Templates\System\Remote Assistance | | Enabled | |
| Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections\Allow users to connect remotely using Remote Desktop Services | | Enabled | |
| Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Trusted Hosts | | Enabled | |
| Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow remote server management through WinRM | | Enabled | |

### Group Policy: Default Domain Controllers Policy

|  |  |  |  |
| --- | --- | --- | --- |
| Group Policy: Default Domain Controllers Policy | | | |
| General policy settings | | | |
| Links | **Applied to:** pacemfg.local\Domain Controllers | | |
| Security filtering | **Applied to:** Authenticated Users (All Computers) | | |
| Delegation | Domain and Enterprise Administrators | | |
| User Configuration | | | |
| No settings deployed | |  | |
| Computer Configuration | | | |
| Windows Settings\Security Settings\Local Policies\User Rights Assignment | | | **Access this computer from the network**  BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, Everyone  **Add workstations to domain**  NT AUTHORITY\Authenticated Users  **Adjust memory quotas for a process**  NT SERVICE\SQLAgent$LPIMWOMEXPRESS, IIS APPPOOL\DefaultAppPool, BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, NT SERVICE\MSSQL$LPIMWOMEXPRESS  **Allow log on locally**  PACEMFG\MWService, BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Account Operators, BUILTIN\Backup Operators, BUILTIN\Administrators  **Back up files and directories**  BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators  **Bypass traverse checking**  NT SERVICE\SQLAgent$LPIMWOMEXPRESS, BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, Everyone, NT SERVICE\MSSQL$LPIMWOMEXPRESS  **Change the system time**  BUILTIN\Server Operators, BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE  **Create a pagefile**  BUILTIN\Administrators  **Debug programs**  BUILTIN\Administrators  **Enable computer and user accounts to be trusted for delegation**  BUILTIN\Administrators  **Force shutdown from a remote system**  BUILTIN\Server Operators, BUILTIN\Administrators  **Generate security audits**  IIS APPPOOL\DefaultAppPool, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE  **Increase scheduling priority**  BUILTIN\Administrators  **Load and unload device drivers**  BUILTIN\Print Operators, BUILTIN\Administrators  **Log on as a batch job**  BUILTIN\Performance Log Users, BUILTIN\Backup Operators, BUILTIN\Administrators, BUILTIN\IIS\_IUSRS, PACEMFG\MWService  **Manage auditing and security log**  BUILTIN\Administrators  **Modify firmware environment values**  BUILTIN\Administrators  **Profile single process**  BUILTIN\Administrators  Profile system performance NT SERVICE\WdiServiceHost,  BUILTIN\Administrators  **Remove computer from docking station**  BUILTIN\Administrators  **Replace a process level token**  NT SERVICE\SQLAgent$LPIMWOMEXPRESS, IIS APPPOOL\DefaultAppPool, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, NT SERVICE\MSSQL$LPIMWOMEXPRESS  **Restore files and directories**  BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators  **Shut down the system**  BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators  **Take ownership of files or other objects**  BUILTIN\Administrators |
| Windows Settings\Security Settings\Local  Policies\Security Options\Domain Controller\ Domain controller: LDAP server signing requirements | | | None |
| Windows Settings\Security Settings\Local  Policies\Security Options\Domain Member\ Domain member: Digitally encrypt or sign secure channel data (always) | | | Enabled |
| Windows Settings\Security Settings\Local  Policies\Security Options\Microsoft Network Server\Microsoft network server: Digitally sign communications (always) | | | Enabled |

## Gates NA Domain versus Pace Domain

The Gates NA Default Domain Policy contains several stronger password policies than the Pace Domain. Please see the **Group Policy Changes Suggested in Pace Domain** section below.

### Group Policy: Gates NA Default Domain Policy

|  |  |  |
| --- | --- | --- |
| Group Policy: Gates NA Default Domain Policy | | |
| General policy settings | | |
| Links | **Applied to:** na.corp (Domain Root) | |
| Security filtering | **Applied to:** Authenticated Users (All Computers and Users) | |
| Delegation | Domain and Enterprise Administrators | |
| User Configuration | | |
| No settings deployed | |  |
| Computer Configuration | | |
| Windows Settings\Security Settings\Account Policies\Password Policy | | Enforce password history: 24 passwords remembered  Maximum password age: 90 days  Minimum password age: 1 days  Minimum password length: 8 characters  Password must meet complexity requirements: Enabled  Store passwords using reversible encryption: Disabled |
| Windows Settings\Security Settings\Account Policies\Account Lockout Policy | | Account lockout duration: 30 minutes  Account lockout threshold: 5 invalid logon attempts  Reset account lockout counter after: 30 minutes |

### Group Policy: Pace Domain Default Domain Policy

|  |  |  |
| --- | --- | --- |
| Group Policy: Pace Default Domain Policy | | |
| General policy settings | | |
| Links | **Applied to:** pacemfg.local (Domain Root) | |
| Security filtering | **Applied to:** Authenticated Users (All Computers and Users) | |
| Delegation | Domain and Enterprise Administrators | |
| User Configuration | | |
| No settings deployed | |  |
| Computer Configuration | | |
| Windows Settings\Security Settings\Account Policies\Password Policy | | Minimum password length: 3 characters  Password must meet complexity requirements: Disabled  Store passwords using reversible encryption: Disabled |
| Windows Settings\Security Settings\Account Policies\Account Lockout Policy | | Account lockout threshold: 0 invalid logon attempts |

### Group Policy Changes Suggested in Pace Domain

|  |  |  |
| --- | --- | --- |
| Group Policy: Changes Suggested on Pace Domain | | |
| General policy settings | | |
| Links | **Applied to:** pacemfg.local (Domain Root) | |
| Security filtering | **Applied to:** Authenticated Users (All Computers and Users) | |
| Delegation | Domain and Enterprise Administrators | |
| User Configuration | | |
| No settings deployed | |  |
| Computer Configuration | | |
| Windows Settings\Security Settings\Account Policies\Password Policy | | **Enforce password history: 24 passwords remembered**  **Maximum password age: 90 days**  **Minimum password age: 1 days**  **Minimum password length: 8 characters**  **Password must meet complexity requirements: Enabled**  Store passwords using reversible encryption: Disabled |
| Windows Settings\Security Settings\Account Policies\Account Lockout Policy | | **Account lockout duration: 30 minutes**  **Account lockout threshold: 5 invalid logon attempts**  **Reset account lockout counter after: 30 minutes** |

## Reference Default Domain Policies

### Group Policy: Gates NA Default Domain Policy

|  |  |  |
| --- | --- | --- |
| Group Policy: Gates NA Default Domain Policy | | |
| General policy settings | | |
| Links | **Applied to:** na.corp (Domain Root) | |
| Security filtering | **Applied to:** Authenticated Users (All Computers and Users) | |
| Delegation | Domain and Enterprise Administrators | |
| User Configuration | | |
| No settings deployed | |  |
| Computer Configuration | | |
| Windows Settings\Security Settings\Account Policies\Password Policy | | Enforce password history: 24 passwords remembered  Maximum password age: 90 days  Minimum password age: 1 days  Minimum password length: 8 characters  Password must meet complexity requirements: Enabled  Store passwords using reversible encryption: Disabled |
| Windows Settings\Security Settings\Account Policies\Account Lockout Policy | | Account lockout duration: 30 minutes  Account lockout threshold: 5 invalid logon attempts  Reset account lockout counter after: 30 minutes |
| Windows Settings\Security Settings\Account Policies\Kerberos Policy | | Enforce user logon restrictions: Enabled  Maximum lifetime for service ticket: 600 minutes  Maximum lifetime for user ticket: 10 hours  Maximum lifetime for user ticket renewal: 7 days  Maximum tolerance for computer clock synchronization:5 minutes |
| Windows Settings\Security Settings\Local Policies\Security Options\Network Access | | Network access: Allow anonymous SID/Name translation: Disabled |
| Windows Settings\Security Settings\Local Policies\Security Options\Network Security | | Network security: Do not store LAN Manager hash value on next password change: Enabled  Network security: Force logoff when logon hours expire: Disabled |
| User Configuration | | |
| Windows Settings\Remote Installation Services\Client Installation Wizard Options | | Custom Setup: Disabled  Restart Setup: Disabled  Tools: Disabled |

### Group Policy: Pace Domain Default Domain Policy

|  |  |  |
| --- | --- | --- |
| Group Policy: Pace Default Domain Policy | | |
| General policy settings | | |
| Links | **Applied to:** pacemfg.local (Domain Root) | |
| Security filtering | **Applied to:** Authenticated Users (All Computers and Users) | |
| Delegation | Domain and Enterprise Administrators | |
| User Configuration | | |
| No settings deployed | |  |
| Computer Configuration | | |
| Windows Settings\Security Settings\Account Policies\Password Policy | | Minimum password length: 3 characters  Password must meet complexity requirements: Disabled  Store passwords using reversible encryption: Disabled |
| Windows Settings\Security Settings\Account Policies\Account Lockout Policy | | Account lockout threshold: 0 invalid logon attempts |
| Windows Settings\Security Settings\Account Policies\Kerberos Policy | | Enforce user logon restrictions: Enabled  Maximum lifetime for service ticket: 600 minutes  Maximum lifetime for user ticket: 10 hours  Maximum lifetime for user ticket renewal: 7 days  Maximum tolerance for computer clock synchronization: 5 minutes |
| Windows Settings\Security Settings\Local Policies\Security Options\Network Access | | Network access: Allow anonymous SID/Name translation: Disabled |
| Windows Settings\Security Settings\Local Policies\Security Options\Network Security | | Network security: Do not store LAN Manager hash value on next password change: Enabled  Network security: Force logoff when logon hours expire: Disabled |
| Windows Settings\Security Settings\ Wireless Network (802.11) Policies\ New  Wireless Network Policy | | Policy Name: New Wireless Network Policy  Policy Description: Sample Description  Policy Type: Windows Vista and Later Releases |
| Windows Settings\Security Settings\ Wireless Network (802.11) Policies\Global Settings | | Use Windows wireless LAN network services for clients: Enabled  Shared user credentials for network authentication: Enabled  Hosted networks: Enabled  Allow user to view denied networks: Enabled  Allow everyone to create all user profiles: Enabled  Only use Group Policy profiles for allowed networks: Disabled |
| Windows Settings\Security Settings\ Wireless Network (802.11) Policies\Network Filters | | Prevent connection to infrastructure networks: Disabled  Prevent connection to adhoc networks: Disabled |
| Windows Settings\Security Settings\ Public Key Policies\Encrypting File System\ Certificates | | Issued To: Administrator  Issued By: Administrator  Expiration Date: 5/1/2111 5:05:53 PM  Intended Purposes: File Recovery |
| Windows Settings\Security Settings\Public Key Policies\ Trusted Root Certification Authorities | | Allow users to select new root certification authorities (CAs) to trust: Enabled  Client computers can trust the following certificate stores:  Third-Party Root Certification Authorities and Enterprise Root Certification Authorities  To perform certificate-based authentication of users and computers, CAs must meet the following criteria:  Registered in Active Directory only |
| Administrative Templates\Windows Components\Windows Update | | Allow Automatic Updates immediate installation: Enabled  Configure Automatic Updates: Enabled  Auto download and notify for install Every day at 03:00 |

## Domain Scripts

### Startup Scripts

**Script: Domain\_Sample\_Startup\_Script.vbs**

Set WSHShell = WScript.CreateObject("WScript.Shell")

'To Enable Remote DCOM in the computer

WshShell.RegWrite "HKLM\SOFTWARE\Microsoft\Ole\EnableDCOM","Y","REG\_SZ"

'To Set Authentication Level to Connect

WshShell.RegWrite "HKLM\SOFTWARE\Microsoft\Ole\LegacyAuthenticationLevel",2,"REG\_DWORD"

'To Set Impersonation level to Impersonate

WshShell.RegWrite "HKLM\SOFTWARE\Microsoft\Ole\LegacyImpersonationLevel",3,"REG\_DWORD"