GP.Pismere

Data collected on: 7/29/2003 1:26:51 PM

General

Details

Domain	WIN.MIT.EDU
Owner	WIN\Domain Admins
Created	3/2/2001 7:26:50 PM
Modified	7/7/2003 3:58:24 PM
User Revisions	91 (AD), 91 (sysvol)
Computer Revisions	152 (AD), 152 (sysvol)
Unique ID	{31B2F340-016D-11D2-945F-00C04FB984F9}
GPO Status	Enabled

Links

Location	Enforced	Link Status	Path
WIN	No	Disabled	WIN.MIT.EDU
Machines	No	Enabled	WIN.MIT.EDU/Machines
JustTesting	Yes	Disabled	WIN.MIT.EDU/Machines/JustT
Moira	No	Enabled	WIN.MIT.EDU/Moira
RIS	No	Enabled	WIN.MIT.EDU/RIS

This list only includes links in the domain of the GPO.

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
NT AUTHORITY\Authenticated Users

WMI Filtering

WMI Filter Name	None
Description	Not applicable

Delegation

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No
WIN\Domain Admins	Edit settings, delete, modify security	No
WIN\Enterprise Admins	Edit settings, delete, modify security	No

Computer Configuration (Enabled)

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout threshold	0 invalid logon attempts

Account Policies/Kerberos Policy

Policy	Setting
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

Local Policies/Audit Policy

Policy	Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit logon events	Success, Failure
Audit object access	Failure
Audit policy change	Success, Failure

Local Policies/Security Options

Interactive Logon

Policy	Setting
Interactive logon: Do not display last user name	Enabled

Network Security

Policy	Setting
Network security: Force logoff when logon hours expire	Disabled

System Services

Messenger (Startup Mode: Manual)

Permissions

Type	Name	Permission
Allow	BUILTIN\Administrators	Full Control
Allow	NT AUTHORITY\Authenticated Users	Read
Allow	BUILTIN\Power Users	Read
Allow	BUILTIN\Power Users	Start, Stop, Pause and continue
Allow	NT AUTHORITY\SYSTEM	Full Control

Auditing
No auditing specified

IBM AFS Client (Startup Mode: Automatic)

Permissions

Type	Name	Permission
Allow	BUILTIN\Administrators	Full Control
Allow	NT AUTHORITY\Authenticated Users	Read
Allow	NT AUTHORITY\Authenticated Users	Start, Stop, Pause and continue
Allow	WIN\Domain Admins	Full Control
Allow	NT AUTHORITY\SYSTEM	Full Control

Auditing
No auditing specified

File System

%SystemRoot%\system32\RestrictedSnapIns

Do not allow permissions on this file or folder to be replaced

Public Key Policies/Autoenrollment Settings

Policy	Setting
Enroll certificates automatically	Enabled
Renew expired certificates, update pending certificates, and remove revoked certificates	Disabled
Update certificates that use certificate templates	Disabled

Public Key Policies/Encrypting File System

Properties

Policy	Setting
Allow users to encrypt files using Encrypting File System (EFS)	Enabled

Certificates

Issued To	Issued By	Expiration Date	Intended Purposes
Administrator	Administrator	3/1/2004 7:37:00 PM	File Recovery

For additional information about individual settings, launch Group Policy Object Editor.

Public Key Policies/Trusted Root Certification Authorities

Properties

Policy	Setting
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 Certifica Authorities
To perform certificate-based authentication of users and computers, CAs must meet the following criteria	Registered in Active Directory only

Administrative Templates

Network/DNS Client

Policy	Setting
Dynamic Update	Disabled

System

Policy	Setting
Turn off Autoplay	Enabled
Turn off Autoplay on:	All drives"

System/Group Policy

Policy	Setting
Scripts policy processing	Enabled
Allow processing across a slow network connection	Enabled
Do not apply during periodic background processing	Disabled
Process even if the Group Policy objects have not changed	Enabled

System/Logon

Policy	Setting
Always wait for the network at computer startup and logon	Enabled

System/Scripts

Policy	Setting
Run logon scripts synchronously	Enabled

System/User Profiles

Policy	Setting
Delete cached copies of roaming profiles	Enabled
Do not detect slow network connections	Enabled