

Effective Server Security Options

Period: **Last 20 week(s)**
 Generated: **Friday, January 11, 2008 3:12:25 PM**
 For: **Brian Bartlett bbartlett@ecora.com**
 By: Ecora Auditor Professional 4.5 - Windows Module 4.5.8010.20310
 Using: Customized FFR Definition based on 'Effective Server Security Options'
 Description: A Fact-Finding report will show values greater than, less than, or unlike a threshold value you set. These reports are very surgical in their precision - you can pull precisely the data you need, but they also offer a wealth of data through hundreds of built-in reports created by experts.

Effective Server Security Options

Table of Contents

Security Options 1

Collected Not-Collected Legend

DEFAULT	The value presented in the report was not directly reported by the target, but implied by the current value or lack of a value for the attribute
UA	Unavailable attribute. The current configuration or version of target platform does not provide a value for this attribute. More detail in logs
FC	Collection of value failed
NS	Value not selected for collection

Security Options

Table 1. BSP/BIGMOUNTAIN

Security Option	Security Option Settings	Overridden By GPO
Accounts: Limit local account use of blank passwords to console logon only	Enabled	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Devices: Allow undock without having to log on	Enabled	
Devices: Prevent users from installing printer drivers	Enabled	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}

Security Option	Security Option Settings	Overridden By GPO
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Devices: Restrict floppy access to locally logged-on user only	Enabled	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Devices: Unsigned driver installation behavior	Warn but allow installation	
Domain controller: Allow server operators to schedule tasks	Enabled	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Domain controller: LDAP server signing requirements	None	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Domain member: Disable machine account password changes	Disabled	
Domain member: Require strong (Windows 2000 or later) session key	Disabled	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Interactive logon: Do not display last user name	Enabled	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Interactive logon: Prompt user to change password before expiration	14 days	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Microsoft network server: Digitally sign communications (always)	Enabled	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Microsoft network server: Digitally sign communications (if client agrees)	Enabled	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}

Security Option	Security Option Settings	Overridden By GPO
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Network access: Do not allow storage of credentials or .NET Passports for network authentication	Disabled	
Network access: Let Everyone permissions apply to anonymous users	Disabled	
Network access: Named Pipes that can be accessed anonymously	COMNAP COMNODE SQL\QUERY SPOOLSS LLSRPC TrkSrv netlogon lsarpc samr browser	
Network access: Remotely accessible registry paths	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion	
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog System\CurrentControlSet\Services\Replicator System\CurrentControlSet\Control\ContentIndex\Catalogs System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows	
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled	
Network access: Shares that can be accessed anonymously	COMCFG DFS\$ CHEYALERT\$	

Security Option	Security Option Settings	Overridden By GPO
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves	
Network security: LAN Manager authentication level	Send NTLM response only	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Network security: LDAP client signing requirements	Negotiate signing	
Recovery console: Allow automatic administrative logon	Disabled	
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled	
Rename administrator account	Donald	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Rename guest account	Gerald	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Shutdown: Clear virtual memory pagefile	Disabled	
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled	
System objects: Default owner for objects created by members of the Administrators group	Administrators group	
System objects: Require case insensitivity for non-Windows subsystems	Enabled	
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled	
System settings: Optional subsystems	Posix	

Table 2. BSP/CHEYENNE

Security Option	Security Option Settings	Overriden By GPO
Accounts: Limit local account use of blank passwords to console logon only	Enabled	
Audit: Audit the access of global system objects	Disabled	
Audit: Audit the use of Backup and Restore privilege	Disabled	
Audit: Shut down system immediately if unable to log security audits	Disabled	
Devices: Allow undock without having to log on	Enabled	
Devices: Allowed to format and eject removable media	Administrators	
Devices: Prevent users from installing printer drivers	Enabled	
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled	
Devices: Restrict floppy access to locally logged-on user only	Disabled	
Devices: Unsigned driver installation behavior	Warn but allow installation	
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	
Domain member: Digitally encrypt secure channel data (when possible)	Enabled	
Domain member: Digitally sign secure channel data (when possible)	Enabled	
Domain member: Disable machine account password changes	Disabled	
Domain member: Maximum machine account password age	30 days	

Security Option	Security Option Settings	Overridden By GPO
Domain member: Require strong (Windows 2000 or later) session key	Disabled	
Interactive logon: Display user information when the session is locked	Do not display user information	
Interactive logon: Do not display last user name	Disabled	
Interactive logon: Do not require CTRL+ALT+DEL	Disabled	
Interactive logon: Message text for users attempting to log on		
Interactive logon: Message title for users attempting to log on		
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10 logons	
Interactive logon: Prompt user to change password before expiration	14 days	
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled	
Interactive logon: Require smart card	Disabled	
Interactive logon: Smart card removal behavior	No Action	
Microsoft network client: Digitally sign communications (always)	Disabled	
Microsoft network client: Digitally sign communications (if server agrees)	Enabled	
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled	
Microsoft network server: Amount of idle time required before suspending session	15 minutes	

Security Option	Security Option Settings	Overridden By GPO
Microsoft network server: Digitally sign communications (always)	Disabled	
Microsoft network server: Digitally sign communications (if client agrees)	Disabled	
Microsoft network server: Disconnect clients when logon hours expire	Enabled	
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled	
Network access: Do not allow storage of credentials or .NET Passports for network authentication	Disabled	
Network access: Let Everyone permissions apply to anonymous users	Disabled	
Network access: Named Pipes that can be accessed anonymously	COMNAP COMNODE SQL\QUERY SPOOLSS NETLOGON LSARPC SAMR BROWSER	
Network access: Remotely accessible registry paths	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion	
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration System\CurrentControlSet\Services\Wins	

Security Option	Security Option Settings	Overridden By GPO
	Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog SYSTEM\CurrentControlSet\Services\CertSvc	
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled	
Network access: Shares that can be accessed anonymously	COMCFG DFS\$	
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves	
Network security: Do not store LAN Manager hash value on next password change	Disabled	
Network security: LAN Manager authentication level	Send NTLM response only	
Network security: LDAP client signing requirements	Negotiate signing	
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	0	
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	0	
Recovery console: Allow automatic administrative logon	Disabled	
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled	
Shutdown: Allow system to be shut down without having to log on	Disabled	
Shutdown: Clear virtual memory pagefile	Disabled	

Security Option	Security Option Settings	Overriden By GPO
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled	
System objects: Default owner for objects created by members of the Administrators group	Administrators group	
System objects: Require case insensitivity for non-Windows subsystems	Enabled	
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled	
System settings: Optional subsystems	Posix	
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Disabled	

Table 3. BSP/PITA1

Security Option	Security Option Settings	Overriden By GPO
Accounts: Limit local account use of blank passwords to console logon only	Enabled	
Audit: Audit the access of global system objects	Disabled	
Audit: Audit the use of Backup and Restore privilege	Disabled	
Audit: Shut down system immediately if unable to log security audits	Disabled	
Devices: Allow undock without having to log on	Enabled	
Devices: Allowed to format and eject removable media	Administrators	
Devices: Prevent users from installing printer drivers	Enabled	

Security Option	Security Option Settings	Overridden By GPO
Devices: Restrict CD-ROM access to locally logged-on user only	Disabled	
Devices: Restrict floppy access to locally logged-on user only	Disabled	
Devices: Unsigned driver installation behavior	Warn but allow installation	
Domain controller: LDAP server signing requirements	None	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Domain member: Digitally encrypt secure channel data (when possible)	Enabled	
Domain member: Digitally sign secure channel data (when possible)	Enabled	
Domain member: Disable machine account password changes	Disabled	
Domain member: Maximum machine account password age	30 days	
Domain member: Require strong (Windows 2000 or later) session key	Disabled	
Interactive logon: Do not display last user name	Disabled	
Interactive logon: Do not require CTRL+ALT+DEL	Disabled	
Interactive logon: Message text for users attempting to log on		
Interactive logon: Message title for users attempting to log on		

Security Option	Security Option Settings	Overridden By GPO
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10 logons	
Interactive logon: Prompt user to change password before expiration	14 days	
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled	
Interactive logon: Require smart card	Disabled	
Interactive logon: Smart card removal behavior	No Action	
Microsoft network client: Digitally sign communications (always)	Disabled	
Microsoft network client: Digitally sign communications (if server agrees)	Enabled	
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled	
Microsoft network server: Amount of idle time required before suspending session	15 minutes	
Microsoft network server: Digitally sign communications (always)	Enabled	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Microsoft network server: Digitally sign communications (if client agrees)	Enabled	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Microsoft network server: Disconnect clients when logon hours expire	Enabled	
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	

Security Option	Security Option Settings	Overridden By GPO
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled	
Network access: Do not allow storage of credentials or .NET Passports for network authentication	Disabled	
Network access: Let Everyone permissions apply to anonymous users	Disabled	
Network access: Named Pipes that can be accessed anonymously	COMNAP COMNODE SQL\QUERY SPOOLSS netlogon lsarpc samr browser	
Network access: Remotely accessible registry paths	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion	
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog	
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled	
Network access: Shares that can be accessed anonymously	COMCFG DFS\$	
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves	

Security Option	Security Option Settings	Overridden By GPO
Network security: Do not store LAN Manager hash value on next password change	Disabled	
Network security: LAN Manager authentication level	Send NTLM response only	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Network security: LDAP client signing requirements	Negotiate signing	
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	0	
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	0	
Recovery console: Allow automatic administrative logon	Disabled	
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled	
Shutdown: Allow system to be shut down without having to log on	Disabled	
Shutdown: Clear virtual memory pagefile	Disabled	
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled	
System objects: Default owner for objects created by members of the Administrators group	Administrators group	
System objects: Require case insensitivity for non-Windows subsystems	Enabled	

Security Option	Security Option Settings	Overriden By GPO
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled	
System settings: Optional subsystems	Posix	
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Disabled	