



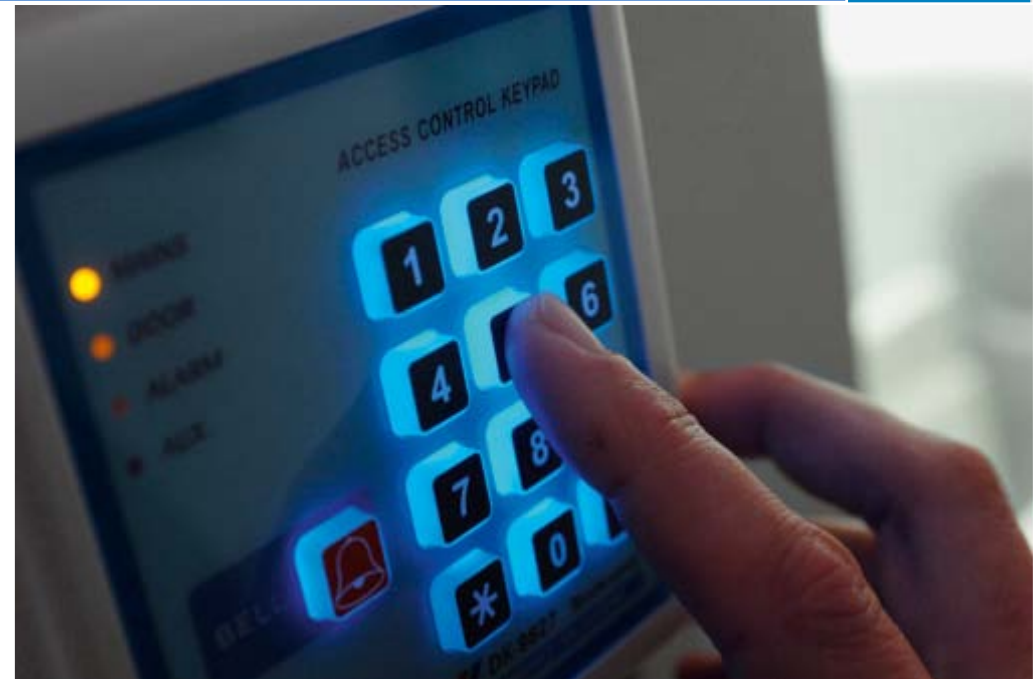
# Security Assessment

## Security Policy Assessment

Prepared for: Prospect Or Customer

Prepared by: Your Company Name

12/3/2014



CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Scan Date:12/1/2014

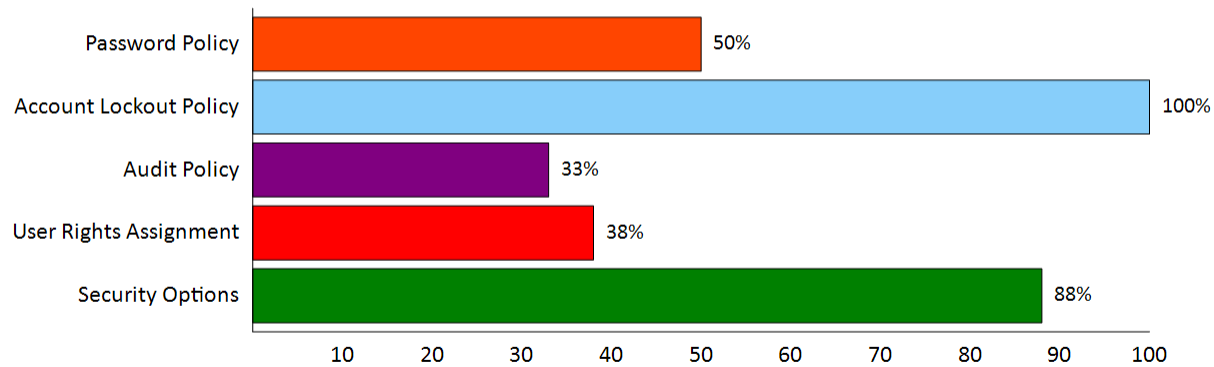


## Table of Contents

- 1 - Summary
- 2 - Domain Policies: CORP.SAMPLECOMPANY.COM
  - 2.1 - Default Domain Policy: CORP.SAMPLECOMPANY.COM
    - 2.1.1 - Account Policies/Password Policy
    - 2.1.2 - Account Policies/Account Lockout Policy
    - 2.1.3 - Account Policies/Kerberos Policy
    - 2.1.4 - Local Policies/Security Options
    - 2.1.5 - Public Key Policies/Encrypting File System
    - 2.1.6 - Public Key Policies/Trusted Root Certification Authorities
  - 2.2 - Default Domain Controllers Policy: CORP.SAMPLECOMPANY.COM
    - 2.2.1 - Local Policies/User Rights Assignment
    - 2.2.2 - Local Policies/Security Options
- 3 - Local Security Settings
  - 3.1 - Account Policies
    - 3.1.1 - Password Policy
    - 3.1.2 - Account Lockout Policy
  - 3.2 - Local Policies
    - 3.2.1 - Audit Policy
    - 3.2.2 - User Rights Assignment
    - 3.2.3 - Security Options

## 1 - Summary

### Policy Consistency



### Sampled Systems

IP Addresses	Computer Name	Operating System
10.0.1.3	DC01	Windows Server 2012 Standard
10.0.1.5, 10.0.7.74	UTIL01	Windows Server 2008 R2 Datacenter
10.0.7.20, 192.168.56.1	SE-Dresden	Windows 7 Professional
10.0.7.28	tandem	Windows 7 Enterprise
172.20.1.3, 10.0.1.3	DC01	Windows Server 2012 Standard

## 2 - Domain Policies: CORP.SAMPLECOMPANY.COM

## 2.1 - Default Domain Policy: CORP.SAMPLECOMPANY.COM

### 2.1.1 - Account Policies/Password Policy

Policy	Setting
Maximum password age	0 days
Minimum password age	30 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

### 2.1.2 - Account Policies/Account Lockout Policy

Policy	Setting
Account lockout threshold	Disabled

### 2.1.3 - 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

### 2.1.4 - Local Policies/Security Options



### Network Access

Policy	Setting
Network access: Allow anonymous SID/Name translation	Disabled

### Network Security

Policy	Setting
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Disabled

## 2.1.5 - Public Key Policies/Encrypting File System

### Certificates

Issued To	Issued By	Expiration Date	Intended Purposes
Administrator	Administrator	3/24/2012 1:32:00 PM	File Recovery

## 2.1.6 - 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 Certification Authorities
To perform certificate-based authentication of users and computers, CAs must meet the following criteria	Registered in Active Directory only

## 2.2 - Default Domain Controllers Policy: CORP.SAMPLECOMPANY.COM

### 2.2.1 - Local Policies/User Rights Assignment

Policy	Setting
Access this computer from the network	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, BUILTIN\Pre-Windows 2000 Compatible Access, BUILTIN\Administrators, NT AUTHORITY\Authenticated Users, Everyone
Add workstations to domain	NT AUTHORITY\Authenticated Users
Adjust memory quotas for a process	IIS APPPOOL\DefaultAppPool, BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, IIS APPPOOL\RDWebAccess
Allow log on locally	BUILTIN\Backup Operators, BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Account Operators, BUILTIN\Administrators
Back up files and directories	BUILTIN\Backup Operators, BUILTIN\Server Operators, BUILTIN\Administrators
Bypass traverse checking	BUILTIN\Pre-Windows 2000 Compatible Access, BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\Authenticated Users, Everyone
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, IIS APPPOOL\RDWebAccess
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
Manage auditing and security log	BUILTIN\Administrators, PRT\Exchange Servers
Modify firmware environment values	BUILTIN\Administrators
Profile single process	BUILTIN\Administrators
Profile system performance	NT SERVICE\WdiServiceHost, BUILTIN\Administrators

Policy	Setting
Remove computer from docking station	BUILTIN\Administrators
Replace a process level token	IIS APPPOOL\DefaultAppPool, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, IIS APPPOOL\RDWebAccess
Restore files and directories	BUILTIN\Backup Operators, BUILTIN\Server Operators, BUILTIN\Administrators
Shut down the system	BUILTIN\Backup Operators, BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Administrators
Take ownership of files or other objects	BUILTIN\Administrators

## 2.2.2 - Local Policies/Security Options

### *Domain Controller*

Policy	Setting
Domain controller: LDAP server signing requirements	None

### *Domain Member*

Policy	Setting
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled

### *Microsoft Network Server*

Policy	Setting
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled

### 3 - Local Security Settings

#### 3.1 - Account Policies

##### 3.1.1 - Password Policy

Policy	Setting	Computers
Enforce password history	24 passwords remembered	UTIL01, DC01
	0 passwords remembered	SE-DRESDEN, TANDEM
Maximum password age	42 days	UTIL01, TANDEM, DC01
	0	SE-DRESDEN
Minimum password age	1 days	UTIL01, TANDEM, DC01
	30 days	SE-DRESDEN
Minimum password length	7 characters	UTIL01, SE-DRESDEN, TANDEM, DC01
Password must meet complexity requirements	Enabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Store passwords using reversible encryption	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01

##### 3.1.2 - Account Lockout Policy

Policy	Setting	Computers
Account lockout duration	Not Applicable	UTIL01, SE-DRESDEN, TANDEM, DC01
Account lockout threshold	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Reset account lockout counter after	Not Applicable	UTIL01, SE-DRESDEN, TANDEM, DC01



## 3.2 - Local Policies

### 3.2.1 - Audit Policy

Policy	Setting	Computers
Audit account logon events	Success	UTIL01
	No auditing	SE-DRESDEN, TANDEM, DC01
Audit account management	Success	UTIL01
	No auditing	SE-DRESDEN, TANDEM, DC01
Audit directory service access	Success	UTIL01
	No auditing	SE-DRESDEN, TANDEM, DC01
Audit logon events	Success	UTIL01
	No auditing	SE-DRESDEN, TANDEM, DC01
Audit object access	No auditing	UTIL01, SE-DRESDEN, TANDEM, DC01
Audit policy change	Success	UTIL01
	No auditing	SE-DRESDEN, TANDEM, DC01
Audit privilege use	No auditing	UTIL01, SE-DRESDEN, TANDEM, DC01
Audit process tracking	No auditing	UTIL01, SE-DRESDEN, TANDEM, DC01
Audit system events	Success	UTIL01
	No auditing	SE-DRESDEN, TANDEM, DC01

### 3.2.2 - User Rights Assignment

Policy	Setting	Computers
Access this computer from the network	Everyone,Authenticated Users,Administrators,Pre-Windows 2000 Compatible Access,ENTERPRISE DOMAIN CONTROLLERS	UTIL01, DC01
	Everyone,Administrators	SE-DRESDEN, TANDEM
Add workstations to domain	Authenticated Users	UTIL01, DC01
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SERVICE,Administrators,DefaultAppPool,RDWebAccess	UTIL01
	LOCAL SERVICE,NETWORK SERVICE,Administrators	SE-DRESDEN
	LOCAL SERVICE,NETWORK	TANDEM



Policy	Setting	Computers
	SERVICE,SQLServer2005MSSQLUser\$tandem\$SQLEXPRESS,Administrators	
	LOCAL SERVICE,NETWORK SERVICE,Administrators,*S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415,*S-1-5-82-604604840-3341247844-1790606609-4006251754-2470522317	DC01
Allow log on locally	Administrators,Account Operators,Server Operators,Print Operators,Backup Operators	UTIL01, DC01
	Everyone,PRT\Domain Admins,Administrators	SE-DRESDEN, TANDEM
Allow log on through Remote Desktop Services	Administrators	UTIL01, DC01
	Administrators,Remote Desktop Users	SE-DRESDEN, TANDEM
Back up files and directories	Administrators,Server Operators,Backup Operators	UTIL01, DC01
	Administrators,Backup Operators	SE-DRESDEN, TANDEM
Bypass traverse checking	Everyone,Authenticated Users,LOCAL SERVICE,NETWORK SERVICE,Administrators,Pre-Windows 2000 Compatible Access	UTIL01, DC01
	Everyone,LOCAL SERVICE,NETWORK SERVICE,Administrators,Users,Backup Operators	SE-DRESDEN
	Everyone,LOCAL SERVICE,NETWORK SERVICE,SQLServer2005MSSQLUser\$tandem\$SQLEXPRESS,Administrators,Users,Backup Operators	TANDEM
Change the system time	LOCAL SERVICE,Administrators,Server Operators	UTIL01, DC01
	LOCAL SERVICE,Administrators	SE-DRESDEN, TANDEM
Change the time zone	LOCAL SERVICE,Administrators,Server Operators	UTIL01, DC01
	LOCAL SERVICE,Administrators,Users	SE-DRESDEN, TANDEM
Create a pagefile	Administrators	UTIL01, SE-DRESDEN, TANDEM, DC01
Create global objects	LOCAL SERVICE,NETWORK SERVICE,Administrators,SERVICE	UTIL01, SE-DRESDEN, TANDEM, DC01
Create symbolic links	Administrators	UTIL01, SE-DRESDEN, TANDEM, DC01
Debug programs	Administrators	UTIL01, SE-DRESDEN, TANDEM, DC01
Deny access to this computer from the network	Marketing_388945a0	UTIL01
	Guest	SE-DRESDEN, TANDEM
Deny log on locally	Marketing_388945a0,ASPNET	UTIL01
	Guest	SE-DRESDEN, TANDEM
Enable computer and user accounts to be trusted for delegation	Administrators	UTIL01, DC01
Force shutdown from a remote system	Administrators,Server Operators	UTIL01, DC01
	Administrators	SE-DRESDEN, TANDEM



Policy	Setting	Computers
Generate security audits	LOCAL SERVICE,NETWORK SERVICE,DefaultAppPool,RDWebAccess	UTIL01
	LOCAL SERVICE,NETWORK SERVICE	SE-DRESDEN, TANDEM
	LOCAL SERVICE,NETWORK SERVICE,*S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415,*S-1-5-82-604604840-3341247844-1790606609-4006251754-2470522317	DC01
Impersonate a client after authentication	LOCAL SERVICE,NETWORK SERVICE,Administrators,IIS_IUSRS,SERVICE	UTIL01
	LOCAL SERVICE,NETWORK SERVICE,Administrators,SERVICE	SE-DRESDEN, TANDEM, DC01
Increase a process working set	Users	UTIL01, SE-DRESDEN, TANDEM
	Users,Window Manager\Window Manager Group	DC01
Increase scheduling priority	Administrators	UTIL01, SE-DRESDEN, TANDEM, DC01
Load and unload device drivers	Administrators,Print Operators	UTIL01, DC01
	Administrators	SE-DRESDEN, TANDEM
Log on as a batch job	Administrators,Backup Operators,Performance Log Users	UTIL01, SE-DRESDEN
	SQLServer2005MSSQLUser\$standem\$SQLEXPRESS,Administrators,Backup Operators,internal Log Users	TANDEM
	Administrators,Backup Operators,internal Log Users	DC01
Log on as a service	NETWORK SERVICE,ASPNET,Administrator,DefaultAppPool,RDWebAccess	UTIL01
	NT SERVICE\ALL SERVICES	SE-DRESDEN, DC01
	SQLServer2005SQLBrowserUser\$standem,SQLServer2005MSSQLUser\$standem\$SQLEXPRESS,NT SERVICE\ALL SERVICES	TANDEM
Manage auditing and security log	Exchange Servers,Administrators	UTIL01, DC01
	Administrators	SE-DRESDEN, TANDEM
Modify firmware environment values	Administrators	UTIL01, SE-DRESDEN, TANDEM, DC01
Perform volume maintenance tasks	Administrators	UTIL01, SE-DRESDEN, TANDEM, DC01
Profile single process	Administrators	UTIL01, SE-DRESDEN, TANDEM, DC01
Profile system performance	Administrators,NT SERVICE\WdiServiceHost	UTIL01, SE-DRESDEN
Remove computer from docking station	Administrators	UTIL01, DC01
	Administrators,Users	SE-DRESDEN, TANDEM
Replace a process level token	LOCAL SERVICE,NETWORK SERVICE,DefaultAppPool,RDWebAccess	UTIL01
	LOCAL SERVICE,NETWORK SERVICE	SE-DRESDEN
	LOCAL SERVICE,NETWORK	TANDEM

Policy	Setting	Computers
	SERVICE,SQLServer2005MSSQLUser\$tandem\$SQLEXPRESS	
	LOCAL SERVICE,NETWORK SERVICE,*S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415,*S-1-5-82-604604840-3341247844-1790606609-4006251754-2470522317	DC01
Restore files and directories	Administrators,Server Operators,Backup Operators	UTIL01, DC01
	Administrators,Backup Operators	SE-DRESDEN, TANDEM
Shut down the system	Administrators,Server Operators,Print Operators,Backup Operators	UTIL01, DC01
	Administrators,Users,Backup Operators	SE-DRESDEN, TANDEM
Take ownership of files or other objects	Administrators	UTIL01, SE-DRESDEN, TANDEM, DC01
Lock pages in memory	PRT\JDresden	SE-DRESDEN
Profile system internal	Administrators,NT SERVICE\WdiServiceHost	TANDEM, DC01

### 3.2.3 - Security Options

Policy	Setting	Computers
Accounts: Administrator account status	Enabled	UTIL01, DC01
	Disabled	SE-DRESDEN, TANDEM
Accounts: Guest account status	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Accounts: Limit local account use of blank passwords to console logon only	Enabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Accounts: Rename administrator account	Administrator	UTIL01, SE-DRESDEN, TANDEM, DC01
Accounts: Rename guest account	Guest	UTIL01, SE-DRESDEN, TANDEM, DC01
Audit: Audit the access of global system objects	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Audit: Audit the use of Backup and Restore privilege	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01
Audit: Shut down system immediately if unable to log security audits	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
DCOM: Machine Access Restrictions in	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01



Policy	Setting	Computers
Security Descriptor Definition Language (SDDL) syntax		
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01
Devices: Allow undock without having to log on	Enabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Devices: Allowed to format and eject removable media	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01
Devices: Prevent users from installing printer drivers	Enabled	UTIL01, DC01
	Disabled	SE-DRESDEN, TANDEM
Devices: Restrict CD-ROM access to locally logged-on user only	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01
Devices: Restrict floppy access to locally logged-on user only	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01
Domain controller: Allow server operators to schedule tasks	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01
Domain controller: LDAP server signing requirements	None	UTIL01, DC01
	Not Defined	SE-DRESDEN, TANDEM
Domain controller: Refuse machine account password changes	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Domain member: Digitally encrypt secure channel data (when possible)	Enabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Domain member: Digitally sign secure channel data (when possible)	Enabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Domain member: Disable machine account password changes	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Domain member: Maximum machine account password age	30 days	UTIL01, SE-DRESDEN, TANDEM, DC01
Domain member: Require strong (Windows 2000 or later) session key	Enabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Interactive logon: Display user information when the session is locked	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01
Interactive logon: Do not display last user	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01



Policy	Setting	Computers
name		
Interactive logon: Do not require CTRL+ALT+DEL	Disabled	UTIL01, DC01
	Not Defined	SE-DRESDEN, TANDEM
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10 logons	UTIL01, SE-DRESDEN, TANDEM, DC01
Interactive logon: Prompt user to change password before expiration	5 days	UTIL01, SE-DRESDEN, TANDEM, DC01
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Interactive logon: Require smart card	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Interactive logon: Smart card removal behavior	No Action	UTIL01, SE-DRESDEN, TANDEM, DC01
Microsoft network client: Digitally sign communications (always)	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Microsoft network client: Digitally sign communications (if server agrees)	Enabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Microsoft network server: Amount of idle time required before suspending session	15 minutes	UTIL01, SE-DRESDEN, TANDEM, DC01
Microsoft network server: Digitally sign communications (always)	Enabled	UTIL01, DC01
	Disabled	SE-DRESDEN, TANDEM
Microsoft network server: Digitally sign communications (if client agrees)	Enabled	UTIL01, DC01
	Disabled	SE-DRESDEN, TANDEM
Microsoft network server: Disconnect clients when logon hours expire	Enabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Microsoft network server: Server SPN target name validation level	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01
Network access: Allow anonymous SID/Name translation	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Network access: Do not allow storage of	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01



Policy	Setting	Computers
passwords and credentials for network authentication		
Network access: Let Everyone permissions apply to anonymous users	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Network access: Named Pipes that can be accessed anonymously	,netlogon,samr,lsarpc	UTIL01, DC01
Network access: Remotely accessible registry paths	System\CurrentControlSet\Control\ProductOptions,System\CurrentControlSet\Control\Server Applications,Software\Microsoft\Windows NT\CurrentVersion	UTIL01, SE-DRESDEN, TANDEM, DC01
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	UTIL01, SE-DRESDEN, TANDEM, DC01
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Network access: Shares that can be accessed anonymously	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves	UTIL01, SE-DRESDEN, TANDEM, DC01
Network security: Allow Local System to use computer identity for NTLM	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01
Network security: Allow LocalSystem NULL session fallback	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01
Network Security: Allow PKU2U authentication requests to this computer to use online identities	Not Defined	UTIL01, SE-DRESDEN, TANDEM
Network security: Configure encryption types	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01



Policy	Setting	Computers
allowed for Kerberos		
Network security: Do not store LAN Manager hash value on next password change	Enabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Network security: Force logoff when logon hours expire	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Network security: LAN Manager authentication level	Send NTLM response only	UTIL01
	Not Defined	SE-DRESDEN, TANDEM, DC01
Network security: LDAP client signing requirements	Negotiate signing	UTIL01, SE-DRESDEN, TANDEM, DC01
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require 128-bit encryption	UTIL01, SE-DRESDEN, TANDEM, DC01
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require 128-bit encryption	UTIL01, SE-DRESDEN, TANDEM, DC01
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01
Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01
Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01
Recovery console: Allow automatic administrative logon	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
Shutdown: Allow system to be shut down without having to log on	Disabled	UTIL01, DC01
	Enabled	SE-DRESDEN, TANDEM
Shutdown: Clear virtual memory pagefile	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01





Policy	Setting	Computers
System cryptography: Force strong key protection for user keys stored on the computer	Not Defined	UTIL01, SE-DRESDEN, TANDEM, DC01
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
System objects: Require case insensitivity for non-Windows subsystems	Enabled	UTIL01, SE-DRESDEN, TANDEM, DC01
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled	UTIL01, SE-DRESDEN, TANDEM, DC01
System settings: Optional subsystems	Posix	UTIL01, SE-DRESDEN, TANDEM, DC01
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
User Account Control: Admin Approval Mode for the Built-in Administrator account	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Elevate without prompting	UTIL01, SE-DRESDEN
	Prompt for consent for non-Windows binaries	TANDEM, DC01
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials	UTIL01, SE-DRESDEN, TANDEM, DC01
User Account Control: Detect application installations and prompt for elevation	Enabled	UTIL01, SE-DRESDEN, TANDEM, DC01
User Account Control: Only elevate executables that are signed and validated	Disabled	UTIL01, SE-DRESDEN, TANDEM, DC01
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled	UTIL01, SE-DRESDEN, TANDEM, DC01
User Account Control: Run all administrators in Admin Approval Mode	Disabled	UTIL01, SE-DRESDEN
	Enabled	TANDEM, DC01
User Account Control: Switch to the secure desktop when prompting for elevation	Disabled	UTIL01, SE-DRESDEN, TANDEM
	Enabled	DC01
User Account Control: Virtualize file and	Enabled	UTIL01, SE-DRESDEN, TANDEM, DC01



Policy	Setting	Computers
registry write failures to per-user locations		
Accounts: Block Microsoft accounts	Not Defined	DC01
Interactive logon: Machine account lockout threshold	Not Defined	DC01
Interactive logon: Machine inactivity limit	Not Defined	DC01
Microsoft network server: Attempt S4U2Self to obtain claim information	Not Defined	DC01