-- !! Students

Data collected on: 19/06/2013 07:44:03

hide all

General hide

Details hide

Domain	
Owner	
Created	19/01/2012 13:38:32
Modified	17/06/2013 14:05:08
User Revisions	115 (AD), 115 (sysvol)
Computer Revisions	3 (AD), 3 (sysvol)
Unique ID	{1AA58F5F-12C4-4BD2-B0DC-02098F2A55AE}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Students	No	Enabled	

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

Security Filtering hide

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

Name
NT AUTHORITY\Authenticated Users

Delegation hide

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
	Edit settings, delete, modify security	No
	Edit settings, delete, modify security	No
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Enabled) hide

Policies hide

Windows Settings hide

Security Settings hide

Public Key Policies/Trusted Root Certification Authorities hide

Properties hide

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

Software Restriction Policieshide

Enforcement

Policy	Setting
Apply software restriction policies to the following	All software files except libraries (such as DLLs)
Apply software restriction policies to the following users	All users
When applying software restriction policies	Ignore certificate rules

Designated File Types

File Extension	File Type
ADE	Microsoft Access Project Extension
ADP	Microsoft Access Project
BAS	BAS File
BAT	Windows Batch File
CHM	Compiled HTML Help file
CMD	Windows Command Script
COM	MS-DOS Application
CPL	Control panel item
CRT	Security Certificate
EXE	Application
HLP	Help file
HTA	HTML Application
INF	Setup Information
INS	INS File
ISP	ISP File
LNK	Shortcut
MDB	Microsoft Access Database

MDE	Microsoft Access MDE Database
MSC	Microsoft Common Console Document
MSI	Windows Installer Package
MSP	Windows Installer Patch
MST	MST File
OCX	ActiveX control
PCD	PCD File
PIF	Shortcut to MS-DOS Program
REG	Registration Entries
SCR	Screen saver
SHS	SHS File
URL	Internet Shortcut
VB	Visual Basic Source file
WSC	Windows Script Component

Trusted Publishers

Trusted publisher management	Allow all administrators and users to manage user's own Trusted Publishers
Certificate verification	None

Software Restriction Policies/Security Levelshide

Policy	Setting
Default Security Level	Unrestricted

Software Restriction Policies/Additional Ruleshide

Hash Ruleshide

(0.2.10.0)

Security Level	Disallowed
Description	TOR project - bypasses filtering
Date last modified	14/10/2010 11:04:51

(15.0.874.106)

Security Level	Disallowed
Description	

Date last modified	04/11/2011 12:39:25

(15.0.874.106)

Security Level	Disallowed
Description	
Date last modified	04/11/2011 12:39:25

(4.65.0.0)

Security Level	Disallowed
Description	ZIP for TOR project - bypasses filtering
Date last modified	14/10/2010 11:04:04

Start Tor Browser.exe; 31 KB; 02/10/2010 03:08:32

Security Level	Disallowed
Description	TOR project - bypasses filtering
Date last modified	14/10/2010 11:04:32

ultra.EXE (1.0.0.1); ultra; Ultrasurf; ultra Application;

Security Level	Disallowed
Description	proxy bypass
Date last modified	12/02/2007 11:41:28

Path Ruleshide

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%

Security Level	Unrestricted
Description	
Date last modified	20/12/2005 09:21:42

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%*.exe

Security Level	Unrestricted
Description	
Date last modified	20/12/2005 09:21:42

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%System32*.exe

Security Level	Unrestricted

Description	
Date last modified	20/12/2005 09:21:42

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%

Security Level	Unrestricted
Description	
Date last modified	20/12/2005 09:21:42

***.mdb**

Security Level	Unrestricted
Description	
Date last modified	24/10/2012 08:57:03

chrome.exe

Security Level	Disallowed
Description	
Date last modified	04/11/2011 12:38:55

Administrative Templateshide
Policy definitions (ADMX files) retrieved from the central store.
System/Group Policyhide

Policy	Setting	Comment
Configure user Group Policy loopback processing mode	Enabled	
Mode:	Merge	

Windows Components/Internet Explorer/Internet Control Panelhide

Policy	Setting	Comment
Disable the Connections page	Enabled	

Windows Components/Internet Explorer/Privacyhide

Policy	Setting	Comment
Establish InPrivate Filtering threshold	Enabled	
Threshold (3-30):	3	

User Configuration (Enabled)hide
Policieshide
Windows Settingshide
Scriptshide
Logonhide
For this GPO, Script order: Not configured

Name	Parameters

userfolder.bat
Logoffhide
For this GPO, Script order: Not configured

Name	Parameters

remove_desktop_ini.bat
Security Settingshide
Software Restriction Policieshide

Enforcement

Policy	Setting
Apply software restriction policies to the following	All software files except libraries (such as DLLs)
Apply software restriction policies to the following users	All users except local administrators
When applying software restriction policies	Ignore certificate rules

Designated File Types

File Extension	File Type
ADE	Microsoft Access Project Extension
ADP	Microsoft Access Project
BAS	BAS File
BAT	Windows Batch File
CHM	Compiled HTML Help file
CMD	Windows Command Script
COM	MS-DOS Application
CPL	Control panel item
CRT	Security Certificate
EXE	Application
HLP	Help file
HTA	HTML Application
INF	Setup Information
INS	INS File
ISP	ISP File
LNK	Shortcut

MDE	Microsoft Access MDE Database
MSC	Microsoft Common Console Document
MSI	Windows Installer Package
MSP	Windows Installer Patch
MST	MST File
OCX	ActiveX control
PCD	PCD File
PIF	Shortcut to MS-DOS Program
REG	Registration Entries
SCR	Screen saver
SHS	SHS File
URL	Internet Shortcut
VB	Visual Basic Source file
WSC	Windows Script Component

Trusted Publishers

Trusted publisher management	Allow all administrators and users to manage user's own Trusted Publishers
Certificate verification	None

Software Restriction Policies/Security Levelshide

Policy	Setting
Default Security Level	Unrestricted

Software Restriction Policies/Additional Ruleshide

Hash Ruleshide

(1.8.0.603)

Security Level	Disallowed
Description	
Date last modified	27/03/2009 12:10:19

(12.1.2.0)

Security Level	Disallowed
Description	

Date last modified	26/09/2011 14:17:09

(2.0.4.0)

Security Level	Disallowed
Description	
Date last modified	19/05/2009 15:31:50

(5.1.2600.5512)

Security Level	Disallowed
Description	cmd.exe
Date last modified	29/11/2011 11:40:16

(7.116.18.0)

Security Level	Disallowed
Description	
Date last modified	19/05/2009 15:32:21

Button Click.exe; 373 KB; 14/03/2007 13:01:20

Security Level	Disallowed
Description	
Date last modified	28/03/2007 15:28:30

Button Click.exe; 373 KB; 22/03/2007 14:16:47

Security Level	Disallowed
Description	
Date last modified	11/02/2008 14:10:26

Cmd.Exe (5.1.2600.2180); cmd; Windows Command Processor; Microsoft® Windows® Operating System; Microsoft Corporation

Security Level	Disallowed
Description	
Date last modified	04/11/2005 13:14:15

Cmd.Exe (5.2.3790.1830); cmd; Windows Command Processor; Microsoft® Windows® Operating System; Microsoft Corporation

Security Level	Disallowed
Description	Command Prompt
Date last modified	04/11/2005 11:23:17

Cmd.Exe (6.1.7601.17514); cmd; Windows Command Processor; Microsoft® Windows® Operating System; Microsoft Corporation

Security Level	Disallowed
Description	
Date last modified	17/09/2012 16:05:47

command.com; 50 KB; 25/03/2003 12:00:00

Security Level	Disallowed
Description	command prompt
Date last modified	04/11/2005 11:30:52

command.com; 50 KB; 31/03/2003 13:00:00

Security Level	Disallowed
Description	
Date last modified	07/10/2009 15:35:18

DIALER.EXE (5.2.3790.1830); DIALER.EXE; Microsoft Windows Phone Dialer; Microsoft® Windows® Operating System; Microsoft Corporation

Security Level	Disallowed
Description	remote dialers
Date last modified	04/11/2005 11:29:48

druglord2.exe; 781 KB; 20/04/2003 10:01:14

Security Level	Disallowed
Description	
Date last modified	04/02/2008 15:53:49

InstallMiniMowbli2.exe; 1100 KB; 11/01/2006 12:21:09

Security Level	Disallowed
Description	

Date last modified	29/11/2006 15:00:14

InstallMiniMowbli2.exe; 1100 KB; 11/01/2006 12:21:09

Security Level	Disallowed
Description	
Date last modified	29/11/2006 15:00:15

mstsc.exe (5.2.3790.1830); mstsc.exe; Remote Desktop Connection; Microsoft® Windows® Operating System; Microsoft Corporation

Security Level	Disallowed
Description	
Date last modified	04/11/2005 11:32:28

mstsc.exe (5.2.3790.3959); mstsc.exe; Remote Desktop Connection; Microsoft® Windows® Operating System; Microsoft Corporation

Security Level	Disallowed
Description	
Date last modified	13/06/2008 15:51:13

mstsc.exe (6.1.7601.17514); mstsc.exe; Remote Desktop Connection; Microsoft® Windows® Operating System; Microsoft Corporation

Security Level	Disallowed
Description	
Date last modified	17/09/2012 16:06:34

PINBALL.EXE (5.1.2600.2180); 3D Pinball; 3D Pinball; 3D Pinball; Cinematronics

Security Level	Disallowed
Description	Games
Date last modified	04/11/2005 11:25:28

SAFlashPlayer.exe (8.0.22.0); Macromedia Flash Player 8.0; Macromedia Flash Player 8.0 r22; Shockwave Flash; Macromedia, Inc.

Security Level	Disallowed
Description	
Date last modified	29/11/2006 14:49:55

SAFlashPlayer.exe (8.0.22.0); Macromedia Flash Player 8.0; Macromedia Flash Player 8.0 r22; Shockwave Flash; Macromedia, Inc.

Security Level	Disallowed
Description	
Date last modified	29/11/2006 14:45:51

setup.exe (8.2.160.0); setup.exe; Setup Launcher ; iPod for Windows 2005-06-26 ; Apple Computer, Inc.

Security Level	Disallowed
Description	IPOD
Date last modified	20/12/2005 09:25:23

telnetc.exe (5.2.3790.2442); telnet.exe; Microsoft Telnet Client; Microsoft® Windows® Operating System; Microsoft Corporation

Security Level	Disallowed
Description	
Date last modified	04/11/2005 11:33:34

Tutor Control Application; AB Tutor Control Application; AB Consulting; ABControl.EXE (6.2.0.0)

Security Level	Disallowed
Description	
Date last modified	14/09/2009 11:08:38

Path Ruleshide

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%

Security Level	Unrestricted
Description	
Date last modified	13/10/2005 13:08:38

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%*.exe

Security Level	Unrestricted
Description	
Date last modified	13/10/2005 13:08:38

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%System32*.exe

Security Level	Unrestricted
Description	

Date last modified	13/10/2005 13:08:38

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%

Security Level	Unrestricted
Description	
Date last modified	13/10/2005 13:08:38

%SystemRoot%\system32\freecell.exe

Security Level	Disallowed
Description	Games
Date last modified	04/11/2005 11:22:47

%SystemRoot%\system32\inkball.exe

Security Level	Disallowed
Description	Games
Date last modified	04/11/2005 11:14:44

%SystemRoot%\system32\mshearts.exe

Security Level	Disallowed
Description	Games
Date last modified	04/11/2005 11:15:03

%SystemRoot%\system32\sol.exe

Security Level	Disallowed
Description	Games
Date last modified	04/11/2005 11:22:42

%SystemRoot%\System32\spider.exe

Security Level	Disallowed
Description	Games
Date last modified	04/11/2005 11:21:40

%SystemRoot%\system32\winmine.exe

Security Level	Disallowed
Description	Games

Date last modified	04/11/2005 11:21:34

***.mdb**

Security Level	Unrestricted
Description	
Date last modified	12/03/2013 15:40:23

\\ashdata\%username%$

Security Level	Disallowed
Description	
Date last modified	20/09/2012 13:21:48

\\ASHDATA\%USERNAME%$\pcclient.exe

Security Level	Unrestricted
Description	
Date last modified	20/09/2012 13:22:40

abcontrol.exe

Security Level	Disallowed
Description	
Date last modified	14/09/2009 11:09:49

c:\documents and settings\%username%\local settings\application data

Security Level	Disallowed
Description	
Date last modified	20/09/2012 13:23:19

c:\documents and settings\%username%\local settings\application data\google

Security Level	Disallowed
Description	
Date last modified	20/09/2012 13:23:43

c:\documents and settings\%username%\local settings\application data\mozilla firefox

Security Level	Disallowed
Description	

Date last modified	26/09/2012 13:06:02

C:\Program Files\ABControl\ABControl.exe

Security Level	Disallowed
Description	
Date last modified	14/09/2009 11:09:33

C:\Program Files\MSN Gaming Zone\Windows\bchkrzm.exe

Security Level	Disallowed
Description	
Date last modified	14/10/2005 14:05:04

C:\Program Files\MSN Gaming Zone\Windows\bckgzm.exe

Security Level	Disallowed
Description	
Date last modified	14/10/2005 14:04:40

C:\Program Files\MSN Gaming Zone\Windows\chkrzm.exe

Security Level	Disallowed
Description	
Date last modified	20/12/2005 09:27:08

C:\Program Files\MSN Gaming Zone\Windows\hrtzzm.exe

Security Level	Disallowed
Description	
Date last modified	14/10/2005 14:05:20

C:\Program Files\MSN Gaming Zone\Windows\Rvsezm.exe

Security Level	Disallowed
Description	
Date last modified	14/10/2005 14:10:43

C:\Program Files\MSN Gaming Zone\Windows\shvlzm.exe

Security Level	Disallowed
Description	

Date last modified	14/10/2005 14:11:03

C:\Program Files\SIMS

Security Level	Disallowed
Description	
Date last modified	19/05/2009 15:32:47

C:\program files\windows nt\pinball\pinball.exe

Security Level	Disallowed
Description	
Date last modified	14/10/2005 13:46:32

c:\windows\temp

Security Level	Disallowed
Description	
Date last modified	21/03/2013 08:47:57

chromesetup.exe

Security Level	Disallowed
Description	
Date last modified	21/03/2013 08:48:20

d:

Security Level	Disallowed
Description	
Date last modified	20/09/2012 13:24:30

e:

Security Level	Disallowed
Description	
Date last modified	20/09/2012 13:24:43

f:

Security Level	Disallowed
Description	

Date last modified	20/09/2012 13:24:53

firefox.exe

Security Level	Disallowed
Description	
Date last modified	26/09/2012 13:06:15

g:

Security Level	Disallowed
Description	
Date last modified	20/09/2012 13:25:48

i:

Security Level	Disallowed
Description	
Date last modified	20/09/2012 13:25:56

l:

Security Level	Disallowed
Description	
Date last modified	20/09/2012 13:26:33

m:

Security Level	Disallowed
Description	
Date last modified	20/09/2012 13:26:25

minecraft.exe

Security Level	Disallowed
Description	
Date last modified	26/09/2011 14:17:40

n:

Security Level	Disallowed
Description	

Date last modified	20/09/2012 13:26:45

Folder Redirectionhide
Documentshide
Setting: Basic (Redirect everyone's folder to the same location)hide
Path: %HOMESHARE%%HOMEPATH%
Optionshide

Grant user exclusive rights to Documents	Enabled
Move the contents of Documents to the new location	Disabled
Also apply redirection policy to Windows 2000, Windows 2000 server, Windows XP, and Windows Server 2003 operating systems	Enabled
Policy Removal Behavior	Leave contents

Musichide
Setting: Follow the Documents folder
Pictureshide
Setting: Follow the Documents folder
Videoshide
Setting: Follow the Documents folder
Internet Explorer Maintenancehide
Connection/Proxy Settingshide

Enable proxy settings

Protocol	Server	Port
HTTP	192.168.3.8	8080
Secure	192.168.3.8	8080
FTP	192.168.3.8	8080
Gopher	192.168.3.8	8080
Socks	192.168.3.8	8080

Exceptions:	Do not use proxy server for addresses beginning with	127.0.0.1, 192.168.3.8, *.curriculum.local, *.ncc.com, 192.168.3.11, frogserver, ash-pce,
	Do not use proxy server for local (intranet) addresses	Enabled

URLs/Important URLshide

Name	URL
Home page URL	http://student.curriculum.local
Search bar URL	Not configured
Online support page URL	Not configured

Security/Security Zones and Content Ratingshide
Security Zones and Privacyhide

These settings will not apply to users that log on to computers that have the Internet Explorer Enhanced Security Configuration (ESC) enabled. To create settings for users on computers that have ESC enabled, create a new GPO and edit that GPO on a computer where ESC is enabled.

Internet (Security Level: Custom)hide

.NET Framework-reliant components

Run components not signed with Authenticode	Enable
Run components signed with Authenticode	Enable

ActiveX controls and plug-ins

Download signed ActiveX controls	Prompt
Download unsigned ActiveX controls	Disable
Initialize and script ActiveX controls not marked as safe	Disable
Run ActiveX controls and plug-ins	Enable
Script ActiveX controls marked safe for scripting	Enable

Downloads

File download	Enable
Font download	Enable

Microsoft VM

Java permissions	High safety

Miscellaneous

Access data sources across domains	Disable
Allow META REFRESH	Enable
Display mixed content	Prompt
Don't prompt for client certificate selection when no certificates or only one certificate exists	Disable
Drag and drop or copy and paste files	Enable
Installation of desktop items	Prompt
Launching applications and unsafe files	Prompt
Launching programs and files in an IFRAME	Prompt
Navigate sub-frames across different domains	Enable
Software channel permissions	Medium safety
Submit nonencrypted form data	Enable

Userdata persistence	Enable

Scripting

Active scripting	Enable
Allow paste operations via script	Enable
Scripting of Java applets	Enable

User Authentication

Logon	Automatic logon only in Intranet zone

Local intranet (Security Level: Custom)hide

.NET Framework-reliant components

Run components not signed with Authenticode	Enable
Run components signed with Authenticode	Enable

ActiveX controls and plug-ins

Download signed ActiveX controls	Prompt
Download unsigned ActiveX controls	Disable
Initialize and script ActiveX controls not marked as safe	Disable
Run ActiveX controls and plug-ins	Enable
Script ActiveX controls marked safe for scripting	Enable

Downloads

File download	Enable
Font download	Enable

Microsoft VM

Java permissions	Medium safety

Miscellaneous

Access data sources across domains	Prompt
Allow META REFRESH	Enable
Display mixed content	Prompt
Don't prompt for client certificate selection when no certificates or only one certificate exists	Enable
Drag and drop or copy and paste files	Enable
Installation of desktop items	Prompt

Launching applications and unsafe files	Enable
Launching programs and files in an IFRAME	Prompt
Navigate sub-frames across different domains	Enable
Software channel permissions	Medium safety
Submit nonencrypted form data	Enable
Userdata persistence	Enable

Scripting

Active scripting	Enable
Allow paste operations via script	Enable
Scripting of Java applets	Enable

User Authentication

Logon	Automatic logon only in Intranet zone

Sites

Require server verification (https:) for all sites in this zone	Disabled
Include all local (intranet) sites not listed in other zones	Enabled
Include all sites that bypass the proxy server	Enabled
Include all network paths (UNCs)	Enabled

Sites in this zone
None

Trusted sites (Security Level: Custom)hide

.NET Framework-reliant components

Run components not signed with Authenticode	Enable
Run components signed with Authenticode	Enable

ActiveX controls and plug-ins

Download signed ActiveX controls	Enable
Download unsigned ActiveX controls	Prompt
Initialize and script ActiveX controls not marked as safe	Prompt
Run ActiveX controls and plug-ins	Enable
Script ActiveX controls marked safe for scripting	Enable

Downloads	
File download	Enable
Font download	Enable
Microsoft VM	
Java permissions	Low safety
Miscellaneous	
Access data sources across domains	Enable
Allow META REFRESH	Enable
Display mixed content	Prompt
Don't prompt for client certificate selection when no certificates or only one certificate exists	Enable
Drag and drop or copy and paste files	Enable
Installation of desktop items	Enable
Launching applications and unsafe files	Enable
Launching programs and files in an IFRAME	Enable
Navigate sub-frames across different domains	Enable
Software channel permissions	Low safety
Submit nonencrypted form data	Enable
Userdata persistence	Enable
Scripting	
Active scripting	Enable
Allow paste operations via script	Enable
Scripting of Java applets	Enable
User Authentication	
Logon	Automatic logon with current username and password
Sites	
Require server verification (https:) for all sites in this zone	Disabled

Sites in this zone
*.alfiesoft.com

https://*.irisconnect.com/
https://eu.irisconnect.com/

Restricted sites (Security Level: Custom)hide

.NET Framework-reliant components

Run components not signed with Authenticode	Disable
Run components signed with Authenticode	Disable

ActiveX controls and plug-ins

Download signed ActiveX controls	Disable
Download unsigned ActiveX controls	Disable
Initialize and script ActiveX controls not marked as safe	Disable
Run ActiveX controls and plug-ins	Disable
Script ActiveX controls marked safe for scripting	Disable

Downloads

File download	Disable
Font download	Prompt

Microsoft VM

Java permissions	Disable Java

Miscellaneous

Access data sources across domains	Disable
Allow META REFRESH	Disable
Display mixed content	Prompt
Don't prompt for client certificate selection when no certificates or only one certificate exists	Disable
Drag and drop or copy and paste files	Prompt
Installation of desktop items	Disable
Launching applications and unsafe files	Disable
Launching programs and files in an IFRAME	Disable
Navigate sub-frames across different domains	Disable
Software channel permissions	High safety

Submit nonencrypted form data	Prompt
Userdata persistence	Disable

Scripting

Active scripting	Disable
Allow paste operations via script	Disable
Scripting of Java applets	Disable

User Authentication

Logon	Prompt for user name and password

Sites

Sites in this zone
None

Privacyhide

Privacy Level	Medium

Web Sites

Always allow	goalonline.co.uk; goalplc.co.uk; goalsci.com
Always block	None

Administrative Templateshide

Policy definitions (ADMX files) retrieved from the central store.

Control Panelhide

Policy	Setting	Comment
Show only specified Control Panel items	Enabled	

List of allowed Control Panel items
access
desk
main
mmsys
microsoft.mouse
desk.cpl,Settings,@Settings
microsoft.display

Control Panel/Add or Remove Programshide

Policy	Setting	Comment

Remove Add or Remove Programs	Enabled

Control Panel/Printershide

Policy	Setting	Comment
Browse the network to find printers	Disabled	
Prevent deletion of printers	Enabled	

Control Panel/Regional and Language Optionshide

Policy	Setting	Comment
Restrict selection of Windows menus and dialogs language	Enabled	
Restrict users to the following language:	English	

Desktophide

Policy	Setting	Comment
Do not add shares of recently opened documents to Network Locations	Enabled	
Don't save settings at exit	Enabled	
Hide Network Locations icon on desktop	Enabled	
Prohibit adjusting desktop toolbars	Enabled	
Prohibit User from manually redirecting Profile Folders	Enabled	
Remove Properties from the Documents icon context menu	Enabled	
Remove the Desktop Cleanup Wizard	Enabled	

Desktop/Desktophide

Policy	Setting	Comment
Desktop Wallpaper	Enabled	
Wallpaper Name:	\\ashdc1\software$\background.JPG	
Example: Using a local path: C:\windows\web\wallpaper\home.jpg		
Example: Using a UNC path: \\Server\Share\Corp.jpg		
Wallpaper Style:	Center	

Policy	Setting	Comment
Enable Active Desktop	Enabled	
Allows HTML and JPEG Wallpaper		

Policy	Setting	Comment
Prohibit adding items	Enabled	

Prohibit changes	Enabled
Prohibit closing items	Enabled
Prohibit deleting items	Enabled
Prohibit editing items	Enabled

Network/Offline Fileshide

Policy	Setting	Comment
Prevent use of Offline Files folder	Enabled	
Prohibit user configuration of Offline Files	Enabled	

Prevents users from changing any cache configuration settings.

Start Menu and Taskbarhide

Policy	Setting	Comment
Change Start Menu power button	Enabled	

Choose one of the following actions: Restart

Policy	Setting	Comment
Clear history of recently opened documents on exit	Enabled	
Clear the recent programs list for new users	Enabled	
Do not display any custom toolbars in the taskbar	Enabled	
Do not keep history of recently opened documents	Enabled	
Lock all taskbar settings	Enabled	
Lock the Taskbar	Enabled	
Prevent changes to Taskbar and Start Menu Settings	Enabled	
Prevent users from adding or removing toolbars	Enabled	
Remove Clock from the system notification area	Disabled	
Remove Default Programs link from the Start menu.	Enabled	
Remove Downloads link from Start Menu	Enabled	
Remove Favorites menu from Start	Enabled	

Menu	
Remove frequent programs list from the Start Menu	Enabled
Remove Games link from Start Menu	Enabled
Remove Homegroup link from Start Menu	Enabled
Remove links and access to Windows Update	Enabled
Remove Logoff on the Start Menu	Enabled
Remove Music icon from Start Menu	Enabled
Remove Network Connections from Start Menu	Enabled
Remove Network icon from Start Menu	Enabled
Remove Pictures icon from Start Menu	Enabled
Remove programs on Settings menu	Enabled
Remove Recent Items menu from Start Menu	Enabled
Remove Run menu from Start Menu	Enabled
Remove the Action Center icon	Enabled
Remove user folder link from Start Menu	Enabled
Remove user's folders from the Start Menu	Disabled

System/Ctrl+Alt+Del Optionshide

Policy	Setting	Comment
Remove Logoff	Enabled	

System/Folder Redirectionhide

Policy	Setting	Comment
Do not automatically make all redirected folders available offline	Enabled	

System/Internet Communication Management/Internet Communication settingshide

Policy	Setting	Comment
Turn off the Windows Messenger Customer Experience Improvement Program	Enabled	

System/Power Managementhide

Policy	Setting	Comment

Prompt for password on resume from hibernate/suspend	Enabled

Windows Components/File Explorer hide

Policy	Setting	Comment
Do not allow Folder Options to be opened from the Options button on the View tab of the ribbon	Enabled	
Do not request alternate credentials	Enabled	
Hide these specified drives in My Computer	Enabled	
Pick one of the following combinations	Restrict D drive only	

Policy	Setting	Comment
Hides the Manage item on the File Explorer context menu	Enabled	
No Computers Near Me in Network Locations	Enabled	
No Entire Network in Network Locations	Enabled	
Prevent access to drives from My Computer	Enabled	
Pick one of the following combinations	Restrict D drive only	

Policy	Setting	Comment
Remove "Map Network Drive" and "Disconnect Network Drive"	Enabled	
Remove Shared Documents from My Computer	Enabled	
Turn off Windows+X hotkeys	Enabled	

Windows Components/Internet Explorer hide

Policy	Setting	Comment
Disable AutoComplete for forms	Enabled	
Turn off tabbed browsing	Enabled	
Turn off the auto-complete feature for web addresses	Enabled	

Windows Components/Internet Explorer/Internet Control Panel hide

Policy	Setting	Comment
Disable the Connections page	Enabled	

Windows Components/Microsoft Management Console hide

Policy	Setting	Comment
Restrict the user from entering author mode	Enabled	
Restrict users to the explicitly permitted list of snap-ins	Enabled	

Windows Components/Windows Installerhide

Policy	Setting	Comment
Prevent removable media source for any installation	Enabled	

Windows Components/Windows Media Playerhide

Policy	Setting	Comment
Prevent CD and DVD Media Information Retrieval	Enabled	
Prevent Music File Media Information Retrieval	Enabled	
Prevent Radio Station Preset Retrieval	Enabled	

Windows Components/Windows Media Player/Playbackhide

Policy	Setting	Comment
Prevent Codec Download	Enabled	

Windows Components/Windows Updatehide

Policy	Setting	Comment
Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box	Enabled	
Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box	Enabled	
Remove access to use all Windows Update features	Disabled	

Preferenceshide

Windows Settingshide

Registryhide

Collection: Registry Wizard Values/HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Explorer/BitBucket/KnownFolder/{FDD39AD0-238F-46AF-ADB4-6C85480369C7}hide

Commonhide

Options

Stop processing items on this extension if an error occurs on this item	No
Run in logged-on user's security context (user policy option)	No

Remove this item when it is no longer applied	No
Apply once and do not reapply	No

Registry item: {FDD39AD0-238F-46AF-ADB4-6C85480369C7}hide
Generalhide

Action	Update

Properties

Hive	HKEY_CURRENT_USER
Key path	Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\KnownFolder\{FDD39AD0-238F-46AF-ADB4-6C85480369C7}

Commonhide
Options

Stop processing items on this extension if an error occurs on this item	No
Run in logged-on user's security context (user policy option)	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

Registry item: NukeOnDeletehide
Generalhide

Action	Update

Properties

Hive	HKEY_CURRENT_USER
Key path	Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\KnownFolder\{FDD39AD0-238F-46AF-ADB4-6C85480369C7}
Value name	NukeOnDelete
Value type	REG_DWORD
Value data	0x1 (1)

Commonhide
Options

Stop processing items on this extension if an error occurs on this item	No
Run in logged-on user's security context (user policy option)	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

Registry item: MaxCapacityhide
Generalhide

Action	Update

Properties

Hive	HKEY_CURRENT_USER
Key path	Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\KnownFolder\{FDD39AD0-238F-46AF-ADB4-6C85480369C7}
Value name	MaxCapacity
Value type	REG_DWORD
Value data	0x1 (1)

Commonhide

Options

Stop processing items on this extension if an error occurs on this item	No
Run in logged-on user's security context (user policy option)	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No