XD2017 CC - Computer - Network Settings

Data collected on: 3/29/2020 12:16:55 AM

General

hide

Details

hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:52 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{029892E3-ED53-4185-913D-321E81C7E47A}
GPO Status	Enabled

Links

hide

Location	Enforced	Link Status	Path
Desktops	No	Enabled	bvt.local/Common Criteria TOE Computers/Desktops

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Windows Firewall with Advanced Security

hide

####### Global Settings

hide

Policy	Setting
Policy version	Not Configured
Disable stateful FTP	Not Configured
Disable stateful PPTP	Not Configured
IPsec exempt	Not Configured
IPsec through NAT	Not Configured
Preshared key encoding	Not Configured
SA idle time	Not Configured
Strong CRL check	Not Configured

####### Domain Profile Settings

hide

Policy	Setting
Firewall state	On
Inbound connections	Not Configured
Outbound connections	Not Configured
Apply local firewall rules	Not Configured
Apply local connection security rules	Not Configured
Display notifications	Not Configured

Allow unicast responses	Not Configured
Log dropped packets	Not Configured
Log successful connections	Not Configured
Log file path	Not Configured
Log file maximum size (KB)	Not Configured

Connection Security Settings hide

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local computer.

Network/Network Connections hide

Policy	Setting	Comment
Require domain users to elevate when setting a network's location	Enabled	

Network/Network Connections/Windows Firewall/Domain Profile hide

Policy	Setting	Comment
Windows Firewall: Protect all network connections	Enabled	

Network/Network Connections/Windows Firewall/Standard Profile hide

Policy	Setting	Comment
Windows Firewall: Protect all network connections	Enabled	

Network/Network Isolation hide

Policy	Setting	Comment
Proxy definitions are authoritative	Enabled	
Subnet definitions are authoritative	Enabled	

Network/WLAN Service/WLAN Settings hide

Policy	Setting	Comment
Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services	Disabled	

Windows Components/Connect hide

Policy	Setting	Comment
Don't allow this PC to be projected to	Enabled	

User Configuration (Enabled) hide

No settings defined.

XD2017 CC - User - Internet Explorer Restrictions

Data collected on: 3/29/2020 12:16:56 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:42 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{12A02C3A-CFA1-4F60-A9B3-C702FF311703}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Common Criteria Users	No	Enabled	bvt.local/Common Criteria Users

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

No settings defined.

User Configuration (Enabled) hide

Policies hide

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/Internet Explorer hide

Policy	Setting	Comment
Configure Media Explorer Bar	Enabled	
Disable the Media Explorer Bar and auto-play feature	Enabled	
Auto-Play Media files in the Media bar when enabled	Disabled	

Policy	Setting	Comment
Configure Outlook Express	Enabled	
Block attachments that could contain a virus	Enabled	

Policy	Setting	Comment
Disable changing accessibility settings	Enabled	
Disable changing Advanced page settings	Enabled	
Disable changing Automatic Configuration settings	Enabled	
Disable changing Calendar and Contact settings	Enabled	
Disable changing color settings	Enabled	
Disable changing connection settings	Enabled	
Disable changing default browser check	Enabled	
Disable changing font settings	Enabled	
Disable changing language settings	Enabled	
Disable changing link color settings	Enabled	
Disable changing Messaging settings	Enabled	
Disable changing Profile Assistant settings	Enabled	
Disable changing ratings settings	Enabled	
Disable changing Temporary Internet files settings	Enabled	
Disable external branding of Internet Explorer	Enabled	
Disable Import/Export Settings wizard	Enabled	
Disable Internet Connection wizard	Enabled	
Display error message on proxy script download failure	Disabled	
Do not allow users to enable or disable add-ons	Enabled	
Identity Manager: Prevent users from using Identities	Enabled	
Let users turn on and use Enterprise Mode from the Tools menu	Disabled	
Notify users if Internet Explorer is not the default web browser	Disabled	
Prevent access to Internet Explorer Help	Enabled	
Prevent changing pop-up filter level	Enabled	
Prevent changing the default search provider	Enabled	
Prevent configuration of how windows open	Enabled	
Select where to open links	Open in existing Internet Explorer window	

Policy	Setting	Comment
Prevent configuration of new tab creation	Enabled	

Select tab opening position	Background

Policy	Setting	Comment
Prevent Internet Explorer Search box from appearing	Enabled	
Prevent managing pop-up exception list	Enabled	
Prevent managing SmartScreen Filter	Enabled	

Select SmartScreen Filter mode	On

Policy	Setting	Comment
Prevent managing the phishing filter	Enabled	

Select phishing filter mode	Automatic

Policy	Setting	Comment
Search: Disable Find Files via F3 within the browser	Enabled	
Search: Disable Search Customization	Enabled	
Turn off ActiveX Opt-In prompt	Enabled	
Turn off add-on performance notifications	Enabled	
Turn off configuration of pop-up windows in tabbed browsing	Enabled	

Select tabbed browsing pop-up behavior	Let Internet Explorer decide

Policy	Setting	Comment
Turn off Managing SmartScreen Filter for Internet Explorer 8	Enabled	

Select SmartScreen Filter mode for Internet Explorer 8	On

Policy	Setting	Comment
Turn off pop-up management	Enabled	
Turn off Quick Tabs functionality	Enabled	
Turn off Reopen Last Browsing Session	Enabled	
Turn off suggestions for all user-installed providers	Enabled	
Turn off the auto-complete feature for web addresses	Enabled	
Turn off the quick pick menu	Enabled	
Turn on compatibility logging	Disabled	
Turn on Suggested Sites	Disabled	

Windows Components/Internet Explorer/Administrator Approved Controls hide

Policy	Setting	Comment
Audio/Video Player	Disabled	
Carpoint	Disabled	
DHTML Edit Control	Disabled	
Investor	Disabled	
Menu Controls	Disabled	
Microsoft Agent	Disabled	
Microsoft Chat	Disabled	
Microsoft Scriptlet Component	Disabled	
Microsoft Survey Control	Disabled	
MSNBC	Disabled	
NetShow File Transfer Control	Disabled	
Shockwave Flash	Disabled	

Windows Components/Internet Explorer/Application Compatibility/Clipboard access hide

Policy	Setting	Comment
Bypass prompting for Clipboard access for scripts running in any process	Disabled	
Bypass prompting for Clipboard access for scripts running in the Internet Explorer process	Disabled	

Windows Components/Internet Explorer/Browser menus hide

Policy	Setting	Comment
File menu: Disable Open menu option	Enabled	
File menu: Disable Save As Web Page Complete	Enabled	
File menu: Disable Save As... menu option	Enabled	

Help menu: Remove 'For Netscape Users' menu option	Enabled
Help menu: Remove 'Send Feedback' menu option	Enabled
Help menu: Remove 'Tip of the Day' menu option	Enabled
Help menu: Remove 'Tour' menu option	Enabled
Hide Favorites menu	Disabled
Tools menu: Disable Internet Options... menu option	Enabled
Turn off Print Menu	Enabled
Turn off Shortcut Menu	Enabled
Turn off the ability to launch report site problems using a menu option	Enabled
View menu: Disable Source menu option	Enabled

Windows Components/Internet Explorer/Delete Browsing History hide

Policy	Setting	Comment
Prevent access to Delete Browsing History	Enabled	

Windows Components/Internet Explorer/Internet Control Panel hide

Policy	Setting	Comment
Disable the Advanced page	Enabled	
Disable the Connections page	Enabled	
Disable the Content page	Enabled	
Disable the General page	Enabled	
Disable the Privacy page	Enabled	
Disable the Programs page	Enabled	
Disable the Security page	Enabled	

Windows Components/Internet Explorer/Internet Settings/Advanced settings/Browsing hide

Policy	Setting	Comment
Turn off configuring underline links	Enabled	
Underline links	Never	

Policy	Setting	Comment
Turn off details in messages about Internet connection problems	Enabled	
Turn on script debugging	Disabled	
Turn on the display of script errors	Disabled	

Windows Components/Internet Explorer/Internet Settings/Advanced settings/Internet Connection Wizard Settings hide

Policy	Setting	Comment
Start the Internet Connection Wizard automatically	Disabled	

Windows Components/Internet Explorer/Internet Settings/AutoComplete hide

Policy	Setting	Comment
Turn off inline AutoComplete in File Explorer	Enabled	
Turn off URL Suggestions	Enabled	
Turn off Windows Search AutoComplete	Enabled	
Turn on inline AutoComplete	Enabled	

Windows Components/Internet Explorer/Offline Pages hide

Policy	Setting	Comment
Disable adding channels	Enabled	
Disable adding schedules for offline pages	Enabled	
Disable all scheduled offline pages	Enabled	
Disable channel user interface completely	Enabled	
Disable downloading of site subscription content	Enabled	

Windows Components/Internet Explorer/Toolbars hide

Policy	Setting	Comment
Disable customizing browser toolbar buttons	Enabled	
Disable customizing browser toolbars	Enabled	
Hide the Command bar	Enabled	
Hide the status bar	Enabled	

Lock all toolbars	Enabled
Lock location of Stop and Refresh buttons	Enabled
Turn off Developer Tools	Enabled
Turn off toolbar upgrade tool	Enabled

IE11 Computer Security Compliance

Data collected on: 3/29/2020 12:16:56 AM

General

hide

Details

hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:02:02 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{16E75426-E3CB-4FB9-936B-C05CDF043475}
GPO Status	Enabled

Links

hide

Location	Enforced	Link Status	Path
Desktops	No	Enabled	bvt.local/Common Criteria TOE Computers/Desktops

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Administrative Templates

hide

Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/Internet Explorer

hide

Policy	Setting	Comment
Prevent "Fix settings" functionality	Disabled	
Prevent bypassing SmartScreen Filter warnings	Enabled	
Prevent bypassing SmartScreen Filter warnings about files that are not commonly downloaded from the Internet	Enabled	
Prevent changing proxy settings	Enabled	
Prevent per-user installation of ActiveX controls	Enabled	
Security Zones: Do not allow users to add/delete sites	Enabled	
Security Zones: Do not allow users to change policies	Enabled	
Security Zones: Use only machine settings	Enabled	
Specify use of ActiveX Installer Service for installation of ActiveX controls	Enabled	
Turn off ActiveX Opt-In prompt	Disabled	
Turn off browser geolocation	Enabled	
Turn off Crash Detection	Enabled	

Turn off the Security Settings Check feature	Disabled
Turn on ActiveX Filtering	Enabled

Windows Components/Internet Explorer/Delete Browsing History hide

Policy	Setting	Comment
Disable "Configuring History"	Enabled	
Days to keep pages in History	40	

Policy	Setting	Comment
Prevent access to Delete Browsing History	Enabled	

Windows Components/Internet Explorer/Internet Control Panel hide

Policy	Setting	Comment
Prevent ignoring certificate errors	Enabled	

Windows Components/Internet Explorer/Internet Control Panel/Advanced Page hide

Policy	Setting	Comment
Allow software to run or install even if the signature is invalid	Disabled	
Check for server certificate revocation	Enabled	
Check for signatures on downloaded programs	Enabled	
Do not allow ActiveX controls to run in Protected Mode when Enhanced Protected Mode is enabled	Enabled	
Turn on 64-bit tab processes when running in Enhanced Protected Mode on 64-bit versions of Windows	Enabled	
Turn on Enhanced Protected Mode	Enabled	

Windows Components/Internet Explorer/Internet Control Panel/Security Page hide

Policy	Setting	Comment
Intranet Sites: Include all network paths (UNCs)	Disabled	
Turn on certificate address mismatch warning	Enabled	

Windows Components/Internet Explorer/Internet Control Panel/Security Page/Internet Zone hide

Policy	Setting	Comment
Access data sources across domains	Enabled	
Access data sources across domains	Disable	

Policy	Setting	Comment
Allow cut, copy or paste operations from the clipboard via script	Enabled	
Allow paste operations via script	Disable	

Policy	Setting	Comment
Allow drag and drop or copy and paste files	Enabled	
Allow drag and drop or copy and paste files	Disable	

Policy	Setting	Comment
Allow font downloads	Enabled	
Allow font downloads	Disable	

Policy	Setting	Comment
Allow installation of desktop items	Enabled	
Allow installation of desktop items	Disable	

Policy	Setting	Comment
Allow loading of XAML files	Enabled	
XAML Files	Disable	

Policy	Setting	Comment
Allow only approved domains to use ActiveX controls without prompt	Enabled	
Only allow approved domains to use ActiveX controls without prompt	Enable	

Policy	Setting	Comment

Allow scripting of Internet Explorer WebBrowser controls	Enabled	
Internet Explorer web browser control	Disable	

Policy	Setting	Comment
Allow script-initiated windows without size or position constraints	Enabled	
Allow script-initiated windows without size or position constraints	Disable	

Policy	Setting	Comment
Allow scriptlets	Enabled	
Scriptlets	Disable	

Policy	Setting	Comment
Allow updates to status bar via script	Enabled	
Status bar updates via script	Disable	

Policy	Setting	Comment
Automatic prompting for file downloads	Enabled	
Automatic prompting for file downloads	Disable	

Policy	Setting	Comment
Don't run antimalware programs against ActiveX controls	Enabled	
Don't run antimalware programs against ActiveX controls	Disable	

Policy	Setting	Comment
Download signed ActiveX controls	Enabled	
Download signed ActiveX controls	Disable	

Policy	Setting	Comment
Download unsigned ActiveX controls	Enabled	
Download unsigned ActiveX controls	Disable	

Policy	Setting	Comment
Enable dragging of content from different domains across windows	Enabled	
Enable dragging of content from different domains across windows	Disable	

Policy	Setting	Comment
Enable dragging of content from different domains within a window	Enabled	
Enable dragging of content from different domains within a window	Disable	

Policy	Setting	Comment
Enable MIME Sniffing	Enabled	
Enable MIME Sniffing	Enable	

Policy	Setting	Comment
Include local path when user is uploading files to a server	Enabled	
Include local directory path when uploading files to a server	Disable	

Policy	Setting	Comment
Initialize and script ActiveX controls not marked as safe	Enabled	
Initialize and script ActiveX controls not marked as safe	Disable	

Policy	Setting	Comment
Java permissions	Enabled	
Java permissions	Disable Java	

Policy	Setting	Comment
Launching applications and files in an IFRAME	Enabled	
Launching applications and files in an IFRAME	Disable	

Policy	Setting	Comment

Logon options	Enabled	
Logon options	Prompt for user name and password	

Policy	Setting	Comment
Navigate windows and frames across different domains	Enabled	
Navigate windows and frames across different domains	Disable	

Policy	Setting	Comment
Run .NET Framework-reliant components not signed with Authenticode	Enabled	
Run .NET Framework-reliant components not signed with Authenticode	Disable	

Policy	Setting	Comment
Run .NET Framework-reliant components signed with Authenticode	Enabled	
Run .NET Framework-reliant components signed with Authenticode	Disable	

Policy	Setting	Comment
Show security warning for potentially unsafe files	Enabled	
Launching programs and unsafe files	Disable	

Policy	Setting	Comment
Turn on Cross-Site Scripting Filter	Enabled	
Turn on Cross-Site Scripting (XSS) Filter	Enable	

Policy	Setting	Comment
Turn on Protected Mode	Enabled	
Protected Mode	Enable	

Policy	Setting	Comment
Use Pop-up Blocker	Enabled	
Use Pop-up Blocker	Enable	

Policy	Setting	Comment
Userdata persistence	Enabled	
Userdata persistence	Disable	

Policy	Setting	Comment
Web sites in less privileged Web content zones can navigate into this zone	Enabled	
Web sites in less privileged Web content zones can navigate into this zone	Disable	

Windows Components/Internet Explorer/Internet Control Panel/Security Page/Intranet Zone hide

Policy	Setting	Comment
Don't run antimalware programs against ActiveX controls	Enabled	
Don't run antimalware programs against ActiveX controls	Disable	

Policy	Setting	Comment
Initialize and script ActiveX controls not marked as safe	Enabled	
Initialize and script ActiveX controls not marked as safe	Disable	

Policy	Setting	Comment
Java permissions	Enabled	
Java permissions	High safety	

Windows Components/Internet Explorer/Internet Control Panel/Security Page/Local Machine Zone hide

Policy	Setting	Comment
Don't run antimalware programs against ActiveX controls	Enabled	
Don't run antimalware programs against ActiveX controls	Disable	

Policy	Setting	Comment
Java permissions	Enabled	
Java permissions	Disable Java	

Policy	Setting	Comment
Turn on SmartScreen Filter scan	Enabled	
Use SmartScreen Filter	Enable	

Windows Components/Internet Explorer/Internet Control Panel/Security Page/Locked-Down Internet Zone hide

Policy	Setting	Comment
Allow only approved domains to use ActiveX controls without prompt	Enabled	
Only allow approved domains to use ActiveX controls without prompt	Enable	

Policy	Setting	Comment
Turn on SmartScreen Filter scan	Enabled	
Use SmartScreen Filter	Enable	

Windows Components/Internet Explorer/Internet Control Panel/Security Page/Locked-Down Intranet Zone hide

Policy	Setting	Comment
Java permissions	Enabled	
Java permissions	Disable Java	

Policy	Setting	Comment
Turn on SmartScreen Filter scan	Enabled	
Use SmartScreen Filter	Enable	

Windows Components/Internet Explorer/Internet Control Panel/Security Page/Locked-Down Local Machine Zone hide

Policy	Setting	Comment
Java permissions	Enabled	
Java permissions	Disable Java	

Policy	Setting	Comment
Turn on SmartScreen Filter scan	Enabled	
Use SmartScreen Filter	Enable	

Windows Components/Internet Explorer/Internet Control Panel/Security Page/Locked-Down Restricted Sites Zone hide

Policy	Setting	Comment
Allow only approved domains to use ActiveX controls without prompt	Enabled	
Only allow approved domains to use ActiveX controls without prompt	Enable	

Policy	Setting	Comment
Java permissions	Enabled	
Java permissions	Disable Java	

Policy	Setting	Comment
Turn on SmartScreen Filter scan	Enabled	
Use SmartScreen Filter	Enable	

Windows Components/Internet Explorer/Internet Control Panel/Security Page/Locked-Down Trusted Sites Zone hide

Policy	Setting	Comment
Java permissions	Enabled	
Java permissions	Disable Java	

Policy	Setting	Comment
Turn on SmartScreen Filter scan	Enabled	
Use SmartScreen Filter	Enable	

Windows Components/Internet Explorer/Internet Control Panel/Security Page/Restricted Sites Zone hide

Policy	Setting	Comment
Access data sources across domains	Enabled	
Access data sources across domains	Disable	

Policy	Setting	Comment
Allow active scripting	Enabled	
Allow active scripting	Disable	

Policy	Setting	Comment
Allow binary and script behaviors	Enabled	
Allow Binary and Script Behaviors	Disable	

Policy	Setting	Comment
Allow cut, copy or paste operations from the clipboard via script	Enabled	
Allow paste operations via script	Disable	

Policy	Setting	Comment
Allow drag and drop or copy and paste files	Enabled	
Allow drag and drop or copy and paste files	Disable	

Policy	Setting	Comment
Allow file downloads	Enabled	
Allow file downloads	Disable	

Policy	Setting	Comment
Allow font downloads	Enabled	
Allow font downloads	Disable	

Policy	Setting	Comment
Allow installation of desktop items	Enabled	
Allow installation of desktop items	Disable	

Policy	Setting	Comment
Allow loading of XAML files	Enabled	
XAML Files	Disable	

Policy	Setting	Comment
Allow META REFRESH	Enabled	
Allow META REFRESH	Disable	

Policy	Setting	Comment
Allow only approved domains to use ActiveX controls without prompt	Enabled	
Only allow approved domains to use ActiveX controls without prompt	Enable	

Policy	Setting	Comment
Allow scripting of Internet Explorer WebBrowser controls	Enabled	
Internet Explorer web browser control	Disable	

Policy	Setting	Comment
Allow script-initiated windows without size or position constraints	Enabled	
Allow script-initiated windows without size or position constraints	Disable	

Policy	Setting	Comment
Allow scriptlets	Enabled	
Scriptlets	Disable	

Policy	Setting	Comment
Allow updates to status bar via script	Enabled	
Status bar updates via script	Disable	

Policy	Setting	Comment
Automatic prompting for file downloads	Enabled	
Automatic prompting for file downloads	Disable	

Policy	Setting	Comment
Don't run antimalware programs against ActiveX controls	Enabled	
Don't run antimalware programs against ActiveX controls	Disable	

Policy	Setting	Comment
Download signed ActiveX controls	Enabled	
Download signed ActiveX controls	Disable	

Policy	Setting	Comment
Download unsigned ActiveX controls	Enabled	
Download unsigned ActiveX controls	Disable	

Policy	Setting	Comment
Enable dragging of content from different domains across windows	Enabled	
Enable dragging of content from different domains across windows	Disable	

Policy	Setting	Comment
Enable dragging of content from different domains within a window	Enabled	
Enable dragging of content from different domains within a window	Disable	

Policy	Setting	Comment
Enable MIME Sniffing	Enabled	
Enable MIME Sniffing	Enable	

Policy	Setting	Comment
Include local path when user is uploading files to a server	Enabled	
Include local directory path when uploading files to a server	Disable	

Policy	Setting	Comment
Initialize and script ActiveX controls not marked as safe	Enabled	
Initialize and script ActiveX controls not marked as safe	Disable	

Policy	Setting	Comment
Java permissions	Enabled	
Java permissions	Disable Java	

Policy	Setting	Comment
Launching applications and files in an IFRAME	Enabled	
Launching applications and files in an IFRAME	Disable	

Policy	Setting	Comment
Logon options	Enabled	
Logon options	Anonymous logon	

Policy	Setting	Comment
Navigate windows and frames across different domains	Enabled	
Navigate windows and frames across different domains	Disable	

Policy	Setting	Comment
Run .NET Framework-reliant components not signed with Authenticode	Enabled	
Run .NET Framework-reliant components not signed with Authenticode	Disable	

Policy	Setting	Comment
Run .NET Framework-reliant components signed with Authenticode	Enabled	
Run .NET Framework-reliant components signed with Authenticode	Disable	

Policy	Setting	Comment
Run ActiveX controls and plugins	Enabled	
Run ActiveX controls and plugins	Disable	

Policy	Setting	Comment
Script ActiveX controls marked safe for scripting	Enabled	
Script ActiveX controls marked safe for scripting	Disable	

Policy	Setting	Comment
Scripting of Java applets	Enabled	
Scripting of Java applets	Disable	

Policy	Setting	Comment
Show security warning for potentially unsafe files	Enabled	
Launching programs and unsafe files	Prompt	

Policy	Setting	Comment
Turn on Cross-Site Scripting Filter	Enabled	
Turn on Cross-Site Scripting (XSS) Filter	Enable	

Policy	Setting	Comment
Turn on Protected Mode	Enabled	
Protected Mode	Enable	

Policy	Setting	Comment
Turn on SmartScreen Filter scan	Enabled	
Use SmartScreen Filter	Enable	

Policy	Setting	Comment
Use Pop-up Blocker	Enabled	
Use Pop-up Blocker	Enable	

Policy	Setting	Comment
Userdata persistence	Enabled	
Userdata persistence	Disable	

Policy	Setting	Comment
Web sites in less privileged Web content zones can navigate into this zone	Enabled	
Web sites in less privileged Web content zones can navigate into this zone	Disable	

Windows Components/Internet Explorer/Internet Control Panel/Security Page/Trusted Sites Zone hide

Policy	Setting	Comment
Don't run antimalware programs against ActiveX controls	Enabled	
Don't run antimalware programs against ActiveX controls	Disable	

Policy	Setting	Comment
Initialize and script ActiveX controls not marked as safe	Enabled	
Initialize and script ActiveX controls not marked as safe	Disable	

Policy	Setting	Comment
Java permissions	Enabled	
Java permissions	High safety	

Windows Components/Internet Explorer/Internet Settings/Component Updates/Periodic check for updates to Internet Explorer and Internet Tools hide

Policy	Setting	Comment
Prevent specifying the update check interval (in days)	Enabled	
Update check interval (in days):	30	

Windows Components/Internet Explorer/Security Features/Consistent Mime Handling hide

Policy	Setting	Comment
Internet Explorer Processes	Enabled	

Windows Components/Internet Explorer/Security Features/Mime Sniffing Safety Feature hide

Policy	Setting	Comment
Internet Explorer Processes	Enabled	

Windows Components/Internet Explorer/Security Features/MK Protocol Security Restriction hide

Policy	Setting	Comment
Internet Explorer Processes	Enabled	

Windows Components/Internet Explorer/Security Features/Notification bar hide

Policy	Setting	Comment
Internet Explorer Processes	Enabled	

Windows Components/Internet Explorer/Security Features/Protection From Zone Elevation hide

Policy	Setting	Comment
Internet Explorer Processes	Enabled	

Windows Components/Internet Explorer/Security Features/Restrict ActiveX Install hide

Policy	Setting	Comment
Internet Explorer Processes	Enabled	

Windows Components/Internet Explorer/Security Features/Restrict File Download hide

Policy	Setting	Comment
Internet Explorer Processes	Enabled	

Windows Components/Internet Explorer/Security Features/Scripted Window Security Restrictions hide

Policy	Setting	Comment
Internet Explorer Processes	Enabled	

Windows Components/RSS Feeds hide

Policy	Setting	Comment
Prevent downloading of enclosures	Enabled	

User Configuration (Enabled) hide

No settings defined.

XD7 CC - Computer - Internet Explorer Customizations

Data collected on: 3/29/2020 12:16:56 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:40 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	2 (AD), 2 (SYSVOL)
Unique ID	{1EA503D9-E637-4BC4-AC03-80616A6FBE7E}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Desktops	No	Enabled	bvt.local/Common Criteria TOE Computers/Desktops

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Administrative Templates

hide

Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/Internet Explorer/Internet Control Panel/Security Page

hide

Policy	Setting	Comment
Site to Zone Assignment List	Enabled	

Enter the zone assignments here.	
https://WQINU-SF-1.bvt.local	1
https://VWFTY-SF-1.bvt.local	1

Windows Components/Internet Explorer/Security Features/Add-on Management

hide

Policy	Setting	Comment
Add-on List	Enabled	

Add-on List	
{238F6F83-B8B4-11CF-8771-00A024541EE3}	1

User Configuration (Enabled)

hide

No settings defined.

Default Domain Policy

Data collected on: 3/29/2020 12:16:56 AM

General

hide

Details

hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 8:49:06 AM
Modified	3/26/2020 9:20:44 PM
User Revisions	0 (AD), 0 (SYSVOL)
Computer Revisions	4 (AD), 4 (SYSVOL)
Unique ID	{31B2F340-016D-11D2-945F-00C04FB984F9}
GPO Status	Enabled

Links

hide

Location	Enforced	Link Status	Path
bvt	No	Enabled	bvt.local

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
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

Account Policies/Password Policy hide

Policy	Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy hide

Policy	Setting
Account lockout threshold	0 invalid logon attempts

Account Policies/Kerberos Policy hide

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/Security Options hide

Network Access hide

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

Network Security hide

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

Public Key Policies/Encrypting File System hide

Certificates hide

Issued To	Issued By	Expiration Date	Intended Purposes
Administrator	Administrator	3/2/2120 8:20:44 PM	File Recovery

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

User Configuration (Enabled) hide

No settings defined.

XD2017 CC - Computer - Server VDA Security Settings

Data collected on: 3/29/2020 12:16:56 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:48 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)

Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{38F2EEF5-96B8-4327-8559-4E65B03877EA}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Server VDA	No	Enabled	bvt.local/Common Criteria TOE Computers/Desktops/VDA/Server VDA

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Local Policies/User Rights Assignment hide

Policy	Setting
Allow log on through Terminal Services	BUILTIN\Remote Desktop Users
Shut down the system	BUILTIN\Administrators

User Configuration (Enabled) hide

No settings defined.

XD2017 CC - User - Installation Restrictions

Data collected on: 3/29/2020 12:16:56 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:44 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{4E2B02FC-B170-495C-BF6D-8EA0F4F37D82}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Common Criteria Users	No	Enabled	bvt.local/Common Criteria Users

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

No settings defined.

User Configuration (Enabled)

hide

Policies

hide

Administrative Templates

hide

Policy definitions (ADMX files) retrieved from the local computer.

System/Driver Installation

hide

Policy	Setting	Comment
Code signing for device drivers	Enabled	
When Windows detects a driver file without a digital signature:	Block	

Policy	Setting	Comment
Configure driver search locations	Enabled	
Do not search floppy disk drives	Enabled	
Do not search CD-ROM drives	Enabled	
Do not search Windows Update	Enabled	

System/Internet Communication Management/Internet Communication settings

hide

Policy	Setting	Comment
Turn off access to the Store	Enabled	
Turn off downloading of print drivers over HTTP	Enabled	
Turn off handwriting recognition error reporting	Enabled	
Turn off Help Experience Improvement Program	Enabled	
Turn off Help Ratings	Enabled	
Turn off Internet download for Web publishing and online ordering wizards	Enabled	
Turn off Internet File Association service	Enabled	
Turn off printing over HTTP	Enabled	
Turn off the "Order Prints" picture task	Enabled	
Turn off the "Publish to Web" task for files and folders	Enabled	
Turn off the Windows Messenger Customer Experience Improvement Program	Enabled	
Turn off Windows Online	Enabled	

Windows Components/Add features to Windows 10

hide

Policy	Setting	Comment
Prevent the wizard from running.	Enabled	

Windows Components/App runtime

hide

Policy	Setting	Comment
Block launching desktop apps associated with a file.	Enabled	
Block launching desktop apps associated with a URI scheme	Enabled	

Windows Components/Application Compatibility

hide

Policy	Setting	Comment
Turn off Program Compatibility Assistant	Enabled	

Windows Components/AutoPlay Policies

hide

Policy	Setting	Comment
Disallow Autoplay for non-volume devices	Enabled	
Prevent AutoPlay from remembering user choices.	Enabled	
Set the default behavior for AutoRun	Enabled	
Default AutoRun Behavior	Do not execute any autorun commands	

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

Windows Components/Desktop Gadgets hide

Policy	Setting	Comment
Restrict unpacking and installation of gadgets that are not digitally signed.	Enabled	
Turn off desktop gadgets	Enabled	
Turn Off user-installed desktop gadgets	Enabled	

Windows Components/Digital Locker hide

Policy	Setting	Comment
Do not allow Digital Locker to run	Enabled	

Windows Components/Windows Error Reporting hide

Policy	Setting	Comment
Disable Windows Error Reporting	Enabled	

Windows Components/Windows Installer hide

Policy	Setting	Comment
Always install with elevated privileges	Disabled	
Prevent removable media source for any installation	Enabled	
Specify the order in which Windows Installer searches for installation files	Enabled	
Search order n = network, m = media (CD), u = URL A few valid examples: nmu, n, nu, mn		

Windows Components/Windows Update hide

Policy	Setting	Comment
Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box	Enabled	
Remove access to use all Windows Update features	Enabled	
Configure notifications:	0 - Do not show any notifications	

XD2017 CC - Computer - Endpoint client drive redirection

Data collected on: 3/29/2020 12:16:56 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:54 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{4E39D3AA-959C-4F7B-80A9-61BABC934EEE}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Server VDA	No	Enabled	bvt.local/Common Criteria TOE Computers/Desktops/VDA/Server VDA

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Preferences hide

Windows Settings hide

Registry hide

UNCEnabled (Order: 1) hide

General hide

Action	Update

Properties

Hive	HKEY_LOCAL_MACHINE
Key path	SOFTWARE\Citrix\UncLinks
Value name	UNCEnabled
Value type	REG_DWORD
Value data	0x0 (0)

Common hide

Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

User Configuration (Enabled) hide

No settings defined.

XD2017 CC - Computer - Prevent RDS Disconnected Sessions

Data collected on: 3/29/2020 12:16:56 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:52 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{52C0A250-091D-471E-ADC7-BD4E7CD8B873}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Server VDA	No	Enabled	bvt.local/Common Criteria TOE Computers/Desktops/VDA/Server VDA

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Preferences hide

Windows Settings hide

Registry hide

MaxDisconnectionTime (Order: 1) hide

General hide

Action	Update

Properties

Hive	HKEY_LOCAL_MACHINE
Key path	SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
Value name	MaxDisconnectionTime
Value type	REG_DWORD
Value data	0x1 (1)

Common hide

Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

User Configuration (Enabled) hide

No settings defined.

XD7 CC - User - Internet Explorer Customizations

Data collected on: 3/29/2020 12:16:56 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:40 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	2 (AD), 2 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{5998F432-F74A-437C-893D-2A34E7DC79CC}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Common Criteria Users	No	Enabled	bvt.local/Common Criteria Users

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

No settings defined.

User Configuration (Enabled)

hide

Policies

hide

Administrative Templates

hide

Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/Internet Explorer

hide

Policy	Setting	Comment
Disable changing home page settings	Enabled	
Home Page	https://VWFTY-SF-1.bvt.local/Citrix/CCWeb/	

XD2017 CC - Computer - Control Panel Restrictions

Data collected on: 3/29/2020 12:16:57 AM

General

hide

Details

hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:56 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{5BC4DB7F-85B4-4C89-9707-E5D9F327DC69}
GPO Status	Enabled

Links

hide

Location	Enforced	Link Status	Path
Desktops	No	Enabled	bvt.local/Common Criteria TOE Computers/Desktops

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Administrative Templates

hide

Policy definitions (ADMX files) retrieved from the local computer.

Control Panel/Regional and Language Options/Handwriting personalization hide

Policy	Setting	Comment
Turn off automatic learning	Enabled	

User Configuration (Enabled) hide

No settings defined.

Default Domain Controllers Policy

Data collected on: 3/29/2020 12:16:57 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 8:49:06 AM
Modified	3/19/2020 10:39:38 AM
User Revisions	0 (AD), 0 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{6AC1786C-016F-11D2-945F-00C04fB984F9}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Domain Controllers	No	Enabled	bvt.local/Domain Controllers

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
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

Local Policies/User Rights Assignment hide

Policy	Setting
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	BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Allow log on locally	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, 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	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, 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	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
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 AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
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

Local Policies/Security Options hide

Domain Controller hide

Policy	Setting
Domain controller: LDAP server signing requirements	None

Domain Member hide

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

Microsoft Network Server hide

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

User Configuration (Enabled) hide

No settings defined.

XD2017 CC - User - App Launch Restrictions

Data collected on: 3/29/2020 12:16:57 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:44 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{79191F83-D6DA-4896-8260-FCFE7595FE5B}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Common Criteria Users	No	Enabled	bvt.local/Common Criteria Users

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

No settings defined.

User Configuration (Enabled) hide

Policies hide

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/Cloud Content hide

Policy	Setting	Comment
Do not suggest third-party content in Windows spotlight	Enabled	
Turn off all Windows spotlight features	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/NetMeeting hide

Policy	Setting	Comment
Disable Chat	Enabled	
Disable NetMeeting 2.x Whiteboard	Enabled	
Disable Whiteboard	Enabled	
Prevent adding Directory servers	Enabled	
Prevent receiving files	Enabled	
Prevent sending files	Enabled	
Prevent viewing Web directory	Enabled	

Windows Components/NetMeeting/Application Sharing hide

Policy	Setting	Comment
Disable application Sharing	Enabled	
Prevent Control	Enabled	
Prevent Desktop Sharing	Enabled	
Prevent Sharing	Enabled	
Prevent Sharing Command Prompts	Enabled	
Prevent Sharing Explorer windows	Enabled	

Windows Components/Sound Recorder hide

Policy	Setting	Comment
Do not allow Sound Recorder to run	Enabled	

Windows Components/Store hide

Policy	Setting	Comment
Turn off the offer to update to the latest version of Windows	Enabled	
Turn off the Store application	Enabled	

Windows Components/Task Scheduler hide

Policy	Setting	Comment
Hide Advanced Properties Checkbox in Add Scheduled Task Wizard	Enabled	
Hide Property Pages	Enabled	
Prevent Task Run or End	Enabled	
Prohibit Browse	Enabled	

Prohibit Drag-and-Drop	Enabled
Prohibit New Task Creation	Enabled
Prohibit Task Deletion	Enabled

Windows Components/Windows Calendar hide

Policy	Setting	Comment
Turn off Windows Calendar	Enabled	

Windows Components/Windows Mail hide

Policy	Setting	Comment
Turn off Windows Mail application	Enabled	

Windows Components/Windows Media Player hide

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/Networking hide

Policy	Setting	Comment
Hide Network Tab	Enabled	

Windows Components/Windows Media Player/Playback hide

Policy	Setting	Comment
Allow Screen Saver	Enabled	
Prevent Codec Download	Enabled	

Windows Components/Windows Media Player/User Interface hide

Policy	Setting	Comment
Do Not Show Anchor	Enabled	
Hide Privacy Tab	Enabled	
Hide Security Tab	Enabled	

Windows Components/Windows Messenger hide

Policy	Setting	Comment
Do not allow Windows Messenger to be run	Enabled	
Do not automatically start Windows Messenger initially	Enabled	

Windows Components/Windows Mobility Center hide

Policy	Setting	Comment
Turn off Windows Mobility Center	Enabled	

Extra Registry Settings hide

Display names for some settings cannot be found. You might be able to resolve this issue by updating the .ADM files used by Group Policy Management.

Setting	State
Software\Policies\Microsoft\System\HotStart\NoHotStart	1
Software\Policies\Microsoft\Windows\Backup\Client\DisableBackupLauncher	1
Software\Policies\Microsoft\Windows\Backup\Client\DisableBackupToDisk	1
Software\Policies\Microsoft\Windows\Backup\Client\DisableBackupToNetwork	1
Software\Policies\Microsoft\Windows\Backup\Client\DisableBackupToOptical	1
Software\Policies\Microsoft\Windows\Backup\Client\DisableBackupUI	1
Software\Policies\Microsoft\Windows\Backup\Client\DisableRestoreUI	1
Software\Policies\Microsoft\Windows\Backup\Client\DisableSystemBackupUI	1
Software\Policies\Microsoft\Windows\SideShow\Disabled	1
Software\Policies\Microsoft\WindowsMediaCenter\MediaCenter	1

XD2017 CC - Computer - SSL Ciphersuite Order

Data collected on: 3/29/2020 12:16:57 AM

General

Details hide

Domain	bvt.local

Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:46 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{8AC67B06-966B-435B-98F0-E089C0C85BD4}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Common Criteria TOE Computers	No	Enabled	bvt.local/Common Criteria TOE Computers

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Local Policies/Security Options hide

System Cryptography hide

Policy	Setting
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Enabled

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local computer.

Network/SSL Configuration Settings hide

Policy	Setting	Comment
SSL Cipher Suite Order	Enabled	
SSL Cipher Suites	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA	

Extra Registry Settings hide

Display names for some settings cannot be found. You might be able to resolve this issue by updating the .ADM files used by Group Policy Management.

Setting	State
SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL\SecureChannelProtocol	TLS12
SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL\SSLCertificateRevocationCheckPolicy	FullAccessCheckAndCrlRequired
SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL\SSLCiphers	

SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL\SSLClientAuthentication	
SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL\SSLClientCertificate	
SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL\SSLEnable	true
SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL\SSLFIPSEnable	true
SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL\SSLPolicyExtensionOID	
SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL\SSLProxyHost	
SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\SSL\SSLSecurityComplianceMode	FIPS

Preferences hide

Windows Settings hide

Registry hide

DisabledByDefault (Order: 1) hide

General hide

Action	Replace

Properties

Hive	HKEY_LOCAL_MACHINE
Key path	SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server
Value name	DisabledByDefault
Value type	REG_DWORD
Value data	0x1 (1)

Common hide

Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

DisabledByDefault (Order: 2) hide

General hide

Action	Replace

Properties

Hive	HKEY_LOCAL_MACHINE
Key path	SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client
Value name	DisabledByDefault
Value type	REG_DWORD
Value data	0x1 (1)

Common hide

Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

DisabledByDefault (Order: 3) hide

General hide

Action	Replace

Properties

Hive	HKEY_LOCAL_MACHINE
Key path	SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client
Value name	DisabledByDefault
Value type	REG_DWORD
Value data	0x0 (0)

Common

hide

Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

DisabledByDefault (Order: 4)

hide

General

hide

Action	Replace

Properties

Hive	HKEY_LOCAL_MACHINE
Key path	SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server
Value name	DisabledByDefault
Value type	REG_DWORD
Value data	0x0 (0)

Common

hide

Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

DisabledByDefault (Order: 5)

hide

General

hide

Action	Replace

Properties

Hive	HKEY_LOCAL_MACHINE
Key path	SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client
Value name	DisabledByDefault
Value type	REG_DWORD
Value data	0x0 (0)

Common

hide

Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

DisabledByDefault (Order: 6)

hide

General

hide

Action	Replace

Properties

Hive	HKEY_LOCAL_MACHINE
Key path	SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server
Value name	DisabledByDefault
Value type	REG_DWORD
Value data	0x0 (0)

Common

hide

Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

User Configuration (Enabled)

hide

No settings defined.

Win10-1607 User Security Compliance

Data collected on: 3/29/2020 12:16:57 AM

General

hide

Details

hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:58 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{9336FB6B-6B5E-41EA-869A-7BC5CAD96983}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Common Criteria Users	No	Enabled	bvt.local/Common Criteria Users

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

No settings defined.

User Configuration (Enabled) hide

Policies hide

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local computer.

Control Panel/Personalization hide

Policy	Setting	Comment
Enable screen saver	Enabled	
Password protect the screen saver	Enabled	

Start Menu and Taskbar/Notifications hide

Policy	Setting	Comment
Turn off toast notifications on the lock screen	Enabled	

XD2017 CC - Computer - Printing Restrictions

Data collected on: 3/29/2020 12:16:57 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:50 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{94BE4B93-642C-452C-B410-806ECA37F9FC}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path

Desktops	No	Enabled	bvt.local/Common Criteria TOE Computers/Desktops

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local computer.

Printers hide

Policy	Setting	Comment
Activate Internet printing	Disabled	
Add Printer wizard - Network scan page (Managed network)	Disabled	
Allow printers to be published	Disabled	
Disallow installation of printers using kernel-mode drivers	Enabled	
Extend Point and Print connection to search Windows Update	Disabled	
Printer browsing	Disabled	

User Configuration (Enabled) hide

No settings defined.

WS2016 Member Server Security Compliance

Data collected on: 3/29/2020 12:16:57 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:58 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{9776129C-231F-4D75-AAF5-01488DE153AB}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Servers	No	Enabled	bvt.local/Common Criteria TOE Computers/Servers

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Local Policies/User Rights Assignment hide

Policy	Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	NT AUTHORITY\Authenticated Users, BUILTIN\Administrators
Act as part of the operating system	
Allow log on locally	BUILTIN\Administrators
Back up files and directories	BUILTIN\Administrators
Create a pagefile	BUILTIN\Administrators
Create a token object	
Create global objects	BUILTIN\Administrators, NT AUTHORITY\SERVICE, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE
Create permanent shared objects	
Create symbolic links	BUILTIN\Administrators
Debug programs	BUILTIN\Administrators
Deny access to this computer from the network	BUILTIN\Guests, NT AUTHORITY\Local account and member of Administrators group
Deny log on locally	BUILTIN\Guests
Deny log on through Terminal Services	BUILTIN\Guests, NT AUTHORITY\Local account
Enable computer and user accounts to be trusted for delegation	
Force shutdown from a remote system	BUILTIN\Administrators
Generate security audits	NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE
Impersonate a client after authentication	BUILTIN\Administrators, NT AUTHORITY\SERVICE, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE
Increase scheduling priority	BUILTIN\Administrators
Load and unload device drivers	BUILTIN\Administrators
Lock pages in memory	
Manage auditing and security log	BUILTIN\Administrators
Modify firmware environment values	BUILTIN\Administrators
Perform volume maintenance tasks	BUILTIN\Administrators
Profile single process	BUILTIN\Administrators
Restore files and directories	BUILTIN\Administrators
Take ownership of files or other objects	BUILTIN\Administrators

Local Policies/Security Options hide

Accounts hide

Policy	Setting
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled

Interactive Logon hide

Policy	Setting
Interactive logon: Smart card removal behavior	Lock Workstation

Microsoft Network Client hide

Policy	Setting
Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled

Network Access hide

Policy	Setting
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled

Network Security hide

Policy	Setting
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Enabled
Network security: LAN Manager authentication level	Send NTLMv2 response only. Refuse LM & NTLM
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Enabled
Require NTLMv2 session security	Enabled
Require 128-bit encryption	Enabled
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Enabled
Require NTLMv2 session security	Enabled
Require 128-bit encryption	Enabled

System Objects hide

Policy	Setting
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled

User Account Control hide

Policy	Setting
User Account Control: Admin Approval Mode for the Built-in Administrator account	Enabled
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent on the secure desktop
User Account Control: Behavior of the elevation prompt for standard users	Automatically deny elevation requests
User Account Control: Detect application installations and prompt for elevation	Enabled
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled
User Account Control: Run all administrators in Admin Approval Mode	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled

Other hide

Policy	Setting
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled
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
Domain member: Require strong (Windows 2000 or later) session key	Enabled
Interactive logon: Machine inactivity limit	900 seconds
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled

Network security: Allow Local System to use computer identity for NTLM	Enabled
Network security: Allow LocalSystem NULL session fallback	Disabled

Windows Firewall with Advanced Security hide

Global Settings hide

Policy	Setting
Policy version	Not Configured
Disable stateful FTP	Not Configured
Disable stateful PPTP	Not Configured
IPsec exempt	Not Configured
IPsec through NAT	Not Configured
Preshared key encoding	Not Configured
SA idle time	Not Configured
Strong CRL check	Not Configured

Domain Profile Settings hide

Policy	Setting
Firewall state	On
Inbound connections	Block
Outbound connections	Allow
Apply local firewall rules	Not Configured
Apply local connection security rules	Not Configured
Display notifications	Not Configured
Allow unicast responses	Not Configured
Log dropped packets	Not Configured
Log successful connections	Not Configured
Log file path	Not Configured
Log file maximum size (KB)	Not Configured

Private Profile Settings hide

Policy	Setting
Firewall state	On
Inbound connections	Block
Outbound connections	Allow
Apply local firewall rules	Not Configured
Apply local connection security rules	Not Configured
Display notifications	Not Configured
Allow unicast responses	Not Configured
Log dropped packets	Not Configured
Log successful connections	Not Configured
Log file path	Not Configured
Log file maximum size (KB)	Not Configured

Public Profile Settings hide

Policy	Setting
Firewall state	On
Inbound connections	Block
Outbound connections	Allow
Apply local firewall rules	Not Configured
Apply local connection security rules	Not Configured
Display notifications	Not Configured
Allow unicast responses	Not Configured
Log dropped packets	Not Configured
Log successful connections	Not Configured
Log file path	Not Configured
Log file maximum size (KB)	Not Configured

Connection Security Settings hide

Advanced Audit Configuration hide

Account Logon hide

Policy	Setting
Audit Credential Validation	Success, Failure

Account Management hide

Policy	Setting
Audit Other Account Management Events	Success, Failure
Audit Security Group Management	Success, Failure
Audit User Account Management	Success, Failure

Detailed Tracking hide

Policy	Setting
Audit PNP Activity	Success
Audit Process Creation	Success

Logon/Logoff hide

Policy	Setting
Audit Account Lockout	Success, Failure
Audit Group Membership	Success
Audit Logoff	Success
Audit Logon	Success, Failure
Audit Special Logon	Success

Object Access hide

Policy	Setting
Audit Removable Storage	Success, Failure

Policy Change hide

Policy	Setting
Audit Audit Policy Change	Success, Failure
Audit Authentication Policy Change	Success
Audit Authorization Policy Change	Success

Privilege Use hide

Policy	Setting
Audit Sensitive Privilege Use	Success, Failure

System hide

Policy	Setting
Audit IPsec Driver	Success, Failure
Audit Other System Events	Success, Failure
Audit Security State Change	Success
Audit Security System Extension	Success, Failure
Audit System Integrity	Success, Failure

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local computer.

Control Panel/Personalization hide

Policy	Setting	Comment
Prevent enabling lock screen camera	Enabled	
Prevent enabling lock screen slide show	Enabled	

Network/Lanman Workstation hide

Policy	Setting	Comment
Enable insecure guest logons	Disabled	

Network/Network Connections/Windows Firewall/Domain Profile hide

Policy	Setting	Comment
Windows Firewall: Protect all network connections	Enabled	

Network/Network Provider hide

Policy	Setting	Comment

Hardened UNC Paths	Enabled

Specify hardened network paths. In the name field, type a fully-qualified UNC path for each network resource. To secure all access to a share with a particular name, regardless of the server name, specify a server name of '*' (asterisk). For example, "*\NETLOGON". To secure all access to all shares hosted on a server, the share name portion of the UNC path may be omitted. For example, "\\SERVER". In the value field, specify one or more of the following options, separated by commas: 'RequireMutualAuthentication=1': Mutual authentication between the client and server is required to ensure the client connects to the correct server. 'RequireIntegrity=1': Communication between the client and server must employ an integrity mechanism to prevent data tampering. 'RequirePrivacy=1': Communication between the client and the server must be encrypted to prevent third parties from observing sensitive data.

Hardened UNC Paths:	
*\NETLOGON	RequireMutualAuthentication=1, RequireIntegrity=1
*\SYSVOL	RequireMutualAuthentication=1, RequireIntegrity=1

You should require both Integrity and Mutual Authentication for any UNC paths that host executable programs, script files, or files that control security policies. Consider hosting files that do not require Integrity or Privacy on separate shares from those that absolutely need such security for optimal performance. For additional details on configuring Windows computers to require additional security when accessing specific UNC paths, visit http://support.microsoft.com/kb/3000483.

System/Device Guard hide

Policy	Setting	Comment
Turn On Virtualization Based Security	Enabled	

Select Platform Security Level:	Secure Boot and DMA Protection
Virtualization Based Protection of Code Integrity:	Enabled with UEFI lock
Credential Guard Configuration:	Enabled with UEFI lock

System/Early Launch Antimalware hide

Policy	Setting	Comment
Boot-Start Driver Initialization Policy	Enabled	

Choose the boot-start drivers that can be initialized:	Good, unknown and bad but critical

System/Group Policy hide

Policy	Setting	Comment
Configure registry policy processing	Enabled	

Do not apply during periodic background processing	Disabled
Process even if the Group Policy objects have not changed	Enabled

System/Logon hide

Policy	Setting	Comment
Do not display network selection UI	Enabled	
Enumerate local users on domain-joined computers	Disabled	

System/Mitigation Options hide

Policy	Setting	Comment
Untrusted Font Blocking	Enabled	

Mitigation Options	Block untrusted fonts and log events

System/Remote Procedure Call hide

Policy	Setting	Comment
Restrict Unauthenticated RPC clients	Enabled	

RPC Runtime Unauthenticated Client Restriction to Apply:	Authenticated

Windows Components/AutoPlay Policies hide

Policy	Setting	Comment
Disallow Autoplay for non-volume devices	Enabled	
Set the default behavior for AutoRun	Enabled	

Default AutoRun Behavior	Do not execute any autorun commands

Policy	Setting	Comment
Turn off Autoplay	Enabled	

Turn off Autoplay on:	All drives

Windows Components/Biometrics/Facial Features hide

Policy	Setting	Comment
Use enhanced anti-spoofing when available	Enabled	

Windows Components/Event Log Service/Application hide

Policy	Setting	Comment
Specify the maximum log file size (KB)	Enabled	
Maximum Log Size (KB)	32768	

Windows Components/Event Log Service/Security hide

Policy	Setting	Comment
Specify the maximum log file size (KB)	Enabled	
Maximum Log Size (KB)	196608	

Windows Components/Event Log Service/System hide

Policy	Setting	Comment
Specify the maximum log file size (KB)	Enabled	
Maximum Log Size (KB)	32768	

Windows Components/File Explorer hide

Policy	Setting	Comment
Configure Windows SmartScreen	Enabled	
Turn off Data Execution Prevention for Explorer	Disabled	
Turn off heap termination on corruption	Disabled	

Windows Components/Remote Desktop Services/Remote Desktop Connection Client hide

Policy	Setting	Comment
Do not allow passwords to be saved	Enabled	

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Device and Resource Redirection hide

Policy	Setting	Comment
Do not allow drive redirection	Enabled	

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Security hide

Policy	Setting	Comment
Always prompt for password upon connection	Enabled	
Require secure RPC communication	Enabled	
Set client connection encryption level	Enabled	
Encryption Level	High Level	
Choose the encryption level from the drop-down list.		

Windows Components/Search hide

Policy	Setting	Comment
Allow indexing of encrypted files	Disabled	

Windows Components/Windows Defender hide

Policy	Setting	Comment
Turn off Windows Defender	Disabled	

Windows Components/Windows Defender/MAPS hide

Policy	Setting	Comment
Configure local setting override for reporting to Microsoft MAPS	Disabled	
Join Microsoft MAPS	Enabled	
Join Microsoft MAPS	Advanced MAPS	

Policy	Setting	Comment
Send file samples when further analysis is required	Enabled	
Send file samples when further analysis is required		

Windows Components/Windows Defender/Real-time Protection hide

Policy	Setting	Comment
Turn on behavior monitoring	Enabled	

Windows Components/Windows Defender/Scan hide

Policy	Setting	Comment
Scan removable drives	Enabled	
Turn on e-mail scanning	Enabled	

Windows Components/Windows Installer hide

Policy	Setting	Comment
Allow user control over installs	Disabled	
Always install with elevated privileges	Disabled	

Windows Components/Windows Logon Options hide

Policy	Setting	Comment
Sign-in last interactive user automatically after a system-initiated restart	Disabled	

Windows Components/Windows PowerShell hide

Policy	Setting	Comment
Turn on PowerShell Script Block Logging	Enabled	
Log script block invocation start / stop events:		

Windows Components/Windows Remote Management (WinRM)/WinRM Client hide

Policy	Setting	Comment
Allow Basic authentication	Disabled	
Allow unencrypted traffic	Disabled	
Disallow Digest authentication	Enabled	

Windows Components/Windows Remote Management (WinRM)/WinRM Service hide

Policy	Setting	Comment
Allow Basic authentication	Disabled	
Allow unencrypted traffic	Disabled	
Disallow WinRM from storing RunAs credentials	Enabled	

Extra Registry Settings hide

Display names for some settings cannot be found. You might be able to resolve this issue by updating the .ADM files used by Group Policy Management.

Setting	State
SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy	0
Software\Policies\Microsoft Services\AdmPwd\AdmPwdEnabled	1
Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging\EnableScriptBlockInvocationLogging	0
SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential	0
System\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand	1
System\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand	1
System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting	2
System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting	2
System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect	0
System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect	0
System\CurrentControlSet\Services\Tcpip6\Parameters\DisableIPSourceRouting	2
System\CurrentControlSet\Services\Tcpip6\Parameters\DisableIPSourceRouting	2

User Configuration (Enabled) hide

Policies hide

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local computer.

Control Panel/Personalization hide

Policy	Setting	Comment
Enable screen saver	Enabled	
Password protect the screen saver	Enabled	

XD2017 CC - User - Shell And Start Menu Restrictions

Data collected on: 3/29/2020 12:16:58 AM

General

hide

Details

hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:42 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{9784F723-CED2-40B8-9679-752BDB387F97}
GPO Status	Enabled

Links

hide

Location	Enforced	Link Status	Path
Common Criteria Users	No	Enabled	bvt.local/Common Criteria Users

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

No settings defined.

User Configuration (Enabled)

hide

Policies

hide

Administrative Templates

hide

Policy definitions (ADMX files) retrieved from the local computer.

Desktop

hide

Policy	Setting	Comment
Do not add shares of recently opened documents to Network Locations	Enabled	
Don't save settings at exit	Enabled	
Hide and disable all items on the desktop	Enabled	
Hide Internet Explorer icon on desktop	Enabled	
Hide Network Locations icon on desktop	Enabled	
Prevent adding, dragging, dropping and closing the Taskbar's toolbars	Enabled	
Prohibit adjusting desktop toolbars	Enabled	
Prohibit User from manually redirecting Profile Folders	Enabled	
Remove Computer icon on the desktop	Disabled	
Remove My Documents icon on the desktop	Enabled	
Remove Properties from the Computer icon context menu	Enabled	

Remove Properties from the Documents icon context menu	Enabled
Remove Properties from the Recycle Bin context menu	Enabled
Remove the Desktop Cleanup Wizard	Enabled

Desktop/Active Directory hide

Policy	Setting	Comment
Enable filter in Find dialog box	Disabled	
Hide Active Directory folder	Enabled	

Desktop/Desktop hide

Policy	Setting	Comment
Desktop Wallpaper	Disabled	
Disable Active Desktop	Enabled	
Disallows HTML and Jpg Wallpaper		

Network/Network Connections hide

Policy	Setting	Comment
Ability to change properties of an all user remote access connection	Disabled	
Ability to delete all user remote access connections	Disabled	
Ability to Enable/Disable a LAN connection	Disabled	
Ability to rename all user remote access connections	Disabled	
Ability to rename LAN connections	Disabled	
Ability to rename LAN connections or remote access connections available to all users	Disabled	
Prohibit access to properties of a LAN connection	Enabled	
Prohibit access to properties of components of a LAN connection	Enabled	
Prohibit access to properties of components of a remote access connection	Enabled	
Prohibit access to the Advanced Settings item on the Advanced menu	Enabled	
Prohibit access to the New Connection Wizard	Enabled	
Prohibit access to the Remote Access Preferences item on the Advanced menu	Enabled	
Prohibit adding and removing components for a LAN or remote access connection	Enabled	
Prohibit changing properties of a private remote access connection	Enabled	
Prohibit connecting and disconnecting a remote access connection	Enabled	
Prohibit deletion of remote access connections	Enabled	
Prohibit Enabling/Disabling components of a LAN connection	Enabled	
Prohibit renaming private remote access connections	Enabled	
Prohibit TCP/IP advanced configuration	Enabled	
Prohibit viewing of status for an active connection	Enabled	
Turn off notifications when a connection has only limited or no connectivity	Enabled	

Network/Offline Files hide

Policy	Setting	Comment
Remove "Work offline" command	Enabled	

Network/Windows Connect Now hide

Policy	Setting	Comment
Prohibit access of the Windows Connect Now wizards	Enabled	

Start Menu and Taskbar hide

Policy	Setting	Comment
Add Logoff to the Start Menu	Disabled	
Add Search Internet link to Start Menu	Disabled	

Add the Run command to the Start Menu	Disabled
Do not allow pinning Store app to the Taskbar	Enabled
Do not search communications	Enabled
Do not search for files	Enabled
Do not search Internet	Enabled
Do not search programs and Control Panel items	Enabled
Do not use the search-based method when resolving shell shortcuts	Enabled
Do not use the tracking-based method when resolving shell shortcuts	Enabled
Lock all taskbar settings	Enabled
Prevent changes to Taskbar and Start Menu Settings	Enabled
Prevent users from adding or removing toolbars	Enabled
Prevent users from customizing their Start Screen	Enabled
Prevent users from uninstalling applications from Start	Enabled
Remove access to the context menus for the taskbar	Enabled
Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands	Enabled
Remove common program groups from Start Menu	Enabled
Remove Default Programs link from the Start menu.	Enabled
Remove Downloads link from Start Menu	Enabled
Remove Games link from Start Menu	Enabled
Remove Help menu from Start Menu	Enabled
Remove Homegroup link from Start Menu	Enabled
Remove links and access to Windows Update	Enabled
Remove Music icon from Start Menu	Enabled
Remove Network Connections from Start Menu	Enabled
Remove Network icon from Start Menu	Enabled
Remove Notifications and Action Center	Enabled
Remove Pictures icon from Start Menu	Enabled
Remove pinned programs list from the Start Menu	Enabled
Remove programs on Settings menu	Enabled
Remove Recorded TV link from Start Menu	Enabled
Remove Run menu from Start Menu	Enabled
Remove Search Computer link	Enabled
Remove Search link from Start Menu	Enabled
Remove See More Results / Search Everywhere link	Enabled
Remove the "Undock PC" button from the Start Menu	Enabled
Remove the networking icon	Enabled
Remove the Security and Maintenance icon	Enabled
Remove the volume control icon	Enabled
Remove Videos link from Start Menu	Enabled
Show "Run as different user" command on Start	Disabled
Show Windows Store apps on the taskbar	Disabled
Turn off all balloon notifications	Enabled
Turn off feature advertisement balloon notifications	Enabled
Turn off notification area cleanup	Enabled

Start Menu and Taskbar/Notifications hide

Policy	Setting	Comment
Turn off notifications network usage	Enabled	
Turn off tile notifications	Enabled	
Turn off toast notifications	Enabled	
Turn off toast notifications on the lock screen	Enabled	

Windows Components/Edge UI hide

Policy	Setting	Comment
Allow edge swipe	Disabled	
Disable help tips	Enabled	
Do not show recent apps when the mouse is pointing to the upper-left corner of the screen	Enabled	

Prevent users from replacing the Command Prompt with Windows PowerShell in the menu they see when they right-click the lower-left corner or press the Windows logo key+X	Enabled
Search, Share, Start, Devices, and Settings don't appear when the mouse is pointing to the upper-right corner of the screen	Enabled
Turn off switching between recent apps	Enabled
Turn off tracking of app usage	Enabled

Windows Components/File Explorer hide

Policy	Setting	Comment
Allow only per user or approved shell extensions	Enabled	
Display the menu bar in File Explorer	Disabled	
Do not allow Folder Options to be opened from the Options button on the View tab of the ribbon	Enabled	
Do not display the Welcome Center at user logon	Enabled	
Do not request alternate credentials	Enabled	
Hide these specified drives in My Computer	Enabled	
Pick one of the following combinations	Restrict A, B and C drives 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 A, B and C drives only	

Policy	Setting	Comment
Remove "Map Network Drive" and "Disconnect Network Drive"	Enabled	
Remove CD Burning features	Enabled	
Remove DFS tab	Enabled	
Remove File Explorer's default context menu	Enabled	
Remove File menu from File Explorer	Enabled	
Remove Hardware tab	Enabled	
Remove Search button from File Explorer	Enabled	
Remove Security tab	Enabled	
Remove Shared Documents from My Computer	Enabled	
Remove the Search the Internet "Search again" link	Enabled	
Turn off display of recent search entries in the File Explorer search box	Enabled	
Turn off shell protocol protected mode	Disabled	
Turn off Windows+X hotkeys	Enabled	

Windows Components/File Explorer/Common Open File Dialog hide

Policy	Setting	Comment
Hide the common dialog back button	Enabled	
Hide the common dialog places bar	Enabled	
Hide the dropdown list of recent files	Enabled	

Windows Components/File Explorer/Explorer Frame Pane hide

Policy	Setting	Comment
Turn off Preview Pane	Enabled	
Turn on or off details pane	Enabled	
Configure details pane	Always hide	

Windows Components/File Explorer/Previous Versions hide

Policy	Setting	Comment
Hide previous versions list for local files	Enabled	
Hide previous versions list for remote files	Enabled	
Hide previous versions of files on backup location	Enabled	

Prevent restoring local previous versions	Enabled
Prevent restoring previous versions from backups	Enabled
Prevent restoring remote previous versions	Enabled

XD2017 CC - User - Control Panel Restrictions

Data collected on: 3/29/2020 12:16:58 AM

General

hide

Details

hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:44 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{9FE9B02B-D104-4344-9E61-08940FCA0A86}
GPO Status	Enabled

Links

hide

Location	Enforced	Link Status	Path
Common Criteria Users	No	Enabled	bvt.local/Common Criteria Users

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Administrative Templates

hide

Policy definitions (ADMX files) retrieved from the local computer.

Control Panel/Personalization

hide

Policy	Setting	Comment
Prevent changing lock screen and logon image	Enabled	
Prevent changing start menu background	Enabled	

User Configuration (Enabled)

hide

Policies

hide

Administrative Templates

hide

Policy definitions (ADMX files) retrieved from the local computer.

Control Panel

hide

Policy	Setting	Comment
Hide specified Control Panel items	Enabled	

List of disallowed Control Panel items
Microsoft.ActionCenter
Microsoft.AdministrativeTools
Microsoft.AutoPlay
Microsoft.BackupAndRestore
Microsoft.BiometricDevices
Microsoft.BitLockerDriveEncryption
Microsoft.ColorManagement
Microsoft.CredentialManager
Microsoft.DateAndTime
Microsoft.DefaultLocation
Microsoft.DefaultPrograms
Microsoft.DesktopGadgets
Microsoft.DeviceManager
Microsoft.DevicesAndPrinters
Microsoft.Display
Microsoft.EaseOfAccessCenter
Microsoft.FolderOptions
Microsoft.Fonts
Microsoft.GameControllers
Microsoft.GetPrograms
Microsoft.GettingStarted
Microsoft.HomeGroup
Microsoft.IndexingOptions
Microsoft.Infrared
Microsoft.InternetOptions
Microsoft.iSCSIInitiator
Microsoft.Keyboard
Microsoft.LocationAndOtherSensors
Microsoft.Mouse
Microsoft.NetworkAndSharingCenter
Microsoft.NotificationAreaIcons
Microsoft.OfflineFiles
Microsoft.ParentalControls
Microsoft.PenAndTouch
Microsoft.PeopleNearMe
Microsoft.PerformanceInformationAndTools
Microsoft.Personalization
Microsoft.PhoneAndModem
Microsoft.PowerOptions
Microsoft.ProgramsAndFeatures
Microsoft.Recovery
Microsoft.RegionAndLanguage
Microsoft.RemoteAppAndDesktopConnections
Microsoft.ScannersAndCameras
Microsoft.Sound
Microsoft.SpeechRecognition
Microsoft.SyncCenter
Microsoft.System
Microsoft.TabletPCSettings
Microsoft.TaskbarAndStartMenu
Microsoft.TextToSpeech
Microsoft.Troubleshooting
Microsoft.UserAccounts
Microsoft.WindowsAnytimeUpgrade
Microsoft.CardSpace
Microsoft.WindowsDefender
Microsoft.WindowsFirewall
Microsoft.MobilityCenter
Microsoft.WindowsSideShow
Microsoft.WindowsUpdate
Microsoft.Language
Microsoft.FileHistory
Microsoft.StorageSpaces
Microsoft.TSAppInstall

Policy	Setting	Comment
Prohibit access to Control Panel and PC settings	Enabled	

Control Panel/Add or Remove Programs hide

Policy	Setting	Comment
Hide Add New Programs page	Enabled	
Hide Add/Remove Windows Components page	Enabled	
Hide Change or Remove Programs page	Enabled	
Hide the "Add a program from CD-ROM or floppy disk" option	Enabled	
Hide the "Add programs from Microsoft" option	Enabled	
Hide the "Add programs from your network" option	Enabled	
Hide the Set Program Access and Defaults page	Enabled	
Remove Add or Remove Programs	Enabled	
Remove Support Information	Enabled	

Control Panel/Display hide

Policy	Setting	Comment
Disable the Display Control Panel	Enabled	
Hide Settings tab	Enabled	

Control Panel/Personalization hide

Policy	Setting	Comment
Prevent changing color and appearance	Enabled	
Prevent changing color scheme	Enabled	
Prevent changing desktop background	Enabled	
Prevent changing desktop icons	Enabled	
Prevent changing mouse pointers	Enabled	
Prevent changing screen saver	Enabled	

Prevent changing sounds	Enabled
Prevent changing theme	Enabled
Prevent changing visual style for windows and buttons	Enabled
Prohibit selection of visual style font size	Enabled

Control Panel/Printers hide

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

Control Panel/Programs hide

Policy	Setting	Comment
Hide "Get Programs" page	Enabled	
Hide "Installed Updates" page	Enabled	
Hide "Programs and Features" page	Enabled	
Hide "Set Program Access and Computer Defaults" page	Enabled	
Hide "Windows Features"	Enabled	
Hide "Windows Marketplace"	Enabled	
Hide the Programs Control Panel	Enabled	

Control Panel/Regional and Language Options hide

Policy	Setting	Comment
Hide Regional and Language Options administrative options	Enabled	
Hide the geographic location option	Enabled	
Hide the select language group options	Enabled	
Hide user locale selection and customization options	Enabled	

XD2017 CC - Computer - Allow CC Admin Logon

Data collected on: 3/29/2020 12:16:58 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:58 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{A7F5DD40-3FD9-431F-B621-A2C15A84F220}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Servers	No	Enabled	bvt.local/Common Criteria TOE Computers/Servers

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Local Policies/User Rights Assignment hide

Policy	Setting
Allow log on locally	BUILTIN\Administrators, ccxdadmins
Shut down the system	BUILTIN\Administrators, ccxdadmins

User Configuration (Enabled) hide

No settings defined.

XD2017 CC - Computer - Shell And Start Menu Restrictions

Data collected on: 3/29/2020 12:16:58 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:48 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{ABDF1D60-D45E-4257-A397-EA6FB6DA6C36}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Desktops	No	Enabled	bvt.local/Common Criteria TOE Computers/Desktops

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local computer.

Control Panel/Personalization hide

Policy	Setting	Comment
Prevent changing lock screen and logon image	Enabled	
Prevent changing start menu background	Enabled	

Windows Components/Credential User Interface hide

Policy	Setting	Comment
Do not display the password reveal button	Enabled	

Windows Components/Data Collection and Preview Builds hide

Policy	Setting	Comment
Allow Telemetry	Enabled	

0 - Security [Enterprise Only]

Policy	Setting	Comment
Disable pre-release features or settings	Disabled	
Do not show feedback notifications	Enabled	
Toggle user control over Insider builds	Disabled	

Windows Components/File Explorer hide

Policy	Setting	Comment
Do not show the 'new application installed' notification	Enabled	
Show hibernate in the power options menu	Disabled	
Show lock in the user tile menu	Disabled	
Show sleep in the power options menu	Disabled	
Turn off Data Execution Prevention for Explorer	Disabled	
Turn off shell protocol protected mode	Disabled	

Windows Components/File Explorer/Previous Versions hide

Policy	Setting	Comment
Hide previous versions list for local files	Enabled	
Hide previous versions list for remote files	Enabled	
Hide previous versions of files on backup location	Enabled	
Prevent restoring local previous versions	Enabled	
Prevent restoring previous versions from backups	Enabled	
Prevent restoring remote previous versions	Enabled	

Windows Components/File History hide

Policy	Setting	Comment
Turn off File History	Enabled	

Windows Components/HomeGroup hide

Policy	Setting	Comment
Prevent the computer from joining a homegroup	Enabled	

Windows Components/Online Assistance hide

Policy	Setting	Comment
Turn off Active Help	Enabled	

Windows Components/Presentation Settings hide

Policy	Setting	Comment
Turn off Windows presentation settings	Enabled	

Windows Components/Search hide

Policy	Setting	Comment
Allow Cortana	Disabled	
Allow Cortana above lock screen	Disabled	
Do not allow locations on removable drives to be added to libraries	Enabled	
Do not allow web search	Enabled	
Don't search the web or display web results in Search	Enabled	
Prevent adding UNC locations to index from Control Panel	Enabled	
Prevent adding user-specified locations to the All Locations menu	Enabled	
Prevent customization of indexed locations in Control Panel	Enabled	

Prevent the display of advanced indexing options for Windows Search in the Control Panel	Enabled

Windows Components/Smart Card hide

Policy	Setting	Comment
Allow Integrated Unblock screen to be displayed at the time of logon	Enabled	

Extra Registry Settings hide

Display names for some settings cannot be found. You might be able to resolve this issue by updating the .ADM files used by Group Policy Management.

Setting	State
Software\Policies\Microsoft\NetworkProjector\DisableNetworkProjector	1
Software\Policies\Microsoft\Windows\System\EnableSmartScreen	2

User Configuration (Enabled) hide

No settings defined.

XD2017 CC - Computer - Internet Explorer Restrictions

Data collected on: 3/29/2020 12:16:58 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:54 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{AC6F11B0-B57D-49A9-9BE7-8CB4FDD83DCB}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Desktops	No	Enabled	bvt.local/Common Criteria TOE Computers/Desktops

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local computer.

System hide

Policy	Setting	Comment
Turn off Data Execution Prevention for HTML Help Executible	Disabled	

Windows Components/Internet Explorer

hide

Policy	Setting	Comment
Automatically activate newly installed add-ons	Disabled	
Disable Automatic Install of Internet Explorer components	Enabled	
Disable Periodic Check for Internet Explorer software updates	Enabled	
Disable showing the splash screen	Enabled	
Disable software update shell notifications on program launch	Enabled	
Install new versions of Internet Explorer automatically	Disabled	
Prevent participation in the Customer Experience Improvement Program	Enabled	
Prevent running First Run wizard	Enabled	
Select your choice	Go directly to home page	

Policy	Setting	Comment
Restrict search providers to a specific list	Enabled	
Turn off ability to pin sites in Internet Explorer on the desktop	Enabled	
Turn off Automatic Crash Recovery	Enabled	

Windows Components/Internet Explorer/Accelerators

hide

Policy	Setting	Comment
Restrict Accelerators to those deployed through Group Policy	Enabled	
Turn off Accelerators	Enabled	

Windows Components/Internet Explorer/Internet Control Panel/Advanced Page

hide

Policy	Setting	Comment
Allow active content from CDs to run on user machines	Disabled	
Allow Install On Demand (except Internet Explorer)	Disabled	
Allow Install On Demand (Internet Explorer)	Disabled	
Allow third-party browser extensions	Disabled	
Always send Do Not Track header	Enabled	
Automatically check for Internet Explorer updates	Disabled	
Do not allow resetting Internet Explorer settings	Enabled	
Do not save encrypted pages to disk	Enabled	
Turn off encryption support	Enabled	
Secure Protocol combinations	Only use TLS 1.2	

Policy	Setting	Comment
Turn off Profile Assistant	Enabled	
Turn off the flip ahead with page prediction feature	Enabled	
Turn on Caret Browsing support	Disabled	

Windows Components/Internet Explorer/Internet Control Panel/General Page

hide

Policy	Setting	Comment
Start Internet Explorer with tabs from last browsing session	Disabled	

Windows Components/Internet Explorer/Internet Control Panel/Security Page

hide

Policy	Setting	Comment
Intranet Sites: Include all local (intranet) sites not listed in other zones	Disabled	
Intranet Sites: Include all sites that bypass the proxy server	Disabled	
Turn on automatic detection of intranet	Disabled	
Turn on Notification bar notification for intranet content	Disabled	

Windows Components/Internet Explorer/Internet Control Panel/Security Page/Internet Zone

hide

Policy	Setting	Comment
Allow active content over restricted protocols to access my computer	Enabled	

Allow active content over restricted protocols to access my computer	Disable

Policy	Setting	Comment
Allow active scripting	Enabled	
Allow active scripting	Enable	

Policy	Setting	Comment
Allow binary and script behaviors	Enabled	
Allow Binary and Script Behaviors	Disable	

Policy	Setting	Comment
Allow file downloads	Enabled	
Allow file downloads	Disable	

Policy	Setting	Comment
Allow loading of XAML Browser Applications	Enabled	
XAML browser applications	Disable	

Policy	Setting	Comment
Allow loading of XPS files	Enabled	
XPS documents	Disable	

Policy	Setting	Comment
Allow META REFRESH	Enabled	
Allow META REFRESH	Enable	

Policy	Setting	Comment
Allow video and animation on a webpage that uses an older media player	Enabled	
Allow video and animation on a Web page that uses a legacy media player	Disable	

Policy	Setting	Comment
Allow websites to open windows without status bar or Address bar	Enabled	
Open windows without address or status bars	Disable	

Policy	Setting	Comment
Allow websites to prompt for information by using scripted windows	Enabled	
Prompt for information using scripted windows	Disable	

Policy	Setting	Comment
Automatic prompting for ActiveX controls	Enabled	
Automatic prompting for ActiveX controls	Disable	

Policy	Setting	Comment
Display mixed content	Enabled	
Display mixed content	Disable	

Policy	Setting	Comment
Run ActiveX controls and plugins	Enabled	
Run ActiveX controls and plugins	Disable	

Policy	Setting	Comment
Script ActiveX controls marked safe for scripting	Enabled	
Script ActiveX controls marked safe for scripting	Disable	

Policy	Setting	Comment
Scripting of Java applets	Enabled	
Scripting of Java applets	Disable	

Policy	Setting	Comment
Submit non-encrypted form data	Enabled	
Submit non-encrypted form data	Enable	

Policy	Setting	Comment
Turn off .NET Framework Setup	Enabled	
.NET Framework Setup	Enable	

Policy	Setting	Comment
Turn off first-run prompt	Enabled	
First-Run Opt-In	Enable	

Policy	Setting	Comment
Turn on SmartScreen Filter scan	Enabled	
Use SmartScreen Filter	Enable	

Windows Components/Internet Explorer/Internet Control Panel/Security Page/Intranet Zone hide

Policy	Setting	Comment
Access data sources across domains	Enabled	
Access data sources across domains	Disable	

Policy	Setting	Comment
Allow active content over restricted protocols to access my computer	Enabled	
Allow active content over restricted protocols to access my computer	Disable	

Policy	Setting	Comment
Allow active scripting	Enabled	
Allow active scripting	Enable	

Policy	Setting	Comment
Allow binary and script behaviors	Enabled	
Allow Binary and Script Behaviors	Disable	

Policy	Setting	Comment
Allow cut, copy or paste operations from the clipboard via script	Enabled	
Allow paste operations via script	Disable	

Policy	Setting	Comment
Allow drag and drop or copy and paste files	Enabled	
Allow drag and drop or copy and paste files	Disable	

Policy	Setting	Comment
Allow file downloads	Enabled	
Allow file downloads	Enable	

Policy	Setting	Comment
Allow font downloads	Enabled	
Allow font downloads	Disable	

Policy	Setting	Comment
Allow installation of desktop items	Enabled	
Allow installation of desktop items	Disable	

Policy	Setting	Comment
Allow loading of XAML Browser Applications	Enabled	
XAML browser applications	Disable	

Policy	Setting	Comment
Allow loading of XAML files	Enabled	
XAML Files	Disable	

Policy	Setting	Comment
Allow loading of XPS files	Enabled	
XPS documents	Disable	

Policy	Setting	Comment

Allow META REFRESH	Enabled	
Allow META REFRESH	Disable	

Policy	Setting	Comment
Allow only approved domains to use ActiveX controls without prompt	Enabled	
Only allow approved domains to use ActiveX controls without prompt	Enable	

Policy	Setting	Comment
Allow scripting of Internet Explorer WebBrowser controls	Enabled	
Internet Explorer web browser control	Disable	

Policy	Setting	Comment
Allow script-initiated windows without size or position constraints	Enabled	
Allow script-initiated windows without size or position constraints	Disable	

Policy	Setting	Comment
Allow scriptlets	Enabled	
Scriptlets	Disable	

Policy	Setting	Comment
Allow updates to status bar via script	Enabled	
Status bar updates via script	Disable	

Policy	Setting	Comment
Allow video and animation on a webpage that uses an older media player	Enabled	
Allow video and animation on a Web page that uses a legacy media player	Disable	

Policy	Setting	Comment
Allow websites to open windows without status bar or Address bar	Enabled	
Open windows without address or status bars	Disable	

Policy	Setting	Comment
Allow websites to prompt for information by using scripted windows	Enabled	
Prompt for information using scripted windows	Disable	

Policy	Setting	Comment
Automatic prompting for ActiveX controls	Enabled	
Automatic prompting for ActiveX controls	Disable	

Policy	Setting	Comment
Automatic prompting for file downloads	Enabled	
Automatic prompting for file downloads	Disable	

Policy	Setting	Comment
Display mixed content	Enabled	
Display mixed content	Disable	

Policy	Setting	Comment
Download signed ActiveX controls	Enabled	
Download signed ActiveX controls	Disable	

Policy	Setting	Comment
Download unsigned ActiveX controls	Enabled	
Download unsigned ActiveX controls	Disable	

Policy	Setting	Comment
Enable dragging of content from different domains across windows	Enabled	

Enable dragging of content from different domains across windows	Disable

Policy	Setting	Comment
Enable dragging of content from different domains within a window	Enabled	
Enable dragging of content from different domains within a window	Disable	

Policy	Setting	Comment
Enable MIME Sniffing	Enabled	
Enable MIME Sniffing	Disable	

Policy	Setting	Comment
Include local path when user is uploading files to a server	Enabled	
Include local directory path when uploading files to a server	Disable	

Policy	Setting	Comment
Launching applications and files in an IFRAME	Enabled	
Launching applications and files in an IFRAME	Disable	

Policy	Setting	Comment
Logon options	Enabled	
Logon options	Automatic logon only in Intranet zone	

Policy	Setting	Comment
Navigate windows and frames across different domains	Enabled	
Navigate windows and frames across different domains	Disable	

Policy	Setting	Comment
Run .NET Framework-reliant components not signed with Authenticode	Enabled	
Run .NET Framework-reliant components not signed with Authenticode	Disable	

Policy	Setting	Comment
Run .NET Framework-reliant components signed with Authenticode	Enabled	
Run .NET Framework-reliant components signed with Authenticode	Disable	

Policy	Setting	Comment
Run ActiveX controls and plugins	Enabled	
Run ActiveX controls and plugins	Enable	

Policy	Setting	Comment
Script ActiveX controls marked safe for scripting	Enabled	
Script ActiveX controls marked safe for scripting	Enable	

Policy	Setting	Comment
Scripting of Java applets	Enabled	
Scripting of Java applets	Disable	

Policy	Setting	Comment
Show security warning for potentially unsafe files	Enabled	
Launching programs and unsafe files	Enable	

Policy	Setting	Comment
Software channel permissions	Enabled	
Software channel permissions	High safety	

Policy	Setting	Comment
Submit non-encrypted form data	Enabled	
Submit non-encrypted form data	Disable	

Policy	Setting	Comment
Turn off .NET Framework Setup	Enabled	
.NET Framework Setup	Disable	

Policy	Setting	Comment
Turn off first-run prompt	Enabled	
First-Run Opt-In	Enable	

Policy	Setting	Comment
Turn on Cross-Site Scripting Filter	Enabled	
Turn on Cross-Site Scripting (XSS) Filter	Enable	

Policy	Setting	Comment
Turn on Protected Mode	Enabled	
Protected Mode	Disable	

Policy	Setting	Comment
Turn on SmartScreen Filter scan	Enabled	
Use SmartScreen Filter	Enable	

Policy	Setting	Comment
Use Pop-up Blocker	Enabled	
Use Pop-up Blocker	Disable	

Policy	Setting	Comment
Userdata persistence	Enabled	
Userdata persistence	Disable	

Policy	Setting	Comment
Web sites in less privileged Web content zones can navigate into this zone	Enabled	
Web sites in less privileged Web content zones can navigate into this zone	Disable	

Windows Components/Internet Explorer/Internet Settings hide

Policy	Setting	Comment
Open Internet Explorer tiles on the desktop	Enabled	
Set how links are opened in Internet Explorer	Enabled	
Default browser launch behavior for links	Always in Internet Explorer on the desktop	

Windows Components/Internet Explorer/Internet Settings/Advanced settings/Browsing hide

Policy	Setting	Comment
Go to an intranet site for a one-word entry in the Address bar	Disabled	

Windows Components/Internet Explorer/Internet Settings/Advanced settings/Multimedia hide

Policy	Setting	Comment
Allow Internet Explorer to play media files that use alternative codecs	Disabled	

Windows Components/Internet Explorer/Internet Settings/Advanced settings/Searching hide

Policy	Setting	Comment
Prevent configuration of search on Address bar	Enabled	
When searching from the address bar:	Do not search from the address bar	

Policy	Setting	Comment
Prevent configuration of top-result search on Address bar	Enabled	
When searching from the Address bar:	Disable top result search	

Windows Components/Internet Explorer/Internet Settings/Component Updates/Help Menu > About Internet Explorer hide

Policy	Setting	Comment
Prevent specifying cipher strength update information URLs	Enabled	
Cipher Strength Update Information URL:	http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=128bit	

Windows Components/Internet Explorer/Privacy hide

Policy	Setting	Comment
Establish Tracking Protection threshold	Enabled	

Threshold (3-30):	3

Policy	Setting	Comment
Turn off InPrivate Browsing	Enabled	
Turn off InPrivate Filtering	Enabled	
Turn off Tracking Protection	Enabled	

Windows Components/Internet Explorer/Security Features hide

Policy	Setting	Comment
Allow fallback to SSL 3.0 (Internet Explorer)	Enabled	

Allow insecure fallback for:	No Sites

Policy	Setting	Comment
Do not display the reveal password button	Enabled	
Turn off Data Execution Prevention	Disabled	
Turn off Data URI support	Enabled	

Windows Components/Internet Explorer/Security Features/Add-on Management hide

Policy	Setting	Comment
Add-on List	Enabled	

Add-on List	
{238F6F83-B8B4-11CF-8771-00A024541EE3}	1

Policy	Setting	Comment
Deny all add-ons unless specifically allowed in the Add-on List	Enabled	
Remove "Run this time" button for outdated ActiveX controls in Internet Explorer	Enabled	
Turn off Adobe Flash in Internet Explorer and prevent applications from using Internet Explorer technology to instantiate Flash objects	Enabled	

Windows Components/Internet Explorer/Security Features/AJAX hide

Policy	Setting	Comment
Allow native XMLHTTP support	Disabled	
Turn off cross-document messaging	Enabled	
Turn off the WebSocket Object	Enabled	
Turn off the XDomainRequest object	Enabled	

Windows Components/Internet Explorer/Security Features/Binary Behavior Security Restriction hide

Policy	Setting	Comment
Install binaries signed by MD2 and MD4 signing technologies	Disabled	

Windows Components/Location and Sensors hide

Policy	Setting	Comment
Turn off location	Enabled	
Turn off location scripting	Enabled	
Turn off sensors	Enabled	

Windows Components/Location and Sensors/Windows Location Provider hide

Policy	Setting	Comment
Turn off Windows Location Provider	Enabled	

Windows Components/RSS Feeds hide

Policy	Setting	Comment
Prevent access to feed list	Enabled	
Prevent automatic discovery of feeds and Web Slices	Enabled	
Prevent subscribing to or deleting a feed or a Web Slice	Enabled	

Turn off background synchronization for feeds and Web Slices	Enabled
Turn on Basic feed authentication over HTTP	Disabled

Extra Registry Settings hide

Display names for some settings cannot be found. You might be able to resolve this issue by updating the .ADM files used by Group Policy Management.

Setting	State
Software\Policies\Microsoft\Internet Explorer\Main\ShowContentAdvisor	0
Software\Policies\Microsoft\MicrosoftEdge\Extensions\ExtensionsEnabled	0
Software\Policies\Microsoft\MicrosoftEdge\F12\AllowDeveloperTools	0
Software\Policies\Microsoft\MicrosoftEdge\Main\AllowInPrivate	0
Software\Policies\Microsoft\MicrosoftEdge\Main\AllowPopups	yes
Software\Policies\Microsoft\MicrosoftEdge\Main\DoNotTrack	1
Software\Policies\Microsoft\MicrosoftEdge\Main\FormSuggest Passwords	no
Software\Policies\Microsoft\MicrosoftEdge\Main\PreventAccessToAboutFlagsInMicrosoftEdge	1
Software\Policies\Microsoft\MicrosoftEdge\Main\SendIntranetTraffictoInternetExplorer	1
Software\Policies\Microsoft\MicrosoftEdge\Main\Use FormSuggest	no
Software\Policies\Microsoft\MicrosoftEdge\PhishingFilter\EnabledV9	1
Software\Policies\Microsoft\MicrosoftEdge\PhishingFilter\PreventOverride	1
Software\Policies\Microsoft\MicrosoftEdge\PhishingFilter\PreventOverrideAppRepUnknown	1
Software\Policies\Microsoft\MicrosoftEdge\SearchScopes\ShowSearchSuggestionsGlobal	0
Software\Policies\Microsoft\MicrosoftEdge\ServiceUI\AllowWebContentOnNewTabPage	0

User Configuration (Enabled) hide

No settings defined.

XD2017 CC - User - System settings

Data collected on: 3/29/2020 12:16:58 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:42 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{AE1168FD-2BD8-4C3B-8C77-2985E63C6039}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Common Criteria Users	No	Enabled	bvt.local/Common Criteria Users

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

No settings defined.

User Configuration (Enabled) hide

Policies hide

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local computer.

System hide

Policy	Setting	Comment
Do not display the Getting Started welcome screen at logon	Enabled	
Don't run specified Windows applications	Enabled	

List of disallowed applications
powershell.exe
PowerShell_ISE.exe
mstsc.exe

Policy	Setting	Comment
Download missing COM components	Disabled	
Prevent access to registry editing tools	Enabled	
Disable regedit from running silently?	Yes	

Policy	Setting	Comment
Prevent access to the command prompt	Enabled	
Disable the command prompt script processing also?	No	

System/Ctrl+Alt+Del Options hide

Policy	Setting	Comment
Remove Task Manager	Enabled	

System/Logon hide

Policy	Setting	Comment
Do not process the legacy run list	Enabled	
Do not process the run once list	Enabled	

System/Scripts hide

Policy	Setting	Comment
Run legacy logon scripts hidden	Enabled	

XD2017 CC - Computer - Security Settings

Data collected on: 3/29/2020 12:16:58 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:50 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{B273F4DF-F2DB-443D-A4D1-798634C4C8B8}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Desktops	No	Enabled	bvt.local/Common Criteria TOE Computers/Desktops

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Local Policies/User Rights Assignment

hide

Policy	Setting
Allow log on through Terminal Services	

Local Policies/Security Options

hide

Devices

hide

Policy	Setting
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	Enabled

Interactive Logon

hide

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

Network Access

hide

Policy	Setting
Network access: Do not allow storage of passwords and credentials for network authentication	Enabled
Network access: Shares that can be accessed anonymously	

Shutdown

hide

Policy	Setting
Shutdown: Allow system to be shut down without having to log on	Disabled

System Settings

hide

Policy	Setting
System settings: Optional subsystems	

User Account Control

hide

Policy	Setting
User Account Control: Only elevate executables that are signed and validated	Enabled

Windows Firewall with Advanced Security

hide

Global Settings

hide

Policy	Setting
Policy version	2.20
Disable stateful FTP	Not Configured
Disable stateful PPTP	Not Configured
IPsec exempt	Not Configured

IPsec through NAT	Not Configured
Preshared key encoding	Not Configured
SA idle time	Not Configured
Strong CRL check	Not Configured

Domain Profile Settings hide

Policy	Setting
Firewall state	On
Inbound connections	Not Configured
Outbound connections	Not Configured
Apply local firewall rules	Not Configured
Apply local connection security rules	Not Configured
Display notifications	Not Configured
Allow unicast responses	Not Configured
Log dropped packets	Not Configured
Log successful connections	Not Configured
Log file path	Not Configured
Log file maximum size (KB)	Not Configured

Private Profile Settings hide

Policy	Setting
Firewall state	On
Inbound connections	Not Configured
Outbound connections	Not Configured
Apply local firewall rules	Not Configured
Apply local connection security rules	Not Configured
Display notifications	Not Configured
Allow unicast responses	Not Configured
Log dropped packets	Not Configured
Log successful connections	Not Configured
Log file path	Not Configured
Log file maximum size (KB)	Not Configured

Public Profile Settings hide

Policy	Setting
Firewall state	On
Inbound connections	Not Configured
Outbound connections	Not Configured
Apply local firewall rules	Not Configured
Apply local connection security rules	Not Configured
Display notifications	Not Configured
Allow unicast responses	Not Configured
Log dropped packets	Not Configured
Log successful connections	Not Configured
Log file path	Not Configured
Log file maximum size (KB)	Not Configured

Connection Security Settings hide

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local computer.

Network/Network Connections/Windows Firewall/Domain Profile hide

Policy	Setting	Comment
Windows Firewall: Protect all network connections	Enabled	

User Configuration (Enabled) hide

No settings defined.

XD2017 CC - Computer - System settings

Data collected on: 3/29/2020 12:16:58 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:46 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{B3A4D97E-24A3-4AB1-8874-77F65CF7C130}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Desktops	No	Enabled	bvt.local/Common Criteria TOE Computers/Desktops

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local computer.

System hide

Policy	Setting	Comment
Do not display Manage Your Server page at logon	Enabled	
Download missing COM components	Disabled	
Restrict potentially unsafe HTML Help functions to specified folders	Enabled	

Enter folder names separated by semi-colons:
Example: %windir%\Help;%windir%\pchealth;%programfiles%

Policy	Setting	Comment
Turn off Data Execution Prevention for HTML Help Executible	Disabled	

System/Internet Communication Management hide

Policy	Setting	Comment
Restrict Internet communication	Enabled	

System/Internet Communication Management/Internet Communication settings hide

Policy	Setting	Comment
Turn off access to all Windows Update features	Enabled	
Turn off access to the Store	Enabled	
Turn off Automatic Root Certificates Update	Disabled	
Turn off downloading of print drivers over HTTP	Enabled	
Turn off Event Viewer "Events.asp" links	Enabled	
Turn off handwriting personalization data sharing	Enabled	
Turn off handwriting recognition error reporting	Enabled	

Turn off Help and Support Center "Did you know?" content	Enabled
Turn off Help and Support Center Microsoft Knowledge Base search	Enabled
Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com	Enabled
Turn off Internet download for Web publishing and online ordering wizards	Enabled
Turn off Internet File Association service	Enabled
Turn off printing over HTTP	Enabled
Turn off Registration if URL connection is referring to Microsoft.com	Enabled
Turn off Search Companion content file updates	Enabled
Turn off the "Order Prints" picture task	Enabled
Turn off the "Publish to Web" task for files and folders	Enabled
Turn off the Windows Messenger Customer Experience Improvement Program	Enabled
Turn off Windows Customer Experience Improvement Program	Enabled
Turn off Windows Error Reporting	Enabled
Turn off Windows Network Connectivity Status Indicator active tests	Enabled
Turn off Windows Update device driver searching	Enabled

System/Logon hide

Policy	Setting	Comment
Always wait for the network at computer startup and logon	Enabled	
Do not display network selection UI	Enabled	
Turn off app notifications on the lock screen	Enabled	
Turn off picture password sign-in	Enabled	

System/Power Management/Sleep Settings hide

Policy	Setting	Comment
Allow standby states (S1-S3) when sleeping (on battery)	Disabled	
Allow standby states (S1-S3) when sleeping (plugged in)	Disabled	

System/Remote Assistance hide

Policy	Setting	Comment
Configure Offer Remote Assistance	Disabled	
Configure Solicited Remote Assistance	Disabled	

System/Server Manager hide

Policy	Setting	Comment
Do not display Server Manager automatically at logon	Enabled	

Windows Components/Windows Error Reporting hide

Policy	Setting	Comment
Disable Windows Error Reporting	Enabled	

Preferences hide

Windows Settings hide

Registry hide

SafeModeBlockNonAdmins (Order: 1) hide

General hide

Action	Update

Properties

Hive	HKEY_LOCAL_MACHINE
Key path	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
Value name	SafeModeBlockNonAdmins
Value type	REG_DWORD
Value data	0x1 (1)

Common hide

Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

User Configuration (Enabled) hide

No settings defined.

IE11 User Security Compliance

Data collected on: 3/29/2020 12:16:58 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:02:00 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{BB70BC6F-2F86-4BC3-A1E4-9A927D60299C}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Common Criteria Users	No	Enabled	bvt.local/Common Criteria Users

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

No settings defined.

User Configuration (Enabled) hide

Policies hide

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/Internet Explorer hide

Policy	Setting	Comment
Disable AutoComplete for forms	Enabled	
Disable changing certificate settings	Enabled	
Turn on the auto-complete feature for user names and passwords on forms	Disabled	

XD2017 CC - Computer - Installation Restrictions

Data collected on: 3/29/2020 12:16:58 AM

General hide

Details

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:54 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{BD48B592-5837-4D5B-B917-19DA189ED5BF}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Desktops	No	Enabled	bvt.local/Common Criteria TOE Computers/Desktops

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/Add features to Windows 10 hide

Policy	Setting	Comment
Prevent the wizard from running.	Enabled	

Windows Components/App Package Deployment hide

Policy	Setting	Comment
Allow all trusted apps to install	Disabled	
Allow deployment operations in special profiles	Disabled	
Disable installing Windows apps on non-system volumes	Enabled	

Windows Components/Desktop Gadgets hide

Policy	Setting	Comment
Restrict unpacking and installation of gadgets that are not digitally signed.	Enabled	
Turn off desktop gadgets	Enabled	
Turn Off user-installed desktop gadgets	Enabled	

Windows Components/Game Explorer hide

Policy	Setting	Comment
Turn off downloading of game information	Enabled	
Turn off game updates	Enabled	
Turn off tracking of last play time of games in the Games folder	Enabled	

Windows Components/Maps hide

Policy	Setting	Comment
Turn off Automatic Download and Update of Map Data	Enabled	

Windows Components/Portable Operating System hide

Policy	Setting	Comment
Windows To Go Default Startup Options	Disabled	

Windows Components/Sync your settings hide

Policy	Setting	Comment
Do not sync	Enabled	
Allow users to turn syncing on.	Disabled	

Policy	Setting	Comment
Do not sync app settings	Enabled	
Allow users to turn "app settings" syncing on.	Disabled	

Policy	Setting	Comment
Do not sync Apps	Enabled	
Allow users to turn "AppSync" syncing on.	Disabled	

Policy	Setting	Comment
Do not sync browser settings	Enabled	
Allow users to turn "browser" syncing on.	Disabled	

Policy	Setting	Comment
Do not sync desktop personalization	Enabled	
Allow users to turn "desktop personalization" syncing on.	Disabled	

Policy	Setting	Comment
Do not sync on metered connections	Enabled	
Do not sync other Windows settings	Enabled	
Allow users to turn "other Windows settings" syncing on.	Disabled	

Policy	Setting	Comment
Do not sync passwords	Enabled	
Allow users to turn "passwords" syncing on.	Disabled	

Policy	Setting	Comment
Do not sync personalize	Enabled	
Allow users to turn "personalize" syncing on.	Disabled	

Policy	Setting	Comment
Do not sync start settings	Enabled	
Allow users to turn "start layout" syncing on.	Disabled	

Windows Components/Windows Color System hide

Policy	Setting	Comment
Prohibit installing or uninstalling color profiles	Enabled	

Windows Components/Windows Installer hide

Policy	Setting	Comment
Allow user control over installs	Disabled	
Allow users to browse for source while elevated	Disabled	
Allow users to patch elevated products	Disabled	
Allow users to use media source while elevated	Disabled	
Prevent Internet Explorer security prompt for Windows Installer scripts	Disabled	
Prevent users from using Windows Installer to install updates and upgrades	Enabled	
Prohibit non-administrators from applying vendor signed updates	Enabled	
Prohibit removal of updates	Enabled	
Prohibit User Installs	Enabled	

User Install Behavior:	Hide User Installs

Policy	Setting	Comment
Remove browse dialog box for new source	Enabled	
Turn off Windows Installer	Enabled	

Disable Windows Installer	Always

Windows Components/Windows Update hide

Policy	Setting	Comment
Allow non-administrators to receive update notifications	Disabled	
Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box	Enabled	
Turn on Software Notifications	Disabled	

Extra Registry Settings hide

Display names for some settings cannot be found. You might be able to resolve this issue by updating the .ADM files used by Group Policy Management.

Setting	State
Software\Policies\Microsoft\Windows\DeliveryOptimization\DODownloadMode	100

User Configuration (Enabled) hide

No settings defined.

XD2017 CC - Computer - Microsoft Win10 Security Compliance Fixes

Data collected on: 3/29/2020 12:16:58 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:52 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{BE187538-E28C-4672-96CE-E93514790BA5}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
VDA	No	Enabled	bvt.local/Common Criteria TOE Computers/Desktops/VDA

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Local Policies/User Rights Assignment

hide

Policy	Setting
Access this computer from the network	BUILTIN\Administrators, BUILTIN\Backup Operators, Everyone, BUILTIN\Users

Administrative Templates

hide

Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Security

hide

Policy	Setting	Comment
Always prompt for password upon connection	Disabled	

User Configuration (Enabled)

hide

No settings defined.

XD2017 CC - Computer - Server VDA AppLocker

Data collected on: 3/29/2020 12:16:59 AM

General

hide

Details

hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:48 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{BEF0B8A2-82C3-40D8-9129-33CF2B390F14}
GPO Status	Enabled

Links

hide

Location	Enforced	Link Status	Path
Server VDA	No	Enabled	bvt.local/Common Criteria TOE Computers/Desktops/VDA/Server VDA

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

System Services

hide

Application Identity (Startup Mode: Automatic)

hide

Permissions
No permissions specified

Auditing
No auditing specified

Application Control Policies

hide

Appx Rules

Policy	Setting
Enforce rules of this type	True

Action	User	Name	Rule Type	Exceptions
Allow	BUILTIN\Administrators	Packaged app: Microsoft.LockApp signed by Microsoft Corporation	Publisher	No
Allow	BUILTIN\Administrators	Packaged app: Microsoft.Windows.AssignedAccessLockApp signed by Microsoft Corporation	Publisher	No
Allow	BUILTIN\Administrators	Packaged app: Microsoft.Windows.Cortana signed by Microsoft Corporation	Publisher	No
Allow	BUILTIN\Administrators	Packaged app: Microsoft.Windows.SecondaryTileExperience signed by Microsoft Corporation	Publisher	No
Allow	BUILTIN\Administrators	Packaged app: Microsoft.AccountsControl signed by Microsoft Corporation	Publisher	No
Allow	BUILTIN\Administrators	Packaged app: Microsoft.XboxGameCallableUI signed by Microsoft Corporation	Publisher	No
Allow	BUILTIN\Administrators	Packaged app: Microsoft.Windows.Apprep.ChxApp signed by Microsoft Corporation	Publisher	No
Allow	BUILTIN\Administrators	Packaged app: Microsoft.Windows.ShellExperienceHost signed by Microsoft Corporation	Publisher	No
Allow	BUILTIN\Administrators	Packaged app: Windows.PrintDialog signed by Microsoft Corporation	Publisher	No
Allow	BUILTIN\Administrators	Packaged app: Microsoft.Windows.CloudExperienceHost signed by Outlook.com, Hotmail, Live.com, MSN	Publisher	No
Allow	BUILTIN\Administrators	Packaged app: Microsoft.AAD.BrokerPlugin signed by Assigned by your organization	Publisher	No
Allow	BUILTIN\Administrators	Packaged app: Windows.MiracastView signed by Microsoft Corporation	Publisher	No
Allow	BUILTIN\Administrators	Packaged app: Microsoft.BioEnrollment signed by Microsoft Corporation	Publisher	No
Allow	BUILTIN\Administrators	Packaged app: windows.immersivecontrolpanel signed by Microsoft Corporation	Publisher	No

Dll Rules hide

No rules of type 'Dll Rules' are defined.

Executable Rules hide

Policy	Setting
Enforce rules of this type	True

Action	User	Name	Rule Type	Exceptions
Allow	Everyone	%PROGRAMFILES%\CITRIX\SYSTEM32\WFSHELL.EXE	Path	No
Allow	Everyone	%SYSTEM32%\NOTEPAD.EXE	Path	No
Allow	Everyone	%SYSTEM32%\TASKHOST.EXE	Path	No

Allow	Everyone	%PROGRAMFILES%\Jonas\JonasAgentSystray.exe	Path	No
Allow	Everyone	%SYSTEM32%\CALC.EXE	Path	No
Allow	Everyone	%SYSTEM32%\TASKHOSTW.EXE	Path	No
Allow	Everyone	%SYSTEM32%\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE	Path	No
Allow	Everyone	%SYSTEM32%\SLUI.EXE	Path	No
Allow	Everyone	%PROGRAMFILES%\CITRIX\SYSTEM32\ICAST.EXE	Path	No
Allow	Everyone	%PROGRAMFILES%\CITRIX\SYSTEM32\CTXMTHOST.EXE	Path	No
Allow	Everyone	%SYSTEM32%\DWM.EXE	Path	No
Allow	Everyone	%SYSTEM32%\CONHOST.EXE	Path	No
Allow	Everyone	%SYSTEM32%\USERINIT.EXE	Path	No
Allow	Everyone	%SYSTEM32%\WIN32CALC.EXE	Path	No
Allow	Everyone	%SYSTEM32%\SVCHOST.EXE	Path	No
Allow	Everyone	%SYSTEM32%\TSTHEME.EXE	Path	No
Allow	BUILTIN\Administrators	*	Path	No
Allow	Everyone	%SYSTEM32%\SIHOST.EXE	Path	No
Allow	Everyone	%SYSTEM32%\GPSCRIPT.EXE	Path	No
Allow	Everyone	%PROGRAMFILES%\CITRIX\VIRTUAL SMART CARD\CITRIX.AUTHENTICATION.VIRTUALSMARTCARD.LAUNCHER.EXE	Path	No
Allow	Everyone	%PROGRAMFILES%\CITRIX\SYSTEM32\MULTIMEDIAREDIRECTOR.EXE	Path	No
Allow	Everyone	%SYSTEM32%\RUNTIMEBROKER.EXE	Path	No
Allow	Everyone	%SYSTEM32%\TASKHOSTEX.EXE	Path	No
Allow	Everyone	%PROGRAMFILES%\CITRIX\SYSTEM32\CMSTART.EXE	Path	No
Allow	Everyone	%WINDIR%\APPLICATION COMPATIBILITY SCRIPTS\ACREGL.EXE	Path	No

Windows Installer Rules hide

No rules of type 'Windows Installer Rules' are defined.

Script Rules hide

No rules of type 'Script Rules' are defined.

User Configuration (Enabled) hide

No settings defined.

XD2017 CC - Computer - Disable Print Screen

Data collected on: 3/29/2020 12:16:59 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:54 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{C012C679-0910-4830-AF79-9196B3BEBD46}

GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
User Devices	No	Enabled	bvt.local/Common Criteria TOE Computers/Desktops/User Devices

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Application Control Policies hide

Appx Rules hide

Action	User	Name	Rule Type	Exceptions
Allow	Everyone	(Default Rule) All signed packaged apps	Publisher	No

Dll Rules hide

No rules of type 'Dll Rules' are defined.

Executable Rules hide

Action	User	Name	Rule Type	Exceptions
Allow	Everyone	(Default Rule) All files located in the Program Files folder	Path	No
Allow	Everyone	(Default Rule) All files located in the Windows folder	Path	No
Allow	BUILTIN\Administrators	(Default Rule) All files	Path	No

Windows Installer Rules hide

No rules of type 'Windows Installer Rules' are defined.

Script Rules hide

No rules of type 'Script Rules' are defined.

Preferences hide

Windows Settings hide

Registry hide

Scancode Map (Order: 1) hide

General hide

Action	Update

Properties

Hive	HKEY_LOCAL_MACHINE
Key path	SYSTEM\CurrentControlSet\Control\Keyboard Layout
Value name	Scancode Map

Value type	REG_BINARY
Value data	00000000000000000040000002ae037e0000037e00000540000000000

Common hide

Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

User Configuration (Enabled) hide

No settings defined.

Win10-1607 Domain Security Compliance

Data collected on: 3/29/2020 12:16:59 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:02:00 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{CADC31A5-CE53-439D-9352-0F1080C49AE3}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
bvt	No	Enabled	bvt.local

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Account Policies/Password Policy hide

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy hide

Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes

User Configuration (Enabled) hide

No settings defined.

XD7 CC - Computer - HDX Single Sign-On Enabled

Data collected on: 3/29/2020 12:16:59 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:42 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	2 (AD), 2 (SYSVOL)
Unique ID	{CC481574-A62A-4B9E-98AC-5AA0493C55D1}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Desktops	No	Enabled	bvt.local/Common Criteria TOE Computers/Desktops

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local computer.

Citrix Components/Citrix Receiver/Storefront hide

Policy	Setting	Comment
Storefront Accounts List	Enabled	

Enter the Storefront account details here:

Store;https://VWFTY-SF-1.bvt.local/Citrix/Store/Discovery;on;Store

Citrix Components/Citrix Receiver/User authentication hide

Policy	Setting	Comment
Local user name and password	Enabled	

Enable pass-through authentication	Enabled
Allow pass-through authentication for all ICA connections	Enabled
Use Novell Directory Server credentials	Disabled

Policy	Setting	Comment
Smart card authentication	Enabled	

Allow smart card authentication	
Use pass-through authentication for PIN	Enabled

Extra Registry Settings hide

Display names for some settings cannot be found. You might be able to resolve this issue by updating the .ADM files used by Group Policy Management.

Setting	State
Software\Policies\Citrix\ICA Client\AutoUpdate\Banned	True
Software\Policies\Citrix\ICA Client\AutoUpdate\LTSROnly	False
Software\Policies\Citrix\ICA Client\CEIP\Enable_CEIP	0

Preferences hide

Windows Settings hide

Registry hide

WSCSupported (Order: 1) hide

General hide

Action	Update

Properties

Hive	HKEY_LOCAL_MACHINE
Key path	SOFTWARE\Wow6432Node\Citrix\Dazzle
Value name	WSCSupported
Value type	REG_SZ
Value data	false

Common hide

Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

User Configuration (Enabled) hide

No settings defined.

Win10-1607 Computer Security Compliance

Data collected on: 3/29/2020 12:17:00 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:38 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{DC5000EF-D65E-476A-934B-774AAEF673B7}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Desktops	No	Enabled	bvt.local/Common Criteria TOE Computers/Desktops

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Local Policies/User Rights Assignment hide

Policy	Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	BUILTIN\Administrators, BUILTIN\Remote Desktop Users
Act as part of the operating system	
Allow log on locally	BUILTIN\Administrators, BUILTIN\Users
Back up files and directories	BUILTIN\Administrators
Create a pagefile	BUILTIN\Administrators
Create a token object	
Create global objects	BUILTIN\Administrators, NT AUTHORITY\SERVICE, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE
Create permanent shared objects	
Create symbolic links	BUILTIN\Administrators
Debug programs	BUILTIN\Administrators
Deny access to this computer from the network	NT AUTHORITY\Local account, BUILTIN\Guests
Deny log on locally	BUILTIN\Guests
Deny log on through Terminal Services	NT AUTHORITY\Local account, BUILTIN\Guests
Enable computer and user accounts to be trusted for delegation	
Force shutdown from a remote system	BUILTIN\Administrators
Generate security audits	NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE
Impersonate a client after authentication	BUILTIN\Administrators, NT AUTHORITY\SERVICE, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE
Increase scheduling priority	BUILTIN\Administrators
Load and unload device drivers	BUILTIN\Administrators
Lock pages in memory	
Manage auditing and security log	BUILTIN\Administrators
Modify firmware environment values	BUILTIN\Administrators
Perform volume maintenance tasks	BUILTIN\Administrators
Profile single process	BUILTIN\Administrators
Restore files and directories	BUILTIN\Administrators
Take ownership of files or other objects	BUILTIN\Administrators

Local Policies/Security Options hide

Accounts hide

Policy	Setting
Accounts: Administrator account status	Disabled
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled

Interactive Logon hide

Policy	Setting
Interactive logon: Smart card removal behavior	Lock Workstation

Microsoft Network Client hide

Policy	Setting
Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled

Network Access hide

Policy	Setting
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
Network access: Do not allow storage of passwords and credentials for network authentication	Enabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled

Network Security hide

Policy	Setting
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Enabled
Network security: LAN Manager authentication level	Send NTLMv2 response only. Refuse LM & NTLM
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Enabled
Require NTLMv2 session security	Enabled
Require 128-bit encryption	Enabled
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Enabled
Require NTLMv2 session security	Enabled
Require 128-bit encryption	Enabled

System Objects hide

Policy	Setting
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled

User Account Control hide

Policy	Setting
User Account Control: Admin Approval Mode for the Built-in Administrator account	Enabled
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent on the secure desktop
User Account Control: Behavior of the elevation prompt for standard users	Automatically deny elevation requests
User Account Control: Detect application installations and prompt for elevation	Enabled
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled
User Account Control: Run all administrators in Admin Approval Mode	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled

Other hide

Policy	Setting
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled
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
Domain member: Require strong (Windows 2000 or later) session key	Enabled
Interactive logon: Machine inactivity limit	900 seconds
Microsoft network server: Amount of idle time required before suspending session	15 minutes

Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled
Network security: Allow Local System to use computer identity for NTLM	Enabled
Network security: Allow LocalSystem NULL session fallback	Disabled
Network security: Allow PKU2U authentication requests to this computer to use online identities.	Disabled

Windows Firewall with Advanced Security hide

Global Settings hide

Policy	Setting
Policy version	Not Configured
Disable stateful FTP	Not Configured
Disable stateful PPTP	Not Configured
IPsec exempt	Not Configured
IPsec through NAT	Not Configured
Preshared key encoding	Not Configured
SA idle time	Not Configured
Strong CRL check	Not Configured

Domain Profile Settings hide

Policy	Setting
Firewall state	On
Inbound connections	Block
Outbound connections	Allow
Apply local firewall rules	Not Configured
Apply local connection security rules	Not Configured
Display notifications	No
Allow unicast responses	Not Configured
Log dropped packets	Yes
Log successful connections	Yes
Log file path	Not Configured
Log file maximum size (KB)	16384

Private Profile Settings hide

Policy	Setting
Firewall state	On
Inbound connections	Block
Outbound connections	Allow
Apply local firewall rules	Not Configured
Apply local connection security rules	Not Configured
Display notifications	No
Allow unicast responses	Not Configured
Log dropped packets	Yes
Log successful connections	Yes
Log file path	Not Configured
Log file maximum size (KB)	16384

Public Profile Settings hide

Policy	Setting
Firewall state	On
Inbound connections	Block
Outbound connections	Allow
Apply local firewall rules	No
Apply local connection security rules	No
Display notifications	No
Allow unicast responses	Not Configured
Log dropped packets	Yes
Log successful connections	Yes
Log file path	Not Configured
Log file maximum size (KB)	16384

Connection Security Settings hide

Advanced Audit Configuration

hide

Account Logon

hide

Policy	Setting
Audit Credential Validation	Success, Failure

Account Management

hide

Policy	Setting
Audit Other Account Management Events	Success, Failure
Audit Security Group Management	Success, Failure
Audit User Account Management	Success, Failure

Detailed Tracking

hide

Policy	Setting
Audit PNP Activity	Success
Audit Process Creation	Success

Logon/Logoff

hide

Policy	Setting
Audit Account Lockout	Success, Failure
Audit Group Membership	Success
Audit Logoff	Success
Audit Logon	Success, Failure
Audit Special Logon	Success

Object Access

hide

Policy	Setting
Audit Removable Storage	Success, Failure

Policy Change

hide

Policy	Setting
Audit Audit Policy Change	Success, Failure
Audit Authentication Policy Change	Success
Audit Authorization Policy Change	Success

Privilege Use

hide

Policy	Setting
Audit Sensitive Privilege Use	Success, Failure

System

hide

Policy	Setting
Audit IPsec Driver	Success, Failure
Audit Other System Events	Success, Failure
Audit Security State Change	Success
Audit Security System Extension	Success, Failure
Audit System Integrity	Success, Failure

Administrative Templates

hide

Policy definitions (ADMX files) retrieved from the local computer.

Control Panel/Personalization

hide

Policy	Setting	Comment
Prevent enabling lock screen camera	Enabled	
Prevent enabling lock screen slide show	Enabled	

Network/Lanman Workstation

hide

Policy	Setting	Comment
Enable insecure guest logons	Disabled	

Network/Network Connections

hide

Policy	Setting	Comment

Prohibit use of Internet Connection Sharing on your DNS domain network	Enabled

Network/Network Connections/Windows Firewall/Domain Profile hide

Policy	Setting	Comment
Windows Firewall: Allow logging	Enabled	

Log dropped packets	Enabled
Log successful connections	Enabled
Log file path and name:	
Size limit (KB):	16384

Policy	Setting	Comment
Windows Firewall: Prohibit notifications	Enabled	
Windows Firewall: Protect all network connections	Enabled	

Network/Network Provider hide

Policy	Setting	Comment
Hardened UNC Paths	Enabled	

Specify hardened network paths. In the name field, type a fully-qualified UNC path for each network resource. To secure all access to a share with a particular name, regardless of the server name, specify a server name of '*' (asterisk). For example, "*\NETLOGON". To secure all access to all shares hosted on a server, the share name portion of the UNC path may be omitted. For example, "\\SERVER". In the value field, specify one or more of the following options, separated by commas: 'RequireMutualAuthentication=1': Mutual authentication between the client and server is required to ensure the client connects to the correct server. 'RequireIntegrity=1': Communication between the client and server must employ an integrity mechanism to prevent data tampering. 'RequirePrivacy=1': Communication between the client and the server must be encrypted to prevent third parties from observing sensitive data.

Hardened UNC Paths:	
*\SYSVOL	RequireMutualAuthentication=1, RequireIntegrity=1
*\NETLOGON	RequireMutualAuthentication=1, RequireIntegrity=1

You should require both Integrity and Mutual Authentication for any UNC paths that host executable programs, script files, or files that control security policies. Consider hosting files that do not require Integrity or Privacy on separate shares from those that absolutely need such security for optimal performance. For additional details on configuring Windows computers to require additional security when accessing specific UNC paths, visit http://support.microsoft.com/kb/3000483.

Network/Windows Connection Manager hide

Policy	Setting	Comment
Prohibit connection to non-domain networks when connected to domain authenticated network	Enabled	

Network/WLAN Service/WLAN Settings hide

Policy	Setting	Comment
Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services	Disabled	

System/Device Installation/Device Installation Restrictions hide

Policy	Setting	Comment
Prevent installation of devices that match any of these device IDs	Enabled	

Prevent installation of devices that match any of these Device IDs:
PCI\CC_0C0A

To create a list of devices, click Show. In the Show Contents dialog box, in the Value column, type a Plug and Play hardware ID or compatible ID

(for example, gendisk, USB\COMPOSITE, USB\Class_ff).

Also apply to matching devices that are already installed.	Enabled

Policy	Setting	Comment
Prevent installation of devices using drivers that match these device setup classes	Enabled	

Prevent installation of devices using drivers for these device setup classes:
{d48179be-ec20-11d1-b6b8-00c04fa372a7}

To create a list of device classes, click Show. In the Show Contents dialog box, in the Value column, type a GUID that represents a device setup class

(for example, {25DBCE51-6C8F-4A72-8A6D-B54C2B4FC835}).

Also apply to matching devices that are already installed.	Enabled

System/Early Launch Antimalware hide

Policy	Setting	Comment
Boot-Start Driver Initialization Policy	Enabled	
Choose the boot-start drivers that can be initialized:	Good, unknown and bad but critical	

System/Group Policy hide

Policy	Setting	Comment
Configure registry policy processing	Enabled	
Do not apply during periodic background processing	Disabled	
Process even if the Group Policy objects have not changed	Enabled	

System/Internet Communication Management/Internet Communication settings hide

Policy	Setting	Comment
Turn off downloading of print drivers over HTTP	Enabled	
Turn off Internet download for Web publishing and online ordering wizards	Enabled	
Turn off printing over HTTP	Enabled	

System/Logon hide

Policy	Setting	Comment
Do not display network selection UI	Enabled	
Enumerate local users on domain-joined computers	Disabled	
Turn on convenience PIN sign-in	Disabled	

System/Mitigation Options hide

Policy	Setting	Comment
Untrusted Font Blocking	Enabled	
Mitigation Options	Block untrusted fonts and log events	

System/Power Management/Sleep Settings hide

Policy	Setting	Comment
Require a password when a computer wakes (on battery)	Enabled	
Require a password when a computer wakes (plugged in)	Enabled	

System/Remote Assistance hide

Policy	Setting	Comment
Configure Solicited Remote Assistance	Disabled	

System/Remote Procedure Call hide

Policy	Setting	Comment
Restrict Unauthenticated RPC clients	Enabled	
RPC Runtime Unauthenticated Client Restriction to Apply:	Authenticated	

Windows Components/App runtime hide

Policy	Setting	Comment
Allow Microsoft accounts to be optional	Enabled	

Windows Components/AutoPlay Policies hide

Policy	Setting	Comment
Disallow Autoplay for non-volume devices	Enabled	
Set the default behavior for AutoRun	Enabled	
Default AutoRun Behavior	Do not execute any autorun commands	

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

Windows Components/Biometrics/Facial Features hide

Policy	Setting	Comment
Use enhanced anti-spoofing when available	Enabled	

Windows Components/Cloud Content hide

Policy	Setting	Comment
Turn off Microsoft consumer experiences	Enabled	

Windows Components/Credential User Interface hide

Policy	Setting	Comment
Enumerate administrator accounts on elevation	Disabled	

Windows Components/Event Log Service/Application hide

Policy	Setting	Comment
Specify the maximum log file size (KB)	Enabled	
Maximum Log Size (KB)	32768	

Windows Components/Event Log Service/Security hide

Policy	Setting	Comment
Specify the maximum log file size (KB)	Enabled	
Maximum Log Size (KB)	196608	

Windows Components/Event Log Service/System hide

Policy	Setting	Comment
Specify the maximum log file size (KB)	Enabled	
Maximum Log Size (KB)	32768	

Windows Components/File Explorer hide

Policy	Setting	Comment
Configure Windows SmartScreen	Enabled	
Turn off Data Execution Prevention for Explorer	Disabled	
Turn off heap termination on corruption	Disabled	

Windows Components/Remote Desktop Services/Remote Desktop Connection Client hide

Policy	Setting	Comment
Do not allow passwords to be saved	Enabled	

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Device and Resource Redirection hide

Policy	Setting	Comment
Do not allow drive redirection	Enabled	

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Security hide

Policy	Setting	Comment
Always prompt for password upon connection	Enabled	
Require secure RPC communication	Enabled	
Set client connection encryption level	Enabled	
Encryption Level	High Level	
Choose the encryption level from the drop-down list.		

Windows Components/RSS Feeds hide

Policy	Setting	Comment
Prevent downloading of enclosures	Enabled	

Windows Components/Search hide

Policy	Setting	Comment
Allow indexing of encrypted files	Disabled	

Windows Components/Windows Defender hide

Policy	Setting	Comment
Turn off Windows Defender	Enabled	

Windows Components/Windows Defender/MAPS hide

Policy	Setting	Comment
Configure local setting override for reporting to Microsoft MAPS	Disabled	
Join Microsoft MAPS	Enabled	

Join Microsoft MAPS	Advanced MAPS

Policy	Setting	Comment
Send file samples when further analysis is required	Enabled	

Send file samples when further analysis is required

Windows Components/Windows Defender/Real-time Protection hide

Policy	Setting	Comment
Turn on behavior monitoring	Enabled	

Windows Components/Windows Defender/Scan hide

Policy	Setting	Comment
Scan removable drives	Enabled	
Turn on e-mail scanning	Enabled	

Windows Components/Windows Installer hide

Policy	Setting	Comment
Allow user control over installs	Disabled	
Always install with elevated privileges	Disabled	

Windows Components/Windows Logon Options hide

Policy	Setting	Comment
Sign-in last interactive user automatically after a system-initiated restart	Disabled	

Windows Components/Windows PowerShell hide

Policy	Setting	Comment
Turn on PowerShell Script Block Logging	Enabled	

Log script block invocation start / stop events:

Windows Components/Windows Remote Management (WinRM)/WinRM Client hide

Policy	Setting	Comment
Allow Basic authentication	Disabled	
Allow unencrypted traffic	Disabled	
Disallow Digest authentication	Enabled	

Windows Components/Windows Remote Management (WinRM)/WinRM Service hide

Policy	Setting	Comment
Allow Basic authentication	Disabled	
Allow unencrypted traffic	Disabled	
Disallow WinRM from storing RunAs credentials	Enabled	

Extra Registry Settings hide

Display names for some settings cannot be found. You might be able to resolve this issue by updating the .ADM files used by Group Policy Management.

Setting	State
Software\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy	0
Software\Policies\Microsoft Services\AdmPwd\AdmPwdEnabled	1
Software\Policies\Microsoft\MicrosoftEdge\Main\FormSuggest Passwords	no
Software\Policies\Microsoft\MicrosoftEdge\PhishingFilter\EnabledV9	1
Software\Policies\Microsoft\MicrosoftEdge\PhishingFilter\PreventOverride	1
Software\Policies\Microsoft\MicrosoftEdge\PhishingFilter\PreventOverrideAppRepUnknown	1
Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging\EnableScriptBlockInvocationLogging	0

SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential	0
SYSTEM\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand	1
SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting	2
SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect	0
SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\DisableIPSourceRouting	2

User Configuration (Enabled) hide

No settings defined.

XD2017 CC - Computer - App Launch Restrictions

Data collected on: 3/29/2020 12:17:00 AM

General hide

Details hide

Domain	bvt.local
Owner	AU8ZY\Domain Admins
Created	3/19/2020 9:01:56 AM
Modified	3/20/2020 1:44:36 AM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{DD93394E-91AD-4BB1-AE9E-FB111782F3A3}
GPO Status	Enabled

Links hide

Location	Enforced	Link Status	Path
Desktops	No	Enabled	bvt.local/Common Criteria TOE Computers/Desktops

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
AU8ZY\Domain Admins	Edit settings, delete, modify security	No
AU8ZY\Enterprise Admins	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

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/App Privacy hide

Policy	Setting	Comment
Let Windows apps access account information	Enabled	

Default for all apps: Force Deny

Put user in control of these specific apps (use Package Family Names):

Force allow these specific apps (use Package Family Names):

Force deny these specific apps (use Package Family Names):

Policy	Setting	Comment
Let Windows apps access call history	Enabled	

Default for all apps:	Force Deny
Put user in control of these specific apps (use Package Family Names):	
Force allow these specific apps (use Package Family Names):	
Force deny these specific apps (use Package Family Names):	

Policy	Setting	Comment
Let Windows apps access contacts	Enabled	

Default for all apps:	Force Deny
Put user in control of these specific apps (use Package Family Names):	
Force allow these specific apps (use Package Family Names):	
Force deny these specific apps (use Package Family Names):	

Policy	Setting	Comment
Let Windows apps access email	Enabled	

Default for all apps:	Force Deny
Put user in control of these specific apps (use Package Family Names):	
Force allow these specific apps (use Package Family Names):	
Force deny these specific apps (use Package Family Names):	

Policy	Setting	Comment
Let Windows apps access location	Enabled	

Default for all apps:	Force Deny
Put user in control of these specific apps (use Package Family Names):	
Force allow these specific apps (use Package Family Names):	
Force deny these specific apps (use Package Family Names):	

Policy	Setting	Comment
Let Windows apps access messaging	Enabled	

Default for all apps:	Force Deny
Put user in control of these specific apps (use Package Family Names):	
Force allow these specific apps (use Package Family Names):	
Force deny these specific apps (use Package Family Names):	

Policy	Setting	Comment
Let Windows apps access motion	Enabled	

Default for all apps:	Force Deny
Put user in control of these specific apps (use Package Family Names):	
Force allow these specific apps (use Package Family Names):	
Force deny these specific apps (use Package Family Names):	

Policy	Setting	Comment
Let Windows apps access notifications	Enabled	

Default for all apps:	Force Deny
Put user in control of these specific apps (use Package Family Names):	
Force allow these specific apps (use Package Family Names):	
Force deny these specific apps (use Package Family Names):	

Policy	Setting	Comment
Let Windows apps access the calendar	Enabled	

Default for all apps:	Force Deny
Put user in control of these specific apps (use Package Family Names):	
Force allow these specific apps (use Package Family Names):	
Force deny these specific apps (use Package Family Names):	

Policy	Setting	Comment
Let Windows apps access the camera	Enabled	

Default for all apps:	Force Deny
Put user in control of these specific apps (use Package Family Names):	
Force allow these specific apps (use Package Family Names):	
Force deny these specific apps (use Package Family Names):	

Policy	Setting	Comment
Let Windows apps access the microphone	Enabled	

Default for all apps:	Force Deny
Put user in control of these specific apps (use Package Family Names):	
Force allow these specific apps (use Package Family Names):	
Force deny these specific apps (use Package Family Names):	

Policy	Setting	Comment
Let Windows apps access trusted devices	Enabled	

Default for all apps:	Force Deny
Put user in control of these specific apps (use Package Family Names):	
Force allow these specific apps (use Package Family Names):	
Force deny these specific apps (use Package Family Names):	

Policy	Setting	Comment
Let Windows apps control radios	Enabled	

Default for all apps:	Force Deny
Put user in control of these specific apps (use Package Family Names):	
Force allow these specific apps (use Package Family Names):	
Force deny these specific apps (use Package Family Names):	

Policy	Setting	Comment
Let Windows apps make phone calls	Enabled	

Default for all apps:	Force Deny
Put user in control of these specific apps (use Package Family Names):	
Force allow these specific apps (use Package Family Names):	
Force deny these specific apps (use Package Family Names):	

Policy	Setting	Comment
Let Windows apps sync with devices	Enabled	

Default for all apps:	Force Deny
Put user in control of these specific apps (use Package Family Names):	
Force allow these specific apps (use Package Family Names):	
Force deny these specific apps (use Package Family Names):	

Windows Components/App runtime hide

Policy	Setting	Comment
Block launching desktop apps associated with a file.	Enabled	
Block launching desktop apps associated with a URI scheme	Enabled	
Block launching Windows Store apps with Windows Runtime API access from hosted content.	Enabled	

Windows Components/Application Compatibility hide

Policy	Setting	Comment
Prevent access to 16-bit applications	Enabled	
Remove Program Compatibility Property Page	Enabled	
Turn off Program Compatibility Assistant	Enabled	

Windows Components/Cloud Content hide

Policy	Setting	Comment
Do not show Windows tips	Enabled	

Turn off Microsoft consumer experiences	Enabled

Windows Components/Digital Locker hide

Policy	Setting	Comment
Do not allow Digital Locker to run	Enabled	

Windows Components/NetMeeting hide

Policy	Setting	Comment
Disable remote Desktop Sharing	Enabled	

Windows Components/OneDrive hide

Policy	Setting	Comment
Prevent the usage of OneDrive for file storage	Enabled	
Prevent the usage of OneDrive for file storage on Windows 8.1	Enabled	

Windows Components/Sound Recorder hide

Policy	Setting	Comment
Do not allow Sound Recorder to run	Enabled	

Windows Components/Store hide

Policy	Setting	Comment
Disable all apps from Windows Store	Enabled	
Turn off Automatic Download and Install of updates	Enabled	
Turn off the offer to update to the latest version of Windows	Enabled	
Turn off the Store application	Enabled	

Windows Components/Windows Calendar hide

Policy	Setting	Comment
Turn off Windows Calendar	Enabled	

Windows Components/Windows Defender/Client Interface hide

Policy	Setting	Comment
Enable headless UI mode	Enabled	
Suppress all notifications	Enabled	

Windows Components/Windows Defender/MAPS hide

Policy	Setting	Comment
Join Microsoft MAPS	Disabled	
Send file samples when further analysis is required	Enabled	
Send file samples when further analysis is required	Never send	

Windows Components/Windows Mail hide

Policy	Setting	Comment
Turn off Windows Mail application	Enabled	

Windows Components/Windows Media Digital Rights Management hide

Policy	Setting	Comment
Prevent Windows Media DRM Internet Access	Enabled	

Windows Components/Windows Media Player hide

Policy	Setting	Comment
Do Not Show First Use Dialog Boxes	Enabled	
Prevent Automatic Updates	Enabled	
Prevent Desktop Shortcut Creation	Enabled	
Prevent Media Sharing	Enabled	
Prevent Quick Launch Toolbar Shortcut Creation	Enabled	

Windows Components/Windows Messenger hide

Policy	Setting	Comment

Do not allow Windows Messenger to be run	Enabled
Do not automatically start Windows Messenger initially	Enabled

Windows Components/Windows Mobility Center hide

Policy	Setting	Comment
Turn off Windows Mobility Center	Enabled	

Extra Registry Settings hide

Display names for some settings cannot be found. You might be able to resolve this issue by updating the .ADM files used by Group Policy Management.

Setting	State
Software\Policies\Microsoft\Windows\Backup\Client\DisableBackupLauncher	1
Software\Policies\Microsoft\Windows\Backup\Client\DisableBackupToDisk	1
Software\Policies\Microsoft\Windows\Backup\Client\DisableBackupToNetwork	1
Software\Policies\Microsoft\Windows\Backup\Client\DisableBackupToOptical	1
Software\Policies\Microsoft\Windows\Backup\Client\DisableBackupUI	1
Software\Policies\Microsoft\Windows\Backup\Client\DisableRestoreUI	1
Software\Policies\Microsoft\Windows\Backup\Client\DisableSystemBackupUI	1
Software\Policies\Microsoft\Windows\SideShow\Disabled	1
Software\Policies\Microsoft\WindowsMediaCenter\MediaCenter	1
Software\Policies\Microsoft\WindowsStore\EnableWindowsStoreOnWTG	0
Software\Policies\Microsoft\WindowsStore\WindowsUpdate\AutoDownload	2

Preferences hide

Windows Settings hide

Registry hide

AllowgameDVR (Order: 1) hide

General hide

Action	Update

Properties

Hive	HKEY_LOCAL_MACHINE
Key path	SOFTWARE\Policies\Microsoft\Windows\GameDVR
Value name	AllowgameDVR
Value type	REG_DWORD
Value data	0x0 (0)

Common hide

Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

User Configuration (Enabled) hide

No settings defined.