



**BOSCH**

# **BVMS Operating System Hardening Tool**

**en**

User Guide



## Table of contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
<b>2</b>	<b>System requirements and restrictions</b>	<b>5</b>
<b>3</b>	<b>Operating System Settings</b>	<b>6</b>
3.1	Activate User Account Control on the server	6
3.2	Deactivate AutoPlay	6
3.3	External Devices	6
3.4	Configuration of user rights assignment	7
3.5	Screen saver	8
3.6	Activate password policy settings	8
3.7	Disable non-essential Windows Services	8
3.8	Windows Operating System user accounts	9
<b>4</b>	<b>Installing the BVMS Operating System Hardening Tool</b>	<b>10</b>
4.1	Attended installation	10
4.2	Unattended installation	10

# 1 Introduction

All BVMS server components, such as the BVMS Management Server and the Video Recording Manager server as well as the workstations used for BVMS Client applications, have to be hardened to protect the video data, the documents and other applications against unauthorized access.

The BVMS Operating System Hardening Tool assists you in hardening Windows servers and workstations by automatically configuring the recommended Local Group Policy Settings in your Windows Operating System.

You can run the BVMS Operating System Hardening Tool either as an executable file or as a PowerShell script. For both, the executable file and the PowerShell script, you can automate the installation process by running the installation in unattended mode.

We recommend running the BVMS Operating System Hardening Tool as an executable file. The PowerShell script is only recommended for experienced users and system administrators. To run the BVMS Operating System Hardening Tool as a PowerShell script, copy the text from the delivered text file, modify the settings according to your needs and execute the script. To start the PowerShell script in unattended mode, an additional parameter is necessary which you can find in the PowerShell script itself.

**Notice!**

Do not use the PowerShell script unless you understand the system settings involved and the consequences of modifying them.

## 2

## System requirements and restrictions

The BVMS Operating System Hardening Tool can only be executed on following Operating Systems:

- Windows 8.1
- Windows 10
- Windows 2012 Server R2
- Windows Server 2016

The BVMS Operating System Hardening Tool detects automatically if it is running on a Windows workstation or on a Windows server, and configures the appropriate settings.

The BVMS Operating System Hardening Tool cannot be executed:

- on a domain controller
- or
- on a computer which is a member of a domain.

The BVMS Operating System Hardening Tool checks the Firewall settings of your computer and shows a message if any Firewall settings are switched off. The Tool itself does not change any Firewall settings.

After execution the BVMS Operating System Hardening Tool saves a log file under:

C:\ProgramData\Bosch\VMS\Log\BVMSOSHARDENINGTool.

In the log file you can find all Local Group Policy Settings which have been changed and all modified values before and after modification.



### Notice!

Note that some changes made by the BVMS Operating System Hardening Tool are not easily reversible, and may adversely affect applications other than BVMS.

## 3 Operating System Settings

By executing the BVMS Operating System Hardening Tool it will change following settings on your Windows Operating System.

### 3.1 Activate User Account Control on the server

**Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options**

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
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials on the secure desktop
User Account Control: Detect application installations and prompt for elevation	Enabled
User Account Control: Only elevate executables that are signed and validated	Disabled
User Account Control: Run all administrators in Admin Approval Mode	Enabled
User Account Control: Switch to the secure desktop when prompting for elevation	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled

**Local Computer Policies -> Computer Configuration -> Administrative Templates -> Windows Components -> Credential User Interface**

Enumerate administrator accounts on elevation	Disabled
---	----------

### 3.2 Deactivate AutoPlay

**Local Computer Policies -> Computer Configuration -> Administrative Templates -> Windows Components -> AutoPlay Policies**

Turn off AutoPlay	Enabled all drives
Default behavior for AutoRun	Enabled, do not execute any AutoRun commands
Turn off AutoPlay for non-volume devices	Enabled

### 3.3 External Devices

**Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options**

Devices: Allow undock without having to log on	Disabled
Devices: Allowed to format and eject removable media	Administrators
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled
Devices: Restrict floppy access to locally logged-on user only	Enabled

### 3.4

## Configuration of user rights assignment

**Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment**

Access Credential Manager as a trusted caller	No one
Access this computer from the network	Authenticated users
Act as part of the operating system	No one
Add workstations to domain	No one
Allow log on through Remote Desktop Services	Administrators, Remote Desktop Users
Change the system time	Administrators
Change the time zone	Administrators, Local Service
Create a page file	Administrators
Create a token object	No one
Create permanent shared objects	No one
Deny access to this computer from the network	Anonymous Logon, Guest group
Deny log on as a batch job	Anonymous Logon, Guest group
Deny log on as a service	No one
Deny log on locally	Anonymous Logon, Guest group
Deny log on through Remote Desktop Services	Anonymous Logon, Guest
Enable computer and user accounts to be trusted for delegation	No one
Force shutdown from a remote system	Administrators
Generate security audits	Local Service, Network Service
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Modify an object label	No one

Modify firmware environment values	Administrators
Perform volume maintenance tasks	Administrators
Profile single process	Administrators
Remove computer from docking station	Administrators
Restore files and directories	Administrators
Shut down the system	Administrators
Synchronize directory service data	No one
Take ownership of files or other objects	Administrators

### 3.5 Screen saver

- Activate password protected screen saver and define timeout time:  
**Local Computer Policies -> User Configuration -> Administrative Templates -> Control Panel -> Personalization**

Enable Screen saver	Enabled
Password protect the screen saver	Enabled
Screen saver timeout	1800 second

### 3.6 Activate password policy settings

- Enabling password policy settings ensures users passwords meet minimum password requirements  
**Local Computer Policies -> Windows Settings -> Security Settings -> Account Policies -> Password Policy**

Enforce password history	10 passwords remembered
Maximum Password Age	90 days
Minimum Password Age	1 day
Minimum Password Length	10 characters
Password must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled

### 3.7 Disable non-essential Windows Services

- Disabling non-essential Windows Services enables a higher security level and minimizes points of attacks.

Application Layer Gateway Service	Disabled
Application Management	Disabled
Computer Browser	Disabled
Distributed Link Tracking Client	Disabled

Function Discovery Provider Host	Disabled
Function Discovery Resource Publication	Disabled
Human Interface Device Access	Disabled
Internet Connection Sharing (ICS)	Disabled
Link-Layer Topology Discovery Mapper	Disabled
Multimedia Class Scheduler	Disabled
Offline Files	Disabled
Remote Access Auto Connection Manager	Disabled
Remote Access Connection Manager	Disabled
Routing and Remote Access	Disabled
Shell Hardware Detection	Disabled
Special Administration Console Helper	Disabled
SSDP Discovery	Disabled

### 3.8

## Windows Operating System user accounts

The Windows Operating System user accounts have to be protected with complex passwords. Servers are normally managed and maintained with Windows administrator accounts, ensure that strong passwords are used for the administrator accounts.

Passwords must contain characters from three of the following categories:

- Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
- Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
- Base 10 digits (0 through 9)
- Non-alphanumeric characters: ~!@#\$%^&\* \_+=` \(){}[];:"'<>.,?/
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

Use of Windows Account Lockout to make it harder for password-guessing attacks to succeed. Windows 8.1 Security Baselines recommendation is 10/15/15:

- 10 bad attempts
- 15 minute lockout duration
- Counter reset after 15 minutes

**Local Computer Policies -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy**

Account lockout duration	Account lockout duration
15 minutes Account lockout threshold 10 failed logon attempts	15 minutes Account lockout threshold 10 failed logon attempts
Reset account lockout counter after	Reset account lockout counter after

- Ensure that all default password of the server and the Windows Operating system are replaced with new strong passwords.

## 4 Installing the BVMS Operating System Hardening Tool

You can install the BVMS Operating System Hardening Tool in attended mode or in unattended mode.

**Notice!**

Before installing the BVMS Operating System Hardening Tool make sure that .NET Framework 4 is installed on your computer.

**Notice!**

Before installing the BVMS Operating System Hardening Tool close all running applications.

### 4.1 Attended installation

**To perform an attended installation:**

1. Start the BVMS Operating System Hardening Tool executable file.  
The Welcome screen is displayed.
2. Accept the Disclaimer and click **Continue**.
3. In the next dialog box click **Apply changes**.  
The BVMS Operating System Hardening Tool starts changing your system settings.
4. After the BVMS Operating System Hardening Tool has finished, click **OK** and restart your computer to activate the changes.

**Note:** If some settings cannot be changed a message is displayed.

### 4.2 Unattended installation

**Notice!**

Before starting the unattended installation, read the end user license agreement (EULA), which is delivered with the BVMS Operating System Hardening Tool.  
Note that starting the installation implies that you have read and accepted the Disclaimer.

**To perform an unattended installation:**

1. Start the Command Prompt (cmd) as Administrator.
2. Change to the directory, where the BVMS Operating System Hardening Tool is stored.
3. Enter the following command:

```
cmd /c BvmsOsHardeningTool.exe -RunUnattendedAndAcceptDisclaimer
```

**Note:** If you use an automation script, enter this command in your script.

This command is necessary to retrieve the error code.

The error code shows if errors occur during the installation:

Error code	Description
0	No errors occur.
100	Computer is a domain controller.
200	Computer is member of a domain.
300	Operating system is not supported.
Any other number	Number of errors occurring during installation.

You can find a detailed description of the errors in the log file.

**Note:** The use of any commands such as `-help` is not taken into consideration.

- After the installation is complete, restart your computer to activate the changes.

**Note:** When you perform the installation in unattended mode, the restart is not done automatically. You have to restart your computer manually.







**Bosch Sicherheitssysteme GmbH**

Robert-Bosch-Ring 5

85630 Grasbrunn

Germany

**[www.boschsecurity.com](http://www.boschsecurity.com)**

© Bosch Sicherheitssysteme GmbH, 2019