

Cybersecurity Guidebook

for BIS and Access Control Systems

Table of contents

1	Introduction	5
1.1	Purpose and audience	5
2	System overview	6
2.1	Background: What is BIS?	6
2.2	BIS overview	6
2.3	Background: What is AMS?	7
2.4	AMS overview	7
2.5	Achieving EN 60839	9
2.5.1	BISACE compliance with EN 60839 standards	9
2.5.2	AMS compliance with EN 60839 standard	10
3	Secure delivery and installation	12
4	Secure configuration	13
4.1	Windows firewall exceptions for Bosch Access Control Systems	13
4.2	Network ports and firewall on BIS server	14
4.2.1	DCOM settings for all BIS Products	14
4.2.2	Setting up Windows firewall	14
4.2.3	Windows firewall: port usage of BIS client	15
4.2.4	Windows firewall: additional settings of Automation and Security Engine	15
4.2.5	Windows firewall: additional settings of Video Engine	15
4.2.6	Windows firewall: additional settings for Access Engine	17
4.2.7	Windows firewall: port usage by SQL server	20
4.2.8	Windows firewall: additional settings for multi server BIS	21
4.2.9	Third party firewalls	21
4.2.10	Third party firewalls: port usage by BIS login and Remote servers	21
4.2.11	Third party firewalls: port usage by BIS client	22
4.2.12	Third party firewalls: additional settings for Automation and Security Engine	22
4.2.13	Third party firewalls: additional settings for Video Engine	22
4.2.14	Third party firewalls: additional settings for Access Engine	22
4.2.15	Third party firewalls: port usage by SQL server	23
4.3	Network ports and firewall on AMS server	23
4.3.1	Settings for external firewall	24
4.3.2	Settings for AMS server to external application or device	25
4.3.3	Settings for MAC to external application or device	25
4.4	BIS HTTPS certificates	25
4.5	BIS shared folder	25
4.6	Secure deployment of Simons Voss offline doors	26
4.7	Secure deployment of IDEMIA Universal BioBridge	26
4.7.1	Secure Operation of the Morpho client server	26
4.7.2	Secure configuration of the connection between the MorphoManager server, BioBridge and the Morpho database	26
4.7.3	Secure configuration of the Intrusion RPS-API	26
4.7.4	Secure configuration of custom DESfire keys for MIFARE DESfire credentials	27
4.7.5	Secure operation of Microsoft SQL Server	27
4.7.6	Secure use of OPC UA:	28
4.7.7	Considerations for Visitor Management	28
4.8	Hardening	28
4.8.1	Security recommendations for AMS user authorizations	29
4.9	Configuration of AMS Intrusion RPS-API	29

4.10	Network encryption	29
4.11	IPsec Transport mode and Tunnel mode	30
4.11.1	IPsec and BIS Access Engine (ACE)	32
4.11.2	Comparison of Transport and Tunnel modes	32
4.11.3	Miscellaneous IP devices without operating system (AMCs, video cameras, etc.)	33
4.12	Transport mode configuration	34
4.12.1	Verify that the rule is restricting communication	39
4.12.2	Set up IPsec on the Remote Client, SQL Server, and Connection Server	39
4.12.3	Test communication between Login Server, Remote Client, SQL Server, and Connection Server	39
4.13	Tunnel mode configuration	40
4.13.1	Promote the Windows Server to a Domain Controller	41
4.13.2	Set up the VPN	47
4.13.3	Configure the VPN clients	50
4.13.4	Direct data traffic through the tunnel	53
4.14	AMS user profiles for third party products	54
4.15	Usage of Milestone XProtect	54
4.16	Usage of OSS-SO	55
4.17	Offline Access Systems	55
4.18	Connection of AMCIPConfig tool to AMC	55
4.19	Security advices for PHG key management	55
5	Secure operation	57
5.1	BIS password management	57
5.2	Password security advice	57
5.3	Data privacy	58
5.3.1	General Data Protection Regulation (GDPR)	58
5.3.2	Deactivation of BIS-ACE logfiles	58
5.3.3	Deactivation of AMS logfiles	60
6	Security update management	61
7	Secure decommissioning	62
7.1	Deinstallation of BIS	62
7.2	Deinstallation of AMS via client setup	62
7.3	Deinstallation of AMS via server setup	63
7.4	Deinstallation of AMS import/export tool	65
7.5	Deinstallation of AMS third party products	65
8	Appendices	66
8.1	Abbreviations used	66
	Glossary	67

1 Introduction

1.1 Purpose and audience

The Cybersecurity guidebook for Access Control Systems describes the following activities:

- Secure installation, configuration and operation of the system.
- Maintenance: updates and decommissioning. It includes secure handling of customer data and deletion of data including passwords.

Intended audience

- Installers and security responsables of access control systems.

2 System overview

2.1 Background: What is BIS?

The Building Integration System (BIS) is a software hub that collects and prioritizes alarms and status messages from its connected subsystems. It continually decides on and carries out appropriate responses, based on a customized, programmable rule-set. If human intervention is required, BIS presents the necessary information to system operators, and carries out the commands that those operators issue via highly customizable, graphical user interface. For forensic purposes, all actions can be logged.

BIS is an open integration platform, and connected subsystems can be of any kind in principle, but standard subsystems are available from Bosch for the following areas:

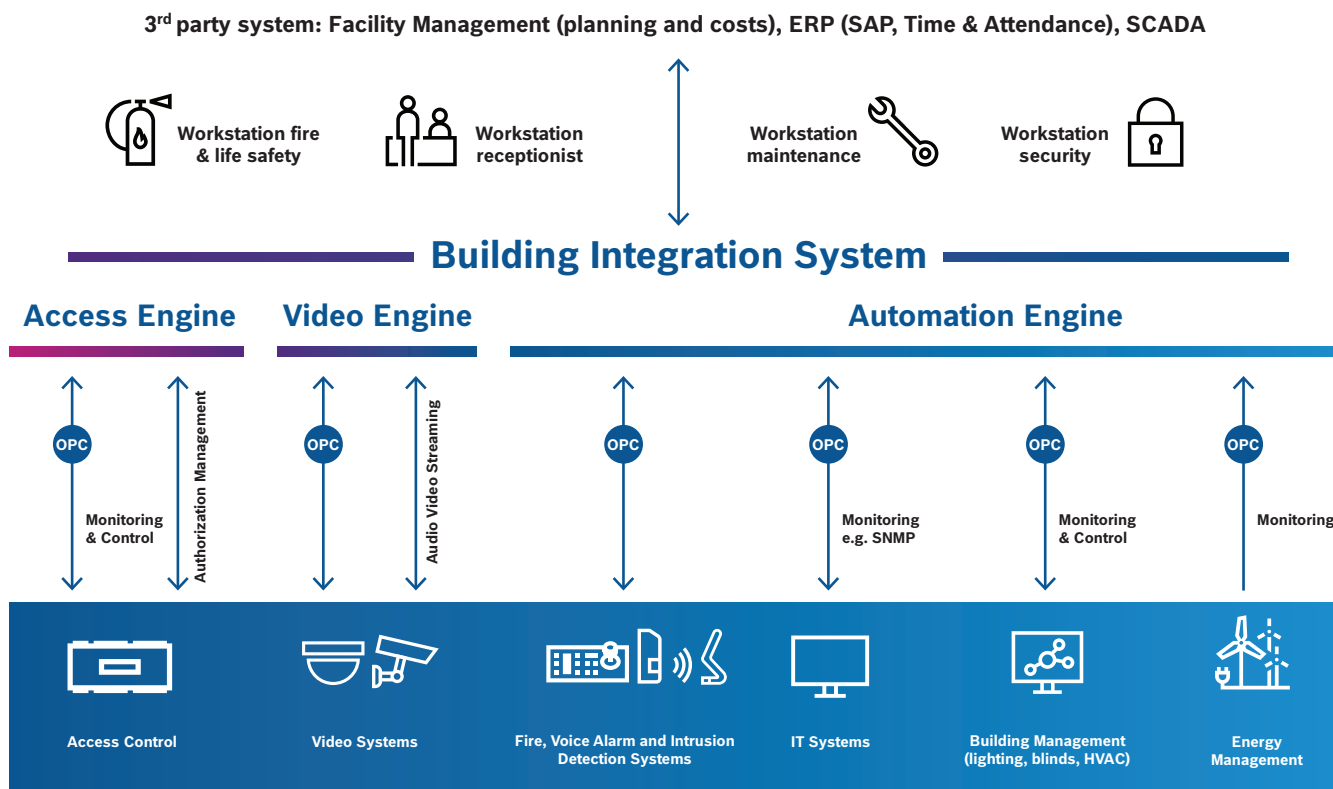
- Access control (Access Engine)
- Intrusion detection (Security Engine)
- Fire detection, environmental control and public address (Automation Engine)
- Video surveillance (Video Engine or BVMS)

Several thousands of BIS installations, integrating millions of detectors in total, are currently in operation all over the world.

2.2 BIS overview

BIS

for customized solutions of integrated building management



2.3 Background: What is AMS?

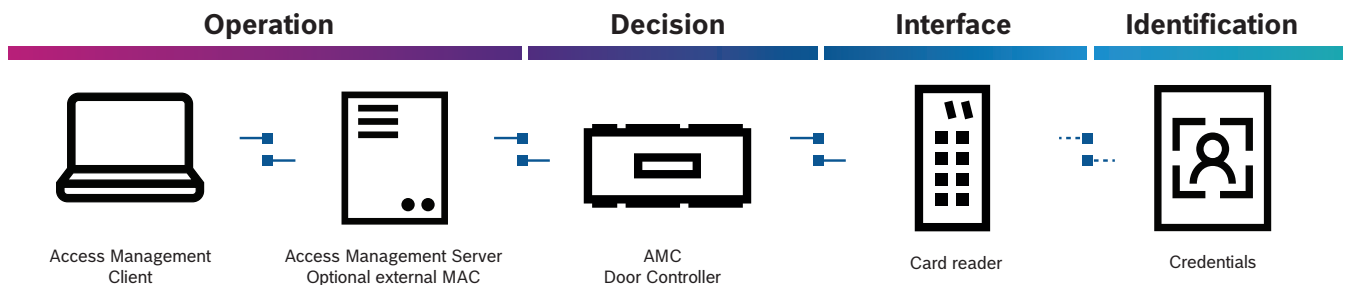
Access Management System (AMS) is an access control system for stand-alone application or for integration with other systems, such as the Bosch video management system BVMS or Bosch B and G series intrusion panels.

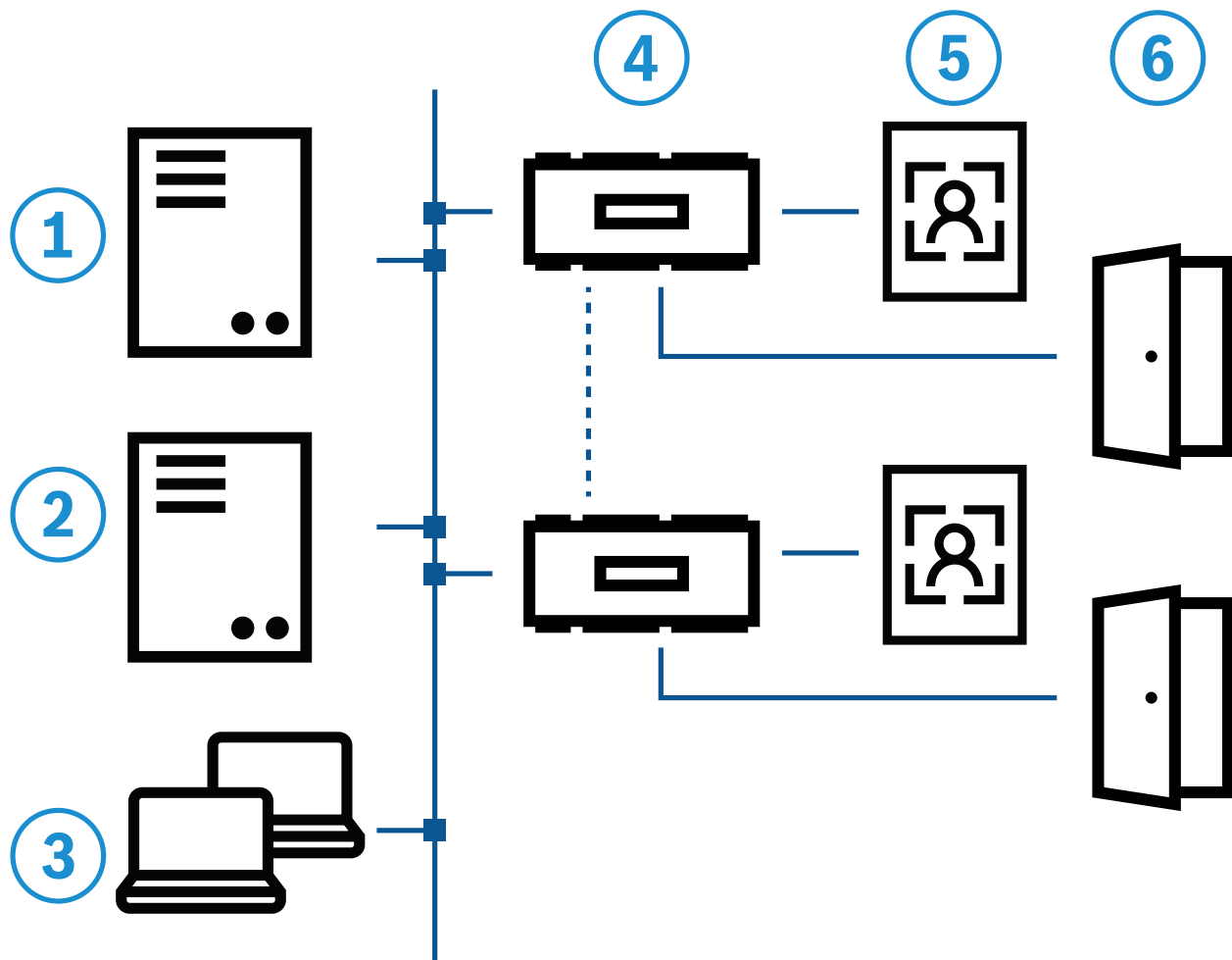
- As a stand-alone system, it features a simple-to-use map and alarm viewer for a rapid assessment of all the devices and entrances on the site.
- As an integrated system, it allows the operator of a video management system to perform door-related tasks like video-based ID verification, to grant and deny access, or to disable doors.
- Intrusion areas can be armed directly from the Map View, and intrusion panel users can be centrally managed.

AMS combines the robustness, performance and features of high-end access control products with a modern UI that makes it faster to install and configure.

The existing portfolio of Bosch access control devices can be easily scanned and integrated. Data privacy and IT security is state-of-the-art, in order to comply with the latest data-protection regulations.

2.4 AMS overview





(1) Access Management Server

The server is the central component for the data management. It coordinates all activities of the other hardware and software components.

(2) Master Access Controller (MAC)

The MAC is an additional security layer to increase system availability. It holds its own database to exchange information between AMCs, even if the management server or the network is down.

(3) Access Management Client

The access Management Client consists of the **Dialog Manager** and the **Map View Software**. The Dialog Manager is the main user interface for configuring the system, and for collecting and maintaining access-related information. In particular, its personnel dialogs are used for enrolling new cardholders, and maintaining their access authorizations and credentials. The Access Management Map View is a simple-to-use application to show door situation of the building in one glance. It shows door, tamper or malfunction alarms and allows sending commands directly from the map

(4) Access Modular Controller (AMC)

The AMC is a robust and reliable field controller to connect to up to 8 doors with readers and door strikes. The AMC can make autonomous decisions and store hundreds of thousands of access events, regardless of network interruptions. AMS also supports serial reader connection with secure OSDPv2 protocol. Communication between the main access control system and the local access controllers is secured by DTLS (with AES-256 encryption).

(5) Readers and credentials

In modern access control systems, personnel can identify themselves by means of physical credentials (e.g. cards), intellectual credentials (e.g. passwords) and biometric credentials (e.g. fingerprints). AMS supports a wide variety of credentials and their readers.

(6) Entrances models

AMS supports a wide variety of entrance types, and provides configuration templates for these in the software, to expedite the configuration process.

2.5 Achieving EN 60839

Introduction

EN 60839 is a family of European international standards for the hardware and software of:

- alarm and electronic security systems
- electronic access control systems

To ensure compliance of your access control system with this standard, parts of the configuration may need to be adapted. The following list contains the most important parts, for a complete list, please consult the standard as adopted in your own country.

2.5.1

BISACE compliance with EN 60839 standards**Special requirements for EN 60839 grades 3 and 4**

- EN 60839 Grade 4 requires OSDP readers with encryption enabled. Without OSDP or without encryption the configuration can only achieve Grade 3.
- EN 60839 Grade 4 requires Active Directory (LDAP) or Windows accounts for all operators of the access control system, and enforced password strength, see the section *Rules for password strength*, page 10 in this chapter.
- Access to the configuration mode must be strictly controlled. This can be achieved, for instance, by locating the computers in secured areas, and by timeouts on login sessions, particularly timeouts for inactivity at application and operating system level.
- Network and electric cabling must be laid in a secure area or encased in pipes.
- Only the card readers may be mounted in non-secured areas; all other devices must be in secured areas.
- The wiring of door contacts must not prevent the door's opening for an emergency evacuation triggered by a fire- or intrusion-prevention system.
- Any duress alarms must be made visible in the alarm-handling program (e.g. BIS).
- The minimum length of verification PINs for biometric or physical credentials must be set to at least 4.
- The minimum length of identification PINs must be set to at least 8.
- The main server computer, connection servers, MAC servers and clients must be synchronized with a network time server.

- Power monitoring must be enabled on local access controllers (e.g. AMCs).
- Offline functioning of local access controllers (e.g. AMCs) is only permitted during network failures. For example, the AMC's **Host timeout** parameter must **not** be set to 0.
- The alarm-handling program (e.g. BIS) must be configured to sort alarms by priority. The priority can be set from 1 (highest) to 99 (lowest).

Rules for password strength

- The minimum password length must be set to at least 8.
Note that this is longer than the length stipulated in the Microsoft security policy below.
- The Microsoft security policy setting: [Passwords must meet complexity requirements](#) must be enabled. Those requirements can be briefly summarized as follows:
- The password may not contain the user's account name or parts of the user's full name that exceed two consecutive characters. Both checks are not case sensitive.
- The password must contain characters from at least three of the following categories:
 - English uppercase characters (A through Z), characters with diacritic marks, Greek and Cyrillic characters
 - English lowercase letters (a through z, German sharp-s, characters with diacritic marks, Greek and Cyrillic characters
 - Base 10 digits (0 through 9)
 - Non-alphanumeric characters (special characters), for example, ! \$ # %, Note however that currency symbols such as the Euro or British Pound are not counted as special characters for this policy setting

2.5.2

AMS compliance with EN 60839 standard

Special requirements for EN 60839 grade 2

- The system meets the requirements for Global anti-passback in terms of using one zone per MAC.
- The different useable times zones of the AMS system depends on the numbers of MACs. A separate time zone can be used for each MAC.
- The wiring of door contacts must not prevent the door's opening for an emergency evacuation triggered by a fire- or intrusion-prevention system.
- Only OSDP readers use encryption on the RS485 interface.
- Access to the configuration mode must be strictly controlled. This can be achieved, for instance, by locating the computers in secured areas, and by timeouts on login sessions, particularly timeouts for inactivity at application and operating system level.
- Network and electric cabling must be laid in a secure area or encased in pipes.
- Only the card readers may be mounted in non-secured areas; all other devices must be in secured areas.
- The minimum length of verification PINs for biometric or physical credentials must be set to at least 4.
- The minimum length of identification PINs must be set to at least 8.
- The main server computer, connection servers, MAC servers and clients must be synchronized with a network time server.
- Power monitoring must be enabled on local access controllers (e.g. AMCs).
- Offline functioning of local access controllers (e.g. AMCs) is only permitted during network failures. For example, the AMC parameter **Host timeout** must not be set to 0.

Rules for password strength

- The minimum length of the password must be at least 5 characters.

3 Secure delivery and installation

The installation package is distributed as a download from the Bosch web catalog and from the download store. You can find the Bosch web catalog and the download store at:

commerce.boschsecurity.com/
downloadstore.boschsecurity.com/index.php

The distribution packages are ZIP files containing all executable binaries for installation, and cabinet files for all supported languages.

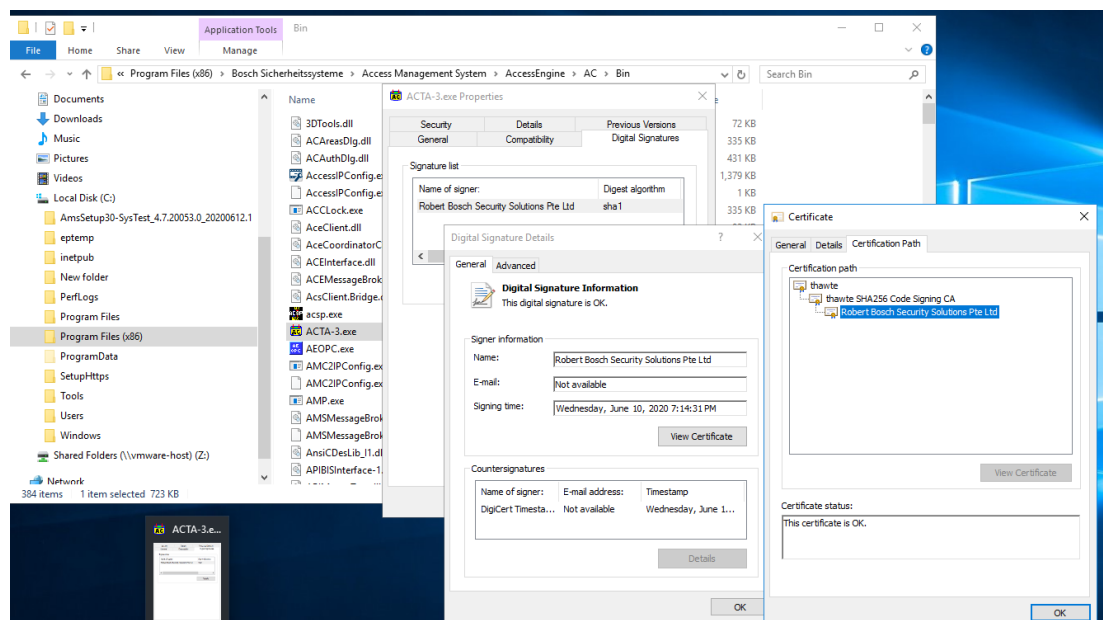
The download store provides SHA256 checksums for all distribution packages, to protect consumers from fraudulent distributions.

Platform	Version	Firmware URL	Checksum
BIS	4.6.9604	BIS_4.6.9604.0_Package_Common_1.zip	SHA256: 8A8633266D4D736DF4E699A7C5EAF41AC72C24F6C56FD06D92C8C4FDB6B0804F
BIS	4.6.9604	BIS_4.6.9604.0_Package_Common_2.zip	SHA256: 97CBFA6C7A433D841419A6AB5E8B3C367C65892DAFC3A06AF8DE4ED605159071
BIS	4.6.9604	BIS_4.6.9604.0_Package_3073_ar.zip	SHA256: AFF9110B9C1C1150199B268502656E60EEC893F9B484EC620B47C4726E21929A
BIS	4.6.9604	BIS_4.6.9604.0_Package_2052_chs.zip	SHA256: 42C208EFA11C8DB04AD4CF105A95EAC78CAD0FC3CCBD74F4303C76B37BAE1EAB
BIS	4.6.9604	BIS_4.6.9604.0_Package_1028_cht.zip	SHA256: DEC3C1A28A3BE16F1475E5F560D257F59FC4B13393D147A9103C9253B43458BA
BIS	4.6.9604	BIS_4.6.9604.0_Package_1031_de.zip	SHA256: F2E3229ADAF48941FFB71A8C3515AEC49054F059AA0FD80D1B6D8FA10145B557
BIS	4.6.9604	BIS_4.6.9604.0_Package_1033_en.zip	SHA256: 48614FC97C707BC4F5B5470E27B129BEC2C45685C2AC3CBF8A034BDA1DF0840
BIS	4.6.9604	BIS_4.6.9604.0_Package_3082_es.zip	SHA256: 871586A17742F073E19D62B8B8BD2DD4C7EF2D320CEBEC62174C469F42BA99B
BIS	4.6.9604	BIS_4.6.9604.0_Package_1036_fr.zip	SHA256: 4C55410003C7335D65EC58AE3E5CC1755A047DFEF0EE6D46965A8E9C646EFAEC
BIS	4.6.9604	BIS_4.6.9604.0_Package_1038_hu.zip	SHA256: EF05E6583225A7239BE43936C0740BD76842A17232AB2132999FE91784E806C0

To verify the integrity of the BIS and AMS distribution packages, download the zip file and check against the checksum found on the BOSCH catalog page using the document *Safe software delivery.pdf*.

Secure delivery of AMS can be further checked with the following procedures:

1. Extract the zip file by using Windows function **Extract All**.
2. All executables of the AMS are signed by Microsoft authenticode by Verisign with a BOSCH specific certificate. Signature check is done by Windows operating system. Validate those properties by checking the file **Properties > tab Digital Signatures > Details > View Certificate > tab Certification Path**. In the following example, the BOSCH certificate is certified by trusted root instant Thawte from DigiCert.



4 Secure configuration

4.1 Windows firewall exceptions for Bosch Access Control Systems

Exceptions for the following apps are required for the apps to communicate through Windows Firewall. For example: external MAC communicates with ACSP service.

The following settings have to be made:

1. To start the Windows Firewall, select **Start > Settings > Control Panel > Windows-Firewall**.
2. Select tab **Allow an app or Feature through Windows Firewall**.
3. Select **Allow another app** (if greyed-out, enable button by selecting “Change settings”).
4. Add the following programs:

Program	File Location
acsp.exe	[Install-path]\AccessEngine\AC\BIN
ACTA-3.exe	[Install-path]\AccessEngine\AC\BIN
BioVerify.exe	[Install-path]\AccessEngine\AC\BIN
Bioldentify.exe	[Install-path]\AccessEngine\AC\BIN
CalTa-3.exe	[Install-path]\AccessEngine\AC\BIN
CDTA-1.exe	[Install-path]\AccessEngine\AC\BIN
EMDP.exe	[Install-path]\AccessEngine\AC\BIN
KCKemas.exe	[Install-path]\AccessEngine\AC\BIN
KCS.exe	[Install-path]\AccessEngine\AC\BIN
Loggifier-2.exe	[Install-path]\AccessEngine\AC\BIN
PictureServer.exe	[Install-path]\AccessEngine\AC\BIN
ReplServer.exe	[Install-path]\AccessEngine\AC\BIN
reps.exe	[Install-path]\AccessEngine\AC\BIN
TAccExc.exe	[Install-path]\AccessEngine\AC\BIN
EMAILSP.exe	[Install-path]\AccessEngine\AC\BIN
master-3.exe	[Install-path]\AccessEngine\AC\BIN
querySrv-2.exe	[Install-path]\AccessEngine\AC\BIN
webSrv-1.exe	[Install-path]\AccessEngine\AC\BIN
DMS.exe	[install-path]\AccessEngine\MAC\BIN
lac.exe	[install-path]\AccessEngine\MAC\BIN

5. Add the following services:

Service	File Location
Bosch.States.Api	[install-path]\States API
Bosch.Map.Api	[install-path]\Map API

Bosch.MapView.Api	[install-path]\Map View API
Bosch.Events.Api	[install-path]\Events API
Bosch.Alarms.Api	[install-path]\Alarms API
Bosch.Ace.IdentityServer	[install-path]\Identity Server
Bosch.Ace.Api	[install-path]\Access API
Bosch.DialogManager.Api	[install-path]\Dialog Manager API
Bosch.Intrusion.Api	[install-path]\Intrusion API
Bosch Ace Visitor Management	[VM-install-path]\
Bosch Ace Visitor Management Client	[VM-client-install-path]\
Bosch.OSS-SO	[install-path]\OSS-SO
Bosch.OSS-SO.Configurator	[install-path]\OSS-SO.Configurator

4.2 Network ports and firewall on BIS server

For Windows 10, Windows Server 2016 and Windows Server 2019 it is assumed that the default settings for the Outbound Rules are set in the Windows Firewall as detailed below.

4.2.1 DCOM settings for all BIS Products

DCOM can use all ports from 1024 to 65535. However the BIS System needs only 3 ports for DCOM services. For security reasons therefore, limit the number of ports that are used for DCOM communication through the properties of **My Computer** in the component services settings (standard protocol).

1. To start DComCnfg click **Start > Run**, enter “DComCnfg” and confirm with **OK**.
2. Select **Component Services > Computers > My Computer** address workplace.
3. Right click **My Computer** for its context menu.
4. Select tab **Standard Protocols > TCP/IP > Properties**.
5. **Add** communication for a port range (e.g. 5000 - 5010 (TCP)).
As a rule of thumb, you should configure 3 ports per OPC server installed at a remote server.
6. To apply the changes, restart the computer.

4.2.2 Setting up Windows firewall

Port settings (TCP):

1. Start Windows Firewall, click **Start > Control Panel > Windows-Firewall**.
Select **Advanced settings**.
2. Select **Inbound Rules**.
3. In the **Actions** pane, select **New Rule**.
4. In the **Rule Type** dialog, select **Port** and click **Next**.
5. On the next page, select **TCP** and **Specific local ports**.
6. Enter the following ports:
 - 25805, 25806, 25902, 25922, 25923 and 26202 (BIS Ports)
 - 5000-5010 (DCOM ports see above)
 - 135 RPC (DCOM) communication

- 80 for HTTP communication
- 443 for HTTPS communication

Program settings (BoschST.BIS.ConfigurationBrowser.exe):

1. Start Windows Firewall, click **Start > Control Panel > Windows-Firewall**.
Select **Advanced settings**.
2. Select **Inbound Rules**.
3. In the **Actions** menu, select **New Rule**.
4. In the **Rule Type** dialog, select **Program**.
5. In the **Program** dialog, select **This program path:** and enter the following path.
*[Installation path]\MgtS\ConfigurationBrowser
\BoschST.BIS.ConfigurationBrowser.exe*

NOTE: All ports can be restricted to an internal network as long as the BIS-server is located in that network.

4.2.3

Windows firewall: port usage of BIS client

Allow the following BIS standard ports for inbound communication with the login server: 25805, 25806, 25902 and 25923 (TCP)

For internal communication (localhost to localhost), the BIS standard ports (25800 - 27050 (TCP)) are required.

If Video Engine is used, allow *BISClient.exe* through the Windows Firewall. Proceed as follows:

1. Start Windows Firewall (click **Start > Control Panel > Windows-Firewall**).
2. Select **Advanced settings**, do the following for Inbound Rules.
3. Add new Rule of type: **Program**.
4. Select **This program path** and add the following path:
C:\Program Files\MgtC\BISClient.exe
or on 64 Bit operating systems, the following:
C:\Program Files (x86)\MgtC\BISClient.exe

4.2.4

Windows firewall: additional settings of Automation and Security Engine

The general settings described in sections *DCOM settings for all BIS Products, page 14* and *Setting up Windows firewall, page 14* are sufficient for the Automation Engine and Security Engine.

4.2.5

Windows firewall: additional settings of Video Engine

General OPC-Server Services and Applications

The OPC-Server can be installed on the Login- or Remote-Server. The standard settings for the DCOM-communication are sufficient for the OPC-Server of the Video Engine, for example the LTC8x00-OPC-Server.

Special OPC-Server Services and Applications

The process ports for communications of the DIVAR OPC-Server of the Video Engine are opened dynamically. Thus it is not sufficient to allow communication through port areas in the Firewall. Instead, the services executable (in this case the DIVAR OPC server) must be added in the Windows Firewall. Therefore the following Programs and Services have to be made in addition to the settings described in section *DCOM settings for all BIS Products, page 14*:

Port settings (UDP):

Select Advanced settings, do the following for Inbound Rules

Add new Rule > Rule Type: Port (UDP)

Allow DCOM port 135 (UDP)

Allow port 1024 - 65535 (UDP/RTP) if Video SDK systems are used

Allow UPnP-Framework (Ports: 2869 (TCP), 1900 (UDP)) if DIVAR systems are used

RTSP 554 (TCP/UDP):

The usage of ports is variable, depending on how the cameras are configured and which types of cameras are used.

For connections to Bosch IP Cameras, Encoder and Decoder:

- Control channel: TCP ports 80 and 1756
- Network scan: UDP ports 1757 and 1758
- Multicast detection: one selectable UDP port (default 1800)
- Multicast video transmission:
For each ip camera / encoder audio or video stream, 1 selectable UDP port
- Unicast UDP transmission: UDP ports dynamically assigned in the range from 1024 to 65000

For connection to DiBos and BRS via VideoSDK OPC-Server (using Web service):

- TCP port 808

For display of Dibos 8.7 via Dibos ImageDecoder-OCX (using DCOM):

- TCP Port 135 plus four TCP ports and four UDP ports dynamically assigned in the range from 1025 to 65535

Program settings (OPC Server and Configuration-Tools for the VIE):

To start Windows Firewall, click **Start > Control Panel > Windows-Firewall**

Select **Advanced settings**, do the following for Inbound Rules

Add new Rules > Rule Type: Program

Allow the following programs:

BVIOpcConfig.exe	[Install-path]\MgtS\Video Engine \BVIOpcConfig
BVIOPCServer.exe	[Install-path]\MgtS\Connections\BVIP
VcsOpcConfig.exe	[Install-path]\MgtS\Video Engine\VCSOpcConfig
VCSOPCServer.exe	[Install-path]\MgtS\Connections\VCS
DivarConfig.exe	[Install-path]\MgtS\Video Engine\DivarOPCConfig
DivarOPCServer.exe	[Install-path]\MgtS\Connections\DivarOPCServer

VideoSdkOPCConfig.exe	[Install-path]\MgtS\Connections\VideoSdkOPCServer
VideoSdkOPCServer.exe	[Install-path]\MgtS\Connections\VideoSdkOPCServer

Firewall Settings for Third Party Video Applications

The Video Engine can also show foreign Video sources. Depending on the technology used, e.g. Active X, additional adjustments have to be made to the firewall settings according to the supplier's description. Please follow the provided documentation and installation information for Windows 7, Windows Server 2008 R2, Windows Server 2016 and firewall for set up and resulting performance.

This concerns the components:

- Bosch BVIP Lite Suite 3.0 Config Manager , Archive Player
- Divar XF Config Tool
- Bosch Video Recording Manager VRM Configurator

For other video web servers refer to their documentation.

Firewall Settings for VRE

The Video Engine can also show VRE sources. The following ports have to be considered:

These ports must be open on the recorders:

- 5008 (TCP), between SM Server and client programs Port rule: open inbound
- 5009 (TCP), between DVR Server and client programs Port rule: open inbound
- 5010 (TCP), between Watchdog Service and client programs Port rule: open inbound
- 5011 (TCP), between Streaming Service and client programs Port rule: open inbound

WebClient and GatewayServer specific ports:

- 9000 and 9999, between WebClient and GatewayServer. Port rule: open inbound

NOTES:

If you are using Windows Firewall, the DVMS installer can automatically create exceptions for the required ports.

If the ports 5008 - 5011 (TCP) are used for VRE the general range for the BIS products has to be enhanced to the range of e.g. 5000 - 5020 (TCP).

4.2.6

Windows firewall: additional settings for Access Engine

Most ports are assigned dynamically for the Access Engine processes.

Exceptions for the firewall

Exceptions for the following programs are required if they are not all running on the same computer

1. To start Windows Firewall, click **Start > Settings > Control Panel > Windows-Firewall**
2. Select tab **Exceptions**
3. Add the programs listed in the tables from *Windows firewall exceptions for Bosch Access Control Systems, page 13*.
4. Add the following from [Installation path]\MgtS\Access Engine\MAC\Bin

- DMS.exe
- LAC.exe
- 5. For Visitor Management (Server) add from *[Visitor Management Server Installation path]\Bosch Sicherheitssysteme\Bosch Visitor Management*
 - Bosch.Ace.VisitorManagement.exe
- 6. For Visitor Management (Client) add from *[Visitor Management Client Installation path]\Bosch Sicherheitssysteme\Bosch Visitor Management*
 - Bosch.Ace.VisitorManagement.Hardware.exe
- 7. For Occupancy Monitor add from *[Occupancy Monitor Installation path]\Bosch Sicherheitssysteme\Bosch Occupancy Monitor*
 - Bosch.Access.Areas.exe
- 8. For SmartSEC add from *[install-path]\MgtS\AMC Gateway*
 - Bosch.AmcGateway.exe

Established ports

The following ports are used in nearly every ACE system. Although they can be reconfigured, this is not recommended.

Component	Purpose	Protocol	Ports
DMS	Access Engine		
Master-3	Master - Name Service (Dynamic ports)	TCP	4999
ACSP-1	DMS-MAC communication	TCP	6001
...
ACSP-n	DMS-MAC communication	TCP	6000+n
RACSP-1	DMS-RMAC communication	TCP	6201
...
RACSP-n	DMS-RMAC communication	TCP	6200+n
ACTA	Database transactors	TCP	Dynamic
CDTA	Database transactors	TCP	Dynamic
CALTA	Database transactors	TCP	Dynamic
MDS	Database read only	TCP	Dynamic
WebSP	Database read only (Old)	TCP	Dynamic
BioVerify	Fingerprint verification (templates on server)	TCP	Dynamic
BioIdentify	Fingerprint identification (templates in device)	TCP	Dynamic
HandVerify	Hand vein verification	TCP	Dynamic
BISLoginService	Login verification	TCP	Dynamic
EMDP	Extended parking tickets verification	TCP	Dynamic

KCKEMAS	Key cabinet from KEMAS	TCP	Dynamic
KCS	Key cabinet from Deister	TCP	Dynamic
Loggifier	Logbook & Event service	TCP	Dynamic
PictureServer	Service to load/save pictures	TCP	Dynamic
REPL	Replication service for hierarchical systems	TCP	Dynamic
REPS	Reporting and printing	TCP	Dynamic
TAccExc	Time attendance exports	TCP	Dynamic
EmailSP	Send emails for parking tickets	TCP	Dynamic
AEOPC	OPC Server for alarm management	DCOM	
MAC			
DMS	Host Communication	TCP	6000
TwinMac	TWIN communication	TCP	6199
LAC	AMC Communicaton	UDP	10001
Visitor Management			
Server	Default port for server, configurable	TCP	5706

Configuration of the DMS

In the DMS the communication ports are configured via the System Parameter Editor (SPEdit). It is started from the BIS Configuration Browser's Tools menu. Although you can find these information in the system's registry it is recommended to use this tool.

In the parameter tree search for the "IPC" node (Example `.. \Micos\SPS\Default\IPC\ACSP-1`).

The parameters are specified as name:port/protocol (e.g. BIS46-DMS-EN:6004/tcp). Name can also be a TCP address in dotted notation.

Many server ports are not specified here. The DMS uses an internal name service. So many service ports are created as dynamic ports. They are registered at the name service and can be retrieved from there. Using this mechanism they do not have to be well known.

If the dynamic ports of the ACE must use a fixed port number to configure external firewalls, configure the port mapping in the registry:

- Copy one of the existing entries like "ACSP-1" rename it to the component name provided in the table before (like "REPS") and change the port value "ip-address:port/tcp"

The component list above is not complete. For example if the SQL-Server exists on a separate computer, further components are possible. The complete list of services are found in the file `PrcTable.tbl` in directory `.. \AccessEngine\AC\Cfg` of the ACE server.

Warning: The Configuration Browser manages the ACSP and MAC entries in registry and must not be changed manual.

Configuration of the MAC

The MAC ports are configured in the registry.

Go to the *HKLM\Software\WOW6432Node\Micos\MAC\IPC* key.

Here you can find the MAC's internal and external communication ports. The values are given as name:port/protocol where the local computer often is given as "." (single dot). Many communication lines use named pipes (noted as "/pipe" as protocol). In this case the port is not a number but a name (string).

4.2.7

Windows firewall: port usage by SQL server

The following settings have to be done on the PC where the corresponding SQL Server is running.

SQL Server for the BIS database connections (Event log/db9000, acedb, BIS Reports)

1. Port settings (UDP):

Start the Windows Firewall (click **Start > Control Panel > Windows-Firewall**)

Select **Advanced settings**, do the following for Inbound Rules

Add new Rule

Rule Type: Port (UDP)

- Allow UDP port 1434 for SQL Server Browser service

2. Port settings (TCP):

To start the Windows Firewall click **Start > Control Panel > Windows-Firewall**

Select **Advanced settings**, do the following for Inbound Rules

Add new Rule

Rule Type: Port (TCP)

- Allow TCP port 443 for SQL Server Browser service

3. Program settings (Sqlservr.exe):

To start the Windows Firewall click **Start > Control Panel > Windows-Firewall**

Select **Advanced settings**, do the following for Inbound Rules

Add new Rule

Rule Type: Program

Allow the following program:

- *C:\Program Files\Microsoft SQL Server\MSSQL15.(INSTANCE_NAME)\MSSQL\Binn\sqlservr.exe*

(in the case of case 32 bit operating systems the path will be

C:\Program Files (x86)\Microsoft SQL Server\MSSQL15.(INSTANCE_NAME)\MSSQL\Binn\sqlservr.exe)

SQL Server for the BIS Reporting Services connections

Allow Port (TCP) for Reporting Services, by default 8080.

To find out the port which is used from the SQL Server for the BIS Reporting Services:

Open Reporting Services Configuration Manager, connect to the RS Instance you use with BIS, and Open view for Web Service URL. The TCP port number is available.

1. Port settings (TCP):

To start the Windows Firewall click **Start > Control Panel > Windows-Firewall**
Select **Advanced settings**, do the following for Inbound Rules

Add new Rule

Rule Type: Port (TCP)

- Allow TCP port (e.g. 8080) for BIS Reporting Service connections

2. Allow 1433 (TCP) to the corresponding port for BIS Reporting Service connections and vice versa

For further information, see:

<http://support.microsoft.com/kb/827422/en-us>

<http://msdn.microsoft.com/de-de/library/cc646023.aspx>

<http://support.microsoft.com/kb/929851/en-us>

4.2.8

Windows firewall: additional settings for multi server BIS

The port that is used for communication between Consumer and Provider BIS Systems is defined in the configuration files.

The document *WCF Configuration.pdf* in folder *BIS\MgtS\Platform* on the installation medium or in the folder *MgtS\Platform* of an installed BIS System contains the details.

4.2.9

Third party firewalls

The following sections describe configuration of firewalls other than the Windows firewall.

4.2.10

Third party firewalls: port usage by BIS login and Remote servers

The BIS products make use of 4 areas of ports: BIS specific ports (port 25800 to port 27050), DCOM ports (may range from 1024 to 65535), standard ports (such as NETBIOS ports 137, 138, 139, 445 and a windows system port (7351).

DCOM can use all ports from 1024 to 65535. However the BIS System needs only 3 ports for DCOM services. For security reasons therefore, limit the number of ports that are used for DCOM communication through the properties of **My Computer** in the component services settings (standard protocol).

Settings for DCOM communication:

1. To start DComCnfg click **Start > Run...**, enter DComCnfg and confirm with **OK**
2. Select **Component Services > Computers > My Computer** address workplace
3. Right click **My Computer** for its context menu
4. Select tab **Standard Protocols > TCP/IP > Properties**
5. **Add** communication for a port range 5000 - 5010 (TCP)
6. To apply the changes, restart the system.

The many firewall products on the market differ greatly in their usage, making it impractical to describe all procedures in detail in this document. At a general level therefore, the following actions need to be performed to set up a third-party firewall for BIS.

- Allow all outbound traffic to localhost to ports in the specified range of ports used by BIS (25800 - 27050 (TCP))
- Allow all inbound traffic coming from localhost to ports in the specified range of ports used by BIS (25800 - 27050 (TCP))
- For communicating between the Remote- and the Login-Server the ports 25922 and 26202 (TCP) are used (inbound to the Login server, outbound on the remote server).
- If the SysTracer application is used the ports 26091, 26099, 26100 and 26098 (TCP) must be opened.
- Allow all outbound traffic to the partner BIS server to ports in the specified range of ports used for DCOM (5000 - 5010 (TCP))
- Allow all inbound traffic coming from the partner BIS server to ports in the specified range of ports used for DCOM (5000 - 5010 (TCP))
- Allow NETBIOS traffic to and from the BIS server partner in the same fashion (ports 137 (UDP), 138 (UDP), 137-139 (TCP), 445 (TCP))
- Allow all outbound traffic to the HTTP port (80 (TCP)) on localhost
- Allow all outbound traffic to port 7351 (TCP, dllhost) on localhost (the port number can vary)

The ports used on the corresponding sender side is undefined, thus restricting the sender ports disables communication.

TCP/IP communication can also (or alternatively) be limited to the executables found in the installation paths of the BIS product.

4.2.11 Third party firewalls: port usage by BIS client

The set up for the BIS Client, as specified in section *Windows firewall: port usage of BIS client, page 15* must also be performed on third party firewalls.

4.2.12 Third party firewalls: additional settings for Automation and Security Engine

The general settings described in sections *DCOM settings for all BIS Products, page 14* and *Setting up Windows firewall, page 14* are sufficient for the Automation Engine and Security Engine.

4.2.13 Third party firewalls: additional settings for Video Engine

The set up for the Video Engine, as specified in section *Windows firewall: additional settings of Video Engine, page 15*, must also be performed also on third party firewall products.

4.2.14 Third party firewalls: additional settings for Access Engine

The set up for the Access Engine, as specified in section *Windows firewall: additional settings for Access Engine, page 17*, must also be performed on third party firewall products.

4.2.15 Third party firewalls: port usage by SQL server

The set up for the SQL Server, as specified in section *Windows firewall: port usage by SQL server, page 20*, must also be performed on third party firewall products.

4.3 Network ports and firewall on AMS server

List of ports with purpose and communication protocol:

Ports can be configured on the server for connection between MAC and DMS. AMC has a fix port. Ports for clients to server and 3rd party software (for example, fingerprint reader) are negotiated by operating system. Therefore, ports cannot be defined.

Port settings for HTTPS communication (TCP):

Important for communication between DMS and Dialog Manager / Map
(see step 2 of SQL Server for the AMS database connections)

SQL Server for AMS database connections

1. Port settings (UDP):

Allows connection for UDP port 1434 for SQL Server Browser service

For Windows Firewall:

To start the Windows Firewall select **Start > Control Panel > Windows-Firewall**

Select **Advanced settings > Inbound Rules > New Rule**

Add new rule:

Rule Type: Port (UDP)

2. Port settings (TCP):

Allow connection for TCP port 443 for SQL Server Browser service

For Windows Firewall:

To start the Windows Firewall select **Start > Control Panel > Windows-Firewall**

Select **Advanced settings > Inbound Rules > New Rule**

Add new rule:

Rule Type: Port (TCP)

3. Program settings (Sqlservr.exe):

Allow the connection for incoming database requests. For example: Dialog manager and badge designer.

For Windows Firewall:

To start the Windows Firewall select **Start > Control Panel > Windows-Firewall**

Select **Advanced settings > Inbound Rules > New Rule**

Add new rule

Rule Type: Program

Select the following program:

```
C:\Program Files\Microsoft SQL Server\MSSQL(INSTANCE_NAME)\MSSQL\Binn
\sqlservr.exe)
```

Select action: "Allow the connection"

Select the connection type applicable for your network connection (Domain, Private or Public)

Windows Firewall exceptions

The connections in the Windows Firewall have to be configured to allow apps on the server to communicate. Refer to *Windows firewall exceptions for Bosch Access Control Systems, page 13* to configure these exceptions.

4.3.1

Settings for external firewall

With an external firewall, connecting clients from external to the AMS server requires the following settings:

- Connections used by AMS client
 - Protocol TCP port 4999
 - HTTPS:63801 Eventvwr
 - some dynamic ports
- Connections used by MAP View client
 - Protocol HTTPS:61802
 - some dynamic ports using SignalR protocol

As ports cannot be set to be fixed for all connections, and for security reasons, we strongly recommend using a VPN Tunnel to connect AMS server to AMS client via 3rd party firewall. So only one port on the external firewall needs to be open.

For MAP View client, the server must be reachable by DNS. See *IPsec Transport mode and Tunnel mode, page 30*.

Restriction for AMCIPOCONFIG / BIOCONFIG tools which uses broadcasting, so normally not useable by remote client.

Settings for other installable tools

- For all, ID Service is needed
 - Protocol HTTPS, Port 44333
- Connections used by Visitor Management Client
 - Protocol HTTPS, Port 5706
- Connections used by Occupancy Monitor Client
 - Protocol HTTPS, Port 6321
- Connections used by Importer Exporter Client
 - Protocol HTTPS, Port 443
- OSSO-SO Configurator
 - Protocol HTTPS, Port 63802
- AMS API (BVMS and Milestone integration)
 - Protocol HTTPS, Port 62904
 - SignalR with Dynamic port

For other tools:

- ACE API / SDK
 - Depend on your implementation, if your developer creates a service on AMS server, ask your developer. If ACE API /SDK connects from a remote host, use VPN Tunnel.

4.3.2 Settings for AMS server to external application or device

- External MAC (600x + 6000 verify also registry and documentation)
- External RMAC (600x + 6000 verify also registry and documentation)
- IDEMIA MorphoManager (see IDEMIA documentation for used ports for database and client connection)
- PCS HandVein (PCS-SDK TCP, see PCS Controller documentation)
- BioEntry W2 Fingerprint reader (HTTPS Port:51211)
- DeisterKey Cabinet (IP Port:2101 unencrypted or IP Port:2601 encrypted)
- Intrusion SDK (TCP/IP Port:7700 and HTTP or HTTPS Port:9000 by default)

4.3.3 Settings for MAC to external application or device

- SmartIntego TCP/IP configured connection
- OTIS TCP Multicast
- RMAC TCP/IP configured ports, verify also documentation.
- AMC UDP configurable, default port: dynamic (MAC) to port:10001 (AMC)

4.4 BIS HTTPS certificates

The Bosch Certificate Tool

BIS by default will install with a self-signed certificate. Nevertheless administrators are recommended to use *BoschCertificateTool.exe* from the folder *<InstallationDrive>:\Mgts\Certificates* to assign a CA-certificate for the BIS Login Server. For the Remote SQL Reporting service, run the tool from *_Install\AddOns\BIS\RemoteSQL\Certificate* folder on the BIS installation media.

4.5 BIS shared folder

Installation of BIS automatically creates the *Mgts* shared folder, which is accessible to the Everyone group. It is recommended to restrict the access and provide the following users and groups with full access to the *\Mgts* shared folder:

- MgtS-Service user
- IIS-USR user
- System group
- Network group
- Administrators group
- BIS Users group (add all users of BIS to the group)

Following that, proceed to remove the access for Everyone group.

4.6 Secure deployment of Simons Voss offline doors

For a secure connection between the BIS Access Engine and Simons Voss gateways, an AES encryption password has to be set.

See BIS Access Engine (ACE) operation help for details.

4.7 Secure deployment of IDEMIA Universal BioBridge

MorphoManager

Biometric access control application from the IDEMIA company. The application works with biometric devices to capture fingerprints and other biometric data. The biometric information is associated with cardholder data in a database. When cardholders present themselves at an IDEMIA biometric access reader, and their biometric data matches a card number in the database, the reader sends the associated card data to the local access controller, such as an AMC2 device, which then makes the decision to grant or deny access.

BioBridge

Interface software connecting MorphoManager with other access control systems.

4.7.1 Secure Operation of the Morpho client server

This section is valid only for systems with IDEMIA biometric readers.

Since Morpho enrollment devices and the Morpho client are served by the Morpho Client server, the following security measures are recommended:

1. Restrict access to the client machine to the smallest practicable number of users.
2. Disable Remote Desktop connections to the client machine, so that direct client access is needed to manage the Morpho client and the enrollment devices.
3. Enforce Administrator permissions for running the Task Manager on the client machine.
4. For starting the Morpho client, disable the login procedures "Auto Login without Windows Credentials" and "No Password". Use either "Credentials with username and Password" or "Auto Login with Windows Credentials".

4.7.2 Secure configuration of the connection between the MorphoManager server, BioBridge and the Morpho database

The OSDP connection between the MorphoManager server, BioBridge and the Morpho database must be encrypted. Follow the instructions in the user documentation: IDEMIA_Integration_ACE.pdf.

4.7.3 Secure configuration of the Intrusion RPS-API

The Intrusion RPS-API (Remote Programming System - Application Programming Interface) is required for the synchronization of cardholder data between the intrusion detection system and the access control system. It is mandatory to install the RPS-API on a different server from the BIS server.

Configure the RPS-API connection in the ACE Dialog Manager in the dialog RPS API Configuration.

For security, select HTTPS, not HTTP, on the ACE side and a corresponding configuration on the RPS-API site.

4.7.4 Secure configuration of custom DESfire keys for MIFARE DESfire credentials

Background

Bosch offers access credentials where the card data is secured by a Bosch DESfire key (MIFARE DESfire), or by Bosch stamp (LEGIC). Using the Bosch DESfire key, the LECTUS Select reader supports both these credential types “out-of-the-box”, that is, up to three different LEGIC advant configurations and up to three different MIFARE DESfire configurations.

A custom DESfire key is provided to the access control system contained in an encrypted parameter file created by a new standalone utility: the Bosch.ReaderConfigTool. A suitably authorized system operator imports the parameter files to the access control system using the Device Editor. In the Device Editor the operator also assigns the parameter files to compatible readers. The access control system then downloads the encryption key securely to those readers.

Security measures:

1. Make sure that the password for the custom encryption key is never seen by unauthorized persons, or transmitted via unsecured network connections.
2. Make sure that the system where password is entered is free of spyware such as key loggers.
3. Do not transmit the parameter file and its password together via the same connection.
4. Make sure that the hard disks of the access control server are encrypted, preferably through hardware encryption by controller rather than by Operating System.
5. Make sure that the access control server has enough memory to avoid creating a pagesys file, from which passwords can be reconstructed.

4.7.5 Secure operation of Microsoft SQL Server

Use the SQL Server Standard/Enterprise Edition with transparent data encryption (TDE). This encrypts the backup files created by the SQL Server also, using the database encryption key. Details are available from Microsoft at:

1. <https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-ver15>

Note that the certificate protecting the database encryption key will be required for restoring these backups. This means that in addition to backing up the database, you must make sure that you keep backups of the server certificates. If the certificate is lost, then the data not be retrievable.

Communication between BIS login server and remote SQL server contents are encrypted by Microsoft generated certificate by default. For more secure communication CA-signed certificates are recommended. Details are available from Microsoft at: <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-ver15>

4.7.6 Secure use of OPC UA:

OPC UA is, by default, not secured; if a secure OPC UA connection is required, use either HTTPS or certificate-based authentication.

The BIS setup program and Configuration Browser place certificates for OPC UA server in the folder <BIS installation drive>\Mgts\PKI.

Allow only "BISUsers" and "Administrators" access to this folder, for example by the following procedure:

1. Right click the PKI folder.
2. From the context menu, select **Properties** and then the **Security** tab.
3. Click the buttons **Advanced** and then **Change permissions**.
4. Select **Disable inheritance** and select **Convert inherited permissions into explicit permissions on this object**.
5. Select each group except "BISUsers" and "Administrators" in the **Principal** column, and remove them all.

Only "BISUsers" and "Administrators" should remain in the permissions table.

4.7.7 Considerations for Visitor Management

Visitor Management is an access control add-on for managing visitors. It typically uses a PC in the reception area, outside of strict access control, where visitors can register themselves, receive a visitor ID, and maintain their own visitor profiles before entering the access controlled area.

Security measures for the PC:

1. The PC runs only an approved browser in kiosk-mode. This mode cannot be broken by an attacker.
2. A polarized screen filter on the monitor allows only the current user to see it.
3. The physical USB- and network-ports are protected from unauthorized access, for example by enclosure in a secure cabinet.
4. The PC is in sight of security personnel at all times. These personnel are vigilant to prevent prolonged access.
5. Network access to the PC is highly restricted.

Security measures for the visitor-ID:

1. Configure an appropriate length for the ID.
2. Visitors must protect their IDs from unauthorized access, and be aware that the ID itself is sufficient to access the profile data that they have entered.

4.8 Hardening

Some general recommendations:

- Install anti-virus and anti-spyware software and keep it up to date.

- The windows software patches and updates shall be installed and shall remain up to date. Windows updates often include patches to newly discovered security vulnerabilities, such as the Heartbleed SSL vulnerability, which affected millions of computers worldwide. Patches for these significant issues should be installed.
- Base libraries from Microsoft like .NetCore 3.1.x must be updated if vulnerabilities are reported too.
- Disable USB ports and drives for removable disks.
- Disable unused NIC ports and management ports, such as the HP ILO (HP Integrated Lights-Out) interface.
- Disable console ports or set password protection.
- Address security issues promptly.
- Disable “Insecure” cipher suites. Cipher suite TLS_RSA_WITH_AES_256_CBC_SHA256 has been tested and is sufficient for the system to work.

4.8.1 Security recommendations for AMS user authorizations

On the AMS server, define only Windows users who are intended to change the AMS setup (files, certificates, registry and licenses), and give them Windows Administrator rights. The file structure containing the certificates and configuration files should only be accessible to Windows Administrator and System users.

4.9 Configuration of AMS Intrusion RPS-API

The Intrusion RPS-API is a software package delivered by Intrusion and is needed for Cardholder Synchronization with the AMS system. It is mandatory to install the RPS-API on a different server from the AMS server.

The RPS-API connection has to be configured in the AMS Dialog Manager in dialog “RPS API Configuration”.

The connection can be configured as HTTPS (default) or HTTP. Since this is a security sensitive link, the recommendation is to configure the connection as HTTPS. This has to be done by choosing HTTPS on the AMS site and a corresponding configuration on the RPS-API site.

4.10 Network encryption

Protection of the connection between all network nodes (clients, server, external MACs) ensured by access control systems:

- Encryption for AMS backend, MAC and Dialog Manager:
 - DTLS and AES-128 between AMC and MAC
 - AES-128 between MAC and DMS
 - AES-128 and HTTPS between Dialogs and DMS
- For a secure connection between MAC and Simons Voss Gateways, an AES encryption password has to be set on the Gateways and on the MAC.

Protection that requires manual action by installer:

- HTTPS for communication between AMS Access API, Map API, Identity Server and States API:
Communication between AMS Access API, Map API, Identity Server and States API is

ensured via https and self-signed certificates. In order to ensure server authentication, the certificate includes the Hostname of the AMS server machine. The Hostname is not known before the installation starts. Therefore a Bosch certificate cannot be used.

- The proper way is that the IT department on the customer site generates and manages the certificate for the customer company.

RSA with key length of 2048 and SHA256 as hashing algorithm is used for the certificates.

- How to install the self-signed certificate is explained in document in the same folder as the Certificate tool.

Recommended optional protection, which require manual setup by installer:

- IPSec via Transport or Tunneling between all network nodes: MAC, DMS, and workstations. (IPSec to AMC is not supported).

It is recommended to setup IPSec between all network nodes to improve data security.

Its main focus is on configuring a secure network environment for the AMS using IPSec on Windows.

4.11

IPsec Transport mode and Tunnel mode

The following implementations are recommended.

IPsec can be implemented in different ways. In this document we consider **Transport mode** and **Tunnel mode**.



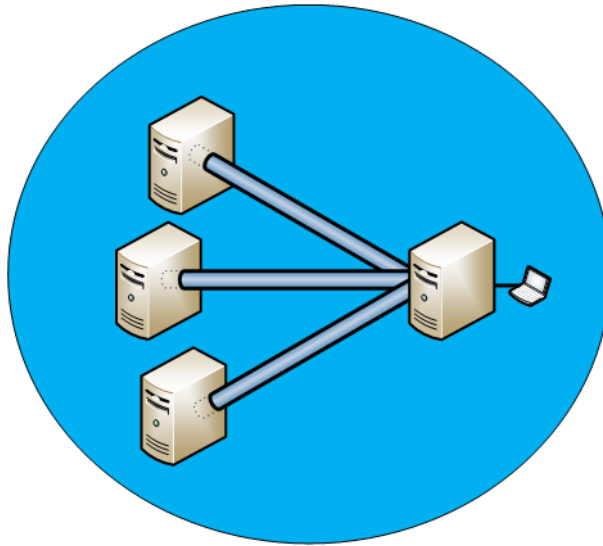
Notice!

When to implement IPsec

For effective troubleshooting it is recommended that your BIS installation be complete and stable across all participating computers in your BIS network before you start to implement IPsec in it.

Introduction to Transport mode

Transport mode is used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host — for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination



The transport mode encrypts only the payload and ESP trailer; so the IP header of the original packet is not encrypted.

The IPsec Transport mode is implemented for client-to-site VPN scenarios.

NAT (Network Address Translation) traversal is not supported with the transport mode.

MSS (Maximum Segment Size) is higher compared to Tunnel mode, as no additional headers are required.

The transport mode is usually used when another tunneling protocol, such as GRE (Generic Routing Encapsulation), L2TP (Layer 2 Tunneling Protocol)) is used to first encapsulate the IP data packet. Then IPsec is used to protect the GRE/L2TP tunnel packets.

Introduction to Tunnel mode

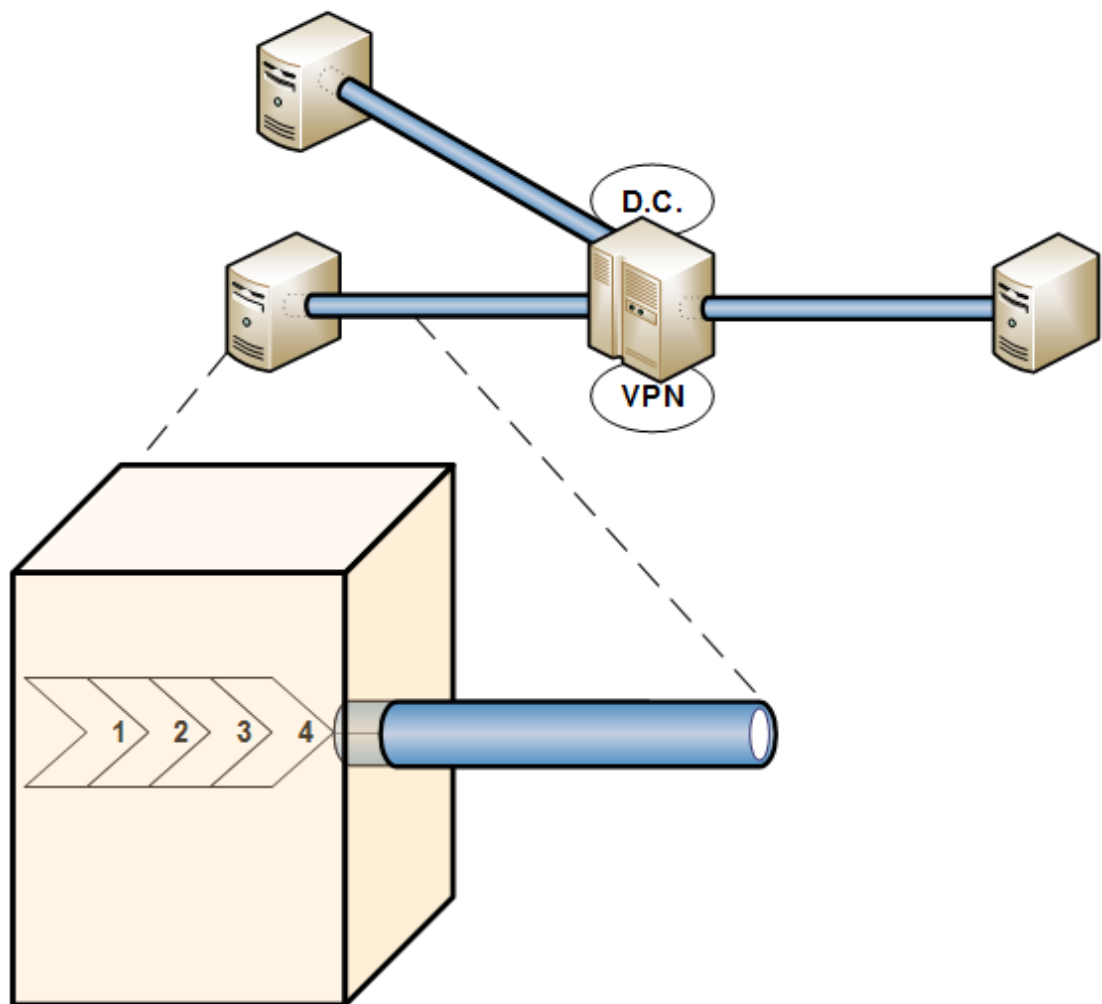
A Windows Server computer is set up as both **Domain Controller** and **VPN server**. This computer keeps track of the names and addresses of all the machines in the BIS network, and provides encrypted tunneling for all connections between them.

Tunnel mode protects the internal routing information by encrypting the IP header of the original packet. The original packet is encapsulated by another set of IP headers.

It is widely implemented in site-to-site VPN scenarios.

NAT traversal is supported.

Additional headers are added to the packet; so the payload MSS is smaller.



1	Application + IP socket	D.C.:	Domain Controller (primary or secondary)
2	Virtual NIC + Layer 2 Tunneling Protocol (L2TP)		
3	IPsec (IP security protocol)	VPN	Virtual Private Network server (software)
4	NIC (Network Interface card)		

4.11.1 IPsec and BIS Access Engine (ACE)



Notice!
For use of IPsec specifically within the BIS Access Engine (ACE), please refer to the ACE Configuration online help.

4.11.2 Comparison of Transport and Tunnel modes

The following table shows some of the main differences between Transport and Tunnel modes.

Transport Mode	Tunnel Mode
Connection Security Rule should be configured the same on all machines	No Connection Security Rule configuration on each machine is required
Firewall has to be enabled on all machines for the Connection Security Rule to take effect	Firewall does not need to be enabled on any machine
No additional server is required to host the VPN server software	Additional computer is required as a Domain Controller that also hosts the VPN server software.
If a security rule is missed out for a particular Endpoint (for example, a client) the machines will not be able to authenticate each other and connection will not be established	If VPN server is down, all secure communication to the Login Server will be down. If this occurs, all machines should reconnect to the VPN server again
	Hosts file may need to be modified in order to resolve hostnames to the VPN IP address

4.11.3 Miscellaneous IP devices without operating system (AMCs, video cameras, etc.)

IP devices such as AMCs and video cameras have no operating system (OS), and therefore no way to be configured for IPsec. Nevertheless the BIS system needs to exchange data and commands with these non-OS devices.

There are 2 ways to enable communication between BIS and non-OS devices using **security rules**:

	When creating the security rule...	Consequences
Variant 1	Define the endpoints of the rule with the specific IP addresses of all the BIS servers and clients, ignoring the non-OS devices	Only the IP addresses of the servers and clients that are specified in the rule will have secured communication. All other computers and non-OS IP devices that communicate with the computer will not have their data encapsulated. This means an implicit exemption for the non-OS devices.
Variant 2	When defining the endpoints, select the radio button Any IP address . Then create another rule to specify IP addresses that are to be exempted.	All communication between the computer and any IP devices will be covered by the rule, including non-OS devices. The non-OS IP devices will not be able to communicate with the computers, until the exemption rule is active, This means an explicit exemption for the non-OS devices.

Variant 2 is preferable as the more explicit of the two, but note that in both cases the data traffic between BIS and the non-OS IP devices is **not** encapsulated.

Where tunneling is used, that is where the computers communicate via the VPN server, no security rules need to be configured for the non-OS IP devices, as they do not connect via the VPN tunnel in the first place.

Communication between non-OS IP devices and BIS Connection servers , where OPC servers typically reside, always lies outside of IPsec. Therefore this communication is not encapsulated.



Notice!

IP communication between BIS computers and IP devices with no operating system can be enabled but not protected by IPsec.

4.12

Transport mode configuration

How to set up IPsec on the Login server or Connection server

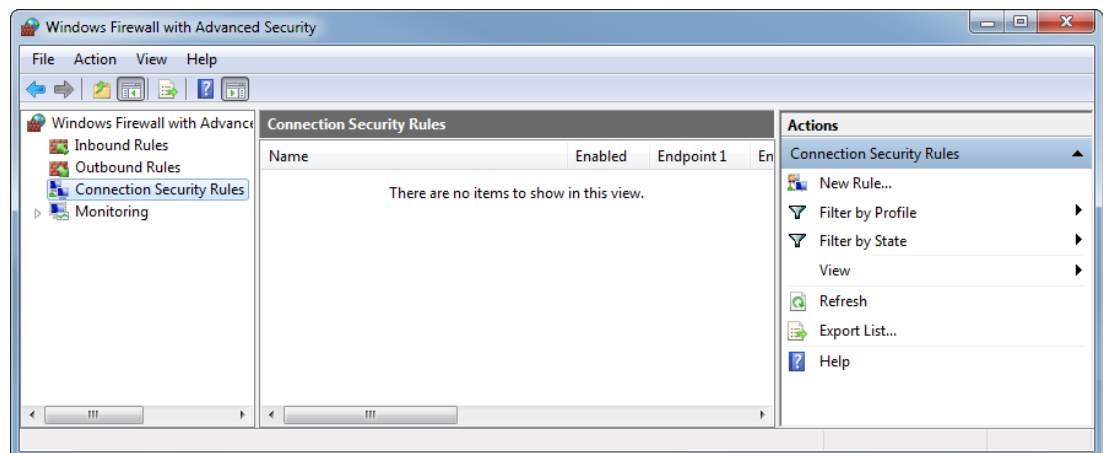


Notice!

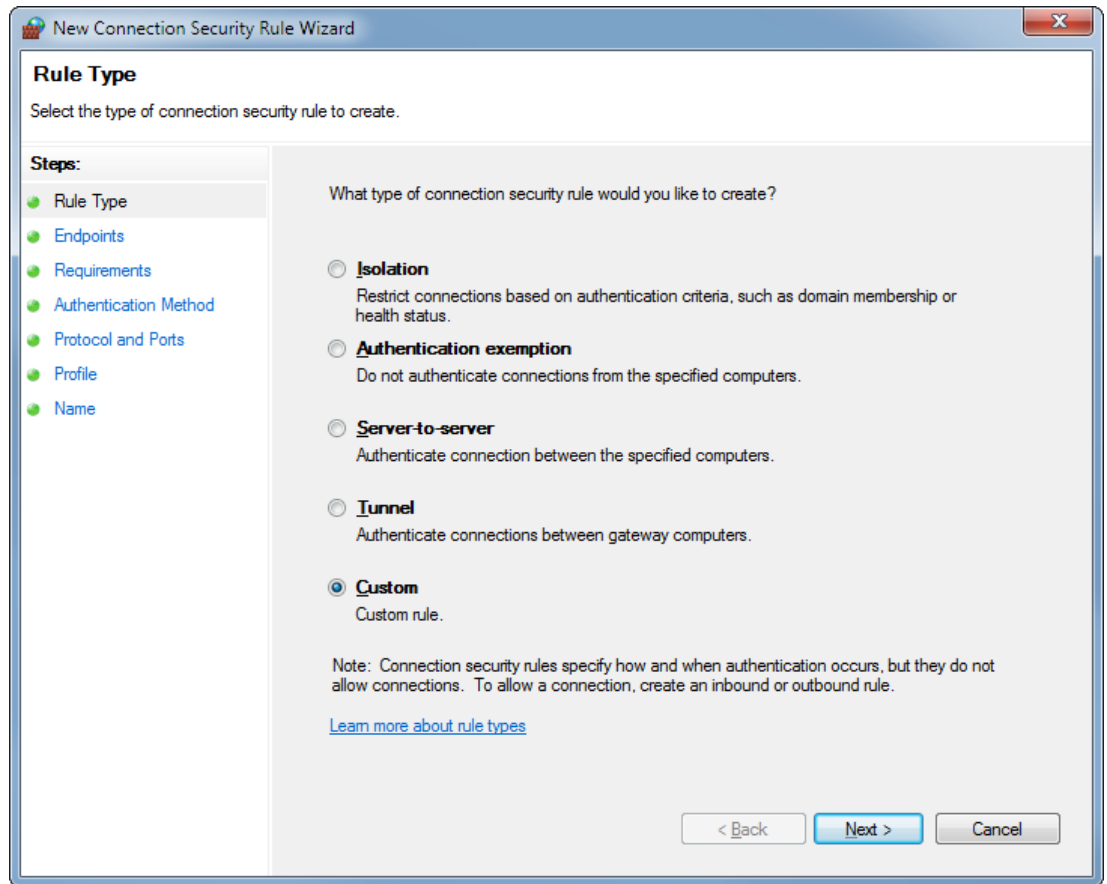
Configuration of IPsec using this method for peer authentication requires that the computers be part of a domain that has computer accounts. The user who is configuring must be logged-on to that domain.

(Refer to Microsoft documentation for more details, for example: <https://msdn.microsoft.com/en-us/library/bb742429.aspx> , Step-by-Step Guide to Internet Protocol Security (IPSec)).

1. Configure Firewall settings for BIS according to the *BIS_Firewall_Configuration.pdf* document.
Configure DCOM settings according to the *DCOM Configuration.pdf* document.
2. Start **Windows Firewall with Advanced Security** > Right-click **Connection Security Rules** and select **New Rule...**



3. Select **Custom** and click **Next>**



4. Add the Endpoints and click **Next>**
Endpoints are the machines with which you would want to have a secure connection.
Endpoint 1 = Login Server's IP address
Endpoint 2 = IP addresses of SQL server, Remote client or Connection server

Endpoints

Specify the computers between which secured connections will be established using IPsec.

Steps:

- Rule Type
- Endpoints**
- Requirements
- Authentication Method
- Protocol and Ports
- Profile
- Name

Create a secured connection between computers in Endpoint 1 and Endpoint 2.

Which computers are in Endpoint 1?

☐ Any IP address

☒ These IP addresses:

10.123.41.7

Add... Edit... Remove

Customize the interface types to which this rule applies: Customize...

Which computers are in Endpoint 2?

☐ Any IP address

☒ These IP addresses:

10.123.41.10
10.123.41.11
10.123.41.5

Add... Edit... Remove

[Learn more about computer endpoints](#)

< Back Next > Cancel

5. Select **Require authentication for inbound and outbound connections** and click **Next>**

Requirements

Specify the authentication requirements for connections that match this rule.

Steps:

- Rule Type
- Endpoints
- Requirements**
- Authentication Method
- Protocol and Ports
- Profile
- Name

When do you want authentication to occur?

☐ Request authentication for inbound and outbound connections
Authenticate whenever possible but authentication is not required.

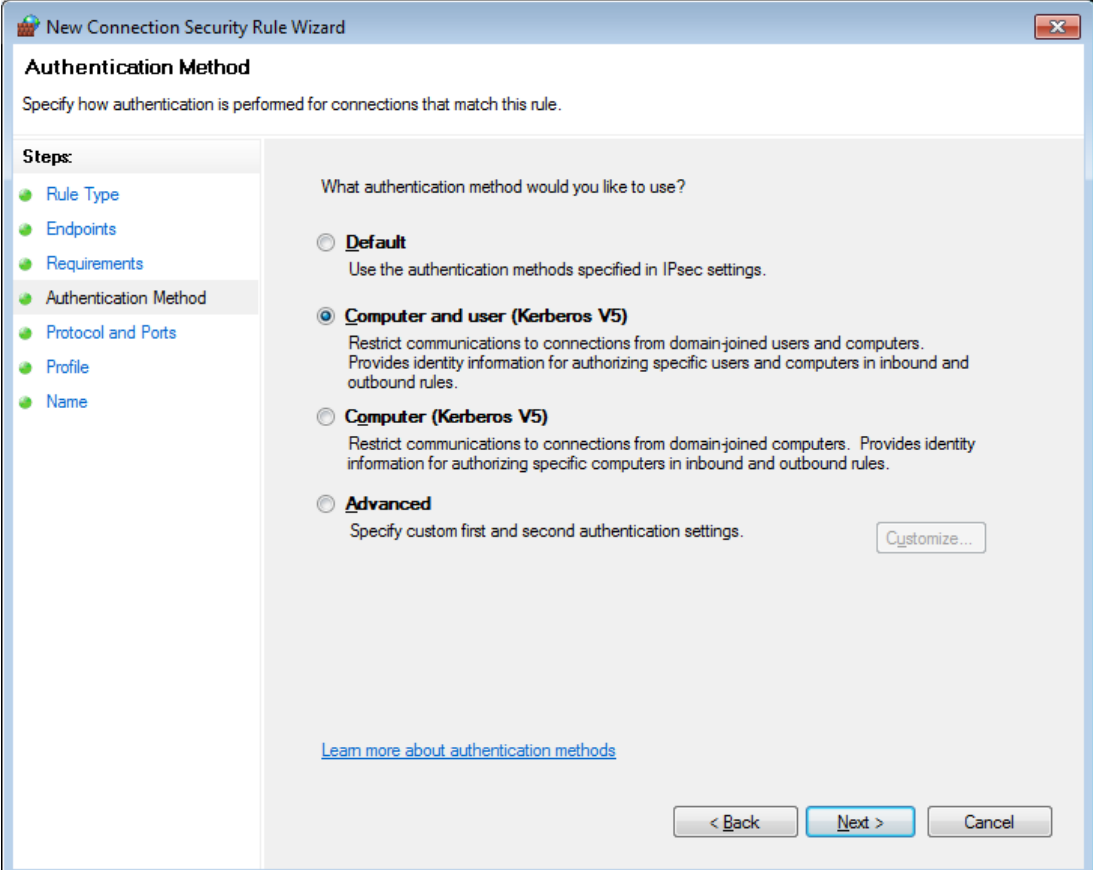
☐ Require authentication for inbound connections and request authentication for outbound connections
Inbound connections must be authenticated to be allowed. Outbound connections are authenticated whenever possible but authentication is not required.

☒ **Require authentication for inbound and outbound connections**
Both inbound and outbound connections must be authenticated to be allowed.

☐ Do not authenticate
No connections will be authenticated.

< Back Next > Cancel

6. Select **Computer and User (Kerberos V5)** and click **Next>**



New Connection Security Rule Wizard

Authentication Method

Specify how authentication is performed for connections that match this rule.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method**
- Protocol and Ports
- Profile
- Name

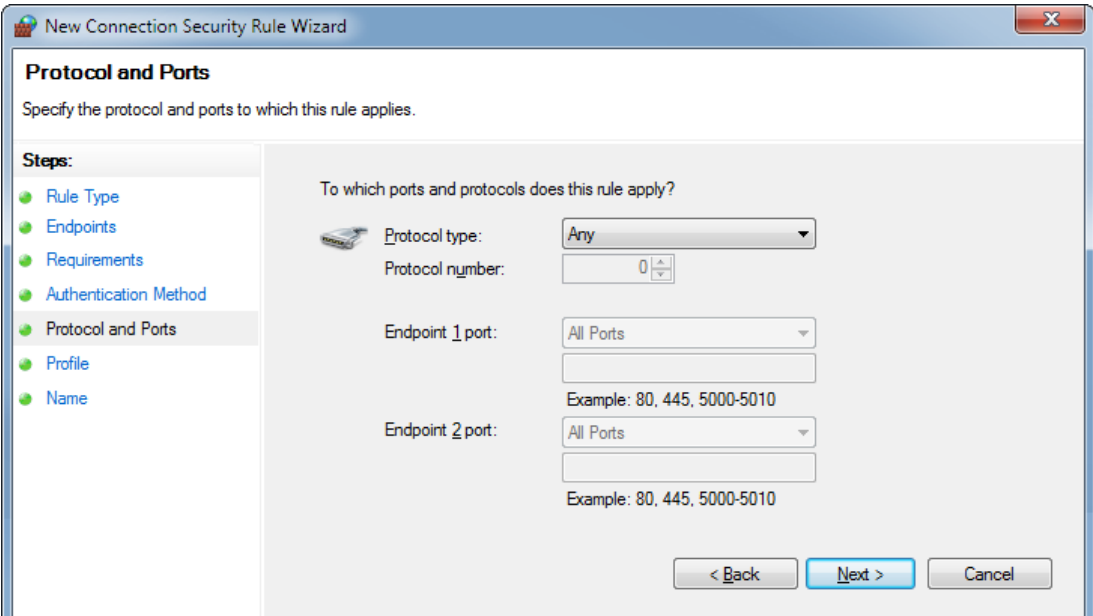
What authentication method would you like to use?

- ☐ **Default**
Use the authentication methods specified in IPsec settings.
- ☒ **Computer and user (Kerberos V5)**
Restrict communications to connections from domain-joined users and computers. Provides identity information for authorizing specific users and computers in inbound and outbound rules.
- ☐ **Computer (Kerberos V5)**
Restrict communications to connections from domain-joined computers. Provides identity information for authorizing specific computers in inbound and outbound rules.
- ☐ **Advanced**
Specify custom first and second authentication settings. [Customize...](#)

[Learn more about authentication methods](#)

< Back Next > Cancel

7. Leave the **Ports and Protocols** as default and click **Next>**



New Connection Security Rule Wizard

Protocol and Ports

Specify the protocol and ports to which this rule applies.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Protocol and Ports**
- Profile
- Name

To which ports and protocols does this rule apply?

Protocol type: Any

Protocol number: 0

Endpoint 1 port: All Ports

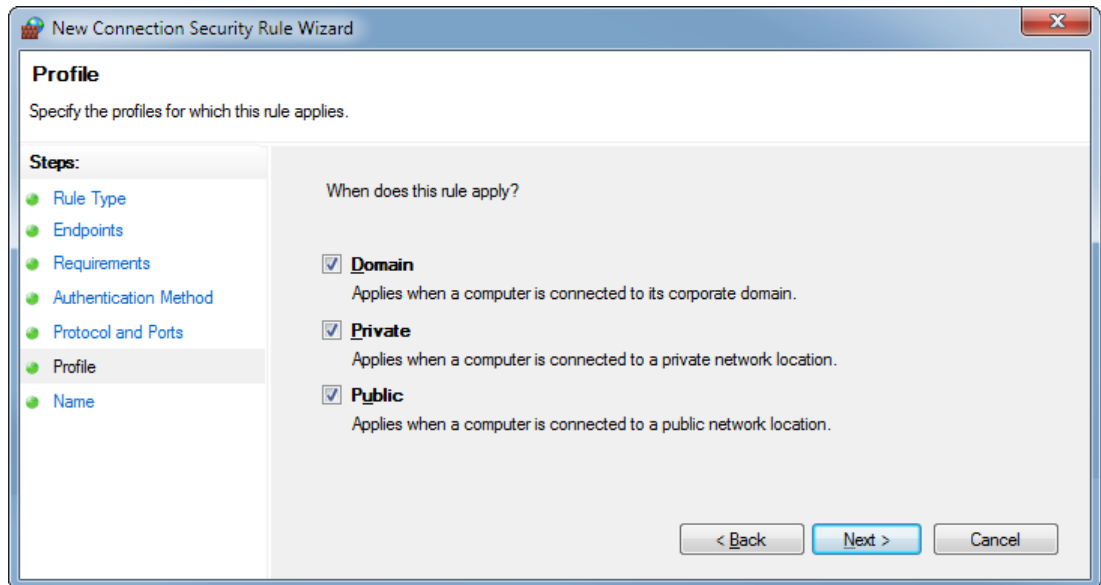
Example: 80, 445, 5000-5010

Endpoint 2 port: All Ports

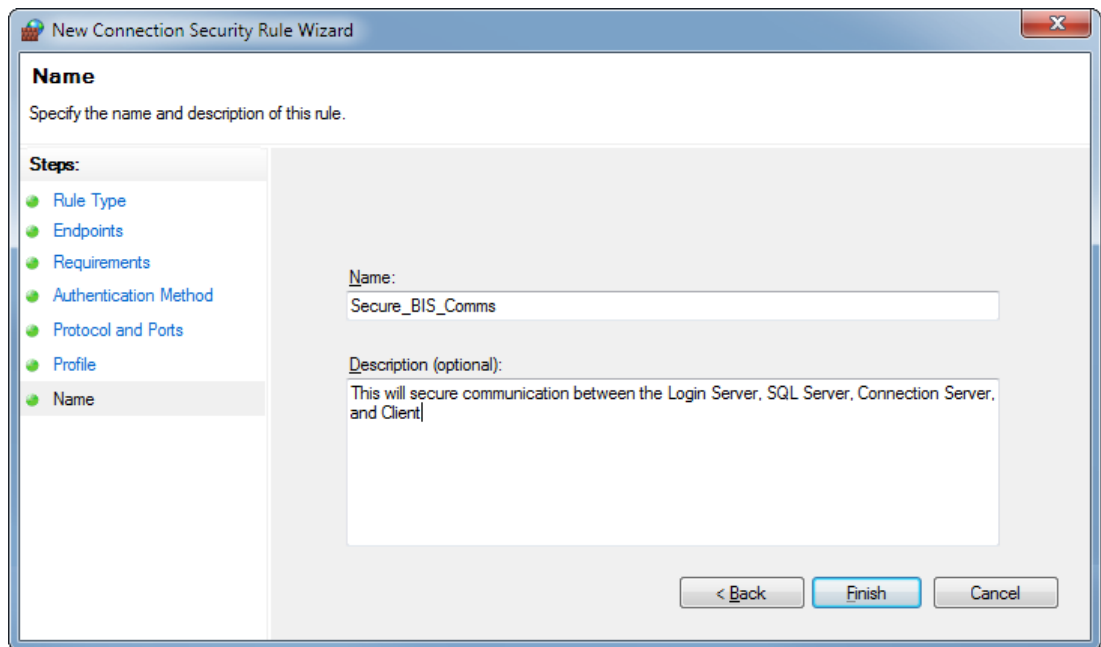
Example: 80, 445, 5000-5010

< Back Next > Cancel

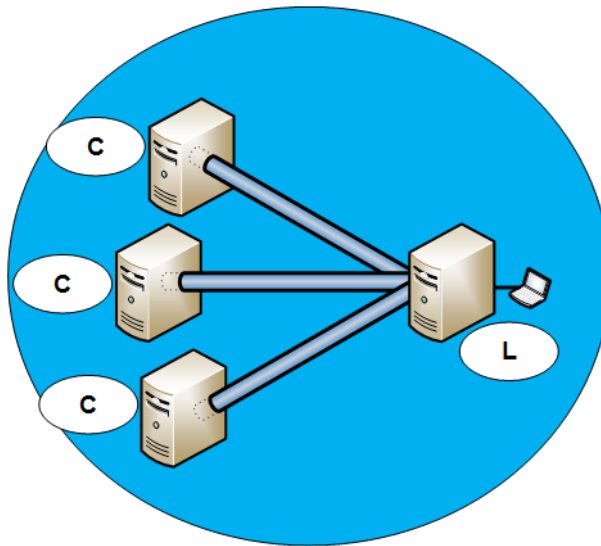
8. Leave the **Profiles** as default (all check boxes selected) and click **Next>**



9. Set a name and description for the rule and click **Finish**



Result: The rule is created and appears in the list of rules.



C	Clients, Connection Servers, Database servers	L	BIS login server
----------	---	----------	------------------

4.12.1

Verify that the rule is restricting communication

1. Enable Windows Firewall and ping the other machines (Remote Client, SQL Server, and Connection Server)

Result: The pings will not succeed: connection cannot be established. This is because the security rule requires **all** the participating machines to be similarly configured before they can communicate.



Notice!

The firewall on each machine must have the same rule.

4.12.2

Set up IPSec on the Remote Client, SQL Server, and Connection Server

1. Copy the exact same settings of the security rule of the BIS Login Server to each of the other machines
2. From the Login Server, ping the other machines again:
Connections can now be established

4.12.3

Test communication between Login Server, Remote Client, SQL Server, and Connection Server

1. Install the packet sniffer Wireshark on all of the machines (<https://www.wireshark.org/>)
2. Start capturing the network traffic from the LAN interface
3. Open the BIS client and connect to the Login Server
4. Network traffic should be encapsulated as shown below:

Capturing from Local Area Connection [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.addr==10.123.41.51` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
5978	75.1890490	10.123.41.51	10.123.41.57	ISAKMP	118	Quick Mode
5979	75.1894110	10.123.41.57	10.123.41.51	ESP	110	ESP (SPI=0xb6412186)
5980	75.1898720	10.123.41.51	10.123.41.57	ESP	110	ESP (SPI=0x7290cd8e)
5981	75.1899640	10.123.41.57	10.123.41.51	ESP	98	ESP (SPI=0xb6412186)
5982	75.1901020	10.123.41.57	10.123.41.51	ESP	398	ESP (SPI=0xb6412186)
5983	75.1932570	10.123.41.51	10.123.41.57	ESP	1514	ESP (SPI=0x7290cd8e)
5984	75.1933620	10.123.41.57	10.123.41.51	ESP	98	ESP (SPI=0xb6412186)
5985	75.1933810	10.123.41.51	10.123.41.57	ESP	1514	ESP (SPI=0x7290cd8e)
5986	75.1934110	10.123.41.57	10.123.41.51	ESP	98	ESP (SPI=0xb6412186)
5987	75.1934220	10.123.41.51	10.123.41.57	ESP	282	ESP (SPI=0x7290cd8e)
5988	75.1934440	10.123.41.57	10.123.41.51	ESP	98	ESP (SPI=0xb6412186)
5998	75.2498390	10.123.41.57	10.123.41.51	ESP	306	ESP (SPI=0xb6412186)
6002	75.2508840	10.123.41.51	10.123.41.57	ESP	1514	ESP (SPI=0x7290cd8e)
6003	75.2509830	10.123.41.57	10.123.41.51	ESP	98	ESP (SPI=0xb6412186)
6004	75.2510040	10.123.41.51	10.123.41.57	ESP	1514	ESP (SPI=0x7290cd8e)
6005	75.2510330	10.123.41.57	10.123.41.51	ESP	98	ESP (SPI=0xb6412186)
6006	75.2511050	10.123.41.51	10.123.41.57	ESP	1238	ESP (SPI=0x7290cd8e)
6007	75.2511340	10.123.41.57	10.123.41.51	ESP	98	ESP (SPI=0xb6412186)
6056	75.6856130	10.123.41.57	10.123.41.51	ESP	110	ESP (SPI=0xb6412186)
6057	75.6859990	10.123.41.51	10.123.41.57	ESP	110	ESP (SPI=0x7290cd8e)
6058	75.6860950	10.123.41.57	10.123.41.51	ESP	98	ESP (SPI=0xb6412186)
6059	75.6861440	10.123.41.57	10.123.41.51	ESP	254	ESP (SPI=0xb6412186)
6060	75.6872580	10.123.41.51	10.123.41.57	ESP	1514	ESP (SPI=0x7290cd8e)
6061	75.6873210	10.123.41.57	10.123.41.51	ESP	98	ESP (SPI=0xb6412186)
6062	75.6873780	10.123.41.51	10.123.41.57	ESP	1514	ESP (SPI=0x7290cd8e)
6063	75.6874050	10.123.41.57	10.123.41.51	ESP	98	ESP (SPI=0xb6412186)
6064	75.6874870	10.123.41.51	10.123.41.57	ESP	1238	ESP (SPI=0x7290cd8e)

+ Frame 1312: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
 + Ethernet II, Src: Hewlett_4f:91:fa (2c:41:38:4f:91:fa), Dst: IPv4mcast_fc (01:00:5e:00:00:fc)
 + Internet Protocol Version 4, Src: 10.123.41.51 (10.123.41.51), Dst: 224.0.0.252 (224.0.0.252)
 + User Datagram Protocol, Src Port: 63928 (63928), Dst Port: 5355 (5355)
 + Link-local Multicast Name Resolution (query)

Notice!

Troubleshooting firewall rules

If computers cannot successfully ping each other after enabling the Windows firewall, ensure that the inbound and outbound firewall rules for **File and Printer Sharing (Echo Request - ICMPv4-In)** are enabled.

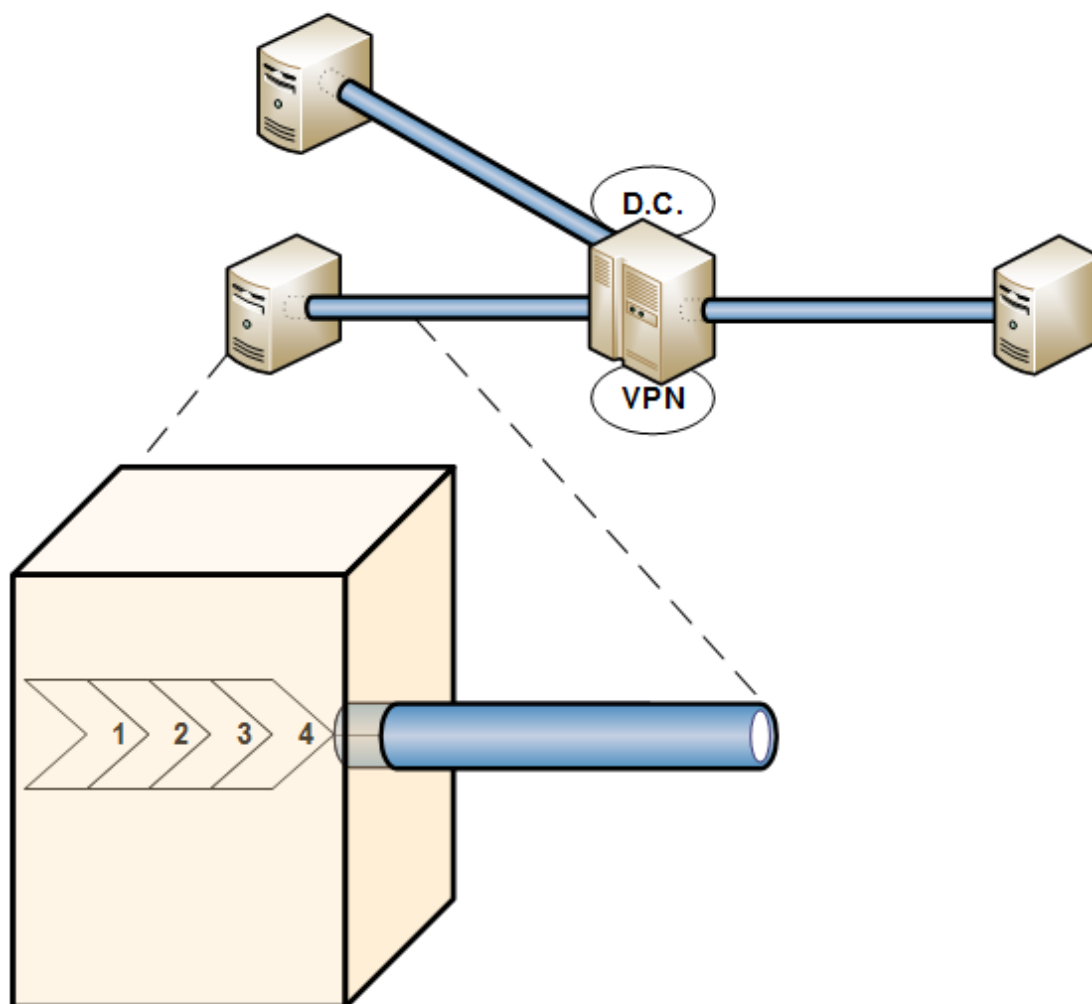
4.13**Tunnel mode configuration****Configuring Windows Server 2012 R2 as a L2TP/VPN Server**

Windows Server 2012 R2 must first be promoted to a Domain Controller, before the VPN can be set up and remote access enabled.

If this has already been done then proceed to the section *Set up the VPN, page 47*

Notice!

Note: The BIS server and VPN server should not be on the same PC

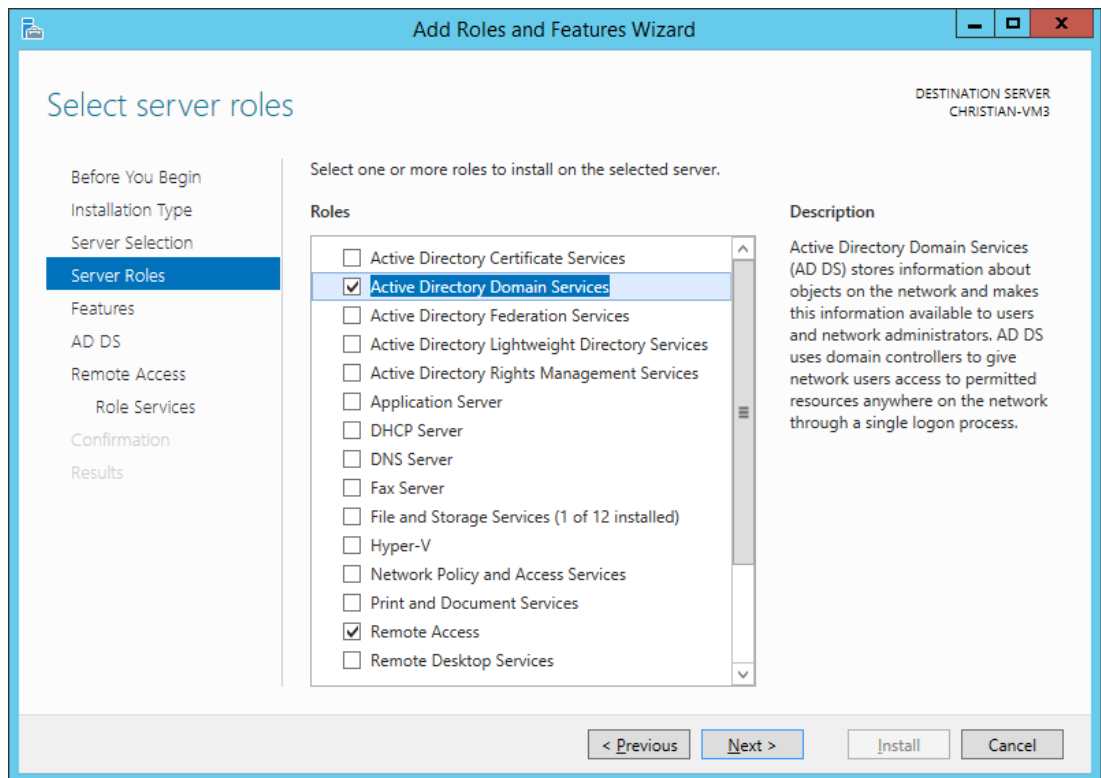


1	Application + IP socket	D.C.:	Domain Controller (primary or secondary)
2	Virtual NIC + Layer 2 Tunneling Protocol (L2TP)		
3	IPsec (IP security protocol)	VPN	Virtual Private Network server (software)
4	NIC (Network Interface card)		

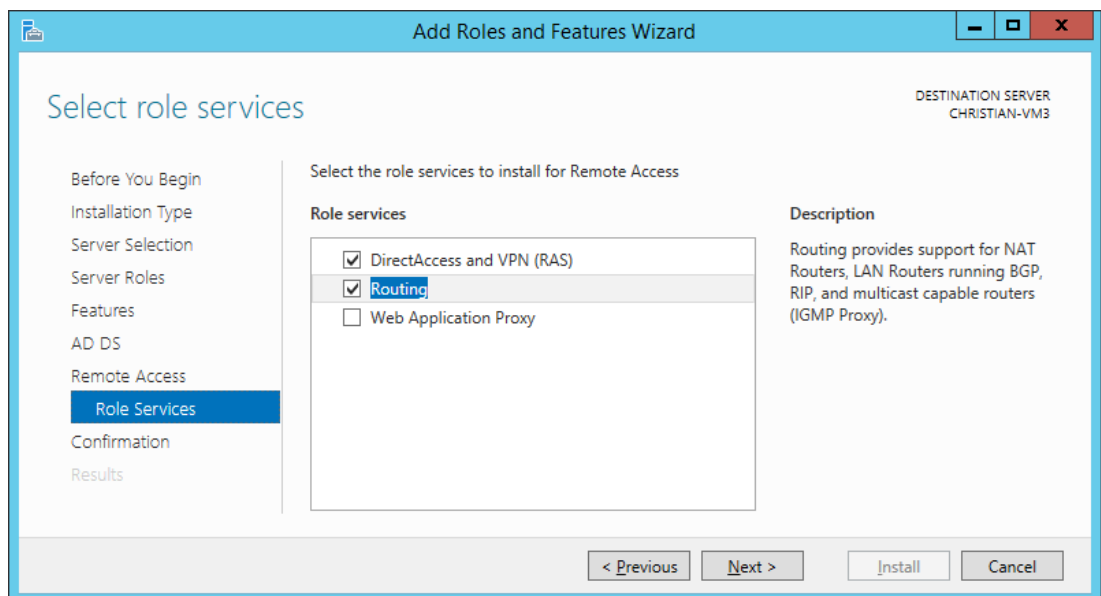
4.13.1

Promote the Windows Server to a Domain Controller

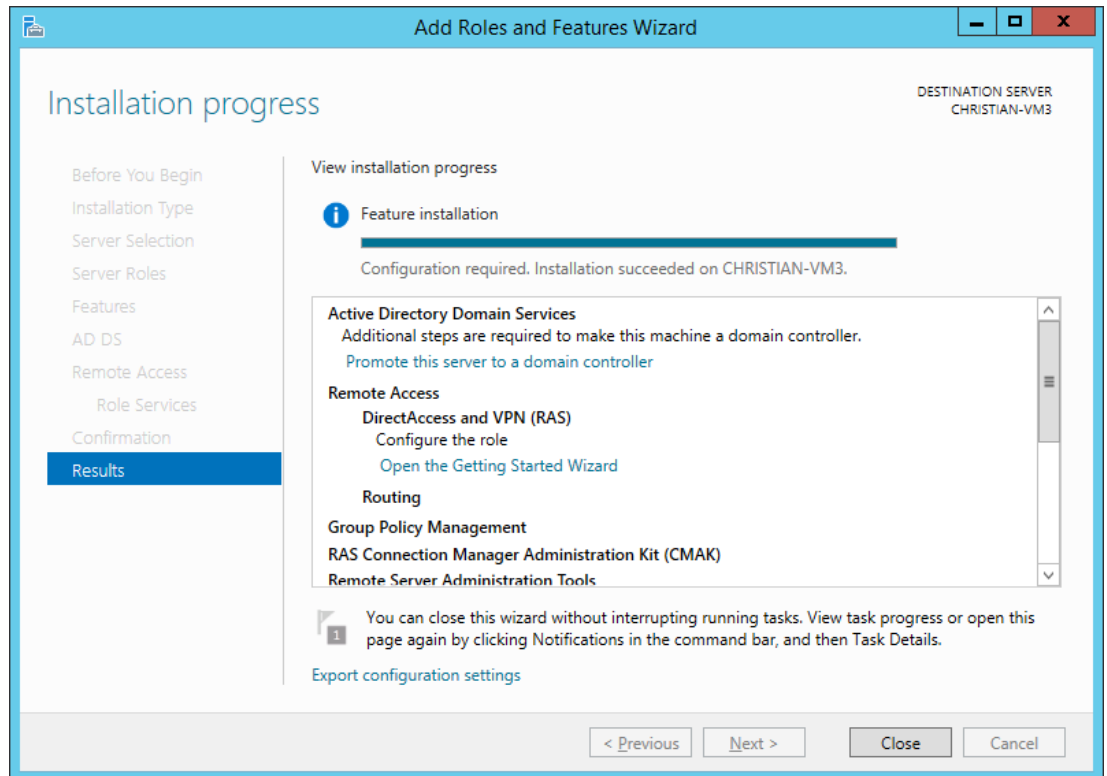
1. Open Server Manager and click **Manage > Add Roles and Features > Select Active Directory Domain Services** and **Remote Access**



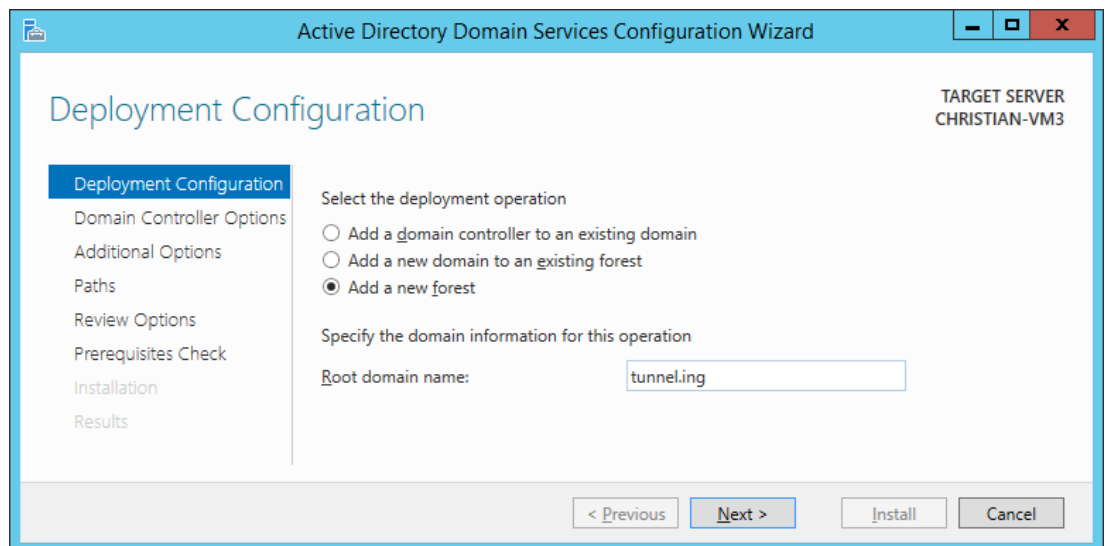
2. Under **Remote Access > Role Services**, select both **DirectAccess and VPN (RAS)** and **Routing**
Click **Next** and then **Install**



3. Click **Promote this server to a domain controller**



4. On the **Deployment Configuration** page select **Add a new forest** and click **Next**



5. On the **Domain Controller Options** page, set a password and click **Next**

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes standard Windows window controls. The main heading is 'Domain Controller Options'. In the top right corner, it says 'TARGET SERVER CHRISTIAN-VM3'. On the left, a vertical navigation pane lists the steps: Deployment Configuration, Domain Controller Options (highlighted), DNS Options, Additional Options, Paths, Review Options, Prerequisites Check, Installation, and Results. The main content area is titled 'Select functional level of the new forest and root domain'. It contains two dropdown menus: 'Forest functional level:' and 'Domain functional level:', both set to 'Windows Server 2012 R2'. Below these, the section 'Specify domain controller capabilities' has three checkboxes: 'Domain Name System (DNS) server' (checked), 'Global Catalog (GC)' (checked), and 'Read only domain controller (RODC)' (unchecked). Further down, the section 'Type the Directory Services Restore Mode (DSRM) password' has two password fields labeled 'Password:' and 'Confirm password:', both filled with dots. At the bottom right of the main area is a link 'More about domain controller options'. The bottom of the window features four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

6. On the **DNS Options** page click **Next**

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window at the 'DNS Options' step. The title bar is the same. The main heading is 'DNS Options'. The target server remains 'CHRISTIAN-VM3'. The left navigation pane now highlights 'DNS Options'. A yellow warning banner at the top of the main content area states: 'A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found...' with a 'Show more' link and a close button. Below the banner, the section 'Specify DNS delegation options' contains a single checkbox labeled 'Create DNS delegation', which is currently unchecked. At the bottom right of the main area is a link 'More about DNS delegation'. The bottom of the window features the same four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

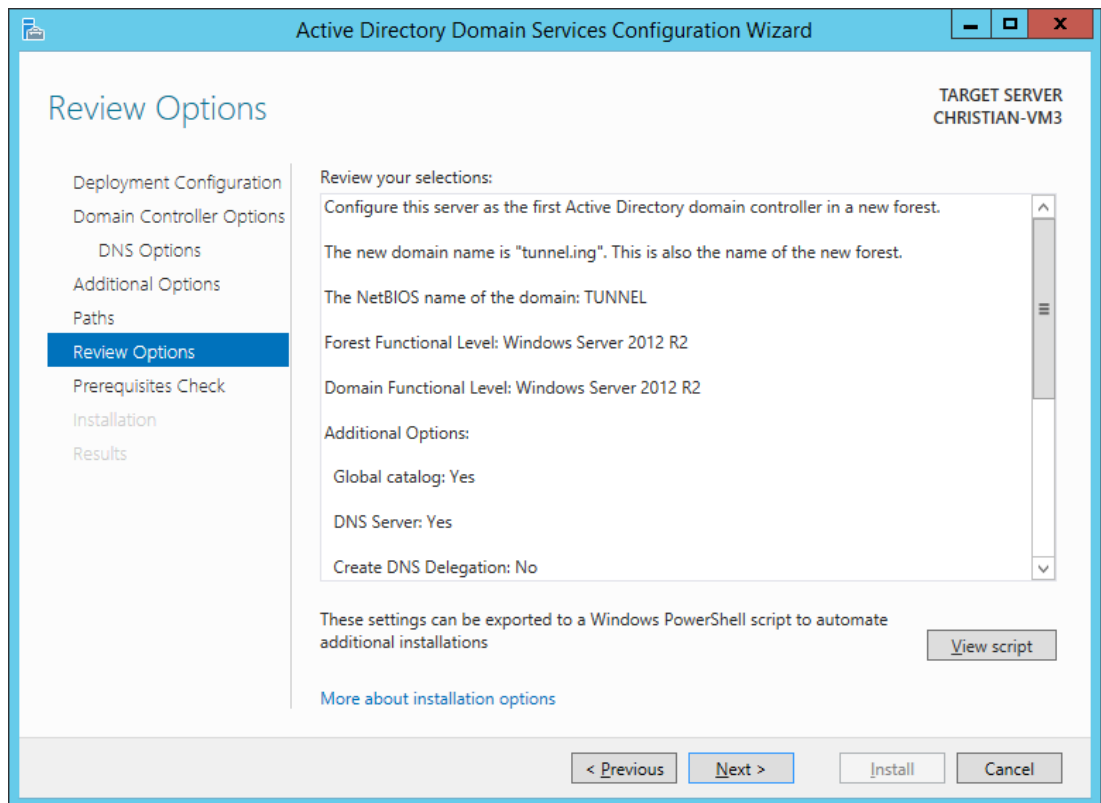
7. On the **Additional Options** page, verify the NetBIOS name and click **Next**

The screenshot shows the 'Additional Options' page of the Active Directory Domain Services Configuration Wizard. The title bar reads 'Active Directory Domain Services Configuration Wizard'. On the right, it says 'TARGET SERVER CHRISTIAN-VM3'. The left sidebar contains a list of steps: Deployment Configuration, Domain Controller Options, DNS Options, Additional Options (highlighted), Paths, Review Options, Prerequisites Check, Installation, and Results. The main area is titled 'Additional Options' and contains the text 'Verify the NetBIOS name assigned to the domain and change it if necessary'. Below this, it says 'The NetBIOS domain name:' followed by a text box containing 'TUNNEL'. At the bottom right of the main area is a link 'More about additional options'. The bottom of the window has four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

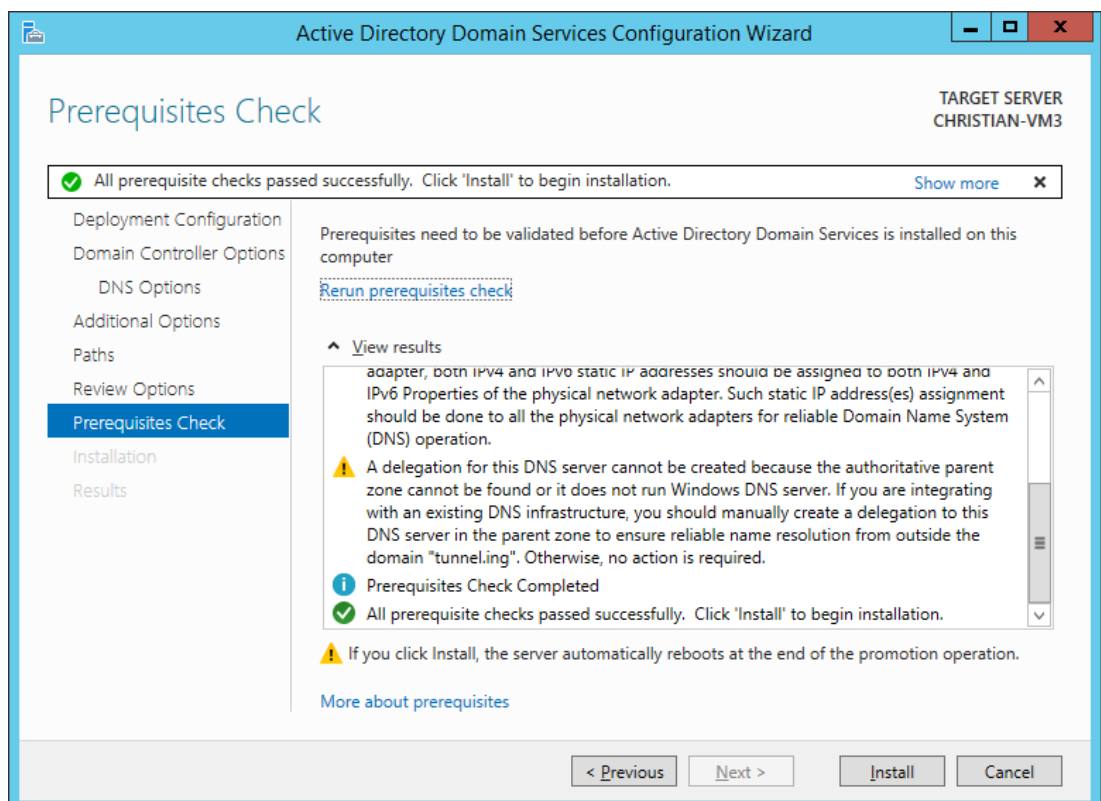
8. On the **Paths** page, click **Next**

The screenshot shows the 'Paths' page of the Active Directory Domain Services Configuration Wizard. The title bar reads 'Active Directory Domain Services Configuration Wizard'. On the right, it says 'TARGET SERVER CHRISTIAN-VM3'. The left sidebar contains a list of steps: Deployment Configuration, Domain Controller Options, DNS Options, Additional Options, Paths (highlighted), Review Options, Prerequisites Check, Installation, and Results. The main area is titled 'Paths' and contains the text 'Specify the location of the AD DS database, log files, and SYSVOL'. Below this, there are three rows of text boxes with folder paths: 'Database folder:' with 'C:\Windows\NTDS', 'Log files folder:' with 'C:\Windows\NTDS', and 'SYSVOL folder:' with 'C:\Windows\SYSVOL'. Each text box has a browse button (three dots) to its right. At the bottom right of the main area is a link 'More about Active Directory paths'. The bottom of the window has four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

9. On the **Review Options** page, click **Next**



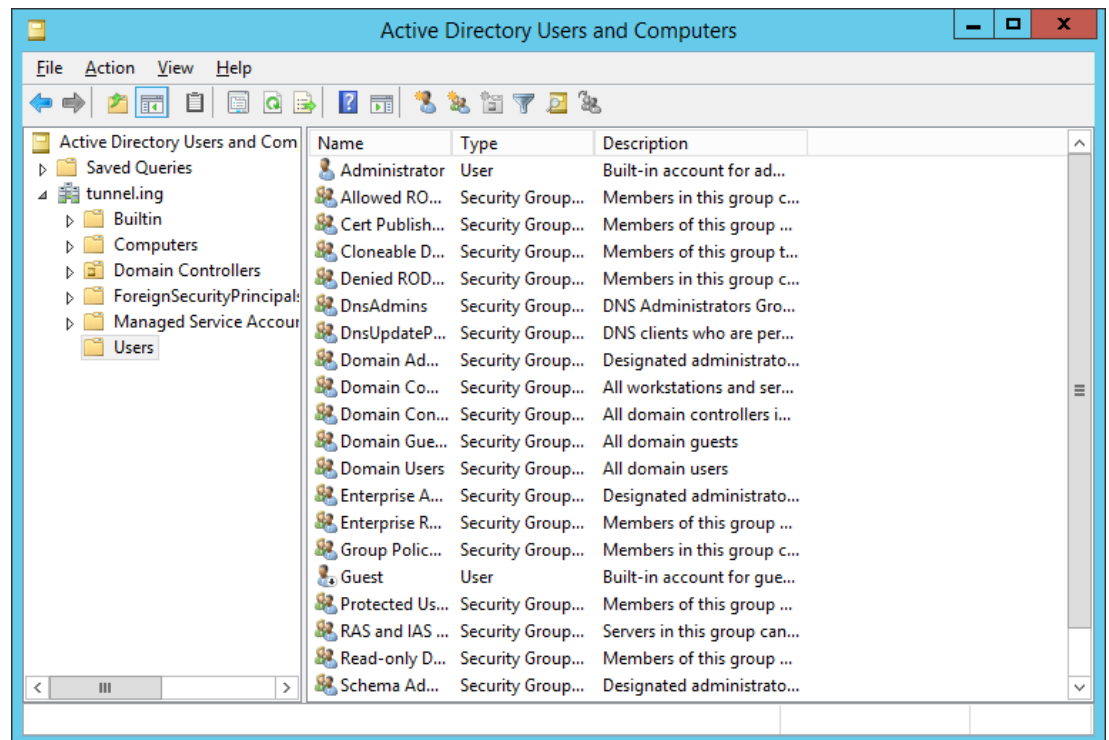
10. On the **Prerequisites Check** page, click **Install**



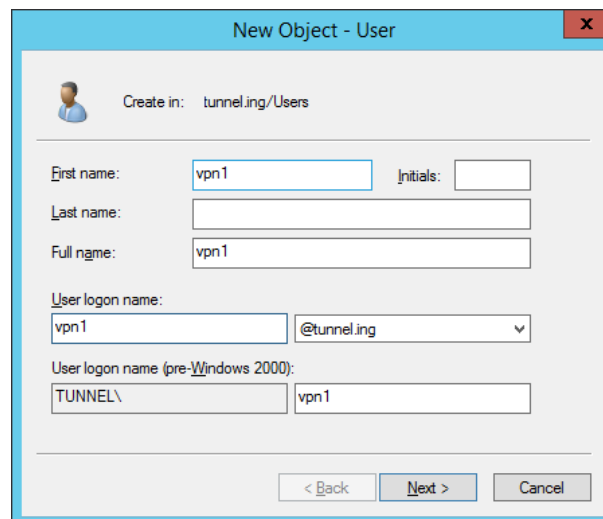
11. After Domain Services have been installed, you will be logged off and the server will restart. Login as an administrator under the created domain.

4.13.2 Set up the VPN

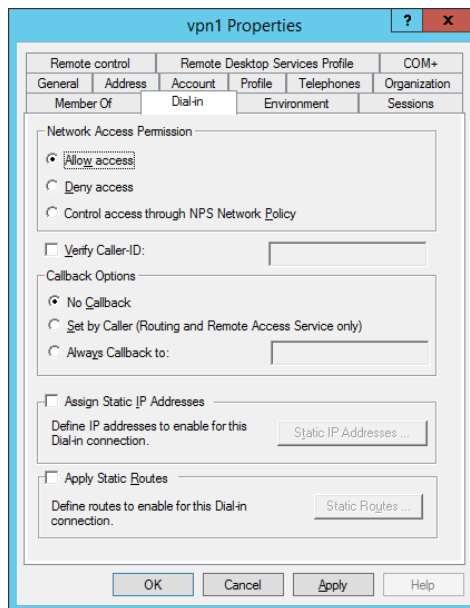
1. Under Windows open **Server Manager > Tools > Active Directory Users and Computers** to create a new user



2. Create a new user



3. Open the **Properties** of that user and click **Dial-in** tab. In the **Network Access Permission** group select **Allow access**



Notice!

Note:

There is an option to assign static IP addresses to users when they dial in. This option can be used to better manage the users and the machines that log on to the VPN server.

To use this option create one VPN user per VPN client and configure accordingly:

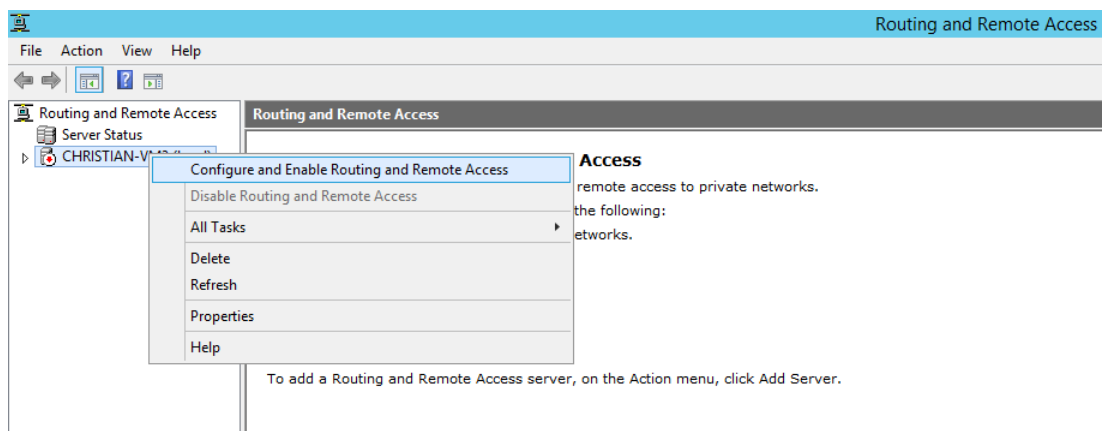
For example:

Assign user vpn1 to 192.168.10.2 where 192.168.10.2 is the Login server.

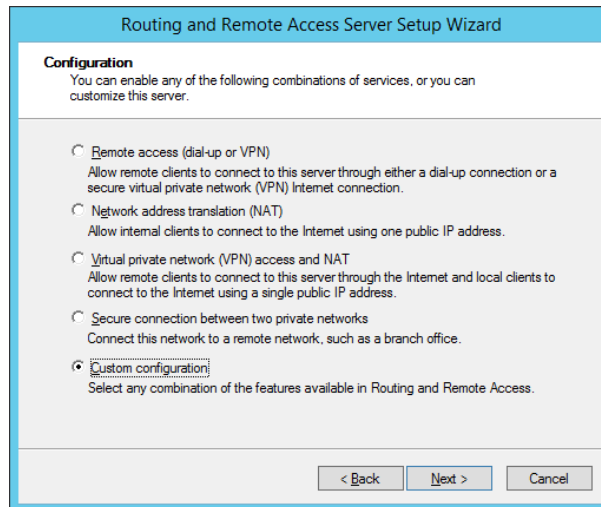
Assign user vpn2 to 192.168.10.3 where 192.168.10.3 is the first remote client.

And so on...

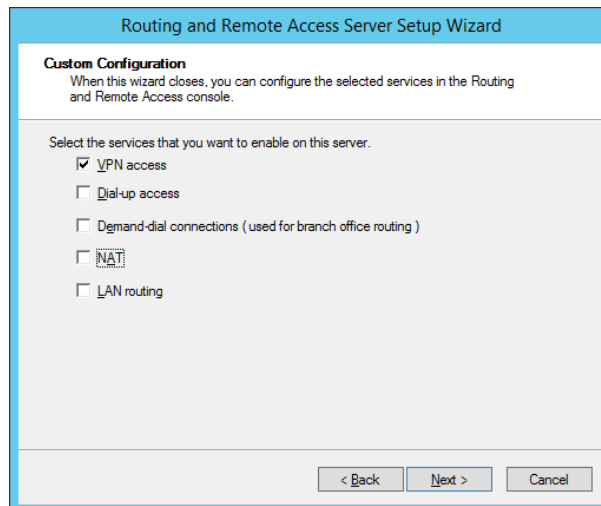
4. Open Server Manager > **Tools** > **Routing and Remote Access**. Right-click the server and select **Configure and Enable Routing and Remote Access**



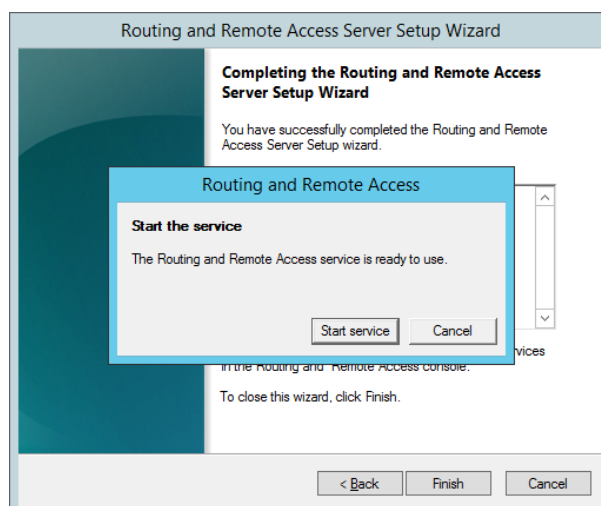
5. Select **Custom configuration** and click **Next**



6. Select **VPN access**



7. Click the buttons **Next** then **Finish** then, in the popup window, **Start service**

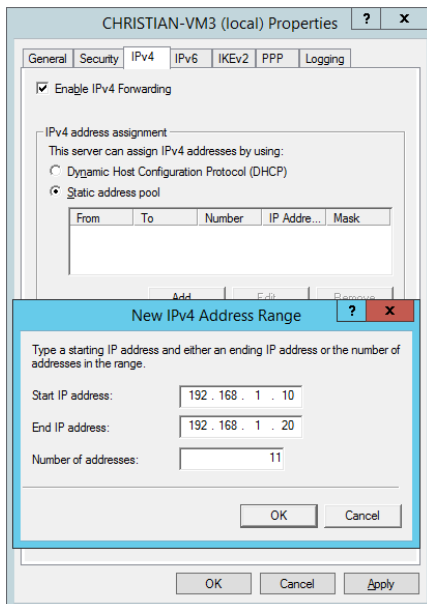


8. Open the properties of the server and click **IPv4** tab. Select **Static address pool** and enter the range of IP addresses that are to be assigned to connecting VPN clients.



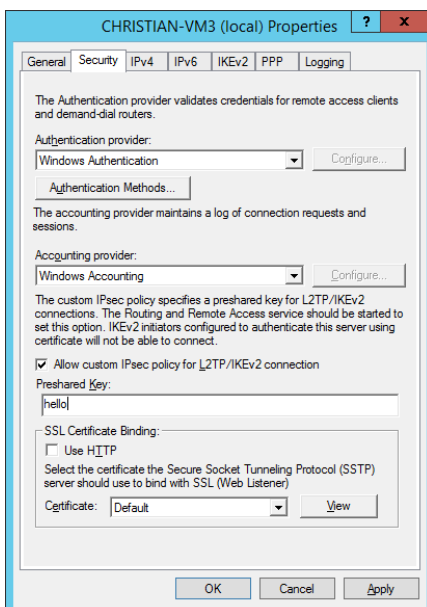
Notice!

Note: DHCP can be used instead of a static address pool for the assignment of IPv4 addresses. Please consult Microsoft documentation for the configuration of DHCP. Using DHCP will avoid the need to edit host tables (as described below) later in the procedure.



9. Encryption of the tunnel:

On the **Security** tab, set a **Preshared Key**, then click **OK**



10. A pop-up window will prompt you to restart **Routing and Remote Access**. Click **OK**

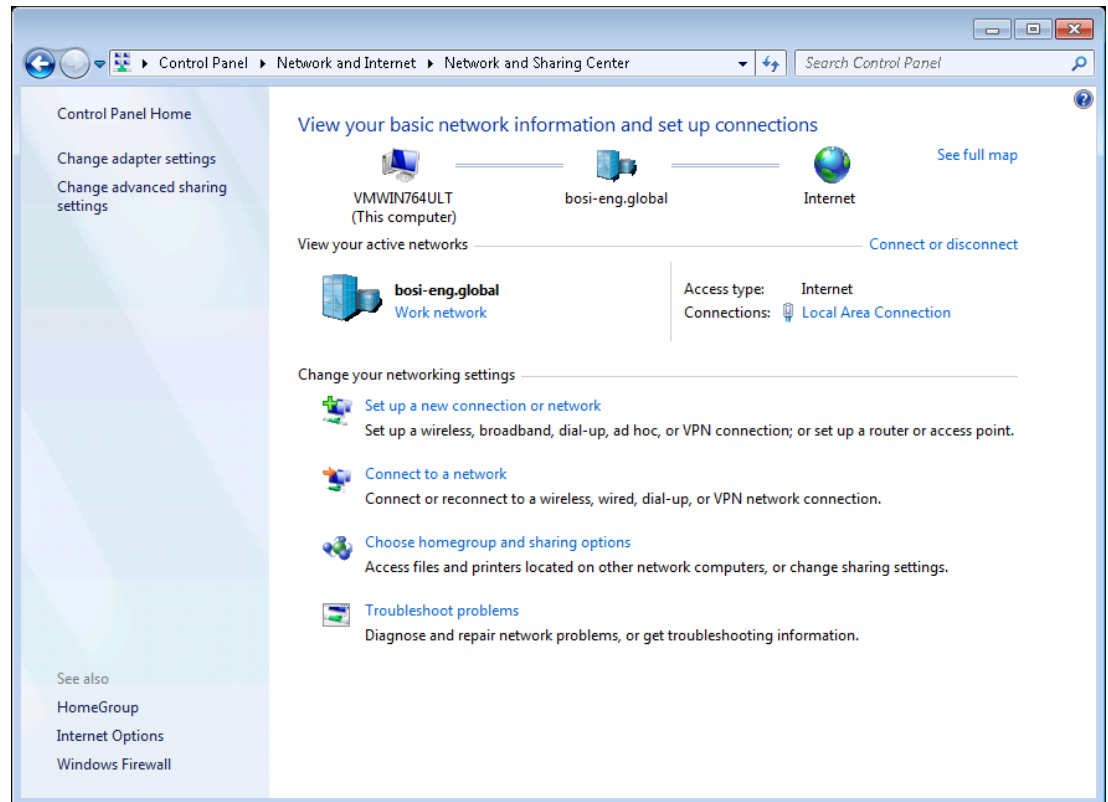
Result: The VPN server is now setup. We proceed to configuring the clients.

4.13.3

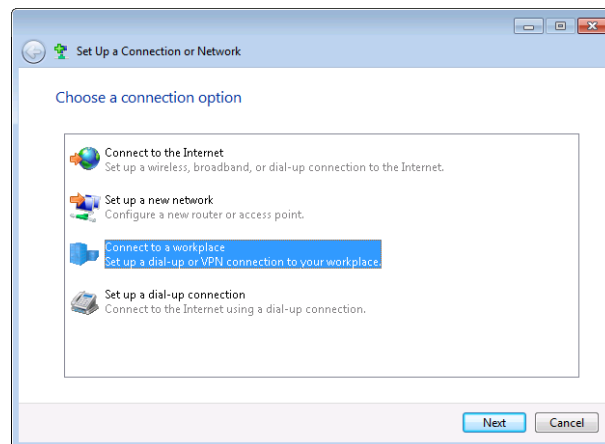
Configure the VPN clients

A VPN client in this context is a computer that sends and receives data via the VPN server that has been set up on the domain controller. The procedure for setting up this VPN server is described in the section *Set up the VPN*, page 47.

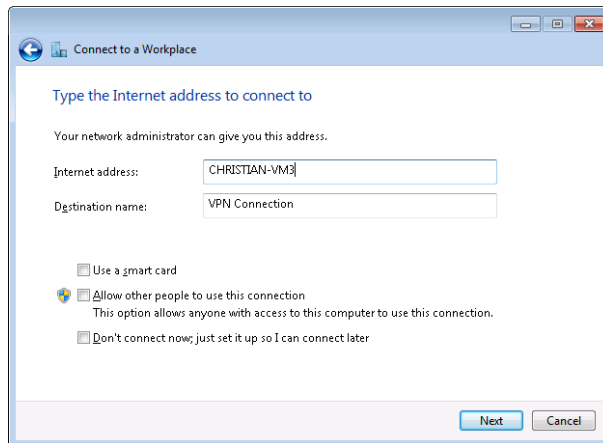
1. On each of the VPN client machines, go to **Network and Sharing Center** and select **Set up a new connection or network**



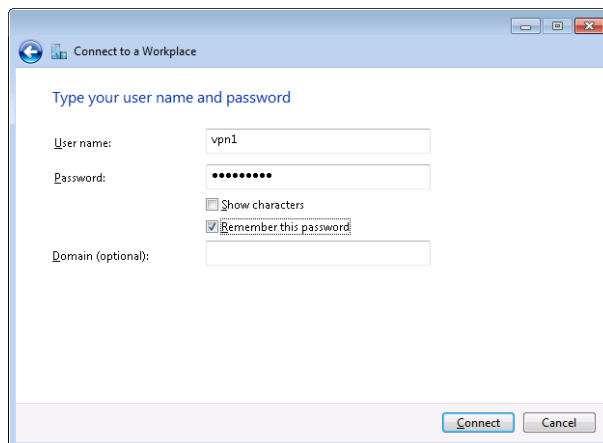
2. Select **Connect to a workplace** and click **Next**.
Take the settings **Use my Internet connection (VPN) > I'll set up an internet connection later**.



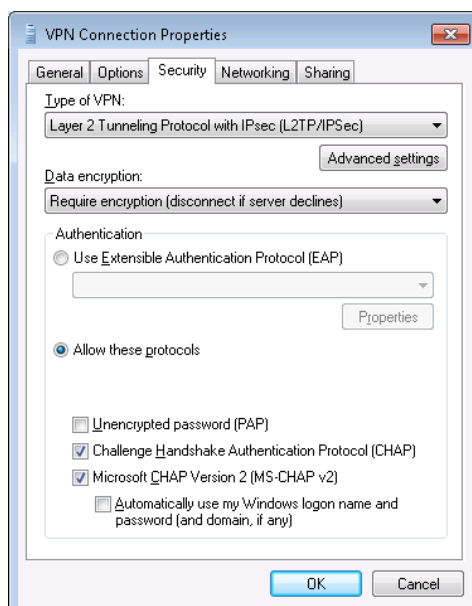
3. On the Connect to a Workplace page, enter the hostname of the VPN server



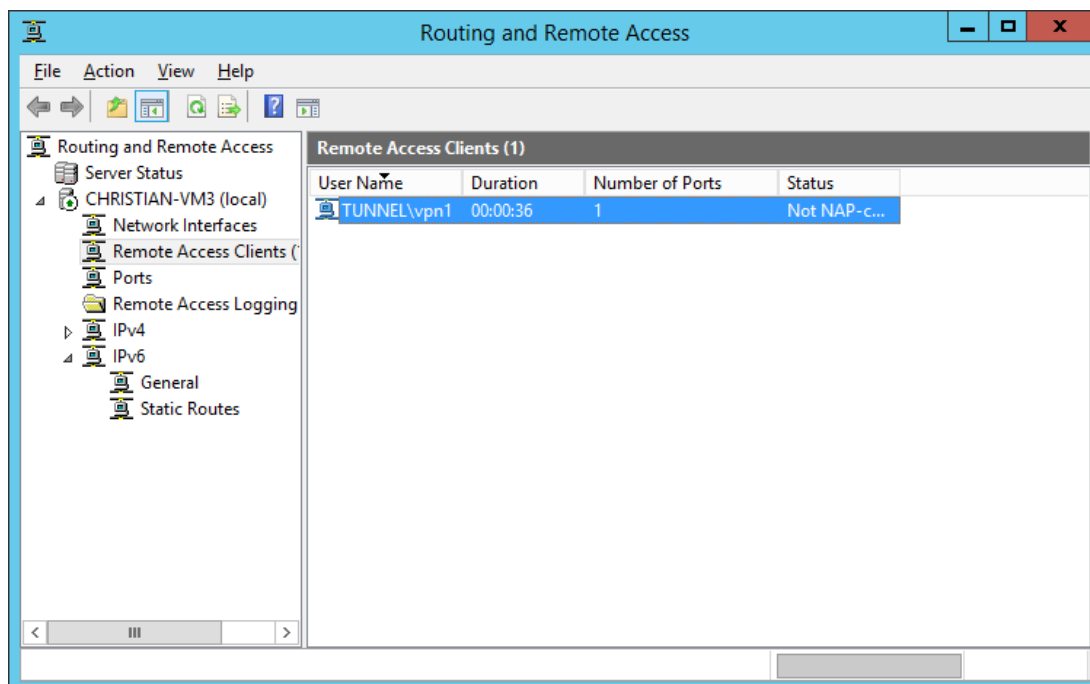
4. Enter the user that you created earlier in the Active Directory, in this case vpn1



5. Go to **Network Connections** and open the Properties of the VPN adapter.
 6. Go to **Security** tab and select Type of VPN **Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)** from the pull-down list.
 7. Click the **Advanced settings** button and enter the same **Preshared key** as you entered the VPN server)



8. On the VPN Server machine start the Routing and Remote Access application and verify that the **Remote Access Client** that you have just set up is visible.



9. The VPN client machine is now connected to the VPN Server. Repeat the steps in this section for all the other clients: (Login Server, Remote Client, SQL Server, and Connection Server).

4.13.4 Direct data traffic through the tunnel



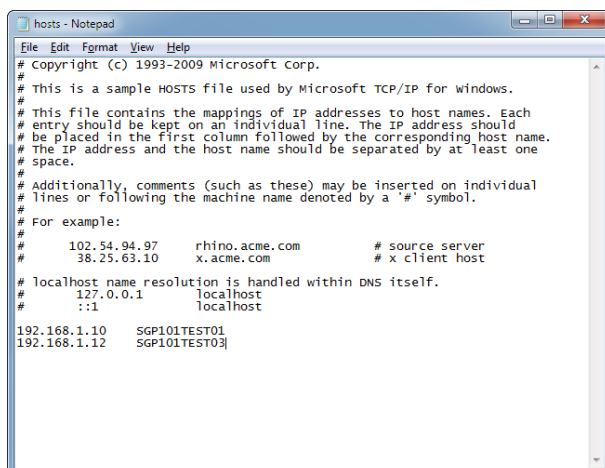
Notice!

Note that the procedure described in this section is not required if a Domain Name Server (DNS) is running on the Domain controller/VPN server.

When a computer connects to the VPN server, it will be assigned a new IP address. In effect, the computer will now have 2 IP addresses that both resolve to the same network name.

- 1 going through the VPN,
- 1 going through the normal network connection.

In order to force the computer to connect via the IP address where the tunneling occurs, you can add that IP address, with its host name, to the hosts file of each VPN client computer. The hosts file is located under: *C:\Windows\System32\drivers\etc*



```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com   # source server
#       38.25.63.10       x.acme.com      # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
192.168.1.10   SGP101TEST01
192.168.1.12   SGP101TEST03
```

**Notice!**

In the scenario described above, there is no need to enable the Firewall and set any security rules on each machine, as the intercommunication will be through the VPN tunnel.

4.14 AMS user profiles for third party products

When using third party products connected to AMS (for example Milestone video management software XProtect), an AMS user has to be configured during Milestone setup to communicate with AMS in operation. For security reason, a special user should be configured in AMS, having only permission to AMS functionality which is needed. This can be done by configuring a dedicated user profile with restricted permissions. This user profile is then to be assigned to this special user.

4.15 Usage of Milestone XProtect

When using third party product Milestone video management software XProtect, the following issue has to be considered.

The AMS - XProtect plugin communicates with AMS services using HTTPS. If the XProtect server and AMS server are on a separate computer, AMS certificate has to be imported on the XProtect server to establish trust with the AMS server for HTTPS communication. Due to a bug in XProtect, the trust validation is turned off, allowing HTTPS communication without installing the certificate. This bug is verified in:

- XProtect 2018 R3 Corporate
- XProtect 2019 R2 Professional+
- XProtect 2019 R2 Corporate+

Other variants e.g. Expert 2019 R2, Professional 2019 R2, Express+ 2019 R2 and Express 2019 R2 might also be affected.

This bug is not present in:

- XProtect 2018 R3 Professional and possibly older versions

We recommend to import AMS certificate regardless, so that bug once the bug is fixed by Milestone the integration will continue to function.

4.16 Usage of OSS-SO

It must be assured that all OSS-SO components are properly installed and configured:

- No LAN-sockets should be exposed to the outside of the system.
- Online-Readers must be properly installed to not expose any attack surface into the Network.
- All signal converters (Ethernet to RS485) must be protected and all standard passwords must be replaced.
- Disable connection interfaces (like telnet) on all signal converters.

A configuration-file is imported into the system. It should be assured this file was not altered by an unauthorized person. Any swap of door IDs could lead to a misconfigured cardholder that has unwanted access rights to an area.

4.17 Offline Access Systems

In an offline access system, any change to an authorization profile of a cardholder is not immediate. This includes actions like blacklisting a cardholder. Any change will only take effect when the targeted cards are presented to an online-reader.

This should be communicated to all staff members interacting with the access system.

4.18 Connection of AMCIPConfig tool to AMC

Recommended option for implementing DTLS encryption on local access controllers (AMCs):

To have a maximum secure connection between the AMCIPConfig Tool and the AMC within the provisioning phase, it is recommended to choose the option “Use Display Key” in the AMCIPConfig Tool.

4.19 Security advices for PHG key management

Reader Config Tool

On DMS level a new standalone utility named ReaderConfigTool, to create sets of reader parameters is provided. This utility is given to customers to prepare their readers and does not need any other parts of the DMS software to be installed and running.

The set of reader parameter is stored in an encrypted file which has to be imported on DMS Device Editor. The file is password protected. The password is needed to import the file in Device Editor and to open the file in the Reader Config Tool for changes.

The following advices have to be followed to ensure the security of the password:

- It is in the responsibility of the customer to take care that no one compromises the password when entered or compromises the password when transmitted.
- It is in the responsibility of the customer to protect the system that no one installs a software to record the password when entered.

- It is in the responsibility of the customer to take care that no one steals the password when transmitted from Reader Config Tool to the DMS Dialog. The password should be transmitted on a different way than the encrypted parameter file.

The sets of reader parameter have to be imported in the Device Editor on DMS level.

- It is in the responsibility of the customer to take care that all hard disks of the system are encrypted (hardware encryption by controller better than by operating system) and enough memory is installed to prevent that the OS creates pagesys files. The pagesys files could be misused to reconstruct the password.

5

Secure operation

5.1

BIS password management

The ChangePassword tool

This tool is mandated for system administrators as the only tool for managing the passwords of BIS internal service users, both for the Windows operating system and for SQL server.

Note:

1. If the DbUserInfo.crp password file has been accidentally deleted, use the tool to update the Mgts-SSRSViewer password, and then update all the other SQL users' passwords with the tool.
2. If a remote SQL instance is used, then the tool will update both local machine and also the remote SQL machine, prompting for the remote admin username and password if required.
3. If connection servers are used, run this tool on each connection server separately to change the Mgts-Service user account password. Make sure the same password is used in all the servers. Similarly if a multi-server BIS environment is used, run the tool on both the machines (provider and consumer) separately, in order to ensure the same Mgts-Service password throughout.

5.2

Password security advice

When starting the dialog manager after Installation of the AMS, the Login window asks for the login with predefined administrator credentials. After successfully logged-in, the System will automatically ask for a new administrator password.

For security reasons it is recommended that you use the following strong password policy for the new administrator password and also for all other passwords within AMS:

- Easy to recall
- At least 8 Symbols
- Should contain:
 - Upper letter
 - Lower letter
 - Digits
 - Special characters
- Should not consist of:
 - Names of family members, friends or pets, birthdates, favorite Rockstar and so on
 - Words which appear in dictionaries
 - No coherent digits or characters like "12345" or "qwert7890"
- Do not complement a simple password by just adding common special characters or digits to the front or to the end
- Do not force user to change the password in frequent time intervals. Because that will lead to bad passwords. Change the password if a good reason exist like that the account or base system is compromised.
- Use a Tool to verify that the Password is "strong"

5.3 Data privacy

5.3.1 General Data Protection Regulation (GDPR)

The GDPR documents mentioned in this chapter refer to product BIS Access Engine, but the documents are also valid for product AMS. For accessing the documents, special “GDPR - Data Protection” permission is needed. The permission can be requested when browsing the documents by using the links.

Bosch Access Control Systems - GDPR

The GDPR was enforced on the 25th of May 2018. As a regulation it was directly applicable to all EU member states without the need for national legislation. As information processed and stored by Bosch access control systems is classified as "sensitive" the GDPR has impact on these systems. Find information about GDPR recommendations at: www.gdpr.org/

5.3.2 Deactivation of BIS-ACE logfiles

By default, BIS performs careful logging of the actions of operators and system components. In some circumstances however the unencrypted BIS server and client logs may present an unacceptable security risk. In this case you can consider disabling these logs.

BIS provides a set of batch command files for disabling all those logs that are normally written to the folder `C:\S3k_Logging\`. The batch files are executed only on the BIS login servers and Connection servers.

Limitations of the batch files with regard to BIS installation logs

The following logs are written by the BIS installation script and are not affected by the batch file to disable logs. Note that these log files contain no security-critical information.

- **InstallIISforBIS**
- **BISSetupLauncher**
- **Escape-1**
- **Escape-2**
- **S3K_Logging\InstallationLogs**

Use of the batch files with regard to OPC servers

OPC servers built using the BIS OPC Framework V4.2 and later (`OPCServerFrameworkExe.exe`) will be affected by the batch files.

OPC servers that were built using older versions of the BIS OPC Framework need to be rebuilt using the 4.2 version before they will be affected.

Limitation

- OPC servers developed by third parties, not using the BIS OPC Framework 4.2 and later, are **not** affected by the batch files. They will continue logging.

Locating the batch files

The batch files can be found in the following folder in the BIS installation medium:
_Install\Tools\DisableLogs\

Disabling logs

1. On the BIS login or connection server, right-click the following batch file and select Run as administrator
DisableLogs.bat
2. You will be asked to confirm your decision, and then a message window will confirm that logging has been disabled.
3. Wait for 15 seconds and then verify that BIS has stopped writing log files. You may use the batch file *DisplayCurrentLogStatus.bat*.
4. Restart the BIS clients.

Contents of the S3k_logging folder

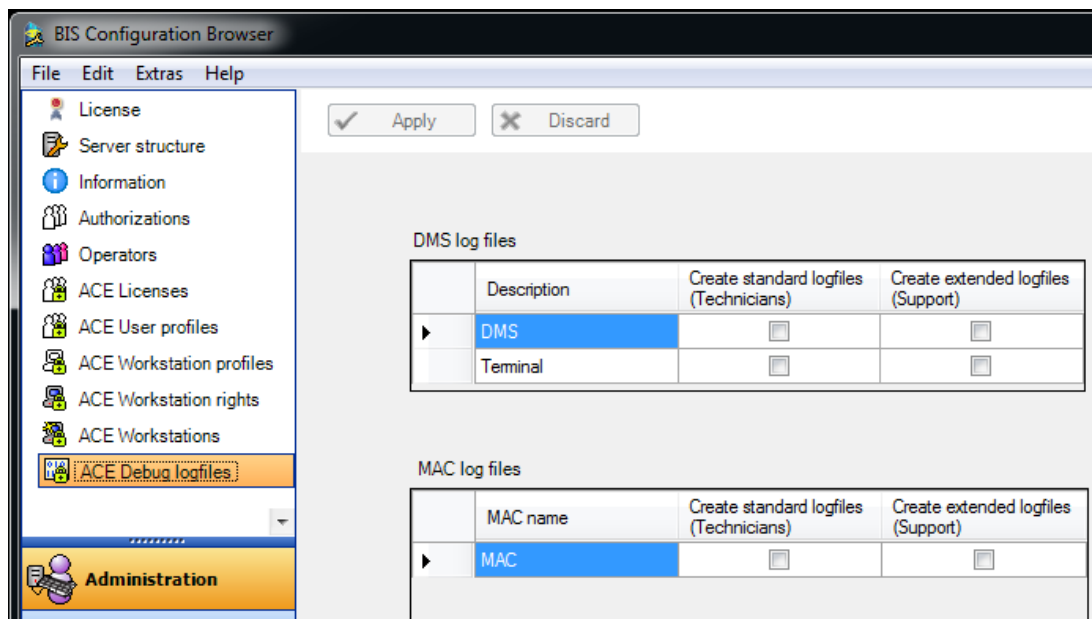
Once logging has stopped you can delete the files within the folder *C:\S3k_Logging*, however it is recommended **not** to delete the folder structure itself.

- If the empty folders are retained then logging can resume immediately when you re-enable logging.
- If the folders are deleted then you will need to restart the BIS server in order to re-create them before logging can resume.

Deactivation of ACE logfiles

To configure the logging for ACE components select the dialog **Administration > ACE Debug logfiles**.

The right to make changes in this dialog must be assigned under the dialog **Administration > ACE User Profiles** dialog.



DMS log files

Under DMS log files you can configure two kinds of logging:

1. **DMS** - All the logs created by server processes.
2. **Terminal** - All logs created by ACE workstation and Configuration Browser dialogs.

MAC log files

Under MAC log files you can configure logs created by the Main Access Controller.



Notice!

MAC restarts automatically

If you make and apply an changes to the log file check boxes, then the MAC process will restart automatically. During the usually short restart period, it will not be able to handle access requests.

Clear all of the checkboxes (default setting) if the default minimal logging is sufficient.

Note that clearing the check boxes does not delete existing log files. Delete the files manually if they are no longer required.

5.3.3

Deactivation of AMS logfiles

Execute the following steps in order to deactivate Debug Logfile creation on the AMS server:

- Login to **Dialog Manager**
- Navigate to Dialog **Configuration > Options > Debug logfiles**
- Clear all checkboxes for “DMS log files” and “MAC log files”
- Click **Save** to save changes

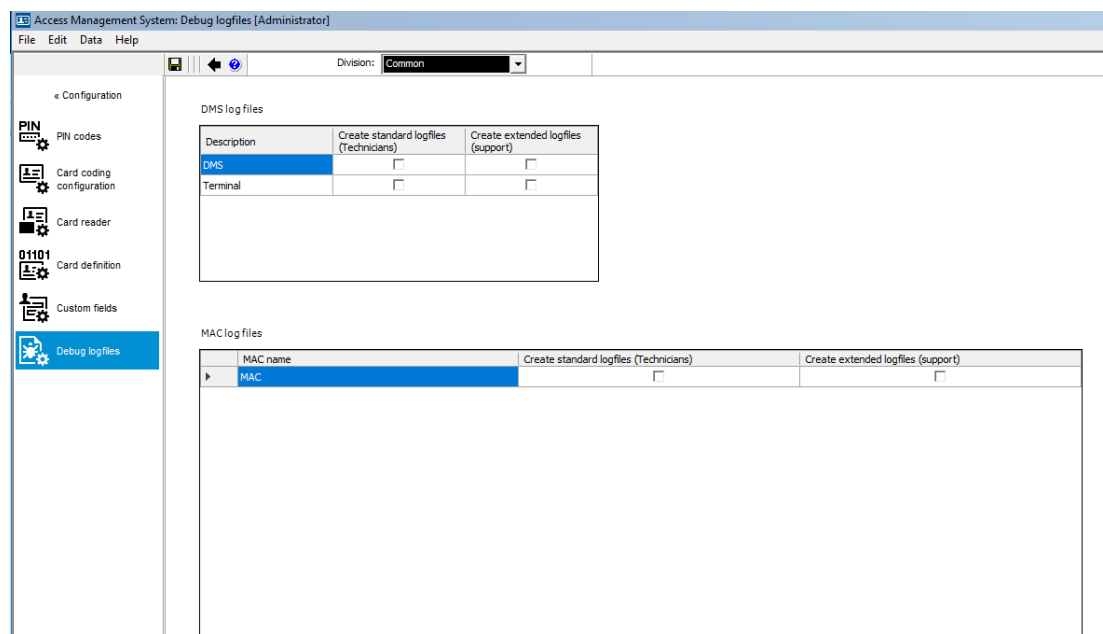


Figure 5.1:

Verify logging has stopped:

- Open file DMSTELE.log in path [install-path]\AccessEngine\MAC\BIN
- Verify last entry “end logging at [date time]”
- In case Debug Logging was never enabled, the file does not exist.

6 Security update management

Update of the AMS System:

With each release, the software will be deinstalled first and installed with the new version again.

The configuration will be kept.

Fresh Installation (deinstallation of the AMS System and Installation of a new Release afterwards):

The configuration will not be kept.

The system provides the possibility to export database and configuration. After a fresh installation, it is possible to import the existing data / configuration.

7 Secure decommissioning

Confidential and sensitive data, e.g. personally identifiable information (PII), certificates or credentials, should be deleted and destructed in a secure manner, where it is appropriate. This section describes deletion of data incl. passwords at the end of lifetime or at a factory reset.

Secure dispose of OPC UA certificates

The BIS uninstallation procedure will not delete the certificates created for OPC UA server connection. Delete these certificates manually from <BIS installation drive>:\Mgts\PKI.

LDAP Security Advice

An AD (Active Directory) user will remain logged in, even after the user is deleted in AD. Verify that the user is logged out before deleting the AD user.

The Windows Server 2012 LDAP host is vulnerable to MS17-010 and can get full access to the Active Directory Domain Controller. Check, that the latest Microsoft security patches are installed.

7.1 Deinstallation of BIS

1. First stop the BIS Server in the BIS manager tab:**System Start/stop** > Button:**Stop Server component**
2. Deinstall the BIS Software via standard Microsoft Windows software administration, e.g. under Windows 7 click **Start** > **Control Panel** > **Programs and Features** . The computer lists all installed software packages. From this list select **BIS - Building Integration System**, click the **Remove** button and follow the directions given by the configuration program
3. In the same way, remove any packages whose names start with "BIS".
4. Reboot the computer after deinstallation

This does not remove third party products, such as Microsoft SQL Server. You will need to deinstall the third party products individually as so desired.

7.2 Deinstallation of AMS via client setup

Assumptions for installed components:

Microsoft Visual C++ 2010 Redistributable (x86)

Microsoft Visual C++ 2019 Redistributable (x86)

Access Management System - Client

Access Management System - Map View

Under the assumption, that the default installation path has not changed:

Installation folder:

C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System

Deinstallation

Deinstallation by executing "Uninstall of Access Management System - Client" in **Windows Programs and Feature**. Deinstallation of components:

- Access Management System - Client
- Access Management System - Map View

The following components have to be deinstalled manually:

- Microsoft Visual C++ 2010 Redistributable (x86)

- Microsoft Visual C++ 2019 Redistributable (x86)

Results:

The following logfiles and path have to be manually removed:

- *C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Client\Bin\DlgMgr.log*
- *C:\ProgramData\Bosch Sicherheitssysteme\Access Management System\Logs*.log*
- The manually installed Certificate “Access Management System Internal CA” has to be manually removed.

The Registry entries under “Micos SPS” and “Bosch Sicherheitssysteme” are removed by the deinstallation.

7.3 Deinstallation of AMS via server setup

Assumptions for installed components:

SQL Server 2017 Express
Microsoft Visual C++ 2010 Redistributable (x86)
Microsoft Visual C++ 2019 Redistributable (x86)
Access Management System - Server
Access Management System - Access API
Access Management System - Map API
Access Management System - States API
Access Management System - Certificates
Access Management System - Alarms API
Access Management System - Events API
Access Management System - Map View API
Rabbit MQ
Erlang

Under the assumption, that the default installation path has not changed:

Installation folder:

C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System

Deinstallation

Deinstallation by executing “Uninstall of Access Management System - Server” in **Windows Programs and Feature**. Deinstallation of components:

- SQL Server 2017 Express (optional)
- Access Management System - Server
- Access Management System - Map API
- Access Management System - MapView API
- Access Management System - States API
- Access Management System - Certificates
- Access Management System - Alarms API
- Access Management System - Events API
- Access Management System - Map View API
- Access Management System - Identity Server

The following components have to be deinstalled manually via Windows Control Panel:

- Microsoft Visual C++ 2010 Redistributable (x86)
- Microsoft Visual C++ 2019 Redistributable (x86)
- Rabbit MQ
- Erlang

Results (see PBI 193964 ACE/S Setup: Uninstall)

- Most of ACE components (except SQL Server) were uninstalled
- ACE services (DMS MAC) were shut down
- ACE components (installed by Windows Installer on ACE setup) were removed
- If the SQL Server instance had been selected for uninstall, the MAPS and STATES part of the SQL database is deleted, but the AMS part remains.
- The Programs and Features list was correctly updated
- Artifacts generated by the running ACE system after Installation are not removed and have to be removed manually
- Backup files
 - C:\Program Files\Microsoft SQL Server\[SQL version]\[SQL Instance]\Backup*
 - C:\Users\[User name]\DOCUMENTS\Backups*
- Log files (DMS and MAC)
 - C:\ProgramData\Bosch Sicherheitssysteme\Access Management System\Logs*
- Logfiles for Rabbit MQ under
 - %appdata% \RabbitMQ\log*
- Logfiles for each API (enable “view hidden items” in windows file manager for AppData):
 - *C:\Users\AMSAccessApi\AppData\Roaming\Bosch Sicherheitssysteme\Access Management system\Logs*
 - *C:\Users\AMSAlarmsApi\AppData\Roaming\Bosch Sicherheitssysteme\Access Management system\Logs*
 - *C:\Users\AMSEventsApi\AppData\Roaming\Bosch Sicherheitssysteme\Access Management system\Logs*
 - *C:\Users\AMSMAPApi\AppData\Roaming\Bosch Sicherheitssysteme\Access Management system\Logs*
 - *C:\Users\AMSMAPViewApi\AppData\Roaming\Bosch Sicherheitssysteme\Access Management system\Logs*
 - *C:\Users\AMSSstatesApi\AppData\Roaming\Bosch Sicherheitssysteme\Access Management system\Logs*
- Logfiles for Identity Server under
 - C:\Users\AMSIIdentityServer\Roaming\Bosch Sicherheitssysteme\Access Management system\Logs*
- Import and Exports
 - C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\AccessEngine*
- Events (files)
- ACE-S database files; even if the SQL Server instance was removed
- MAC Shared
- MAC:
 - C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\AccessEngine\MAC\Db\Save\CTSUSCAT.FCS*

- Registry entries:
 - *HKEY_LOCAL_MACHINE -> SOFTWARE -> WOW6432Node -> Security systems*
 - *HKEY_LOCAL_MACHINE -> SOFTWARE -> WOW6432Node -> Micos -> MAC and SPS*

7.4 Deinstallation of AMS import/export tool

The AMS Import Export Tool is not part of the AMS Setup. It is an optional component with a dedicated Setup. The AMS Import Export Tool has to be deinstalled manually via Windows Control Panel. After deinstallation, the following artifacts have to be deleted manually:

- *C:\inetpub\wwwroot\ImportExportWebApp\Content\files\import*
- *C:\inetpub\wwwroot\ImportExportWebApp\Content\files\export*
- *C:\inetpub\wwwroot\ImportExportWebApp\logs*
- *C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\ImportExportACEWS\logs*

7.5 Deinstallation of AMS third party products

Simons&Voss Software "SmartIntego" has to be uninstalled manually on the Workstation under Programs and Features. Also the corresponding SmartIntego import files (.ikp) and export files (.csv) have to be manually deleted.

8 Appendices

8.1 Abbreviations used

ACE Access Control Engine
AES Advanced Encryption Standard
AMC Access Modular Controller
AMS Access Management System
API Application Programming Interface
BIS Building Integration System
BT Bosch Building Technologies
DMS Data Management System
GDPR General Data Protection Regulation
IP Internet Protocol
LAC Local Access Controller
MAC Master Access Controller
RPS Remote Programming System
SEP Security Engineering Process
SQL Structured Query Language
SSL Secure Sockets Layer. Obsolete: see TLS
TCP Transmission Control Protocol
TLS Transport Layer Security
UDP User Datagram Protocol

Glossary

1.MAC (first MAC)

The primary MAC (Master Access Controller) in a BIS Access Engine (ACE) or Access Manager (AMS) system. It can reside on the same computer as the DMS, but it can also reside, like a subsidiary MAC, on a separate computer known as a MAC server.

AES

The Advanced Encryption Standard (AES) is a worldwide standard specification for the encryption of electronic data

Connection server

(Hardware) A computer that runs OPC server software with which external devices communicate by OPC protocol. The BIS setup program can be used to turn a Windows system into a potential Connection server.

Local Access Controller (LAC)

A hardware device that sends access commands to peripheral access control hardware, such as readers and locks, and processes requests from that hardware for the overall access control system. The most common LAC is an Access Modular Controller or AMC.

NAT

Network address translation (NAT) is a technique for mapping one IP address space into another. It helps to avoid IPv4 address shortages.

RPS

Remote Programming Software. A program that manages fire or intrusion control panels on a network.

SSL

Secure Sockets Layer; an encryption protocol for data transmission in IP-based networks

TCP

Transmission Control Protocol. Connection-oriented communication protocol used to transmit data over an IP network. Offers a reliable and ordered data transmission.

TLS

Transport Layer Security; TLS 1.0 and 1.1 are the standard advanced developments of SSL 3.0 (see SSL)

UDP

User Datagram Protocol. A connectionless protocol used to exchange data over an IP network. UDP is more efficient than TCP for video transmission because of lower overhead.

Bosch Security Systems B.V.

Torenallee 49

5617 BA Eindhoven

Netherlands

www.boschsecurity.com

© Bosch Security Systems B.V., 2022

Building solutions for a better life.

202203181720