Building Integration System

en Cybersecurity guidebook

Table of contents

1 Security

Use latest software

Before operating the device for the first time, make sure that you install the latest applicable release of your software version. For consistent functionality, compatibility, performance, and security, regularly update the software throughout the operational life of the device. Follow the instructions in the product documentation regarding software updates.

The following links provide more information:

– General information: https://www.boschsecurity.com/xc/en/support/product-security/
– Security advisories, that is a list of identified vulnerabilities and proposed solutions: https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

Bosch assumes no liability whatsoever for any damage caused by operating its products with outdated software components.

2 Purpose of the document and target 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 responsibles of access control systems.

3 System concept and considerations

3.1 Background: What is BIS?

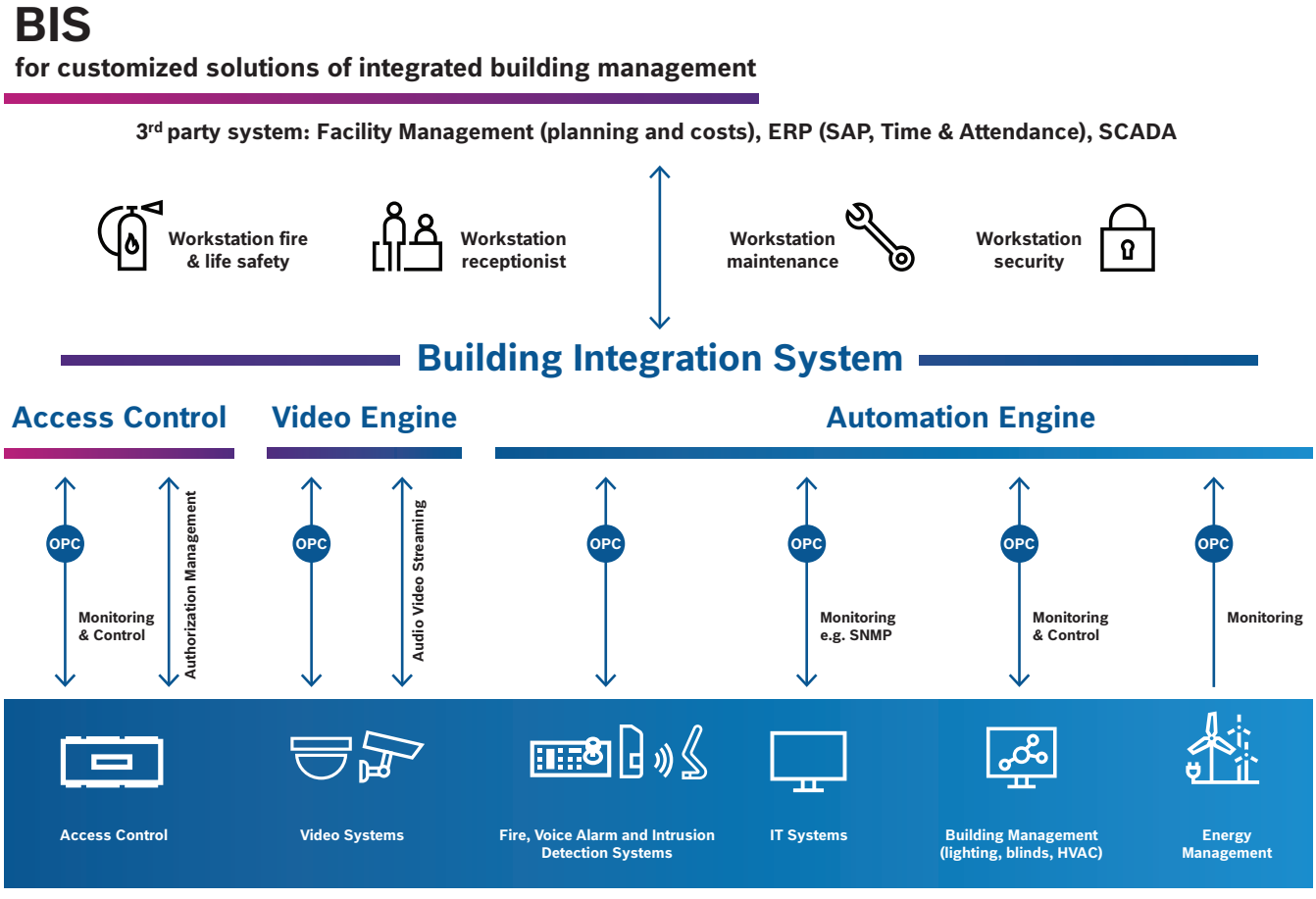
The Building Integration System (BIS) is a software hub that collects and prioritizes alarms and status messages from its connected subsystems. It continually decides on and carries out appropriate responses, based on a customized, programmable rule-set. If human intervention is required, BIS presents 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:

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

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

3.2 BIS overview



3.3 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.

3.3.1 BIS 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 SSO or Windows accounts for all operators of the access control system, and enforced password strength, see the section Rules for password strength 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.
- Opening of the enclosure of the user interface, intended to be installed outside of the controlled area or that could be accessible from outside the controlled area, shall result in tamper detection if manipulation of the internal elements can cause an access granted condition. The tamper detection shall occur before the tamper mechanism can be defected.
  - Bosch reader portfolio: Manipulation of the internal elements installed outside of the controlled area cannot cause an access granted condition. The tamper detection shall occur before the tamper mechanism can be defeated. Opening the enclosure does result in tamper detection.
  - For Wiegand readers, the tamper connection must be additionally wired and parameterized.
  - The enclosures of the EACS components accessible from outside the controlled area shall meet the required IP and IK ratings:
    IP4X
    IK04
    LECTUS duo, LECTUS secure, ARD-FPBEW2-H2 meet the requirements.
- 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.
- For EN 60839 Grade 3, do not use authentication by PIN alone.
- The different useable times zones of the BIS system depends on the numbers of MACs. A separate time zone can be used for each MAC.
- The main server computer, connection servers, MAC servers and clients must be synchronized with a network time server. Local access controllers (e.g. AMCs) synchronize with their MACs.

- Power monitoring must be enabled on local access controllers (e.g. AMCs).
- The status of all access points must be monitored. Appropriate equipment must be installed at these points (e.g. frame contacts).
- 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).
- All operator-initiated changes shall be logged with type, operator ID, time and date of the occurrence.
- The system meets the requirements for Global anti-passback in terms of using one zone per MAC.
- For EN 60839 Grade 4, do not use Web based Visitor Management. Installations that include Visitor Management can attain a maximum of Class 3.

3.4 NIS2 Regulation

3.4.1 Overview

The NIS2 Regulation (Network and Information Systems Directive 2) is an European Union's updated cybersecurity law that came into effect in January 2023, with member states required to transpose it into national law by October 2024.

NIS2 is an EU's response to growing cybersecurity threats, expanding both the scope and the strength of cybersecurity obligations for essential and important entities across Europe. It aims to ensure a high common level of cybersecurity, minimize risks, and protect critical services for citizens and businesses.

3.4.2 Target audience

Essential Sectors:

- Energy (electricity, oil, gas).
- Transport (air, rail, water, road).
- Banking and financial market infrastructure.
- Health sector.
- Drinking water supply and distribution.
- Digital infrastructure.
- ICT service management.
- Public administration.
- Space.

Important Sectors:

- Postal and courier services.
- Waste management.
- Manufacturing of critical products.
- Digital providers.
- Research organizations.

3.4.3 Purpose

NIS2 aims to strengthen cybersecurity across the EU by establishing common security standards and incident reporting requirements for critical sectors by creating a more resilient digital ecosystem across Europe while ensuring consistent cybersecurity standards.

For Organizations:

- Implement appropriate cybersecurity risk management measures.
- Report significant incidents within 24 hours (early warning) and provide detailed reports within 72 hours.
- Ensure supply chain security.
- Conduct regular security assessments.
- Provide cybersecurity training for staff.

For Member States:

- Establish national cybersecurity strategies.
- Designate competent authorities.
- Create Computer Security Incident Response Teams (CSIRTs).
- Impose effective, proportionate, and dissuasive penalties.

3.4.4 Regulatory compliance requirements

The following sections are requirements to take into consideration when implementing physical access control to comply with NIS (Network and Information Systems) regulations, here are the key considerations for planning and configuration:

3.4.4.1 Risk assessment and documentation

- Conduct thorough risk assessments of all physical access points.
- Document security measures and maintain compliance records.
- Establish incident reporting procedures for security breaches.
- Regular security audits and reviews.

3.4.4.2 Access control principles

Principle of least privilege - minimum necessary access

Principle of Least Privilege (PoLP) ensures that users and systems only have access to the minimum level of permissions required to perform their tasks. By implementing granular permissions, the configuration minimizes the risk of unauthorized access and potential abuse. It limits exposure and reduces the likelihood of privilege escalation attacks, as each user or system component only operates within the boundaries necessary for its role.

Need-to-know basis - role-based access control

Protect data on a Need-to-know basis, implemented through role-based access control which grants users access to sensitive data only if it is required for their role.

Separation of Duty - prevent single points of failure

Separation of Duty (SoD) refers to the dividing of responsibilities among multiple individuals to prevent a single point of failure. An example of implementation is the Two-Person Principle which requires an operation to be performed by two authorized users.

Regular access reviews - periodic validation of permissions

Periodic audits of access rights and user activities to ensure compliance with Access Control Principles.

3.4.5 Technical implementation

3.4.5.1 Multi-layered security

- Perimeter security (gates, barriers, surveillance)

Refer to Access Management System manual in **Configuring Entrances**.

- Building access control (card readers, biometrics)

– Zone-based access (different security levels for different areas)

Refer to Access Management System manual in **Configuring areas of access control.**

– Critical infrastructure protection (server rooms, network equipment)

3.4.5.2 Authentication methods

Multi-factor authentication (card + PIN/biometric)

– Multi-factor authentication

It requires additional credential factors (card/token, PIN, biometric or mobile credential) from the user requesting access. This measure prevents unauthorized users from gaining access using a stolen credential.

To enable multi-factor authentication, select readers that support multiple credential factors with card reading, keypad, biometric and/or Bluetooth Low Energy (BLE) components.

– Enabling multi-factor authentication with keypad readers:

When a PIN is used in combination with another credential factor, it is called a Verification PIN.

Refer to Access Management System manual in **PIN codes for personnel**.

– Enabling multi-factor authentication with biometric readers:

For Bosch Fingerprint reader, refer to Access Management System manual in **Enrolling fingerprint data**.

For IDEMIA devices, refer to Access Management System manual in **Configuring IDEMIA Universal BioBridge**.

– Enabling 2nd-factor authentication with BLE-enabled readers:

Enable in the Setup Access App when configuring the reader. Refer to Mobile Access Quick Installation Guide.

Biometric systems for high-security areas

– Biometric systems

It can be used as an additional authentication method to increase security. Unlike tokens or PIN codes that can be stolen, copied or forgotten, biometrics are much more difficult to clone or steal and will not be misplaced.

– Biometric readers can be configured to for several different identification modes:
– By Card OR Biometry, depending on what the credential holder presents to the reader. The user can identify themselves EITHER by card OR by biometric credentials.
– By Card AND Biometry, that is the user must verify through biometric credentials that they are the true owner of the card.
– By Biometry only: users are to identify themselves by biometric credentials only.

The Bosch Fingerprint reader offers easy enrollment of fingerprints and management of cardholder data in AMS. IDEMIA biometric devices integrate with AMS through MorphoManager and BioBridge.

Visitor management systems

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.

Refer to Access Management System cybersecurity guidebook manual in **Considerations for Visitor Management**, for more information.

Temporary access credentials with expiration

It is possible to assign a Temporary card with a validity period.

A temporary card is a temporary replacement for a card that has been misplaced by a regular cardholder. It is a duplicate that contains all the authorizations and limitations of the original, including rights for offline doors.

To prevent abuse, the system can optionally block one or all of the cardholder's other cards for a limited period, or until unblocked manually.
Temporary cards are therefore unsuitable for use as visitor cards.
Refer to Access Management System manual in **Temporary cards**.

3.4.5.3 Monitoring and Logging

- Real-time access monitoring. Refer to *Operating Swiper ticker* on AMS Map View user manual.
- Comprehensive audit trails (who, when, where). Refer to *Using the alarm audit trail* dialog on AMS Map View user manual.
- Integration with SIEM (Security Information and Event Management) (SIEM) systems. Refer to Access Control API whitepaper.
- Video surveillance integration.

BVMS integration.
Refer to Video surveillance integration.

Milestone XProtect integration
Refer to Access Management System manual in **Configuring Milestone XProtect to use AMS**.
Automated alerts for unauthorized access attempts. Refer to *Operating Swiper ticker* on AMS Map View user manual.

3.4.6 System configuration

3.4.6.1 Access zones and Policies

- Define security zones based on criticality.
- Time-based access restrictions.

Time Models
Refer to Access Management System manual in **Configuring the calendar**.

Option to temporarily deny access
Refer to Access Management System manual in **Blocking access for personnel**.

- Anti-passback controls

Also referred to as "Double access control," Anti-passback is a simple form of Access Sequence Monitoring in which a cardholder is prevented from entering an Area twice within a defined time period, unless the card has been scanned to exit that Area in the meantime. Anti-passback deters a person from passing credentials back through an entrance for use by an unauthorized second person. This requires both entrance and exit readers at the areas' entrances.
For configuring a reader for access sequence monitoring, refer to Access Management System manual in **Readers**.

- Tailgating detection

Tailgating is when an unauthorized user circumvents access control by closely following an authorized cardholder through an entrance without presenting their own credentials.
The best defense against tailgating, either accidental or deliberate, is the singling of cardholder accesses. With this configuration, only one person can pass through at a time. This can be done with a turnstile or Mantrap.

- Creating a Mantrap

A Mantrap uses two interlocking doors that create a single-person entry vestibule.
Entrance models 01 and 03 can be used to program a Mantrap. Use the check box Mantrap option to make the necessary additional signals available.

Refer to Access Management System manual in **Mantrap door models**.

– Emergency access procedures

Threat Level Management.

Refer to Access Management System manual in **Concepts of Threat Level Management.**

3.4.6.2 Integration requirements

– HR system integration for automated provisioning/deprovisioning.
– IT system integration for unified identity management - SSO.
– (Fire safety system integration).
– Building management system connectivity.

AMS 6.0 can be integrated with Building Integration System (BIS 6.0 and above).

3.4.7 Operational considerations

3.4.7.1 Personnel management

– Background checks for personnel with critical access.
– Regular training on security procedures.
– Clear escalation procedures.
– Contractor and visitor access protocols.

Refer to Access Management System manual in **Managing visitors**.

3.4.7.2 Business continuity

– Redundant systems and backup power.
– Emergency access procedures.
– Threat Level Management.

Refer to Access Management System manual in **Concepts of Threat Level Management**.

– Disaster recovery planning.
– System availability requirements (99.9%+ uptime).

3.4.7.3 Data protection

– GDPR compliance for biometric/personal data.
– Secure storage of access logs.
– Data retention policies.
– Privacy impact assessments.

3.4.8 Vendor selection criteria

– Compliance certifications (ISO 27001, Common Criteria).
– Scalability and future expansion capability.
– Interoperability with existing systems.

For comprehensive security management, there are many options for integrating the Bosch Access Control system.

AMS features integrations with other Bosch products:

– Building Integration System (BIS 6.0 and above)
– Bosch Video Management System (BVMS 10.1 or higher)
– B and G Series Intrusion Control Panels
  – Refer to Access Management System manual in **Configuring intrusion areas and panels**.
– Connection to third party products is possible via open and secure protocols.
– AMS features a RESTful API for development of custom integrations.

  - Refer to Access Control API whitepaper.
- Support and maintenance capabilities
- Cybersecurity features (encrypted communications, secure protocols)
- Bosch Client-Server communication supports the use of both self-signed certificates and certificates signed by a Certificate Authority (CA). HTTP Secure (HTTPS) is used through Transport Layer Security (TLS/DTLS) to secure web communication.
- Data transfer between the server and other components is encrypted through AES-128.
- Communication between access controllers and central server are encrypted using minimum AES 256-bit encryption with custom keys and a protocol from the TLS family (minimum version 1.2). It is possible to set individually customized encryption keys for every access controller to allow highest possible security.

Secure Controller-Reader communication

Open Supervised Device Protocol v2 (OSDPv2) with Secure Channel supports AES-128 encrypted communication between reader and controller.

Additionally, OSDPv2 utilizes two-way communication. This allows constant monitoring of readers, via the same communication channels, in order to detect tampering or device removal. OSDP is an open protocol and has several other benefits, such as the ability to send commands to the reader, improved system interoperability and more.

Secure Readers

For installations where vandalism or exposure to elements is a concern, choose readers with high IP and IK ratings.

Secure Credentials

For secure communication, use 13.56 megahertz smart card technology in the latest formats.

The credential data should be protected and encrypted in the secure sector of a card.

Bosch makes its own secure code (Bosch Code) which is stored within the secure area of the smart card, thus providing the highest level of security for credentials.

3.4.9 Implementation timeline

1. **Phase 1**: Risk assessment and system design.
2. **Phase 2**: Critical areas implementation.
3. **Phase 3**: Full deployment and integration.
4. **Phase 4**: Testing, training, and go-live.
5. **Phase 5**: Monitoring and continuous improvement.

4 Secure 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 for all supported languages.
The download store provides SHA256 checksums for all distribution packages, to protect consumers from fraudulent distributions.
Secure delivery of the package can be further checked with the following procedures:

1. Extract the zip file by using Windows function **Extract All**.
2. All executables of the package 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**.

Recommendation for secure installation
In case of operating Bosch access control software (AMS, BIS, Visitor Management, Credential Management, Mobile Access) in a corporate network environment, it is recommended to use certificates issued by a corporate CA (Certificate Authority). Certificates should be arranged before the installation of any of the backend systems. Please refer to software manuals available on the online catalog for more information.
It is strongly recommended to upgrade all identified outdated components to their respective latest stable and secure versions and to check all system requirements before installation.
System requirements are available on the software respective release notes and datasheet.

5 Secure configuration

5.1 Network ports and firewall on BIS server

For Windows 10, Windows Server 2019 and Windows Server 2022 it is assumed that the default settings for the Outbound Rules are set in the Windows Firewall as detailed below.

5.1.1 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.

5.1.2 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.

5.1.3 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`

5.1.4 Windows firewall: additional settings of Automation and Security Engine

The general settings described in sections *DCOM settings for all BIS Products, page 16* and *Setting up Windows firewall, page 16* are sufficient for the Automation Engine and Security Engine.

5.1.5 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 16*:

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:

BVIPOpcConfig.exe	`[Install-path]\MgtS\Video Engine \BVIPOpcConfig`
BVIPOPCServer.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 10, Windows Server 2019, Windows Server 2022 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).

5.1.6 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:
   https://msdn.microsoft.com/de-de/library/cc646023.aspx
   https://support.microsoft.com/kb/929851/en-us

Note: The setup for SQL Server as described above must be performed on third party firewall products.

5.1.7 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.

5.1.8 Third party firewalls

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

5.1.9 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 **Default 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.

5.1.10 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 17* must also be performed on third party firewalls.

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

The general settings described in sections *DCOM settings for all BIS Products, page 16* and *Setting up Windows firewall, page 16* are sufficient for the Automation Engine and Security Engine.

5.1.12 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 17*, must also be performed also on third party firewall products.

5.1.13 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 19*, must also be performed on third party firewall products.

5.2 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:

– 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.
When configuring SQL Server, create dedicated SQL accounts with limited and scoped privileges and use these accounts for operation.
Avoid using the default 'sa' or any built-in administrative accounts for application or remote access, as the 'sa' account is a prime target for attackers due to its unrestricted privileges. During initial setup, the 'sa' account may be necessary for installation and database creation, but it must be disabled afterward or replaced with dedicated operator accounts that have equivalent permissions.

Notice!
Operational Security Risk
To mitigate security risks, disable the 'sa' account when not in use.

Communication between 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

5.3 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.

5.4 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, must be updated if vulnerabilities are reported. After the software is installed, always check for Microsoft updates.
- 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.
- It is strongly recommended to use TLS 1.3.TLS versions 1.0 and 1.1 are deprecated and considered insecure.
- Disable “Insecure” cipher suites. Cipher suite TLS_RSA_WITH_AES_256_CBC_SHA256 has been tested and is sufficient for the system to work.
- Enable SMB signing (Server Message Block) as advised by Microsoft, see https://learn.microsoft.com/en-us/windows-server/storage/file-server/smb-signing-overview#policy-locations-for-smb-signing.

5.4.1 Security recommendations for user authorizations

On the AMS or BIS server, define only Windows users who are intended to change the 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.

5.4.2 Session and Token Timeout Configuration for Secure SSO

To reduce the risk of session hijacking, session tokens should be short-lived and refreshed frequently. The balance between security and user friendliness is always a trade off when it comes to token lifetimes. We preconfigured the values of all tokens in a way we consider secure enough for general Access Systems but for more secure environments we recommend the configuration below. If you have special requirements regarding token lifetime you can adjust all values in the Identity Provider settings.
The following configuration uses time in hh:mm:ss and the values are aligned with industry best practices and security standards:

1. Log in the BIS server.
2. Using Windows Explorer, navigate to the “IdentityProvider” subfolder of the BIS installation directory. Usually, this folder is located at:
   `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\IdentityProvider`
3. Use a text editor to edit the file used during SSO configuration “appsettings.Customer.json”:

After

```
{
"OpenIdProvider": {
```

Insert the following:

```
"AccessTokenLifetime": "00:30:00",
"IdentityTokenLifetime": "00:30:00",
"RefreshTokenLifetime": "12:00:00",
```

1. Save the file.
2. In IIS Manager -> Application Pools, restart "Identity Provider AppPool".

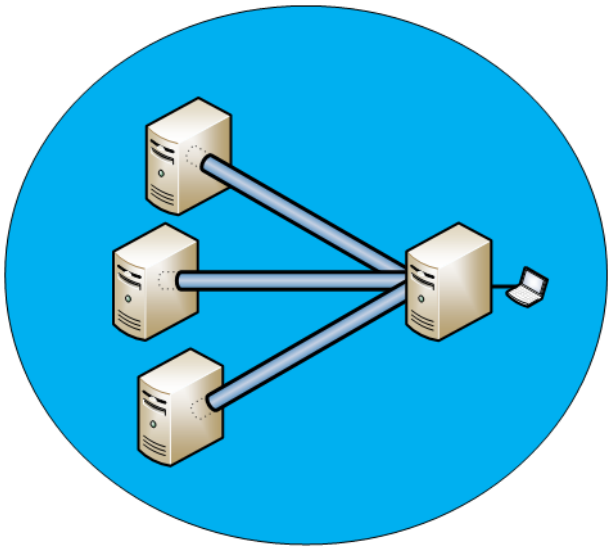
5.5 IPsec Transport mode and Tunnel mode

The following implementations are recommended.

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

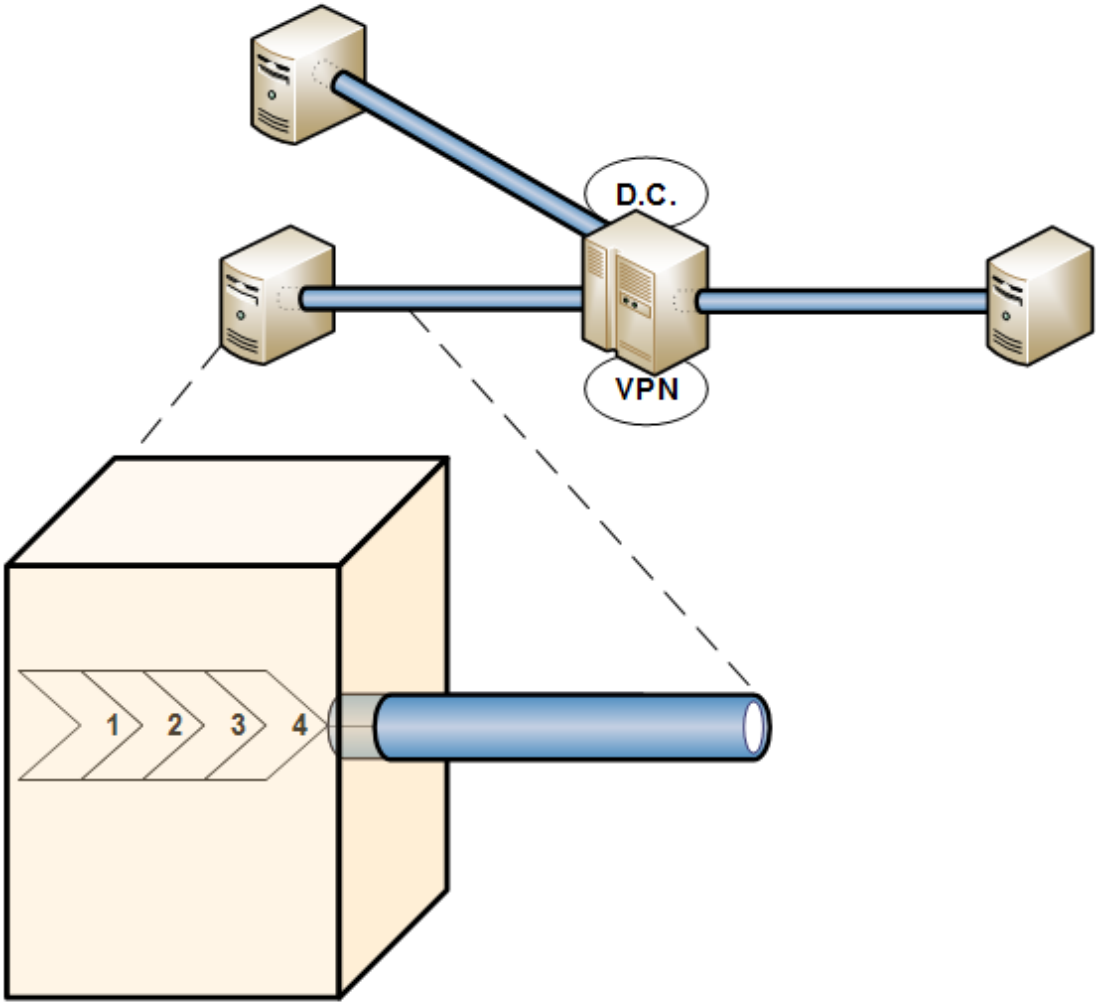
Notice!
When to implement IPsec
For effective troubleshooting it is recommended that your BIS installation be complete and stable across all participating computers in your BIS network before you start to implement IPsec in it.

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)		

5.5.1 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

5.5.2 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.

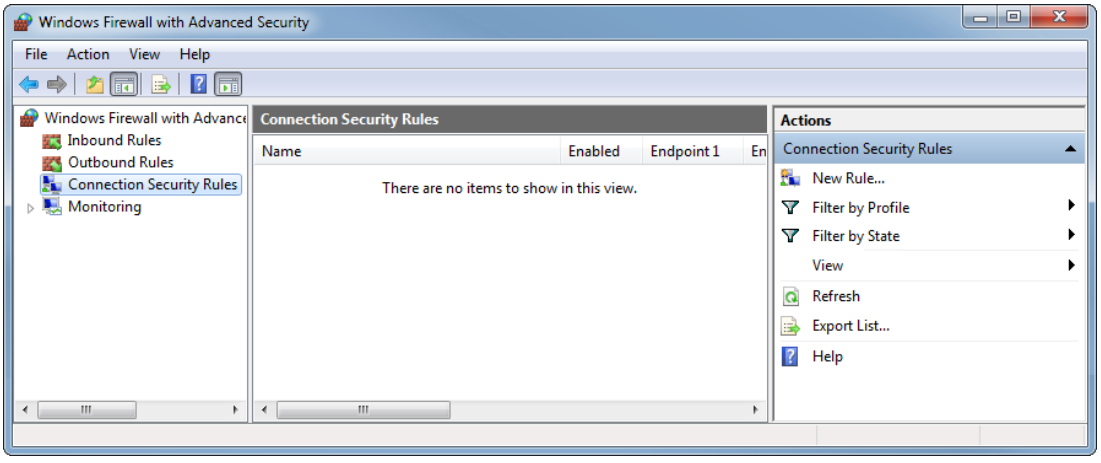
Notice!
IP communication between BIS computers and IP devices with no operating system can be enabled but not protected by IPsec.

5.6 Transport mode configuration

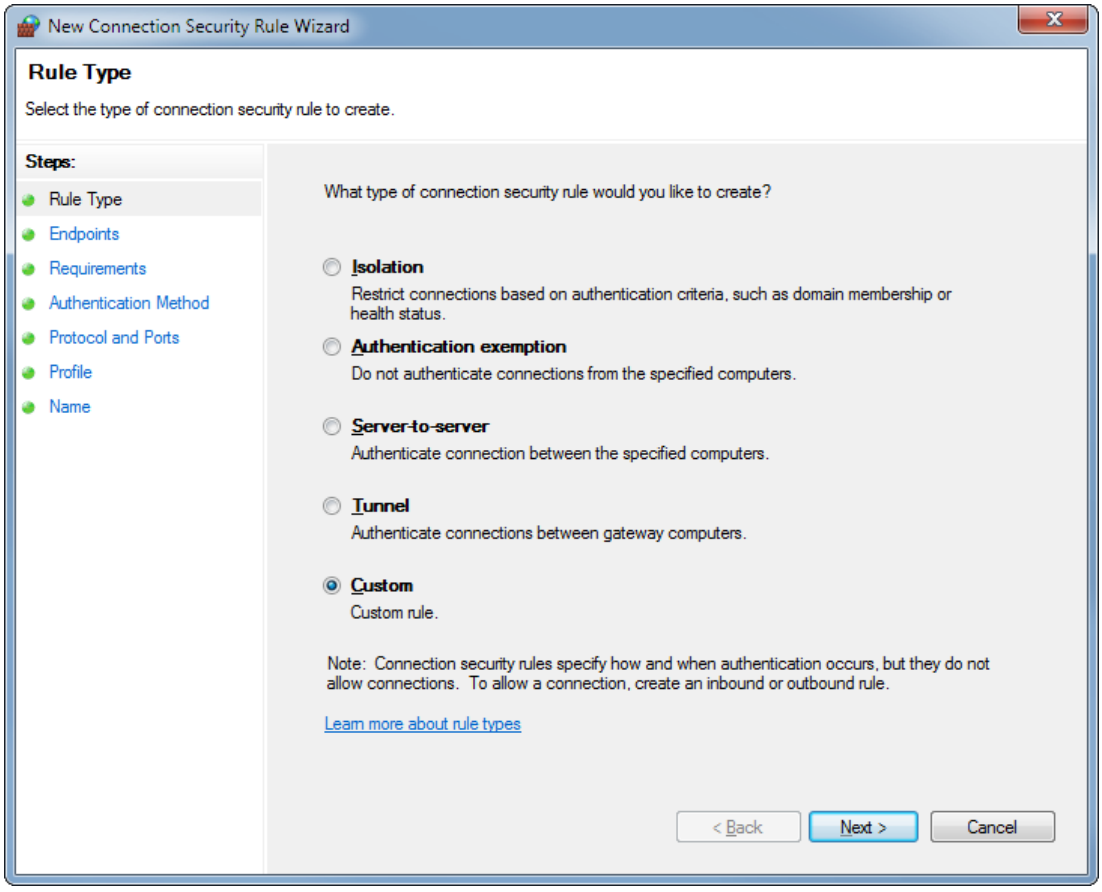
How to set up IPSec on the Login server or Connection server

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)).

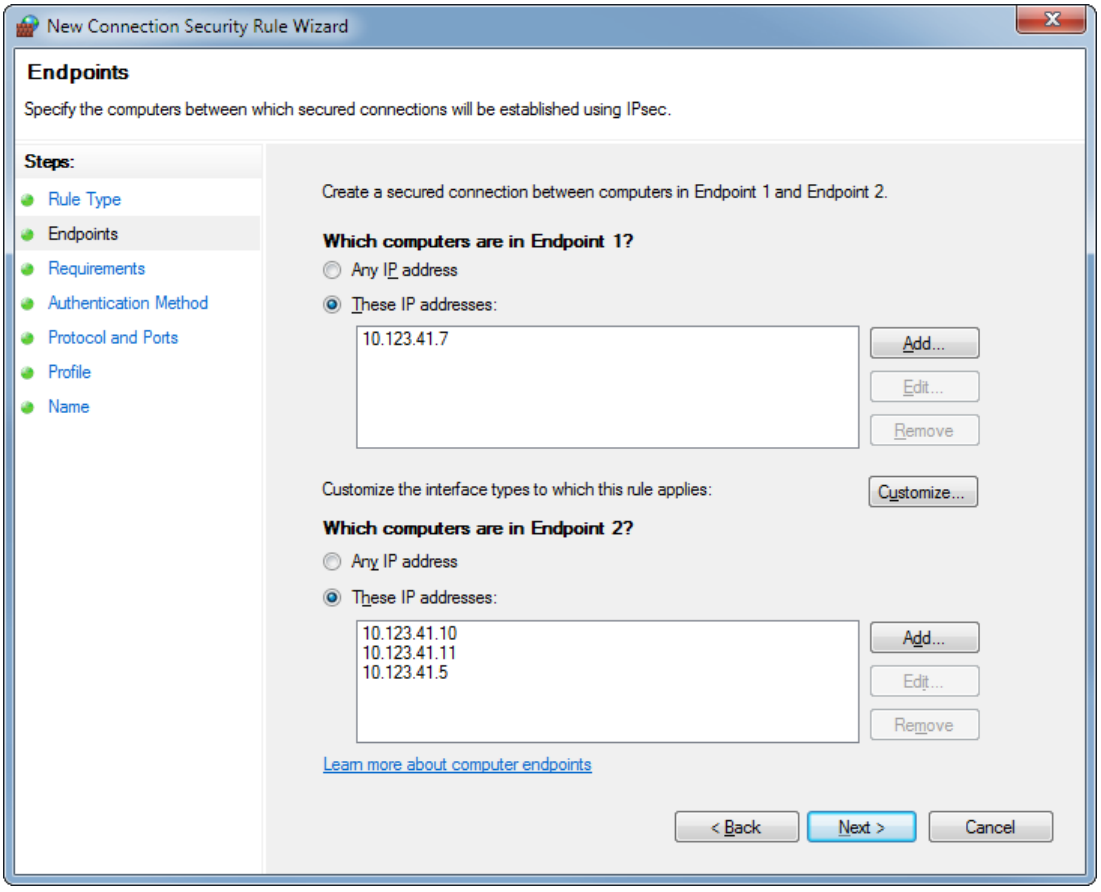
1. Configure Firewall settings for BIS. Document and DCOM settings according to the information on the documentation. Refer to the software installation manual and cybersecurity manual for more information.
2. Start **Windows Firewall with Advanced Security** > Right-click **Connection Security Rules** and select **New Rule...**



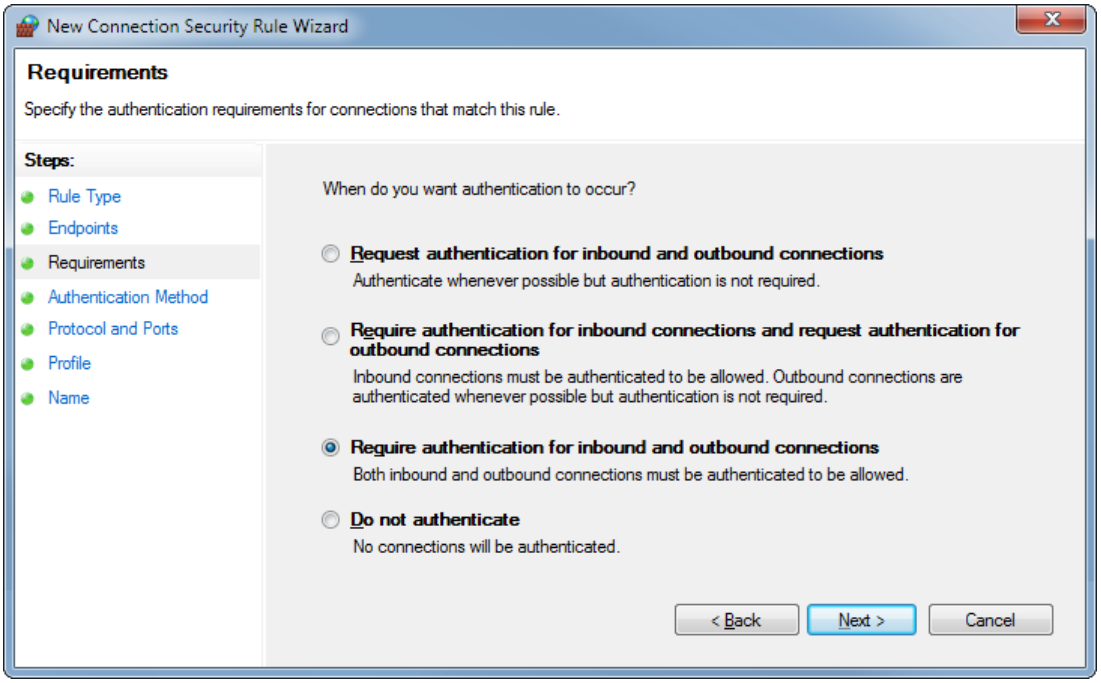
3. Select **Custom** and click **Next>**



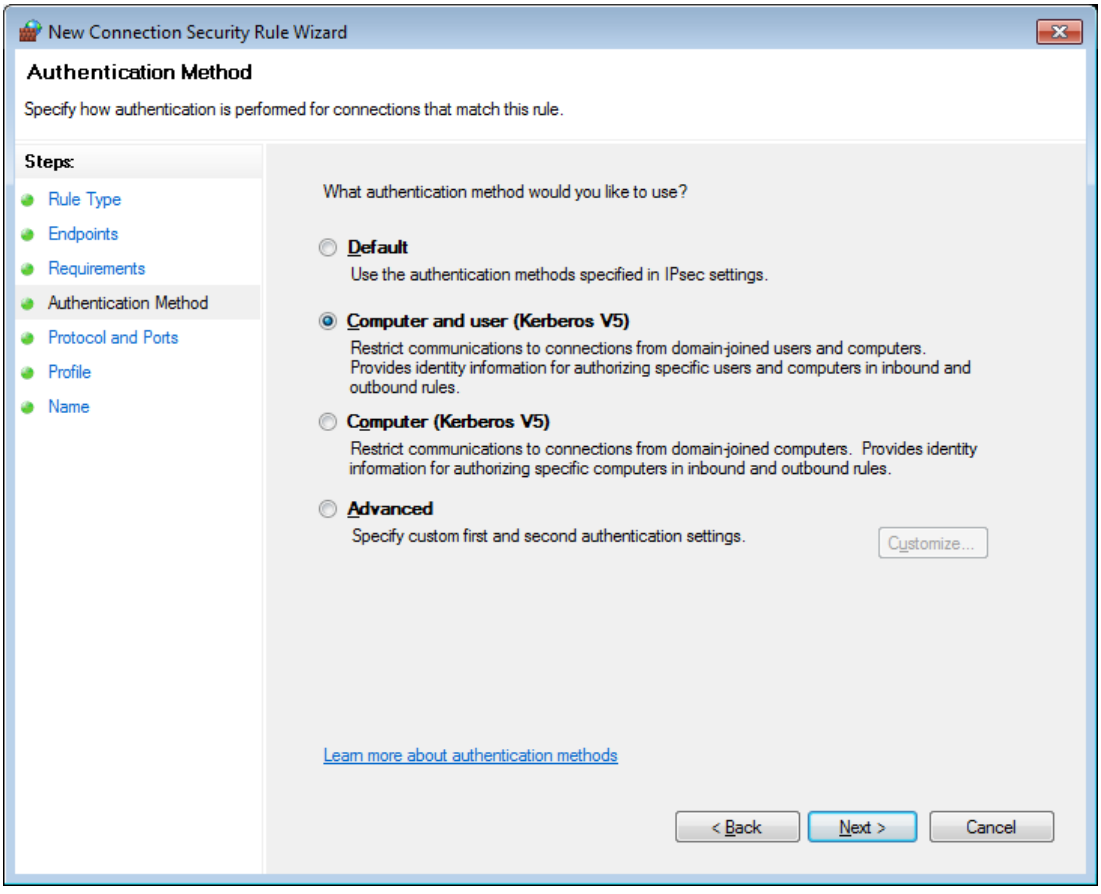
4. Add the Endpoints and click **Next>**
   Endpoints are the machines with which you would want to have a secure connection.
   Endpoint 1 = Login Server's IP address
   Endpoint 2 = IP addresses of SQL server, Remote client or Connection server



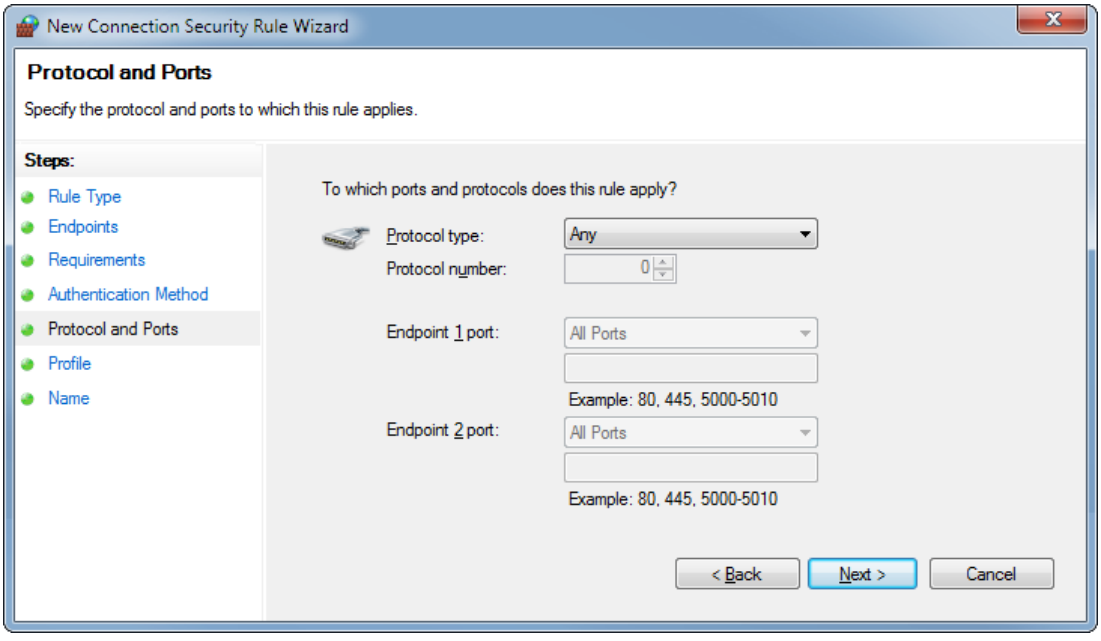
5. Select **Require authentication for inbound and outbound connections** and click **Next>**



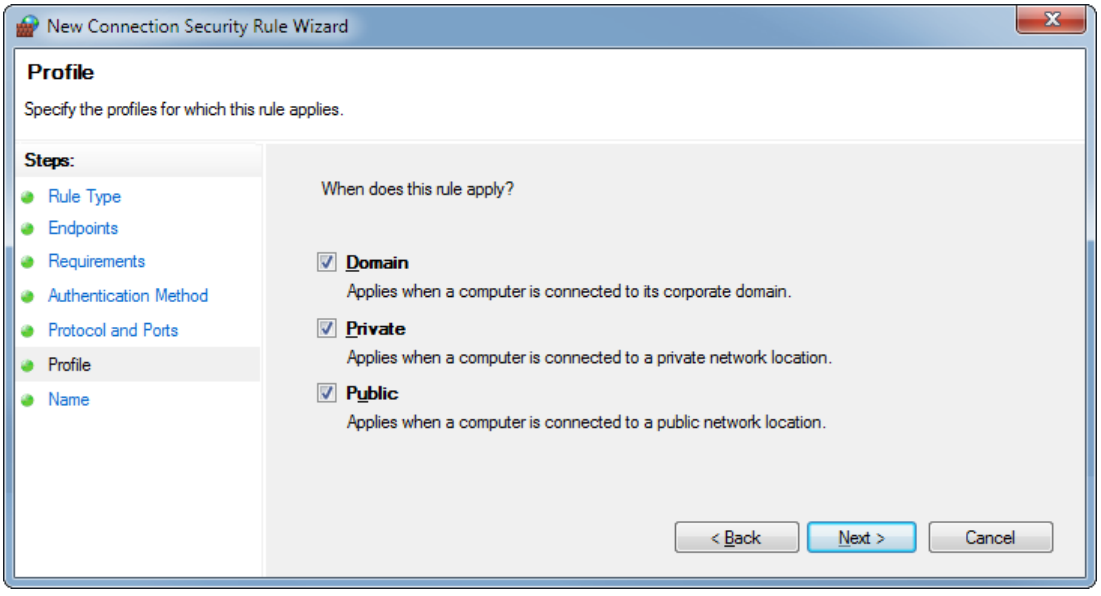
6. Select **Computer and User (Kerberos V5)** and click **Next>**



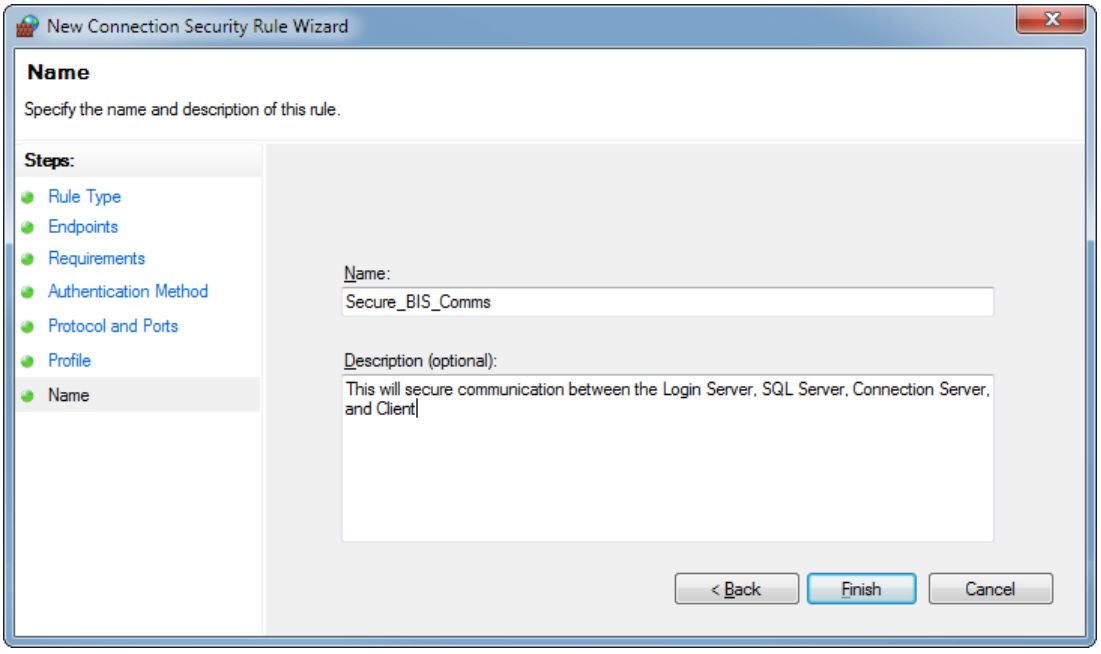
7. Leave the **Ports and Protocols** as default and click **Next>**



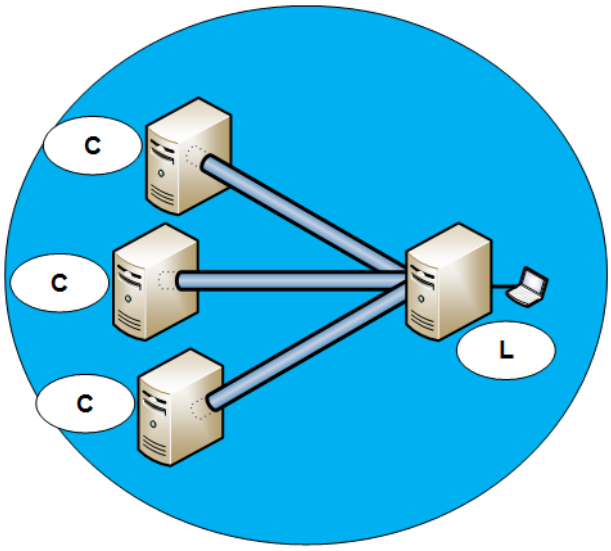
8. Leave the **Profiles** as default (all check boxes selected) and click **Next>**



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

5.6.1 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.

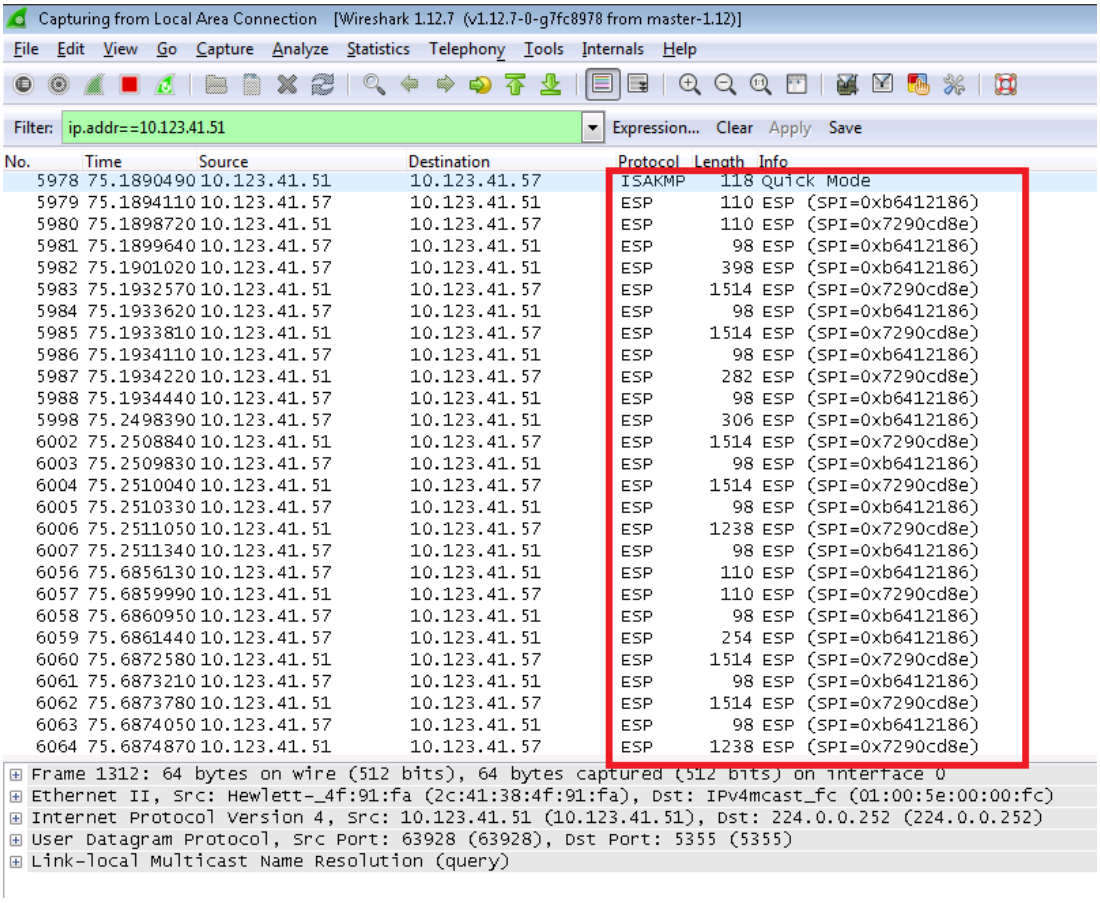
Notice!
The firewall on each machine must have the same rule.

5.6.2 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

5.6.3 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:



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.

5.7 Tunnel mode configuration

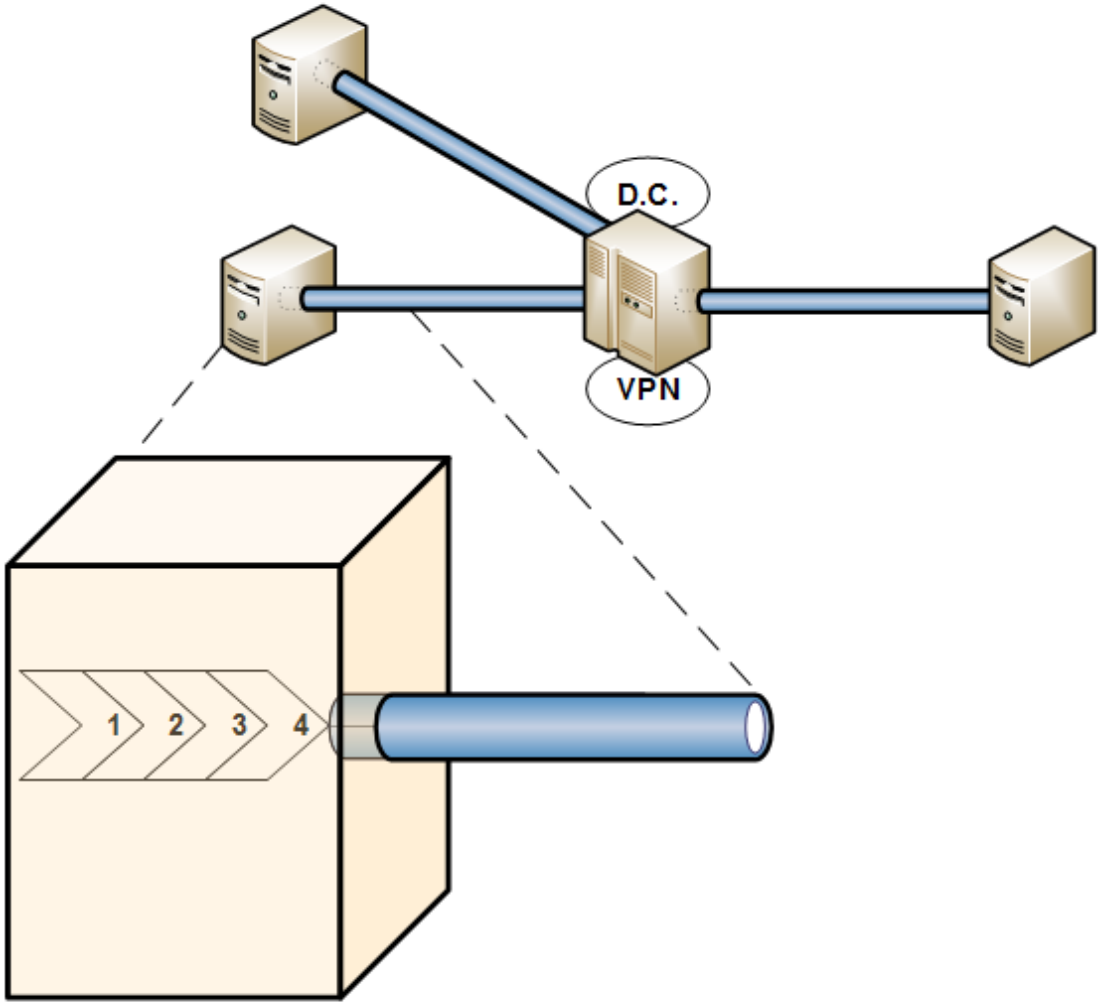
Configuring Windows Server 2019 or 2022 as a L2TP/VPN Server

Windows Server 2019 or 2022 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 41*

Notice!

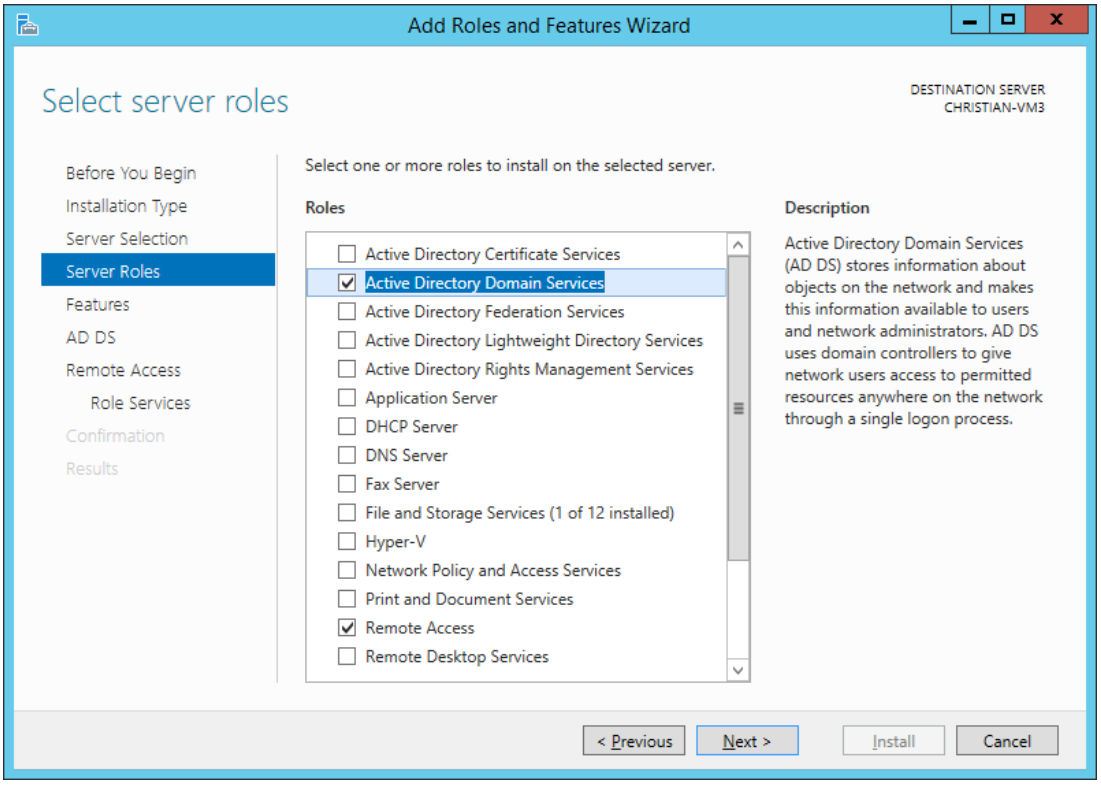
Note: The BIS server and VPN server should not be on the same PC



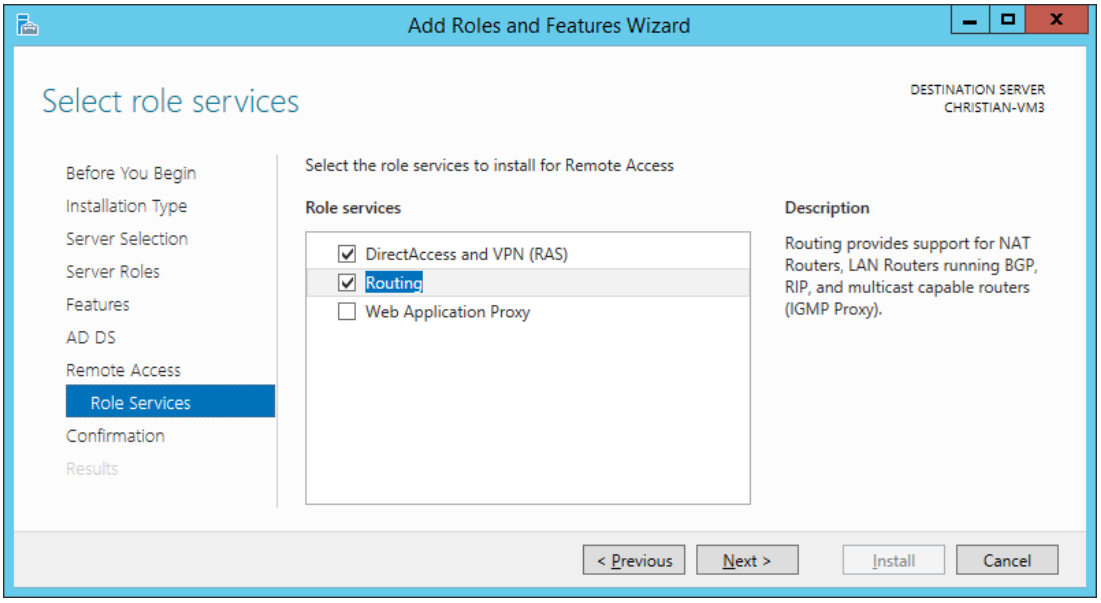
1	Application + IP socket	**D.C:**	Domain Controller (primary or secondary)
2	Virtual NIC + Layer 2 Tunneling Protocol (L2TP)		
3	IPsec (IP security protocol)	**VPN**	Virtual Private Network server (software)
4	NIC (Network Interface card)		

5.7.1 Promote the Windows Server to a Domain Controller

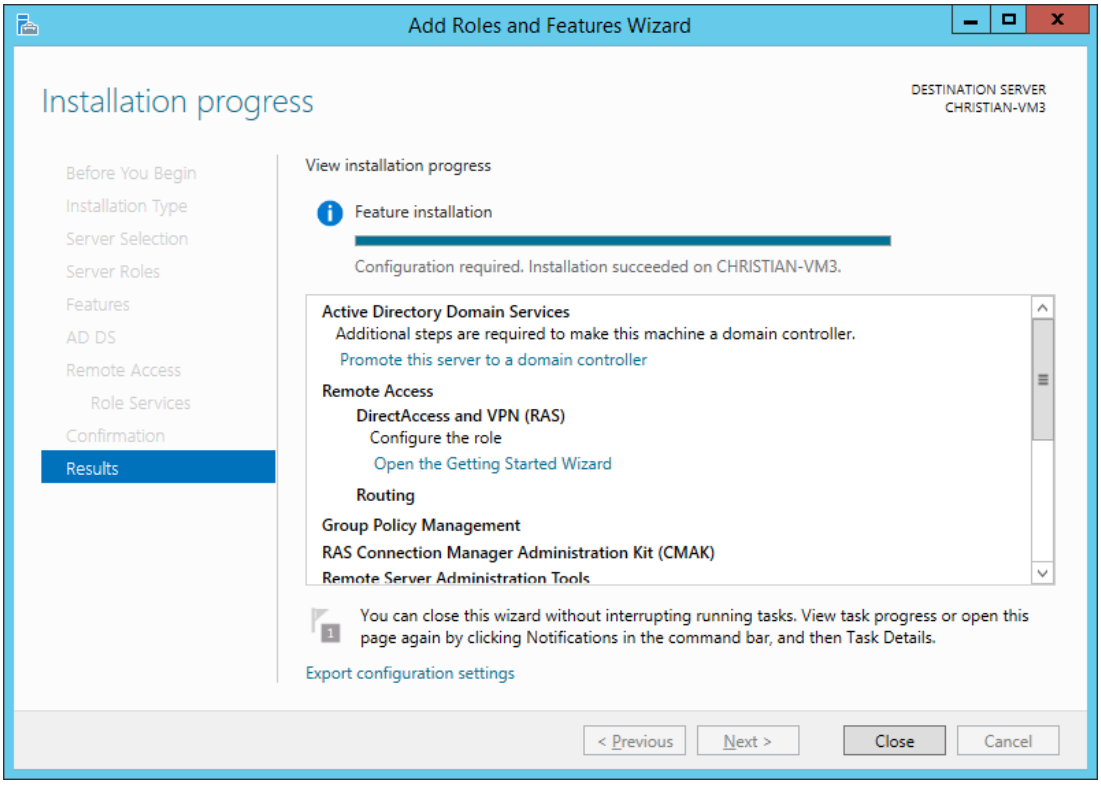
1. Open Server Manager and click **Manage** > **Add Roles and Features** > Select **Active Directory Domain Services** and **Remote Access**



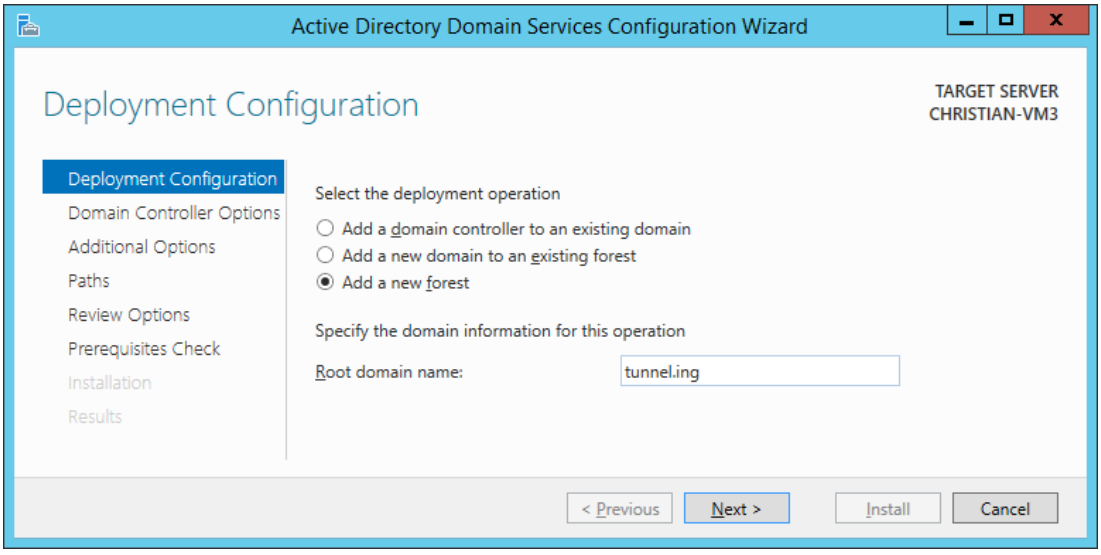
2. Under **Remote Access** > **Role Services**, select both **DirectAccess and VPN (RAS)** and **Routing**
Click **Next** and then **Install**



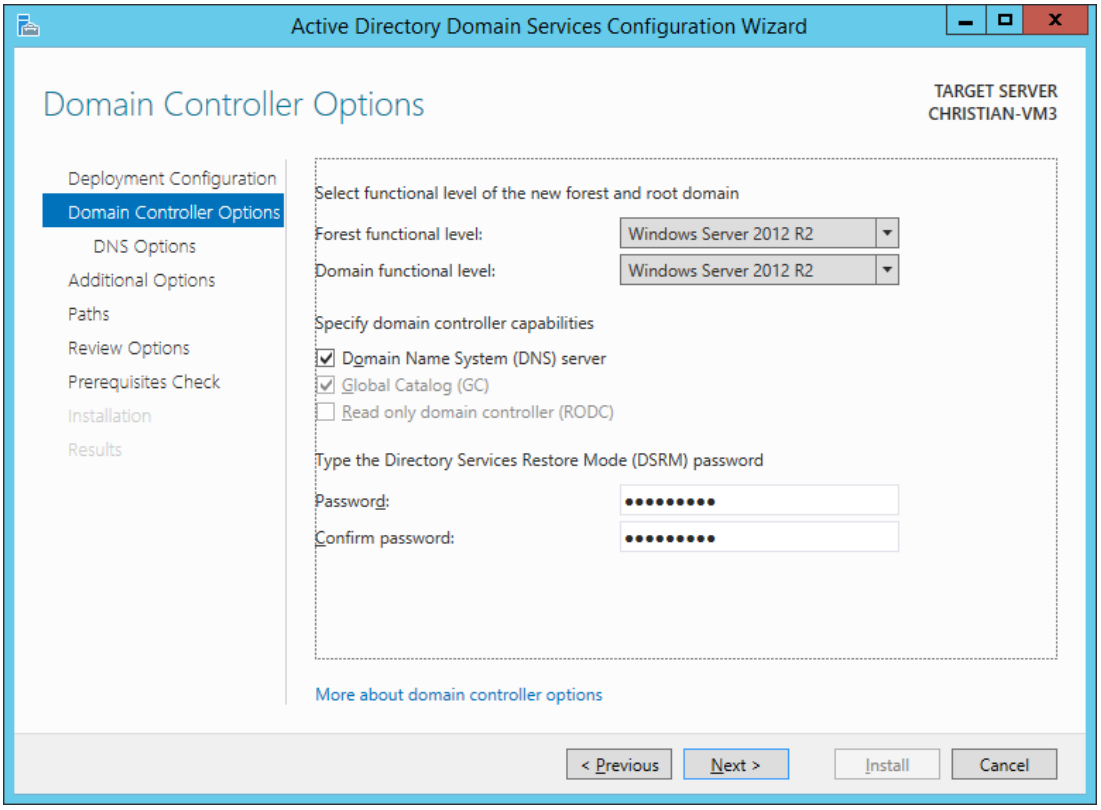
3. Click **Promote this server to a domain controller**



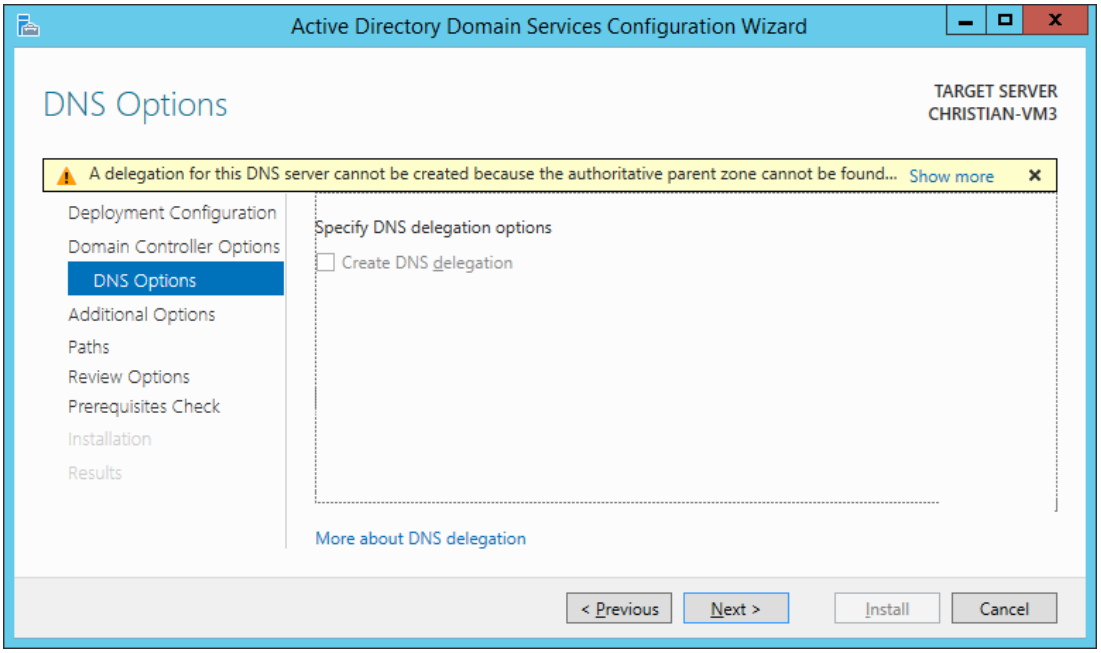
4. On the **Deployment Configuration** page select **Add a new forest** and click **Next**



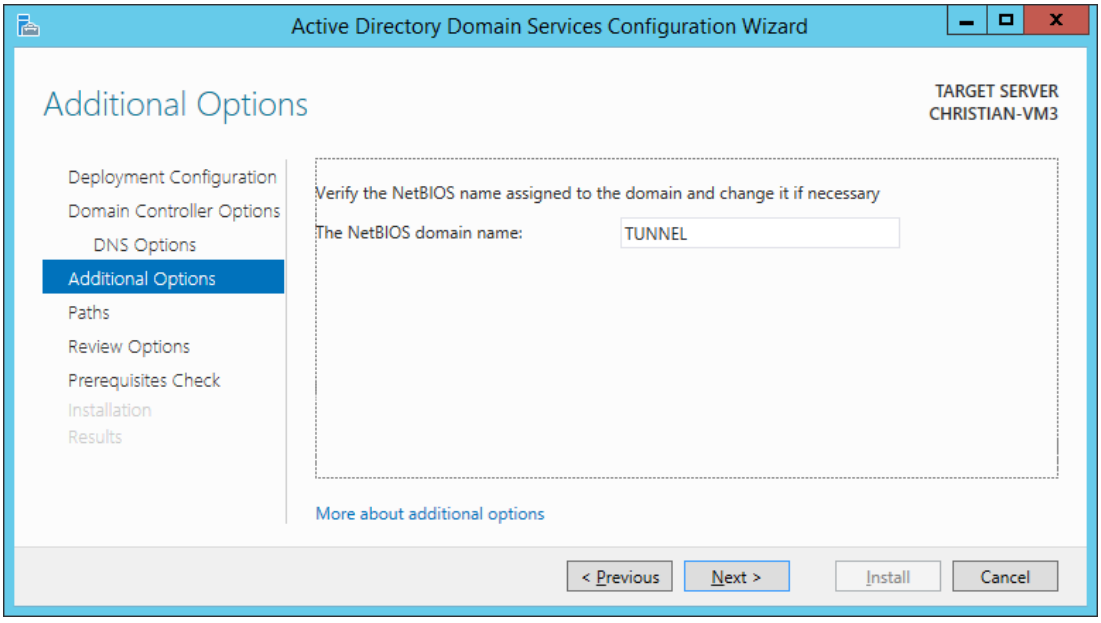
5. On the **Domain Controller Options** page, set a password and click **Next**



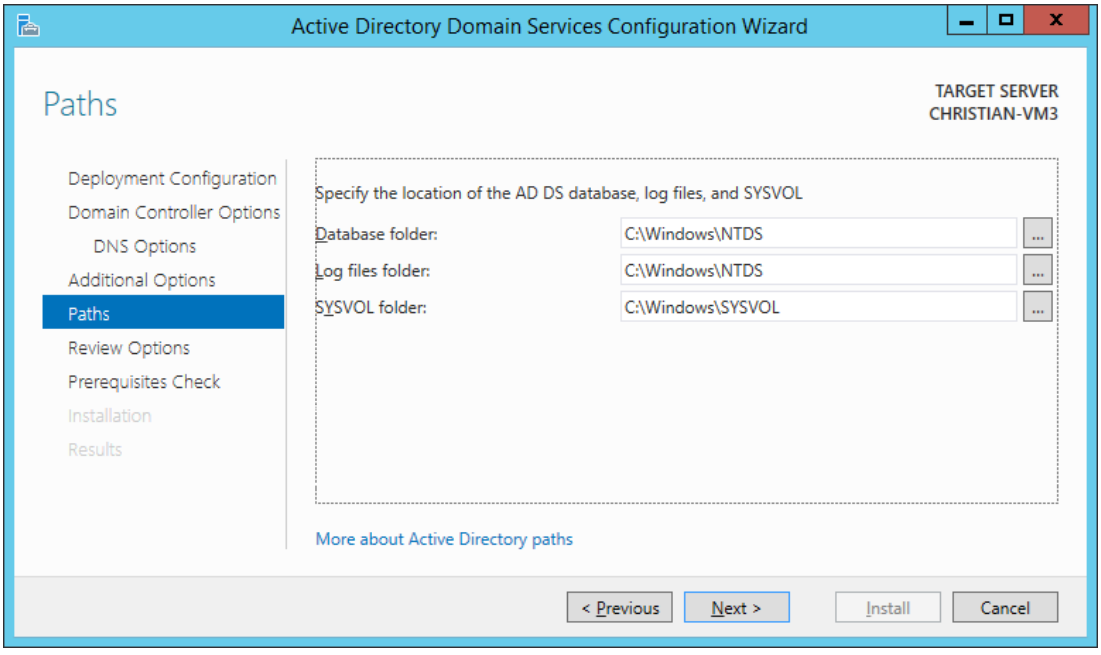
6. On the **DNS Options** page click **Next**



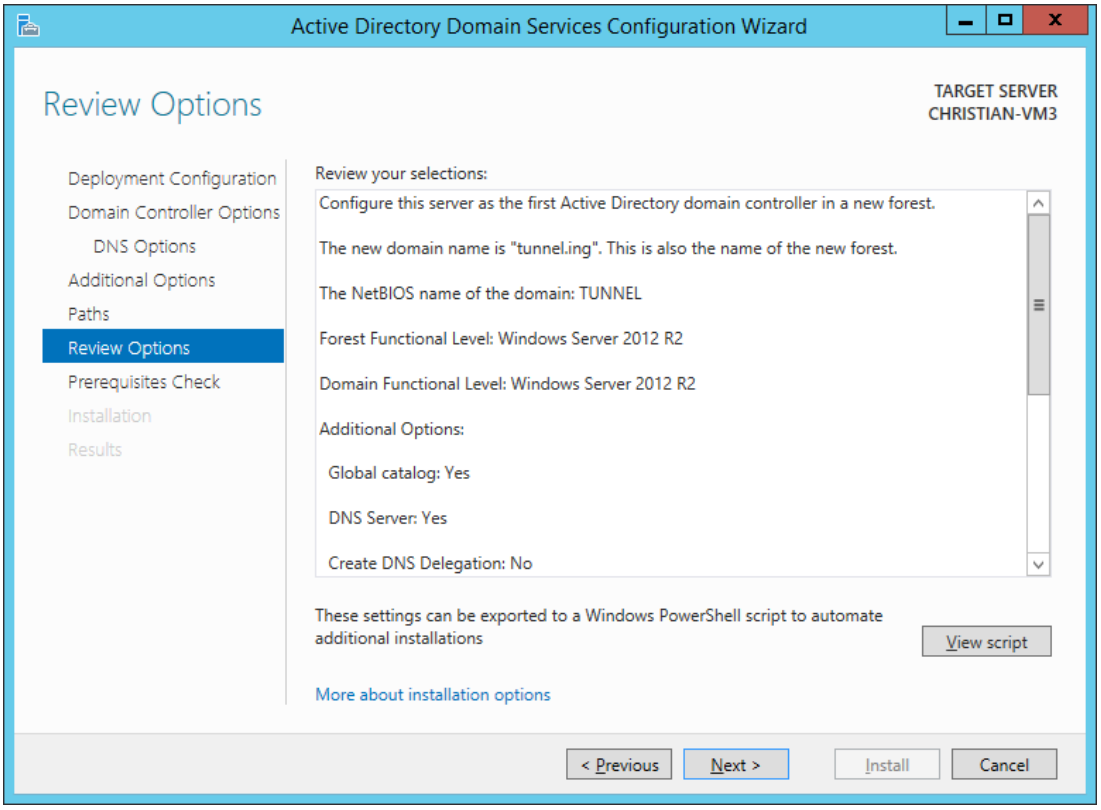
7. On the **Additional Options** page, verify the NetBIOS name and click **Next**



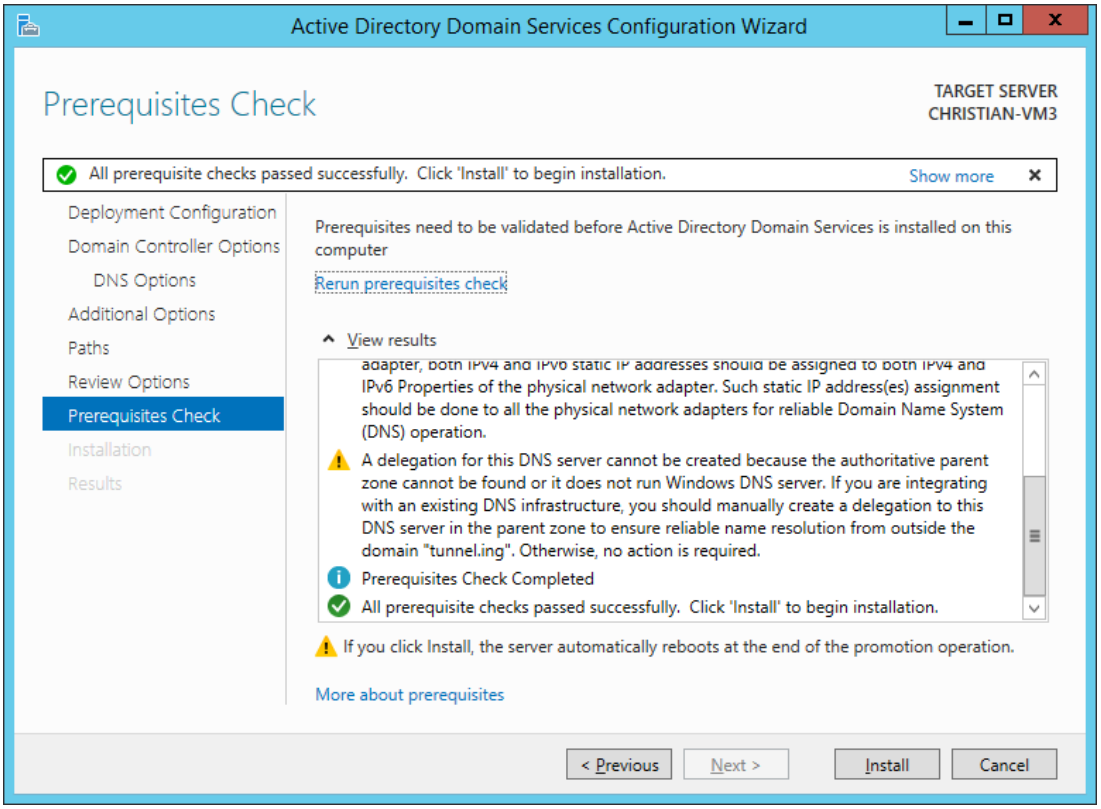
8. On the **Paths** page, click **Next**



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



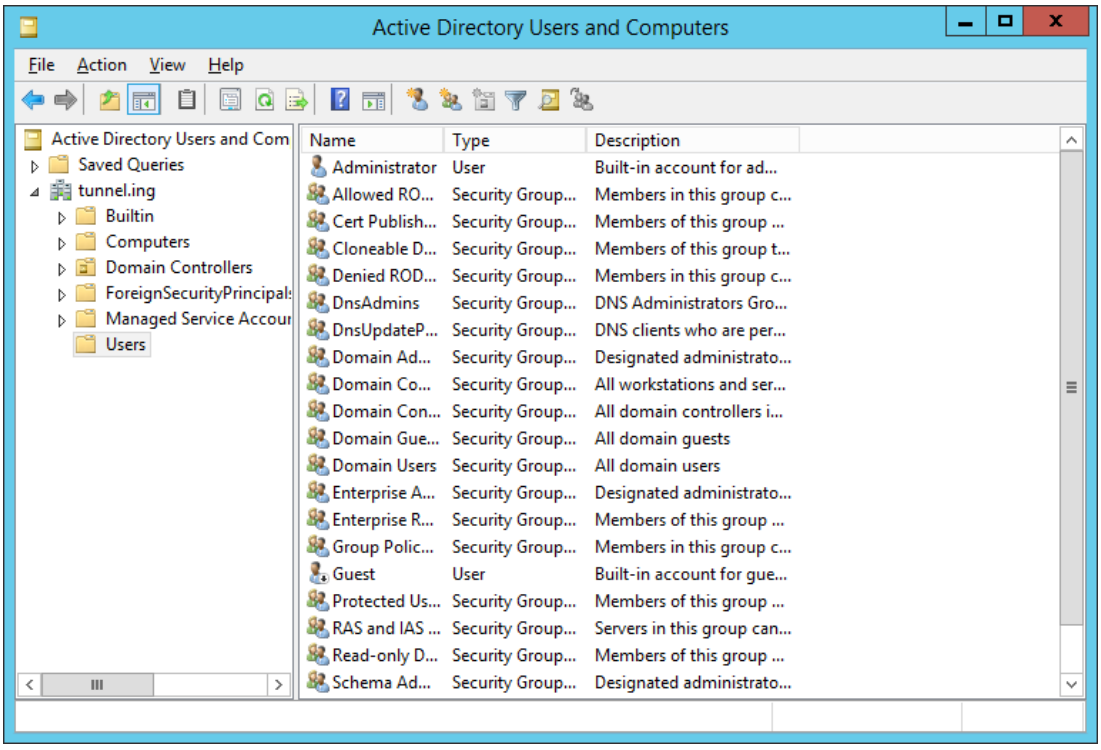
10. On the **Prerequisites Check** page, click **Install**



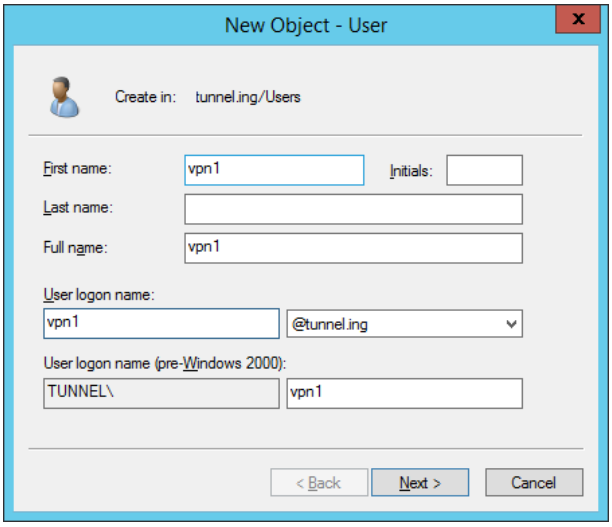
11. After Domain Services have been installed, you will be logged off and the server will restart. Login as an administrator under the created domain.

5.7.2 Set up the VPN

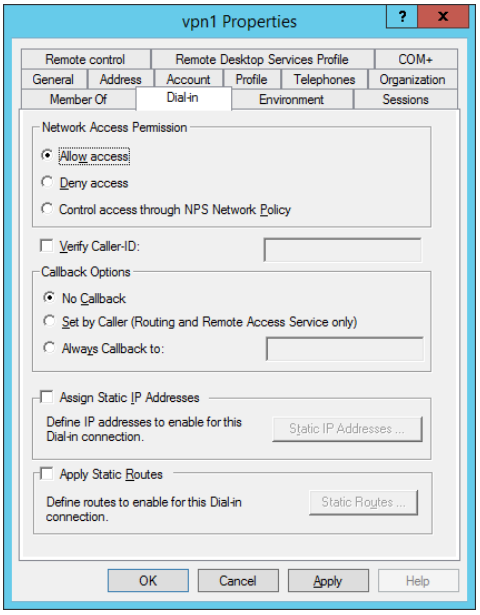
1. Under Windows open **Server Manager** > **Tools** > **Active Directory Users and Computers** to create a new user



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:

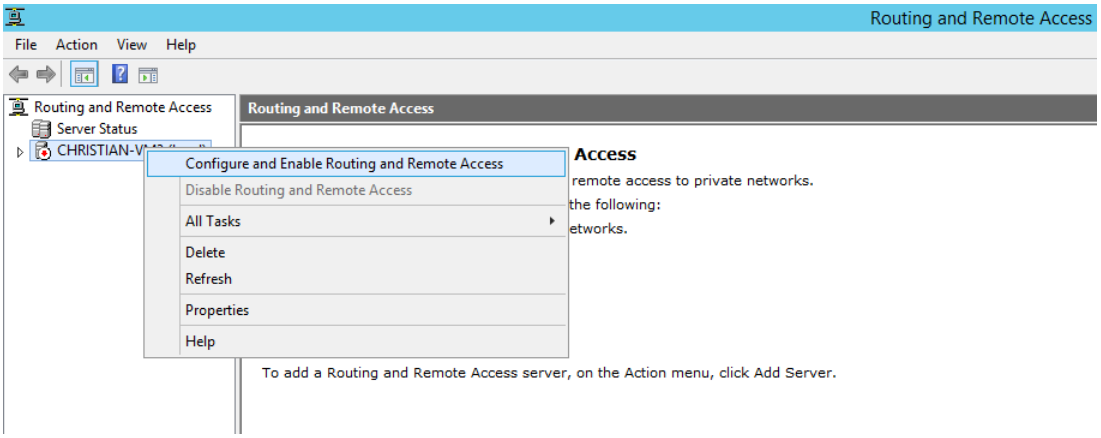
For example:

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

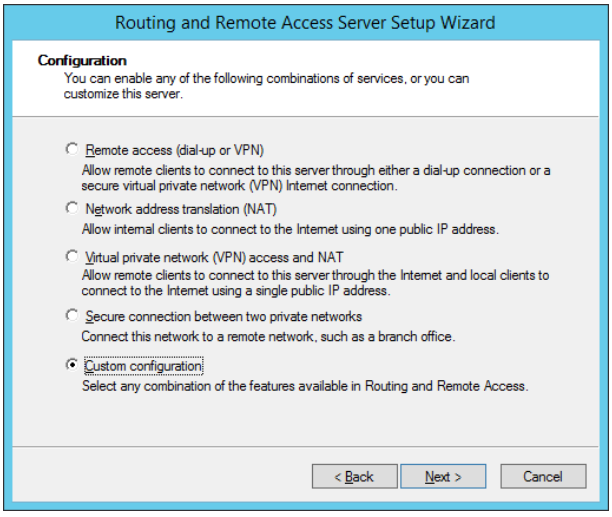
Assign user vpn2 to 192.168.10.3 where 192.168.10.3 is the first remote client.

And so on...

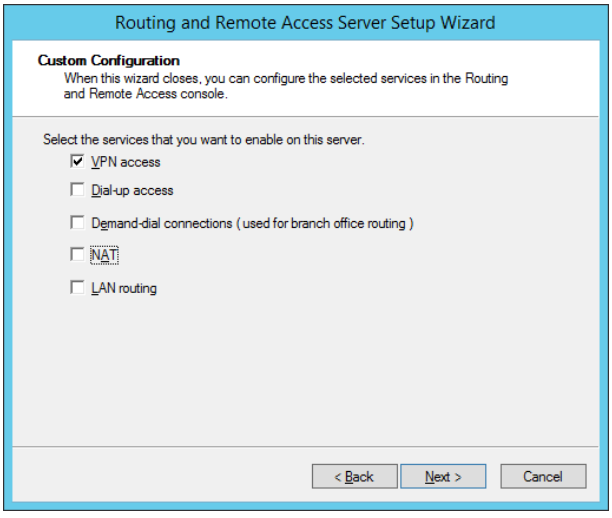
4. Open Server Manager > **Tools** > **Routing and Remote Access**. Right-click the server and select **Configure and Enable Routing and Remote Access**



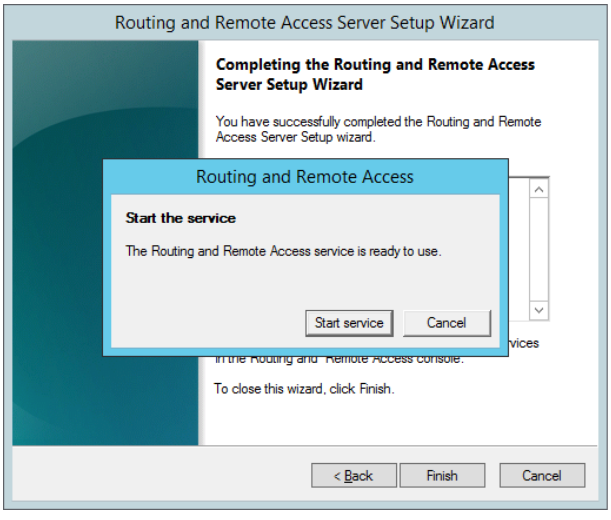
5. Select **Custom configuration** and click **Next**



6. Select **VPN access**

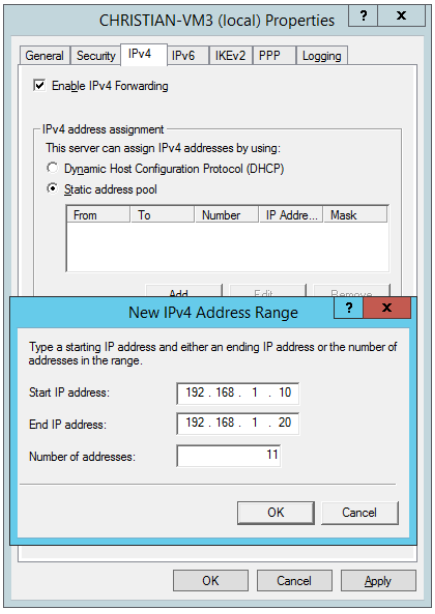


7. Click the buttons **Next** then **Finish** then, in the popup window, **Start service**

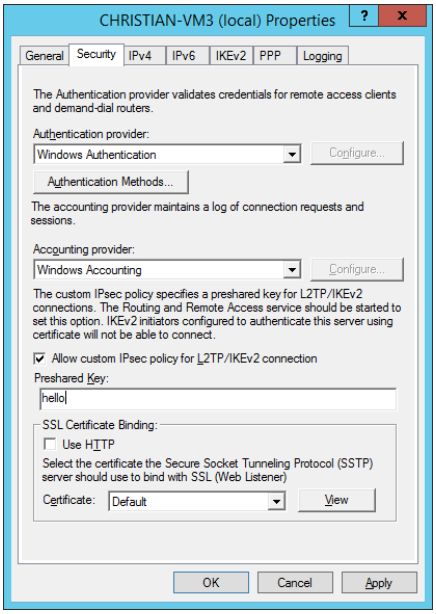


8. Open the properties of the server and click **IPv4** tab. Select **Static address pool** and enter the range of IP addresses that are to be assigned to connecting VPN clients.

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**



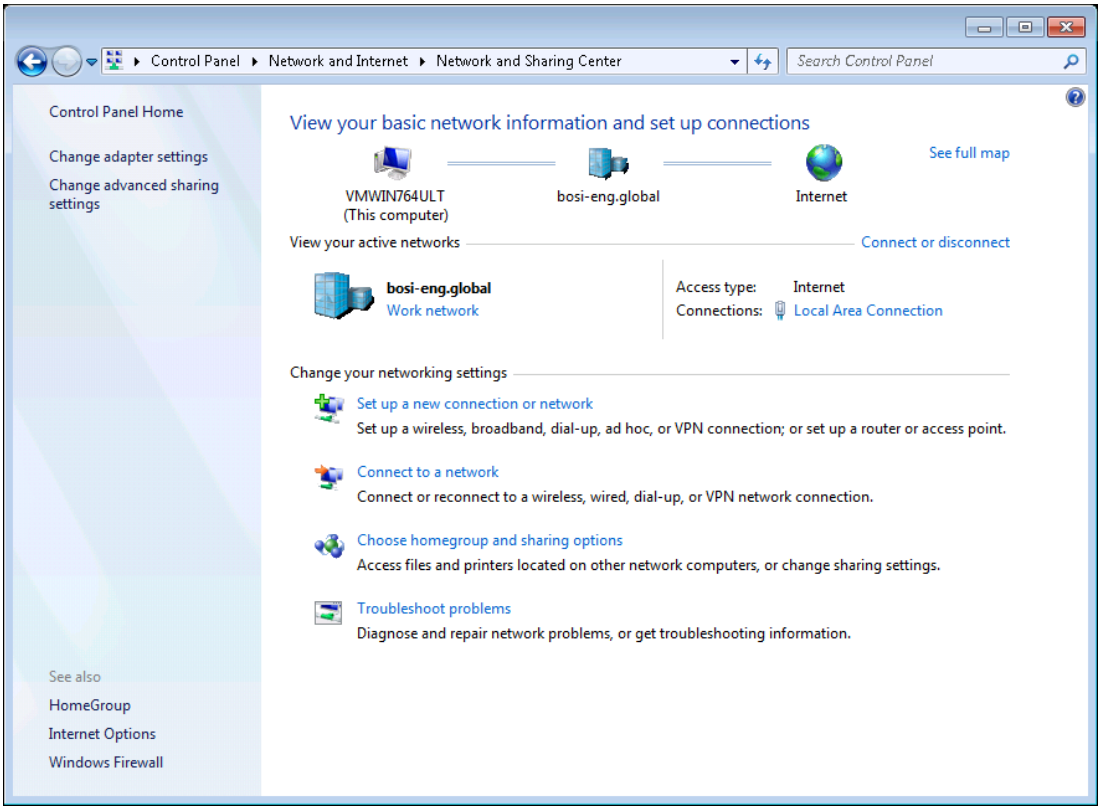
10. A pop-up window will prompt you to restart **Routing and Remote Access**. Click **OK**

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

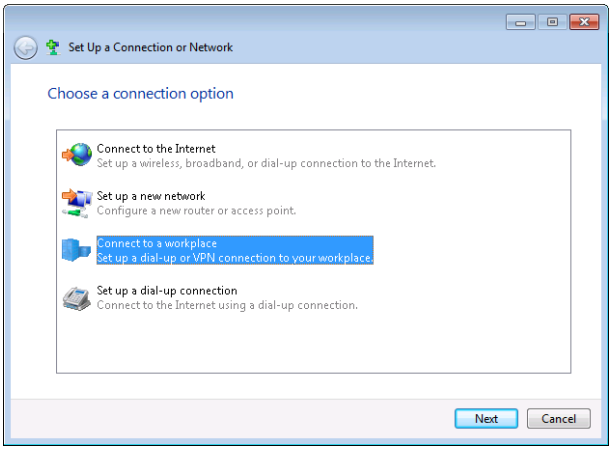
5.7.3 Configure the VPN clients

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 41*.

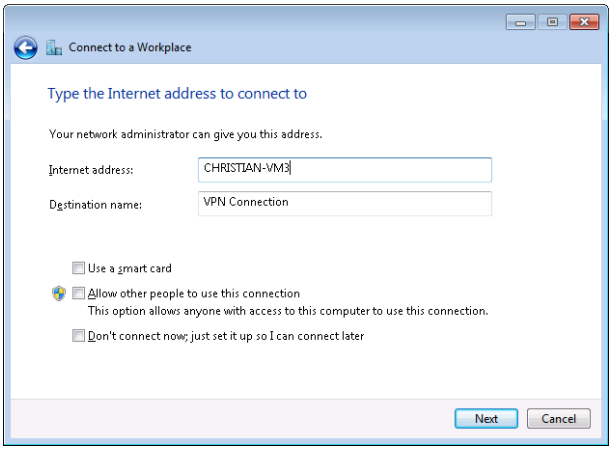
1. On each of the VPN client machines, go to **Network and Sharing Center** and select **Set up a new connection or network**



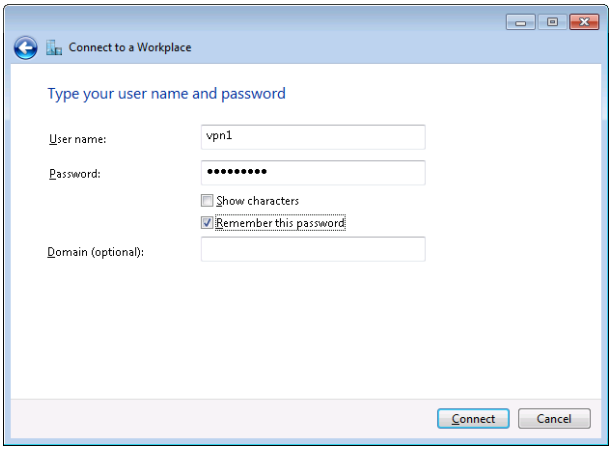
2. Select **Connect to a workplace** and click **Next**.
   Take the settings **Use my Internet connection (VPN)** > **I'll set up an internet connection later.**



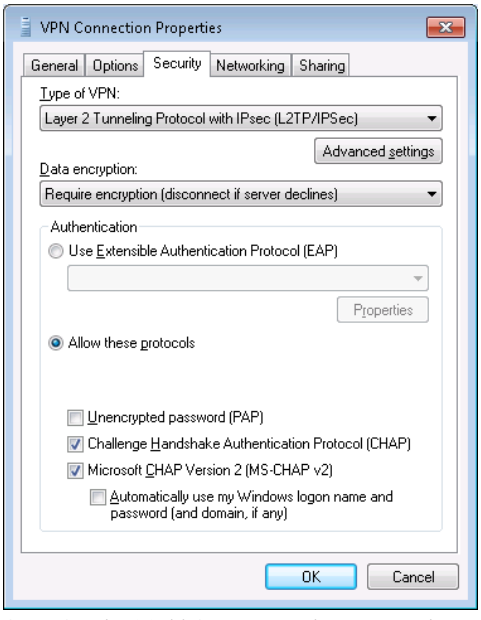
3. On the Connect to a Workplace page, enter the hostname of the VPN server



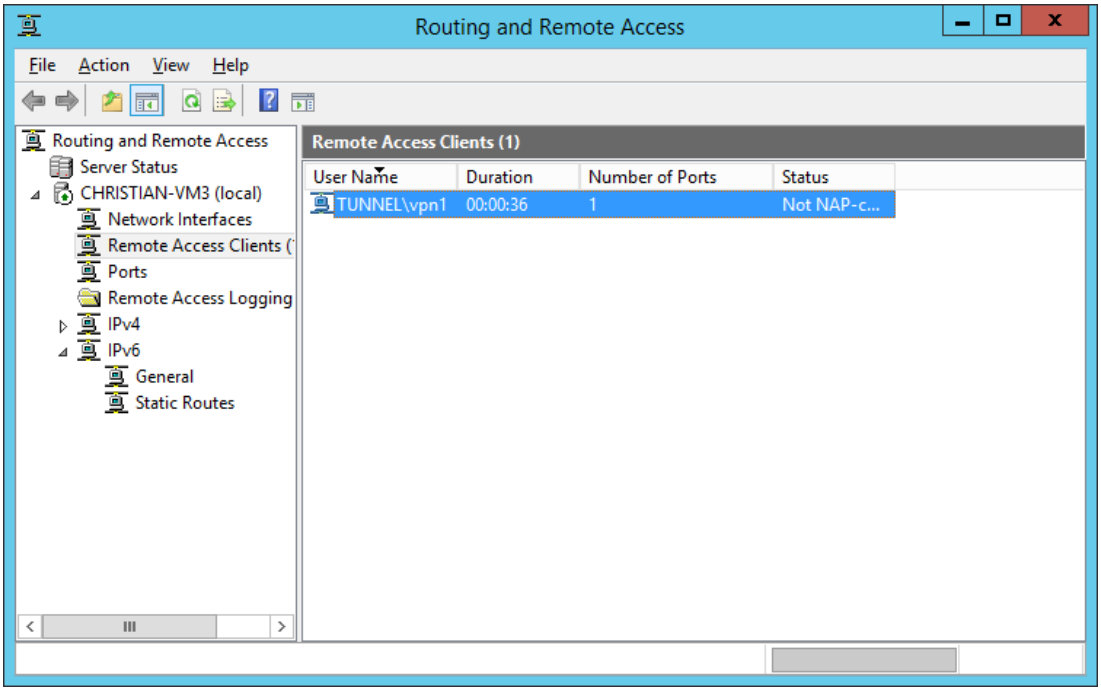
4. Enter the user that you created earlier in the Active Directory, in this case vpn1



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).

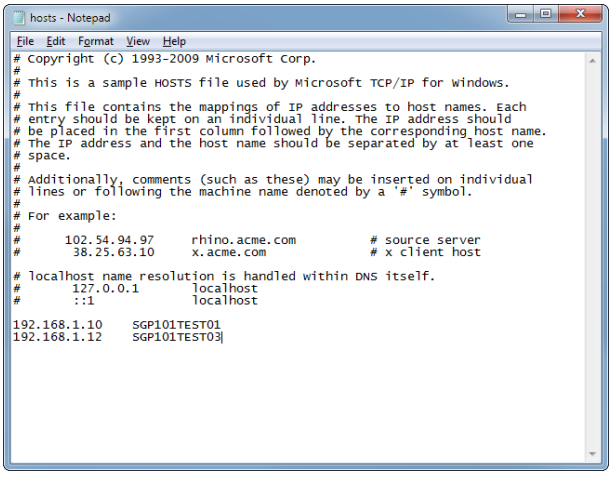
5.7.4 Direct data traffic through the tunnel

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`



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.

6 Secure operation

6.1 Deactivation of BIS 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.

6.2 Administrator and Service Account Password Management

After installing BIS, all default and privileged user accounts must have their passwords changed immediately. This includes:

- Default privileged accounts:
  - "Administrator"
  - "BIS"
- Users with access to the configuration browser:

Update their passwords via the configuration browser interface.

The ChangePassword Tool

System administrators must use the ChangePassword tool to manage the passwords of internal BIS service users across both the Windows operating system and SQL Server environments.

Usage Scenarios

1. Password file deleted:

If the `DbUserInfo.crp` password file is deleted, use the tool to:

- Update the Mgts-SSRSViewer password.
- Update all other SQL user passwords.

1. Remote SQL instance:

- The tool will update both the local machine and the remote SQL server.
- Admin credentials for the remote machine will be requested if necessary.

2. Connection servers or multi-server BIS environments:

- Run the tool individually on each connection server.
- Ensure the same Mgts-Service password is used across all servers.
- In a provider-consumer (multi-server) setup, the tool must be run separately on both machines.

6.3 BIS Operator Password Management

When a BIS operator changes their password, the client retrieves the applicable password policy from the BIS login server. The password dialog will enforce these policy settings dynamically.

Password Length Configuration

The minimum password length is customizable via:

- **Local Security Policy > Account Policies > Password Policy**

Limitations:

- If configured length is 0 to 3 characters, BIS will still enforce a minimum of 4 characters.
- If configured length is above 50 characters, BIS limits passwords to 50 characters maximum.

6.4 Password Policies and Strength Requirements

To maintain strong security across the BIS system, follow the guidelines below when setting or changing passwords for all user accounts.

General Best Practices:

- Change default credentials immediately after installation.
- Use a tool or password manager to verify password strength.
- Change passwords only when there is a valid reason (e.g., compromise), not on arbitrary schedules, to avoid weak user behavior.

Recommended Password Composition:

- Easy to recall but difficult to guess.
- Minimum of 8 characters.
- Must include at least three of the following character types:
  - Uppercase letters (A-Z), including diacritic, Greek, and Cyrillic characters.
  - Lowercase letters (a-z), including sharp-s (ß), diacritics, Greek, and Cyrillic characters.
  - Base-10 digits (0-9).
  - Special characters (e.g., ! $ # %).

Note: Currency symbols like the Euro (€) or British Pound (£) are not considered special characters for policy compliance.

Avoid Using:

- Names of family, friends, pets, birthdates, or pop culture references.
- Dictionary words or common patterns like "12345" or "qwerty".
- Simple passwords modified with just a special character at the beginning or end (e.g., "Password1!").

Technical Enforcement (Microsoft Policy Requirements)

Ensure the following Microsoft security policy setting is enabled:

Passwords must meet complexity requirements

This enforces:

- Passwords must not contain the username or more than two consecutive characters from the full name (case-insensitive).
- Must meet the complexity described above.

6.5 Password management with SSO

When Single Sign-On (SSO) is enabled, password management for SSO-authenticated users (operators) is delegated to the external identity provider and is not configurable within BIS.
Please refer to the system identity provider's documentation for details on password management policies and procedures.

7 Security monitoring

Because requirements are constantly changing, 100% security is never guaranteed. Therefore, a structured vulnerability and incident management process is established at Bosch to professionally manage potential product security vulnerabilities and incidents.

The professional systematic handling of reported security vulnerabilities as well as transparency towards our customer is very important for us. That is why we investigate all vulnerability reports. We perform an evaluation of product security vulnerabilities according to the Common Vulnerability Scoring System (CVSS). CVSS is a free and open industry standard for assessing the severity of computer system security vulnerabilities. Scores are calculated based on a formula that depends on several metrics that approximate ease of exploit and the impact of exploit. Scores range from 0 to 10, with 10 being the most severe.

In case of confirmed vulnerability, we inform customers about an identified security vulnerability in product or solution and its remediation by publishing of security advisory. All security advisories contain:

- Description of the vulnerability with Common Vulnerabilities and Exposures (CVE) reference and CVSS score.
- Identity of known affected products and software/hardware versions.
- Information on mitigating factors and workarounds.
- Timeline and the location of available fixes or other remedial measures.

You can find the list of published Security Advisories on our website https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html.

Whenever you think you have identified a vulnerability or any other security issue related to a Bosch product or service, contact the Bosch Product Security Incident Response Team (PSIRT): https://psirt.bosch.com.

8 Secure disposal and 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.

8.1 Uninstallation of BIS

1. First stop the BIS Server in the BIS manager tab:**System Start/stop** > Button:**Stop Server component**
2. Uninstall 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 uninstallation

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

9 Appendices

For more information, software downloads, and documentation, go to the respective product pages in the product catalog: https://www.boschsecurity.com

9.1 Abbreviations used

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 Access Management System (AMS). 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 outdated encryption protocol for data transmission in IP-based networks (see TLS).

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 is a cryptographic protocol for secure network communication.

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

Building solutions for a better life

202510301108