BeyondInsight
Installation Guide 6.10

TC:2/11/2020

Table of Contents

BeyondInsight Installation Guide

This guide provides instructions and procedures for installing your BeyondInsight software.

Two software components comprise the solution: BeyondInsight management console and BeyondTrust Network Security Scanner. Analytics & Reporting is a supplementary configuration launched from the console and does not require a separate installer. Having a conceptual understanding of BeyondInsight's architecture is valuable before installing and configuring the components.

BeyondInsight is the industry's most innovative, comprehensive privileged access management platform that maximizes visibility, simplifies deployment, automates tasks, improves security and reduces privilege-related risks.

BeyondInsight does not perform vulnerability scans directly. Instead, it sends requests to the Network Security Scanner, which is the engine that performs all vulnerability assessments. It can run as standalone software, but when paired with BeyondInsight, scan results are sent securely to the management console to populate the SQL Server database.

Analytics & Reporting is an additional web-based interface that provides comprehensive analytical tools and that creates reports from collective scan data. It facilitates trending and delta reports, anomaly detection, regulatory compliance, and prioritization.

Note: *By default, the scanner is installed as a standalone component that does not initially recognize the console. You will configure the scanner to receive scan job requests from BeyondInsight and send completed scan results back securely.*

Note: *This guide assumes familiarity with Microsoft Server and SQL Server 2012 and later versions.*

BeyondInsight Requirements

The table below indicates the minimum software and hardware requirements for BeyondInsight.

Operating System	Windows Server 2012, 2012 R2, 2016 (64-bit), and 2019 (64-bit) ***Note:*** *Integration with Windows Server Update Services on Windows Server 2016+ is not supported.*
Database	Microsoft SQL Server 2012-2017 Microsoft SQL Standard or Enterprise Editions Microsoft SQL Server Reporting Services Microsoft SQL Server Analysis Services Microsoft SQL Server Integration Services ***Note:*** *SQL Server collation must be set to* ***SQL_Latin1_ProductNames.CP1_CI_AS****.*
Processor	Intel Dual Core 2.0 GHz (or compatible) ***Tip:*** *Assign two processors when installing BeyondTrust Network Security Scanner and the management console on a single virtual machine. This greatly improves performance.*
Memory	16 GB (requires x64 OS)
Hard Drive	500 MB (software install) 40 GB (database minimum)
Network	Network Interface Card (NIC) with TCP/IP enabled
Server Requirements	Microsoft .NET Framework version 4.7.2 with Application Server Role, Windows Process Activation Service Support, HTTP Activation Microsoft Internet Information Server (IIS) 7.0 or later with ASP.NET support and Web Server (IIS) Role
Client Requirements	Adobe Flash Player 32.0 or later

Note: *Installation on domain controllers or small business servers is not supported.*

Server Requirements

After you configure BeyondInsight, ensure the following IIS roles, server roles, and features in Server Manager are set.

Note: *Some features are selected by default.*

Windows Server 2012

- Web Server (IIS)
  - Common HTTP Features
    - Default Document
    - Directory Browsing
    - HTTP Errors
    - Static Content
    - HTTP Redirection
  - Health and Diagnostics
  - Performance
  - Security
    - Request Filtering
    - Basic Authentication
    - Client Certificate Mapping Authentication
    - Digest Authentication
    - IIS Client Certificate Mapping Authentication
    - IP and Domain Restrictions
    - URL Authorization
    - Windows Authentication
  - Application Development
    - .NET Extensibility 3.5
    - .NET Extensibility 4.5
    - ASP.NET 3.5
    - ASP.NET 4.5
    - ISAPI Extensions
    - ISAPI Filters
- Application Server
  - .NET Framework 4.5
  - Web Server (IIS) Support
  - Windows Process Activation Service Support
    - HTTP Activation
- Application Server Features
  - .NET Framework 4.7.2 Features
    - .NET Framework 4.7.2
    - HTTP Activation

- .NET Framework 4.5 Features
  - .NET Framework 4.5
  - ASP.NET 4.5
  - WCF Services
    - HTTP Activation
    - TCP Port Sharing

Windows Server 2016

- Web Server (IIS)
  - Common HTTP Features
    - Default Document
    - Directory Browsing
    - HTTP Errors
    - Static Content
    - HTTP Redirection
  - Health and Diagnostics
  - Performance
  - Security
    - Request Filtering
    - Basic Authentication
    - Client Certificate Mapping Authentication
    - Digest Authentication
    - IIS Client Certificate Mapping Authentication
    - IP and Domain Restrictions
    - URL Authorization
    - Windows Authentication
  - Application Development
    - .NET Extensibility 3.5
    - .NET Extensibility 4.5
    - ASP.NET 3.5
    - ASP.NET 4.5
    - ISAPI Extensions
    - ISAPI Filters
  - Management Tools
    - IIS Management Console
    - IIS Management Scripts and Tools
    - Management Service

- Application Server
  - Windows Process Activation Service
    - Process Model
    - .NET Environment 3.5
    - Configuration APIs
- Application Server Features
  - .NET Framework 4.7.2 Features
    - .NET Framework 4.7.2
    - HTTP Activation
  - .NET Framework 4.7.2 Features
    - .NET Framework 4.7.2
    - ASP.NET 4.6
    - WCF Services
      - HTTP Activation
      - TCP Port Sharing

Windows Server 2019

- Web Server (IIS)
  - Common HTTP Features
    - Default Document
    - Directory Browsing
    - HTTP Errors
    - Static Content
    - HTTP Redirection
  - Health and Diagnostics
  - Performance
  - Security
    - Request Filtering
    - Basic Authentication
    - Client Certificate Mapping Authentication
    - Digest Authentication
    - IIS Client Certificate Mapping Authentication
    - IP and Domain Restrictions
    - URL Authorization
    - Windows Authentication
  - Application Development
    - .NET Extensibility 3.5
    - .NET Extensibility 4.5

        - ASP.NET 3.5
        - ASP.NET 4.7
        - ISAPI Extensions
        - ISAPI Filters
    - Management Tools
        - IIS Management Console
        - IIS Management Scripts and Tools
        - Management Service
- Application Server
    - Windows Process Activation Service
        - Process Model
        - .NET Environment 3.5
        - Configuration APIs
- Application Server Features
    - .NET Framework 4.7.2 Features
        - .NET Framework 4.7.2
        - HTTP Activation
    - .NET Framework 4.7.2 Features
        - .NET Framework 4.7.2
        - ASP.NET 4.6
        - WCF Services
            - HTTP Activation
            - TCP Port Sharing

Client Requirements

BeyondInsight and Analytics & Reporting use a browser-based interface, making the client a web browser. Therefore, the requirements apply to any machine, including the machine where BeyondInsight is installed, that uses a browser to access BeyondInsight or Analytics & Reporting consoles.

Database Requirements

Before installing the console, log in as a domain or local administrator and install the SQL Server database.

Supported Versions:

- SQL Server 2012 and 2012 R2
- SQL Server 2014
- SQL Server 2016
- SQL Server 2017

> ***Note:*** *Microsoft SQL Server Express is not supported and will cause installation errors if attempted.*

Components to Install:

- Database Engine Services
- Analysis Services
- Reporting and Integration Services
- SQL Server Management Studio

Service Accounts:

- SQL Server 2012, 2014: Accept the **default service accounts**. An individual account is automatically created for each service.
- Set the SQL Server Agent start mode as **Automatic** (the default is Manual).
- Select **Windows authentication mode**.

> ***Note:*** *You can select **Mixed mode authentication**, if desired, and provide the **sa** account password. However, this is not necessary when SQL Server resides on the same machine as the console.*

- Select **Add Current User** when setting the **SQL Server Administrator** and **Analysis Services Administrator**.

Database Permissions Matrix

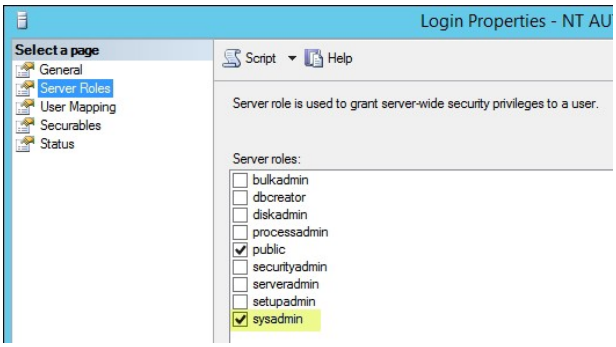
Permission	SQL Server
SQL Authentication (SQL Local or SQL Remote)	Assign the SQL Server account the role of **sysadmin**.
Windows Authentication (SQL Local)	Assign **NT AUTHORITY\SYSTEM** the role of **sysadmin**, if not previously assigned. Add **NT AUTHORITY\NETWORK SERVICE** as a **Login** account in SQL Server, if not previously added. On the BeyondInsight database, assign **NT AUTHORITY\NETWORK SERVICE** the roles of **db_owner** and **REM3Admins**. ***Note:*** *REM3Admins is a custom role created by the installer.*

Permission	SQL Server

Windows Authentication (SQL Remote, where SQL Server and BeyondInsight are on the same domain or in trusted domains of a forest)	In SQL Server, create a local Windows group and add the group to the SQL Server instance.
	
	On the BeyondInsight database, assign the account the roles of **db_owner** and **REM3Admins**.
	
	Add each BeyondInsight machine to this local group, including any Event Collector machines or Password Safe worker node machines, in the format:
	
	`'Domain\MachineName1$',`
	`'Domain\MachineName2$'`
	
	Note: *Windows Authentication is not supported on remote standalone systems. UVM appliances and software must be on the domain or a trusted domain in a forest.*

Set the Server Role on NT AUTHORITY\SYSTEM

1. In SQL Server Management Studio, go to **Security > Logins**.
2. Right click **NT AUTHORITY\SYSTEM** and select **Properties**.
3. Select **Server Roles > sysadmin**, then click **OK**.



ADOMD.net Requirement

The BeyondInsight web server uses SQL ADOMD.net components to communicate with the SQL Analysis Services cube. In cases where the web server does not have SQL installed, you must manually install the ADOMD.net components. The **SQL_AS_ADOMD.msi** file is included with BeyondInsight and can be found in the **Support** folder. After installing the ADOMD.net components, you may need to restart IIS.

Port Requirements

BeyondInsight

Function	Traffic	Port
Database Connectivity	Management console to SQL Server, Analytics & Reporting to SQL Server	1433
Event Collector	BeyondTrust Network Security Scanner to BeyondInsight	21690
Enterprise Vulnerability Management Central Policy	Endpoint to the console	v1: 2000 v2: 443
Central Policy	BeyondTrust Network Security Scanner to the console	v1: 10001 v2: 443
Update Servers	SyncIt or EUS to the BeyondTrust server	443 or 80
BeyondTrust Updater Enterprise		443

Function	Traffic	Port
Client Browser	User to BeyondInsight or Analytics & Reporting	443 or 80
Privilege Management for Desktops	Connector to web services	443

UVM Appliance

Function	Traffic	Port
Database Connectivity	BeyondInsight to SQL Server, Analytics & Reporting to SQL Server	1433
Event Collector	Network Security Scanner or Privilege Management to BeyondInsight	21690
Mobile Agents and Privilege Management for Desktops	Connector to web services	443
Update Servers	SyncIt or EUS to the BeyondTrust server	443 or 80
Android Mobile Connector	Android agents to BeyondInsight	21691
Enterprise Vulnerability Management	Endpoint to BeyondInsight	v1: 2000 v2: 443
Central Policy	BeyondTrust Network Security Scanner to the console	v1: 10001 v2: 443
Update Servers	SyncIt or EUS to the BeyondTrust server	443 or 80
Client Browser	User to BeyondInsight or Analytics & Reporting	443 or 80
Windows Passwords	Password Safe service to client	135, 139, 445, 389
UNIX, Linux, Other	Password Safe service to client	22
Database	Password Safe service to client	1433
RDP Client and Target Proxy Session Monitoring		4489, 3389
SSH Client and Target Proxy Session Monitoring		4422, 22
High Availability BeyondInsight		443, 5022
Email Notifications		25
Appliance Discovery Tool		4069

Password Safe

Function	Service	Port	Protocol
System Discovery			
User enumeration	nb-ssn, ms-ds	139, 445	TCP
Hardware enumeration*	nb-ssn, ms-ds	139, 445	TCP
Software enumeration†	nb-ssn, ms-ds	139, 445	TCP
Local scan services	ms-ds	445	TCP
Password Change			
Windows password change‡	adsi-ldap	389	TCP
Windows update and restart services*	wmi	135	TCP
Active Directory password change‡	adsi-ldap	135	TCP

Function	Service	Port	Protocol
User and computer authentication, forest-level trusts	kerberos	88	TCP and UDP
UNIX, Linux, macOS	ssh	22	TCP
Oracle	oracle-listener	1521	TCP
Microsoft SQL Server	netlib	1433	TCP
HP ILO	ssh	22	TCP
Dell DRAC	ssh	22	TCP
Session Management			
Remote Desktop	rdp	3389	TCP
SSH	ssh	22	TCP
Appliance			
Mail server integration	smtp	25	TCP
Active Directory integration	ldap	389	TCP
Backup	smb	445	TCP
Time Protocol	ntp	123	TCP
High-availability replication (pair)	sql-mirroring, https	5022, 443	TCP

* WMI service running on target

† Remote registry service running on target

‡ As a fallback, uses ms-ds, 445, TCP

Install the BeyondInsight and BeyondTrust Network Security Scanner

Install the BeyondInsight Software

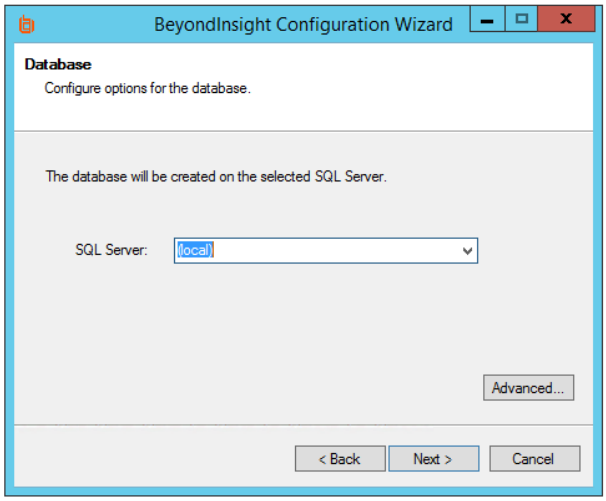
1. After BeyondTrust generates your customer license, you will receive an email that includes a link to download product installers. Download the installers to your system.
2. Run the downloaded BeyondInsight installer.
3. Enter the console license key (serial number).
4. Follow the default prompts.
5. When prompted, supply the license registration information.

> ***Note:*** *If you have already installed BeyondTrust Network Security Scanner, the license registration information automatically populates.*

> ***Note:*** *Required audit upgrades download after the installation is complete. Audit upgrades may take some time to complete, depending on the number of pending updates.*

Run the Configuration Wizard

1. After the software is installed, the BeyondInsight Configuration Wizard automatically starts.
2. On the **Database** page, set **SQL Server** to **(local)** if the server is on the same machine and will use the logged on Windows credentials to connect.
3. Otherwise, click the **Advanced** button to enter database information, including the server name, database name, and database credentials.



> ***Note:*** *If you select an existing BeyondInsight database, the database version number must match the installer version.*

4. The **Web Site Information** page informs you that the console will be implemented as the default IIS web site.
5. On the **Agent Password** page, create a password that will be used to configure the connection between the scanner and the console. This password is required to retrieve Central Policy information and to import certificates using the Events Client Configuration tool. The created password must match the machine's password requirements.
6. On the **Event Server Information** page, you may configure SNMP.
7. On the **Email Information** page, you may provide a default SMTP mail server and account. This may be used, for example, to automatically email a report after a vulnerability scan completes.

> ***Note:*** *The SMTP mail server and email address you provide are not verified by the configuration wizard.*

8. On the **Administrator Password** page, create an initial login account to the console. This account will have full rights to the console. The created password must match the machine's password requirements.

> ***Note:*** *This is NOT the local machine administrator or domain administrator account.*

9. The database is now created. Please plan for this process to take about ten minutes.
10. Once complete, click **Finish**.
11. The management console now starts in your default browser. You can log in with the administrator credentials created during this process.

Install the Network Security Scanner

1. To install the scanner, run the downloaded Network Security Scanner installer.
2. Enter the license key (serial number).
3. Follow the default prompts.
4. When prompted, supply the license registration information.
5. The auto-update process runs, contacting the BeyondTrust servers. This can take several minutes.
6. Once complete, the Network Security Scanner automatically starts.

Set Up BeyondInsight Certificates

Certificates are used for secure communication between agents and BeyondInsight. Two types of certificates are used:

- **SSL certificate:** Required to encrypt communication
- **Client certificate:** Required to authenticate a client

You can use BeyondInsight certificates or create custom certificates using the BeyondInsight Configuration Tool.

Work with BeyondInsight Certificates

The following certificates are used for communication between BeyondTrust software and BeyondInsight:

- **eEyeEmsCA:** Certification authority (CA) certificate
- **EmsClientCert:** Client authentication certificate
- **eEyeEmsServer:** Server authentication certificate

The CA certificate generates and validates client and server certificates. It is located on both the agent and the server in Trusted Root Certification Authorities in the Local Machine Store.

When connecting to BeyondInsight Web Service (for example, when Privilege Management for Desktops connects to the Event Service), the EmsClientCert is used to authenticate the client, and the SSL certificate is used to encrypt the data. This prevents anonymous connections to the services. Typically, a certification authority such as VeriSign validates anonymous clients.

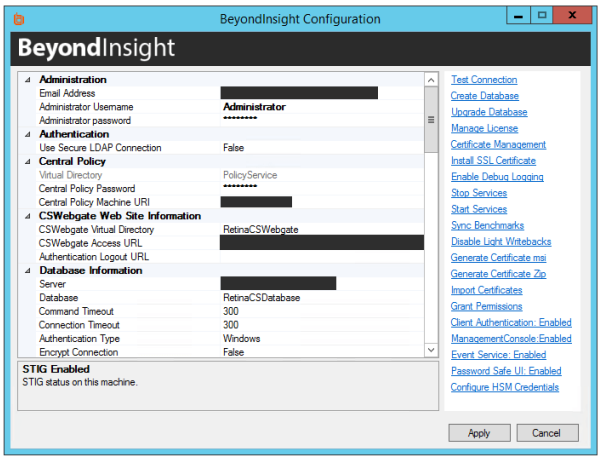
With BeyondInsight, a self-signed certificate is created and distributed with the client certificate. BeyondInsight can then work in a variety of environments, especially where network connectivity is an issue. This avoids the need to register each system instance with an online CA.

Internally, each client certificate contains a private-public key pair. During the SSL handshake, the server requests the client certificate. The client authenticates the certificate before initiating the connection, and the server validates it again when it is received.

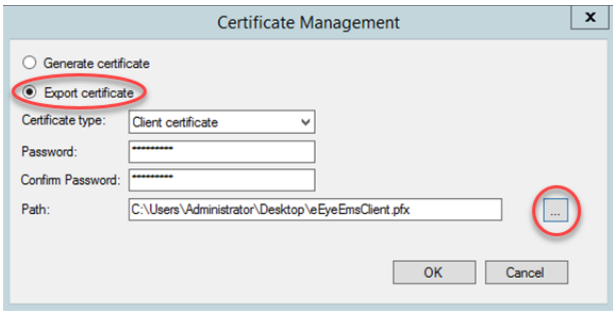
Install the eEyeEmsServer certificate on the server in the **Local Machine Store**, under the **Personal Store**. To verify that the certificate is valid, double-click the certificate.

The EmsClientCert certificate is used for communication between the agent and server when sending and receiving events. It is also used for communication between the agent and server when deploying Privilege Management Endpoint Protection Platform agents. The certificate must be exported from the server and then imported on the agent.

1. Open the BeyondInsight Configuration Tool.
2. Click the **Certificate Management** link.



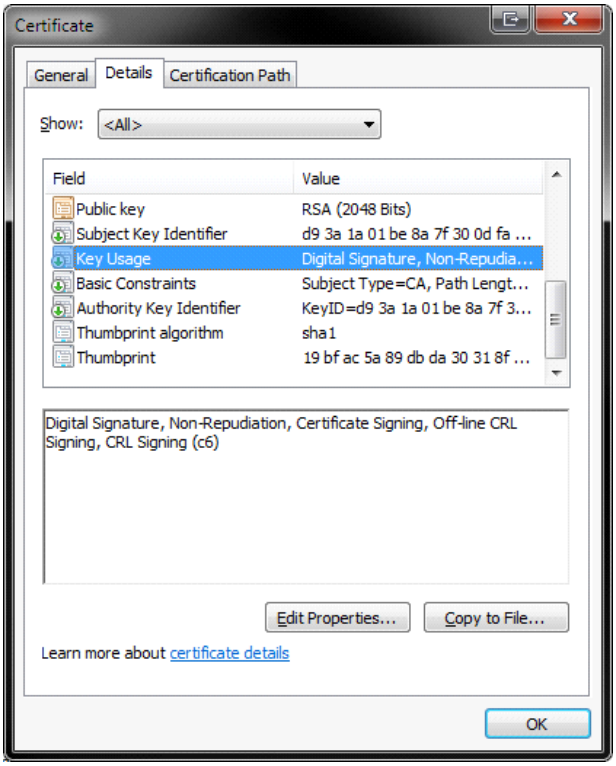
3. Select **Export certificate**.
4. Select **Client Certificate** as the **Certificate type**.
5. Enter a chosen **Password**. We recommend that you use the existing BeyondInsight Central Policy password.
6. Click the ellipses (**...**) to browse to your desired location.
   a. Enter a **File name** and select **Certificate files (*.pfx)** as the **Save as type**. We recommend that you name the certificate **eEyeEmsClient.pfx**.
   b. Click **Save**.
   c. Verify the **Path** has been filled in correctly.
7. Click **OK**.



Troubleshoot BeyondInsight Certificates

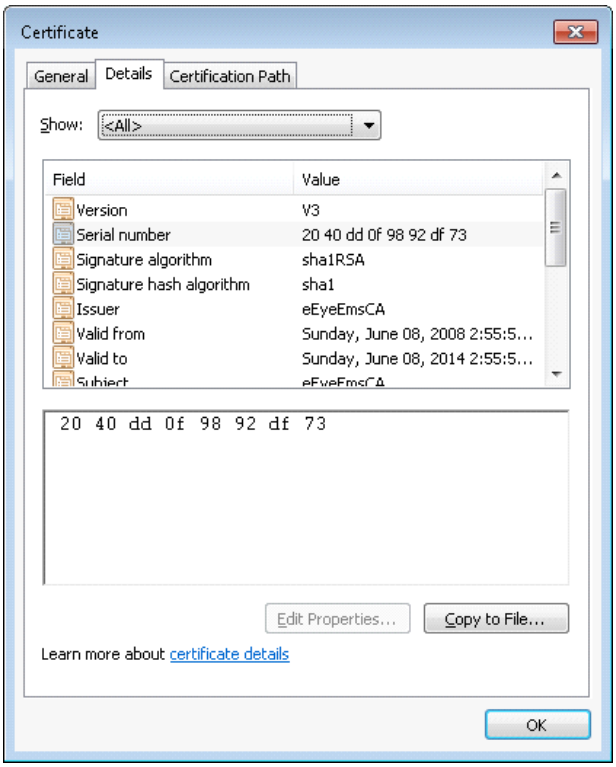
When troubleshooting certificate issues, check the following:

- **Is the eEyeEmsCA certificate expired?**
- **Does the certificate store have more than one version of the eEyeEmsCA certificate?**
- **Does the eEyeEmsCA certificate have the correct usage identifiers in place?**
- **Does the EmsClientCert certificate have the correct usage identifiers in place? Does it have the private key present?**



- **Does the eEyeEmsCA exist on both the agent and the server?** Make sure the certificate on the agent has the same serial number as the certificate on the BeyondInsight server. To view the serial number, double-click the certificate in the certificate manager.
- **Was the eEyeEmsCA certificate regenerated or removed?** Regenerating or removing the eEyeEmsCA certificate invalidates any certificate that was generated using the old CA certificate. This breaks the communication between the agents and the server until the client and server certificates are regenerated on the server and the new client certificate is deployed on all agents connecting to BeyondInsight.
- **Did the Central Policy password change?** If you change the Central Policy password using the BeyondInsight Configuration Tool, the password change is not automatically applied to EmsClientCert.pfx.

  If you change the Central Policy password and then deploy Privilege Management Endpoint Protection Platform on a target, the package includes the certificate with the old password. In this scenario, the events communication will not be successfully configured on the target. Using the BeyondInsight Configuration Tool, generate a new client certificate with a new password that matches the Central Policy password.



Use a Domain PKI for BeyondInsight Communication

If you choose to create a custom certificate, keep in mind the following considerations:

- You can modify templates using the **Certificate Templates Console** (**certtmpl.msc**).
- The default Computer template meets the requirements for BeyondInsight communication. However, to update any particular BeyondInsight configuration settings, you must copy the Computer template and make your changes in the copy.
- To issue the new template, use the **certsrv.msc** snap-in.

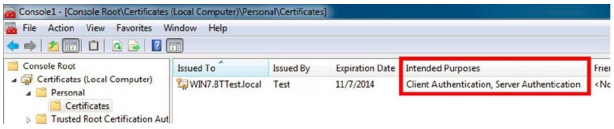
> For detailed procedures on creating a custom domain certificate, please see Microsoft's documentation.

Prerequisites

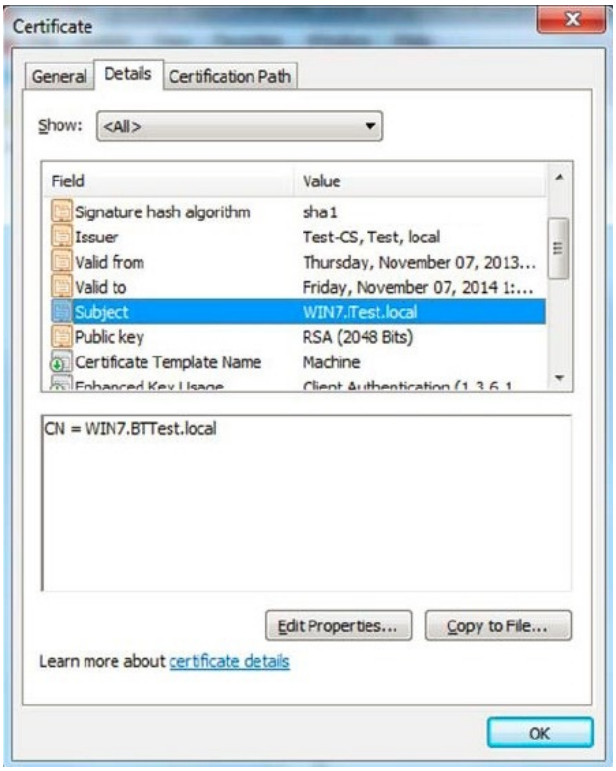
- Domain member server with Active Directory Certificate Services installed and configured.
- Certificate Authority Web Enrollment role installed

Requirements

- The certificates must be configured as **Server Authentication** and **Client Authentication** in the **Intended Purposes** section of the certificate.

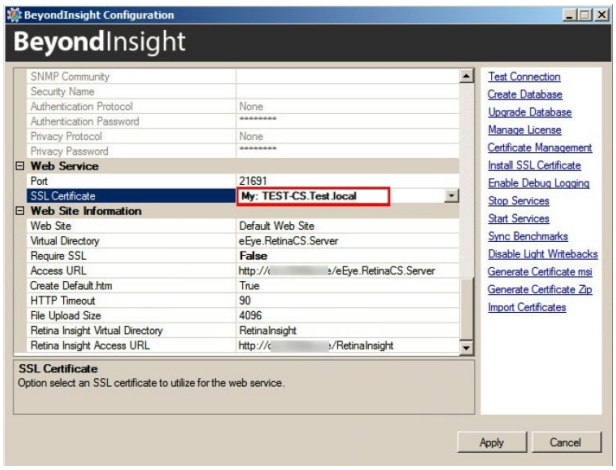


- The **Subject** key must contain common text for all client certificates.



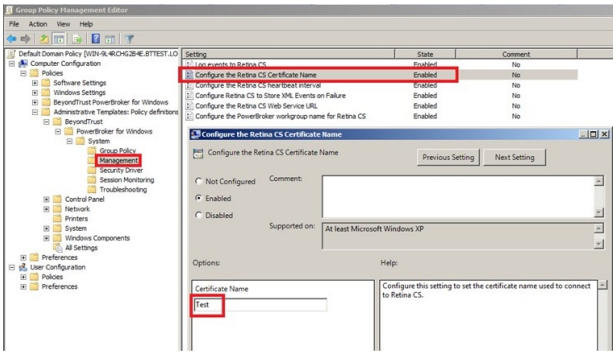
Assign the SSL Web Service Certificate in BeyondInsight

1. Start the BeyondInsight Configuration Tool.
2. Scroll to **Web Service** in the list.
3. Select the domain PKI certificate from the list.
4. Click **Apply**.



Configure a Client Certificate for Privilege Management for Desktops

1. In **Group Policy Management Editor**, edit the group policy you use for your Privilege Management for Desktops targets.
2. Go to **Administrative Templates > BeyondTrust > Privilege Management for Desktops > System > Management**.
3. Double-click the setting **Configure the BeyondInsight Certificate Name**.
4. Enter the common text you used in the client certificate **Subject** key.



Configure Auto Enrollment

1. In **Group Policy Management Editor**, edit the group policy you use for your Privilege Management for Desktops targets.
2. Go to **Computer Configuration > Windows Settings > Security Settings > Public Key Policies > Automatic Certificate Request Settings**.
3. Right-click in the right pane and select **New > Automatic Certificate Request**.
4. Go through the wizard. On the **Certificate Template** page, select the custom template.

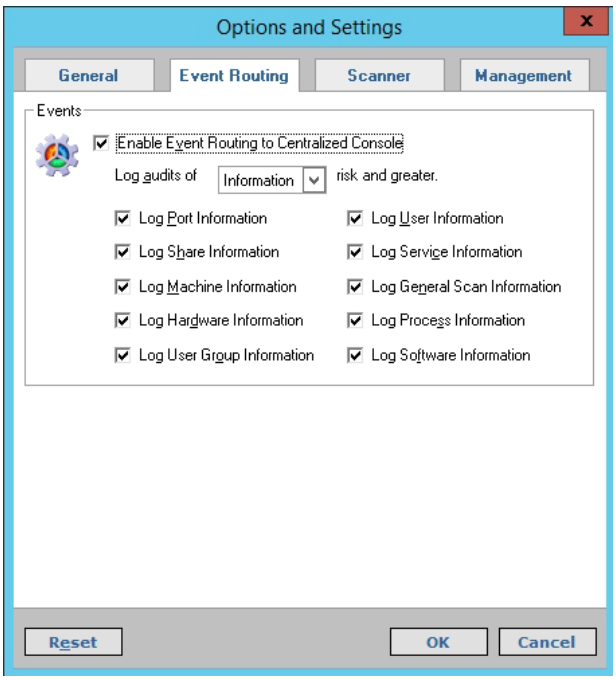
Configure BeyondTrust Network Security Scanner Connections to BeyondInsight

Once the BeyondTrust Network Security Scanner and the console are installed, they must be configured to work together by configuring both Central Policy and Events Client.

Configure Central Policy

Central Policy enables Network Security Scanner to pull scan requests from the console and send scan status updates to the console.

1. To configure Central Policy, run the Network Security Scanner.
2. Select **Tools > Options**.
3. Select the **Event Routing** tab, and then select **Enable Event Routing to Centralized Console**.
4. Select the **Management** tab, and then select **Enable Central Policy**.
5. Enter the required information.
   - **Central Policy Server:** Name or IP address of the machine where the console is installed. If the scanner and console are on the same machine, you can use **localhost**.
   - **Password:** Use the agent password that was defined during BeyondInsight configuration.
   - **Agent Name:** Enter a name that will identify the scanner in the console.



> For more information about the agent password, please see "Run the Configuration Wizard" on page 14.

6. Click the **Test** button.
7. After a few seconds, you should see a confirmation that the connection from the scanner to the console was successful.

   If you instead receive a message that *The connection was refused by the specified server*, verify that the **NT AUTHORITY\SYSTEM** account is assigned the **sysadmin** server role.

> For more information, please see "Database Permissions Matrix" on page 10.

Configure Events Client

The Events Client enables Network Security Scanner to securely send completed scan data to the management console, where it is extracted to populate the database.

1. To configure the Events Client:
   - In Windows 2012 or above, click **Start > Apps > BeyondTrust > Events Client Configuration**.

2. Go through the Events Client installation wizard.

   a. On the **Select a Client Certificate** page, choose a certificate to use.

   > For more information, please see "Set Up BeyondInsight Certificates" on page 16.

   b. When prompted for a password, enter the agent password created during BeyondInsight configuration.

   > For more information about the agent password, please see "Run the Configuration Wizard" on page 14.

   c. On the **Test Connection** page, click **Next**, wait a few seconds, and then verify that a test message was successfully sent to the application bus.

Configure BeyondInsight Analytics & Reporting

Before you can use Analytics & Reporting, make sure that SQL Analysis Services, SQL Reporting and Integration Services, and SQL Report Server are installed and working.

Assign Permissions for Analytics & Reporting

In many cases, an account with local admin or domain admin privileges will suffice. However, in some more advanced deployments, you may desire to assign more specific permissions to installation and user accounts.

Installation User Permissions

When installing Analytics & Reporting, the user account requires SQL Server database access. Ideally, assign the account the **sysadmin** server role. Otherwise, make sure at least the following SQL Server permissions are assigned to the account.

ALTER database	BULKINSERT
CREATE Role	CREATE Application Role
CREATE Schema	CREATE Type
CREATE Table	ALTER Table
UPDATE Table	CREATE UNIQUE NONCLUSTERED INDEX
CREATE NONCLUSTERED INDEX	CREATE PROCEDURE
ALTER PROCEDURE	EXECUTE PROCEDURE
CREATE VIEW	ALTER VIEW
GRANT EXEC, SELECT, INSERT, UPDATE, DELETE	

Configuration User Permissions

The configuration user is the account entered on the **Installation Credentials** page of the configuration wizard. This account requires:

- Local administrator rights to **SQL Analysis Services** so they can deploy the Analysis Services cube
- Permission to create a registry key under **HKEY_LOCAL_MACHINE\SOFTWARE\EEYE**
- The **Log on as Batch Job** security policy on the SQL Server

BeyondInsight Configuration Database Roles

Member in Role	Database
sysadmin	BeyondInsight reporting Required to: • Install the SQL job and the SSIS packages • Create the BeyondInsight reporting database • View SQL job statuses and details. Alternatively, add the configuration user to the **SQLAgentRole** of the **MSDB** database on the BeyondInsight server for lower privileges.
db_owner	BeyondInsight Required to install the stored procedures for BeyondInsight reporting to synchronize data from the BeyondInsight management console.
System User	This role is at the root of the SQL Reporting Services management web site and is required to read information from SSRS.
Browser	This role is on the root folder settings for the SQL Report Services management web site and is required to read and run reports deployed to SSRS.
Content Manager	This role is on the root folder settings for the SQL Report Services management web site and is required to deploy reports to SSRS.

Web Proxy User Permissions

The web proxy user is the account entered on the **Web Service Credentials** page of the configuration wizard.

Note: *These permissions are automatically set up during installation if the installing user has sufficient rights.*

Web Proxy User Roles

Member in Role	Database
BeyondInsightReader	BeyondInsight reporting
BeyondInsightUser	BeyondInsight management console
BeyondInsightReader	BeyondInsight Reporting cube in SQL Analysis Services
System User	This role is at the root of the SQL Reporting Services management web site and is required to read information from SSRS.
Browser	This role is on the root folder settings for the SQL Report Services management web site and is required to read and run reports deployed to SSRS.

SSRS Proxy User Permissions

The SSRS proxy user is the account entered on the SQL Reporting Services (SSRS) page of the configuration wizard.

Note: *These permissions are automatically set up during installation if the installing user has sufficient rights.*

SSRS Proxy User Roles

Member in Role	Database
BeyondInsightReader	BeyondInsight reporting
BeyondInsightUser	BeyondInsight management console
BeyondInsightReader	BeyondInsight Reporting cube in SQL Analysis Services

SQL Agent Service Permissions

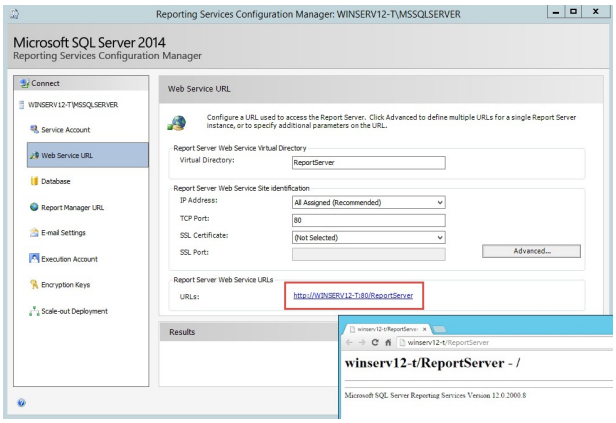
This account runs the daily sync job and requires permission to process the BeyondInsight SSAS database.

SSAS Proxy User Roles

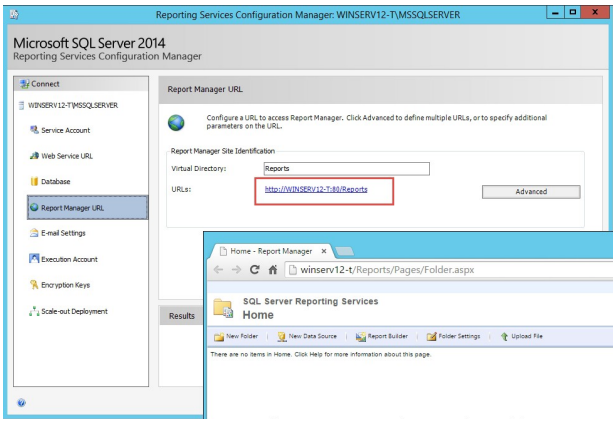
Member in Role	Database
BeyondInsightSSIS	BeyondInsight
BeyondInsightUser	BeyondInsight management console

Verify SQL Report Server Functionality

1. To verify that SQL Report Server is working properly:
   - In Windows 2012 or above, click **Start > Apps > Microsoft SQL Server 20xx > SQL Server 20xx Reporting Services Configuration Manager**.
2. After connecting, select **Web Service URL**.
3. Under **Report Server Web Service URL**, click the link and verify the confirmation web page.



4. Select **Report Manager URL**.
5. Under **Remote Manager Site Identification**, click the link and verify the confirmation web page.



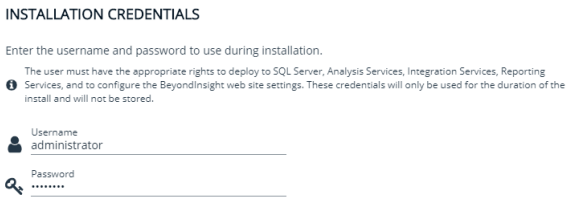
Configure Analytics & Reporting

For more information on the permissions needed to install and use Analytics & Reporting, please see the BeyondInsight Analytics & Reporting Guide at www.beyondtrust.com/docs/beyondinsight-password-safe/documents/bi/bi-analytics-and-reporting.pdf.

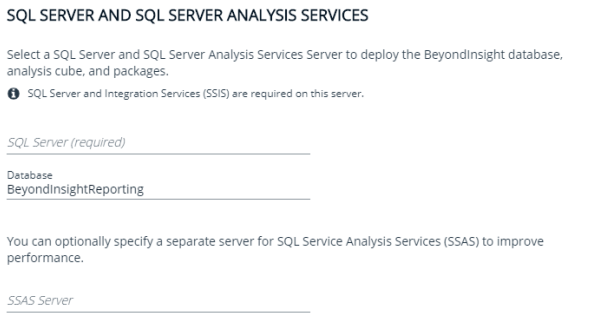
IMPORTANT!

Be careful not to refresh the browser during this process, as doing so will reload the page, requiring you to log in again.

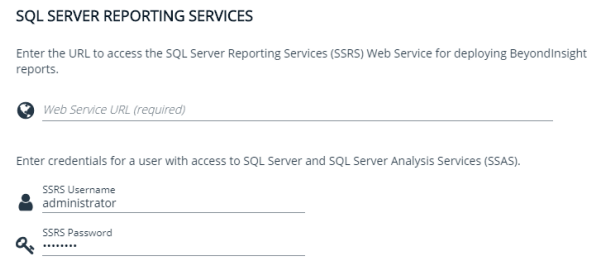
1. Log into the BeyondInsight management console, and then click **Configuration** in the left menu.
2. In the Analytics & Reporting tile, click **Configuration**.
3. Re-enter the administrative credentials used to log into the console.
4. Click **Configure Now**.
5. On the **Installation Credentials** page, enter the local or domain administrator credentials.



6. On the **SQL Server and SQL Server Analysis Services** page, enter the database name.

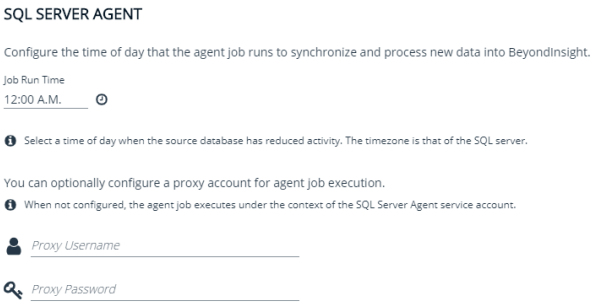


7. On the **SQL Server Reporting Services** page, enter the web service URL in the form of `http://<machine name>:80/ReportServer`.

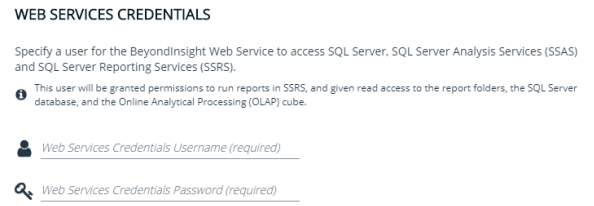


8. On the **SQL Server Agent** page, set a job run time, then enter an administrative username and password to use as a proxy.

> ***Note:*** *You cannot leave this field blank, as the default SQL Server Agent service account created during SQL Server installation does not have the necessary write permissions to the BeyondInsight Reporting database.*

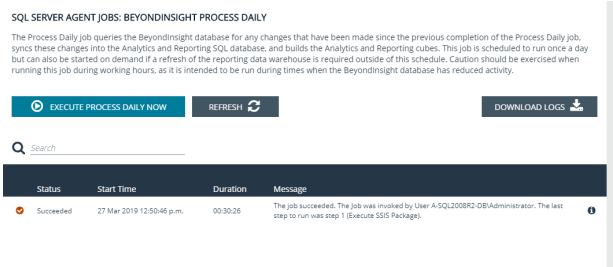


9. On the **Web Services Credentials** page, the username and password should automatically populate. Click **Deploy**.
10. Deployment progress is shown while the BeyondInsight Reporting database is created. When database creation is complete, click **Finish**.
11. Once the deployment completes, select the option to synchronize data now. This critical process reads the database created during management console configuration. It finds the scan results and synchronizes them with the newly created reporting database.



By default, synchronization occurs every day at 12:00 am unless otherwise specified in the **SQL Server Agent** settings. You can also run the synchronization manually. Synchronization takes several minutes to complete.

12. Verify successful synchronization by selecting the **SQL Server Agent Jobs** tab and then clicking **Refresh**.



Patch Management Module

Requirements

- BeyondInsight management console 2.0 or later
- Windows Server 2012 WSUS

Note: *Background Intelligent Transfer Service (BITS) and Windows Server Update Services (WSUS) must be enabled on all clients.*

- Internet Information Services (IIS)
- Windows PowerShell
- .NET Framework 4.5 Features
- The maximum supported version for Microsoft System Center Configuration Manager (SCCM) integration is SCCM 2012 R2 (5.0.7958.1000)

Note: *The SCCM integration supports only a simple topology of a single standalone primary site. BeyondTrust does not currently support a group of connected primary and secondary sites with a central administration site at the top-level site of the hierarchy.*

For more information regarding SCCM topology and configuration, please see Microsoft documentation regarding designing a hierarchy of sites for Configuration Manager at https://docs.microsoft.com/en-us/configmgr/core/plan-design/hierarchy/design-a-hierarchy-of-sites.

Note: *Make sure your license includes the Patch Management module before attempting an install.*

Note: *The Patch Management module cannot be installed on domain controllers or small business servers.*

For more information about Patch Management, please see the *BeyondInsight User Guide* at beyondtrust.com/docs/beyondinsight-password-safe/documents/bi/6-10/bi-user-6-10.pdf.

Mixed WSUS Environments

The fundamental challenge with mixed scenarios with different operating systems has to do with the WSUS API version. To support local publishing activities (anything that involves adding a third-party update to the WSUS database), the same version of WSUS must be installed on both the BeyondInsight server and the WSUS server. Otherwise, the third-party patch service returns the error *Failed to publish <package>. Publishing operation failed because the console and remote server versions do not match*, and no third-party updates will be available.

Currently, two supported production versions of WSUS can contribute to this situation:

- WSUS v6.2: runs on Windows Server 2012
- WSUS v6.3: runs on Windows Server 2012 R2

To avoid this error, make sure all WSUS servers and BeyondInsight servers have the same WSUS patches installed.

For information on how Windows Server 2012 and WSUS work together, please see:

- Windows Server Update Services Overview at https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh852345(v=ws.11)
- Deploy Windows Server Update Services in Your Organization at https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh852340(v=ws.11)

Install the WSUS Administration Console Using PowerShell

Open a Windows PowerShell console as an administrator, and execute the following command:

```
Install-WindowsFeature -Name UpdateServices-UI
```

Note: *This command only installs the console and does not run a post-install task.*

Resolve Internal HTTP Error 500.19

If you have installed Windows Server 2012, IIS, WSUS, and BeyondInsight on the same server, you may see **HTTP Error 500.19** when you try to log into BeyondInsight.

The cause starts with the fact that Windows Server 2012 is exclusively a 64-bit operating system. When WSUS is installed, **suscomp.dll** is defined globally and loaded in every application pool as a 64-bit file. However, the BeyondInsight application pool is 32-bit. Thus, when the 64-bit **suscomp.dll** attempts to load, an error occurs.

There are two options to resolve this issue:

Option 1:

1. Back up IIS.
2. Open **IIS Manager**.
3. Click the server module node in the tree and select **Modules**.
4. Right-click **DynamicCompressionModule** and select **Unlock**.
5. Right-click **StaticCompressionModule** and select **Unlock**.
6. Open the default web site, then open **Modules**.
7. Right-click **DynamicCompressionModule** and select **Remove**.
8. Right-click **StaticCompressionModule** and select **Remove**.
9. Perform **IISRESET** from an elevated command prompt.

Option 2:

Install BeyondInsight and WSUS on separate Windows Server 2012 servers.

Configure Privilege Management for Unix & Linux

You can use BeyondInsight to manage Privilege Management for Unix & Linux event logs. Configure BeyondInsight and Privilege Management for Unix & Linux to work together to send event logs to the BeyondInsight management console.

> ***Note:*** *Privilege Management for Unix & Linux was formerly known as PowerBroker for Unix and Linux.*

Requirements

- BeyondInsight 4.5 or later
- Privilege Management for Unix & Linux 7.5 or later

Generate a Certificate

1. Open the BeyondInsight Configuration Tool and select **Certificate Management**.
2. Select **Export certificate**.
3. Select **Client certificate**.
4. Enter a password for the export file and provide the destination in the **Path** field.
5. Click **OK** to export the certificate as a PKCS#12 file (with a .pfx extension).
6. Using **BeyondTrust FIPS Object Module for OpenSSL**, convert the certificate from PKCS#12 (*.pfx) to PEM (*.pem):

```
openssl pkcs12 -clcerts -in <full path of pfx> -out <full path of target pem> -nodes
```

7. Securely copy the certificate to the Privilege Management for Unix & Linux master and log server hosts.
8. In the settings file, assign the path and file name of this certificate to the keyword **sslrcscertfile**.

Export the BeyondInsight Server SSL Certificate

1. Open the **Windows Certificate Manager** (**certmgr.msc**) and expand the **Trusted Root Certification Authorities** folder.
2. In the details pane, select the BeyondInsight server SSL certificate from the **Issued To** field.
3. The certificate name contains the hostname of the BeyondInsight server and the text **eEye EMS CA**.

   Example:

   - RCS hostname: **LA-HOST-01**
   - Certificate name: **LA-HOST-01 eEye EMS CA**
4. From the **Action** menu, select **All Tasks > Export**.
5. In the **Certificate Export Wizard**:
   a. Select **No** when asked to export the private key, then click **Next**.
   b. Select the **DER-encoded binary X.509 (*.CER)** format, then click **Next**.
   c. Provide the target destination of the certificate, then click **Next**.
   d. Confirm the settings, then click **Finish** to export the certificate.

6. Using **BeyondTrust FIPS Object Module for OpenSSL**, convert the certificate from DER (*.der) to PEM (*.pem):

```
openssl x509 -inform der -in <full path of der> -out <full path of target pem>
```

7. Securely copy the certificate to the Privilege Management for Unix & Linux master and log server hosts.
8. In the settings file, assign the path and file name of this certificate to the keyword **sslrcscafile**.

> For more information about importing certificates, please see the *Privilege Management for Unix & Linux Install Guide* at beyondtrust.com/docs/privilege-management/documents/unix-linux/10-2/pmul-install-10-2.pdf.

Configure Keywords

If you have not already done so during installation of Privilege Management for Unix & Linux, set the following keywords in **pb.settings** on the master and log server hosts:

- rcshost
- rcswebsvcport
- sslrcscertfile
- sslrcscafile
- rcseventstorefile

> For a complete list of the keywords that must be configured, please see the *Privilege Management for Unix & Linux documentation* at beyondtrust.com/docs/privilege-management/unix-linux.htm.

Configure Endpoint Privilege Management

You can configure Privilege Management for Desktops to forward events to BeyondInsight. Before proceeding, make sure you have the appropriate license key for BeyondInsight and that you have installed all components for Privilege Management for Desktops and for BeyondInsight.

Generate a Certficate

Generate a client certificate using the BeyondInsight Configuration Tool. A certificate must be deployed to any asset where you capture events with Privilege Management for Desktops.

After you have generated a certificate, you can create an MSI. You can then set up a group policy with the MSI and deploy the certificate to your Privilege Management for Desktops assets.

> ***Note:*** *Do not generate a client certificate if one has already been created for BeyondTrust Network Security Scanner. You can use the existing client certificate for your Privilege Management for Desktops assets.*

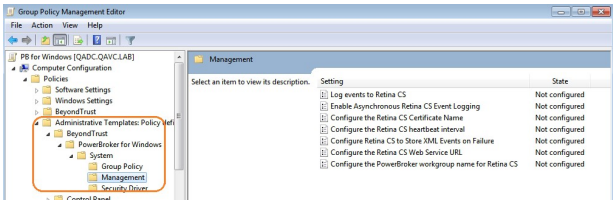
1. Open the BeyondInsight Configuration Tool and select **Certificate Management**.
2. Select **Generate Certificate**.
3. Select **Client Certificate**.
4. Enter a password.
5. Click **OK**.

Create an MSI File

1. Run the BeyondInsight Configuration Tool.
2. Click **Generate Certificate MSI**.
3. The **certinstaller.msi** is created in **C:\Program Files (x86)\eEye Digital Security\Retina CS\Utilities\msi**.

Configure Privilege Management for Desktops

1. Install the Privilege Management for Desktops components.
2. Run the **Group Policy Management Editor**.
3. Go to the **Management** folder in the **Administrative Templates** section.
4. Set the following options.



Setting	Description
Log events to BeyondInsight	Activates event forwarding to BeyondInsight
Enable Asynchronous BeyondInsight Event Logging	Sends event logs to the System event log when BeyondInsight cannot process the events.
Configure the BeyondInsight Certificate Name	Sets the BeyondInsight certificate name, eEyeEmsClient.

Setting	Description
Configure the BeyondInsight heartbeat interval	Configure a regular interval to send heartbeat events to verify the connection between Privilege Management and BeyondInsight (event ID 28701). The default interval is 360 minutes (6 hours).
Configure BeyondInsight to Store XML Events on Failure	Create a path where the event data XML file will be stored when the file cannot be sent to BeyondInsight.
Configure the BeyondInsight Web Service URL	Enter the URL for the BeyondInsight web service in the format of **https://example/EventService/Service.svc**.
Configure the Privilege Management Workgroup Name for BeyondInsight	Enter a workgroup name, needed for asset matching in BeyondInsight.
Enable BeyondInsight Trace Logging	Enable to create a trace log if events are not flowing correctly into BeyondInsight.

Configure AD Bridge

You can configure Privilege Management Identity Services to forward events to BeyondInsight. Before proceeding, make sure you have the appropriate license key for BeyondInsight and that you have installed all components for Privilege Management Identity Services and BeyondInsight.

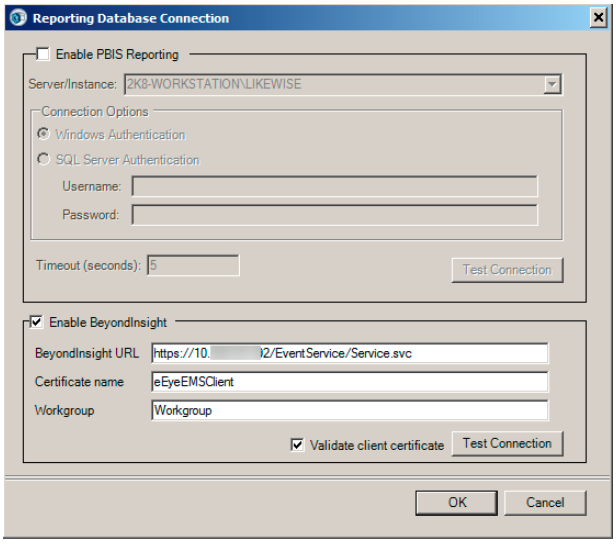
> ***Note:*** *AD Bridge was formerly known as PowerBroker Identity Services.*

Generate a Certificate

1. Open the BeyondInsight Configuration Tool and select **Certificate Management**.
2. Select **Generate Certificate**.
3. Select **Client Certificate**.
4. Enter a password.
5. Click **OK**.

Configure AD Bridge

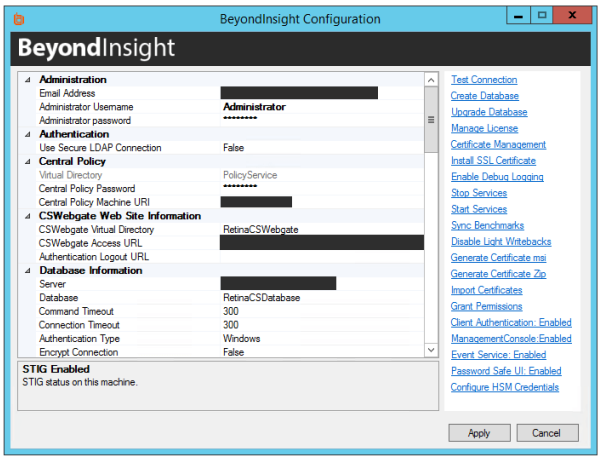
1. On the AD Bridge server, run the **DBUtilities** tool.
2. Select the **Enable BeyondInsight** check box.
3. Enter the URL to the BeyondInsight server.
4. Enter the name of the client certificate generated earlier.
5. Optionally, create a workgroup name. A workgroup name can be used as a unique identifier.
6. Select the **Validate client certificate** check box.
7. Click **Test Connection** to ensure the connection between the servers works properly.



Use the BeyondInsight Configuration Tool

After your initial configuration of BeyondInsight, you can modify settings and configure additional settings using the BeyondInsight Configuration Tool.

> For more information on the settings defined during installation, please see "Run the Configuration Wizard" on page 14.



Setting	Description
Test Connection	Click to test the connection to the SQL Server database.
Create Database	Click to create a new database.
Upgrade Database	Click to upgrade your database.
Manage License	Use the License Manager to update your license or to transfer the license, removing it from the installation computer and moving it to another computer.
Certificate Management	Generate a certificate and export it to a preferred location. Certificates are used by the Events Client to ensure secure data transmission. The certificate password must be the same as the Central Policy password.
Install SSL Certificate	Create an SSL certificate to establish a secure connection to IIS. ***Note:*** *A certificate generated here is not certified by a trusted certificate authority. If you use this certificate, an invalid certificate message will be displayed to browsers connected to IIS.* You can use SSL when creating Active Directory queries or creating Active Directory user groups in the console. For more information, please see the *BeyondInsight User Guide*.
Enable Debug Logging	Use this feature when troubleshooting with the BeyondTrust Support team.
Stop and Start Services	Click to start and stop the BeyondInsight services.
Sync Benchmarks	Synchronize the benchmark templates that reside in the database with the templates that reside on the server.
Disable Light Writebacks	Light writeback is used by the Patch Management module to make sure that patches are deployed and items are no longer vulnerable. If you are not using the Patch Management module, you can turn off light writebacks.

Setting	Description
Generate Certificate msi	Create an MSI file that contains a client certificate. You can then set up a group policy with the MSI and deploy the certificate to your assets.
Generate Certificate Zip	Used with Privilege Management for Unix & Linux.
Import Certificates	Used with Privilege Management for Unix & Linux.
Grant Permissions	Grants permission to all stored procedures in the schema so that services and web services can run those procedures.
Client Authentication	Click to enable or disable authentication. When disabled, SSL client certificates are ignored. When enabled, client certificates are required, rather than simply accepted. To confirm settings, go to the SSL Settings in IIS for the BeyondInsight server.
Management Console	For environments with multiple console installations, you can disable services to save resources. For example, if you are running Password Safe and would like to deploy more than one console, you would not need services running on the secondary consoles. ***Note:*** *This setting applies to software installations, not hardware appliance installations.*

Change the Access URL

The default URL to access the BeyondInsight web site is **https://<server name>/WebConsole**. To change the default URL:

1. On the BeyondInsight server, select **Start > All Programs > BeyondTrust > BeyondInsight > BeyondInsight Configuration**.
2. Scroll to **Web Site Information**.
3. Change the URL, making sure the address starts with **https://**.
4. Click **Apply**.

Configure Session Timeout

A user can remain logged into the console while inactive for a maximum of twenty minutes. To change this timeout:

1. On the BeyondInsight server, select **Start > All Programs > BeyondTrust > BeyondInsight > BeyondInsight Configuration**.
2. Scroll to **Web Site Information**.
3. Change the session timeout value.
4. Click **Apply**.

Manage Your BeyondInsight License

Use the BeyondInsight Configuration Tool to update your license. You must upgrade your license to extend your maintenance or to apply a purchased asset count (for example, 500 assets to 1,000 assets).

1. On the server hosting BeyondInsight, select **Start > All Programs > BeyondTrust > BeyondInsight > BeyondInsight Configuration**.
2. Click **Manage License**.
3. On the **License Management** page, select **Update License**.
4. Click **Next**.
5. Click **Finish**.
6. Click **Apply** to close the BeyondInsight Configuration Tool.

Note: *After your license key expires, you can continue to log into the console. However, product updates are no longer provided.*

Configure Windows Authentication to the Database

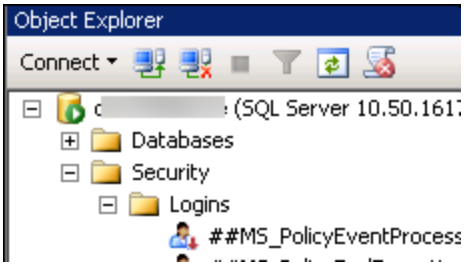
As a security best practice for PCI DSS compliance, use Windows authentication for database access.

> For more information, please see "Database Permissions Matrix" on page 10.

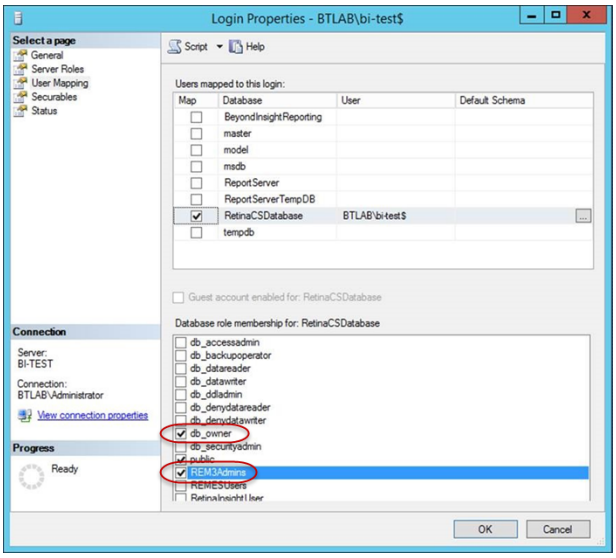
Change Database Authentication

You can set up Windows authentication on your SQL Server database.

1. Log into SQL Server.
2. Create a SQL Server login, such as **Domain\RemoteServerName$**.



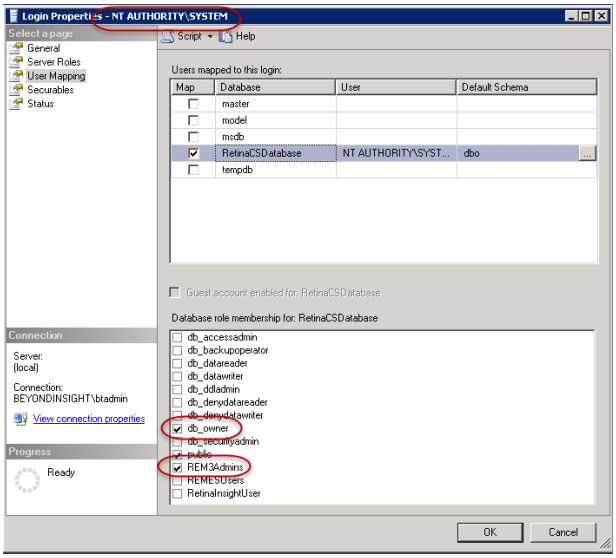
3. Go to the properties for the new login, and create a user mapping to the BeyondInsight database and the **REM3Admins** role.



SQL Server 2012

In an environment where SQL Server 2012 and BeyondInsight are installed on different servers, SQL Server uses **Domain\MachineName$** for Windows authentication.

However, when SQL Server 2012 and BeyondInsight are on the same server, SQL Server must use **NT AUTHORITY\NETWORK SERVICE** for Windows authentication. This account is not created by default on SQL Server 2012. You must therefore create the **NT AUTHORITY\NETWORK SERVICE** account in SQL Server before changing the authentication mode. Permissions assigned on the BeyondInsight database must include **db_owner** and **REM3Admins**, a custom role created by the installer.



Upgrade BeyondInsight

Please visit the Product Change Log to get the details of each release of BeyondTrust BeyondInsight software.

Download the Installation Package

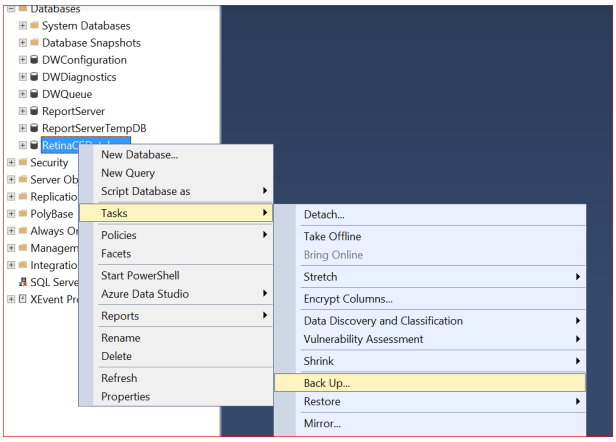
Download the appropriate installer by logging into the BeyondTrust Support Portal at beyondtrust.com/myportal/downloads.

> ***Note:*** *You must have a BeyondTrust Support account to log into the Support Portal.*

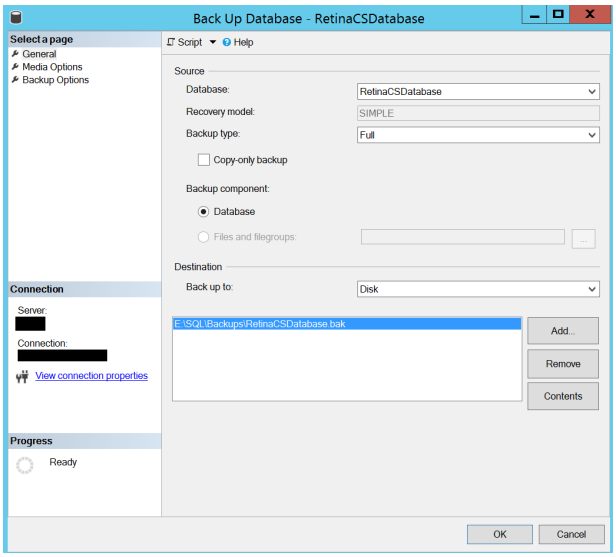
Backup the BeyondInsight Database

> ***Note:*** *Prior to upgrading, BeyondTrust strongly recommends that you create a backup of your BeyondInsight database in SQL Management Studio.*

1. Open SQL Management Studio
2. In Object Explorer, navigate to your BeyondInsight database.
3. Right-click on the database name, and then select **Tasks > Back Up ...**

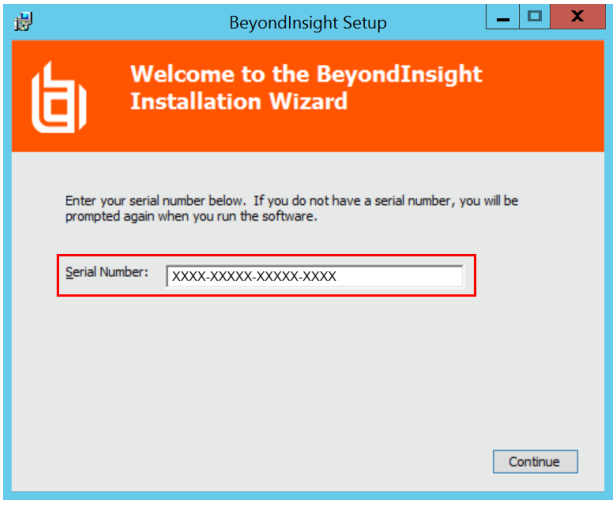


4. Choose a location to store the backup of your database.

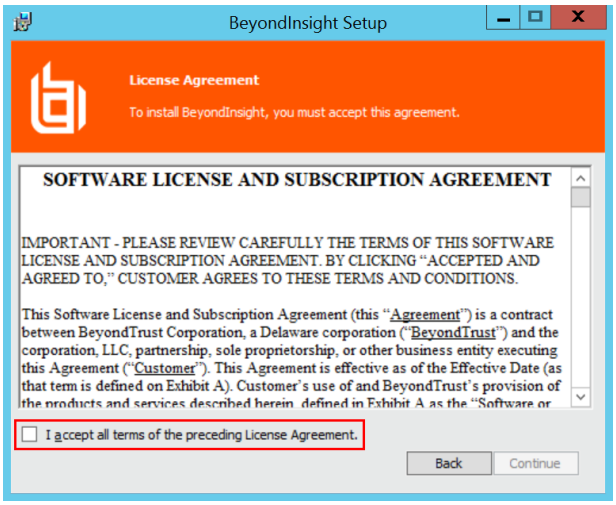


Run the Installer

1. Double-click the installer .exe or .msi file. In upgrade scenarios, the **Serial Number** field auto-populates with your BeyondInsight serial number.
2. Click **Continue**.

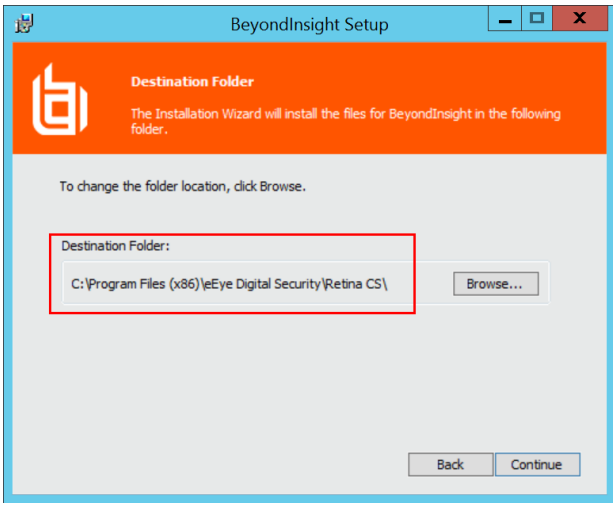


3. Check the box to accept the License Agreement, and then click **Continue**.

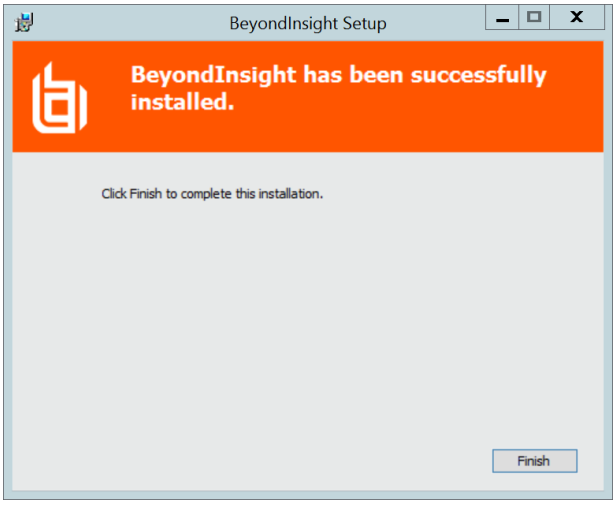


4. Verify the **Destination Folder** where BeyondInsight is installed, and then click **Continue** to begin the upgrade installation.

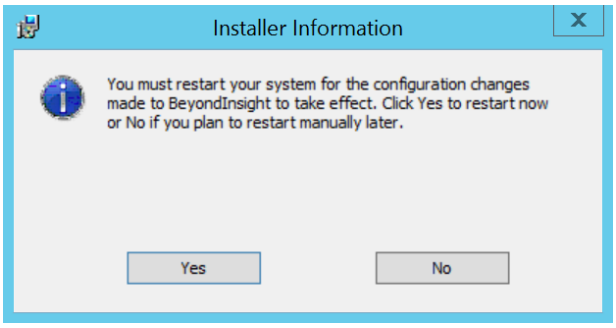
> ***Note:*** *Selecting a Destination Folder other than the folder where BeyondInsight is installed will cause the upgrade to fail.*



5. When the upgrade installation is complete, click **Finish**.



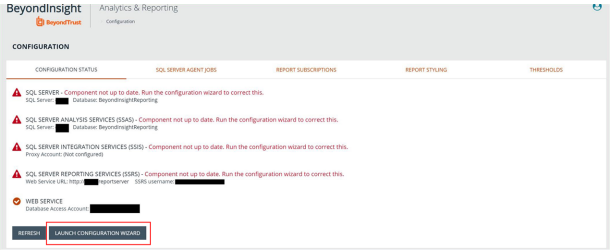
6. Your system must be restarted for the upgrade to take effect. Click **Yes** to restart immediately, or **No** to manually restart later.



Run the Analytics & Reporting Configuration Wizard

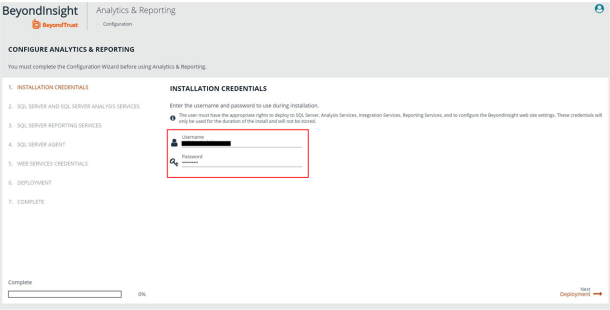
After the system reboots, the Reporting Services components must be updated.

1. Open BeyondInsight and navigate to **Configuration > Analytics & Reporting**.
2. Click the **Launch Configuration Wizard** button.

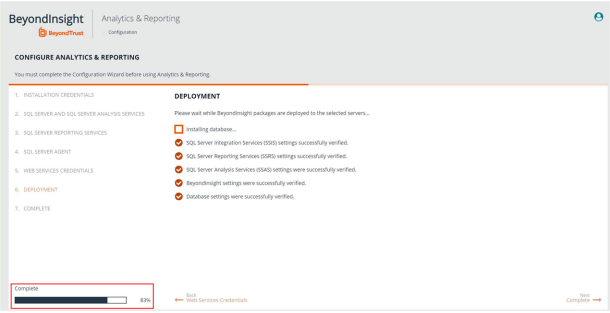


3. In upgrade scenarios, the **Username** and **Password** fields are auto-populated.

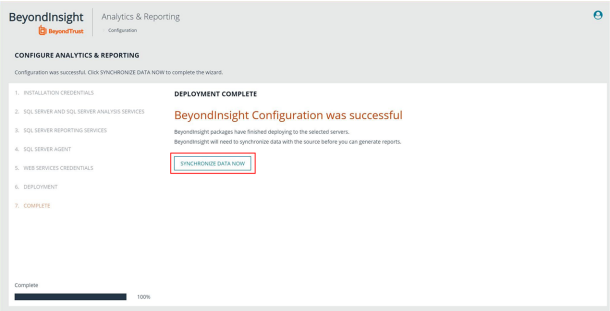
> ***Note:*** *The user credentials must have the appropriate rights to deploy to SQL Server, Analysis Services, Integration Services, and to configure the BeyondInsight web site settings.*



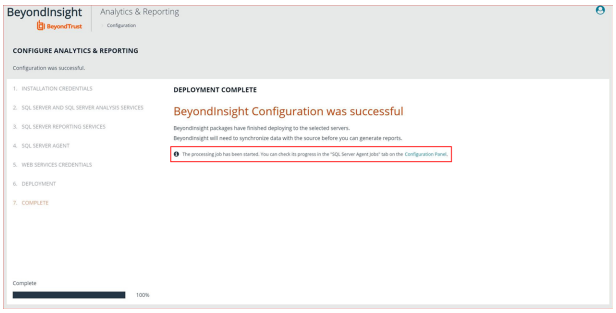
4. Click **Deployment**. Upgrades to the Reporting Services components are upgraded automatically. A status bar at the bottom left shows the progress.



5. When the installation completes, click the **Synchronize Data Now** button to start the data sync, or you can wait for the synchronization to occur as scheduled.



6. When the synchronization has started, BeyondInsight displays a link to the **Configuration Panel**.



7. Click the **Configuration Panel** link to view the **SQL Server Agent Jobs** tab, with the synchronization job status listed.