



BeyondTrust

BeyondInsight 22.3 Installation Guide

Table of Contents

BeyondInsight Installation Guide	3
BeyondInsight Software and Hardware Requirements	4
Set Up BeyondInsight Certificates	16
Configure BeyondTrust Discovery Scanner Connections to BeyondInsight	22
Configure BeyondInsight Analytics & Reporting	24
Configure Privilege Management for Unix & Linux	29
Configure Endpoint Privilege Management	31
Configure AD Bridge	33
Use the BeyondInsight Configuration Tool	34
Manage Your BeyondInsight License	36
Configure Windows Authentication to the Database	39
Upgrade BeyondInsight	41

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 Discovery 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 sends scan requests to the Discovery Scanner, which is the engine that performs all discovery scans on your network. 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.





Note: The Web Policy Editor (WPE) is not installed out of the box with BeyondInsight. Please contact your BeyondTrust representative for assistance with installing the WPE and its associated WPE service in your BeyondInsight environment.

BeyondInsight Software and Hardware Requirements

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

Operating System	Windows Server 2012, 2012 R2, 2016 (64-bit), 2019 (64-bit), and 2022 (64-bit)  Note: Integration with Windows Server Update Services on Windows Server 2016+ is not supported.
Database	Microsoft SQL Server 2012-2022 Microsoft SQL Standard or Enterprise Editions Microsoft SQL Server Reporting Services Microsoft SQL Server Analysis Services Microsoft SQL Server Integration Services Microsoft Azure SQL  Note: SQL Server collation must be set to SQL_Latin1_General_CP1_CI_AS .
Database Services	Microsoft SQL Server Reporting Services Microsoft SQL Server Analysis Services Microsoft SQL Server Integration Services  Note: All three services are required to support BeyondTrust Analytics & Reporting.
Processor	Intel Dual Core 2.0GHz (or compatible)  Tip: Assign two processors when installing BeyondTrust Discovery Scanner and the management console on a single virtual machine. This greatly improves performance.
Memory	16GB (requires x64 OS)
Hard Drive	500MB (software install) 40GB (database minimum)

Network	Network Interface Card (NIC) with TCP/IP enabled
Server Requirements	<p>Microsoft .NET Framework version 4.7.2 with Application Server Role, Windows Process Activation Service Support, HTTP Activation</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;">  Note: <i>The BeyondInsight installation includes .NET Framework 4.7.2; .NET does not need to be preinstalled.</i> </div> <p>Microsoft Internet Information Server (IIS) 7.0 or later with ASP.NET support and Web Server (IIS) Role</p>

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

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.

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
- Management Tools

Features

- .NET Framework 3.5 Features
 - .NET Framework 3.5 (includes .NET 2.0 and 3.0)
 - Windows Process Activation Service Support
- Windows Process Activation Service
 - Process Model
 - .NET Environment 3.5
 - Configuration APIs

Windows Server 2016

- Web Server (IIS)
 - Common HTTP Features
 - Default Document
 - Directory Browsing
 - HTTP Errors
 - Static Content
 - HTTP Redirection
 - Health and Diagnostics
 - HTTP Logging
 - Performance
 - Static Content Compression

- 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 4.6
 - ASP.NET 3.5
 - ASP.NET 4.6
 - ISAPI Extensions
 - ISAPI Filters
- Management Tools
 - IIS Management Console
 - IIS 6 Management Compatibility
 - IIS 6 Metabase Compatibility
 - IIS Management Scripts and Tools
 - Management Service

Features

- .NET Framework 3.5 Features
 - .NET Framework 3.5 (includes .NET 2.0 and 3.0)
 - HTTP Activation
- .NET Framework 4.6 Features
 - .NET Framework 4.6
 - ASP.NET 4.6
 - WCF Services
 - HTTP Activation
 - TCP Port Sharing
- Windows Process Activation Service
 - Process Model
 - .NET Environment 3.5
 - Configuration APIs

Windows Server 2019

- Web Server (IIS)
 - Common HTTP Features
 - Default Document
 - Directory Browsing
 - HTTP Errors
 - Static Content
 - HTTP Redirection
 - Health and Diagnostics
 - HTTP Logging
 - Performance
 - Static Content Compression
 - 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 4.7
 - ASP.NET 3.5
 - ASP.NET 4.7
 - ISAPI Extensions
 - ISAPI Filters
 - Management Tools
 - IIS Management Console
 - IIS Management Scripts and Tools
 - Management Service

Features

- .NET Framework 3.5 Features
 - .NET Framework 3.5 (includes .NET 2.0 and 3.0)
 - HTTP Activation
- .NET Framework 4.7 Features
 - .NET Framework 4.7
 - ASP.NET 4.7
 - WCF Services
 - HTTP Activation
 - TCP Port Sharing
- Windows Process Activation Service
 - Process Model
 - .NET Environment 3.5
 - Configuration APIs

Windows Server 2022

- Web Server (IIS)
 - Common HTTP Features
 - Default Document
 - Directory Browsing
 - HTTP Errors
 - Static Content
 - HTTP Redirection
 - Health and Diagnostics
 - HTTP Logging
 - Performance
 - Static Content Compression
 - 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 4.7
 - ASP.NET 3.5
 - ASP.NET 4.7
 - ISAPI Extensions
 - ISAPI Filters
- Management Tools
 - IIS Management Console
 - IIS Management Scripts and Tools
 - Management Service

Features

- .NET Framework 3.5 Features
 - .NET Framework 3.5 (includes .NET 2.0 and 3.0)
 - HTTP Activation
- .NET Framework 4.7 Features
 - .NET Framework 4.7
 - ASP.NET 4.7
 - WCF Services
 - HTTP Activation
 - TCP Port Sharing
- Windows Process Activation Service
 - Process Model
 - .NET Environment 3.5
 - Configuration APIs

Database Requirements

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

Supported Versions

- **On Premises**
 - SQL Server 2012 and 2012 R2
 - SQL Server 2014
 - SQL Server 2016

- SQL Server 2017
- SQL Server 2019
- SQL Server 2022



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

- **Cloud**
 - Azure SQL (a minimum of 200 DTUs is recommended.)



Note: Increases in size of Azure SQL database might be required in the future as usage grows.



Note: While Azure SQL database can be used for the console SQL Server Database, if the Analytics and Reporting features of the product are desired, those still need to be hosted on premises.

Components to Install

- Database Engine Services



Note: While **Full Text Search** is enabled by default, additional steps are required to create a full-text index and catalog in order to run a keyword search for Password Safe Session Recordings. For more information, please see [Get Started with Full-Text Search](https://docs.microsoft.com/en-us/sql/relational-databases/search/get-started-with-full-text-search?view=sql-server-ver15) at <https://docs.microsoft.com/en-us/sql/relational-databases/search/get-started-with-full-text-search?view=sql-server-ver15>.

- 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

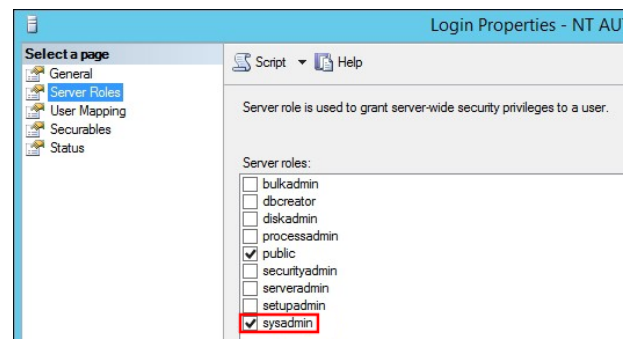
Permission	SQL Server
SQL Authentication (SQL Local or SQL Remote)	Assign the SQL Server account the role of sysadmin .
Windows Authentication (SQL Local)	<p>Assign NT AUTHORITY\SYSTEM the role of sysadmin, if not previously assigned.</p> <p>Add NT AUTHORITY\NETWORK SERVICE as a Login account in SQL Server, if not previously added.</p> <p>On the BeyondInsight database, assign NT AUTHORITY\NETWORK SERVICE the roles of db_owner and REM3Admins.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Note: <i>REM3Admins is a custom role created by the installer.</i> </div>
Windows Authentication (SQL Remote, where SQL Server and BeyondInsight are on the same domain or in trusted domains of a forest)	<p>In SQL Server, create a local Windows group and add the group to the SQL Server instance.</p> <p>On the BeyondInsight database, assign the account the roles of db_owner and REM3Admins.</p> <p>Add each BeyondInsight machine to this local group, including any Event Collector machines or Password Safe worker node machines, in the format:</p> <p>'Domain\MachineName1\$',</p> <p>'Domain\MachineName2\$'</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Note: <i>Windows Authentication is not supported on remote standalone systems. U-Series Appliances and software must be on the domain or a trusted domain in a forest.</i> </div>

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**, and 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 might need to restart IIS.

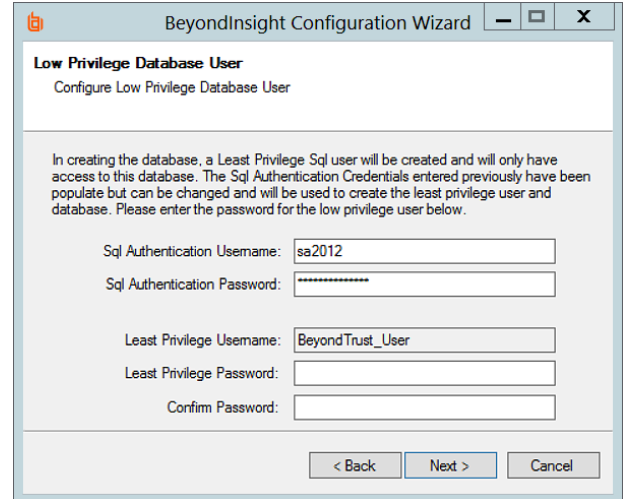


Least Privilege Database User Account Setup

The installation of BeyondInsight requires the creation of a Least Privilege Database User account within the Configuration Wizard. The SQL Authentication Credentials entered previously in the Configuration Wizard are populated by default, but can be changed and are used to create the least privilege user account and database.

The Least Privilege Database User Account is granted the following permissions by default:

- **General**
 - Enforce password policy
 - Enforce password expiration
- **Server Roles**
 - Public
- **User Mapping**
 - Mapped to the RetinaCSDatabase created in previous screens
- **Securables**
 - Connect SQL: Grant
 - View any database: Deny
- **Status**
 - Settings
 - Permissions to connect to database engine: Grant
 - Login: Enabled



Port Requirements

BeyondInsight

Function	Traffic	Port
Database Connectivity	Management console to SQL Server, Analytics & Reporting to SQL Server	1433
Event Collector	BeyondTrust Discovery Scanner to BeyondInsight	21690
Discovery Scanner Central Policy	BeyondTrust Discovery Scanner to the console	443
BeyondTrust Updater Enterprise		443
Client Browser	User to BeyondInsight or Analytics & Reporting	443 or 80
Privilege Management for Desktops	Connector to web services	443

U-Series Appliance

Function	Traffic	Port
Database Connectivity	BeyondInsight to SQL Server, Analytics & Reporting to SQL Server	1433
Event Collector	Discovery Scanner or Privilege Management to BeyondInsight	21690
Privilege Management for Desktops	Connector to web services	443
Discovery ScannerCentral Policy	BeyondTrustDiscovery Scanner to the console	443
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

Password Safe

Function	Service	Port
System Discovery		
User enumeration	nb-ssn, ms-ds	TCP 139, 445
Hardware enumeration	nb-ssn, ms-ds	TCP 139, 445
WMI service running on target		
Software enumeration	nb-ssn, ms-ds	TCP 139, 445
Remote registry service running on target		
Local scan service	ms-ds	TCP 445
Password Change		
Windows password change	adsi-ldap adsi-ldaps	TCP / UDP 389 TCP 636 / UDP 389
As a fallback, uses ms-ds, 445, TCP		
Windows update and restart services	wmi	TCP 135
WMI service running on target		
Active Directory password change	adsi-ldap adsi-ldaps	TCP 135 TCP 636 / UDP 389
As a fallback, uses ms-ds, 445, TCP		
User and computer authentication, forest-level trusts	kerberos	TCP / UDP 88
UNIX, Linux, macOS	ssh	TCP 22
Oracle	oracle-listener	TCP 1521

Function	Service	Port
Microsoft SQL Server	netlib	TCP 1433
HP ILO	ssh	TCP 22
Dell DRAC	ssh	TCP 22
<i>Session Management</i>		
Remote Desktop	rdp	TCP 3389
SSH	ssh	TCP 22
<i>U-Series Appliance</i>		
Mail server integration	smtp	TCP 25
Active Directory integration	ldap ldaps	TCP / UDP 389 TCP 636 / UDP 389
Backup	smb	TCP 445
Time Protocol	ntp	UDP 123
High-availability replication (pair)	sql-mirroring, https	TCP 5022, 443

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 certificate 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.



Note: Only the "Generate Certificate MSI" option should be used for the endpoint clients. These endpoint clients must have the .NET Framework 4.7.2 installed as a prerequisite to running the MSI.



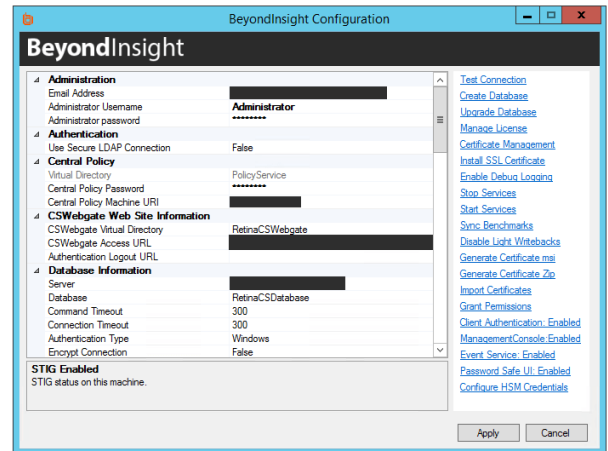
Note: The "Generate Certificate Zip" option should only be used to transfer certificates between BeyondInsight servers.

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.

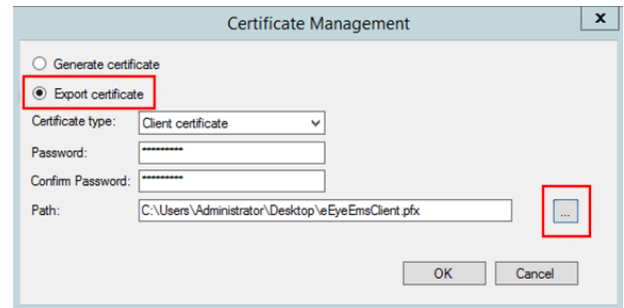


The EmsClientCert certificate is used for communication between the agent and server when sending and receiving events. The certificate must be exported from the server and then imported on the agent.

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



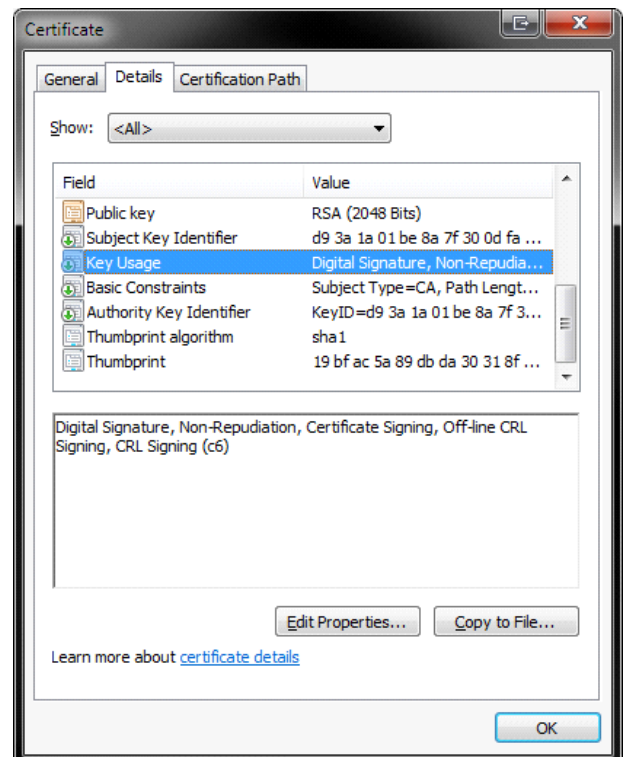
3. Select **Export certificate**.
4. Select **Client Certificate** as the **Certificate type**.
5. Enter a chosen **Password**. We recommend that you use the existing BeyondInsight Central Policy password.
6. Click the ellipses (...) to browse to your desired location.
 - Enter a **File name** and select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



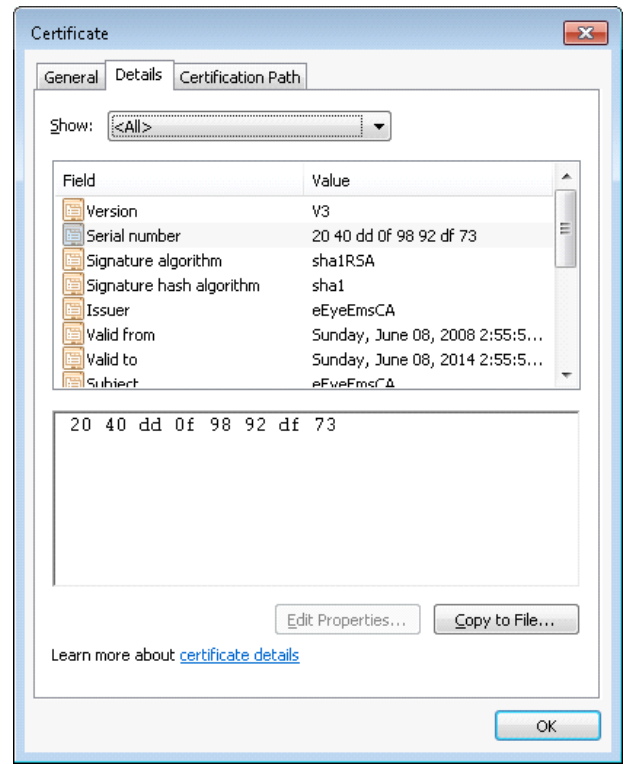
Troubleshoot BeyondInsight Certificates

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.



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.



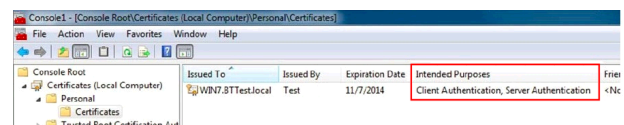
For detailed procedures on creating a custom domain certificate, please see Microsoft's documentation.

Prerequisites

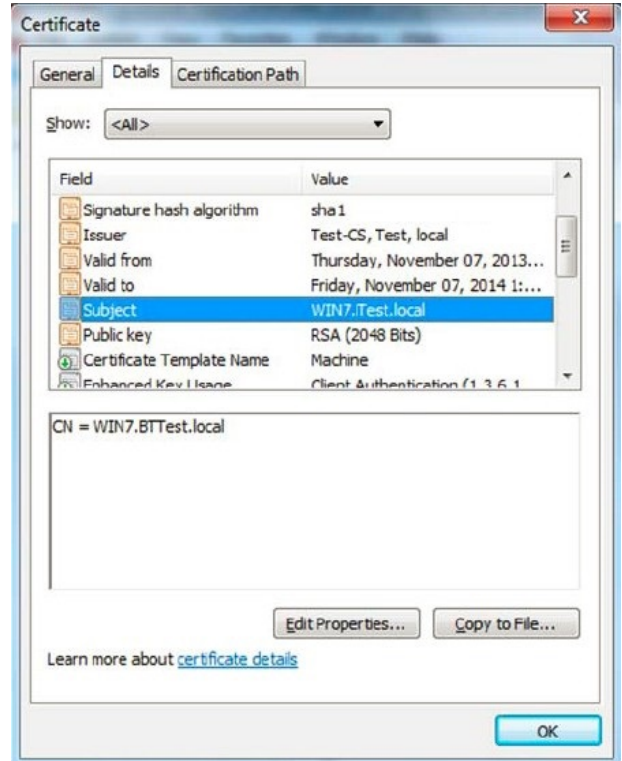
- Domain member server with Active Directory Certificate Services installed and configured.
- Certificate Authority Web Enrollment role installed

Requirements

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

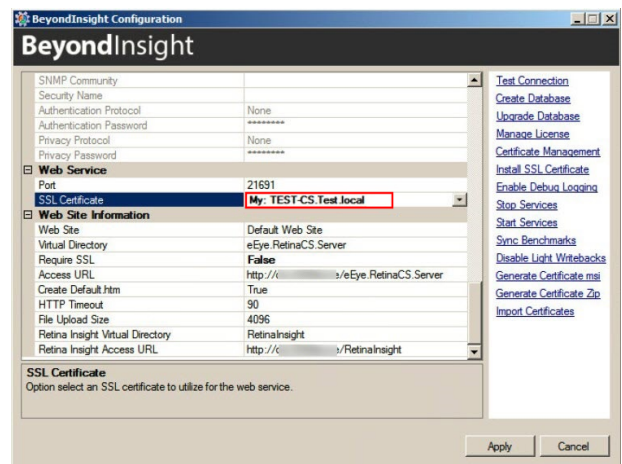


- The **Subject** key must contain common text for all client certificates.



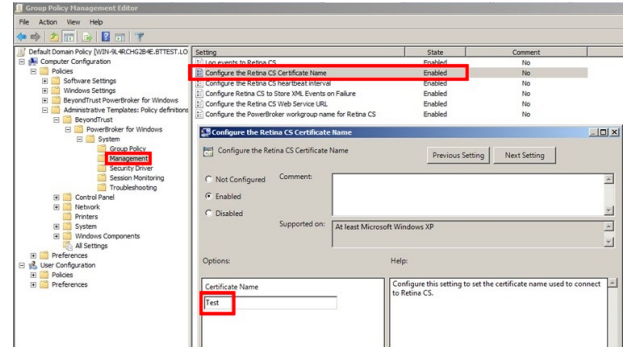
Assign the SSL Web Service Certificate in BeyondInsight

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 within 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 Discovery Scanner Connections to BeyondInsight

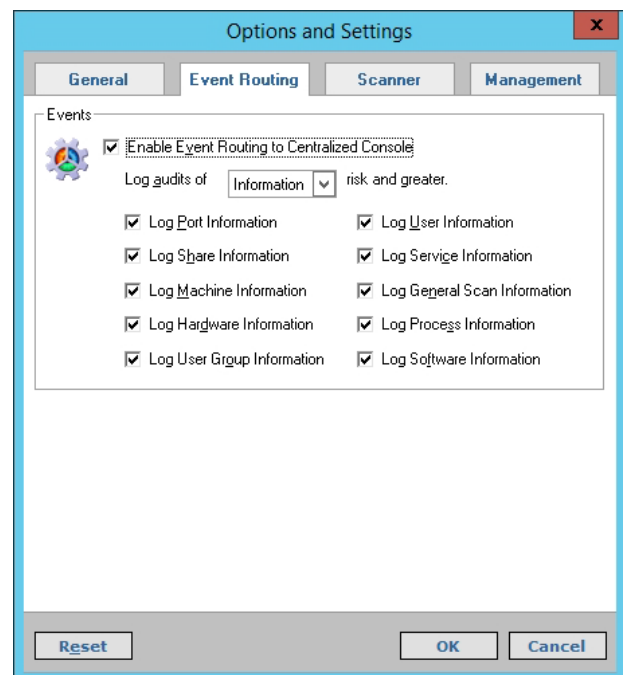
Once the BeyondTrust Discovery Scanner and the console are installed, they must be configured to work together by configuring both Central Policy and Events Client.

Configure Central Policy

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

- To configure Central Policy, run the Discovery Scanner.
- Select **Tools > Options**.
- Select the **Event Routing** tab, and then select **Enable Event Routing to Centralized Console**.
- Select the **Management** tab, and then select **Enable Central Policy**.
- 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 defined during BeyondInsight configuration.
 - Agent Name:** Enter a name that identifies the scanner in the console.
- Click the **Test** button.
- After a few seconds, you 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 the following: "[Database Permissions Matrix](#)" on page 12

Configure Events Client

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

- To configure the Events Client:
 - In Windows 2012 or above, click **Start > Apps > BeyondTrust > Events Client Configuration**.
- Go through the Events Client Installation Wizard.
 - On the **Select a Client Certificate** page, choose a certificate to use.
 - When prompted for a password, enter the agent password created during BeyondInsight configuration.

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



For more information, please see the following: "[Set Up BeyondInsight Certificates](#)" on page 16

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.



IMPORTANT!

Analytics & Reporting is not supported on an external SQL Server, because the replication of the credentials of the BeyondTrust Admin account presents a security threat to the host. Analytics & Reporting is supported only on the main console node.

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: <ul style="list-style-type: none"> • 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 website and is required to read information from SSRS.
Browser	This role is on the root folder settings for the SQL Report Services management website 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 website 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 website and is required to read information from SSRS.
Browser	This role is on the root folder settings for the SQL Report Services management website 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

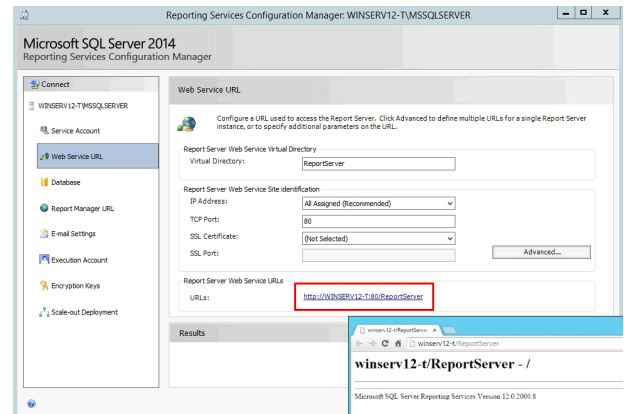
SQL Agent Service Permissions

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

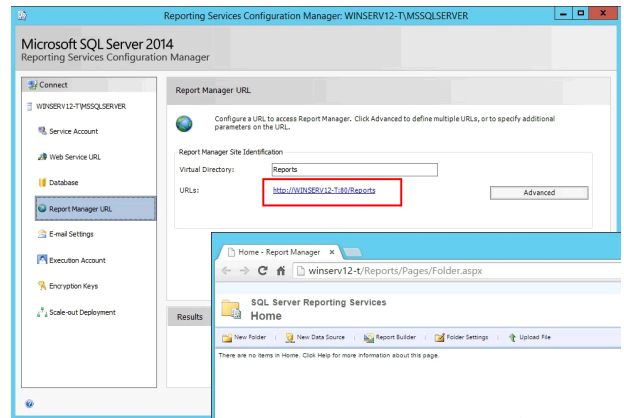
SSAS Proxy User Roles	
Member in Role	Database
BeyondInsightSSIS	BeyondInsight
BeyondInsightUser	BeyondInsight management console

Verify SQL Report Server Functionality

- To verify that SQL Report Server works properly:
 - In Windows 2012 or later, click **Start > Apps > Microsoft SQL Server 20xx > SQL Server 20xx Reporting Services Configuration Manager**.
- After connecting, select **Web Service URL**.
- 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



Note: Be careful not to refresh the browser during this process, because doing so reloads the page, requiring you to log in again.

1. Log in to 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 in to the console.
4. Click **Configure Now**.
5. On the **Installation Credentials** page, enter the local or domain administrator credentials.

INSTALLATION CREDENTIALS

Enter the username and password to use during installation.

The user must have the appropriate rights to deploy to SQL Server, Analysis Services, Integration Services, Reporting Services, and to configure the BeyondInsight web site settings. These credentials will only be used for the duration of the install and will not be stored.

Username
administrator

Password

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

SQL SERVER AND SQL SERVER ANALYSIS SERVICES

Select a SQL Server and SQL Server Analysis Services Server to deploy the BeyondInsight database, analysis cube, and packages.

SQL Server and Integration Services (SSIS) are required on this server.

SQL Server (required)

Database
BeyondInsightReporting

You can optionally specify a separate server for SQL Service Analysis Services (SSAS) to improve performance.

SSAS Server

- On the **SQL Server Reporting Services** page, enter the web service URL in the format:

http://<machine name>:80/ReportServer.

- On the **SQL Server Agent** page, set a job run time, and 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.

- On the **Web Services Credentials** page, the username and password automatically populate. Click **Deploy**.
- Deployment progress is shown while the BeyondInsight Reporting database is created. When database creation is complete, click **Finish**.
- Once the deployment completes, select the option to synchronize data. 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.

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

SQL SERVER REPORTING SERVICES

Enter the URL to access the SQL Server Reporting Services (SSRS) Web Service for deploying BeyondInsight reports.

 *Web Service URL (required)* _____


Enter credentials for a user with access to SQL Server and SQL Server Analysis Services (SSAS).

 *SSRS Username*
administrator _____

 *SSRS Password*
..... _____

SQL SERVER AGENT

Configure the time of day that the agent job runs to synchronize and process new data into BeyondInsight.

Job Run Time
12:00 A.M. 

 Select a time of day when the source database has reduced activity. The timezone is that of the SQL server.

You can optionally configure a proxy account for agent job execution.


 When not configured, the agent job executes under the context of the SQL Server Agent service account.

 *Proxy Username* _____

 *Proxy Password* _____

WEB SERVICES CREDENTIALS

Specify a user for the BeyondInsight Web Service to access SQL Server, SQL Server Analysis Services (SSAS) and SQL Server Reporting Services (SSRS).


 This user will be granted permissions to run reports in SSRS, and given read access to the report folders, the SQL Server database, and the Online Analytical Processing (OLAP) cube.

 *Web Services Credentials Username (required)* _____


 *Web Services Credentials Password (required)* _____

SQL SERVER AGENT JOBS: BEYONDINSIGHT PROCESS DAILY

The Process Daily job queries the BeyondInsight database for any changes that have been made since the previous completion of the Process Daily job. It syncs these changes into the Analytics and Reporting SQL database, and builds the Analytics and Reporting cubes. This job is scheduled to run once a day but can also be started on demand if a refresh of the reporting data warehouse is required outside of this schedule. Caution should be exercised when running this job during working hours, as it is intended to be run during times when the BeyondInsight database has reduced activity.

 EXECUTE PROCESS DAILY NOW  REFRESH  DOWNLOAD LOGS

 Search _____

Status	Start Time	Duration	Message
 Succeeded	27 Mar 2019 12:50:46 p.m.	00:30:26	The job succeeded. The job was invoked by user A-SQL2009R2-CBI\Administrator. The last step to run was step 1 (Execute SSIS Packages).



For more information on the permissions needed to install and use Analytics & Reporting, please see the [BeyondInsight Analytics & Reporting Guide](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/analytics/index.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/analytics/index.htm>.

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.

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 policy 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 host name of the BeyondInsight server and the text **eEye EMS CA**.



Example:

- *RCS host name: 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**:
 - Select **No** when asked to export the private key, and then click **Next**.
 - Select the **DER-encoded binary X.509 (*.CER)** format, and then click **Next**.
 - Provide the target destination of the certificate, and then click **Next**.
 - Confirm the settings, and then click **Finish** to export the certificate.

- 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>
```

- Securely copy the certificate to the Privilege Management for Unix & Linux policy and log server hosts.
- 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](https://www.beyondtrust.com/docs/privilege-management/unix-linux/install/solr-installations.htm) at <https://www.beyondtrust.com/docs/privilege-management/unix-linux/install/solr-installations.htm>.

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 policy 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 Admin Guide](https://www.beyondtrust.com/docs/privilege-management/unix-linux/admin/index.htm) at <https://www.beyondtrust.com/docs/privilege-management/unix-linux/admin/index.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 Certificate

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 certificate installation file. You can then set up a group policy with the MSI file 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 Discovery Scanner. You can use the existing client certificate for your Privilege Management for Desktops assets.

Note: Any Privilege Management for Desktops asset to which the MSI is deployed via group policy must have the .NET Framework 4.7.2 prerequisite installed.

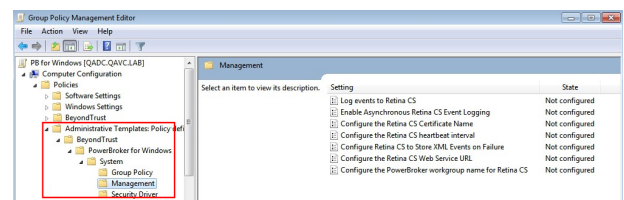
1. Open the BeyondInsight Configuration Tool and select **Certificate Management**.
2. Select **Generate Certificate**.
3. Select **Client Certificate**.
4. Enter a password.
5. Click **OK**.

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)\Eye 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.
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 is 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 AD Bridge 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 AD Bridge and BeyondInsight.



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

Generate a Certificate

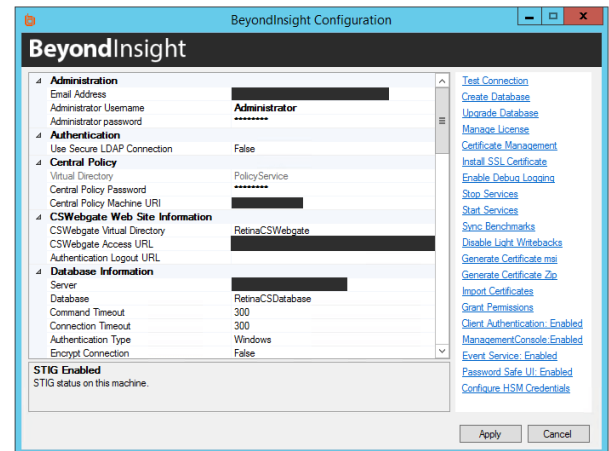
1. Open the BeyondInsight Configuration Tool and select **Certificate Management**.
2. Select **Generate Certificate**.
3. Select **Client Certificate**.
4. Enter a password.
5. Click **OK**.



Configure AD Bridge



1. On the AD Bridge server, run the **DBUtilities** tool.
2. Check the **Enable BeyondInsight** 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. Check the **Validate client certificate** 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.



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	<p>Create an SSL certificate to establish a secure connection to IIS.</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p> 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.</p> </div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p> Note: 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 at https://www.beyondtrust.com/docs/beyondinsight-password-safe/documents/bi/bi-user.pdf.</p> </div>
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.

Setting	Description
Generate Certificate msi	<p>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.</p> <div style="border: 1px solid black; padding: 5px; background-color: #e6f2ff;">  Note: Any system on which the MSI is to be executed needs to have the .NET Framework 4.7.2 prerequisite installed. </div>
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	<p>Click to enable or disable authentication. When disabled, SSL client certificates are ignored. When enabled, client certificates are required, rather than simply accepted.</p> <p>To confirm settings, go to the SSL Settings in IIS for the BeyondInsight server.</p>
Management Console	<p>For environments with multiple console installations, you can disable services to save resources. For example, if you run Password Safe and would like to deploy more than one console, you do not need services running on the secondary consoles.</p> <div style="border: 1px solid black; padding: 5px; background-color: #e6f2ff;">  Note: This setting applies to software installations, not hardware U-Series Appliance installations. </div>

Change the Access URL

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

1. On the BeyondInsight server, go to **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

Online Activation

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, go to **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.



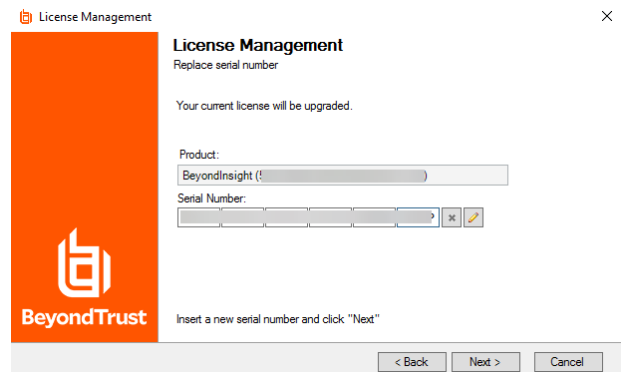
Note: After your license key expires, you can continue to log in to the console. However, product updates are no longer provided.

Offline Activation - U-Series Appliance Only

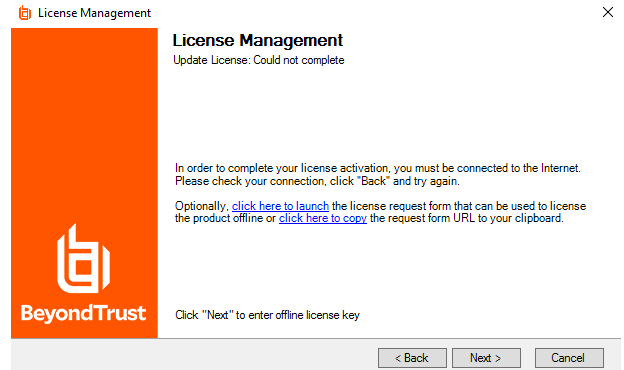
If internet access is not available, you can generate a license key offline.

To activate the license offline:

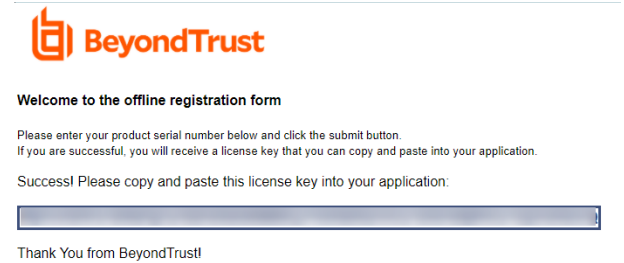
1. On the server hosting BeyondInsight, go to **Start > All Programs > BeyondTrust > BeyondInsight > BeyondInsight Configuration**.
2. Click **Manage License**.
3. Enter the BeyondInsight license key (serial number) provided by BeyondTrust in the **Serial Number** box on the license management utility.



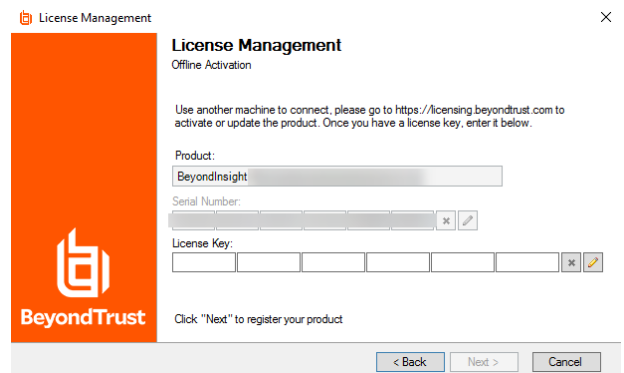
4. Click **Next**. This step fails because there is no Internet access.



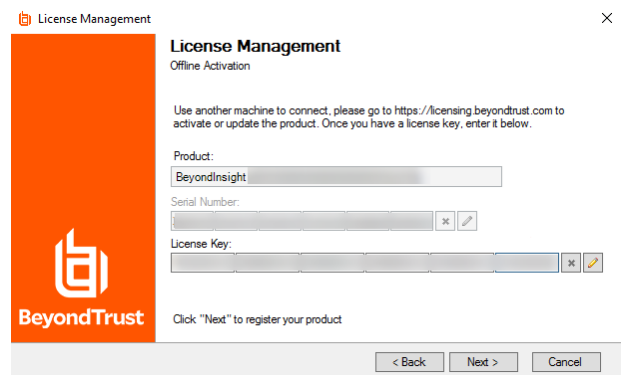
5. Access a machine that has Internet access and browse to the offline licensing form: <https://licensing.beyondtrust.com>.
6. Submit the BeyondInsight license key (serial number) provided to you by BeyondTrust and used during the install process and on the first step of the license management utility.
7. Copy the license key generated for your instance of BeyondInsight.



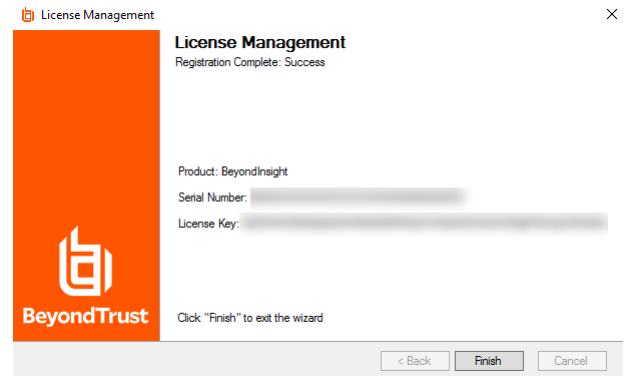
8. Return to the offline system license management utility and click **Next** to get to the page requesting a license key.



9. Insert the license key that you obtained from the offline licensing form result.



10. Click **Next** to complete the offline registration process.



11. Click **Finish** to close the license management utility.

Repeat these steps for all U-Series Appliances in your deployment.

Configure Windows Authentication to the Database

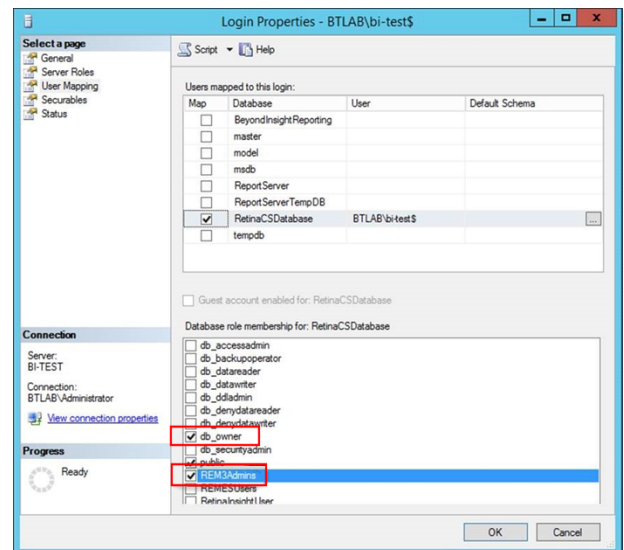
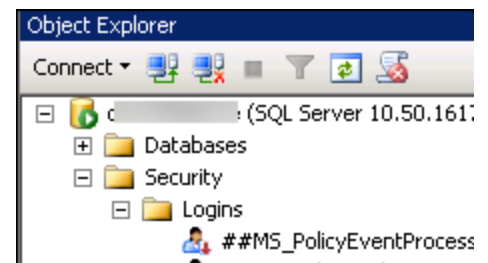
As a security best practice for PCI DSS compliance, use Windows authentication for database access.

i For more information, please see "*Database Permissions Matrix*" on page 12.

Change Database Authentication

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

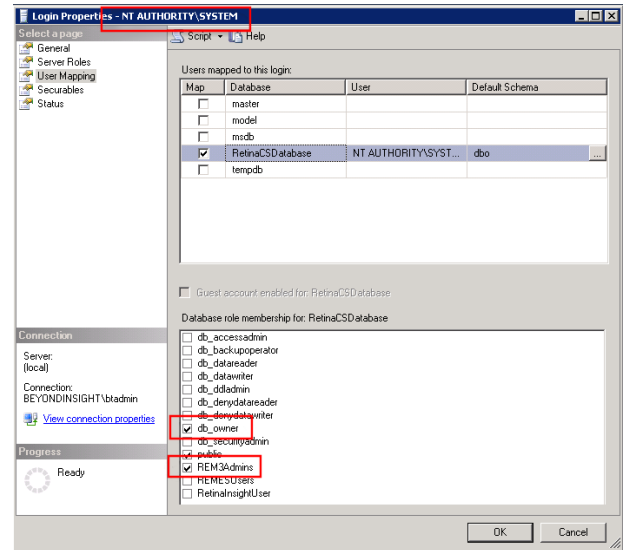
1. Log in to SQL Server.
2. Create a SQL Server login, such as **Domain\RemoteServerName\$**.
3. Go to the properties for the new login, and create a user mapping to the BeyondInsight database and the **REM3Admins** role.



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

i Please visit the [Release Notes](https://www.beyondtrust.com/docs/release-notes/index.htm) at <https://www.beyondtrust.com/docs/release-notes/index.htm> to get the details of each release of BeyondTrust BeyondInsight software.

Download the Installation Package

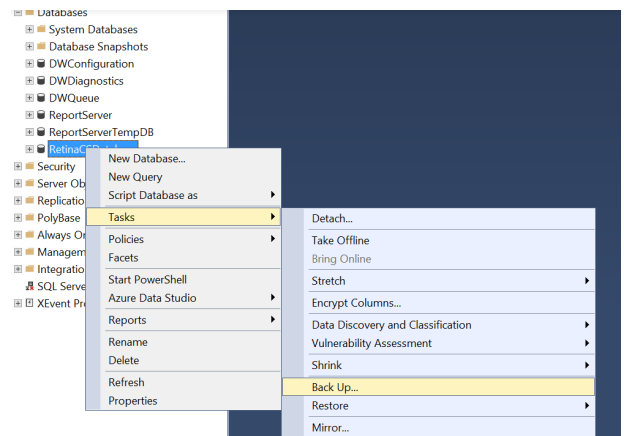
Download the appropriate installer by logging into the BeyondTrust Support Portal at [beyondtrust.com/myportal/downloads](https://www.beyondtrust.com/myportal/downloads).

Note: You must have a BeyondTrust Support account to log in to the Support Portal.

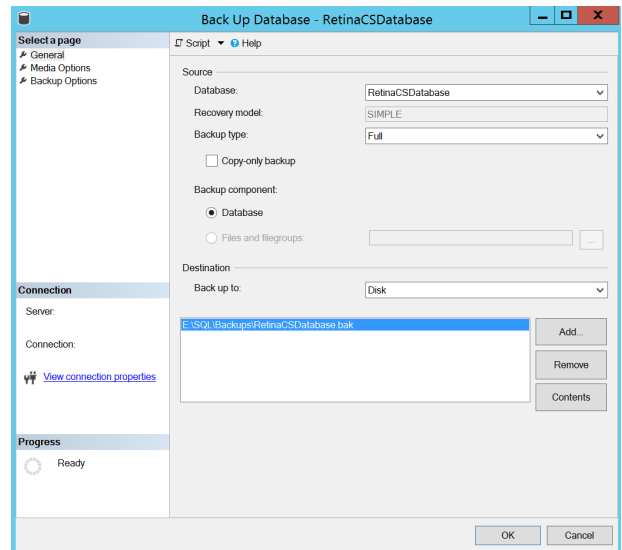
Backup the BeyondInsight Database

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 the database name, and then select **Tasks > Back Up**
- ...



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

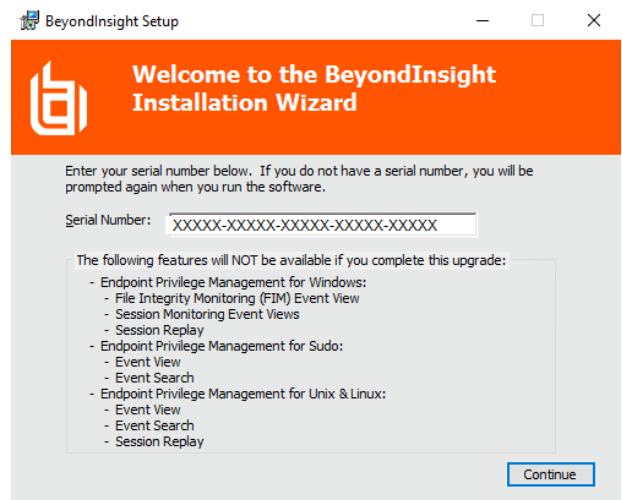


Run the Installer

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



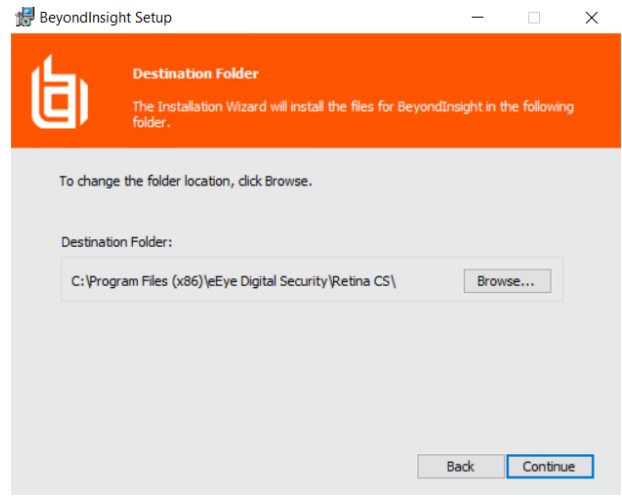
Note: *BeyondInsight 7.0 and later releases do not include support for a number of features. These are listed in the installer on the first step. Proceeding with the installation, in upgrade situations, removes your ability to access the particular functions listed here. You may contact BeyondTrust Support to obtain the Flash SWF files to restore these functions, but this is a manual process.*



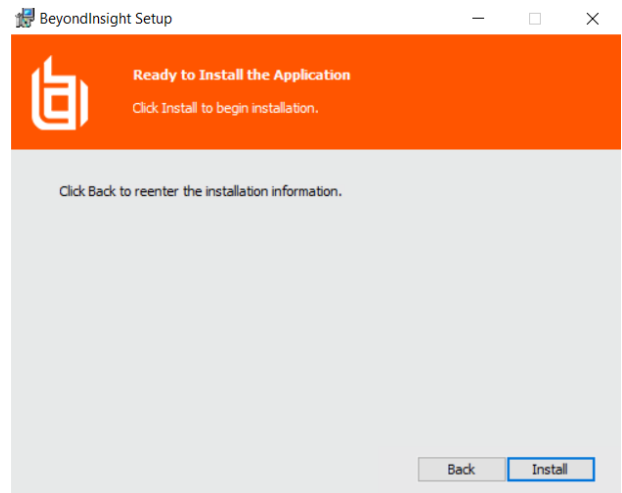
3. Verify the **Destination Folder** where BeyondInsight is installed, and then click **Continue** to begin the upgrade.

! IMPORTANT!

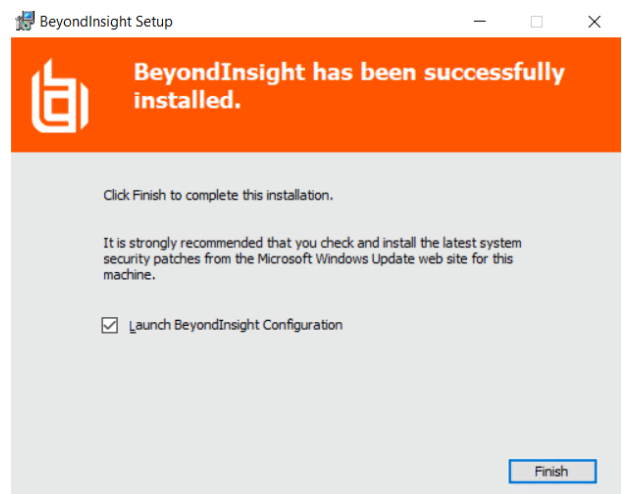
Selecting a destination folder other than the folder where BeyondInsight is installed will cause the upgrade to fail.



4. Click **Install**



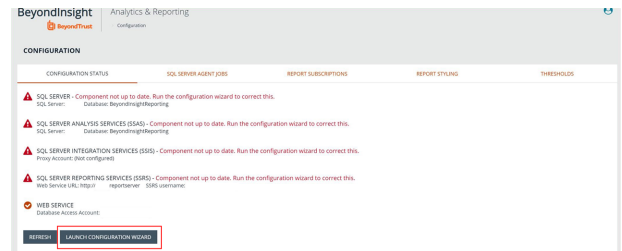
5. When the upgrade installation is complete, click **Finish**.



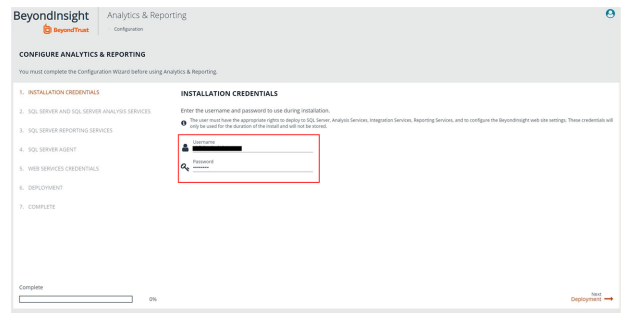
Run the Analytics & Reporting Configuration Wizard

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.

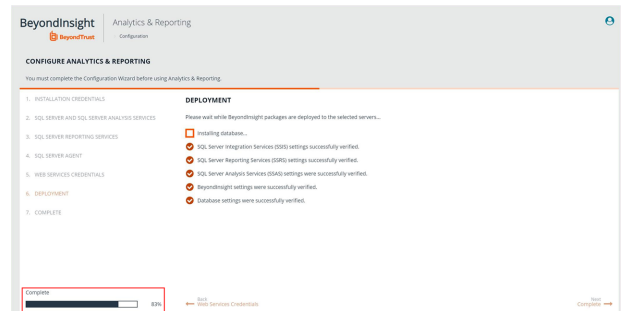


3. In upgrade scenarios, the **Username** and **Password** fields are auto-populated.

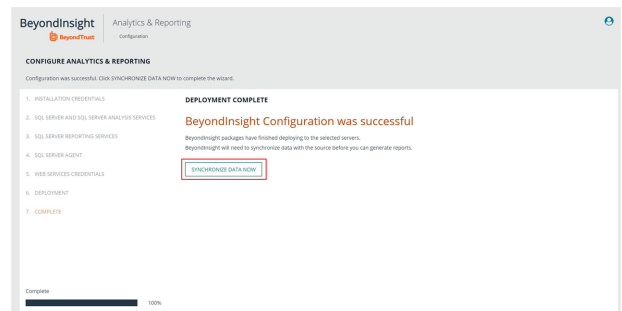


Note: The user credentials must have the appropriate rights to deploy to SQL Server, Analysis Services, Integration Services, and to configure the BeyondInsight website settings.

4. Click **Deployment**. Upgrades to the Reporting Services components are installed 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.

