BeyondTrust

BeyondInsight Event Server Installation Guide 4.1.x

Table of Contents

Install BeyondInsight Event Server	3
Installation Overview	3
Run the Installer	4
Update the Events Client	4
Windows Authentication	5
Export and Import Certificates for Event Server Configuration	6
Export the Certificate	6
Import the EmsClientCert and eEyeEmsServer Certificates	7
Import the eEyeEmsCA Certificate	7
Confirm Certificates for BeyondInsight Server and Event Server	9
Export and Import Crypto Keys for Event Server Configuration	0
Export the Key	0
Import the Key	0
Configure BeyondInsight Custom Certificates	1
Client Certificate Overview1	1
Certificate Registry Keys	2
Validate Certificates	3

Install BeyondInsight Event Server

The event collector role collects events and serves policy for BeyondTrust integrations. Event Server is FIPS 140-2 compliant and supports TLS versions up to TLS 1.2.



You can deploy additional event collectors to scale BeyondInsight to accommodate regional deployments in larger environments. However, it is not a typical installation scenario. It is recommended that BeyondTrust's Professional Services advise you on whether this installation scenario is suited to your BeyondInsight deployment.

For more information about BeyondTrust Professional Services, please see https://www.beyondtrust.com/services/all-services.

Installation Overview

Use the following instructions to deploy BeyondInsight and the event collectors. The following install files and port requirements must be in place:

- BeyondInsight
- Event Server and patches. Confirm the latest version with BeyondTrust. A license is required.
- Port 21690 must be listening for TCP traffic. The port is used to receive SSL encrypted events from agents.

All files can be downloaded from the client portal.

Note: The license key for all event collectors must match the license key for the main BeyondInsight installation.

Below is a high level overview of the installation steps.

- 1. Run the Event Server installer and set up the connection to the database.
- 2. Set up the crypto keys.

For more information, please see "Export and Import Crypto Keys for Event Server Configuration" on page 10.

- 3. Export the crypto key from the primary BeyondInsight server.
- 4. Import the key to all Event Server machines.
- 5. Set up the certificates.

For more information, please see "Export and Import Certificates for Event Server Configuration" on page 6.

- 6. Export the three certificates with private keys from primary BeyondInsight server.
- 7. Import the certificates to all event collector machines.

BeyondTrust

- 8. Configure scanners to point to the Central Policy and send events to the Event Server.
- 9. If using Windows authentication, the Event Server machine name must be added to a local group created on the SQL Server host.

For more information, please see the BeyondInsight Install Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/install/windows-authentication.htm.

Run the Installer

1

- 1. Run the Event Server installer.
- 2. Click Next on the Welcome page.
- 3. Click the check box to accept the licensing terms.
- 4. Select the location for the installation.
- 5. Configure the connection to the database.
 - Enter the IP address of the server hosting SQL Server.
 - Enter the name of the database and include the credentials.
 - Select the Trust Server Certificate check box.
 - Select the Use Encryption check box.

8	Event Server Configuration
Database Information	1
<u>S</u> erver:	WIN-PFR4RL9CJT5
<u>D</u> atabase:	RetinaCSDatabaseRemote
	Trusted Connection (Windows Authentication)
<u>U</u> ser Name:	sa
Password:	•••••
Confirm Password:	******
Time <u>o</u> ut:	300 🗘
	Trust Server Certificate
	Use Encryption
	Test Co <u>n</u> nection
Log Settings	
Pat <u>h</u> :	C:\Program Files (x86)\BeyondTrust\BeyondTrust Event Ser
Log <u>L</u> evel:	Info 🗸
Log <u>T</u> ype:	File V
Apply	QK <u>C</u> ancel

4

Note: If the connection to the database is lost, all events are stored in an encrypted local database. There are no limits on the number of events that can be stored.

- 6. Click Test Connection to ensure the Event Server machine can successfully contact the database machine.
- 7. Set the log settings, including location for the log file, level of logging, and log type.
- 8. Click Apply.

Update the Events Client

You must update the IP address for the client to establish a connection to the Event Server.

1. Start the Events Client.

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs



2. Click the Receiver tab.

🛱 Events Client Sett	tings		×		
ProxyConfiguration	Workgroup	Certificate	Scheduler		
Enabled Applications Receiver					
Select the Events Se workstation.	erver that will rec	ceive events fr	om this		
<u>H</u> ost: 127.0.0.1					
Port: 21690					
<u>T</u> est Con	nection				
		OK	Cancel		

3. Click OK.

i

Windows Authentication

If you use Windows authentication for the Event Server, you must create a local group on the SQL Server host. This group requires **db_ owner** access to the BeyondInsight database and is assigned the **REM3Admins** role.

You must add each Event Server machine name to this local group. For example, DomainName\EventServerMachineName\$.

For more information, please see the <u>BeyondInsight Install Guide</u> at <u>https://www.beyondtrust.com/docs/beyondinsight-</u> password-safe/bi/install/windows-authentication.htm.

Export and Import Certificates for Event Server Configuration

The following BeyondInsight certificates must be exported from the primary BeyondInsight server and then imported on the Event Server:

- eEyeEmsCA: root certificate
- EmsClientCert: client authentication certificate
- eEveEmsServer: server authentication certificate

Export the Certificate

To export the certificate using the Certificates snap-in, follow the steps below:

- 1. Run mmc.exe.
- 2. Select File > Add/Remove snap-in.
- 3. Select Certificates, and then click Add.
- 4. Select Computer Account, and then click Next.
- Select Local Computer, and then click Finish. 5.
- 6. Click OK.
- 7. Expand Certificates.
- 8. Expand Personal, and then select Certificates.
- 9. Right-click eEyeEmsClient > All Tasks > Export.
 - Click Next.
 - Select Yes, export the private key.
 - · Select the check boxes: Include all certificates in the certification path if possible and Export all extended properties.
 - · Enter a password. The password is needed when you import the certificate.
 - · Click browse. Save the file with a .pfx extension, and the click Next.
 - Click Finish.
- 10. Copy the exported file to a network share.



Select the format you want to use:
C DER encoded binary X.509 (.CER)
C Bage-64 encoded X.509 (,CER)
C gryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
\square Include all certificates in the certification path if possible
Personal Information Exchange - PKCS #12 (.PFX)
\square Include all certificates in the certification path if possible
\square Delete the private key if the export is successful
Export all extended properties
C Microsoft Serialized Certificate Store (.SST)

6

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

Import the EmsClientCert and eEyeEmsServer Certificates

You must import the **EmsClientCert** and **eEyeEmsServer** certificates on every Event Server you deploy. These certificates are imported to the **Personal** store.

To import the certificate using the Certificates snap-in, follow the steps below:

- 1. Open the Certificates snap-in.
- 2. Right-click the **Personal** folder, and then select **All Tasks > Import**.
- 3. Click Next on the first page of the import wizard.
- 4. Click Browse
- 5. On the **Open** dialog box, ensure that the file type is selected from the list. The certificate file has a .pfx extension.
- 6. Find the file and click Open. Click Next.
- 7. Enter the certificate password. This is the password that you created when you exported the certificate.



Passw	ord
То	maintain security, the private key was protected with a password.
Ty	be the password for the private key.
	Password:
	•••••
	Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
	Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
	 Mark this key as exportable. This will allow you to back up or transport your keys at a later time. Include all extended properties.
earn n	Mark this key as exportable. This will allow you to back up or transport your keys at a later time. Include all extended properties. ore about <u>protecting private keys</u>
earn n	 Mark this key as exportable. This will allow you to back up or transport your keys at a later time. Include all extended properties. about <u>protecting private keys</u>

- 8. Ensure the Include all extended properties check box is selected.
- 9. Click Next.
- 10. The certificate must be imported to the Personal store. Click Next.
- 11. Click Finish.

Import the eEyeEmsCA Certificate

To import the eEyeEmsCA certificate to the Trusted Root store, follow the steps below:

- 1. Open the Certificate Manager snap-in.
- 2. Expand Trusted Root Certification Authorities.
- 3. Right-click the **Certificates** folder, and then select **All Tasks > Import**.

- 4. Click Next on the first page of the import wizard.
- 5. Click Browse.
- 6. On the **Open** dialog box, ensure that the file type is selected from the list. The certificate file has a .pfx extension.
- 7. Enter the certificate password. This is the password that you created when you exported the certificate.
- 8. Ensure the Include all extended properties check box is selected.
- 9. Click Next.
- 10. The certificate must be imported to the Trusted Root store. Click **Next**.



11. Click Finish.

Confirm Certificates for BeyondInsight Server and Event Server

Confirm certificates on the BeyondInsight server and Event Server are the same by reviewing the information in the **Thumbprint** for the certificate.

Double-click the certificate, and then select the **Details** tab.

Certificate	×
General Details Certification Pat	h]
Show: <all></all>	▼
Field	
Subject	eEyeEmsCA
Public key	RSA (2048 Bits)
Subject Key Identifier	07 42 0f a2 ad f1 19 56 32 7b
Key Usage	Digital Signature, Non-Repudia
Basic Constraints	Subject Type=CA, Path Lengt
Authority Key Identifier	KeyID=07 42 0f a2 ad f1 19 5
Thumbprint algorithm	sha1
Thumbprint	86 84 06 d9 c7 74 4a da 27 cd 💌
86 84 06 d9 c7 74 4	a da 27 cd 23 d0 88 14
UI 10 e2 35 54 Ca	
<u> </u>	
Learn more about certificate detail	<u>s</u>
	ОК

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

Export and Import Crypto Keys for Event Server Configuration

Export the Key

Perform the following steps on the primary BeyondInsight server to export the crypto key:

- 1. Go to the BeyondInsight installation directory. For example, by default: \Program Files (x86)\eEye Digital Security\Retina CS\.
- 2. Run xmltodatabasesynctool.exe.
- 3. Click Cryptography Key.
- 4. Verify Export Key is selected.
- 5. Enter a password.
- 6. Click Export.
- 7. Copy RetinaCS.eKey to a network share.

Import the Key

Perform the following steps on each event collector server to import the crypto key:

- 1. Access the network share where you exported the crypto key and copy to the Event Server computer.
- 2. Run xmltodatabasesynctool.exe.
- 3. Click Cryptography Key.
- 4. Select Import Key.
- 5. Enter the password that you created when you exported the key.
- 6. Click Import.
- 7. Find the key, and then click Open.
- 8. After you import a crypto key, you must set the following values to NULL in the dbo.Version table Access code and Expiry. In SQL Server Management Studio, run the following query on the BeyondInsight database:

update version set AccessCode = null, Expiry = null

depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

©2003-2023 Beyond Trust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. Beyond Trust is not a chartered bank or trust company, or

Configure BeyondInsight Custom Certificates

In your BeyondInsight configuration, you can create certificates rather than use the certificates created and issued by BeyondInsight. You must configure custom certificates in the registry.

Client Certificate Overview

Client certificates are used to authenticate clients and ensure secure transmission of data between agents and BeyondInsight. Each client certificate contains a public and private 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 when it is received.

You can use BeyondInsight generated self-signed client certificates or your own certificates. This allows BeyondInsight to operate in a variety of environments and removes the need to register each system instance with an internet certificate authority.

Client certificates must contain the below details:

- The intended purpose for the certificate. For example, Server Authentication, Client Authentication, or both.
- A Key Usage value of Digital Signature, Key Encipherment, Data Encipherment, Key Agreement.

depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

©2003-2023 Beyond Trust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. Beyond Trust is not a chartered bank or trust company, or

Certificate Registry Keys

The custom certificates in the certificate chain must be added to the correct locations. Review the following tables to confirm the correct locations for the server and client certificates.

BeyondInsight (Server Side)

[HKEY_LOCAL_MACHIN	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\eEye\EMS\Client]			
Кеу	Value	Туре	Description	
storename	MY	REG_SZ	The store name. The default value is $\ensuremath{\textbf{MY}}$ if the key is not present.	
servercertname	eEyeEmsServer	REG_SZ	The server certificate name. Use the name of your trusted certificate.	
			The default value is eEyeEmsServer if the key is not present. Used by Application Bus.	
certname	eEyeEmsClient	REG_SZ	Needs to be created. The client certificate name. Use the name of your trusted certificate. The default value is eEyeEmsClient if the key is not present. Used by Event Server.	
ValidateCertChain	0	DWORD	Needs to be created. Set to 0 to turn certificate chain validation off. This is the required value.	



Validate Certificates

Review the following section to confirm the certificates you created meet the BeyondInsight requirements:

• Confirm the value for the **Key Usage**. The key usage must indicate that the certificate can be used as a digital signature.

Certificate	×
General Details Certification Path	
Show: <all></all>	▼
Field	Value 🔺
Public key	RSA (2048 Bits) 60 80 aa 44 03 30 11 14 e2 19
Key Usage	Digital Signature, Key Encipher
Enhanced Key Usage Basic Constraints Authority Key Identifier Thumbprint algorithm Thumbprint	Server Authentication (1.3.6 Subject Type=End Entity, Pat KeyID=58 d4 37 b9 33 39 8b sha1 39 37 54 f9 87 36 an fr 96 35 , Data Encipherment, Key Agreement
Ed	it Properties Copy to File
	ОК

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

- BeyondTrust
 - Confirm the value for the Enhanced Key Usage. Enhanced key usage must indicate that the certificate can be used for server authentication, client authentication, or both.

• Verify the **Subject** entry. Note the value provided is the name of the certificate that needs to be added to the registry. This example shows the name of the BeyondTrust client certificate.

General Details Certification Pa	th	
Show: <all></all>	•	
Field	Value	*
🛅 Public key	RSA (2048 Bits)	
🛐 Subject Key Identifier	60 80 aa 44 03 30 11 14 e2 19	
Key Usage	Digital Signature, Key Encipher	
Enhanced Key Usage	Server Authentication (1.3.6	
Basic Constraints	Subject Type=End Entity, Pat	Ξ
authority Key Identifier	KeyID=58 d4 37 b9 33 39 8b	
📺 Thumbprint algorithm	sha 1	
Server Authentication (1 3 6 1 5	39 37 54 f9 87 36 an fr 96 35	•
Server Authentication (1.3.6.1.5 Client Authentication (1.3.6.1.5.	39 37 54 f9 87 36 an fr 96 35 .5.7.3.1) 5.7.3.2)	

ertificate General Details Certification Pa	t h
Show: <all></all>	•
Field	Value 🔺
Serial number Signature algorithm Signature hash algorithm Signature hash algorithm Valid from	f8 ad ae 5b 0d 72 b6 a1 sha256RSA sha256 eEyeEmsCA May-02-13 11:49:50 AM
	eEveEmsClient
Public key	RSA (2048 Bits)
CN = eEyeEmsClient	
Learn more about <u>certificate deta</u>	Edit Properties
	ОК

14

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs