BeyondTrust

BeyondInsight Event Server Installation Guide 4.1.x

TC:5/14/2019

Table of Contents

Install BeyondInsight Event Server

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

IMPORTANT!

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.
- BeyondTrust Network Security Scanner
- 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 Vulnerability Management Configuration.

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.

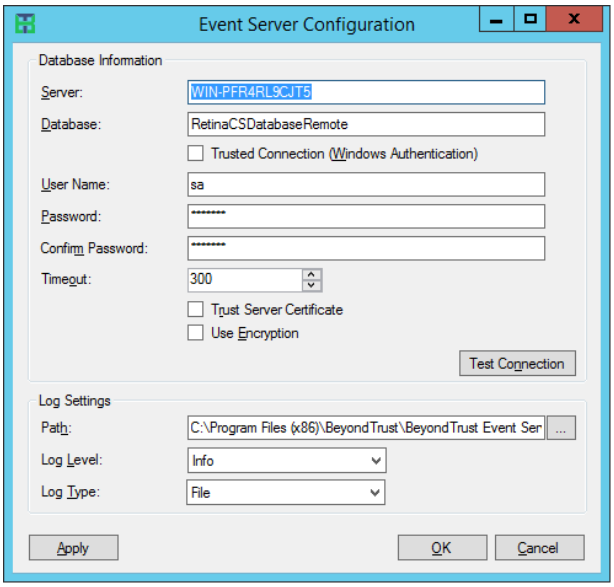
6. Export the three certificates with private keys from primary BeyondInsight server.
7. Import the certificates to all event collector machines.

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 Installation Guide*.

Run the Installer

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.



***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.*

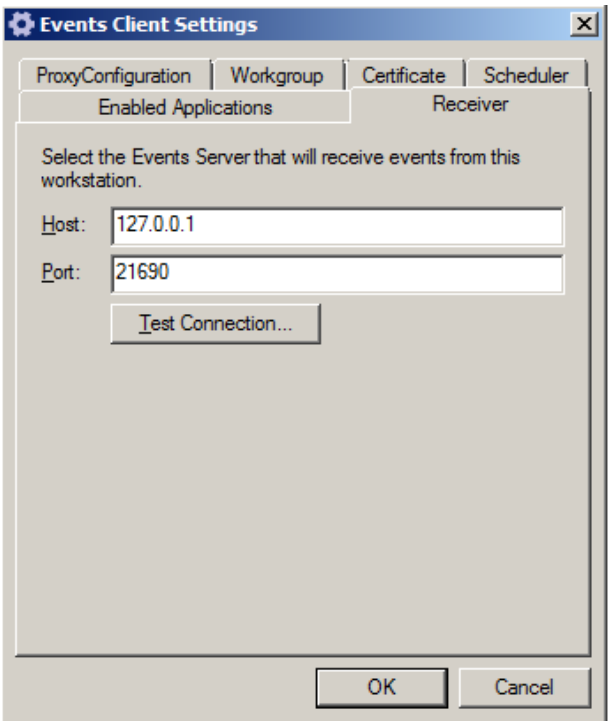
6. Click **Test Connection** to ensure the Event Server machine can successfully contact the database machine.
7. Set the log settings, including location for the log file, level of logging, and log type.
8. Click **Apply**.

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.

2. Click the **Receiver** tab.



3. Click **OK**.

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 *BeyondInsight Installation Guide*.

Export and Import Certificates for Event Server Configuration

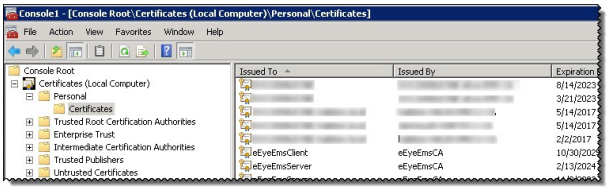
The following BeyondInsight certificates must be exported from the primary BeyondInsight server and then imported on the Event Server:

- **eEyeEmsCA:** root certificate
- **EmsClientCert:** client authentication certificate
- **eEyeEmsServer:** server authentication certificate

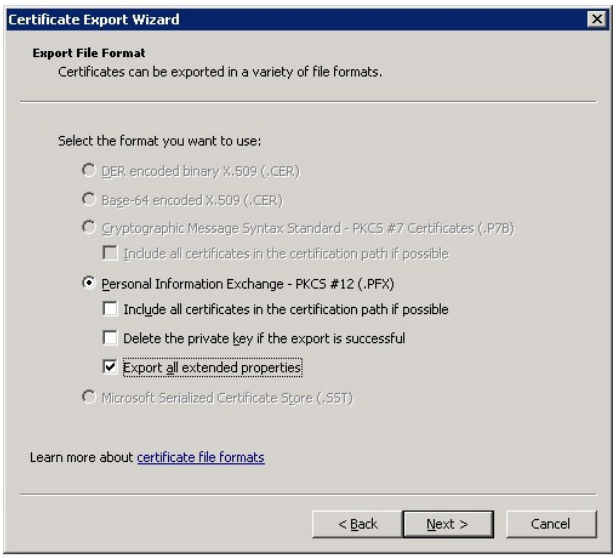
Export the Certificate

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**.
5. Select **Local Computer**, and then click **Finish**.
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 then click **Next**.
    - Click **Finish**.



10. Copy the exported file to a network share.

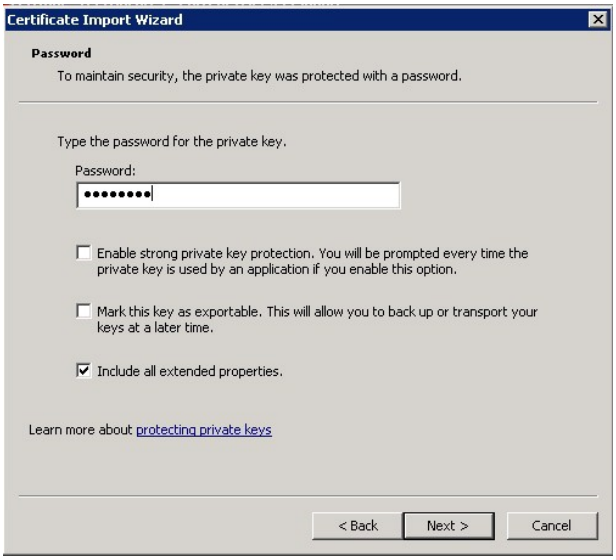
Import the EmsClientCert and eEyeEmsServer Certificates

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.



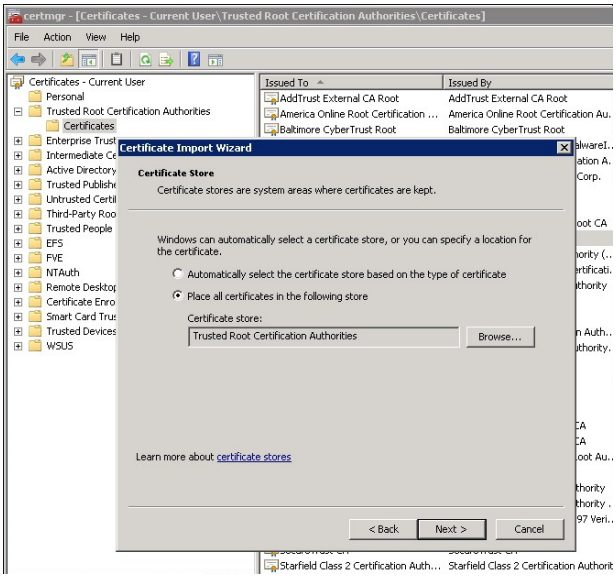
8. Ensure the **Include all extended properties** check box is selected.
9. Click **Next**.
10. The certificate must be imported to the **Personal** store. Click **Next**.
11. Click **Finish**.

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**.

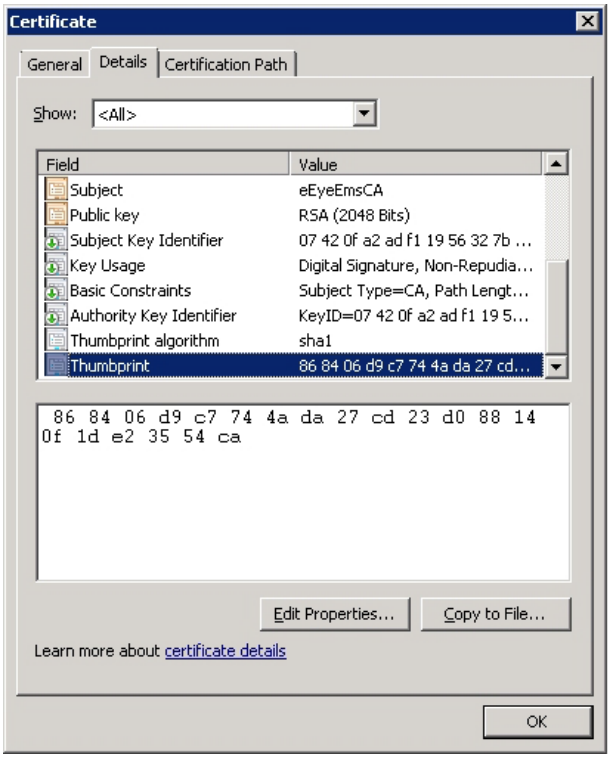


11. Click **Finish**.

Confirm Certificates for BeyondInsight Server and Event Servers

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

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



Export and Import Crypto Keys for Vulnerability Management Configuration

The crypto key is used for Vulnerability Management credentialed scans and password change actions.

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
```

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.

Requirements

- Vulnerability Management 6.3 or later on the client side (this version supports custom certificates).
- Event Server 4.1

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**.

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_MACHINE\SOFTWARE\Wow6432Node\eEye\EMS\Client]			
Key	**Value**	**Type**	**Description**
storename	MY	REG_SZ	The store name. The default value is **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.

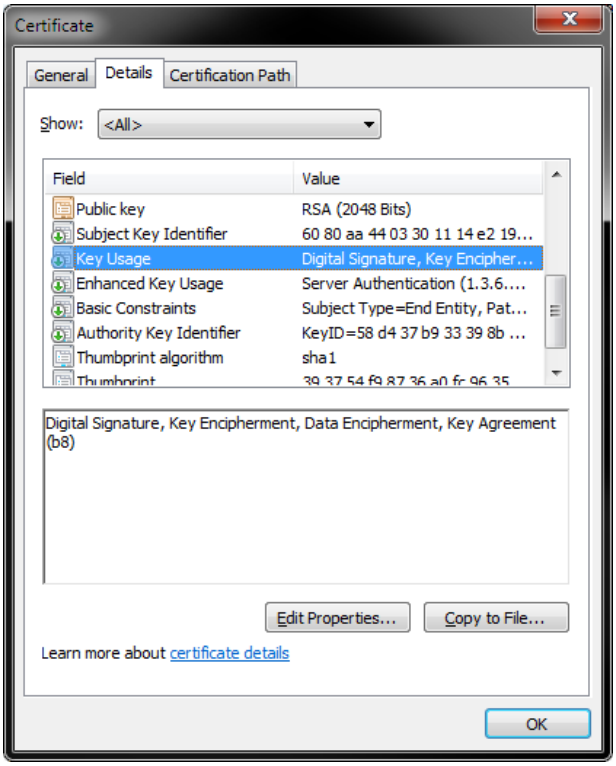
Vulnerability Management (Client Side)

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\eEye\EMS\Client]			
Key	**Value**	**Type**	**Description**
storename	MY	REG_SZ	The store name. The default value is **MY** if the key is not present.
certname	eEyeEmsClient	REG_SZ	Needs to be created. The client certificate name. The default value is **eEyeEmsClient** if the key is not present. Used by Event Server.
ValidateCertChain	0	DWORD	Needs to be created. The default value is **1**. Set to **0** to turn certificate chain validation off. This is the required value.
disableclientauthentication	true	REG_SZ	Needs to be created. Turns off client authentication when set to **true**.

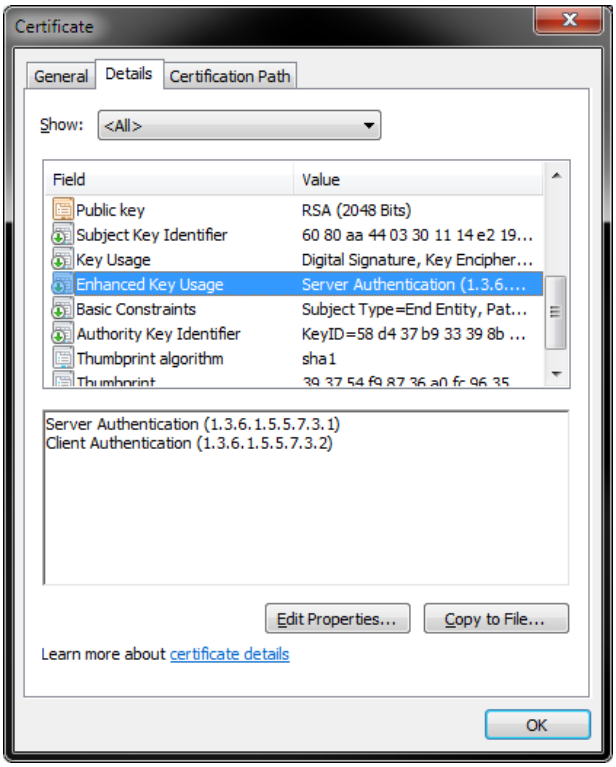
Validate Certificates

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.



- 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.