BeyondTrust

Privilege Management
PMC On Premises Installation Guide
2.4.x

TC:4/3/2020

Table of Contents

Attributes to Record

The following attributes are defined during the deployment process. Where they are defined and subsequently used is listed here. We recommend you make a note of these as you go and record them for reference later. The attributes to record are listed below:

Certificate Passwords

Several passwords are generated by the deployment wizard. You must make a note of these when prompted. Failure to note these passwords will mean that you will not have the passwords for your certificates and will not be able to install them anywhere else.

For more information, please see "Certificates Tab" on page 27

Attributes Defined and Used for all Types of Authentication

Attribute Name	Defined	Used
Server URL	This is the DNS of your SSL Certificate with **:9443** appended to it. It's displayed in full on the **Finish** tab. For more information, please see "Finish Tab" on page 32.	"Log into PMC" on page 37 "Configure Endpoints" on page 41
Tenant ID GUID	This is displayed on the **Authentication** tab for Windows Active Directory and LDAPS authentication. For more information, please see "Authentication Tab" on page 27. For Azure Active Directory authentication, see "Create the Azure AD Tenant" on page 15.	"Authentication Tab" on page 27
Authorization Provider	This is the URL for PMC with **:8443/oauth** appended to it. This is shown on the **Finish** tab of the deployment wizard. For more information, please see "Finish Tab" on page 32.	

Attribute Name	Defined	Used
PMC Portal Application ID	Only required for Azure Active Directory authentication. For more information, please see "Create the PMC Application" on page 17.	"Authentication Tab" on page 27
PMC Portal Key	Only required for Azure Active Directory authentication. For more information, please see "Create the PMC Application" on page 17.	"Authentication Tab" on page 27

Prerequisites

There are several prerequisites prior to running the PMC deployment wizard. Please review each section before you start your deployment:

If your deployment is managed by Professional Services, please ensure you specify any naming convention before starting deployment as service names cannot be changed after deployment.

Machine Prerequisites

PMC must be deployed from a local or mapped drive on your computer. Prior to starting the deployment of PMC, ensure that you copy the PMC deployment media to a local or mapped drive.

You need three types of machine for the PMC deployment:

- "Deployment Machine" on page 9
- "Cluster Nodes" on page 9
- "SQL Server Machine" on page 10

The PMC deployment tool installs a specific version of the Service Fabric Runtime, it is not a prerequisite. The PMC deployment tool will fail if it's already installed. Once you have deployed PMC to your cluster, do not upgrade the Service Fabric Runtime unless BeyondTrust has confirmed that it is compatible.

Ensure that there are no pre-existing security products and or restrictive GPOs are present on these servers that can interfere with the install.

Tip: *When you introduce new media to a machine, it is common for the package to be tagged as coming from the internet, which causes issues when you run the scripts. To resolve this issue, do one of the following:*

- *Right-click the package and select **Properties**. On the **General** tab, check the **Unblock** box and click **OK**.*
- *Within PowerShell, and from the root folder of the build media following extraction, type:*

```
dir -recurse | unblock-file
```

Deployment Machine

The Deployment machine must be running: Windows 10 or Windows Server 2016.

You need to open port 5895 from the deployment machine to all nodes and port 1433 (or SQL Server port used) to SQL Server. Ports 8443, 19000, 19080 must be open from deployment machine to the Service Fabric nodes, and 9443 to the Portal node.

Cluster Nodes

The PMC deployment supports three or five node deployment. Each deployment node must be running Windows Server 2012 R2 or Windows Server 2016. The PMC Deployment Wizard installs Microsoft Service Fabric on each node; you do not need to install this as a prerequisite.

All ports below should be open in-between each of the nodes, as well as 1443 (or SQL Server port used) from the nodes to SQL, as these are required for the runtime of the application.

- 8443
- 9443
- 19080
- 19000
- 1433

SQL Server Machine

The SQL Server machine is used for both the PMC management databases and reporting database, if configured. The SQL Server machine must be running SQL Server 2012 R2 or SQL Server 2016. You also need to install SQL Server Management studio to manage your databases.

You need a SQL account with administration rights for the PMC database creation. SQL server also needs to be in **Mixed** mode to allow for the use of a SQL account.

If you are using reporting, you must install the Privilege Management Reporting database prior to running the PMC deployment wizard as the wizard configures the connection to the Privilege Management database for you.

For more information, please see "Report Database Prerequisite" on page 19.

Note: *SQL Server Express is not supported.*

Ports that are Configured by the Deployment

The deployment tool configures several ports for PMC communication as it runs through the deployment of PMC. If you need to configure these ports manually, please see the following lists.

Ports required for inbound external communication to PMC (outside of the PMC cluster):

Source	Destination	Port Number	Machines	Reason
End Point Networks (normally ANY)	Load Balancer	443	All PMC Cluster Nodes	Client communication over TLS
Trusted Admin IPs Any additional systems calling the API	Load Balancer	8443	All PMC Cluster Nodes	API and MMC over TLS
Trusted Admin IPs	PMC Cluster Nodes	9443	PMC Cluster Node where the PMC portal is installed	PMC admin over TLS
Trusted Admin IPs	PMC Cluster	19000 19080	Deployment machine All PMC Cluster Nodes where the PMC Portal is installed	Communicating with Microsoft Service Fabric cluster, upgrading Service Fabric cluster run-time and viewing the Service Fabric Explorer portal. Used to connect to the portal from outside of the cluster.
Trusted Admin IPs	PMC Cluster Nodes	19001 19002 19003 19081	Deployment machine All PMC Cluster Nodes	Communicating with Microsoft Service Fabric cluster, upgrading Service Fabric cluster run-time and viewing the Service Fabric Explorer portal. Internal between nodes.
Trusted Admin IPs	PMC Cluster Nodes	3389	All PMC Cluster Nodes	Required for remote desktop
Trusted Admin IPs	The Reporting database	1433	Microsoft Management Console (MMC)	The MMC needs to talk to the reporting database for Event Import

Ports required for internal communication inside of the PMC cluster:

Source	Destination	Port Number	Machines	Reason
PMC Cluster Nodes and Deployment Machine	PMC Cluster Nodes and Deployment Machine	135 137 138 139 445	Deployment machine All PMC Cluster Nodes	Microsoft Service Fabric Cluster Communication between nodes, diagnostics, and load balancing
Load Balancer PMC Cluster Nodes	PMC Cluster Nodes	443	All PMC Cluster Nodes	HTTPS
PMC Cluster Nodes	PMC Management PMC Reporting	1433	SQL Machine	Database and Service Fabric cluster communication
PMC Cluster Nodes	PMC Cluster Nodes	6379	PMC Cluster Node where Redis Application Cache is installed	Redis Port
Load Balancer PMC Cluster Nodes	PMC Cluster Nodes	8443	All PMC Cluster Nodes	HTTPS
PMC Cluster Nodes	PMC Cluster Nodes	20001 - 20031	Deployment machine All PMC Cluster Nodes	Internal services to send requests to command processors without using HTTP or HTTPS.
PMC Cluster Nodes	PMC	7081 - 7082	All PMC Cluster Nodes	Internal Java communication
PMC Cluster Nodes	PMC	1433	SQL Machine	SQL

Ports required for outbound communication from the PMC cluster:

Source	Destination	Port Number	Machines	Reason
All PMC Objects	DNS Servers	80/443	N/A	DNS
All PMC Objects	Required	443	N/A	Will vary from customer to customer. Start with **ANY** and tighten, if required.

User and Domain Prerequisites

PMC supports two types of deployment: domain-joined machines and machines that are not connected to a domain:

Computers managed by PMC must be on the network to communicate with the service.

Domain Installs

The PMC deployment wizard must be run as an Administrator user on the deployment machine. The PMC deployment wizard requires a domain user account that is part of the Administrators group on all the service fabric deployment nodes and the SQL machine.

You can use a different account for running the PMC deployment wizard. The account must be an administrator on the deployment machine and must be connected to the same domain as the nodes.

Non-domain Installs

For non-domain installs, you need a user account that is a member of the Administrator group on all the service fabric cluster nodes. The same account must be used on the deployment machine to run the deployment script, as well as all your deployment nodes and the SQL machine.

In addition, you must run the script **Enable-WinRMwithSSL.ps1** on each PMC deployment node using the account that is a member of the Administrators account. This enables WinRM which is required for the deployment to succeed. This script can be found in the **Deployment** folder.

SSL Certificate Prerequisites

You need an SSL certificate for production deployments. Wildcards are not supported for production deployments. The PMC deployment wizard can generate an SSL certificate for evaluation deployments.

Note: *The DNS of the SSL certificate forms the URL for PMC so you should be able to relate it to PMC.*

IMPORTANT!

Service Fabric does not accept SSL certificates which have been provisioned with Cryptography API: Next Generation (CNG) based providers. Your SSL certificate must be provisioned with a CryptoAPI Cryptography Service provider.

If you are using a Subject Alternative Name (SAN) on the SSL, the SAN must include the core domain name.

If you are using an SSL certificate that is trusted by a global provider you do not need to do any further steps. If your SSL certificate is not trusted by a global provider you need to install the root of your SSL certificate into the trusted root of the local machine of the node where you install PMC before you can log in to PMC:

To install the root of your SSL certificate:

1. Copy the CER portion of your root certificate to the node where you installed PMC. By default, this is the first node.
2. Double-click the certificate and select **Install Certificate**.
3. Select **Local Machine** and click **Next**.
4. Select **Place all certificates in the following store** and click **Browse**.

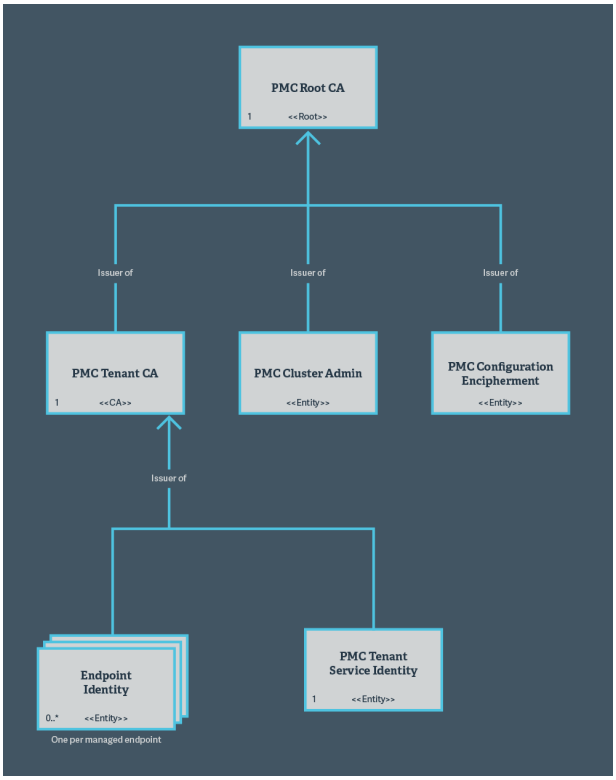
5. Select the second option, **Trusted Root Certification Authorities** and click **OK**.
6. Click **Next** and then **Finish** to complete the installation.

The rest of the PMC certificate chain that is required is generated for you by the PMC deployment wizard.

You need to know the DNS of your SSL certificate so you can set up your chosen method of authentication before you continue.

PMC Certificate Chain

PMC uses certificate-based security to ensure identity and communications security. The image depicts the relationship of the certificates used in the system. Customers are expected to use certificates generated by the deployment tool. This information is provided for transparency and to assist where certificates created outside the PMC deployment tool are desired.



Authentication Prerequisites

PMC supports three types of authentication:

- Windows Active Directory, no PMC specific prerequisites required
- Lightweight Directory Access Protocol Secured (LDAPS), no PMC specific prerequisites required
- Microsoft Azure Active Directory.

For more information, please see "Microsoft Azure AD Authentication" on page 15.

You need to know your method of authentication and configure it for PMC prior to running the PMC deployment tool as some of the authentication settings are required.

You also need to know the DNS for your SSL Certificate, this forms your Portal URL when combined with the PMC port number **9443**.

Mutual Authentication

PMC can only manage endpoints over networks that support mutual authentication. If a Web Application Firewall (WAF) is used in your PMC deployment, then the WAF must support mutual authentication.

Microsoft Azure AD Authentication

You need the following components in Microsoft Azure to authenticate with PMC:

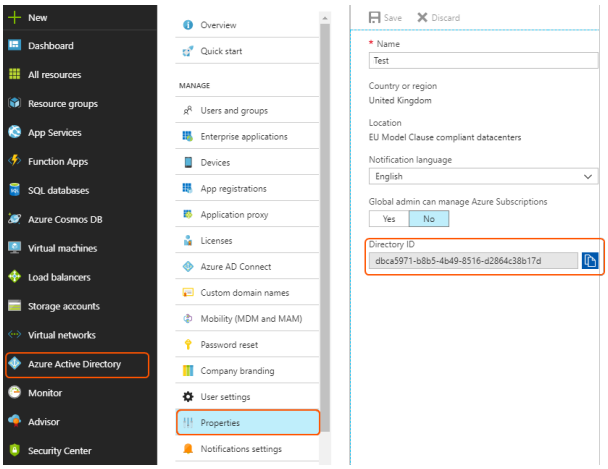
- "Create the Azure AD Tenant" on page 15
- "Create your User in the Tenant" on page 16
- "Create the PMC Application" on page 17

Create the Azure AD Tenant

You need a subscription in Microsoft Azure AD to use it for PMC authentication. By default you have a tenant as part of your subscription. You can either use this default tenant or you can create a new tenant to hold your PMC applications.

Obtain the GUID for your Tenant

You need the GUID for your tenant in Microsoft Azure. Ensure you are in the correct Tenant and click **Azure Active Directory** from the left. Click **Properties**, the GUID for your tenant is the **Directory ID**.



IMPORTANT!

*Record this Directory ID GUID as it is your Tenant ID for Azure. You need to paste it into the PMC deployment tool on the **Authentication** tab and enter it in to PMC to configure the connection.*

Create your User in the Tenant

You need to define the username for the user that will log into PMC for the first time. You can use the default username provided with your tenant or create a new one.

```
username@directoryname.example.com
```

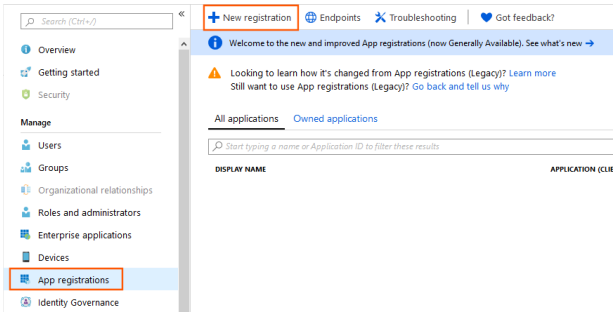
To create a new user:

1. Ensure you are in the Active Directory Tenant that you are using for PMC. You can check and change this from the top right-hand menu.
2. From the left menu, click **Azure Active Directory** and select your PMC Azure Active Directory Tenant from the list if you have more than one.
3. Click **User** in the **Create** menu on the right-hand side.
    - Type in the name of the user, for example, **Joe Bloggs**.
    - The username must take the form **username@directoryname.example.com**. For example: **joe.bloggs@directoryname.example.com**.
    - You can optionally enter some additional information in the **Profile** option, such as their full name and additional work information.
4. Leave the **Properties**, **Groups**, and **Directory role** as the default.
5. Check the **Show Password** box and copy the **Password** to your clipboard. Keep this somewhere safe as you'll need it the first time you log into PMC. This is a temporary password that you can change later on in PMC.
6. You'll receive a notification in the top right-hand corner when the user has been created.

Create the PMC Application

To create the PMC application:

1. Ensure you are in the correct Active Directory Tenant. You can check and change this from the top right-hand menu.
2. From the left menu, click **Azure Active Directory**.
3. Click **App registrations** to display the App registrations panel.
4. On the **App registrations** panel, click **New registration**.



5. Enter the Name as **PMC Portal**.
6. Leave the default Application Type as **Web**.
7. Enter the following string for the **Redirect-URL** and replace the **<DNSofSSLCertificate>** with the DNS you're using.

```
https://<DNSofSSLCertificate>:8443/oauth/signin-oidc
```

8. Click **Create** to finish creating the PMC Portal Application.
9. You need to enter a second Reply URL to the application. Click **Authentication** to add the following string below the first one. Replace the **<DNSofSSLCertificate>** with the DNS you're using.

```
https://<DNSofSSLCertificate>:8443/oauth/signout-callback-oidc
```

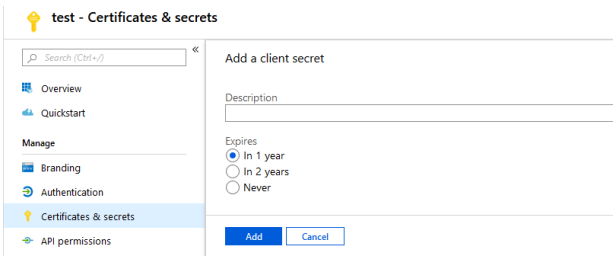
10. Click **Save**.

Generate a Key for your Application

You need to generate a key for your PMC application if you are using LDAPS to authenticate. Once you generate a key you will not be able to access it again in the portal so you must write it down at time of creation.

To generate a key for the PMC application:

1. Click **Azure Active Directory** > **App registrations**. If your application doesn't display, click **All applications**.
2. Click your PMC application that you created previously, and then **Certificates & secrets**.
3. Click **New client secret**.
4. Enter a description for your client secret and set the expiration date. If your key expires you cannot authenticate.



5. Click **Add** to see and copy your key value.

IMPORTANT!

*Record the key for your PMC application. You need the key for the **Authentication** tab of the PMC deployment wizard.*

Obtain the GUID for your Portal Application

Select the PMC application you created. The Application ID is the GUID for your PMC application.

IMPORTANT!

*Record the Application ID for your PMC Portal Application. You need the ID for the **Authentication** tab of the PMC deployment wizard.*

Report Database Prerequisite

If you are using Reporting with PMC you need to set up the Privilege Management Reporting database prior to running the PMC deployment wizard. The PMC wizard configures the connection to Reporting but doesn't create the databases.

The Privilege Management Reporting database must be set up to use SQL authentication or Windows authentication for PMC.

Note: *Check the Release Notes for PMC and Privilege Management Reporting version compatibility.*

For more information about hardware sizing details, please see"Privilege Management Reporting Database Sizes" on page 19

Install the Privilege Management Reporting Database

1. On your SQL Server machine, run the **PrivilegeManagementReportingDatabase_x.x.xx** installer and click **Next**.
2. Accept the End User License Agreement and click **Next**.
3. Select the Database server you want to use from the drop-down list. The name of the database is set to **BeyondTrustReporting**. You can change this if required.
4. You need to change the selection here to **SQL Authentication** or **Windows Authentication** for PMC integration. If you are connecting PMC to an existing Privilege Management Reporting instance you need to change the type of authentication used by SQL.

Note: *You can only use Windows authentication in a domain-joined deployment.*

For more information, please see https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/change-server-authentication-mode.

5. Click **Next**. The **Configure Event Parser Database User** dialog box appears. You do not need to configure this user as it's managed by PMC. Click **Next**.
6. The **Configure Reporting Services Database User** dialog box appears. You do not need to configure this user as it's managed by PMC. Click **Next**.
7. The **Configure Data Admin Database User** dialog box appears. You do not need to configure this user as it is managed by PMC. Click **Next**.
8. Click **Next** and then **Install** to finish the installation. You have now installed the Privilege Management Reporting Database. The PMC deployment wizard will configure the connection to the database.

Note: *You do not need to install the Event Parser or Reporting Pack as PMC includes event centralization and reporting .*

Privilege Management Reporting Database Sizes

These figures are based on the assumption that there are 10 events per day per managed computer, each event is 4KB, and there is 6 months data retention. We also assume Privilege Management Reporting is the only application running on the database server.

Managed Computers	CPU	Memory	Database
10,000	2	12 GB	67.5 GB
25,000	4	16 GB	168.75 GB
50,000	6	16 GB	337.5 GB
75,000	6	22 GB	506.25 GB
100,000	8	24 GB	675 GB
150,000	8	24 GB	1012.5 GB
200,000	8	32 GB	1350 GB

PMC Management Database Prerequisites

The PMC deployment wizard can create and configure the PMC management databases. Alternatively, if you have a separate team within your business who are going to create and configure the PMC management databases, please follow the instructions in this section.

Using Azure AD Authentication:

For a manual set up, you need to create and configure the PMC management databases prior to running the PMC deployment wizard as the wizard checks for them.

For more information, please see "Azure AD Authentication - Create and Configure the PMC Management Databases" on page 21.

Using Windows Active Directory or LDAPS Authentication:

For a manual set up, you need to create the PMC management databases prior to running the PMC deployment wizard as the wizard checks for them. In this instance, you will configure the databases after the PMC deployment as the database scripts need the Tenant ID GUID, which is generated for you by the deployment wizard. The database scripts also need PMC Admin Username and PMC Admin Email Address which you are prompted to enter on the **Authentication** tab.

For more information, please see "Authentication Tab" on page 27.

The configuration of the PMC management databases also requires the Tenant GUID, which is generated for you by the deployment tool and also displayed on the **Authentication** tab.

For more information, please see "Windows AD and LDAPS Authentication - Create the PMC Management Databases" on page 22.

Azure AD Authentication - Create and Configure the PMC Management Databases

You need the following information to create and configure the PMC management databases.

Attribute	Location
TenantID	This is your Tenant ID GUID from Microsoft Azure. For more information, please see "Create the Azure AD Tenant" on page 15.
Account Name	This is your account name for PMC. For more information, please see "Create your User in the Tenant" on page 16.
Email Address	This is the email address associated with the Account Name.

The scripts to configure the databases are in the **SQL** folder of the PMC deployment package.

To create and configure the PMC management database manually:

1. Create a database called **Avecto.IC3.Database.Management**. Ensure the logged on user has the **dbo.owner** SQL server permission.
2. Execute the **Avecto.IC3.Database.Management.sql** script.
3. Edit the **AuthorizationModel.sql** script and replace `<TENANTID>` on the fourth line of the script with your information:
    - `<TENANT ID>`
4. Execute the now modified **AuthorizationModel.sql** script.
5. Edit the **CreateJobAgentServiceUser** script and replace the following placeholder with your information:
    - `<TENANT ID>`
6. Execute the now modified **CreateJobAgentServiceUser.sql** script.
7. Edit the **CreateAutomationClientUser.sql** script and replace the following placeholder with your information:
    - `<TENANT ID>`
8. Execute the now modified **CreateAutomationClientUser.sql** script.
9. Edit the **CreateAdministratorUser.sql** script and replace the following placeholders with your information:
    - `<TENANT ID>`
    - `<ACCOUNT NAME>`
    - `<EMAIL ADDRESS>`
10. Execute the now modified **CreateAdministratorUser.sql** script.
11. Edit the **CreateSystemConfigurationSettingsDefault.sql** script and replace the following placeholders with your information:
    - `<TENANT ID>`
12. Execute the now modified **CreateSystemConfigurationSettingsDefault.sql** script.
13. You need to open the firewall port for the instance of SQL. If this is the default instance, the port number is 1433, otherwise see "PMC Database Tab" on page 29.

The PMC management database is now created.

Create and to set up the PMC Blob Storage database manually:

1. Create a database called **Avecto.IC3.Database.BlobStorage**. Ensure the database has SQL server authentication with the **dbo.owner** permission.
2. Execute the **Avecto.IC3.Database.BlobStorage.sql** script.

The database for the blob storage is now created.

Windows AD and LDAPS Authentication - Create the PMC Management Databases

For Windows Active Directory and LDAPS authentication you need to configure the PMC management databases after you have run the PMC deployment wizard, however you need to create the databases before you run the PMC deployment wizard.

To create the PMC management databases manually:

1. Log into your SQL Server machine with your credentials.
2. Create a database called **Avecto.IC3.Database.Management**. Both SQL and Windows authentication is supported. Ensure the database has the **dbo.owner** permission, as this is required for creation. This user is not subsequently used by PMC, as you configure a different user to communicate with the PMC services when you set up the PMC services.

3. Create a database called **Avecto.IC3.Database.BlobStorage.sql**. Ensure the database has the **dbo.owner** permission. This user is not subsequently used by PMC, as you configure a different user to communicate with the PMC services when you set up the PMC services.

Deploy PMC

The PMC system is deployed using a PowerShell-based tool that is executed from the deployment machine. The deployment tool connects to the database server and PMC cluster nodes to install and verify prerequisites and make configuration changes.

The PMC deployment tool configures a number of ports when it deploys PMC.

For more information, please see "Ports that are Configured by the Deployment" on page 11.

The default PowerShell execution policy is **Restricted**, which stops any scripts running. To set the execution policy:

1. Open PowerShell as an elevated application.
2. Navigate to the **Deployment** folder in the PMC package.
3. Run **Set-ExecutionPolicy unrestricted -scope CurrentUser -f**

For information on how to configure the setting using Group Policy, please see the Microsoft document Set-ExecutionPolicy at https://technet.microsoft.com/en-us/library/hh849812.aspx.

PMC Deployment Tool Tabs

The PMC system is deployed using a PowerShell-based tool that is executed from the deployment machine. The deployment tool connects to the database server and PMC cluster nodes to install and verify prerequisites and make configuration changes.

The PMC deployment tool configures a number of ports when it deploys PMC.

For more information, please see "Ports that are Configured by the Deployment" on page 11.

The default PowerShell execution policy is **Restricted**, which stops any scripts running. To set the execution policy:

1. Open PowerShell as an elevated application.
2. Navigate to the **Deployment** folder in the PMC package.
3. Run **Set-ExecutionPolicy unrestricted -scope CurrentUser -f**

For information on how to configure the setting using Group Policy, please see the Microsoft document Set-ExecutionPolicy at https://technet.microsoft.com/en-us/library/hh849812.aspx.

To start the on-premise deployment of PMC, run **BeyondTrust PMC Deployment Wizard.ps1**.

There are several tabs that you will step through. These are listed in order below. Please ensure that you monitor your deployment until it has completed. Once the machine and software prerequisites are in place, a typical PMC installation will complete in less than 30 minutes.

1. "PMC EULA" on page 25
2. "Welcome Tab" on page 25
3. "Installation Tab" on page 25

PMC EULA

You need to accept the End User License Agreement (EULA) to install PMC. After you have read the agreement, check the box at the bottom of the screen and click **Next**.

Click **Next** to proceed to the **Welcome Tab**.

For more information, please see "Welcome Tab" on page 25

Welcome Tab

The **Welcome** screen introduces you to the PMC deployment wizard. If you are performing a non-domain joined install, ensure that you are using the same user to run the PMC deployment as you have set up in the Windows Administrators group on the deployment PMC cluster nodes and SQL machine and you have run the PowerShell script to enable WinRM. This script can be found in the **Deployment** folder.

For more information, please see "Report Database Prerequisite" on page 19.

For Windows Directory and LDAPS authentication, the PMC deployment wizard generates a Tenant ID GUID that is used for the PMC management database configuration and the PMC adapter set up after deployment. You need to copy this Tenant ID GUID from the PowerShell window at the start of the deployment, or from the **Authentication** tab where it is displayed again once you select Windows Active Directory. You can disregard this Tenant ID GUID for Azure authentication as you use the Tenant GUID from Azure for this purpose.

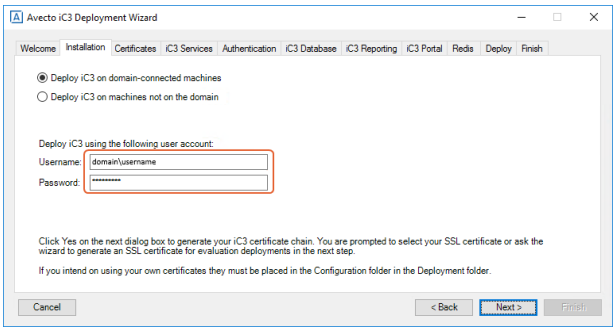
Click **Next** to proceed to the **Installation Tab**.

For more information, please see "Installation Tab" on page 25.

Installation Tab

Choose between deploying PMC to domain-connected machines or machines not on a domain.

Enter the domain and username as well as the password for the user that is a member of the Windows Administrators group on your deployment PMC cluster nodes and SQL machine.



When you click **Next** the PMC deployment wizard validates that this user exists and is a member of the Windows Administrators group, the wizard stops if this is not the case.

Certificate Check and Creation

After validating the user, the PMC deployment wizard generates the PMC certificate chain.

The following certificates are generated:

- PMC Configuration Encipherment
- PMC Tenant CA
- PMC Tenant Service Identity
- PMC Cluster Admin
- PMC Root

If you have previously run the deployment with this build but not completed it the certificates are in the **Configuration** folder within the **Deployment** folder. You can use the same certificates if you made a note of the passwords, otherwise you can delete the certificates and the PMC deployment wizard can generate a new chain when prompted.

The PMC deployment wizard prompts you for an SSL certificate. If this is an evaluation deployment you can click **Yes** to generate an SSL certificate, otherwise click **No** to browse to the PFX part of the SSL certificate that you intend to use for PMC.

If you allow the deployment utility to generate an evaluation certificate it will contain an asterisk to indicate a wildcard. You need to replace this wildcard with your domain when prompted to do so on the **PMC Portal** tab. Wildcards are supported for evaluation deployments, however multiple sub-domains are not.

The use of an SSL certificate that contains a wildcard is not supported for production deployments. You must supply your own SSL certificate for a production deployment with the appropriate domain.

***Note:** Generating an SSL certificate is only supported for evaluation deployments as it is not rooted to a public certificate authority that is trusted by Windows or Mac.*

Click **Next** to proceed to the **Certificates Tab**.

For more information, please see "Certificates Tab" on page 27.

If you allow the deployment utility to generate an evaluation certificate it will contain an asterisk to indicate a wildcard. You need to replace this wildcard with your domain when prompted to do so on the **PMC Portal** tab. Wildcards are supported for evaluation deployments, however multiple sub-domains are not.

The use of an SSL certificate that contains a wildcard is not supported for production deployments. You must supply your own SSL certificate for a production deployment with the appropriate domain.

Note: *Generating an SSL certificate is only supported for evaluation deployments as it is not rooted to a public certificate authority that is trusted by Windows or Mac.*

Click **Next** to proceed to the .

Certificates Tab

The passwords for the certificates are generated automatically and displayed here (only) so you can record them. The SSL password is shown on this screen if you chose to automatically generate it for an evaluation deployment. If you provided your own SSL certificate you need to provide the password for it on this tab.

IMPORTANT!

Record all the passwords before you proceed. If you do not record the passwords you will not be able to access them again after the deployment.

Click **Next** to proceed to the **PMC Services Tab**.

For more information, please see "PMC Services Tab" on page 27.

PMC Services Tab

Select an option depending on the size of your PMC node cluster.

Enter the names of your deployment PMC deployment nodes here. The names and existing software are validated when you proceed. In addition the PMC deployment tool validates that Service Fabric has not already been installed on the nodes. It will fail if Service Fabric is already present.

Click **Next** to proceed to the **Authentication Tab**.

For more information, please see "Authentication Tab" on page 27.

Authentication Tab

This tab is split into two sections. In the first half you need the enter the PMC Admin Username and PMC Email Address for your PMC administrator.

1. Enter your PMC Admin Username and PMC Admin Email. The PMC Admin Email must take the form **<username>@<Domain>.com**.

> ***Note:*** *If you are configuring your databases manually then you need to ensure that you use the same PMC Admin Username and PMC Admin Email that you entered here for the script.*

In the second section you need to select the type of authentication provider. You can choose from:

- **Windows Active Directory**
- **LDAPS**
- **Azure Active Directory**

Windows Active Directory

1. The **Tenant ID** is generated by the deployment tool. You can change it if required, but you must ensure that it matches the GUID used to set up the PMC management database (if this was done manually). If you change the GUID and the deployment tool is setting up the PMC management database then it will use the new GUID that you provide here.
2. Enter the domain of your Windows Active Directory.

LDAPS

1. The **Tenant ID** is generated by the deployment tool. You can change it if required, but you must ensure that it matches the GUID used to set up the PMC management database (if this was done manually). If you change the GUID and the deployment tool is setting up the PMC management database then it will use the new GUID that you provide here.
2. Enter the domain of your LDAPS (Lightweight Directory Access Protocol over SSL).
3. Enter the LDAPS Distinguished Name (DN).
4. Enter the LDAPS filter.

Azure Active Directory

1. Enter your Azure Tenant ID.

> For instructions on getting this Tenant ID if you did not make a note of it when configuring Azure AD, please see "Create the Azure AD Tenant" on page 15.

2. Enter your Azure Application ID.

> For instructions on getting this GUID if you did not make a note of it when you configured Azure AD, please see "Create the PMC Application" on page 17.

3. Enter your designated key for your PMC Portal application.

> For instructions on generating and saving this key if you did not create and make a note of it when you configured Azure AD, please see "Create the PMC Application" on page 17.

Click **Next** to proceed to the **PMC Database Tab**.

For more information, please see "PMC Database Tab" on page 29.

PMC Database Tab

If you have created the PMC management databases manually prior to starting this deployment, select **I have already created the PMC databases**.

If you want the PMC deployment wizard to create and configure the PMC management databases, select **I want to create and configure the PMC databases automatically** to allow the wizard to create and configure the PMC databases.

1. Enter the **SQL Hostname**, **Instance**, and **Port number**. If the instance is not the default instance, you need to find the port number for your named instance and enter it here.
2. Enter your SQL credentials, these need to have the **SQL sysadmin** permission. These credentials are only used to set up the PMC management database. They are not subsequently used by PMC, as authentication with the PMC management database is done using the credentials specified in the next section of the dialog.
3. Choose from **SQL authentication** or **Windows authentication** and enter the credentials. If your deployment is non-domain-joined, you must use SQL authentication. This user manages the authentication of the PMC Management database with the PMC application services. The wizard creates this user if it doesn't already exist and assigns the **db_datareader**, **db_datawriter**, and **execute** permissions. You can only use Windows authentication in a domain-joined deployment.
4. Click **Next** to proceed to the **PMC Reporting** tab.

For more information, please see "PMC Reporting Tab" on page 29.

The authentication you choose here is the same as the authentication for the **PMC Reporting** tab.

Obtain the SQL Port for a Specific Instance

To obtain the SQL instance port number:

1. Open the SQL Server Configuration Manager.
2. From the left-hand menu, navigate to **SQL Server Network Configuration** > **Protocols for 'Instance Name'**.
3. In the right-hand panel, right-click on **TCP/IP** and scroll down to the last section called **IPAll**. The port number is listed to right of **TCP Dynamic Ports**.

Click **Next** to proceed to the **PMC Reporting** tab.

For more information, please see "PMC Reporting Tab" on page 29.

PMC Reporting Tab

Select **I have already created the Reporting database** if someone in your organization has created the Reporting database and you want the wizard to configure the connection to PMC, or select **I do not want to configure Reporting** if you are not using reporting with PMC.

The SQL Hostname, SQL Instance, SQL Database, and SQL Port that you provide are validated at this stage.

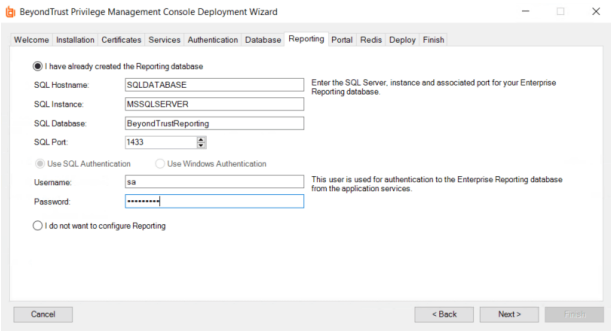
To configure the connection to the Privilege Management Reporting database:

*If there is no named instance, the default instance name of **MSSQLSERVER** should be used.*

1. Enter the SQL Hostname, Instance, and Port number. If the instance is not the default instance you need to find the port number for your named instance and enter it here.

For more information, please see "Obtain the SQL Port for a Specific Instance" on page 30.

2. Choose from **SQL authentication** or **Windows authentication** and enter the credentials of the user that you created in the prerequisites. If your deployment is non-domain-joined, you must use SQL authentication. This user manages the authentication of the Privilege Management Reporting database with the PMC application services.



The PMC deployment wizard needs a user with the **dbo.owner** permission to configure Reporting for PMC. After the installation completes, the user permissions can be reduced to **dbo_datareader**, **db_datawriter**, and **execute**.

The following script demotes the user. Replace **myusername** with your username.

```
EXECUTE sp_addrolemember 'db_datareader', 'myusername'
EXECUTE sp_addrolemember 'db_datawriter', 'myusername'
GRANT EXECUTE ON SCHEMA::dbo TO [myusername]
EXECUTE sp_droprolemember 'db_owner', 'myusername'
```

Obtain the SQL Port for a Specific Instance

To obtain the SQL instance port number:

1. Open the SQL Server Configuration Manager.
2. From the left-hand menu, navigate to **SQL Server Network Configuration** > **Protocols for 'Instance Name'**.
3. In the right-hand panel, right-click on **TCP/IP** and scroll down to the last section called **IPAll**. The port number is listed to right of **TCP Dynamic Ports**.

Click **Next** to proceed to the **PMC Portal Tab**

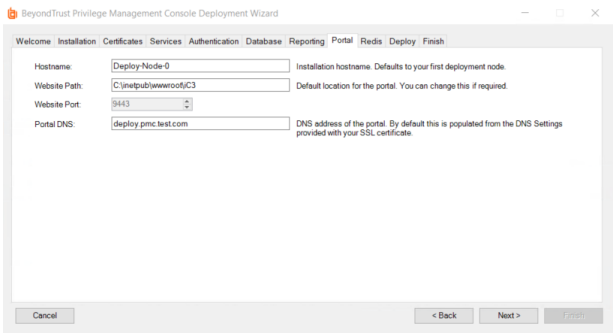
For more information, please see "PMC Portal Tab" on page 30.

PMC Portal Tab

This tab configures where PMC is installed. We recommend you install PMC to the first node in your cluster.

To configure the location for PMC:

1. The **Hostname** is pre-populated with your first node but you can edit this if required.
2. You can change the **Website path** to install PMC to a different location on the node if required.
3. The port number for the PMC portal is **9443**. This cannot be changed.
4. The **PMC Portal DNS** is populated from the DNS Settings provided with your SSL certificate. If you generated a certificate for an evaluation deployment or provided an SSL certificate with a wildcard in for an evaluation deployment, you need to delete the asterisk character and replace it with your domain before you proceed.



Click **Next** to proceed to the **Redis Tab**

For more information, please see "Redis Tab" on page 31.

Redis Tab

This tab configures where the Redis application cache is installed. We recommend you install the Redis application cache on the first node in your cluster. The Redis instance should be behind a firewall and only accessible from the cluster nodes and the deployment box.

To configure the location for the Redis application cache:

1. The **Redis Hostname** is pre-populated with your first node in your PMC cluster, but you can edit this if required.
2. You can change the **Redis Install Path** to a different location on the node if required.
3. The port number for Redis is **6379**. This cannot be changed.

The Redis password is shown on this tab. You can change this before you proceed if required.

IMPORTANT!

Record the Redis password before you proceed. You can decrypt it at a later stage if you forget but it's easier to record it at this stage.

Click **Next** to proceed to the **Deploy Tab**.

For more information, please see "Deploy Tab" on page 31.

Deploy Tab

A summary of all your PMC deployment messages is displayed in the window. You can review these if required. When you are ready to start your PMC deployment, click **Next**.

A typical PMC deployment takes about 30 minutes but can take longer depending on machine specifications and network connectivity.

Once deployment has finished the **Finish Tab** displays.

For more information, please see "Finish Tab" on page 32.

Finish Tab

The **Finish** tab gives you the Server URL you need to access PMC. This is the DNS of your SSL certificate with the PMC port **9443** appended to it.

Please copy and paste the contents of the PowerShell window that you used for deployment. This information may be required to validate provided deployment parameters.

IMPORTANT!

Record the Server URL as you will need it to log into PMC.

You should now log into your Service Fabric Dashboard to confirm you have deployed PMC successfully.

For more information, please see "View the Health of your Service Fabric Cluster" on page 35.

Resolution of DNS

You need to be able to resolve the DNS before you can log into PMC. If you are using a public DNS that has not yet been created, you will need to create manual entries in the host files of the machines that need to communicate, such as the cluster nodes (including where the portal is installed).

Deployment Logs

All the events from the PowerShell script during setup and deployment are logged in a folder in this directory:

```
C:\Users\<yourusername>\AppData\Roaming\Avecto\AvectoIC3DeploymentWizard
```

AppData is a hidden folder. You can access it by viewing hidden items in Windows Explorer or typing in `%appdata%` into Windows Explorer.

The **BeyondTrust PMC Deployment Wizard.ps1** script contains the setup and deployment logs including the Windows Directory and LDAPS GUID that was generated.

Windows AD and LDAPS - Manually Configure the PMC Management Databases

You only need to do the steps in this chapter if you are using Windows Active Directory or LDAPS to authenticate with PMC, and you created your databases manually rather than allowing the PMC deployment wizard to create them. You need the following information to configure the PMC management databases manually.

Attribute	Location
TenantID	This is the Tenant ID GUID that is generated for you by the PMC deployment tool. For more information, please see "Authentication Tab" on page 27.
Account Name	This is your account name for PMC. It should match the PMC Admin Username that you entered on the **Authentication** tab. For more information, please see "Authentication Tab" on page 27.
Email Address	This is the email address for PMC, for example, **username@directoryname.onmicrosoft.com**.

The scripts to configure the databases are in the **SQL** folder of the PMC deployment package.

You need to ensure that you open the firewall port for the instance of SQL. If this is the default instance, the port number is **1433**. Otherwise see "PMC Database Tab" on page 29.

To create and configure the PMC management database manually:

1. Create a database called **Avecto.IC3.Database.Management**. Ensure the database has SQL server authentication and the user has the **dbo.owner** permission.
2. Execute the **Avecto.IC3.Database.Management.sql** script.
3. Edit the **AuthorizationModel.2_0.sql** script and replace `<TENANTID>` on the fourth line of the script with your information:
   - `<TENANTID>`
4. Execute the now modified **AuthorizationModel.sql** script.
5. Edit the **CreateJobAgentServiceUser** script and replace the following placeholder with your information:
   - `<TENANT ID>`
6. Execute the now modified **CreateJobAgentServiceUser.sql** script.
7. Edit the **CreateAutomationClientUser.sql** script and replace the following placeholder with your information:
   - `<TENANT ID>`
8. Execute the now modified **CreateAutomationClientUser.sql** script.

9. Edit the **CreateAdministratorUser.sql** script and replace the following placeholders with your information:
    - `<TENANT ID>`
    - `<ACCOUNT NAME>`
        - This is your account name for PMC. It should match the PMC Admin Username that you entered on the Authentication tab.
    - <EMAIL ADDRESS>
        - This is the email address for PMC, for example, **username@directoryname.onmicrosoft.com**.

> For more information, please see "Authentication Tab" on page 27.

10. Execute the now modified **CreateAdministratorUser.sql** script.
11. Edit the **CreateSystemConfigurationSettingsDefault.sql** script and replace the following placeholders with your information:
    - `<TENANT ID>`
12. Execute the now modified **CreateSystemConfigurationSettingsDefault.sql** script.

The PMC management database is now created.

To set up the PMC Blob Storage database manually:

Execute the **Avecto.IC3.Database.BlobStorage.sql** script against the **Avecto.IC3.Database.BlobStorage** database that you created earlier.

The database for the blob storage is now created.

The PMC management database is now created.

To set up the PMC Blob Storage database manually:

1. Execute the 'Avecto.IC3.Database.BlobStorage.sql' script against the 'Avecto.IC3.Database.BlobStorage' database that you created earlier.

The database for the blob storage is now created.

View the Health of your Service Fabric Cluster

The Microsoft Azure Service Fabric Explorer can tell you very quickly if there are any issues in your deployment and can help you identify where any issues are. The dashboard shows you how many nodes and applications are in your cluster. Any errors or warnings are highlighted here.

You can drill down into each of the applications, cluster nodes, and system services on the left-hand panel. This information can be combined with the logs to troubleshoot PMC, if required.

You can view the status of your Microsoft Service Fabric once you have installed the PMC Cluster Admin certificate onto the machine you are using. The PMC Cluster Admin certificate is installed by the PMC deployment wizard on the deployment machine by default.

Install the PMC Cluster Admin Certificate

Before you can view the Service Fabric Explorer you must install the Cluster Admin Certificate:

1. Navigate to the Configuration folder in the **Deployment** folder and copy the **IC3ClusterAdmin.pfx** file to the machine you want to use to view the status of your Service Fabric.
2. Double-click the PFX file and select **Current User**. Click **Next**.
3. The path to the certificate is populated automatically as you've run the certificate. Click **Next**.
4. Enter the password for the PMC Cluster Admin certificate and click **Next**.
5. Select **Place all certificates in the following store** and click **Browse**.
6. Leave the default of **Personal** and click **OK**.
7. Click **Next** and then **Finish** to complete the certificate installation.

View Service Fabric Explorer

Use the following URL to view to the status of your Service Fabric Cluster. Replace **<Your IP>** with the IP address of the first node in your PMC cluster.

```
https://<Your PMC Portal IP>:19080
```

You need to choose your PMC Cluster Administration certificate to authenticate yourself with when you browse to the URL.

Set up a Load Balancer

> ***Note:*** *The Load Balancer must be installed after you have installed PMC, not before.*

You need to install and configure a load balancer to balance the load across the cluster before you continue. You can choose which load balancer you use to do this. There are four rules that need to be created:

Rule One

Traffic coming in from your endpoints on port 443 needs to be balanced across all PMC cluster nodes.

Rule Two

Traffic coming in from trusted admin IPs and the PMC cluster on port 8443 needs to be balanced across all PMC cluster nodes.

Sticky sessions / session affinity are required for port 8443.

Rule Three

Traffic coming in from trusted admin IPs on port 9443 should **not** be balanced across the PMC cluster. It must be directed at the node where the PMC portal is deployed.

Rule Four

Traffic coming in from trusted admin IPs on 19080 (Service Fabric Explorer) and 19000 (Service Fabric interface using PowerShell) needs to be balanced across your PMC cluster nodes.

Timeout Settings

You need to check the timeout settings on the load balancer to ensure that they are set to five minutes as this is the timeout setting applied to the Reporting Gateway service for PMC. If you do not adjust the timeout settings in your load balancer, where present, reports in PMC may time out unexpectedly.

SSL Certificate

Some load balancers may require your SSL certificate to be uploaded or installed. See the specific documentation for your load balancer for these requirements. If your load balancer requires the SSL certificate you must not terminate SSL at the load balancer.

Log into PMC

You need to be able to resolve the DNS before you can log into PMC. If you are using a public DNS that has not yet been created, you will need to create manual entries in the host files of the machines that need to communicate, such as the cluster nodes (including where the portal is installed).

To log into PMC:

Navigate to the Server URL of PMC. It is the DNS of your SSL certificate with the PMC port number of **9443** appended to it.

For more information, please see "Finish Tab" on page 32.

You can also get the Server URL from your web.config file.

1. Navigate to the web.config file. The default location for the web.config file on the portal node is **c:\inetpub\wwwroot\iC3**.
2. Open the **web.config** file with a text editor and locate the following entry:

```
<add key="Avecto.IC3.Authentication.WSFederation.Realm" value="https://test.ic3.avecto.com:9443" />
```

This is the Server URL you need to log into PMC.

3. Enter the user name and password that was either manually set up for you by your PMC management database creator or that you inserted through the PMC deployment wizard on the **Authentication Tab**.

For more information, please see "Authentication Tab" on page 27.

4. When you first log in you are asked to confirm the time and date settings. You can change these if required.

You can now configure the connection to the Privilege Management MMC PMC snap-in.

For more information, please see "Configure PMC to Connect to the Policy Editor" on page 38.

For information on extracting the PMC Portal logs, adapter logs, and node logs, please See "Logs" on page 45 .

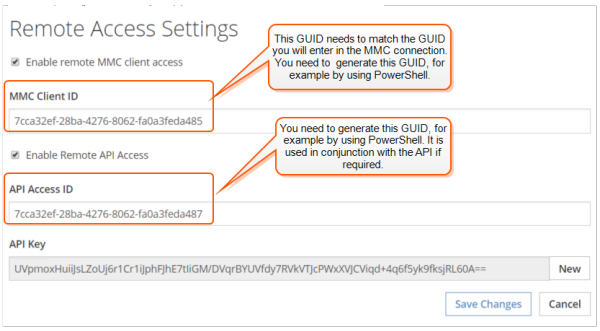
Configure PMC to Connect to the Policy Editor

You need to configure PMC to allow the Privilege Management MMC snap-in to communicate with the PMC services.

1. Click **Administration** > **Settings** > **Remote Access Settings** from the top menu.
2. Check the **Enable remote MMC client access** box. You need to generate a new GUID and enter it here. You need to use the same GUID when you configure the MMC. This is the **MMC Client ID** in the MMC. There are many ways to generate a GUID, for example,c you can use a PowerShell cmdlet:

```
new-guid
```

3. You need to generate a new GUID for the **API Access ID**. Check the **Enable Remove API Access** box. Paste the new GUID into the **API Access ID** field. The **API Key** is automatically generated. You can click **New** to regenerate the API key click if required. This GUID is required if you want to use the PowerShell API.



Once you have configured PMC you also need to configure the Privilege Management MMC PMC snap-in to communicate with it.

For more information, please see "Configure the Privilege Management MMC PMC snap-in" on page 39.

Configure the Privilege Management MMC PMC snap-in

You need to install and configure the Privilege Management MMC on the machine you will use to administrate PMC policy.

For more information, please see "Set up a Load Balancer" on page 36.

The installation packages differ based on your operating system:

- For 32-bit (x86) systems run **PrivilegeManagementPolicyEditor_x86.exe**
- For 64-bit (x64) systems run **PrivilegeManagementPolicyEditor_x64.exe**

For compatible versions, please see the Release Notes, at https://www.beyondtrust.com/support/changelog.

Add and Configure the Privilege ManagementPMC Snap-in

You need to use the Privilege Management MMC PMC snap-in for the Microsoft Management Console (MMC) to manage policy for endpoints managed by PMC.

To load the Privilege ManagementPMC snap-in for the MMC:

1. Run **mmc.exe** from the **Start** menu.
2. **File** > **Add/Remove Snap-in** and select **Privilege Management Settings (PMC)**. Click **Add**.
3. Select the **Privilege Management** Settings (PMC) node and click PMC Connection on the left-hand side under **Settings**.

***Note:** Ensure you install the **Privilege Management Settings (PMC** snap-in, rather than just **Privilege Management Settings**.*

The next step is to configure the MMC to connect to PMC.

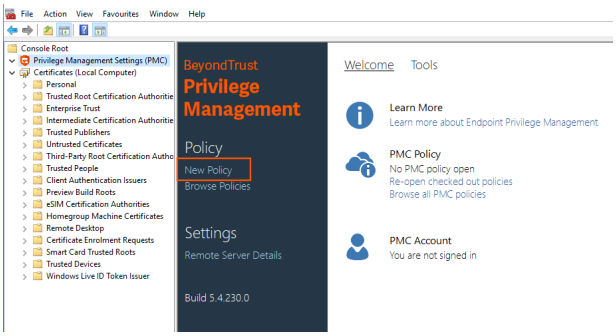
Setting	What to enter
Connection	
Server URL	This is the URL for PMC with **8443** in the **Port** field. This is shown on the **Finish** tab of the deployment wizard. For more information, please see "Finish Tab" on page 32.
Tenant ID	This is the same TenantID GUID you provided to the installation script.
Authorization Provider	
URL	This is the URL for PMC with **:8443/oauth** appended to it. For more information, please see "Finish Tab" on page 32.

Setting	What to enter
Identification	
MMC Client ID	This needs to be the same GUID that you generated and used in the PMC connection settings called **Application ID**. For more information, please see "Configure PMC to Connect to the Policy Editor" on page 38. You can generate this GUID in many ways, for example, by using the PowerShell cmdlet `new-guid`.
Client Return URI	Enter **http://defendpoint-mmc.com**. This string does not resolve but needs to be as stated.
Amend token resource ID	Check this box. This string needs to be **https://api.ic3.avecto.com**. This string does not resolve but needs to be as stated.

Confirm Connection to PMC

You should now confirm that you can access PMC from the PMC Privilege Management management console snap-in.

1. Click **New Policy** in the Privilege Management MMC snap-in.



2. Enter your credentials for PMC when prompted and click **Sign in**.
3. If you clicked **Create** you are prompted to enter a name for your policy. If you clicked **PMC Policies**, you are taken to a list of policies in PMC.

If you receive an error connecting to PMC, ensure you have entered the correct options in both PMC and the PMC Privilege Management MMC snap-in.

Configure Endpoints

You need to install Privilege Management on the target operating system as well as the PMC adapter.

IMPORTANT!

Install the Privilege Management client first and then the adapter. Failure to do so in this order results in specific events not being generated which PMC needs. Should you happen to install the client and the adapter out of order, you can restart the adapter service to force it to detect the client.

For more information on the management of your endpoints using PMC, please see the PMC Administration Guide, at https://www.beyondtrust.com/docs/privilege-management/windows.htm.

***Note:** The adapters poll every 60 minutes by default. An additional delay is applied based on the CPU load of the node that the adapter is connected to. The minimum supported adapter poll time is 5 minutes.*

Install the Windows Adapter for PMC

IMPORTANT!

As of version 2.4, all releases of Privilege Management are signed only with a SHA-256 code signing certificate. Previous versions were dual signed with SHA-1 and SHA-256 certificates. The decision to drop SHA-1 certificates was made to avoid weaknesses in the SHA-1 algorithm and to align to industry security standards. For more information, please see 2019 SHA-2 Code Signing Support requirement for Windows and WSUS at https://support.microsoft.com/en-gb/help/4472027/2019-sha-2-code-signing-support-requirement-for-windows-and-wsus.

If you intend to deploy Privilege Management version 2.4 or later to Windows 7 or Windows Server 2008 R2 machines, you must ensure the following KBs are installed prior to installation of this product:

- *KB4490628*
- *KB4474419*

We strongly recommend you keep your systems up to date with the latest Windows security updates.

The PMC client adapter installers can be found in the **AdapterInstallers** folder of the PMC deployment. You need to use the Windows Command Prompt to install the Windows PMC Adapter.

You can install and automatically authorize Windows machines to connect to PMC using the command line.

***Note:** You must uninstall any existing PMC Windows Adapter prior to installing a new Windows adapter for PMC.*

There are five parameters for the PMC Adapter, one of which is optional:

- **TenantID**: For Windows Directory and LDAPS, this GUID is generated for you by the deployment tool and you should already have a note of it.

For more information on getting this GUID for Microsoft Azure authentication, please see "Create the Azure AD Tenant" on page 15.

- **InstallationID**: You get this from the PMC portal. Click **Administration** > **Agent Installation**. Copy the **Installation ID** for this script.
- **InstallationKey**: You get this from the PMC portal. Click **Administration** > **Agent Installation**. Copy the **Installation Key** for this script.
- **ServerURL**: This is the URL for your PMC portal.

Note: *There is no port number or slash character at the end of this URL.*

- **GroupID** (Optional): If supplied, this will auto-authorize the endpoint and assign it to the specified group. If that group doesn't exist, the computer will remain in the pending state. You get this from PMC. Click the group you want to use. The **Group ID** is shown in the **Summary** page. Copy the **Group ID** for this script.

To install adapters:

Note: *Include the **GroupID** to automatically group and authorize the endpoint.*

1. Navigate to the location of the Adapter installer. By default, this is the **AdapterInstallers** folder.
2. Enter the command line with the required attributes and press enter. The Adapter installer launches. Proceed through the installation wizard as required.

Below is an example command line. The line breaks must be removed before you run the script.

```
msiexec.exe /i "PrivilegeManagementConsoleAdapter_x64.msi"
TENANTID="<TenantID_GUID>"
INSTALLATIONID="<InstallationID>"
INSTALLATIONKEY="<InstallationKey>"
SERVICEURI="<PMC URL>"
GROUPID="<PMC GroupID GUID>"
```

Add the following argument if you don't want the Adapter service to start automatically. This option is useful when Privilege Management and the PMC adapter are being installed to an image that will be reused to create many individual computers. If the adapter is not disabled in this scenario, the PMC adapter will immediately join the PMC instance indicated.

```
SERVICE_STARTUP_TYPE=Disabled
```

You can start the **IC3Adapter** service manually later in the Services.

Example

```
msiexec.exe /i "PrivilegeManagementConsoleAdapter_x64.msi" TENANTID="6b75f647-d3y7-4391-9278-
002af221cc3f" INSTALLATIONID="08A1CD8F-FAE4-479F-81B4-00751A55EEB8"
INSTALLATIONKEY="ABCDEFGHIJKLMNO" SERVICEURI="https://test.pmc.avecto.com" GROUPID="fcc4022e-12fa-
4246-87w8-0de9a1483a68"
SERVICE_STARTUP_TYPE=Disabled
```

Configure the Windows PMC Adapter

When the PMC Adapter communicates with the PMC Portal, it uses HTTPS. If there is a proxy in place that this communication goes through, it must be configured for the PMC Adapter user which is separate to the logged on user account.

The endpoint needs to be configured to use proxy settings for the whole machine rather than the individual user. The following registry key needs to be edited to make this change:

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings]

The Data value must read **0**. This specifies the whole machine (**1** specifies per user).

Name	Type	Data
ProxySettingsPerUser	REG_DWORD	0

Ensure the iC3Adapter User Has the "User Can Log on as a Service" Right

When you install the PMC Adapter it creates a user called **iC3Adapter** as part of the installation process. The **iC3Adapter** user is granted the rights to **Log on as a Service** by the installation process. If you have a Group Policy in place that revokes this permission you need to ensure the **iC3Adapter** user is excluded as it needs the **Log on as a Service** right.

For more information, please see Add the Log on as a service Right to an Account at https://technet.microsoft.com/en-gb/library/cc794944(v=ws.10).aspx.

The computers with Privilege Management and the Privilege Management PMC adapter installed with the Installation ID and Installation Key will now appear in the **Computers** grid in PMC.

Install the Mac Adapter for PMC

The PMC client adapter installers can be found in the **AdapterInstallers** folder of the PMC deployment. You need to use the Terminal to install the Mac PMC Adapter.

You can install and automatically authorize Mac machines to connect to PMC using the command line.

Note: *You must uninstall any existing PMC Mac Adapter prior to installing a new Mac adapter for PMC.*

There are six parameters, two of which are optional:

- **TenantID**

For more information on getting this GUID for Microsoft Azure authentication, please see "Create the Azure AD Tenant" on page 15.

- **InstallationID**. You get this from PMC. Click **Administration** > **Agent Installation**. Copy the Installation ID for this script.
- **InstallationKey**. You get this from PMC. Click **Administration** > **Agent Installation**. Copy the Installation Key for this script.
- **ServerURI**. This is the URL for your PMC portal.

Note: *There is no slash on the end of this URL. A port number is not required.*

- **GroupID** (Optional). If supplied, this will auto authorize the endpoint and assign it to the specified group. If that group doesn't exist the computer will remain in the pending state. You obtain this from PMC. Click the Group you want to use. The **Group ID** is shown in the **Summary** page. Copy the **Group ID** for this script.
- **Cacertificateid** (Optional). If you are using a Root CA certificate that is trusted by a global provider, you do not need to add this parameter. If it's not, the Root CA certificate must be added to the **System** keychain (not Login). The Root CA certificate must also be set to **Trusted** in the **System** keychain. The SHA-1 thumbprint of the Root CA certificate is the required value for the field.

To install adapters:

Note: *Include the **GroupID** to automatically group and authorize the endpoint.*

1. Navigate to the location of the Adapter installer. By default, this is the **AdapterInstallers** folder.
2. Mount the DMG and run the following command line from the Terminal. Once the Adapter installer launches, proceed through the installation wizard as required.

Below is an example command line. The line breaks must be removed before you run the script.

```
sudo /Volumes/PrivilegeManagementConsoleAdapter/install.sh tenantid="750e85d1-c851-4d56-8c76-
b9566250cf1d" installationid="95a10760-2b96-4a0e-ab65-ed7a5e8f1649"
installationkey="VGhpcyBzZWNyZXQgaTYzIGJlZW4gQmFzZTY0IGVuY29kZWQ="
serviceuri="https://test.ic3.avecto.com" groupid="fcc4022e-12fa-4246-87w8-0de9a1483a68"
cacertificateid="b36b7345ff30aa7fb15fcd985fe2989c3e11aba7"
```

The computers with Privilege Management for Mac client and the PMC adapter installed with the Installation ID and Installation Key will now appear in the **Computers** grid in PMC.

Logs

There are four locations where you can extract logs:

These logs are useful for troubleshooting and may be required by BeyondTrust Technical Support in some circumstances.

Deployment Logs

All the events from the PowerShell script during setup and deployment are logged in a folder in this directory:

```
C:\Users\<yourusername>\AppData\Roaming\Avecto\AvectoIC3DeploymentWizard
```

AppData is a hidden folder. You can access it by viewing hidden items in Windows Explorer or typing in `%appdata%` into Windows Explorer.

The **BeyondTrust PMC Deployment Wizard.ps1** script contains the setup and deployment logs including the Windows Directory and LDAPS GUID that was generated.

Portal Logs

The log file on the node with the portal is in the following directory if you kept the default installation path in the PMC deployment wizard: **C:\inetpub\wwwroot\iC3\Logs**.

This file is appended to at run-time so you need to close it to refresh it.

Cluster Node Service Logs

You can get the logs from each node in your PMC cluster from the deployment machine. There are two methods of achieving this:

Specific Node by URL

To obtain the logs from a specific node in your cluster:

1. Copy and install the PMC Cluster Admin Certificate (*.pfx) portion to the machine you are downloading the logs to.
2. Log into the node itself or a machine that can communicate with the node and open a browser.
3. Navigate to the following string where **IPADDRESS** is the IP of the node that you want the logs from:

https://IPADDRESS:8443/node-diagnostics/v1/logs

4. This will trigger the download of a zip file which contains the logs for that node. This zip file can be shared with BeyondTrust Technical Support if required for troubleshooting.

All Nodes Using PowerShell

You need to install the PMC Cluster Admin certificate prior to running the PowerShell script:

1. Copy and install the PMC Cluster Admin certificate (*.pfx) portion to the machine you are downloading the node logs to.
2. Double-click the PMC Cluster Admin certificate and click **Install Certificate**.
3. Select **Current User** and click **Next**.
4. Click **Next** to confirm that you're installing the certificate.
5. Enter the password for the PMC Cluster Admin Certificate and click **Next**.
6. Select **Place all certificates in the following store** and click **Browse**.
7. Select the default of **Personal** and click **OK** and **Next**.
8. Click **Finish** to complete the certificate installation.

You may need to modify the hosts file so it can resolve the DNS settings of the nodes that you are connecting to.

To download the logs from all your nodes:

1. Navigate to the PowerShell folder in the PMC deployment package.
2. Copy the PowerShell file **NodeDiagnosticsLogsDownload** to the machine you are downloading the logs to.
3. Run PowerShell as an administrator. The script requires the following parameters:
    - Cluster Admin Thumbprint. Press **Enter** to move on to the next parameter.
    - An array of IPs or Domain Names of the Node machines. Press **Enter** after each IP address. Press **Enter** twice to finish entering IP addresses and move on to the final parameter.
    - Download location for the files. This is a path on the local drive of the machine you are downloading the logs to, for example, **C:\pmclogs**.

> For information on how to obtain the thumbprint of the certificate, please see https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/how-to-retrieve-the-thumbprint-of-a-certificate.

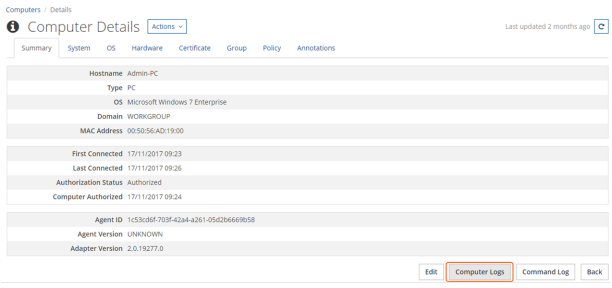
4. Press **Enter** to run the PowerShell script and download the files to the chosen location.

Adapter Logs

You can retrieve the most recent adapter log from PMC if you need to send them to BeyondTrust Technical Support for analysis:

To retrieve logs:

1. Click the **Computers** tile in PMC.
2. Select the computer you want to retrieve the logs for.
3. On the **Computer Details** tab click **Computer Logs**:



Upgrade On-Premise Deployments

There are several steps you need to go through for the On Premise deployments.

IMPORTANT!

You must upgrade your reporting database to 5.5 in order to use PMC 2.4.

Upgrade the Management Database

Prior to upgrading your application, you must ensure your management database is up-to-date as this process is not managed with the upgrade scripts.

You need to upgrade the **Avecto.IC3.Database.Management** database before you upgrade the application. Please review the Release Notes to see if there are any changes to the database. If there are no changes to the database, you can proceed to the application.

For more information, please see "Upgrade the Application" on page 48.

Upgrade the Database

1. Connect to your database using SQL Server Management Studio.
2. Expand the **Databases** node under Object Explorer.
3. After you successfully connect, expand the **Databases** node under **Object Explorer**, right-click on the **Avecto.IC3.Database.Management** database and click **New Query**.
4. Select **File** > **Open** > **File** and navigate to the **SupportFiles** folder and locate **SQL.zip**. for the version you are upgrading to.
5. Unzip **SQL.zip** and locate the **Avecto.IC3.Database.Management.sql** script. This contains all the database migrations required to perform an upgrade.
6. Run the script by pressing **F5** or click **Execute**.

Copy and execute the following query to confirm that your upgrade was successful:

```
Select Top (1000) [MigrationID]
   ,[ContextKey]
   ,[Model]
   ,[ProductVersion]
FROM [dbo].[__MigrationHistory]
```

Ensure one of the entries is **AdapterPollingTimeInMinutes**. The **SystemParameter** table should also be present.

Upgrade the Application

Update Service Fabric Runtime

> For more information, please see https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-cluster-upgrade-windows-server.

```
Connect-ServiceFabricCluster
-ConnectionEndpoint $ClusterEndpoint `
-KeepAliveIntervalInSec 1000 `
-X509Credential `
-ServerCertThumbprint $ServerCertThumbprint `
-FindType FindByThumbprint `
-FindValue $ClusterAdminThumbprint `
-StoreLocation CurrentUser `
-StoreName My
```

2. Run **PowerShell.exe** as an administrator, paste the following code in, and press **Return**. You must provide the following parameters:
    - **$ClusterEndpoint**: This is your PMC DNS with the port number **19000** appended to it. For example, **$mydns$:19000**
    - **$ServerCertThumbprint**: This is the thumbprint of your SSL certificate.
    - **$ClusterAdminThumbprint**: This is the thumbprint of your **IC3ClusterAdmin** certificate.
3. Type **Get-ServiceFabricClusterUpgrade** into PowerShell to check the current Service Fabric Runtime version. Make a note of the **TargetCodeVersion**.
4. Type the following into PowerShell to copy the Service Fabric Cluster package into the cluster image store. The **-Code** and **-CodePackagePath** need to point to the *.cab Service Fabric Runtime that you downloaded earlier.

```
Copy-ServiceFabricClusterPackage -Code -CodePackagePath "<name of the .cab file including the path to it>" -ImageStoreConnectionString "fabric:ImageStore"
```

5. Start a cluster upgrade to the version that you just copied to the image store. The code version number can be found at the end of the download.

```
Start-ServiceFabricClusterUpgrade -Code -CodePackageVersion "<code version #>" -Monitored -FailureAction Rollback
```

6. Monitor the upgrade to check it has completed successfully. You can view the status of the upgrade under **UpgradeDomainStatus** when you run the below command and the **TargetCodeVersion** will be updated to the version that you upgraded to.

```
Get-ServiceFabricClusterUpgrade
```

Enable WinRM with SSL on the Node Hosting the Portal

1. Connect to your machine hosting the portal and copy the **Enable-WinRMWithSSL.ps1** script from the build folder to the Node Hosting the desktop.
2. Run PowerShell as an administrator and navigate to the location of **Enable-WinRMWithSSL.ps1**
3. Type **.\Enable-WinRMWithSSL -SubjectName $NodeHostingPortal -ForceNewSSLCert**.

Perform Upgrade on the Deployment Machine

You need the **On Prem** folder for the version of PMC that you are upgrading to.

1. Copy the **Upgrades** folder from the build you want to upgrade to onto the deployment machine. This contains all the files needed to prepare and upgrade your environment.

> ***Note:*** *If you need to change any values in the configuration (for example, the location of the portal and connection strings, you must provide them as an argument to the* ***PrepUpgradeConfig.ps1*** *script before you run it. For more information, please see .*

2. You are now ready to run the **PrepUpgradeConfig.ps1** script. If you changed the location of the portal from the default, you need to supply it as an optional argument. For example, in an elevated PowerShell window, type `PrepUpgradeConfig.ps1 -PortalWebsiteVmLocation "C:\MyFolder\iC3"`. When you press **Return** you will be prompted for the mandatory parameters listed below. If you did not change the location and do not need to change any other parameters, type `PrepUpgradeConfig.ps1` and press **Return**.

    - **ClusterEndpoint**: Your DNS with **:19000** applied at the end. For example, **pmctest.example.com:19000** (no **https://** needed at the start).
    - **ClusterAdminThumbprint**: The thumbprint output during initial deployment for the PMC Cluster Admin certificate.
    - **ServerCertThumbprint**: The thumbprint of your SSL certificate.
    - **PortalVmAdminUsername**: The administrator user name for the node hosting the PMC portal.
    - **PortalVmPassword**: The password for the node hosting the PMC portal.
    - **PortalVmIpAddress**: The IP address of the node hosting the PMC portal.
    - **ParametersConfigFilePath**: The full file path of the parameter config file in the **Upgrades** folder. For example: **C:\Users\myuser\Desktop\Upgrades\Production.3node.xml**
    - **WebConfigFilePath**: The full file path of the web config file in the **Upgrades** folder. For example: **C:\Users\myuser\Desktop\Upgrades\Web.Production.config**

    When this script is executed, a text file containing all of the original values is output to the location in which the script is run. This must be saved to a secure location in case these values are needed. In the event that they are needed, the required value must be copied from this text file into the config file.

3. Copy the **Package.zip** folder from the **SupportFiles** folder (the version you are upgrading to) to your deployment box and unzip it.
4. Connect to the Deployment Machine (ensure you have the Cluster Administration *.pfx certificate portion installed on the machine before continuing).
5. Open Powershell as admin and run the **UpdateServiceFabricAppSetting.ps1** (in the **Upgrades** folder) script with the following parameters:

- **ClusterAddress**: The DNS Name of your cluster postfixed with **:19000**. For example, **PMCcert.PMC:19000**.
- **ServerCertThumbprint**: The thumbprint of the **ClusterAdminCertificate**.
- **ClusterAdminThumbprint**: The thumbprint of the **ClusterAdminCertificate** (same as **ServerCertThumbprint**).
- **UpdateConfigParameters**: The event pump service **Avecto.IC3.Fabric.EndpointEventPump.EventProcessingDisabled** set to **true**

For example:

```
.\UpdateServiceFabricAppSetting.ps1 -ClusterAddress "pmc.domain.com:19000" -ServerCertThumbprint
"54761d496fe75fd4fe81a488fa709e4e79613385" -ClusterAdminThumbprint
"54761d496fe75fd4fe81a488fa709e4e79613385 " -UpdateConfigParameters @
{"Avecto.IC3.Fabric.EndpointEventPump.EventProcessingDisabled" = "true";}
```

6. The update will apply to each node one at a time. You can check update status through Service Fabric Manager.
7. Once the update is complete, run the following command in PowerShell to check if the setting is applied:

   ```
   Get-ServiceFabricApplication -ApplicationName fabric:/IC3.Fabric
   ```

   This will output the application configuration:

   The Avecto.IC3.Fabric.EndpointEventPump.EventProcessingDisabled parameter should be set to **true**.

8. Through SSMS, pause the SQL Agent job / Service broker queue, and then make sure the **CopyFromStaging** job has finished running.
9. From your PowerShell instance, navigate to the **UpgradeApp.ps1** script in the **Upgrades** folder and provide the following parameters:
   - **PackagePath**: The path to the unzipped Package folder you copied over. For example: **C:\Users\myuser\Desktop\Package**
   - **AppParamsPath**: The location of the **Production.3Node.xml** file in the **Upgrades** folder. For example: **C:\Users\myuser\Desktop\Upgrades\Production.3node.xml**
   - **ClusterAddress**: Your DNS with **:19000** applied at the end, for example, **pmctest.example.com:19000** (no **https://** needed at the start).
   - **ClusterAdminThumbprint**: The thumbprint output during the deployment for the PMC Cluster Admin certificate.
   - **ServerCertThumbprint**: The thumbprint of your SSL certificate.
10. The script will run and begin the upgrade process. To check the progress, navigate to ServiceFabric explorer, expand the cluster, and select **Applications** from the tree view. In the right-hand work pane, you will see **Upgrades in progress** text. Click on this to see the progress for each node. It shows the current version and the target version you are upgrading to. During the upgrade, ServiceFabric will display several warnings as each domain is taken down. Upon completion of an upgrade, these warnings should be removed. During the upgrade, the policy on endpoints is still be applied and the policy will remain functional.

Check for Successful Upgrade

You can check if your upgrade was successful by navigating to **Cluster** > **Applications** in Service Fabric. The application shown on the right should match the version you upgraded to.

Upgrade Issues

If an upgrade runs and fails, it will automatically rollback once it detects errors in Service Fabric. After a period of 30 minutes, these errors should be removed and another attempt at an upgrade can begin.

Error on subsequent upgrade after failed upgrade

When the UpgradeApp script is run again, there may be an error in PowerShell (see below). However, the script will continue to run and begin the upgrade process and (assuming all parameters are correct) finish successfully.

If you receive an error that states *Application type and version already exists at <path>*, then the error is due to the previous failed run leaving the application type and version provisioned in Service Fabric. Running the script again will clash as it is the same version. The script itself will continue and overwrite this version.

To avoid seeing this error, you can navigate to Service Fabric explorer and manually unprovision the new version of the application before re-running the script. However, you cannot roll back to previous versions if you unprovision the application. You can do this by navigating to the **Cluster** > **Applications** > **IC3.FabricType** node and click **Unprovision**.

Upgrade the Portal

Lastly you need to upgrade the portal. Please follow the steps below.

1. Log on to the machine where the portal is hosted.
2. Create a new folder under **C:\inetpub\wwwroot** named with the new version number.
3. Copy the contents of the new portal package into the folder you just created.
4. Rename the **Web.production.config** file that was created previously by the **PrepUpgradeConfig.ps1** script to **web.config** and copy into the new portal folder with the version you just created. This will overwrite the existing one.
5. Open Internet Information Services (IIS) and navigate to **Sites** > **iC3Portal**.
6. Under **Basic Settings**, select the new physical path you have created and click **OK**.

Upgrade Privilege Management Reporting

IMPORTANT!

You must upgrade your reporting database to 5.5 in order to use PMC 2.4.

Prerequisites

Run the out of box script from the install media under **\Upgrades**.

1. Pause event pump by running powershell scripts, with the `-ForceRestart` option.
2. Once ServiceFabric shows upgrade complete, run the following to show if the update was applied.

   ```
   Get-ServiceFabricApplication -ApplicationName fabric:/IC3.Fabric
   ```

3. Disable the **PGInsertData** SQL Agent job / Service broker queue.
4. Wait for any **CopyFromStaging** job to finish.
5. Upgrade the reporting database.
6. Turn back on Service Fabric components.

Upgrade Steps

To upgrade a Privilege Management database using SQL scripts:

1. The SQL scripts are provided as part of the Privilege Management installers, located in the Privilege Management Reporting release folder, which can be found in the BeyondTrust portal. Alternatively, you can contact BeyondTrust Technical Support.

> ***Note:*** *There is a README file provided in this directory to assist you.*

2. Run the following SQL query to return the version of the database. For example, **4.3.16**:

```
select * from DatabaseVersion
```

> ***Note:*** *This SQL will work for Privilege Management Reporting databases 4.5 and later.*

3. Execute the upgrade script where the name is the next version number and carry on applying these until the desired version is reached.

For example, if your current database version is **4.3.16** and you want to upgrade to version **5.0.0**, run the following scripts in order:

- **Script_4.5.0_Updates.sql**
- **Script_5.0.0_Updates.sql**

Please check the SQL log for any errors and contact BeyondTrust Technical Support if necessary.

4. Run and execute the following SQL query against the reporting database to return the versions in the InstallShield table:

```
SELECT * FROM [dbo].[InstallShield]
```

5. Open the InstallShield query file. This is available in the **SQL** folder, and is a Privilege Management Reporting artifact.
6. Copy the relevant **INSERT** lines from this query file that are not included in the database table. For example, if the upgrade is from 5.1.1 to 5.4, you need to copy these lines:

```
INSERT [dbo].[InstallShield] ([ISSchema]) VALUES (N'5.3.0          ')
INSERT [dbo].[InstallShield] ([ISSchema]) VALUES (N'5.4.0          ')
```

7. Copy these into a query against the Reporting Database and execute it.
8. View the InstallShield table by running the query below. These values will be added.

```
SELECT * FROM [dbo].[InstallShield]
```

Turn on Service Fabric Components

You need to turn back on the Service Fabric settings for incoming events.

1. Connect to the Deployment Machine (ensure you have the Cluster Administration *.pfx certificate portion installed on the machine before continuing).
2. Open Powershell as admin and run the **UpdateServiceFabricAppSetting.ps1** (in the **Upgrades** folder) script with the following parameters:
   - **ClusterAddress**: The DNS Name of your cluster postfixed with **:19000**. For example, **PMCcert.PMC:19000**.
   - **ServerCertThumbprint**: The thumbprint of the **ClusterAdminCertificate**.
   - **ClusterAdminThumbprint**: The thumbprint of the **ClusterAdminCertificate** (same as **ServerCertThumbprint**).
   - **UpdateConfigParameters**: The event pump service **Avecto.IC3.Fabric.EndpointEventPump.EventProcessingDisabled** set to true

   For example:

   ```
   .\UpdateServiceFabricAppSetting.ps1 -ClusterAddress "pmc.domain.com:19000" -ServerCertThumbprint
   "54761d496fe75fd4fe81a488fa709e4e79613385" -ClusterAdminThumbprint
   "54761d496fe75fd4fe81a488fa709e4e79613385 " -UpdateConfigParameters @
   {"Avecto.IC3.Fabric.EndpointEventPump.EventProcessingDisabled" = "false";}
   ```
3. The update will apply to each node one at a time. You can check update status through Service Fabric Manager.
4. Once the update is complete, run the following command in PowerShell to check if the setting is applied:

   ```
   Get-ServiceFabricApplication -ApplicationName fabric:/IC3.Fabric
   ```

   This will output the application configuration:

   The **Avecto.IC3.Fabric.EndpointEventPump.EventProcessingDisabled** parameter should be set to **false**.
5. Through SSMS, start the SQL Agent job /Service broker queue.
6. Check the Reporting in PMC to confirm events are flowing through to the database.

Change Application Parameters Before Upgrade

You can use the script to update values in both the **Production.3Node.xml** or the **Web.config** file that are provided as part of the upgrade in the **Upgrade** folder, if required. You need to use the script to do this rather than edit the files directly, otherwise any changes will be overwritten by the script.

1. Run PowerShell as an administrator and navigate to the location of the **PrepUpgradeConfig.ps1** script in the **Upgrades** folder.
2. To change values in the **Production.3Node.xml** file, use the following command:

```
PrepUpgradeConfig.ps1 -UpdateApplicationParameters @{"String.Name.One" = "argument";
"String.Name.Two" = "argument";}
```

For example:

```
PrepUpgradeConfig.ps1 -UpdateApplicationParameters @{"Avecto.IC3.Authentication.Domain"
"https://login.microsoftonline.com/53c8dbb9-fb9b-467a-8930-f23d8e0199c9";}
```

3. To change values in the **Web.config** file, use the following command:

```
 PrepUpgradeConfig.ps1 -UpdateWebConfigParameters @{"String.Name.One" = "argument}
```

For example:

```
 PrepUpgradeConfig.ps1 -UpdateWebConfigParameters @{"Avecto.IC3.Log.Seq.Host" =
"https://localhost:5391"}
```

Rotate your SSL Certificates

Prior to your certificates expiring, you need to rotate them. This section details how to achieve this with on-premises deployments.

To rotate your SSL certificate, please first copy it to your deployment machine.

Install the New Certificates on the Nodes

1. On the deployment machine, run **PowerShell.exe** with admin privileges.
2. Navigate to the following folder in the deployment kit **\Upgrades\SSLCertRotation\OnPrem** in PowerShell and run **InstallCerts.ps1**. You will be asked for the following parameters:
    - **newSslCertPath**: This is the absolute path to the new SSL certificate *.pfx portion on the deployment machine.
    - **newSslCertPassword**: This is the password of the new SSL certificate.
    - **newSslThumbprint**: This is the thumbprint of the new SSL certificate.
    - **adminUsername**: This is the user name required to access to each node. It is the same as the username for deployment. Please include domain if relevant.
    - **adminPassword**: This is the password required to access to each node using the **adminUsername** account.
    - **domainBasedInstall**: Choose **Y** or **N**, depending on whether or not your deployment is domain-joined.
    - **nodes**: You will be prompted for the each of the nodes where the certificate needs to be installed. If your deployment is domain-joined then you need to provide the computer names, otherwise you will need to provide IP address. If this is a three node deployment please press **Enter** to proceed past the remaining node parameters.

IMPORTANT!

The nodes and the deployment machine must all be domain joined, or not at all. You cannot have a mix of non-domain joined and domain joined machines or the scripts will fail.

Configure Internet Information Services (IIS)

1. Log into your machine hosting the portal, and navigate to **Internet Information Services** (IIS).
2. Locate the PMC Portal site, right-click on it and select **Bindings**.
3. Select the single binding for port 9443 and click **Edit**.
4. Select the new SSL certificate. You can identify it from the furthest expiration date and click **OK**.
5. Click **OK** to confirm the new binding.

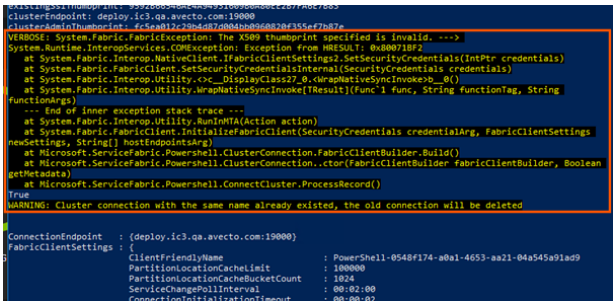
Upgrade the Service Fabric Cluster

Note: *This process takes approximately 20 minutes.*

1. On the deployment machine, run **PowerShell.exe** with admin privileges.
2. Navigate to the following folder in the deployment kit **\Upgrades\SSLCertRotation\OnPrem** in PowerShell and run **UpdateClusterConfig.ps1**. You will be asked for the following parameters:

- **newSslThumbprint**: This is the thumbprint of the new SSL certificate.
- **clusterConfigPath**: This defaults to **C:\ProgramData\SF\ClusterConfig.json** on node 0 of the ServiceFabric cluster. If the **clusterConfigPath** is the default, this can be left blank.
- **clusterAddress**: This is the address of the Service Fabric cluster, for example, **dns:19000**.
- **adminUsername**: This is the user name required to access to each node. It is the same as the username for deployment. Please include domain if relevant.
- **adminPassword**: This is the password required to access to each node using the **adminUsername** account.
- **node0ComputerName**: This is the name of node 0 for domain-joined deployments, or the IP address of node 0 if your deployment is non-domain joined.
- **domainJoinedInstall**: Choose **Y** or **N**, depending on whether or not your deployment is domain-joined.

3. The script will exit when the upgrade is started. You can check the upgrade process by running **CheckClusterUpgradeProgress.ps1.** If this script shows a *X509 thumbprint specified is invalid* warning as depicted in the screenshot, you can disregard it. This is expected when rotating the SSL certificate.



4. Once the certificate expiry warnings have gone from each node you can see if the upgrade was successful. The nodes should appear without any warnings once the upgrade has completed.

Make the PMC Application Configuration Changes

1. On the deployment machine, run **PowerShell.exe** with admin privileges.
2. The setting for the SSL Thumpbprint has to be updated using this script first, instead of inputting it as a script parameter. You can also use this method to allow multiple configuration settings to be updated.

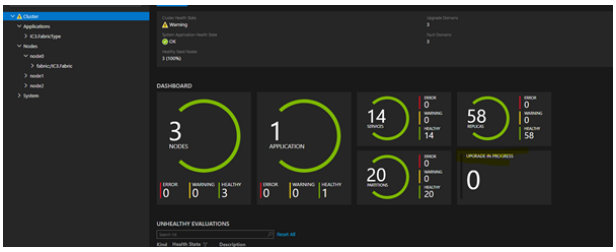
    - Example:

```
.\UpdateServiceFabricAppSetting.ps1 -UpdateConfigParameters @
{"Avecto.IC3.Certificates.SSL.Thumbprint" = "newthumbprint"}.
```

3. Navigate to the **\Upgrades** folder in the deployment kit in PowerShell and run **UpdateServiceFabricAppSetting.ps1**. You will be asked for the following parameters:

    - **clusterAddress**: This is the address of the Service Fabric cluster, for example, **dns:19000**.
    - **ServerCertThumbprint**: This is the thumbprint of the new SSL certificate.
    - **ClusterAdminThumbprint**: The thumbprint of the Cluster Admin certificate setting.
    - **NewValue**: The thumbprint of the new SSL certificate.

This will perform a rolling upgrade on the service fabric cluster. You can check the status of this using the Service Fabric explorer, which shows **Upgrades in progress**. Click this link to view the progress.



For more information on how to use the Service Fabric Explorer, please see View Service Fabric Explorer at "View the Health of your Service Fabric Cluster" on page 35.

Apply Windows Updates

We recommend you disable automatic Windows Updates on your cluster nodes and manage this process manually. BeyondTrust recommends you use the Service Fabric Patch Orchestration application provided by Microsoft. This ensures only one cluster is offline at any one time.

PMC Scripts

The three PowerShell scripts that follow are supplied with PMC to support your installation. The use of these is optional:

- **Deactivate Duplicate Agents**
- **Deactivate Inactive Agents**
- **NodeDiagnosticsLogsDownload**

For more information, please see the following:

- "Deactivate Duplicate Agents" on page 57
- "Deactivate Inactive Agents" on page 58
- "Cluster Node Service Logs" on page 45

Deactivate Duplicate Agents

The script to deactivate agents with multiple hostnames is called **DeactivateDuplicateAgents.ps1** and is supplied by BeyondTrust in the PowerShell folder.

Description

The script returns a list of agents that it has identified as duplicates. In each set of duplicate agents, the ones with the oldest timestamps are flagged for deactivation. These agents are immediately removed from PMC. The script pauses for five minutes before it deactivates the agents to ensure that other tasks aren't running. Lastly the script will confirm the number of agents that it has deactivated. On deactivation, the **Authorization Status** of the agent will change to **Deactivated**. You can view the **Authorization Status** of an agent in the **Computer Details** page in PMC.

This script takes five parameters:

- **client_id**
- **client_secret**
- **tenant_id**
- **cloudServiceDnsName**
- **platformApiPort**

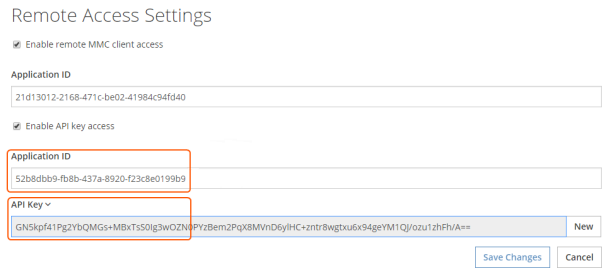
You can run the script in PowerShell without the parameters and you'll be prompted for each one in turn or you can build the full command line before pasting it into PowerShell.

Example Script

```
.\DeactivateDuplicateAgents.ps1 -client_id "<client_id>" -client_secret "<client_secret>" -tenant_id
"<tenant_id>" -cloudServiceDnsName "<cloudServiceDnsName>" -platformApiPort "<port number>"
```

client_id

This is the **Application ID** that is below the **Enable API key** access check box in the **Remove Access Settings** page in PMC.



client_secret

This is the **API Key** in the PMC c**Settings** page.

tenant_id

For Windows Directory and LDAPS the GUID is generated by the deployment tool and you should have a note of it already.

> For instructions on getting this GUID for Microsoft Azure authentication, please see "Microsoft Azure AD Authentication" on page 15.

cloudServiceDnsName

This is your PMC URL. Do not include the **https://** or the port when entering. For example, **pmc.example.com**.

platformApiPort

This is the port number the API connects on. It is usually 8443.

Deactivate Inactive Agents

The script to deactivate inactive agents is called **DeactivateNonActiveAgents.ps1** and is supplied by BeyondTrust in the PowerShell folder.

Description

When running, the script states that it's retrieving a list of Agents that have not connected for the defined number of days (**inactiveDays**) since a date and time. The date and time will be the date of the system minus the number set for **inactiveDays**. It then details how many agents have been identified and confirms that it will request to deactivate a specified number of agents. The script

pauses for five minutes before it deactivates the agents to ensure that other tasks aren't running. The script will confirm the number of agents that it has deactivated. On deactivation, the **Authorization Status** of the agent will change to **Deactivated**. You can view the **Authorization Status** of an agent in the **Computer Details** page in PMC.

This script takes six parameters:

- **client_id**
- **client_secret**
- **tenant_id**
- **cloudServiceDnsName**
- **inactiveDays**
- **platformAPIPort**

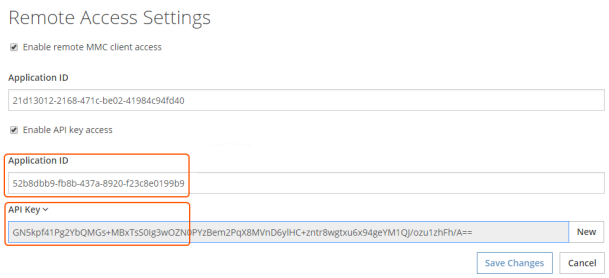
You can run the script in PowerShell without the parameters and you'll be prompted for each one in turn or you can build the full command line before pasting it into PowerShell.

Example Script

```
.\DeactivateNonActiveAgents.ps1 -client_id "<client_id>" -client_secret "<client_secret>" -tenant_id
"<tenant_id>" -cloudServiceDnsName "<cloudServiceDnsName>" -inactiveDays "<inactiveDays>" -
platformApiPort "<port number>"
```

client_id

This is the **Application ID** that is below the **Enable API key** access check box in the **Remove Access Settings** page in PMC.



client_secret

This is the **API Key** in the PMC **Settings** page.

tenant_id

For Windows Directory and LDAPS the GUID is generated by the deployment tool and you should have a note of it already.

> For instructions on getting this GUID for Microsoft Azure authentication, please see "Microsoft Azure AD Authentication" on page 15.

cloudServiceDnsName

This is your PMC URL. Do not included the **https://** or the port when entering, for example **test.ic3.example.com**.

inactiveDays

This is the number of days the tenant has been inactive and has to be a minimum of 15.

platformApiPort

This is the port number the API connects on. It should be 8443.