



BeyondTrust

Privilege Management PMC Azure Installation Guide 2.4.x

Table of Contents

Introduction	6
PMC Components	6
Adapters	6
Deployment Package	6
Prerequisites	8
Deployment Attributes	8
Ports Configured by the Deployment	8
Deployment Machine Prerequisites	10
PowerShell	11
DNS Name of SSL Certificate Prerequisites	11
Production Environments	11
Evaluation Environments	12
Microsoft Azure Prerequisites	12
Subscription Requirements	12
Location for Deployment	13
Usage and Quotas	14
Subscription ID	14
Directory ID	14
PMC Application User	15
PMC Application	15
Microsoft Azure Application ID	16
Application Key	17
Load Balancer Prerequisites	17
Privilege Management Reporting Database Sizes	18
Deploy PMC	20
Deployment Errors	23
Enable Auto-indexing	23
Azure Parameters	25
Azure AD Authentication Domain	25
Azure App ID	25
Azure App Key	25

Cluster VMs Username	25
Cluster VMs Password	25
Reporting Database Username	26
Reporting Database Password	26
PMC Application SQL Username	26
PMC Application SQL Password	26
Initial Portal Admin Username	26
Jump Box and Portal VM Username	26
Jump Box and Portal VM Password	26
KeyVaultName	27
KeyVaultResourceGroupName	27
Location	27
Public IP Address	27
ResourceGroupName	27
SQL Administrator Username	27
SQL Administrator Password	27
SSL DNS Name	28
SSL Certificate Password	28
SSL Certificate Thumbprint	28
SubscriptionId	28
Password Policy	28
PMC Architecture Overview	29
PMC Certificates	29
SSL	30
PMC Configuration Encipherment	30
PMC Tenant Certificate Authority	30
PMC Tenant Service Identity	30
PMC Cluster Admin	30
PMC Root	31
PMC Cluster Admin	31
PMC Root	31
PMC Certificate Chain	31
Post-Deployment Steps	32

Resolve DNS Settings	32
Install your SSL Certificate	33
Turn off Jump Box	33
Clean Deployment Machine	33
Deployment Folder Deletion	34
Certificate Removal	34
Cluster Admin	34
Remove Public IP Address from Azure Firewall Exceptions	34
View the Health of your Service Fabric Cluster	36
Install the PMC Cluster Admin Certificate	36
View the Service Fabric Dashboard	36
Log in and Configure PMC	37
Connect PMC to Policy Editor	38
Configure the Privilege Management MMC PMC snap-in	39
Add and Configure the Privilege Management PMC Snap-in	39
Confirm Connection to PMC	41
Configure Endpoints	42
Privilege Management Clients	42
Privilege Management Adapters	42
Install the Windows Adapter for PMC	44
Configure the Windows PMC Adapter	46
Ensure the iC3Adapter User Has the "User Can Log on as a Service" Right	46
Install the Mac Adapter for PMC	46
Logs	48
Portal Logs	48
Cluster Node Service Logs	48
Specific Node by URL	48
All Nodes Using PowerShell	48
Adapter Logs	49
Upgrade an Azure Deployment	49
Turn on your Jump box	50
Upgrade the Database	50
Prerequisites	50

Upgrade Process	50
Upgrade the Application	51
Enable WinRM with SSL on the Portal VM	51
Perform Upgrade on the Jump Box VM	51
Check for Successful Upgrade	53
Upgrade Issues	53
Error on subsequent upgrade after failed upgrade	53
Upgrade the Portal	54
Upgrade Privilege Management Reporting	54
Upgrade Steps	54
Change Application Parameters Before Upgrade	56
Rotate the SSL Certificates	57
Import the Certificate Into your KeyVault	57
Update the Scale Set ARM Template	57
Update the Portal/Jumpbox VMs ARM Template	58
Configure Internet Information Services (IIS)	59
Make the PMC Application Configuration Changes	59
Perform Database Backups for Long-Term Retention	61
Apply Windows Updates	62
PMC Supporting Scripts	63
Deactivate Duplicate Agents	64
Description	64
Example Script	64
Deactivate Inactive Agents	65
Description	65
Example Script	65

Introduction

Privilege Management Console (PMC) is a management platform for Privilege Management that allows you to manage your endpoints from one central location. This guide takes you through installing and configuring PMC.

PMC Components

This section describes the components of the PMC management platform and Privilege Management agents.

- **PMC Adapter:** The PMC Adapter manages the communication between Privilege Management and PMC.
- **PMC Portal:** The Internet Information Services (IIS) application that hosts PMC. This is deployed onto an Azure infrastructure as a service (IaaS) virtual machine.
- **Load balancer:** The purpose of the load balancer is to evenly distribute the workload to maximize performance and capacity. A load balancer allows for dynamic scaling of PMC without requiring any reconfiguration at the client side. The external load balancer is deployed as a service within Azure. It distributes the incoming network traffic from the adapter across the PMC cluster. This maximizes speed and capacity across your infrastructure.

You can optionally configure an internal load balancer, if required. When an internal load balancer is configured alongside the external load balancer, the portal traffic is routed through the internal load balancer, rather than the external load balancer.

- **Application Services:** The application services are deployed in Azure and are contained in the PMC Service Fabric cluster.
- **Application Cache:** A Redis cache is deployed as a service in Azure, and stores information from the PMC services and databases to maximize performance.
- **Microsoft SQL databases:** There are three Azure SQL databases: one for the endpoint audit data that is used for reporting and two for the PMC application services data.
 - **Privilege Management Reporting database:** Contains the Privilege Management auditing data for the PMC reports.
 - **PMC Management database:** This is the core PMC database. It holds the majority of data visible in PMC (for example, Computers, Groups, and Users).
 - **PMC Blob Storage database:** This database is used for holding BLOB data (Binary Large Objects). This is limited to Policy Documents and Adapter Logs, when requested from PMC.

Adapters

Endpoints you want to manage with PMC need Privilege Management and the Privilege Management PMC adapter installed. Versions of the PMC adapter are available for both Windows and Mac operating systems. Onboarding of endpoints into PMC for management is completed as the final step of the deployment, and requires parameters which are managed from the PMC portal.

Deployment Package

You can get the PMC deployment package from your BeyondTrust consultant.

The PMC deployment package contains the following folders and files:

- **AdapterInstallers:** Contains the installer for the adapter.



For information on installing the endpoint software, please see "[Configure Endpoints](#)" on page 42.

- **Deployment:** Contains an **AzurePaas** folder that contains the resources for deploying the PMC platform to Azure.
- **Encipherment:** Contains the PowerShell scripts that you can use to encrypt and decrypt strings for PMC.
- **Powershell:** Contains PowerShell scripts that may be used to perform tasks on endpoints in bulk.

i For more information, please see ["PMC Supporting Scripts"](#) on page 63.

After you have deployed PMC, you need to delete the deployment package from the deployment machine.

i For information on deleting the deployment package, please see ["Post-Deployment Steps"](#) on page 32.

Prerequisites

You need to complete a number of considerations before you start deploying PMC:

Deployment Attributes

Deploy PMC to Azure using a PowerShell script. You need to supply several arguments to the script, some of which you will collect during the deployment process.



For a full list of arguments in alphabetical order, please see ["Azure Parameters" on page 25](#).



Tip: We recommend you open a text editor such as Windows Notepad now, so you can make note of these arguments as you acquire them. You will gather the following attributes as part of the prerequisites.

- DNS Name of SSL certificate
- Microsoft Azure subscription ID
- Azure Location
- Azure Directory ID
- PMC Application User
- PMC Application Key

Ports 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

Source	Destination	Port Number	Machines	Reason
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

Source	Destination	Port Number	Machines	Reason
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.

Deployment Machine Prerequisites

You need a virtual or physical machine to deploy PMC from. This machine is known as the deployment machine. The deployment machine must be either Windows 10 or Windows Server 2016.

You must have the ability to run **PowerShell.exe** as an administrator on this machine.



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
```

PowerShell

PMC is deployed using a PowerShell script that you will supply arguments to when prompted. The following tasks need to be performed in the PowerShell instance that you will use to deploy PMC:

1. Run **PowerShell.exe** as an administrator.
2. Navigate to the **Azure Paas** PMC deployment folder.
3. Type **set-executionpolicy unrestricted -scope currentUser -f** and press **Enter** to set the execution policy.
4. Type **install-module -name sqlserver -allowclobber** and press **Enter** to install the SQL Server module. You may be prompted that the repository is not trusted. Install the modules to proceed.
5. Type **install-module -name azurearm -allowclobber** and press **Enter** to install the Azure Resource Manager. You may be prompted to install the NuGet module as well.
6. Type **connect-azurermaccount** and press **Enter** to log into your Microsoft Azure account.

Please leave this instance of **PowerShell.exe** open, as you will use it to determine some of your Azure prerequisites and to subsequently deploy PMC to Microsoft Azure. If you do close the instance before you deploy PMC, please rerun steps 1, 2, 3, and 6.

DNS Name of SSL Certificate Prerequisites

You must know or decide on the DNS Name of your SSL certificate before you proceed. The DNS Name is part of your SSL certificate. For example: **pmc.ssldns.name**.

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 certificate, the SAN must include the core domain name.

The type of SSL certificate you can use should be driven by the type of environment you're deploying PMC to. This section covers:

- Production Environments
- Evaluation Environments



For more information on the certificate chain, please see "[PMC Certificates](#)" on page 29.

If the portal Virtual Machine (VM) does not trust the Certificate Authority (CA) you provide, you must install the SSL certificate onto your portal VM after deployment. You would need to install the SSL certificate onto the portal VM if the Certificate Authority was not issued by a trusted root authority, for example.



For more information, please see "[Install your SSL Certificate](#)" on page 33.

Production Environments

When you are deploying PMC to a production environment:

- You must supply your own SSL certificate. The SSL certificate can be self-signed or signed by a globally trusted authority. If it is self-signed, there are some additional steps to do after deployment which are detailed in this guide.
- You may use multiple subdomains; we recommend that you use a Subject Alternative Name (SAN) list.
- Wildcard characters in the DNS Name of the SSL certificate are not supported.

- You need to know the DNS Name of your SSL certificate.
- You need to know the password for your SSL certificate.
- You need to know the thumbprint for your SSL certificate. You can obtain this using the **Get-PfxCertificate .sslCertificate.pfx** command in PowerShell, where you specify the path to your SSL certificate. You will be prompted to enter the password for the certificate.



***Tip:** Please ensure you know the DNS of your SSL certificate before you proceed. It is required multiple times throughout the deployment of PMC.*

Evaluation Environments

- You need to decide on the DNS Name of the SSL certificate before you start the deployment as you will be prompted to enter it to allow a certificate to be generated
- Wildcard characters are supported, but multiple subdomains are not
- The generated SSL certificate is self-signed by the PMC root certificate authority



***Tip:** Please make a note of the DNS Name you decide on before you proceed. It is required multiple times throughout the deployment of PMC.*

Microsoft Azure Prerequisites

You need to meet the following prerequisites in Microsoft Azure. Please ensure your subscription meets the minimum requirements and extract the information you need.

- "Subscription Requirements" on page 12
- "PMC Application User" on page 15
- "PMC Application" on page 15

Subscription Requirements

If you do not yet have an Azure subscription, go to <https://azure.microsoft.com/> to get started. Please read these instructions to ensure your quota is adequate.

There are two considerations for your subscription that you must check before you proceed:

- "Location for Deployment" on page 13
- "Usage and Quotas" on page 14



IMPORTANT!

If you employ regex rules for naming conventions in your Azure subscription, be sure to name any new resources per your regex requirements; otherwise, you will receive resource naming errors, such as the errors displayed in this example.

```

Creating Resource Group rgkvpmc22test in location eastus
New-AzureRmResourceGroup : 'resourceGroupName' does not match expected pattern '^[a-z0-9-]{3,24}$'.
At C:\temp\iC3 - PMC 2.2 Azure PaaS Deployment Kit - 1.2.34206\CreateKeyVaultAndAddCerts.ps1:22 char:8
+ [void](New-AzureRmResourceGroup -Name $resourceGroupName -Location $l ...)
+ ~~~~~
+ CategoryInfo          : CloseError: (:) [New-AzureRmResourceGroup], ValidationException
+ FullyQualifiedErrorId : Microsoft.Azure.Commands.ResourceManager.Cmdlets.Implementation.NewAzureResourceGroupCmdlet

Creating key vault kvpmc22test
New-AzureRmKeyVault : 'vaultName' does not match expected pattern '^[a-z0-9-]{3,24}$'.
At C:\temp\iC3 - PMC 2.2 Azure PaaS Deployment Kit - 1.2.34206\CreateKeyVaultAndAddCerts.ps1:25 char:10
+ $retKV = New-AzureRmKeyVault -VaultName $vaultName -ResourceGroupName ...
+ ~~~~~
+ CategoryInfo          : CloseError: (:) [New-AzureRmKeyVault], ValidationException
+ FullyQualifiedErrorId : Microsoft.Azure.Commands.KeyVault.NewAzureKeyVault

```

Location for Deployment

Within your subscription, you may not be able to deploy PMC to some regions. You can optionally check which regions are available before you start to ensure you can deploy PMC there. This information is also validated before PMC is deployed.

In the instance of **PowerShell.exe** that you have on your deployment machine:

1. Type **Get-AzureRmComputeResourceSku** and press **Enter** to determine which regions are available to you.

In this screenshot, the **westus** location is not available in this subscription for **Standard_D1_V2**.

```

PS C:\Users\Administrator\Desktop> Get-AzureRmComputeResourceSku | where {$_.Locations.Contains("westus")};

```

ResourceType	Name	Location Zones	Restriction	Capability	Value
virtualMachines	Standard_D1_v2	westus	NotAvailableForSubscription	MaxResourceVolumeMB	51200
virtualMachines	Standard_D2_v2	westus	NotAvailableForSubscription	MaxResourceVolumeMB	102400
virtualMachines	Standard_D3_v2	westus	NotAvailableForSubscription	MaxResourceVolumeMB	204800
virtualMachines	Standard_D4_v2	westus	NotAvailableForSubscription	MaxResourceVolumeMB	409600
virtualMachines	Standard_D5_v2	westus	NotAvailableForSubscription	MaxResourceVolumeMB	819200

2. Choose the location closest to you that does not have anything listed in the **Restriction** column. Deploying PMC to a region that is farther away can result in deployment errors caused by network latency.



Tip: Make a note of your chosen location now, as you will be prompted for it when you deploy PMC.

You can further filter this by region to check it for restrictions if you know the name of the region you want to deploy to:

```
Get-AzureRmComputeResourceSku | where {$_.Locations.Contains("westus")};
```

Usage and Quotas

To deploy PMC, you need a Microsoft Azure subscription that has the following minimum quota:

- **Quota:** Standard Dv2 Family vCPUs
- **Provider:** Microsoft.Compute
- **Location:** Select one geographically close to you
- **Usage:** 14 free

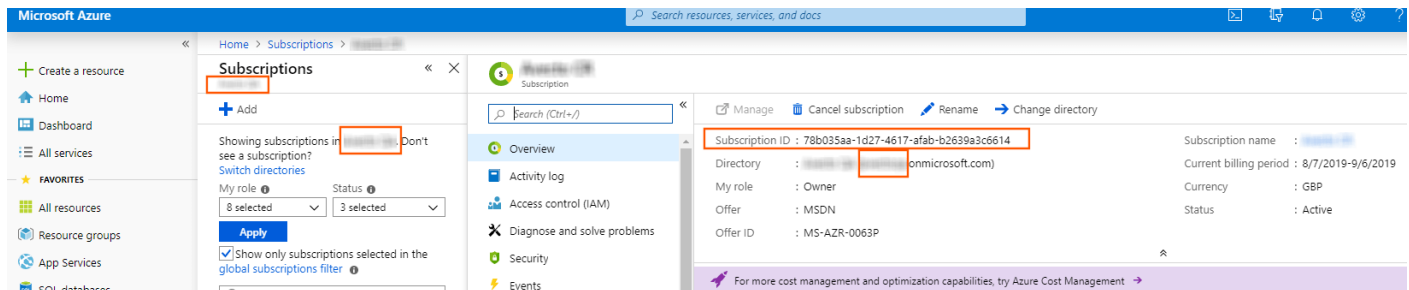
This is checked and validated prior to deployment.

Subscription ID



Tip: You need to obtain your **Subscription ID**, as this is used when you deploy PMC. Please make a note of the **Subscription ID** from this section.

In the provided example, the orange boxes indicate where the name of your Azure subscription is displayed. The **Subscription ID** is also shown.



The screenshot shows the Microsoft Azure portal interface. On the left, the 'Subscriptions' link is highlighted with an orange box. In the main content area, the 'Showing subscriptions in' dropdown menu is open, and the subscription name is highlighted with an orange box. On the right, the 'Subscription ID' field is highlighted with an orange box. The subscription details pane shows the following information:

Subscription ID	: 78b035aa-1d27-4617-afab-b2639a3c6614	Subscription name	: [redacted]
Directory	: [redacted] onmicrosoft.com	Current billing period	: 8/7/2019-9/6/2019
My role	: Owner	Currency	: GBP
Offer	: MSDN	Status	: Active
Offer ID	: MS-AZR-0063P		

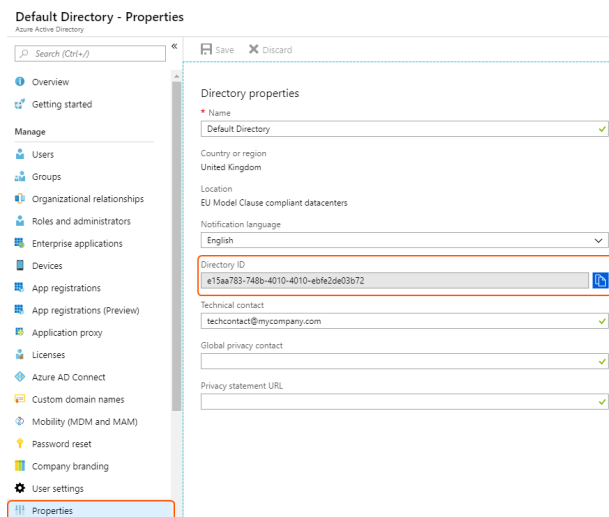
Directory ID



Tip: Please make a note of the **Directory ID**, as you will need it when you deploy PMC.

To obtain your Directory ID:

1. Go to **Azure Active Directory > Properties**. The **Directory ID** is shown on the right, in the **Directory properties** pane.
2. Click the icon to the right to copy it to your clipboard. Also make note of it in your list of prerequisite attributes.



PMC Application User

A user is created as part of your Azure subscription. To view the users in your subscription, go to **Azure Active Directory > Users**.

Because PMC authenticates with an Azure Active Directory, the username must take the form **pmcadmin@companyname.onmicrosoft.com**.

This user is the first administration user that will access PMC. This user does not need to be added to any specific privileges or group assignments.

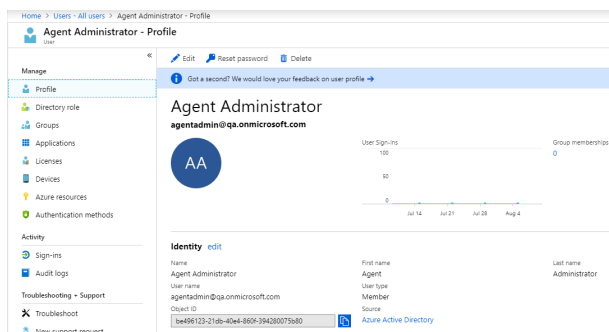
If you are working with a federated Azure Active Directory, the username format can be **username@domain.com**.



For instructions on creating a new user, please see [Add or delete users using Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory) at <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory>.



Tip: Make a note of the full username in the form shown, as well as the password, as you'll need it for the PMC deployment.



PMC Application

You need to create one application in Azure for PMC. This application needs some specific configuration once you have created it. You need to know the DNS Name of your SSL certificate.

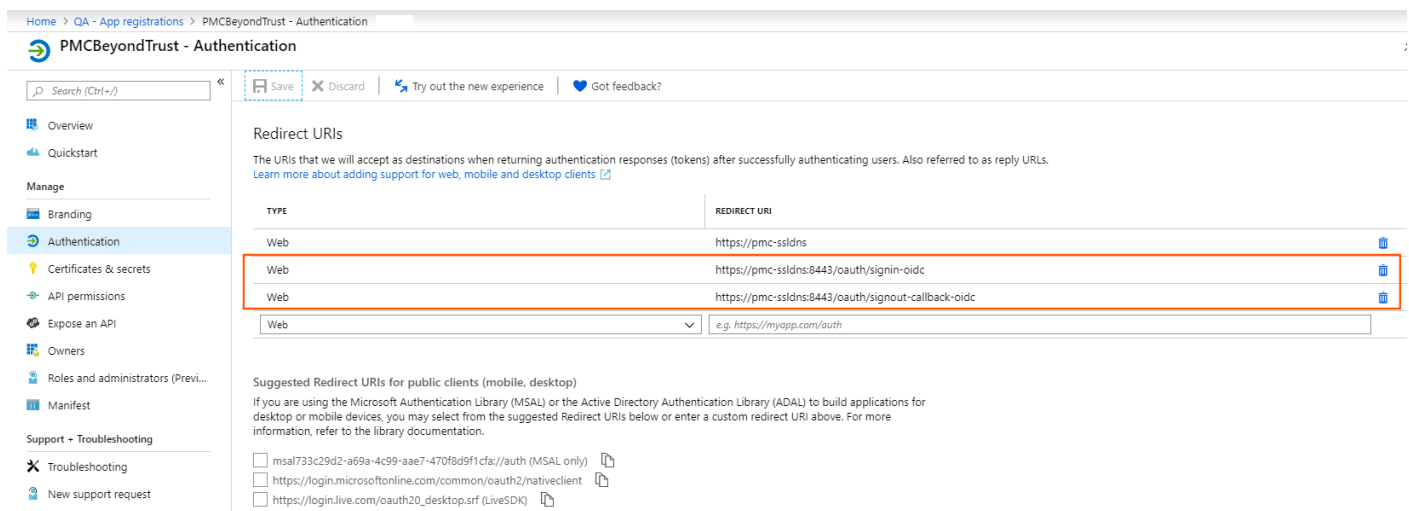


For more information, please see ["DNS Name of SSL Certificate Prerequisites"](#) on page 11.

To create a new application in Azure:

1. Click **Azure Active Directory** > **App registrations**.
2. Click **New registration** and enter the following details:
 - **Name:** The name of your application. We recommend **PMC-application**.
 - **Application Type:** Leave the default selection of **Web**.
 - **Sign-on URL:** This should be in the format of a valid domain name, which can be anything, as long as it can be resolved by DNS. We recommend you use the DNS Name of your SSL certificate, as it forms part of your Reply URLs. For example, **https://PMC.sslidns.name**. These are added in the next step.
3. Click **Create**. The application is created.
4. Click **Authentication** and enter the following values as two new URLs in addition to the value that's already there. You don't need the original Redirect URL; you can delete this if you want to. For example, if the DNS Name of your SSL certificate is **PMC.sslidns.name**, the Redirect URLs would be:

```
https://PMC.sslidns.name:8443/oauth/signin-oidc
https://PMC.sslidns.name:8443/oauth/signout-callback-oidc
```



Home > QA - App registrations > PMCBeyondTrust - Authentication

PMCBeyondTrust - Authentication

Search (Ctrl+/) Save Discard Try out the new experience Got feedback?

Overview Quickstart Manage Branding Authentication Certificates & secrets API permissions Expose an API Owners Roles and administrators (Previous) Manifest Support + Troubleshooting Troubleshooting New support request

Redirect URIs

The URIs that we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URIs. [Learn more about adding support for web, mobile and desktop clients](#)

TYPE	REDIRECT URI
Web	https://pmc-sslidns
Web	https://pmc-sslidns:8443/oauth/signin-oidc
Web	https://pmc-sslidns:8443/oauth/signout-callback-oidc
Web	e.g. https://myapp.com/auth

Suggested Redirect URIs for public clients (mobile, desktop)

If you are using the Microsoft Authentication Library (MSAL) or the Active Directory Authentication Library (ADAL) to build applications for desktop or mobile devices, you may select from the suggested Redirect URIs below or enter a custom redirect URI above. For more information, refer to the library documentation.

- ☐ msal733c29d2-a69a-4c99-aae7-470fbd9f1cfa://auth (MSAL only)
- ☐ https://login.microsoftonline.com/common/oauth2/nativeclient
- ☐ https://login.live.com/oauth20_desktop.srf (LiveSDK)

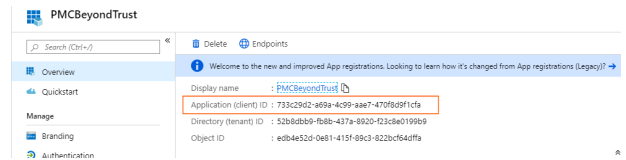
5. Click **Save**.

Microsoft Azure Application ID



Tip: You need the **Application ID** of your application for the deployment script. Please make a note of your **Application ID** now.

To find your Application ID, navigate to the application you just created. The Application ID is shown to the right, in the **Overview** pane.



Application Key



*You need the **Client secret** for the deployment script. Once it has been generated, please make a note of it. You will not be able to view it again.*

You need to generate a secret string for your PMC application.

1. In your application, click **Certificates & secrets**.
2. Enter a description for the new key. We recommend **PMC-key**. Select the expiration parameters. We recommend you set the key to **Never expires**. If the key expires, you will need to re-deploy PMC.
3. Click **Save**. The key value is displayed. You cannot retrieve this key after you leave this page in Microsoft Azure.

PMCBeyondTrust - Certificates & secrets

Search (Ctrl+F)

Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest
Support + Troubleshooting
Troubleshooting
New support request


Copy the new client secret value. You won't be able to retrieve it after you leave this blade.

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates
Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.
[Upload certificate](#)
No certificates have been added for this application.

THUMBPRINT	START DATE	EXPIRES

Client secrets
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.
[New client secret](#)

DESCRIPTION	EXPIRES	VALUE
pmc-key	8/9/2021	:Bto*FYCA0nAPn.6lq7xn3A+bd3060Z 

Load Balancer Prerequisites

PMC supports two load balancer configurations:

- External load balancer
- External and internal load balancer

You will be prompted to choose if you want to configure an internal load balancer in addition to the default external load balancer in the deployment script. If you want to configure an internal load balancer, and you'd like to use your existing IP ranges from a peered network, modify this parameter file **before** you start the deployment.

If you configure an internal load balancer, all traffic for PMC will be routed through it. The external load balancer is only used for Microsoft requirements, such as ServiceFabric and SQL Server updates.

The **addressPrefix** and **subnet0Prefix** are CIDR notation, which is used to specify the IP range for a VNet. The subnet has to be within the range of the address. If you do add the prefix parameters manually, **10.1.1.0/27** is used for both. If you add these values, you must update the load balancer address in the **PMCMPTemplate_InternalExternalLB.json** template, otherwise you will receive an error stating that the default load balancer address is not within the subnet range you specified.

The **clientIP** is the public IP address of the machine you are deploying from. You enter this as part of the deployment. The address is used to set the firewall rules allowing access to SQL Server databases.

1. Locate and open the **PMCMPTemplateParameterValues.json** file.



Note: Other values in this template must not be edited.

2. Go to the bottom of the file and locate the following lines:

```
"clientIP": {
  "value": "193.240.178.130"
}
```

3. Duplicate them twice, so that you have three instances of **ClientIP**.
4. Change the two new instances of **ClientIP** to **addressPrefix** and **subnet0Prefix**:

```
"addressPrefix": {
  "value": "193.240.178.130"
}

"subnet0Prefix": {
  "value": "193.240.178.130"
}
```

5. Change the IP address to match the range for your network and save the file.

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

Managed Computers	CPU	Memory	Database
150,000	8	24 GB	1012.5 GB
200,000	8	32 GB	1350 GB
250,000	8	32 GB	1687.5 GB

Deploy PMC

The infrastructure setup script provisions the hardware your PMC installation runs on.



For more information on the parameters used here, please see ["Azure Parameters" on page 25](#).

The arguments you supply here are not validated until you have entered all the parameters and have started to deploy PMC to Microsoft Azure.

Please verify the arguments you provide, specifically that:

- All passwords meet the password policy.



For more information, please see ["Password Policy" on page 28](#).

- The location you choose is available in your subscription.



For more information, please see ["Location for Deployment" on page 13](#).

- The **keyvault** resource group name is unique in Microsoft Azure, not just your subscription.
- The information you are providing from your subscription is correct.

Deploy PMC to Microsoft Azure using PowerShell

1. If you are supplying your own SSL certificate, rename your SSL certificate **sslCertificate.pfx** and place it in the **Certs** folder of the **AzurePaaS** folder.
2. In the same PowerShell window where you ran the prerequisites, change to the **AzurePaaS** folder.
3. Type **PMCAzurePaaSInstall.ps1** and press **Enter**.
4. Enter the following parameters when requested and press **Enter** after each one.
 - a. **Azure Subscription ID:** You made a note of this when you configured your subscription. For example, **6d01f381-e870-4964-83f3-6cc0cbb1c048**.



For more information, please see ["Subscription ID" on page 14](#).

- b. **SSL DNS Name:** The DNS Name of the SSL certificate you supplied or the DNS Name of the SSL certificate you want the deployment tool to generate. For example, **PMC.sslidns.name**.



For more information, please see ["DNS Name of SSL Certificate Prerequisites" on page 11](#).

- c. **Resource Group Name:** The name of the resource group that will be created in Microsoft Azure. We recommend you prefix it with **PMC**. For example, **PMC-rg-mycompany**.
- d. **KeyVault Name:** The name of the keyvault that will be created in Microsoft Azure. We recommend you prefix it with **PMC**. For example, **PMC-kv-mycompany**.



IMPORTANT!

The keyvault name must be unique within Microsoft Azure, not just your subscription. The uniqueness of this name is not validated until deployment.

- e. **KeyVault Resource Group Name:** The name of the resource group for the **keyvault** in Microsoft Azure. For example, **PMC-kv-rg-mycompanyname**.
- f. **Location:** The location in Microsoft Azure that you will deploy PMC to.



For more information, please see "[Location for Deployment](#)" on page 13.

- g. The deployment script will now try and log into your Microsoft Azure account and validate the number of free cores in your chosen **Location**. If your Microsoft Azure credentials are known to the deployment machine prior to this point, it will log in automatically. Otherwise, you are prompted to enter your credentials for Microsoft Azure. Please enter your details to continue. If you do not have enough free cores, the deployment will not proceed.
- h. **Do you require an internal Azure load balancer to be configured?:** By default, PMC does not use an internal load balancer, however you can enter **y** here to configure one. Otherwise, enter **n**.



For more informationPlease see "[Load Balancer Prerequisites](#)" on page 17.

- i. **What is your public IP address?:** You can obtain your public IP address by opening a browser on your deployment machine and navigating to <https://www.whatismyip.com/what-is-my-public-ip-address/>.
- j. **Enter the username for the scale set VMs administrator login.** This is the administrator username that you will use to access the **node** virtual machines that are created by the deployment script. For example, **PMCScalesetadmin**.
- k. **Enter the password for the scale set VMs administrator login.** This is the administrator password that you will use to access the **node** virtual machines that are created by the deployment script. All passwords must conform to the policy in Azure.



For more information, please see "[Password Policy](#)" on page 28.


- l. **Enter the username for the Portal & Jump Box VMs administrator login.** This is the administrator username that you will use to access the **jump box** and **portal** virtual machines that are created by the deployment script. For example, **PM Cvadmin**.
- m. **Enter the password for the Portal & Jump Box VMs administrator login.** The Jump Box is a virtual machine that is created by the deployment and is subsequently used to administer aspects of PMC. This is the administrator password that you will use to access the **jump box** and **portal** virtual machines that are created by the deployment script. All passwords must conform to the policy in Azure.



For more information, please see "[Password Policy](#)" on page 28.

- n. **Enter the username for the SQL Administrator accounts.** This is the SQL administrator username that will be used to create the databases by the deployment script. For example, **PM Csqladmin**.

- o. **Enter the password for the SQL Administrator accounts.** This is the SQL administrator password that will be used to create the databases by the deployment script. All passwords must conform to the policy in Azure.


 For more information, please see ["Password Policy" on page 28.](#)

- p. **Supplied SSL.** If you have renamed your own SSL certificate to **sslcertificate.pfx** and put it in the **Cert** folder, type **y**, otherwise type **n**.
- q. **Enter the username of the PMC application SQL user to be created.** This is the SQL PMC application user that manages communication on a day to day basis with the PMC databases. For example, **PMCSqlapplication**.


IMPORTANT!

The PMC application SQL username must be different to the SQL Administrator username as the users are inserted into the same databases by the deployment script.


- r. **Enter the password of the PMC application SQL user to be created.** This is the SQL PMC application password that manages communication on a day to day basis with the PMC databases. All passwords must conform to the policy in Azure.

 For more information, please see ["Password Policy" on page 28.](#)

- s. If you supplied your own SSL certificate, you are prompted to enter the password for it now.

 For more information, please see ["DNS Name of SSL Certificate Prerequisites" on page 11.](#)


- t. If you supplied your own SSL certificate, you are prompted to enter the thumbprint for it now.

 For more information, please see ["DNS Name of SSL Certificate Prerequisites" on page 11.](#)

- u. **Configuring Reporting?** Enter **y** to configure Reporting in PMC; otherwise enter **n**.

If you selected **y** to **Configuring Reporting**:

- i. **Enter the username of the Reporting application SQL user to be created.** This is the SQL username that will be used to manage communication to the Reporting database. For example, **PMCSqlreporting**.
- ii. **Enter the password of the Reporting application SQL user to be created.** This is the SQL password that will be used to manage communication to the Reporting database. All passwords must conform to the policy in Azure.

 For more information, please see ["Password Policy" on page 28.](#)

- v. **Enter the initial portal administrator username.** This is the administrator username you will use to log into the PMC portal for the first time. You set this up in Azure. For example, **PMCAadmin@companyname.onmicrosoft.com**.



For more information, please see ["PMC Application User" on page 15](#).

- w. **Enter Azure AD Authentication Domain.** This is the following link with your **Directory ID** appended to it. For example, **https://login.microsoftonline.com/e15aa783-748b-4010-4010-ebfe2de03b72**.



For more information, please see ["Directory ID" on page 14](#).

- x. **Enter Azure AD App ID.** This is your Microsoft Azure PMC Application ID. For example, **4a01d381-e860-7352-83b3-6dd4cbb1b048**.



For more information, please see ["Microsoft Azure Prerequisites" on page 12](#).

- y. **Enter Azure AD App key.** This is the key you created in your PMC Azure Application. For example, **AHN9Rqp0Paa9ahwbW24fbcW4phZCp3GdmnBTrcuOPaa=**.



For more information, please see ["Application Key" on page 17](#).



Note: When you deploy PMC to Azure, run the **Deploy-IC3Application.ps1** installation script and provide the parameters when prompted. Passing parameters into the script using a text file is not supported functionality.



Note: When you press **Enter**, the script will start to deploy PMC to Microsoft Azure.

Deployment Errors

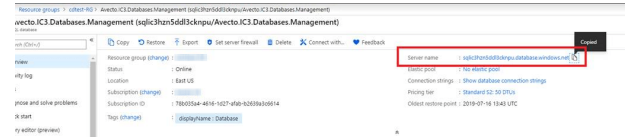
If you receive any errors during the deployment, you can terminate the script by pressing **CTRL+C**. You can rerun the script at any time and provide the same parameters using the **Up** and **Down** arrows to select them. If you receive an error message, please contact BeyondTrust Technical Support.

Enable Auto-indexing

After you have completed deployment of your Azure deployment of PMC, auto-indexing needs to be enabled. This is accomplished by using SQL Server Management Studio to update the Auto Index setting of the System Parameters table in the Management Database.

1. Open the Azure Portal and navigate to your Resource Group.
2. From the resource group, select the **Avecto.IC3.Databases.Management** SQL database.

3. Select the **Server name** from this menu and copy it.



4. Open **Microsoft SQL Server Management Studio** and enter the server name you copied into the **Server name** field.
5. Log in using the SQL admin credentials that were specified in the installation script.

i For more information, please see ["Deploy PMC" on page 20](#).

6. Open the **Avecto.IC3.Databases.Management** database and expand **Tables**.
7. Right-click the **dbo.SystemParameter** table and select **Edit Top 200 Rows**.
8. Locate **AutoIndexMaintenaceEnabled** in the **ParameterName** column and change its value from **0** to **1** to enable auto-indexing.

Azure Parameters

These are the parameters that are required by the script. They are listed in alphabetical order.



Note: When you deploy PMC to Azure, run the **Deploy-iC3Application.ps1** installation script and provide the parameters when prompted. Passing parameters into the script using a text file is not supported functionality.

Azure AD Authentication Domain

Enter Azure AD Authentication Domain: The following link with your **Directory ID** appended to it. For example, <https://login.microsoftonline.com/e15aa783-748b-4010-4010-ebfe2de03b72>.



For more information, please see ["Directory ID" on page 14](#).

Azure App ID

Enter Azure AD App ID: Your Microsoft Azure PMC Application ID. For example, **4a01d381-e860-7352-83b3-6dd4cbb1b048**.



For more information, please see ["Microsoft Azure Prerequisites" on page 12](#).

Azure App Key

Enter Azure AD App key: The key you created in your PMC Azure Application. For example, **AHN9Rqp0Paa9ahwbW24fbcW4phZCp3GdmnBTrcuOPaa=**.



For more information, please see ["Application Key" on page 17](#).

Cluster VMs Username

This is the administrator username you will use to access the **node** virtual machines that are created by the deployment script. For example, **pmcscalesetadmin**.

Cluster VMs Password

This is the administrator password you will use to access the **node** virtual machines that are created by the deployment script. All passwords must conform to the policy in Azure.



For more information, please see ["Password Policy" on page 28](#).

Reporting Database Username

This is the SQL username that will be used to communicate with the Privilege Management Reporting database. For example, **pmcsqlreporting**.

Reporting Database Password

This is the SQL password that will be used to communicate with the Privilege Management Reporting database. All passwords must conform to the policy in Azure.

i For more information, please see ["Password Policy" on page 28](#).

PMC Application SQL Username

This is the SQL username that will be used for all subsequent communication required between PMC and the databases. For example, **pmcsqluser**.

PMC Application SQL Password

This is the SQL username that is used for all subsequent communication required between PMC and the databases. All passwords must conform to the policy in Azure.

i For more information, please see ["Password Policy" on page 28](#).

Initial Portal Admin Username

This is the administrator username you will use to log into the PMC portal for the first time. You set this up in Azure. For example, **pmcadmin@www.example.com**.

i For more information, please see ["PMC Application User" on page 15](#).

Jump Box and Portal VM Username

This is the administrator username you will use to access the **jump box** and **portal** virtual machines that are created by the deployment script. For example, **pmcvmadmin**.

Jump Box and Portal VM Password

This is the administrator password you will use to access the **jump box** and **portal** virtual machines that are created by the deployment script. All passwords must conform to the policy in Azure.

i For more information, please see ["Password Policy" on page 28](#).

KeyVaultName

This is the name of the keyvault that will be created in Microsoft Azure. We recommend you prefix it with **PMC** . For example, **pmc-kv-mycompany** .



IMPORTANT!

This must be unique not only in your subscription, but within Microsoft Azure. The uniqueness of this name is not validated until deployment.

KeyVaultResourceGroupName

This is the name of the resource group for the **keyvault** in Microsoft Azure. For example, **pmc-kv-rg-mycompanyname** .

Location

This is the location in Microsoft Azure that you will deploy PMC to.



For more information, please see "Location for Deployment" on page 13.

Public IP Address

You can obtain your public IP address by opening a browser on your deployment machine and navigating to <https://www.whatismyip.com/what-is-my-public-ip-address/>.

ResourceGroupName

This is the name of the resource group that will be created in Microsoft Azure. We recommend you prefix it with **pmc** . For example, **pmc-rg-mycompany** .

SQL Administrator Username

This is the SQL administrator username that will be used to create the databases by the deployment script. For example, **pmcsqldadmin** . These credentials are duplicated by the deployment script to set up the PMC Management and Blob storage database, and the Enterprise Reporting database.



Note: The SQL Administration username must be different from the PMC Application SQL username, as the users are inserted into the same databases by the deployment script.

SQL Administrator Password

This is the SQL administrator password that will be used to create the databases by the deployment script. These credentials are duplicated by the deployment script to set up the PMC Management and Blob storage database, and the Enterprise Reporting

database. All passwords must conform to the policy in Azure.

i For more information, please see ["Password Policy" on page 28](#).

SSL DNS Name

This is the DNS Name of the SSL certificate you supplied, or the DNS Name of the SSL certificate that you want the deployment tool to generate. For example, **pmc.ssldns.name**.

i For more information, please see ["DNS Name of SSL Certificate Prerequisites" on page 11](#).

SSL Certificate Password

If you supplied your own SSL certificate, you are prompted to enter the password for it now.

i For more information, please see ["DNS Name of SSL Certificate Prerequisites" on page 11](#).

SSL Certificate Thumbprint

If you supplied your own SSL certificate, you are prompted to enter the thumbprint for it now.

i For more information, please see ["DNS Name of SSL Certificate Prerequisites" on page 11](#).

SubscriptionId

You made a note of this when you configured your subscription. For example, **6d01f381-e870-4964-83f3-6cc0cbb1c048**.

i For more information, please see ["Subscription ID" on page 14](#).

Password Policy

The password used during the PMC deployment must be between 8 and 16 characters, and meet at least three of the following four rules:

- Use of lowercase characters
- Use of uppercase characters
- Use of numbers (0-9)
- Use of the following symbols:

% ^ & * - _ = [] { } | : ' , . ? / ~ ()

! IMPORTANT!

Be sure to avoid use of the following symbols in the Azure deployment script, as this will break the deployment:

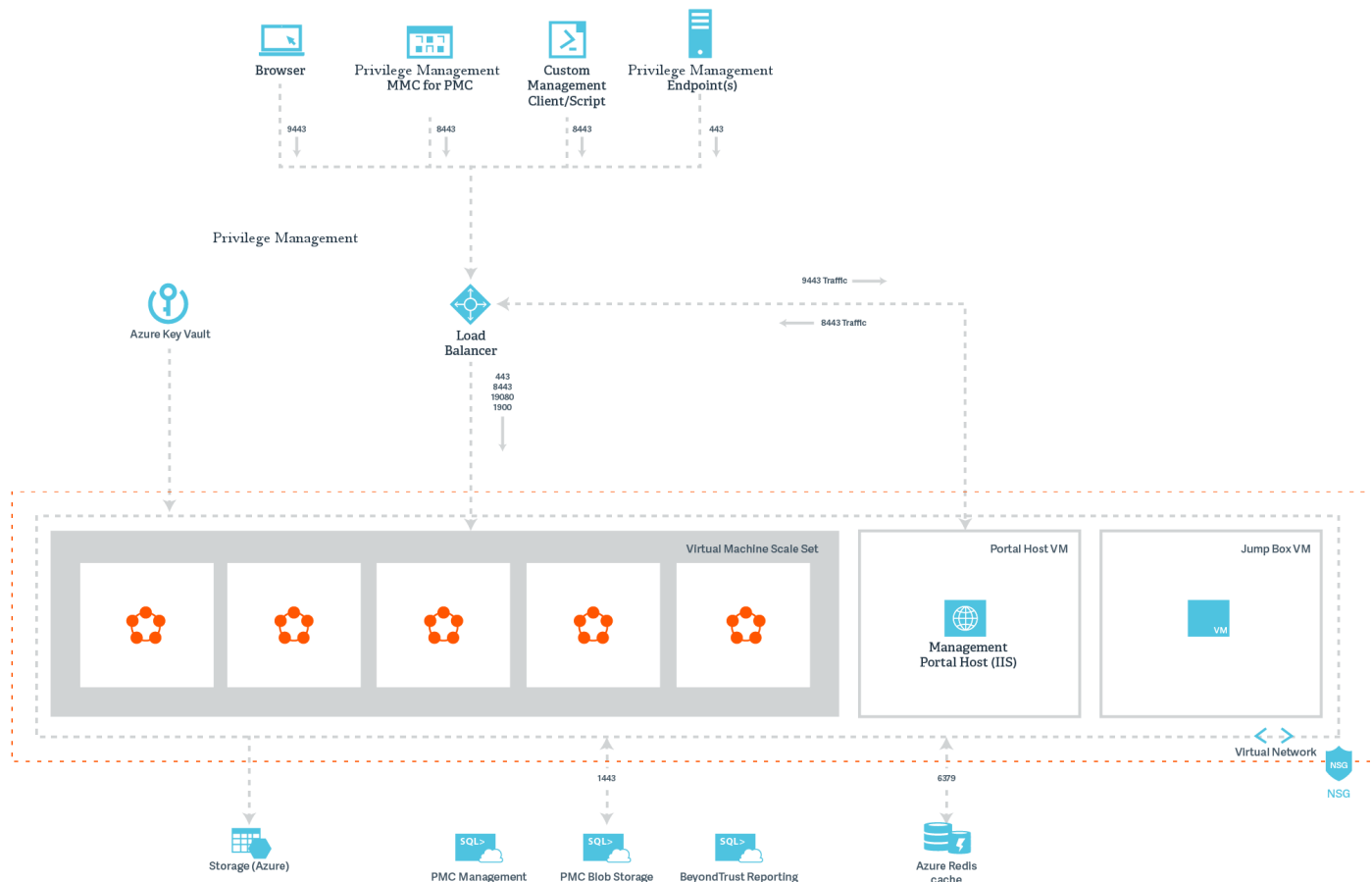
! \$ @



For best practice on choosing a strong password, please see the Microsoft article [Strong Passwords](https://docs.microsoft.com/en-us/sql/relational-databases/security/strong-passwords?view=azuresqlldb-mi-current) at <https://docs.microsoft.com/en-us/sql/relational-databases/security/strong-passwords?view=azuresqlldb-mi-current>.

PMC Architecture Overview

This diagram shows the architecture for PMC hosted in Azure.



PMC Certificates

Several certificates are generated as part of the PMC installation.

The PMC deployment process generates the following certificates:

- SSL (for evaluation deployments only)
- PMC Configuration Encipherment
- PMC Tenant Certificate Authority
- PMC Tenant Service Identity
- PMC Cluster Admin
- PMC Root

This document details where to install these certificates for your PMC deployment.



For more information on the certificate chain, please see "PMC Certificate Chain" on page 31.

SSL

An SSL certificate is required to secure communication to PMC. PMC uses SSL to secure the communication for the PMC cluster. The deployment script can generate an SSL certificate to be used for evaluation deployments, however for production deployments you must provide your own SSL certificate.

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.

PMC Configuration Encipherment

This certificate is used to encrypt and decrypt data for Service Fabric Cluster and PMC. It is required to manually encrypt strings for the web portal and Service Fabric cluster.

PMC Tenant Certificate Authority

This is the issuing certificate authority (CA) for the Tenant Service Identity certificate and the Tenant Endpoint Identity certificates, as well as the validator of them. Without it, the endpoints will not be able to get certificates to authenticate with the service. The private key strength is set to the recommended 4096-bit size.

PMC Tenant Service Identity

This certificate represents the identity of the PMC service. It is installed onto each role in the PMC service cluster. Internal communication between roles in the PMC cluster is secured using short-lived authentication tokens. This certificate is used to sign and validate these tokens.

PMC Cluster Admin

This certificate is used to secure the Microsoft Azure Service Fabric cluster. It is required to view the health of your Service Fabric dashboard.

PMC Root

As the root of the chain, this identity forms the trust anchor for subordinate elements. It is the issuer of the Tenant certificate authority. The private key strength is set to the recommended 4096-bit size.

PMC Cluster Admin

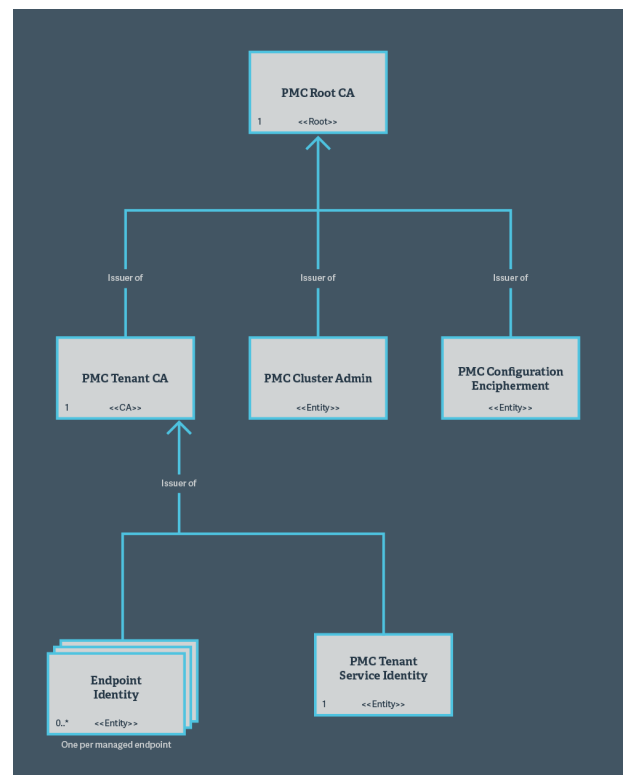
This certificate is used to secure the Microsoft Azure Service Fabric cluster. It is required to view the health of your Service Fabric dashboard.

PMC Root

As the root of the chain, this identity forms the trust anchor for subordinate elements. It is the issuer of the Tenant certificate authority. The private key strength is set to the recommended 4096-bit size.

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.



Post-Deployment Steps

You need to perform the following steps after PMC has deployed successfully:

- "Resolve DNS Settings" on page 32
- "Install your SSL Certificate" on page 33
- "Turn off Jump Box" on page 33
- "Clean Deployment Machine" on page 33
- "Remove Public IP Address from Azure Firewall Exceptions" on page 34

Resolve DNS Settings

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).

If you use a single, external load balancer, you need to add an entry in the host file that points to the IP of your **internal** load balancer and your DNS Name. If you use the external load balancer only, you need to add an entry to your host file that points to the IP of your load balancer.

You can find your internal load balancer IP address in Azure:

1. Select **Resource Groups** and locate the one that you named for the PMC deployment. For example, **PMC-rg-mycompany**.
2. Click the **Type** column to order the list by type and look for **Load balancer**. If you configured an internal load balancer as well as an external load balancer, you will see two load balancers in the list.
3. If you have configured one external load balancer (default), you will only see one load balancer in the list. Click that load balancer name to see the IP address.
4. If you configured an internal load balancer as well as the external load balancer, click the load balancer name postfixed with **internal** to see the IP address.

In this example, there is an internal load balancer configured, as well as the default external one.


<input type="checkbox"/>	NAME ↑	TYPE ↑
<input type="checkbox"/>	jumpBoxVm_OsDisk01	Disk
<input type="checkbox"/>	portalVm_OsDisk01	Disk
<input type="checkbox"/>	lbdqrm47npvyco4	Load balancer
<input type="checkbox"/>	lbdqrm47npvyco4-internal	Load balancer
<input type="checkbox"/>	jumpBoxVMNicdrqm47npvyc	Network interface
<input type="checkbox"/>	portalVMNicdrqm47npvyco4	Network interface


5. The **Public IP address** is shown on the bottom right of the **Overview** panel. To resolve your DNS Name, you can add an entry for this IP address with the DNS Name of your SSL certificate in the Portal VM **host** file and, as well as to endpoints you want to be able to connect to PMC.

Host file entry example:

```
20.37.139.54      PMC.ssl dns.name
```

Your Portal VM and Jump Box VM are listed alongside your load balancers in your resource group. They are of **Type** Virtual Machine and their names are **portalVM** and **jumpBoxVM**, respectively.

 For information on connecting to a virtual machine in Azure, please see [How to connect and sign on to an Azure virtual machine running Windows](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/connect-logon) at <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/connect-logon>.

 **Tip:** If you have configured an internal load balancer, you will need to use a VPN or peered network to complete the setup.

Install your SSL Certificate

If you use 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, before you can log into PMC, you need to install the SSL root certificate into the trusted root store of the local machine of the node where PMC is installed:

1. Copy the CER portion of the 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 required PMC certificate chain is generated for you by the PMC deployment script.

Turn off Jump Box

Once the deployment has finished and you have confirmed it was successful, you need to disable the **jump box** until you need access to it. The Jump Box was created by the deployment script.

IMPORTANT!

Do not delete the jump box. Be sure to only disable it.

Turning off the **jump box** after the PMC installation finishes decreases the attack vector of the PMC network. You can turn the **jump box** on when required.

1. Go to the Azure Portal.
2. Navigate to the resource group for this PMC installation.
3. Click the **jump box** VM.
4. Click **Stop**.
5. The machine will shutdown. To turn it back on, click **Start**.

Clean Deployment Machine

There are two steps that need to be completed on your deployment machine:

- "Deployment Folder Deletion" on page 34
- "Certificate Removal" on page 34

Deployment Folder Deletion

Before you delete your **Deployment** folder, copy the **Certs** folder to a secure location, as you will need to keep these certificates. The **Deployment** folder contains certificates and other sensitive files. You need to delete this folder from the deployment machine. You can use the PowerShell command **Remove-Item** to purge the data from your deployment machine. This function does not use the Recycle Bin.

Certificate Removal

The certificates can be retrieved from your **jump box** or the Azure key vault.

During the PMC installation, certain certificates are created and installed on the deployment machine. These should be removed from your deployment box using these instructions:

1. Open Microsoft Management Console (MMC).
2. Click **File**, and then **Add/Remove Snap-in**.
3. Select **Certificates** from the **Available snap-ins** section.
4. Click **Add >**.
5. Click **Finish**.
6. Click **OK**.
7. Expand **Certificates**.
8. Delete the following certificates from your deployment machine by right-clicking and selecting **Delete** from the context menu:
 - iC3ClusterAdmin
 - iC3ConfigurationEncipherment
 - iC3RootCA
 - iC3TenantCA
 - iC3TenantServiceIdentity
 - iC3SSL
9. Save and close the MMC.

Cluster Admin

A certificate called **ClusterAdmin** is also installed during the PMC deployment process. It is used when connecting to the ServiceFabric instance within the PMC network. There is no security risk in keeping this certificate on your deployment machine. In addition, you need to install this certificate to view the health of your service fabric cluster.

Remove Public IP Address from Azure Firewall Exceptions

The PMC infrastructure setup script creates a firewall exception for your public IP during setup. Follow these steps to remove the exception:

1. Go to the Azure Portal.
2. Navigate to the resource group for this PMC installation.

- [illegible]

-
- The screenshot shows the Azure portal interface for managing a SQL server. The left-hand navigation pane includes sections for 'Overview', 'Security', and 'Firewalls and virtual networks'. The 'Firewalls and virtual networks' section is expanded, showing options like 'SQL elastic pools', 'Deleted databases', 'Import/Export history', 'Properties', 'Locks', and 'Automation script'. The main content area is titled 'sql3ca02c7b0 - Firewalls and virtual networks' and contains a 'Connections' tab. This tab displays a list of connections. The first connection, 'Allow Client IP to SQL', is highlighted. It shows the 'RULE NAME' as 'Allow Client IP to SQL', the 'START IP' as '193.240.130.178', and the 'END IP' as '193.240.130.178'. A 'Delete' button is visible next to the connection name. Below the list, there is a note about connections from the VNET/Subnet.

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 pane. This information can be combined with the logs to troubleshoot PMC, if required.

You can view the health of your Microsoft Service Fabric cluster using your **jump box** or another machine that can connect to PMC. To do so, you must install the PMC Cluster Admin certificate.

Install the PMC Cluster Admin Certificate

1. Locate your **IC3ClusterAdmin.pfx** file either from the **Certs** folder in the deployment machine or where you copied it to.
2. On the machine you want to use to view the Service Fabric Cluster, double-click the certificate file and select **Current User**. Click **Next**.
3. The path to the certificate is populated automatically as you run the certificate. Click **Next**.
4. Enter the password for the 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 the Service Fabric Dashboard

Use the following URL to view the status of your Service Fabric cluster. Replace **PMC.ssldns.name** with the DNS name used for the PMC service (should match your SSL certificate). You can obtain this from Azure. This link will work on the **jump box** but if you want to use it on any other machine, you need to manually configure the firewall port **19080** to allow communication.

```
https://<ssldns>:19080
```

You need to choose your PMC Cluster Administration certificate to authenticate with when you browse to the URL if you are using Google Chrome. On some versions of Google Chrome, you may need to use incognito mode to view the Service Fabric Health dashboard.

Log in and Configure PMC

To log into PMC:

1. Navigate to the Server URL of PMC. It is the DNS Name of your SSL certificate with the PMC port number of **9443** appended to it. For example, **https://ssldns:9443/**.
2. Enter the user name and password you set as your portal administrator. For example, **PMCAadmin@companyname.onmicrosoft.com**. These credentials are in your Azure Active Directory.
3. 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 "[Connect PMC to Policy Editor](#)" on page 38.



For instructions on extracting the PMC Portal logs, adapter logs, and node logs, please see "[Logs](#)" on page 48.

Connect PMC to 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. Use the same GUID when you configure the MMC. This is the **MMC Client ID** in the MMC.

REMOTE ACCESS SETTINGS

☒ Enable remote MMC client access

MMC Client ID

df215e17-a5c3-4d3a-8023-415e636f44e5



☒ Enable Remote API Access

API Access ID

b476bb1d-937f-470b-b7de-906df4bb19ec

API Key

aR9+g3E3o7y/uBv2btjImObrx2mO5SCrYpqhJD0rUNrr1UjjghvNlgsKVjQ767V/F68omcdxB/HMDHMMMP4RHA==

New

Save Changes

Cancel



Note: There are many ways to generate a GUID. For example, you can use a PowerShell cmdlet:

```
new-guid
```

3. Check the **Enable API key access** box. This GUID is required if you want to use the PowerShell API. Once again, you need to generate this GUID.

Now that 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.

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**.

You can obtain these downloads from the BeyondTrust Connect portal.



For compatible versions, please see the [Release Notes](https://www.beyondtrust.com/support/changelog) at <https://www.beyondtrust.com/support/changelog>.

Add and Configure the Privilege Management PMC 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 Management PMC snap-in for the MMC:

1. Run **mmc.exe** from the **Start** menu.
2. Navigate to **File > Add/Remove Snap-in** and select **Privilege Management Settings (PMC)**. Click **Add**.
3. Click **OK**.



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.

PMC Connection

Connection

Server URL

https://pmc.example.com/

Tenant ID

33bff851-eec4-47d7-ae05-852143f0aadf

Port

443

[Test URL](#)

Authorization provider

URL

https://pmc.example.com:8443/oauth

[Test URL](#)

Identification

MMC Client ID

a6255a36-2910-4596-bfba-49f80e7b63bf

Client Return URI

http://defendpoint-mmc.com

☒ Amend token resource ID

URL

https://api.pmc.avecto.com

If you change this value, you'll also need to update the value in your server configuration

i

Tenant ID can be found in the configuration of your server hosting provider.

The MMC Client ID and Client Return URI can be found in the settings of your authorization provider. The MMC Client ID must also match the one in "Remote Access Settings" within the PMC web interface.

OK

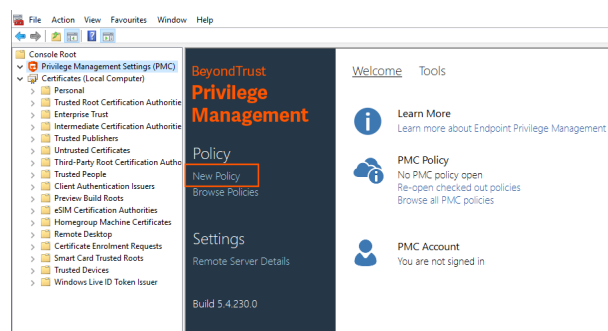
Cancel

Setting	What to Enter
Connection	
Server URL	The URL for PMC with 8443 in the Port field.
Tenant ID	The Tenant ID GUID that you are using to authenticate with PMC. You can obtain it from Microsoft Azure for Azure Directory authentication.
Authorization Provider	
URL	The URL for PMC with :8443/oauth appended to it.
Identification	
MMC Client ID	<p>This needs to be the same GUID you generated and used in the PMC connection settings called Application ID.</p> <div style="border: 1px solid orange; padding: 10px; margin: 10px 0;"> <p>i For more information, please see "Connect PMC to Policy Editor" on page 38.</p> </div> <p>There are many ways to generate a GUID. For example, you can use a PowerShell cmdlet:</p> <pre>new-guid</pre>
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.PMC.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 MMC 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.



For more information on endpoint management, please see the [PMC Administration Guide](https://www.beyondtrust.com/docs/privilege-management/windows.htm) at <https://www.beyondtrust.com/docs/privilege-management/windows.htm>.



IMPORTANT!

Install Privilege Management 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.



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.

Privilege Management Clients

You need to choose your Privilege Management client as described below.

For Windows endpoints

- For 32-bit (x86) systems, run **PrivilegeManagementForWindows_x86.exe**.
- For 64-bit (x64) systems, run **PrivilegeManagementForWindows_x64.exe**.

You can also install the Privilege Management for Windows MSI in silent mode with the PMC switch enabled:

```
Msiexec.exe /i PrivilegeManagementForWindows_x.xxx.x.msi IC3MODE=1 /qn /norestart
```

This will install the Windows client in silent mode with the PMC switch enabled.

For Mac endpoints

- Run **PrivilegeManagementConsoleMacOSAdapter.dmg**.



For compatible versions, please see the [Release Notes](https://www.beyondtrust.com/support/changelog) at <https://www.beyondtrust.com/support/changelog>.

Privilege Management Adapters

You can choose to automatically assign endpoints to groups and authorize them in one step using the **GroupID** parameter for the Windows adapters. PMC computer groups should be created in PMC prior to installing agents on a large scale. You should work with

your implementation consultant to determine the best computer grouping approach for your needs.

The Privilege Management adapters are installed using the command prompt in Windows or the terminal for Mac.



For more information, please see ["Install the Windows Adapter for PMC" on page 44](#).



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.

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](https://support.microsoft.com/en-gb/help/4472027/2019-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 instructions on getting this GUID for Microsoft Azure authentication, please see ["Directory ID" on page 14](#).

- **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.

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

The computers with Privilege Management and 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 Windows Directory and LDAPS, this GUID is generated for you by the deployment tool and you should already have a note of it.

i For more information on getting this GUID for Microsoft Azure authentication, please see ["Directory ID" on page 1](#).

- **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-b9566250cfd" 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 three locations where you can extract logs:

- **Portal Logs**
- **Node Logs**
- **Adapter Logs**

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

Portal Logs

1. Log into the portal VM remote machine from Azure with the credentials you set up when you deployed PMC.
2. Navigate to the following directory: **C:\inetpub\wwwroot\iC3\Logs**. This file is appended to at run-time, so you need to close it to refresh it.

The portal logs should be checked if there are any issues logging into the portal, or if the Service Health Fabric isn't healthy.

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**
- **All Nodes Using PowerShell**

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 from Microsoft Azure 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

This method may be used to script the request of logs from every node for support purposes.

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**. Click **OK** and then **Next**.
8. Click **Finish** to complete the certificate installation.

You may need to modify the hosts file so it can resolve the DNS Name of your PMC instance.

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.ps1** 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:\PMCl**ogs.

i For details on how to obtain the certificate thumbprint if it is required, please see [How to: Retrieve the Thumbprint of a Certificate](https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/how-to-retrieve-the-thumbprint-of-a-certificate) at <https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/how-to-retrieve-the-thumbprint-of-a-certificate>.

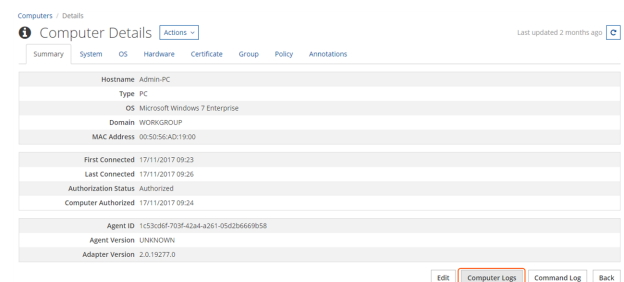
4. Press **Enter** to run the PowerShell script and download the files to the chosen location.

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 an Azure Deployment

There are several steps you need to go through for the Azure deployments. Be sure to download the **AzurePaaS** folder for the version of PMC that you are upgrading to. It is in the **File Downloads** area of the [Customer Support Portal](#), at

<https://beyondtrustcorp.service-now.com/csm>.



IMPORTANT!

You must upgrade your reporting database to 5.4 in order to use PMC 2.3.

Turn on your Jump box

You need to use your **jump box** to upgrade your Azure deployment. You should have disabled this after you deployed PMC. To re-enable it:

1. Go to the Azure Portal.
2. Navigate to the resource group for this PMC installation.
3. Click the **jump box** virtual machine (VM).
4. Click **Start**.
5. The machine will now start up. To turn it back off, click **Stop**.

Upgrade the Database

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

Prerequisites

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, proceed to the application.



For more information, please see the following:

- "Upgrade the Application" on page 51.
- [Release Notes](https://www.beyondtrust.com/support/changelog) at www.beyondtrust.com/support/changelog.

Upgrade Process

1. Go to the Azure Portal.
2. Navigate to the Resource Group for this PMC installation.
3. Click the **Type** column header to order the list by type.
4. Click the SQL database called **Avecto.IC3.Management** (with some characters post-fixed).
5. Locate the **Server name**. This is shown on the top right:

Resource group (change)	: dfyazure-RG	Server name	: sqlc3pwoyppquq7bu.database.windows.net
Status	: Online	Elastic pool	: No elastic pool
Location	: East US 2	Connection strings	: Show database connection strings
Subscription (change)	: Avecto	Pricing tier	: Standard S2: 50 DTUs
Subscription ID	: 78b035aa-1d27-4617-afab-b2639a3c6614	Oldest restore point	: 2019-01-23 00:00 UTC
Tags (change)	: displayName : Database		

6. Using SQL Server Management Studio, log into the database using the **Server name** from Azure and the SQL administration credentials you created when you deployed PMC.
7. After you have successfully connected, expand the **Databases** node under **Object Explorer**, right-click on the **Avecto.IC3.Database.Management** database and click **New Query**.
8. Select **File > Open > File** and navigate to the **AzurePaaS\DeployDatabases\SQL** folder for the version you are upgrading to.
9. Locate the **Avecto.IC3.Database.Management.sql** script. This contains all the database migrations required to perform an upgrade.
10. 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

Enable WinRM with SSL on the Portal VM

1. Connect to your Portal VM and copy the **Enable-WinRMWithSSL.ps1** script from the **AzurePaas** folder to the Portal VM.
2. Run PowerShell as an administrator and navigate to the location of **Enable-WinRMWithSSL.ps1**
3. Type **.\Enable-WinRMWithSSL -SubjectName portalVm -ForceNewSSLCert**.

Perform Upgrade on the Jump Box VM

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

1. On the Jump Box VM that you turned on, copy the **Upgrades** folder from the build you wish to upgrade to onto the Jump Box. 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 *"Change Application Parameters Before Upgrade"* on page 56.

2. Copy your **ClusterAdminCert.pfx** file to the Jump Box. This certificate should have been placed in a secure location after the deployment and removed from the Jump Box.



For more information, please see *"Post-Deployment Steps"* on page 32.

3. Import the certificate into your **Current User > Personal** location.

If you changed the default location of the Portal when you installed PMC, you need to provide the following argument to the upgrade script before you run it:

```
-PortalWebsiteVmLocation "C:\MyFolder\PMC"
```

4. 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\PMC"**. When you press **Enter**, 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 **Enter**.

- **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 output during the deployment for the PMC Cluster Admin certificate (same as the **ClusterAdminThumbprint**).
- **PortalVmAdminUsername**: The administrator username for the portal machine that was entered in the initial deployment.
- **PortalVmPassword**: The password for the portal machine that was entered in the initial deployment.
- **PortalVmIpAddress**: The IP address of the portal machine.
- **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 will need to be saved to a secure location in case these values are needed. In the event that they are needed, the required value will need to be copied from this text file into the config file.

 **IMPORTANT!**

Skip the next step if you are upgrading from 2.3 or higher, and continue with the step that follows.

5. When upgrading from a version prior to 2.3, run the **EnableDatabaseAutoindexing.ps1** script in the **Upgrades** folder and provide the following parameters:
 - **enciphermentCertificateThumbprint**: The certificate thumbprint for the applications encipherment certificate.
 - **managementSqlAdminLogin**: The username for a privileged user account on the PMC Management Database. This privileged user account requires **ALTER SCHEMA** permissions.
 - **managementSqlAdminLoginPassword**: The password for the privileged user account in the PMC Management Database.
 - **erSqlAdminLogin**: The username for a privileged user account in the Reporting database.
 - **erSqlAdminLoginPassword**: The password for the privileged user account in the Reporting database.
 - **appParametersFilePath**: The full path to the application parameters file, **ParametersConfigFilePath**, which is referenced in the previous step.

The script prompts the user with *Do you want to retrieve database server connection details from your Azure subscription (requires login)? Y/N.*

- **Y:** The Azure login screen will display before the remainder of the script runs.
- **N:** The script will prompt the user with *Please enter the PMC Management Database server (e.g. sqlpmcgggds.database.windows.net, followed by Please enter the Enterprise Reporting Database server (e.g. sqlerdfgfagds.database.windows.net).*

The script adds two new entries to the application parameters file, **Production.5Node.xml**, which contains encrypted connection strings for the privileged accounts for the PMC management and Reporting databases. The file can then be used in step 7. In addition, the script connects to the management database and changes the **AutoIndexMaintenanceEnabled** system parameter from **0** to **1**, enabling the auto-index feature.

6. Copy the **Package.zip** folder from the **AzurePaaS** folder (the version you are upgrading to) to your Jump Box and unzip it.
7. 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.5Node.xml** file in the **Upgrades** folder. For example, **C:\Users\myuser\Desktop\Upgrades\Production.5node.xml**.
 - **ClusterAddress:** Your DNS with **:19000** applied at the end. For example, **PMCTest.example.com:19000** (no **HTTPS://** prefix needed).
 - **ClusterAdminThumbprint:** The thumbprint output during the deployment for the PMC Cluster Admin certificate.
 - **ServerCertThumbprint:** The thumbprint output during the deployment for the PMC Cluster Admin certificate (same as the **ClusterAdminThumbprint**).
8. The script will run and begin the upgrade process. To check the progress, navigate to Service Fabric 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, Service Fabric 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 have upgraded to.

Upgrade Issues

Should an upgrade run and fail, 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.

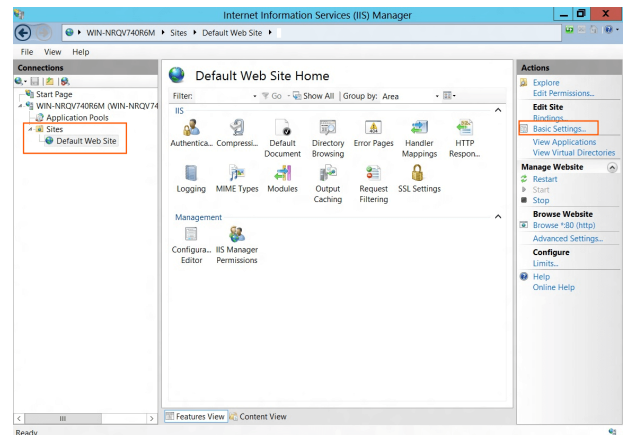
If you receive an error that states *Application type and version already exists at <path>*, then the error is due to the previous failed run leaving the application type and version provisioned in Service Fabric. Running the script again will clash as it is the same version.

The script 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 rerunning 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 onto Portal VM.
2. Create a new folder under **C:\inetpub\wwwroot** named with the new version number.
3. Open the zip file you downloaded from the [Customer Support Portal](#), navigate to the **Azure Paas\DeployPortal\SupportFiles** folder, and copy the contents of the **Portal.zip** file 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**, then to your PMC Portal.
6. In the **Actions** menu under **Basic Settings**, select the new physical path you have created and click **OK**.



Upgrade Privilege Management Reporting

This guide assumes there is a working installation of the Privilege Management Reporting 4.0 or later installed.

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]
```

Change Application Parameters Before Upgrade

You can use the script to update values in both the **Production.5Node.xml** or the **Web.config** file that are provided as part of the upgrade in the **AzurePaaSUpgrade** 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.5Node.xml** file, use the following command:

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

For example:

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

Rotate the SSL Certificates

Prior to your certificates expiring, you need to rotate them. This section details how to achieve this with Azure PaaS deployments.

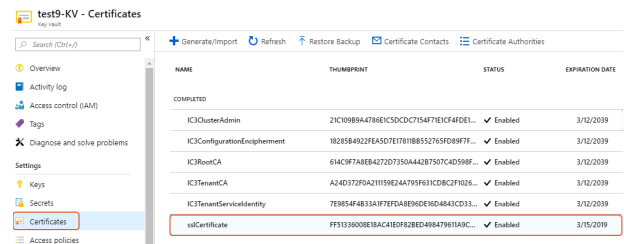
Import the Certificate Into your KeyVault

1. Log into Microsoft Azure.
2. Navigate to **All Resources** and order the list by **Type**.
3. Locate the KeyVault associated with your PMC environment and click it.

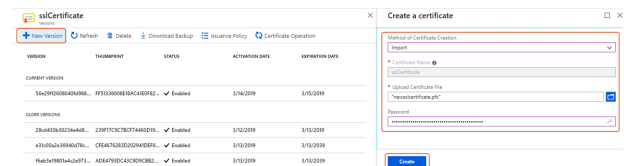


Note: If you don't see the certificate you may need to modify the permissions of the user. Click **Access Policies** and add your user with the **Certificate Management Operations > Get, List, and Import**.

4. Select the **sslcertificate** in the list and click **New Version**.



5. Select **Import** from **Method of Certificate Creation**.
6. Select your new SSL certificate pfx file in the **Upload certificate file** dialog box.
7. Enter the SSL certificate password and click **Create**.
8. Once the certificate has been created, click it in the list of certificates.
9. From the properties, make a secure note of the **X.509 SHA-1 Thumbprint**, **Key Identifier**, and **Secret Identifier**.



X.509 SHA-1 Thumbprint (in hex)

8F745732DA2BBF0A1CDF8D33EF7519EAD9830FE

Key Identifier

https://ic3dr.vault.azure.net/keys/sslcertificate/46ecf8d8bc28451e9c847685e7fa41e1

Secret Identifier

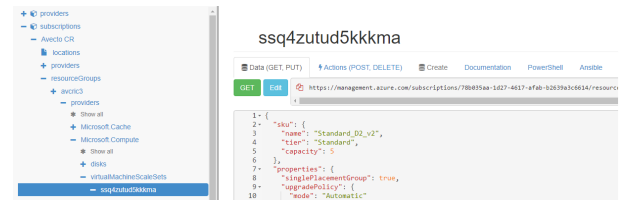
https://ic3dr.vault.azure.net/secrets/sslcertificate/46ecf8d8bc28451e9c847685e7fa41e1

Update the Scale Set ARM Template

In order for the new certificate to be pushed to the virtual machines in the scale set:

1. Log into Microsoft Azure.
2. Navigate to <https://resources.azure.com/> and select the subscription where your PMC instance is deployed.
3. Click **Read/Write** to the right of that dropdown.

- On the left, select **subscriptions > resourceGroups > your resource group > providers > Microsoft.Compute > VirtualMachineScaleSets** and select the scaleset.



- Click **Edit**.
- Navigate to the **virtualMachineProfile.Secrets.vaultCertificates** array.



- Add the following text to the end. Do not overwrite the existing SSL Certificate URL; add this as a final new entry in the array, replacing the **\$secretidentifier\$** with the secret identifier obtained from the KeyVault.

```
{
  "certificateUrl": "$secretidentifier$",
  "certificateStore": "My"
}
```

- Click **Put**. You will see a green tick when the action has completed.

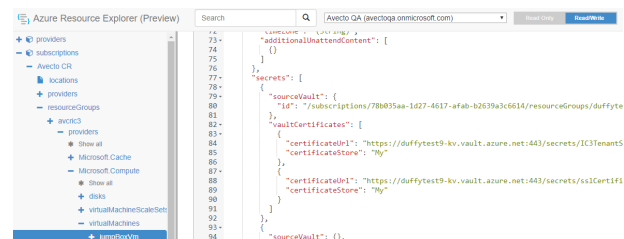


Note: You can confirm that this update has completed by clicking **instanceView** from the scale set menu on the left. Once it has completed, the time and date stamp will be updated.



Update the Portal/Jumpbox VMs ARM Template

- Navigate to <https://resources.azure.com/> and select the subscription where your PMC instance is deployed.
- Click **Read/Write** to the right of that dropdown.
- On the left, select **subscriptions > resourceGroups > your resource group > providers > Microsoft.Compute > VirtualMachines**, and select either the **PortalVM** or the **JumpBoxVM**. You need to repeat these steps for both virtual machines.



- Click **Edit**.
- Navigate to the **osProfile.secrets.vaultCertificates** array as before.
- Add the following text to the end. Do not overwrite the existing SSL Certificate URL; add this as a final new entry in the array, replacing the **\$secretidentifier\$** with the secret identifier obtained from the KeyVault.

```
{
  "certificateUrl": "$secretidentifier$",
  "certificateStore": "My"
}
```

- Click **Put**. You will see a green tick when the action has completed.



Tip: You can confirm that this update has completed by clicking **Instance View** from the scale set menu on the left-hand side. Once it has completed, the time and date stamp will be updated.



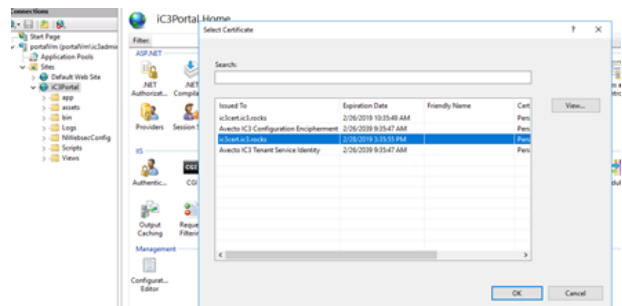
Note: Ensure you have completed the steps above for both the **PortalVM** and the **JumpBoxVM**.

Configure Internet Information Services (IIS)

- Open a remote desktop session to the PortalVM either from the Jump Box or by downloading the RDP file from Azure.
- Open Internet Information Services (IIS).
- Select **IC3Portal** from sites.
- Click **Bindings** on the right.
- Edit the single binding for port 9443. In the certificate, click **Select**.
- Select the new SSL certificate and click **OK**.



Tip: You can typically identify the new SSL certificate by examining the expiration dates and choosing the one that is most distant.



Make the PMC Application Configuration Changes

- Remote desktop onto JumpBox (ensure you have the Cluster Administration *.pfx certificate portion installed on the machine before continuing).
- The setting for the SSL Thumbprint 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.

For example:

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

2. 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**).
3. Once the upgrade is complete, you can check access from the portal. You can monitor the upgrade to the application using Service Fabric explorer.

Perform Database Backups for Long-Term Retention

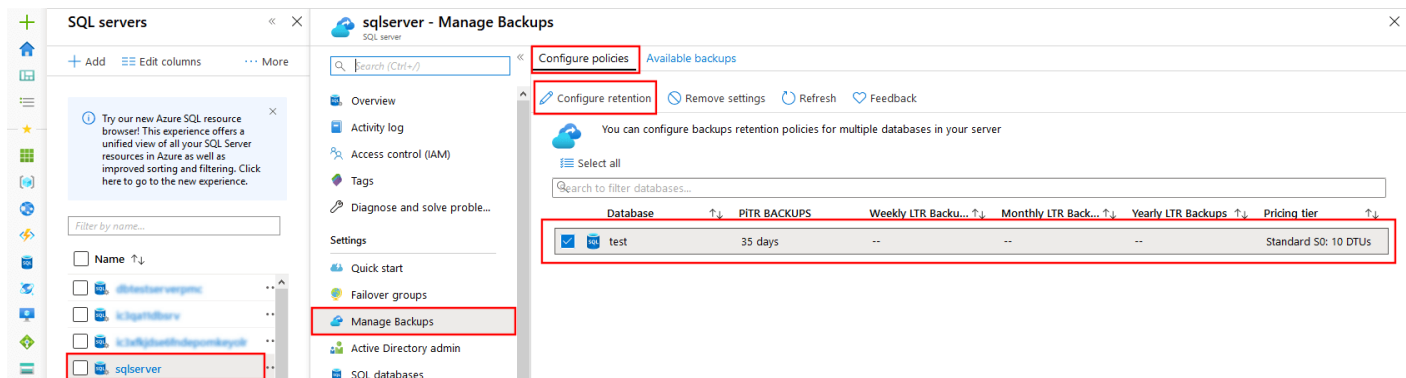
By default, a Privilege Management implementation in Azure has Point In Time Recovery (PITR) enabled for seven days. However, if you wish to enable a long-term backup retention policy (LTR) for any of your Management, Blob, or Reporting databases, you may configure the policy to retain backups in separate Blob storage containers for up to ten years.



Note: Microsoft provides LTR backup services at an additional cost. You can use the [Azure pricing calculator](#) to learn more.

Enable LTR for a database

1. In the Azure portal, navigate to **Azure Services > SQL servers**.
2. Select the SQL server that contains the database you wish to back up.
3. Click **Manage Backups**.
4. Ensure you are on the **Configure policies** tab.
5. Check the box to select the desired database.
6. Click **Configure Retention**.



Database	PITR BACKUPS	Weekly LTR Backups	Monthly LTR Backups	Yearly LTR Backups	Pricing tier
<input checked="" type="checkbox"/> test	35 days	--	--	--	Standard S0: 10 DTUs

7. In the **Configure policies** pane, check any of the **Weekly**, **Monthly**, or **Yearly LTR Backups** boxes, and choose the retention period for each.
8. Click **Apply**.

Configure policies

SQL server

Point In Time Restore Configuration

Configure PITR backup retention Days

Long-term Retention Configurations

☒ Weekly LTR Backups ⓘ
 How long would you like weekly backups to be kept?

2 Week(s)

☒ Monthly LTR Backups ⓘ
 How long would you like the first backup of each month to be kept?

2 Month(s)

☒ Yearly LTR Backups ⓘ
 Which weekly backup of the year would you like to retain?

Week 52

 How long would you like this annual backup to be kept?

1 Year(s)

Apply

Cancel

Once you have made a backup, you can restore it from the **Manage Backups** pane, on the **Available backups** tab.



For more information, please see [Manage Azure SQL Database long-term backup retention](https://docs.microsoft.com/en-us/azure/sql-database/sql-database-long-term-backup-retention-configure) at <https://docs.microsoft.com/en-us/azure/sql-database/sql-database-long-term-backup-retention-configure>.

Apply Windows Updates

This section details how to manage your Windows Updates on the servers running PMC.

To manage Windows updates for PMC, you need to install the Service Fabric Patch Orchestration application into the Service Fabric Cluster.



For more information, please see [Patch the Windows operating system in your Service Fabric cluster](https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-patch-orchestration-application) at <https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-patch-orchestration-application>.

We recommend you use the Service Fabric Patch Orchestration application to perform updates, as it ensures that the updates only take one node of the cluster offline at a time.

PMC Supporting Scripts

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

- "Deactivate Duplicate Agents" on page 64
- "Deactivate Inactive Agents" on page 65
- **NodeDiagnosticsLogsDownload**



For more information, please see *Cluster Node Service Logs* at "Logs" on page 48.

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**: The **Application ID** that is below the **Enable API key** access check box in the **Remove Access Settings** page in PMC.
- **client_secret**: The **API Key** in the **PMCSettings** page.
- **tenant_id**: The GUID for Microsoft Azure authentication. For Windows Directory and LDAPS this is generated by the deployment tool; you should have already made a note of this.



For instructions on getting the **tenant_id**, please see ["Directory ID" on page 14](#).

- **cloudServiceDnsName**: The PMC URL. Do not include **https://** or the port when entering. For example, **PMC.example.com**.
- **platformApiPort**: The port number the API uses. It is usually 8443.

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>"
```

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**: The **Application ID** that is below the **Enable API key** access check box in the **Remove Access Settings** page in PMC.
- **client_secret**: The **API Key** in the **PMCSettings** page.
- **tenant_id**: The GUID for Microsoft Azure authentication. For Windows Directory and LDAPS this is generated by the deployment tool; you should have already made a note of this.



For instructions on getting the **tenant_id**, please see ["Directory ID" on page 14](#).

- **cloudServiceDnsName**: The PMC URL. Do not include **https://** or the port when entering. For example, **PMC.example.com**.
- **inactiveDays**: The number of days the tenant has been inactive. The minimum is 15.
- **platformApiPort**: The port number the API uses. It is usually 8443.

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>"
```