Privilege Management
iC3 On Premises Installation Guide
2.2.35697.0 GA

Powered by Avecto

Table of Contents

Attributes to Record

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

- "Certificate Passwords" on page 6
- Azure AD Authentication only - "Attributes Defined and Used for all Types of Authentication" on page 6

Certificate Passwords

Several passwords are generated by the deployment wizard. You must make a note of these when prompted as well. Failure to note these passwords down will mean that you won't have the passwords for your certificates and won't be able to install them anywhere else These are all defined on the Certificates tab, please see "Certificates Tab" on page 20 for more information.

Attributes Defined and Used for all Types of Authentication

Attribute Name	Defined	Used
Server URL	This is the DNS of your SSL Certificate with ':9443' appended to it. It's displayed in full on the "Finish Tab" on page 25	"Log into iC3" on page 31 "Configure Endpoints" on page 35
Tenant ID GUID	This is displayed on the Authentication tab for Windows Active Directory and LDAPS authentication, see "Authentication Tab" on page 20 for more details. For Azure Active Directory authentication, see "Create the Azure AD Tenant" on page 11.	"Authentication Tab" on page 20
Authorization Provider	This is the URL for iC3 with ':8443/oauth' appended to it. This is shown on the Finish tab of the deployment wizard, see "Finish Tab" on page 25 for more details.	.
iC3 Portal Application ID	Only required for Azure Active Directory authentication, see "Obtain the GUID for your Portal Application" on page 14	"Authentication Tab" on page 20
iC3 Portal Key	Only required for Azure Active Directory authentication, see "Generate a Key for your Application" on page 13	"Authentication Tab" on page 20

Prerequisites

There are several prerequisites prior to running the iC3 deployment wizard. Please review each section before you start your deployment:

If your deployment is being managed by Professional Services please ensure you specify any naming convention prior to deployment commencing as service names cannot be changed after deployment.

- "Machine Prerequisites" on page 8
- "User and Domain Prerequisites" on page 10
- "SSL Certificate Prerequisites" on page 10
- "Authentication Prerequisites" on page 11
- "Report Database Prerequisite" on page 15
- "iC3 Management Database Prerequisites" on page 16

Machine Prerequisites

iC3 must be deployed from a local or mapped drive on your computer. Prior to starting the deployment of iC3, ensure that you copy the iC3 deployment media to a local or mapped drive.

You need three types of machine for the iC3 deployment:

- "Deployment Machine" on page 8
- "Cluster Nodes" on page 8
- "SQL Server Machine" on page 9

***Note:** Ensure you take snapshots of your virtual machines prior to deployment so you can rollback in case of any issues. For hardware specifications, see "Hardware Sizes" on page 52.*

The iC3 deployment tool installs a specific version of the Service Fabric Runtime, it is not a prerequisite. The iC3 deployment tool will fail if it's already installed. Once you have deployed iC3 to your cluster, do not upgrade the Service Fabric Runtime unless BeyondTrust has confirmed that it is compatible.

Ensure that there are no pre-existing security products and or restrictive GPOs are present on these servers that can interfere with the install. Once iC3 is installed, the security products and settings can be restored back to the nodes.

***Tip:** When you introduce new media to a machine it is quite 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**, then on the **General** tab, check the **Unblock** box. Click **OK**.*
- *Within PowerShell, and from the root folder of the build media following extraction, type:* `dir -recurse | unblock-file`

Deployment Machine

The Deployment machine needs to be running Windows 10, Windows Server 2012 R2 or Windows Server 2016.

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

Cluster Nodes

The iC3 deployment supports three or five node deployment. Each deployment node needs to be running Windows Server 2012 R2 or Windows Server 2016. The iC3 Deployment Wizard installs Microsoft Service Fabric on each node, you do not need to install this as a prerequisite.

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

- 8443
- 9443
- 19080

- 19000
- 1433

SQL Server Machine

The SQL Machine is used for both the iC3 management databases and reporting database, if configured. The SQL Server machine needs to be running SQL Server 2012 R2 or SQL Server 2016. You also need to install SQL Server Management studio to manage your databases.

You need a SQL account with administration rights for the iC3 database creation. SQL server also needs to be in **Mixed** mode to allow for the use of a SQL account.

If you are using reporting, you also need to install the Privilege Management Enterprise Reporting database prior to running the iC3 deployment wizard as the wizard configures the connection to the Privilege Management database for you. See "Report Database Prerequisite" on page 15 for more information.

> ***Note:*** *SQL Server Express is not supported.*

User and Domain Prerequisites

iC3 supports two types of deployment; domain-joined machines and machines that are not connected to a domain:

- "Domain Installs" on page 10
- "Non-domain Installs" on page 10

Computers being managed by iC3 need to be on the network to communicate with the service.

Domain Installs

The iC3 deployment wizard must be run as an Administrator user on the deployment machine. The iC3 deployment wizard requires a domain user account that is part of the Administrators group on all the service fabric deployment nodes and the SQL machine.

You can use a different account for running the iC3 deployment wizard providing it is an administrator on the deployment machine.

Non-domain Installs

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

In addition, you need to run the script 'Enable-WinRMwithSSL.ps1' on each iC3 deployment node using the account that is a member of the Administrators account. This enables WinRM which is required for the deployment to succeed. This script can be found in the 'Deployment' folder.

SSL Certificate Prerequisites

You need an SSL certificate for production deployments. Wildcards are not supported for production deployments. The iC3 deployment wizard can generate an SSL certificate for evaluation deployments.

> ***Note:*** *The DNS of the SSL certificate forms the URL for iC3 so you should be able to relate it to iC3.*

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

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

If you are using an SSL certificate that is trusted by a global provider you do not need to do any further steps. If your SSL certificate is not trusted by a global provider you need to install the root of your SSL certificate into the trusted root of the local machine of the node where you install iC3 before you can log in to iC3:

To install the root of your SSL certificate:

1. Copy the CER portion of your root certificate to the node where you installed iC3. 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 iC3 certificate chain that is required is generated for you by the iC3 deployment wizard.

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

Authentication Prerequisites

iC3 supports three types of authentication:

- Windows Active Directory, no iC3 specific prerequisites required
- Lightweight Directory Access Protocol Secured (LDAPS), no iC3 specific prerequisites required
- Microsoft Azure Active Directory, see the "Microsoft Azure AD Authentication" on page 11 section

You need to know your method of authentication and configure it for iC3 prior to running the iC3 deployment tool as some of the authentication settings are required. You also need to know the DNS for your SSL Certificate, this forms your Portal URL when combined with the iC3 port number '9443'.

Microsoft Azure AD Authentication

You need the following components in Microsoft Azure to use it to authenticate with iC3:

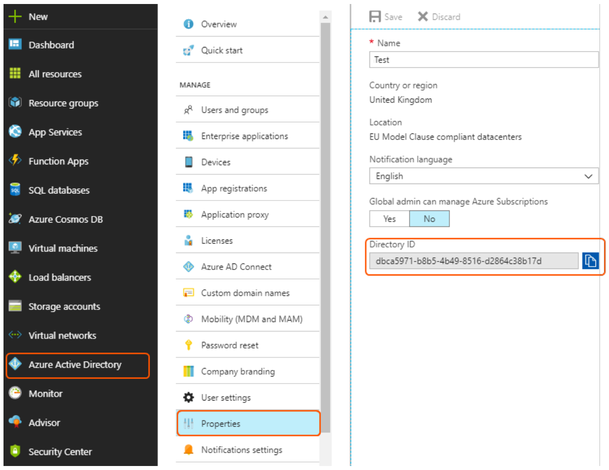
- "Create the Azure AD Tenant" on page 11
- "Create your User in the Tenant" on page 12
- "Create the iC3 Application" on page 12

Create the Azure AD Tenant

You need a subscription in Microsoft Azure AD to use it for iC3 authentication. By default you have a tenant as part of your subscription. You can either use this default tenant or you can create a new tenant to hold your iC3 applications.

Obtain the GUID for your Tenant

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



* Name
Test

Country or region
United Kingdom

Location
EU Model Clause compliant datacenters

Notification language
English

Global admin can manage Azure Subscriptions
Yes [✓ No]

Directory ID
dbca5971-b8b5-4b49-8516-d2864c38b17d

*Record this Directory ID GUID as it is your Tenant ID for Azure. You need to paste it into the iC3 deployment tool on the **Authentication** tab and enter it in to iC3 to configure the connection.*

Create your User in the Tenant

You need to define the username for the user that will log into iC3 for the first time. You can use the default username provided with your tenant or create a new one.

```
username@directoryname.onmicrosoft.com
```

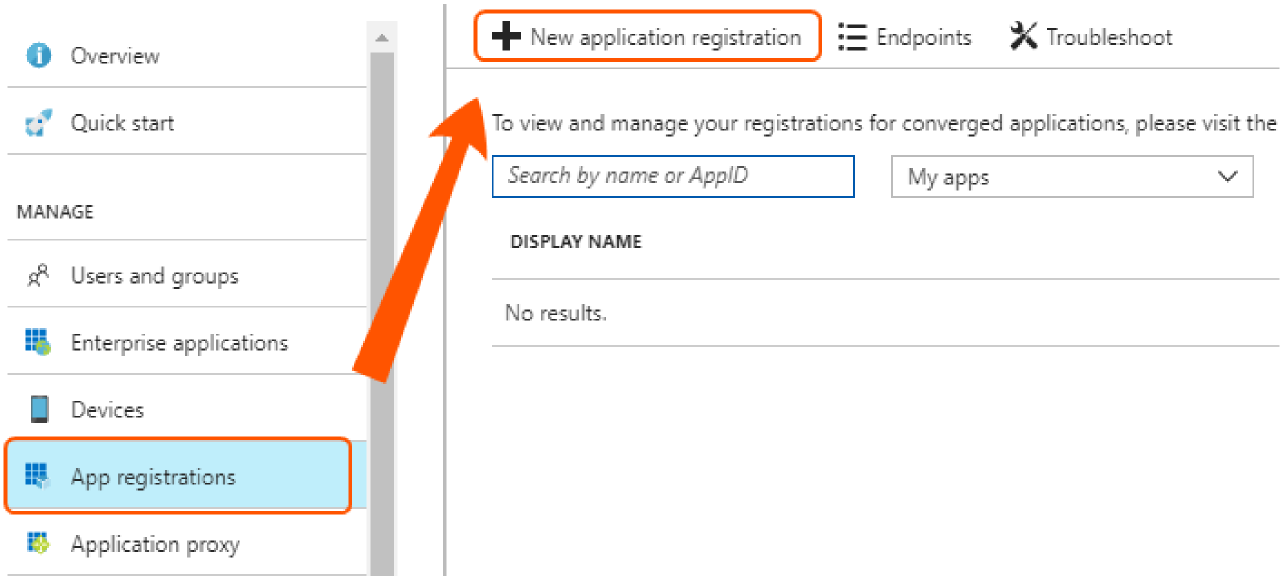
To create a new user:

1. Ensure you are in the Active Directory Tenant that you are using for iC3. You can check and change this from the top right-hand menu.
2. From the left menu, click **Azure Active Directory** and select your iC3 Azure Active Directory Tenant from the list if you have more than one.
3. Click **User** in the **Create** menu on the right-hand side.
    a. Type in the name of the user, for example, 'Joe Bloggs'.
    b. The username must take the form "username@directoryname.**onmicrosoft.com**". For example: "joe.bloggs@directoryname.**onmicrosoft.com**".
    c. You can optionally enter some additional information in the **Profile** option such as their full name and additional work information.
4. Leave the **Properties**, **Groups** and **Directory role** as the default.
5. Select the **Show Password** check box and copy the **Password** to your clipboard. Keep this somewhere safe as you'll need it the first time you log into iC3. This is a temporary password that you can change later on in iC3.
6. You'll receive a notification in the top right-hand corner when the user has been created.

Create the iC3 Application

To create the iC3 Application:

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



5. Enter the Name as **iC3 Portal**.
6. Leave the default Application Type as **Web app / API**.
7. Enter the following string for the Reply-URL and replace the '<DNSofSSLCertificate>' with the DNS you're using.

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

8. Click **Create** to finish creating the iC3 Portal Application.
9. You need to enter a second Reply URL to the application. Click **Settings** > **Reply URLs** and add the following string below the first one. Replace the '<DNSofSSLCertificate>' with the DNS you're using.

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

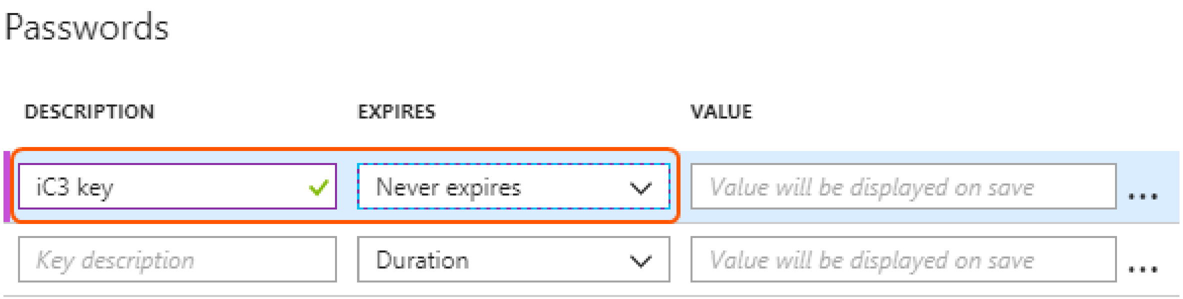
10. Click **Save**.

Generate a Key for your Application

You need to generate a key for your iC3 application if you are using LDAPS to authenticate. Once you generate a key you will not be able to access it again in the portal so you must write it down at time of creation.

To generate a key for the iC3 application:

1. Click **Azure Active Directory** > **App registrations**. If your application doesn't display click **View all applications**.
2. Click your iC3 application that you created previously and then **Settings** > **Keys**.
3. Enter a description for your key and set the expiration date. If your key expires you will not be able to authenticate. Click **Save** to see and copy your key value.



Passwords

DESCRIPTION	EXPIRES	VALUE
iC3 key ✓	Never expires	Value will be displayed on save
Key description	Duration	Value will be displayed on save

*Record the key for your iC3 application as you'll need it for the **Authentication** tab of the iC3 deployment wizard.*

Obtain the GUID for your Portal Application

Select the iC3 application you have created. The Application ID is the GUID for your iC3 application.

*Record the Application ID for your iC3 Portal Application as you'll need it for the **Authentication** tab of the iC3 deployment wizard.*

Report Database Prerequisite

If you are using reporting with iC3 you need to set up the Privilege Management Enterprise Reporting database prior to running the iC3 deployment wizard. The iC3 wizard configures the connection to Enterprise Reporting but doesn't create the databases.

The Privilege Management Enterprise Reporting database must be set up to use SQL authentication for iC3.

> ***Note:*** *Check the Release Notes for iC3 and Privilege Management Enterprise Reporting version compatibility.*

See "Enterprise Reporting Database Sizes" on page 53 for hardware sizing details.

Installing the Privilege Management Reporting Database:

1. On your SQL Server machine, run the DefendpointReportingDatabase_x.x.xx installer and click **Next**.
2. Accept the End User Licence Agreement and click **Next**.
3. Select the Database server you want to use from the drop-down. The name of the database is set to 'AvectoReporting'. You can change this if required.
4. You need to change the selection here to **SQL Authentication** for iC3 integration. If you are connecting iC3 to an existing Privilege Management Enterprise Reporting instance you need to change the type of authentication used by SQL, see https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/change-server-authentication-mode.
5. Click **Next**. The **Configure Event Parser Database User** dialog box appears. You do not need to configure this user as it's managed by iC3. Click **Next**.
6. The **Configure Reporting Services Database User** dialog box appears. You do not need to configure this user as it's managed by iC3. Click **Next**.
7. The **Configure Data Admin Database User** dialog box appears. You do not need to configure this user as it's managed by iC3. Click **Next**.
8. Click **Next** and then **Install** to finish the installation. You have now installed the Privilege Management Reporting Database. The iC3 deployment wizard will configure the connection to the database.

> ***Note:*** *You do not need to install the Event Parser or Reporting Pack as iC3 includes event centralization and reporting .*

iC3 Management Database Prerequisites

The iC3 deployment wizard can create and configure the iC3 management databases. Alternatively, if you have a separate team within your business who are going to create and configure the iC3 management databases, please follow the instructions in this section.

Using Azure AD Authentication

For a manual set up, you need to create and configure the iC3 management databases prior to running the iC3 deployment wizard as the wizard checks for them, see "Azure AD Authentication - Create and Configure the iC3 Management Databases" on page 16 for more information.

Using Windows Active Directory or LDAPS Authentication

For a manual set up, you need to create the iC3 management databases prior to running the iC3 deployment wizard as the wizard checks for them. In this instance, you will configure the databases after the iC3 deployment as the database scripts need the Tenant ID GUID which is generated for you by the deployment wizard. The database scripts also need iC3 Admin Username and iC3 Admin Email Address which you are prompted to enter on the Authentication tab, see "Authentication Tab" on page 20 for more details.

The configuration of the iC3 management databases also requires the Tenant GUID which is generated for you by the deployment tool and also displayed on the Authentication tab, see "Windows AD and LDAPS Authentication - Create the iC3 Management Databases" on page 17 for more information.

Azure AD Authentication - Create and Configure the iC3 Management Databases

You need the following information to create and configure the iC3 management databases.

Attribute	Location
TenantID	This is your Tenant ID GUID from Microsoft Azure, see "Create the Azure AD Tenant" on page 11.
Account Name	This is your account name for iC3, see "Create your User in the Tenant" on page 12.
Email Address	This is the email address associated with the Account Name.

The scripts to configure the databases are in the 'SQL' folder of the iC3 deployment package.

To create and configure the iC3 management database manually:

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

8. Execute the now modified 'CreateAutomationClientUser.sql' script.
9. Edit the 'CreateAdministratorUser.sql' script and replace the following placeholders with your information:
   - <TENANT ID>
   - <ACCOUNT NAME>
   - <EMAIL ADDRESS>
10. Execute the now modified 'CreateAdministratorUser.sql' script.
11. Edit the 'CreateSystemConfigurationSettingsDefault.sql' script and replace the following placeholders with your information:
    - <TENANT ID>
12. Execute the now modified 'CreateSystemConfigurationSettingsDefault.sql' script.
13. You need to open the firewall port for the instance of SQL. If this is the default instance, the port number is 1433, otherwise see "Obtain the SQL Port for a Specific Instance" on page 22.

The iC3 management database is now created.

Create and to set up the iC3 Blob Storage database manually:

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

The database for the blob storage is now created.

Windows AD and LDAPS Authentication - Create the iC3 Management Databases

For Windows Active Directory and LDAPS authentication you need to configure the iC3 management databases after you have run the iC3 deployment wizard, however you need to create the databases before you run the iC3 deployment wizard.

To create the iC3 management databases manually:

1. Log into your SQL Server machine with your credentials.
2. Create a database called 'Avecto.IC3.Database.Management'. Both SQL and Windows authentication is supported. Ensure the database has the dbo.owner permission as this is required for creation. This user is not subsequently used by iC3 as you configure a different user to communicate with the iC3 services when you set up the iC3 services.
3. Create a database called 'Avecto.IC3.Database.BlobStorage.sql'. Ensure the database has the dbo.owner permission. This user is not subsequently used by iC3 as you configure a different user to communicate with the iC3 services when you set up the iC3 services.

Deploy iC3

The iC3 system is deployed using a PowerShell-based tool that is executed from the deployment machine. The deployment tool connects to the database server and iC3 cluster nodes to install and verify prerequisites and make configuration changes.

The iC3 deployment tool configures a number of ports when it deploys iC3, see appendix "Ports that are Configured by the Deployment" on page 43 for more information.

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

1. Open PowerShell as an elevated application.
2. Navigate to the Deployment folder in the iC3 package.
3. Run `Set-ExecutionPolicy unrestricted -scope CurrentUser -f`

> ***Note:** This article shows how to configure the setting using Group Policy: http://technet.microsoft.com/en-us/library/hh849812.aspx*

iC3 Deployment Tool Tabs

To start the on-premise deployment of iC3, run `Avecto IC3 Deployment Wizard.ps1`.

There are several tabs that you will step through. These are listed in order below. Please ensure that you monitor your deployment until it has completed. Once the machine and software prerequisites are in place, a typical iC3 installation will complete in less than 30 minutes.

1. "iC3 EULA" on page 18
2. "Welcome Tab" on page 19
3. "Installation Tab" on page 19
4. "Certificates Tab" on page 20
5. "iC3 Services Tab" on page 20
6. "Authentication Tab" on page 20
7. "iC3 Database Tab" on page 21
8. "iC3 Reporting Tab" on page 22
9. "iC3 Portal Tab" on page 24
10. "Redis Tab" on page 24
11. "Deploy Tab" on page 25
12. "Finish Tab" on page 25

iC3 EULA

You need to accept the End User License Agreement (EULA) to install iC3. After you have read the agreement, select the check box at the bottom of the screen and click **Next**.

Click **Next** to proceed to the "Welcome Tab" on page 19.

Welcome Tab

The **Welcome** screen introduces you to the iC3 deployment wizard. If you are performing a non-domain joined install, ensure that you are using the same user to run the iC3 deployment as you have set up in the Windows Administrators group on the deployment iC3 cluster nodes and SQL machine and you have run the PowerShell script to enable WinRM, see "Non-domain Installs" on page 10 for more information. This script can be found in the 'Deployment' folder.

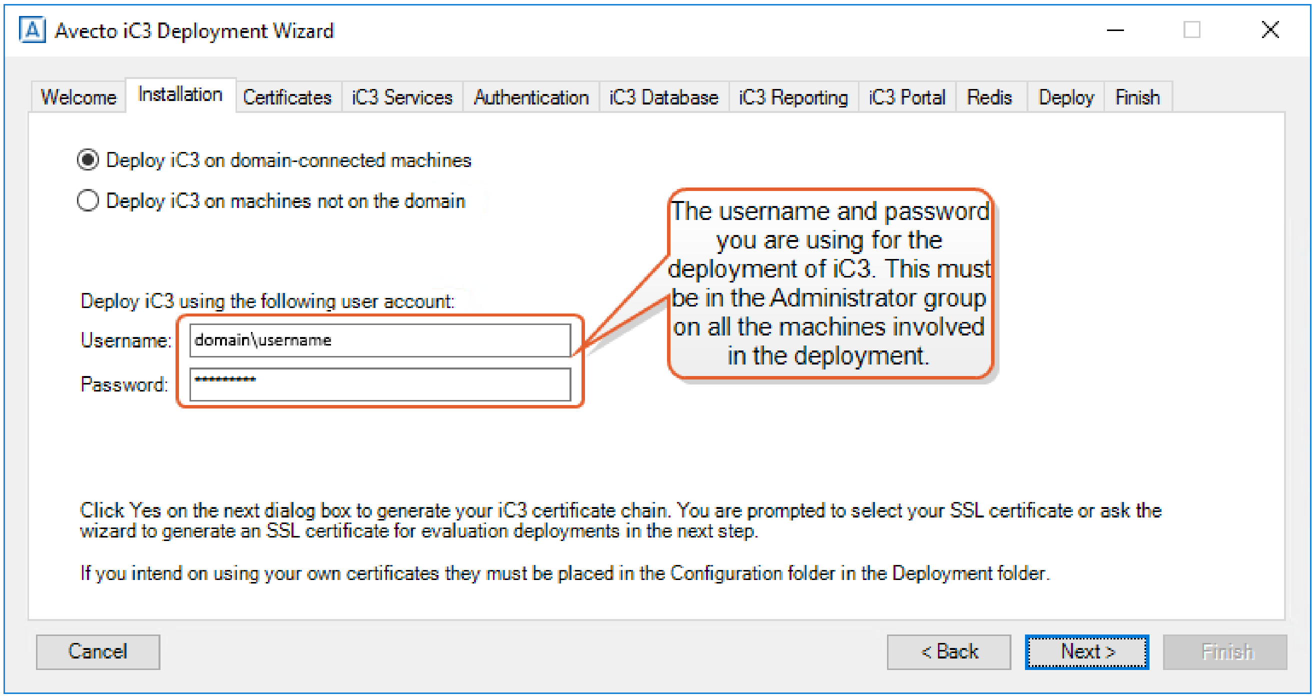
For Windows Directory and LDAPS authentication, the iC3 deployment wizard generates a Tenant ID GUID that is used for the iC3 management database configuration and the iC3 adapter set up after deployment. You need to copy this Tenant ID GUID from the PowerShell window at the start of the deployment, or from the **Authentication** tab where it is displayed again once you select Windows Active Directory. You can disregard this Tenant ID GUID for Azure authentication as you use the Tenant GUID from Azure for this purpose.

Click **Next** to proceed to the "Installation Tab" on page 19.

Installation Tab

Choose between deploying iC3 to domain-connected machines or machines not on a domain.

Enter the domain and username as well as the password for the user that is a member of the Windows Administrators group on your deployment iC3 cluster nodes and SQL machine.



● Deploy iC3 on domain-connected machines

○ Deploy iC3 on machines not on the domain

Deploy iC3 using the following user account:

Username: domain\username

Password: **********

The username and password you are using for the deployment of iC3. This must be in the Administrator group on all the machines involved in the deployment.

Click Yes on the next dialog box to generate your iC3 certificate chain. You are prompted to select your SSL certificate or ask the wizard to generate an SSL certificate for evaluation deployments in the next step.

If you intend on using your own certificates they must be placed in the Configuration folder in the Deployment folder.

When you click **Next** the iC3 deployment wizard validates that this user exists and is a member of the Windows Administrators group, the wizard stops if this is not the case.

Certificate Check and Creation

After validating the user, the iC3 deployment wizard generates the iC3 certificate chain.

The following certificates are generated:

- iC3 Configuration Encipherment
- iC3 Tenant CA
- iC3 Tenant Service Identity
- iC3 Cluster Admin
- iC3 Root

If you have previously run the deployment with this build but not completed it the certificates are in the 'Configuration' folder within the 'Deployment' folder. You can use the same certificates if you made a note of the passwords, otherwise you can delete the certificates and the iC3 deployment wizard can generate a new chain when prompted.

The iC3 deployment wizard prompts you for an SSL certificate. If this is an evaluation deployment you can click **Yes** to generate an SSL certificate, otherwise click **No** to browse to the PFX part of the SSL certificate that you are going to use for iC3.

If you allow the deployment utility to generate an evaluation certificate it will contain the 'star' character to indicate a wildcard. You need to replace this wildcard with your domain when prompted to do so on the **iC3 Portal** tab. Wildcards are supported for evaluation deployments, however multiple sub-domains are not.

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

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

Click **Next** to proceed to the "Certificates Tab" on page 20.

Certificates Tab

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

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

Click **Next** to proceed to the "iC3 Services Tab" on page 20.

iC3 Services Tab

Select an option depending on the size of your iC3 node cluster, see "Hardware Sizes" on page 52 for more information. Enter the names of your deployment iC3 deployment nodes here. The names and existing software are validated when you proceed. In addition the iC3 deployment tool validates that Service Fabric has not already been installed on the nodes, it will fail if Service Fabric is already present.

Click **Next** to proceed to the "Authentication Tab" on page 20.

Authentication Tab

This tab is split into two sections. In the first half you need the enter the iC3 Admin Username and iC3 Email Address for your iC3 administrator.

1. Enter your iC3 Admin Username and iC3 Admin Email. The iC3 Admin Email must take the form:

`<username>@<Domain>.com`

> ***Note:*** *If you are configuring your databases manually then you need to ensure that you use the same iC3 Admin Username and iC3 Admin Email that you entered here for the script.*

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

- "Windows Active Directory" on page 21
- "LDAPS" on page 21
- "Azure Active Directory" on page 21

Windows Active Directory

1. The **Tenant ID** is generated by the deployment tool. You can change it if required, but you must ensure that it matches the GUID used to set up the iC3 management database (if this was done manually). If you change the GUID and the deployment tool is setting up the iC3 management database then it will use the new GUID that you provide here.
2. Enter the domain of your Windows Active Directory.

LDAPS

1. The **Tenant ID** is generated by the deployment tool. You can change it if required, but you must ensure that it matches the GUID used to set up the iC3 management database (if this was done manually). If you change the GUID and the deployment tool is setting up the iC3 management database then it will use the new GUID that you provide here.
2. Enter the domain of your LDAPS (Lightweight Directory Access Protocol over SSL).
3. Enter the LDAPS Distinguished Name (DN).
4. Enter the LDAPS filter.

Azure Active Directory

1. Enter your Azure Tenant ID. See "Obtain the GUID for your Tenant" on page 11 for instructions on getting this Tenant ID GUID if you didn't make a note of it when you configured Azure AD.
2. Enter your Azure Application ID. See "Obtain the GUID for your Portal Application" on page 14 for instructions on getting this GUID if you didn't make a note of it when you configured Azure AD.
3. Enter your designated key for your iC3 Portal application. See "Generate a Key for your Application" on page 13 for instructions on generating and saving this key if you didn't create and make a note of it when you configured Azure AD.

Click **Next** to proceed to the "iC3 Database Tab" on page 21.

iC3 Database Tab

If you have created the iC3 management databases manually prior to starting this deployment, select **I have already created the iC3 databases**.

If you want the iC3 deployment wizard to create and configure the iC3 management databases, select **I want to create and configure the iC3 databases automatically** to allow the wizard to create and configure the iC3 databases.

1. Enter the SQL Hostname, Instance and Port number. If the instance is not the default instance you need to find the port number for your named instance and enter it here. See "Obtain the SQL Port for a Specific Instance" on page 22 for more details.
2. Enter your SQL credentials, these need to have the SQL sysadmin permission. These credentials are only used to set up the iC3 management database. They are not subsequently used by iC3, as authentication with the iC3 management database is done using the credentials specified in the next section of the dialog.

3. Choose from **SQL authentication** or **Windows authentication** and enter the credentials. This user manages the authentication of the iC3 management database with the iC3 application services. This user needs the db_datareader and db_datawriter permissions. You can only use Windows authentication in a domain-joined deployment.
4. Click **Next** to proceed to the "iC3 Reporting Tab" on page 22.

The authentication you choose here is the same as the authentication for the iC3 Reporting tab.

Obtain the SQL Port for a Specific Instance

To obtain the SQL instance port number:

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

Click **Next** to proceed to the "iC3 Reporting Tab" on page 22.

iC3 Reporting Tab

Select **I have already created the Reporting database** if someone in your organization has created the Enterprise Reporting database and you want the wizard to configure the connection to iC3 or select **I do not want to configure Reporting** if you are not using reporting with iC3.

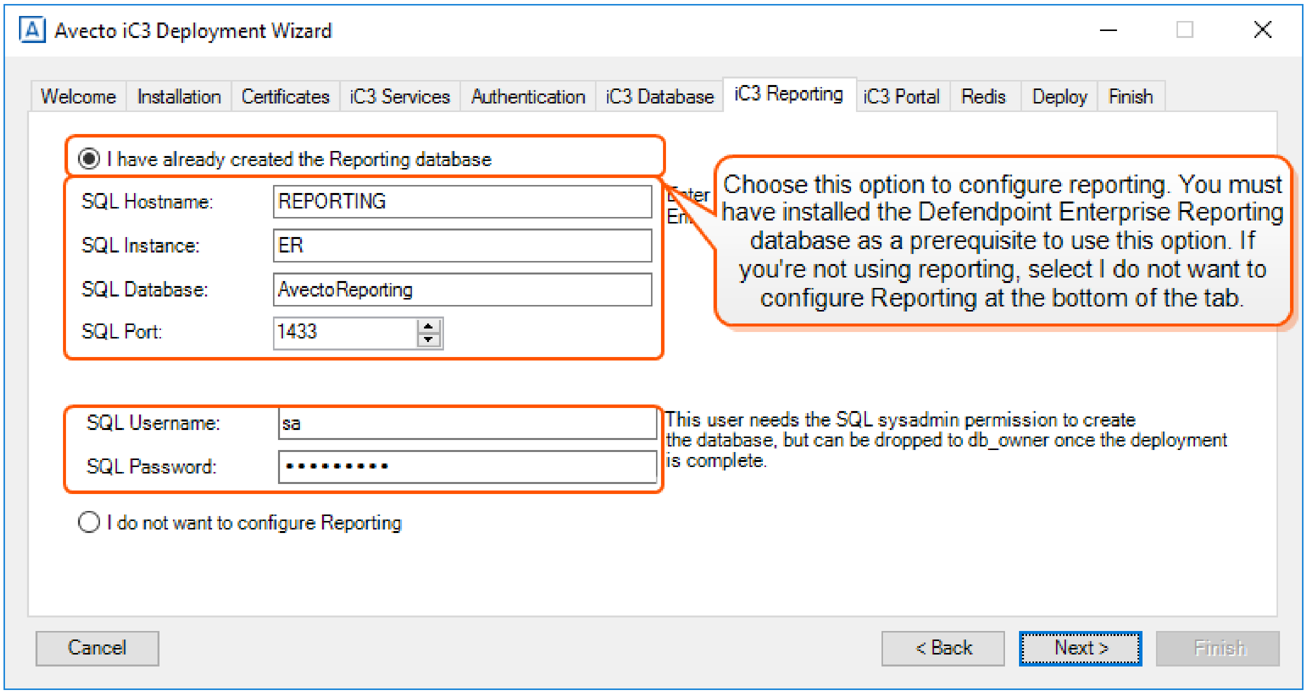
The SQL Hostname, SQL Instance, SQL Database and SQL Port that you provide are validated at this stage.

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

To configure the connection to the Privilege Management reporting database:

1. Enter the SQL Hostname, Instance and Port number. If the instance is not the default instance you need to find the port number for your named instance and enter it here. See "Obtain the SQL Port for a Specific Instance" on page 23 for more details.
2. Choose from **SQL authentication** or **Windows authentication** and enter your associated credentials. This user manages the authentication of the iC3 management database with the iC3 application services. This user needs the db_datareader and db_datawriter permissions. You can only use Windows Authentication in a domain-joined deployment.

The iC3 deployment wizard needs a user with SQL sysadmin to configure Enterprise Reporting for iC3 but this user can be demoted to dbo.owner after the installation has finished.



● I have already created the Reporting database

SQL Hostname: REPORTING

SQL Instance: ER

SQL Database: AvectoReporting

SQL Port: 1433

Choose this option to configure reporting. You must have installed the Defendpoint Enterprise Reporting database as a prerequisite to use this option. If you're not using reporting, select I do not want to configure Reporting at the bottom of the tab.

SQL Username: sa

SQL Password: ••••••••••

This user needs the SQL sysadmin permission to create the database, but can be dropped to db_owner once the deployment is complete.

○ I do not want to configure Reporting

Obtain the SQL Port for a Specific Instance

To obtain the SQL instance port number:

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

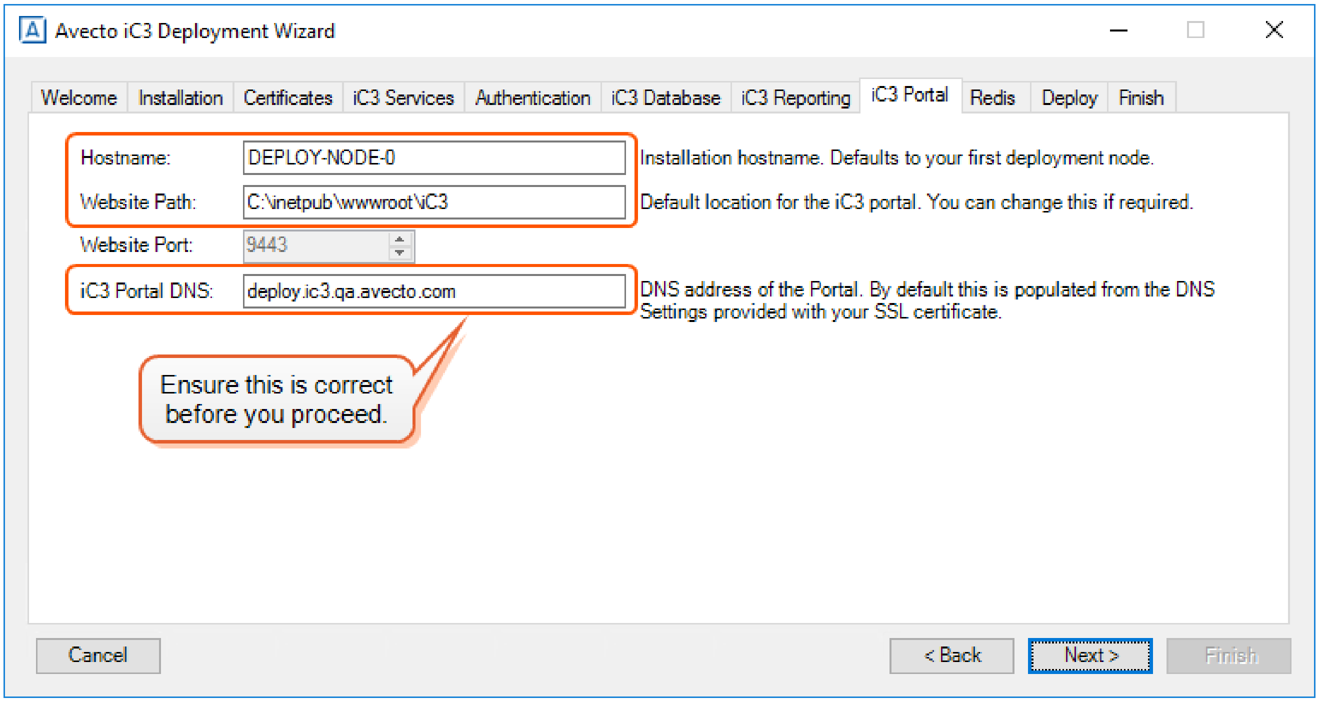
Click **Next** to proceed to the "iC3 Portal Tab" on page 24.

iC3 Portal Tab

This tab configures where iC3 is installed. We recommend you install iC3 to the first node in your cluster.

To configure the location for iC3:

1. The **Hostname** is pre-populated with your first node but you can edit this if required.
2. You can change the **Website path** to install iC3 to a different location on the node if required.
3. The port number for the iC3 portal is 9443. This cannot be changed.
4. The **iC3 Portal DNS** is populated from the DNS Settings provided with your SSL certificate. If you generated a certificate for an evaluation deployment or provided an SSL certificate with a wildcard in for an evaluation deployment, you need to delete the 'star' character and replace it with your domain before you proceed.



Hostname: DEPLOY-NODE-0 — Installation hostname. Defaults to your first deployment node.

Website Path: C:\inetpub\wwwroot\iC3 — Default location for the iC3 portal. You can change this if required.

Website Port: 9443

iC3 Portal DNS: deploy.ic3.qa.avecto.com — DNS address of the Portal. By default this is populated from the DNS Settings provided with your SSL certificate.

Ensure this is correct before you proceed.

Click **Next** to proceed to the "Redis Tab" on page 24.

Redis Tab

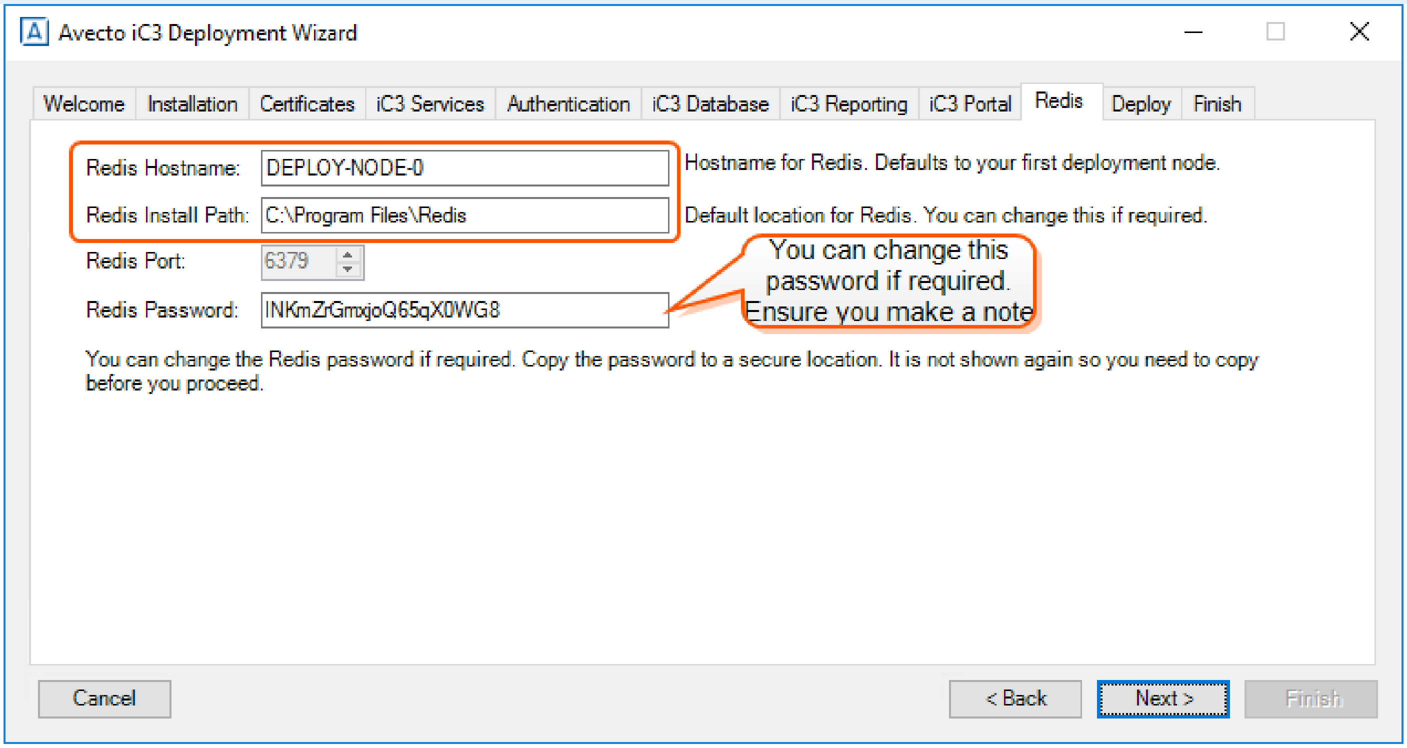
This tab configures where the Redis application cache is installed to. We recommend you install the Redis application cache to the first node in your cluster. The Redis instance should be behind a firewall and only accessible from the cluster nodes and the deployment box.

To configure the location for the Redis application cache:

1. The **Redis Hostname** is pre-populated with your first node in your iC3 Cluster but you can edit this if required.
2. You can change the **Redis Install Path** to a different location on the node if required.
3. The port number for Redis is 6379. This cannot be changed.

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

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


Avecto iC3 Deployment Wizard

Redis Hostname: DEPLOY-NODE-0 — Hostname for Redis. Defaults to your first deployment node.

Redis Install Path: C:\Program Files\Redis — Default location for Redis. You can change this if required.

Redis Port: 6379

Redis Password: INKmZrGmxjoQ65qX0WG8

You can change this password if required. Ensure you make a note

You can change the Redis password if required. Copy the password to a secure location. It is not shown again so you need to copy before you proceed.

Click **Next** to proceed to the "Deploy Tab" on page 25.

Deploy Tab

A summary of all your iC3 deployment messages is displayed in the window. You can review these if required. When you are ready to start your iC3 deployment click **Next**.

A typical iC3 deployment takes about 30 minutes but can take longer depending on machine specifications and network connectivity.

Once deployment has finished the "Finish Tab" on page 25 is shown.

Finish Tab

The **Finish** tab gives you the Server URL you need to access iC3. This is the DNS of your SSL certificate with the iC3 port '9443' appended to it.

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

Record the Server URL as you will need it to log into iC3.

You should now log into your Service Fabric Dashboard to confirm you have deployed iC3 successfully, see "View the Health of your Service Fabric Cluster" on page 29.

Resolution of DNS

You need to be able to resolve the DNS before you can log into iC3. If you are using a public DNS that has not yet been created, you will need to create manual entries in the host files of the machines that need to communicate such as the cluster nodes (including where the portal is installed).

Deployment Logs

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

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

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

The folder 'AvectoIC3DeploymentWizard.ps1' contains the setup and deployment logs including the Windows Directory and LDAPS GUID that was generated.

Windows AD and LDAPS - Manually Configure the iC3 Management Databases

You only need to do the steps in this chapter if you are using Windows Active Directory or LDAPS to authenticate with iC3, and you created your databases manually rather than allowing the iC3 deployment wizard to create them. You need the following information to configure the iC3 management databases manually.

Attribute	Location
TenantID	This is your Tenant ID GUID that is generated for you by the iC3 deployment tool, see "Authentication Tab" on page 20 for more information.
Account Name	This is your account name for iC3. It should match the iC3 Admin Username that you entered on the Authentication tab. See "Authentication Tab" on page 20 for more information.
Email Address	This is the email address for iC3, for example `username@directoryname.onmicrosoft.com`

The scripts to configure the databases are in the 'SQL' folder of the iC3 deployment package.

You need to ensure that you open the firewall port for the instance of SQL. If this is the default instance, the port number is 1433. Otherwise see "Obtain the SQL Port for a Specific Instance" on page 22.

To create and configure the iC3 management database manually:

1. Create a database called 'Avecto.IC3.Database.Management'. Ensure the database has SQL server authentication and the user has the dbo.owner permission.
2. Execute the 'Avecto.IC3.Database.Management.sql' script.
3. Edit the 'AuthorizationModel.2_0.sql' script and replace <TENANTID> on the fourth line of the script with your information:
   - <TENANT ID>
4. Execute the now modified 'AuthorizationModel.sql' script.
5. Edit the 'CreateJobAgentServiceUser' script and replace the following placeholder with your information:
   - <TENANT ID>
6. Execute the now modified 'CreateJobAgentServiceUser.sql' script.
7. Edit the 'CreateAutomationClientUser.sql' script and replace the following placeholder with your information:
   - <TENANT ID>
8. Execute the now modified 'CreateAutomationClientUser.sql' script.
9. Edit the 'CreateAdministratorUser.sql' script and replace the following placeholders with your information:
   - <TENANT ID>
   - <ACCOUNT NAME>
     - This is your account name for iC3. It should match the iC3 Admin Username that you entered on the Authentication tab. See "Authentication Tab" on page 20 for more information.

- <EMAIL ADDRESS>
    - This is the email address for iC3, for example

      ```
      username@directoryname.onmicrosoft.com
      ```

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

The iC3 management database is now created.

To set up the iC3 Blob Storage database manually:

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

The database for the blob storage is now created.

View the Health of your Service Fabric Cluster

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

You can drill down into each of the applications, cluster nodes and system services on the left-hand panel. This information can be combined with the logs to troubleshoot iC3 if required.

You can view the status of your Microsoft Service Fabric once you have installed the iC3 Cluster Admin certificate onto the machine you are using. The iC3 Cluster Admin certificate is installed by the iC3 deployment wizard on the deployment machine by default.

Install the iC3 Cluster Admin Certificate

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

1. Navigate to the Configuration folder in the Deployment folder and copy the 'IC3ClusterAdmin.pfx' file to the machine you want to use to view the status of your Service Fabric.
2. Double-click the PFX file and select **Current User**. Click **Next**.
3. The path to the certificate is populated automatically as you've run the certificate. Click **Next**.
4. Enter the password for the iC3 Cluster Admin certificate and click **Next**.
5. Select **Place all certificates in the following store** and click **Browse**.
6. Leave the default of **Personal** and click **OK**.
7. Click **Next** and then **Finish** to complete the certificate installation.

View Service Fabric Explorer

Use the following URL to view to the status of your Service Fabric Cluster. Replace '<Your IP>' with the IP address of the first node in your iC3 cluster.

```
https://<Your iC3 Portal IP>:19080
```

You need to choose your iC3 Cluster Administration certificate to authenticate yourself with when you browse to the URL.

Set up a Load Balancer

***Note:** The Load Balancer must be installed after you have installed iC3, not before.*

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

Rule One

Traffic coming in from your endpoints on port 443 needs to be balanced across all iC3 cluster nodes.

Rule Two

Traffic coming in from trusted admin IPs and the iC3 cluster on port 8443 needs to be balanced across all iC3 cluster nodes.

Sticky sessions / session affinity are required for port 8443.

Rule Three

Traffic coming in from trusted admin IPs on port 9443 should **not** be balanced across the iC3 cluster. It must be directed at the node where the iC3 portal is deployed.

Rule Four

Traffic coming in from trusted admin IPs on 19080 (Service Fabric Explorer) and 19000 (Service Fabric interface using PowerShell) needs to be balanced across your iC3 cluster nodes.

Timeout Settings

You need to check the timeout settings on the load balancer to ensure that they are set to five minutes as this is the timeout setting applied to the Reporting Gateway service for iC3. If you do not adjust the timeout settings in your load balancer, where present, reports in iC3 may time out unexpectedly.

SSL Certificate

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

Log into iC3

You need to be able to resolve the DNS before you can log into iC3. If you are using a public DNS that has not yet been created, you will need to create manual entries in the host files of the machines that need to communicate such as the cluster nodes (including where the portal is installed).

To log into iC3:

1. Navigate to the Server URL of iC3. This was shown on the "Finish Tab" on page 25. It is the DNS of your SSL certificate with the iC3 port number of '9443' appended to it.

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

a. Navigate to the web.config file. The default location for the web.config file on the portal node is:

```
c:\inetpub\wwwroot\iC3
```

b. Open the web.config file with a text editor and locate the following entry:

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

This is the Server URL you need to log into iC3.

2. Enter the user name and password that was either manually set up for you by your iC3 management database creator or that you inserted through the iC3 deployment wizard on the "Authentication Tab" on page 20.
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 iC3 snap-in, see "Configure iC3 to Connect to the Policy Editor" on page 32.

See "Logs" on page 39 for information on extracting the iC3 Portal logs, adapter logs and node logs.

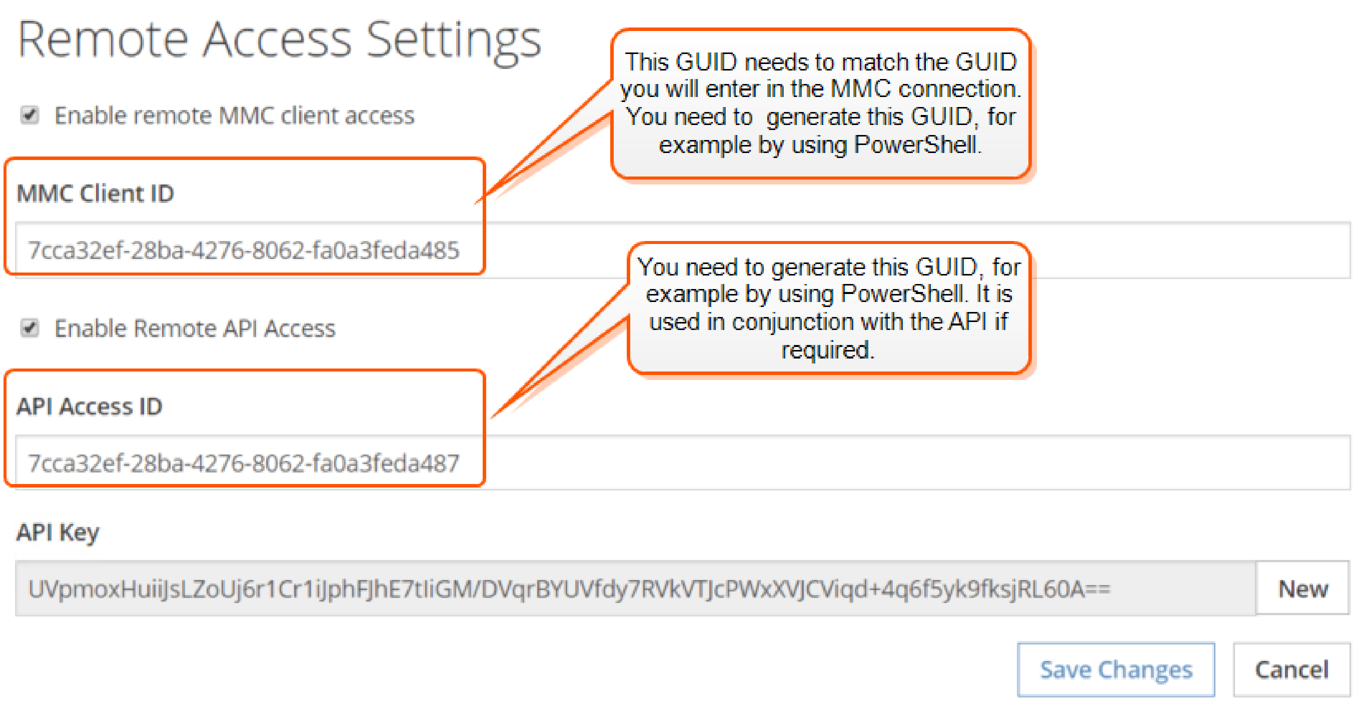
Configure iC3 to Connect to the Policy Editor

You need to configure iC3 to allow the Privilege Management MMC snap-in to communicate with the iC3 services.

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

```
new-guid
```

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



Remote Access Settings

☑ Enable remote MMC client access

MMC Client ID: 7cca32ef-28ba-4276-8062-fa0a3feda485

This GUID needs to match the GUID you will enter in the MMC connection. You need to generate this GUID, for example by using PowerShell.

☑ Enable Remote API Access

API Access ID: 7cca32ef-28ba-4276-8062-fa0a3feda487

You need to generate this GUID, for example by using PowerShell. It is used in conjunction with the API if required.

API Key: UVpmoxHuiiJsLZoUj6r1Cr1iJphFJhE7tliGM/DVqrBYUVfdy7RVkVTJcPWxXVJCViqd+4q6f5yk9fksjRL60A==

Now you have configured iC3 you also need to configure the Privilege Management MMC iC3 snap-in to communicate with it. See "Configure the Privilege Management MMC iC3 snap-in" on page 33 for instructions on how to do this.

Configure the Privilege Management MMC iC3 snap-in

You need to install and configure the Privilege Management MMC on the machine you will use to administrate iC3 policy. See "Set up a Load Balancer" on page 30 for details of the machines that are allowed to connect.

The installation packages differ based on your operating system:

- For 32-bit (x86) systems run DefendpointManagementConsoles_x86.exe
- For 64-bit (x64) systems run DefendpointManagementConsoles_x64.exe

You can obtain these downloads from the Avecto Connect portal. See the Release Notes for compatible versions.

Add and Configurethe Privilege Management iC3 Snap-in

You need to use the Privilege Management MMC iC3 snap-in for the Microsoft Management Console (MMC) to manage policy for endpoints managed by iC3.

To load the Privilege Management iC3 snap-in for the MMC:

1. Run 'mmc.exe' from the Start menu.
2. **File** > **Add/Remove Snap-in** and select 'Defendpoint Settings (iC3)'. Click **Add**.
3. Select the Defendpoint Setting (iC3) node and click iC3 Connection on the left-hand side under Settings.

Note: *Ensure you install the 'Defendpoint Settings (iC3)' snap-in, rather than just 'Defendpoint Settings'.*

The next step is to configure the MMC to connect to iC3.

Setting	What to enter
Connection	
Server URL	This is the URL for iC3 with '8443' in the Port field. This is shown on the Finish tab of the deployment wizard, see "Finish Tab" on page 25 for more details.
Tenant ID	This is the same TenantID GUID you provided to the installation script.
Authorization Provider	
URL	This is the URL for iC3 with ':8443/oauth' appended to it. This is shown on the Finish tab of the deployment wizard, see "Finish Tab" on page 25 for more details.
Identification	
MMC Client ID	This needs to be the same GUID that you generated and used in the iC3 connection settings called 'Application ID'. See "Configure iC3 to Connect to the Policy Editor" on page 32 for more information. You can generate this GUID in many ways, for example by using the PowerShell cmdlet `new-guid`.
Client Return URI	Enter 'http://defendpoint-mmc.com'. This string does not resolve but needs to be as stated.
Amend token resource ID	Select this check box. This string needs to be 'https://api.ic3.avecto.com'. This string does not resolve but needs to be as stated.

Confirm Connection to iC3

You should now confirm that you can access iC3 from the iC3Privilege Management management console snap-in.

1. Click **Create Policy** or **iC3 Policies** in the Privilege Management Management MMC snap-in.
2. Enter your credentials for iC3 when prompted and click **Sign in**.
3. If you clicked **Create** you are prompted to enter a name for your policy. If you clicked **iC3 Policies** you are taken to a list of policies in iC3.

If you receive an error connecting to iC3 ensure you have entered the correct options in both iC3 and the iC3 Privilege Management MMC snap-in.

Configure Endpoints

You need to install the Privilege Management client for the target operating system as well as the iC3 adapter. The iC3 Administration Guide has more information on the management of your endpoints using iC3.

> ***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.*

Defendpoint Clients

You need to choose your Privilege Management client for Windows or Mac operating systems as described below.

For Windows endpoints:

- For 32-bit (x86) systems run DefendpointClient_x86.exe
- For 64-bit (x64) systems run DefendpointClient_x64.exe

You can also install the Privilege Management Windows client MSI in silent mode with the iC3 switch enabled:

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

This will install the Windows client in silent mode with the iC3 switch enabled.

For Mac endpoints:

- Run Defendpoint_x.x.xxxxx.x.pkg

You can obtain these downloads from the Avecto Connect portal. See the Release Notes for compatible versions.

Defendpoint Adapters

You can choose to automatically assign endpoints to groups and authorize them in one step using the `GroupID` parameter for the Windows and Mac adapters. iC3 computer groups should be created in iC3 prior to installing agents at large scale. You should work with your implementation consultant to determine the best computer grouping approach for your needs.

The Defendpoint adapters are installed using the command prompt in Windows and the terminal for Mac operating systems, see:

- "Install the Windows Adapter for iC3" on page 35
- "Install the Mac Adapter for iC3" on page 37

Install the Windows Adapter for iC3

The iC3 client adapter installers can be found in the 'AdapterInstallers' folder of the iC3 deployment. You need to use the Windows Command Prompt to install the Windows iC3 Adapter.

You can install and automatically authorize Windows machines to connect to iC3 using the command line.

> ***Note:*** *You must uninstall any existing iC3 Windows Adapter prior to installing a new Windows adapter for iC3.*

There are five parameters for the iC3 Adapter, one of which is optional:

- `TenantID`, see "Obtain the GUID for your Tenant" on page 11 for instructions on getting this GUID for Microsoft Azure authentication.
- `InstallationID`. You get this from the iC3 portal. Click **Administration** > **Agent Installation**. Copy the Installation ID for this script.
- `InstallationKey`. You get this from the iC3 portal. Click **Administration** > **Agent Installation**. Copy the Installation Key for this script.
- `ServerURL`, this is the URL for your iC3 portal.
  Please note that there is no port number or slash character on 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 iC3. 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.

Example command line

The line breaks must be removed before you run the script.

```
msiexec.exe /i "AvectoIC3Adapter_x64_x.x.xxxx.x.msi"
TENANTID="<TenantID_GUID>"
INSTALLATIONID="<InstallationID>"
INSTALLATIONKEY="<InstallationKey>"
SERVICEURI="<ic3 URL>"
GROUPID="<iC3 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 iC3 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 iC3 adapter will immediately join the iC3 instance indicated.

```
SERVICE_STARTUP_TYPE=Disabled
```

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

Example

```
msiexec.exe /i "AvectoIC3Adapter_x64_x.x.xxxxx.0.msi" TENANTID="6b75f647-d3y7-4391-9278-
002af221cc3f" INSTALLATIONID="08A1CD8F-FAE4-479F-81B4-00751A55EEB8"
INSTALLATIONKEY="ABCDEFGHIJKLMNO" SERVICEURI="https://test.ic3.avecto.com" GROUPID="e531374a-55b9-
4516-g156-68f5s32f5e57"
SERVICE_STARTUP_TYPE=Disabled
```

Configure the Windows iC3 Adapter

When the iC3 Adapter communicates with the iC3 Portal it uses HTTPS. If there is a proxy in place that this communication goes through, it must be configured for the iC3 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 iC3 Adapter it creates a user called **iC3Adapter** as part of the installation process. The **iC3Adapter** user is granted the rights to "Log on as a Service" by the installation process. If you have a Group Policy in place that revokes this permission you need to ensure the **iC3Adapter** user is excluded as it needs the "Log on as a Service" right. For details of how to do this, see the Microsoft Knowledgebase article https://technet.microsoft.com/en-gb/library/cc794944(v=ws.10).aspx.

The computers with the Privilege Management client and Privilege Management iC3 adapter installed with the Installation ID and Installation Key will now appear in the Computers grid in iC3.

Install the Mac Adapter for iC3

The iC3 client adapter installers can be found in the 'AdapterInstallers' folder of the iC3 deployment. You need to use the Terminal to install the Mac iC3 Adapter.

You can install and automatically authorize Mac machines to connect to iC3 using the command line.

> ***Note:*** *You must uninstall any existing iC3 Mac Adapter prior to installing a new Mac adapter for iC3.*

There are six parameters, two of which are optional:

- `TenantID`, see "Obtain the GUID for your Tenant" on page 11 for instructions on getting this GUID for Microsoft Azure authentication.
- `InstallationID`. You get this from iC3. Click **Administration** > **Agent Installation**. Copy the Installation ID for this script.
- `InstallationKey`. You get this from iC3. Click **Administration** > **Agent Installation**. Copy the Installation Key for this script.
- `ServerURL`, this is the URL for your iC3 portal.
  Please note that there is no port number or slash on 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 obtain this from iC3. 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.*

> ***Note:*** *Include the Cacertificateid if your Root CA certificate is not issued by a trusted global provider.*

1. Navigate to the location of the Adapter installer. By default this is the **AdapterInstallers** folder.
2. Mount the DMG and place the iC3 adapter onto the desktop. Run the following command line from the Terminal. Once the Adapter installer launches, proceed through the installation wizard as required.

Example command line

The line breaks must be removed before you run the script.

```
sudo /Avecto_ic3_Adapter_x_x_x/install.sh tenantid="750e85d1-c851-4d56-8c76-b9566250cf1d"
installationid="95a10760-2b96-4a0e-ab65-ed7a5e8f1649"
installationkey="VGhpcyBzZWNyZXQgaTYzIGJlZW4gQmFzZTY0IGVuY29kZWQ="
serviceuri="https://test.ic3.avecto.com" groupid="fcc4022e-12fa-4246-87w8-0de9a1483a68"
cacertificateid="b36b7345ff30aa7fb15fcd985fe2989c3e11aba7"
```

The computers with the Privilege Management client and Privilege Management iC3 adapter installed with the Installation ID and Installation Key will now appear in the Computers grid in iC3.

Logs

There four locations where you can extract logs:

- "Deployment Logs" on page 39
- "Portal Logs" on page 39
- "Cluster Node Service Logs" on page 39
- "Adapter Logs" on page 41

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

Deployment Logs

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

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

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

The folder 'AvectoIC3DeploymentWizard.ps1' contains the setup and deployment logs including the Windows Directory and LDAPS GUID that was generated.

Portal Logs

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

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

Cluster Node Service Logs

You can get the logs from each node in your iC3 cluster from the deployment machine. There are two methods of achieving this:

- "Specific Node by URL" on page 40
- "All Nodes Using PowerShell" on page 40

Specific Node by URL

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

1. Copy and install the iC3 Cluster Admin Certificate (*.pfx) portion to the machine you are downloading the logs to.
2. Log into the node itself or a machine that can communicate with the node and open a browser.
3. Navigate to the following string where IPADDRESS is the IP of the node that you want the logs from:

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

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

All Nodes Using PowerShell

You need to install the iC3 Cluster Admin certificate prior to running the PowerShell script:

1. Copy and install the iC3 Cluster Admin certificate (*.pfx) portion to the machine you are downloading the node logs to.
2. Double-click the iC3 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 iC3 Cluster Admin Certificate and click **Next**.
6. Select **Place all certificates in the following store** and click **Browse**.
7. Select the default of 'Personal' and click **OK** and **Next**.
8. Click **Finish** to complete the certificate installation.

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

To download the logs from all your nodes:

1. Navigate to the PowerShell folder in the iC3 deployment package.
2. Copy the PowerShell file 'NodeDiagnosticsLogsDownload' to the machine you are downloading the logs to.
3. Run PowerShell as an administrator. The script requires the following parameters:
    - Cluster Admin Thumbprint. See https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/how-to-retrieve-the-thumbprint-of-a-certificate for details of how to obtain the thumbprint of the certificate if required. 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:\ic3logs' (without the quotes).

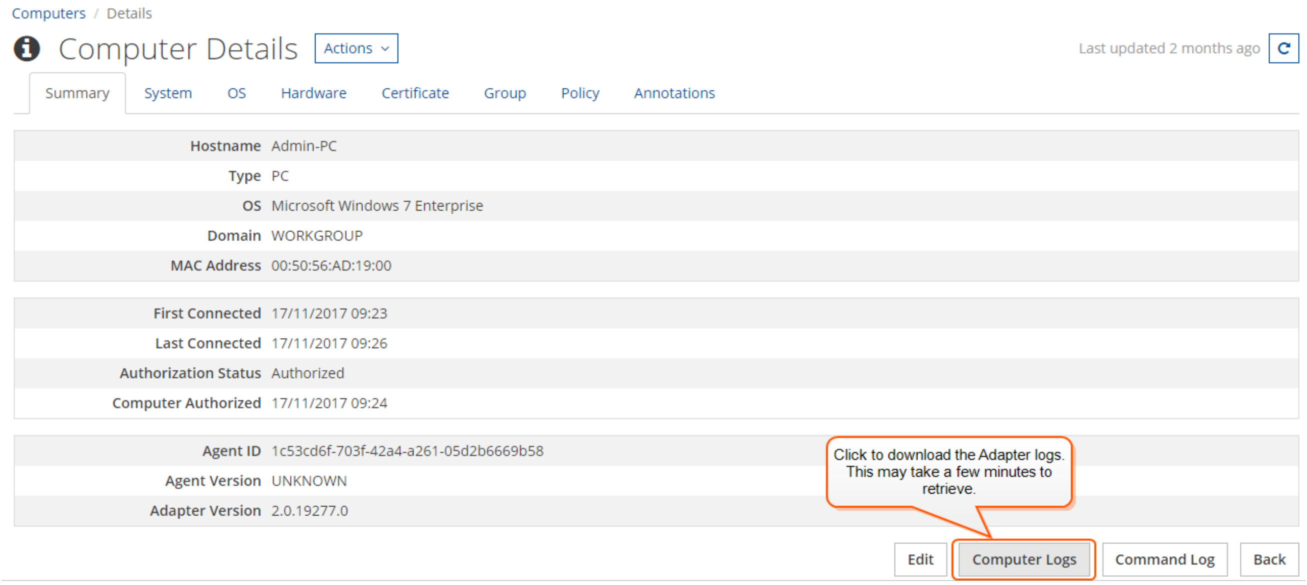
3. Press **Enter** to run the PowerShell script and download the files to the chosen location.

Adapter Logs

You can retrieve the most recent adapter log from iC3 if you need to send them to Avecto Support for analysis:

To retrieve logs:

1. Click the **Computers** tile in iC3.
2. Select the computer you want to retrieve the logs for.
3. On the **Computer Details** tab click **Computer Logs**:



Hostname	Admin-PC
Type	PC
OS	Microsoft Windows 7 Enterprise
Domain	WORKGROUP
MAC Address	00:50:56:AD:19:00
First Connected	17/11/2017 09:23
Last Connected	17/11/2017 09:26
Authorization Status	Authorized
Computer Authorized	17/11/2017 09:24
Agent ID	1c53cd6f-703f-42a4-a261-05d2b6669b58
Agent Version	UNKNOWN
Adapter Version	2.0.19277.0

Click to download the Adapter logs. This may take a few minutes to retrieve.

Appendices

The following appendices may be used to support your iC3 deployment.

- "Ports that are Configured by the Deployment" on page 43
- "Hardware Sizes" on page 52
- "iC3 Scripts" on page 53
- "iC3 Certificate Chain" on page 57

Ports that are Configured by the Deployment

The deployment tool configures several ports for iC3 communication as it runs through the deployment of iC3. If you need to configure these ports manually please see the following lists:

Ports that are required for inbound external communication to iC3 (outside of the iC3 cluster):

Source	Destination	Port Number	Machines	Reason
End Point Networks (normally ANY)	Load Balancer	443	All iC3 Cluster Nodes	Client communication over TLS
Trusted Admin IP's Any additional systems calling the API	Load Balancer	8443	All iC3 Cluster Nodes	API and MMC over TLS
Trusted Admin IP's	iC3 Cluster Nodes	9443	iC3 Cluster Node where the iC3 portal is installed	iC3 admin over TLS
Trusted Admin IP's	iC3 Cluster	19000 19080	Deployment machine All iC3 Cluster Nodes where the iC3 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 IP's	iC3 Cluster Nodes	19001 19002 19003 19081	Deployment machine All iC3 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 IP's	iC3 Cluster Nodes	3389	All iC3 Cluster Nodes	Required for remote desktop
Trusted Admin IP's	The Enterprise Reporting database	1433	Microsoft Management Console (MMC)	The MMC needs to talk to the reporting database for Event Import

Ports that are required for internal communication inside of the iC3 cluster:

Source	Destination	Port Number	Machines	Reason
iC3 Cluster Nodes and Deployment Machine	iC3 Cluster Nodes and Deployment Machine	135 137 138 139 445	Deployment machine All iC3 Cluster Nodes	Microsoft Service Fabric Cluster Communication between nodes, diagnostics, load balancing
Load Balancer iC3 Cluster Nodes	iC3 Cluster Nodes	443	All iC3 Cluster Nodes	HTTPS
iC3 Cluster Nodes	iC3 Management iC3 Enterprise Reporting	1433	SQL Machine	Database and Service Fabric cluster communication
iC3 Cluster Nodes	iC3 Cluster Nodes	6379	iC3 Cluster Node where Redis Application Cache is installed	Redis Port
Load Balancer iC3 Cluster Nodes	iC3 Cluster Nodes	8443	All iC3 Cluster Nodes	HTTPS
iC3 Cluster Nodes	iC3 Cluster Nodes	20001 - 20031	Deployment machine All iC3 Cluster Nodes	Internal services to send requests to command processors without using HTTP / HTTPS.
iC3 Cluster Nodes	iC3	1433	SQL Machine	SQL

Ports that are required for outbound communication from the iC3 cluster:

Source	Destination	Port Number	Machines	Reason
All iC3 Objects	DNS Servers	80/443	N/A	DNS
All iC3 Objects	Required	443	N/A	Will vary from customer to customer. Start with ‘ANY’ and tighten if required.

Rotate your SSL Certificates

Prior to your certificates expiring you need to rotate them. This section details how to achieve this with On-Premise deployments.

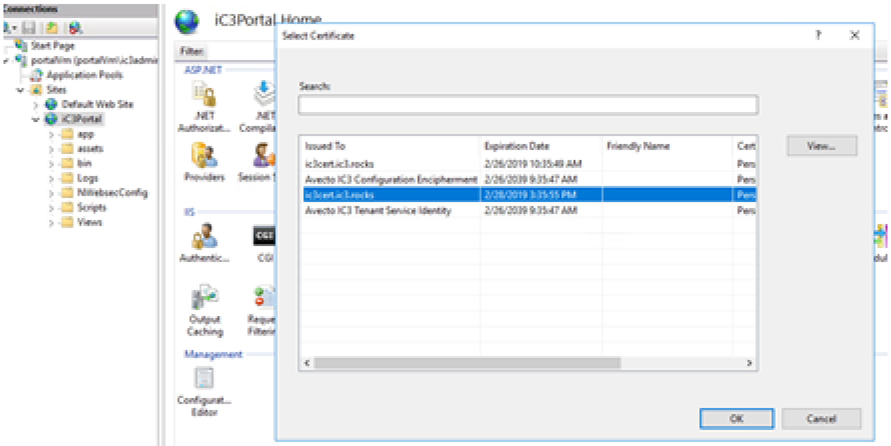
To rotate your SSL certificate, please first copy it to your deployment machine.

Install the New Certificates on to the Nodes

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

Configure Internet Information Services (IIS)

1. Log into your Portal VM and navigate to **Internet Information Services** (IIS).
2. Locate the iC3 Portal site, right-click on it and select **Bindings**.
3. Select the single binding for port 9443 and click **Edit**.
4. Select the new SSL certificate. You can identify it from the furthest expiration date and click **OK**.
5. Click **OK** to confirm the new binding.



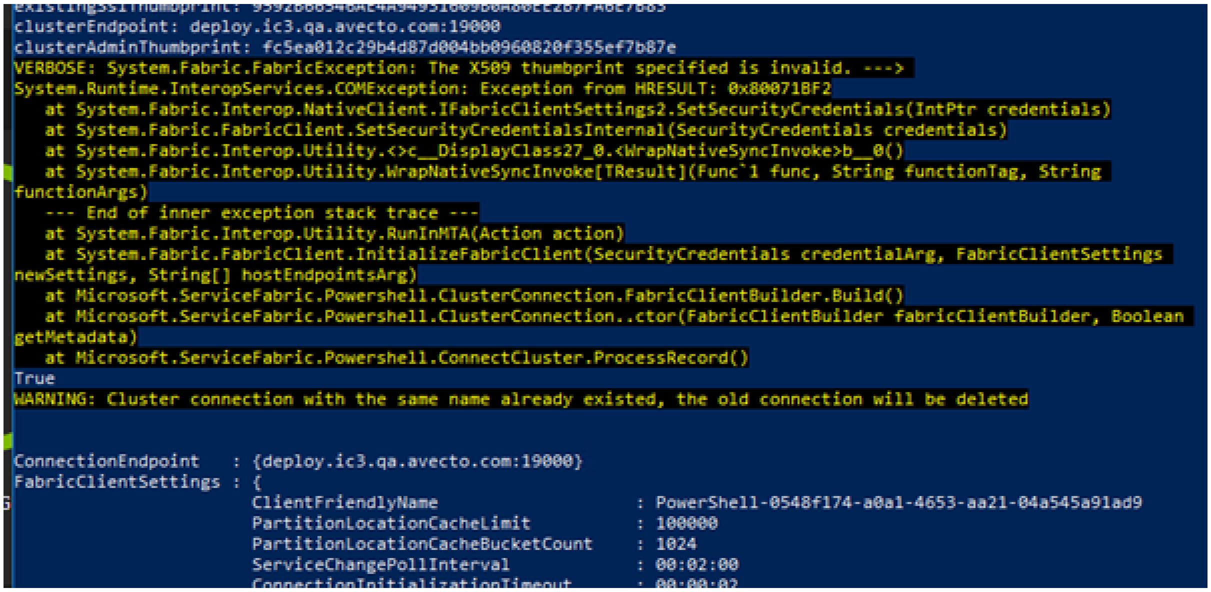
Issued To	Expiration Date	Friendly Name	Cert
ic3cert.ic3.rocks	2/26/2019 10:35:49 AM		Pers
Avecto IC3 Configuration Encipherment	2/26/2039 9:35:47 AM		Pers
ic3cert.ic3.rocks	2/28/2019 3:35:55 PM		Pers
Avecto IC3 Tenant Service Identity	2/26/2039 9:35:47 AM		Pers

Upgrade the ServiceFabric Cluster

> ***Note:*** *This process takes approximately 20 minutes.*

1. On the deployment machine, run **PowerShell.exe** with admin privileges.
2. Navigate to the following folder in the deployment kit **\Upgrades\SSLCertRotation\OnPrem** in PowerShell and run `UpdateClusterConfig.ps1`. You will be asked for the following parameters:
    - a. **newSslThumbprint** – This is the thumbprint of the new SSL certificate.
    - b. **clusterConfigPath** – This defaults to `C:\ProgramData\SF\ClusterConfig.json` on node 0 of the ServiceFabric cluster. If the `clusterConfigPath` is the default, this can be left blank.
    - c. **clusterAddress** – This is the address of the ServiceFabric cluster, for example, `$dns$:19000`.
    - d. **adminUsername** - This is the username required to access to each node. It is the same as the username for deployment. Please include domain if relevant.
    - e. **adminPassword** - This is the password required to access to each node using the **adminUsername** account.
    - f. **node0ComputerName** - This is the name of node 0 for domain-joined deployments, or the IP address of node 0 if your deployment is non-domain joined.
    - g. **domainJoinedInstall** - Set this to `$true` or `$false` depending on whether or not your deployment is domain-joined.

4. The script will exit when the upgrade is started. You can check the upgrade process by running `CheckClusterUpgradeProgress.ps1.` If this script shows a warning as shown below, you can diregard it. This is expected when rotating the SSL certificate.



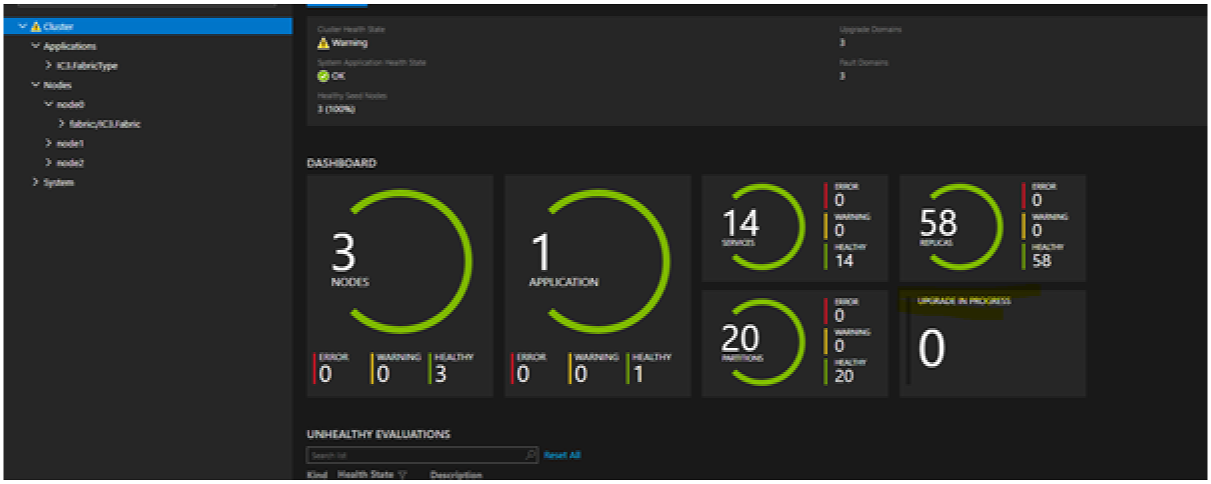
```
existingSslThumbprint:
clusterEndpoint: deploy.ic3.qa.avecto.com:19000
clusterAdminThumbprint: fc5ea012c29b4d87d004bb0960820f355ef7b87e
VERBOSE: System.Fabric.FabricException: The X509 thumbprint specified is invalid. --->
System.Runtime.InteropServices.COMException: Exception from HRESULT: 0x80071BF2
   at System.Fabric.Interop.NativeClient.IFabricClientSettings2.SetSecurityCredentials(IntPtr credentials)
   at System.Fabric.FabricClient.SetSecurityCredentialsInternal(SecurityCredentials credentials)
   at System.Fabric.Interop.Utility.<>c__DisplayClass27_0.<WrapNativeSyncInvoke>b__0()
   at System.Fabric.Interop.Utility.WrapNativeSyncInvoke[TResult](Func`1 func, String functionTag, String
functionArgs)
   --- End of inner exception stack trace ---
   at System.Fabric.Interop.Utility.RunInMTA(Action action)
   at System.Fabric.FabricClient.InitializeFabricClient(SecurityCredentials credentialArg, FabricClientSettings
newSettings, String[] hostEndpointsArg)
   at Microsoft.ServiceFabric.Powershell.ClusterConnection.FabricClientBuilder.Build()
   at Microsoft.ServiceFabric.Powershell.ClusterConnection..ctor(FabricClientBuilder fabricClientBuilder, Boolean
getMetadata)
   at Microsoft.ServiceFabric.Powershell.ConnectCluster.ProcessRecord()
True
WARNING: Cluster connection with the same name already existed, the old connection will be deleted


ConnectionEndpoint   : {deploy.ic3.qa.avecto.com:19000}
FabricClientSettings : {
                       ClientFriendlyName                   : PowerShell-0548f174-a0a1-4653-aa21-04a545a91ad9
                       PartitionLocationCacheLimit          : 100000
                       PartitionLocationCacheBucketCount    : 1024
                       ServiceChangePollInterval            : 00:02:00
                       ConnectionInitializationTimeout      : 00:00:02
```

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

Make the iC3 Application Configuration Changes

1. On the deployment machine, run **PowerShell.exe** with admin privileges.
2. The setting for the SSL Thumpbrint 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.
    a. For example `.\UpdateServiceFabricAppSetting.ps1 -UpdateConfigParameters @{"Avecto.IC3.Certificates.SSL.Thumbprint" = "newthumbprint"}`.
3. Navigate to the following folder in the deployment kit **\Upgrades\SSLCertRotation\OnPrem** in PowerShell and run `UpdateServiceFabricAppSetting.ps1`. You will be asked for the following parameters:
    a. **clusterAddress** - This is the address of the ServiceFabric cluster, for example `$dns$:19000`.
    b. **ServerCertThumbprint** – This is the thumbprint of the new SSL certificate.
    c. **ClusterAdminThumbprint** – The thumbprint of the Cluster Admin certificate setting.
    d. **NewValue** – The thumbprint of the new SSL certificate.

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



Upgrading On-Premise Deployments

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

- "Upgrade the Database" on page 48
- "Upgrade the Application" on page 48
- "Upgrade Issues" on page 51
- "Upgrade the Portal" on page 51
- "Upgrade Issues" on page 51
- "Upgrade the Portal" on page 51

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, you can proceed to the application. Please see "Upgrade the Application" on page 48 for more information.

Upgrade the Database

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

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

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

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

Upgrade the Application

Update ServiceFabric Runtime

On the machine you are running the upgrade from, you need to update the ServiceFabric Runtime.

1. Download the latest version of the ServiceFabric RunTime. You can obtain this from Microsoft, please see https://go.microsoft.com/fwlink/?LinkId=730690. This is a *.cab file.
2. Run **PowerShell.exe** as an administrator and paste the following code in and press **Return**. You will need to provide the following parameters:
   - **$ClusterEndpoint** - This is your iC3 DNS with the port number 19000 appended to it. For example `https://$mydns$:19000`
   - **$ServerCertThumbprint** - This is the thumbprint of your SSL certificate.
   - **$ClusterAdminThumbprint** - This is the thumbprint of your **IC3ClusterAdmin** certificate.

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

3. Type `Get-ServiceFabricClusterUpgrade` into PowerShell to check the current ServiceFabric Runtime version. Make a note of the **TargetCodeVersion**.
4. Type the following into PowerShell to copy the ServiceFabric Cluster package into the cluster image store. The `-Code` and `-CodePackagePath` need to point to the *.cab ServiceFabric Runtime that you downloaded earlier.

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

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

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

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

```
Get-ServiceFabricClusterUpgrade
```

Enable WinRM with SSL on the Portal VM

1. Connect to your Portal VM and copy the **Enable-WinRMWithSSL.ps1** script from the build folder to the PortalVM.
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 Deployment Machine

You need the **On Prem** folder for the version of iC3 that you are upgrading to.

1. On the Deployment machine, copy the **Upgrades** folder from the build you wish to upgrade to onto the Deployment machine. This contains all the files needed to prepare and upgrade your environment.

If you changed the default location of the Portal when you installed iC3, you need to provide the following argument to the upgrade script before you run it:

```
-PortalWebsiteVmLocation "C:\MyFolder\iC3"
```

If you need to change any values in the configuration (for example, the location of the portal and connection strings, you need to provide them as an argument to the **PrepUpgradeConfig,ps1** script before you run it.

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 **Upgrade** folder if required. You need to use the script to do this rather than edit the files directly, otherwise any changes will be overwritten by the script.

2. Run PowerShell as an administrator and navigate to the location of the **PrepUpgradeConfig,ps1** script in the **Upgrades** folder.
3. To change values in the **Production.5Node.xml** file, use the following command:

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

For example:

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

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

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

For example:

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

5. Run the **PrepUpgradeConfig.ps1** script with any arguments required as detailed above and then provide the following information when prompted.
   a. **ClusterEndpoint** – Your DNS with ":19000" applied at the end, e.g. "ic3test.mycompany.com:19000" (no "https://" needed at the start).
   b. **ClusterAdminThumbprint** – The thumbprint output during initial deployment for the iC3 Cluster Admin certificate.
   c. **ServerCertThumbprint** - The thumbprint of your SSL certificate.
   d. **PortalVmAdminUsername** – The administrator username for the portal machine that was entered in the initial deployment.
   e. **PortalVmPassword** – The password for the portal machine that was entered in the initial deployment.
   f. **PortalVmIpAddress** – The IP address of the portal machine.
   g. **ParametersConfigFilePath** – The full file path of the parameter config file in the **Upgrades** folder e.g. `C:\Users\myuser\Desktop\Upgrades\Production.5node.xml`
   h. **WebConfigFilePath** – The full file path of the web config file in the **Upgrades** folder e.g. `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.

6. Copy the **Package.zip** folder from the **SupportFiles** folder (the version you are upgrading to) to your deployment box and unzip it.
7. From your PowerShell instance, navigate to the **UpgradeApp.ps1** script in the **Upgrades** folder and provide the following parameters:
   a. **PackagePath** – The path to the unzipped Package folder you copied over, for example `C:\Users\myuser\Desktop\Package`
   b. **AppParamsPath** – The location of the **Production.5Node.xml** file in the **Upgrades** folder, e.g. `C:\Users\myuser\Desktop\Upgrades\Production.5node.xml`
   c. **ClusterAddress** – Your DNS with ":19000" applied at the end, e.g. `ic3test.avecto.com:19000` (no `https://` needed at the start).
   d. **ClusterAdminThumbprint** – The thumbprint output during the deployment for the iC3 Cluster Admin certificate
   e. **ServerCertThumbprint** - The thumbprint of your SSL certificate.
8. The script will run and begin the upgrade process. To check the progress, navigate to ServiceFabric explorer, expand the cluster and select **Applications** from the tree view. In the right-hand work pane, you will see "Upgrades in progress" text. Click on this to see the progress for each node. It shows the current version and the target version you are upgrading to. During the upgrade, ServiceFabric will display several warnings as each domain is taken down. Upon completion of an upgrade, these warnings should be removed. During the upgrade, the policy on endpoints is still be applied and the policy will remain functional.

Check for Successful Upgrade

You can check if your upgrade was successful by going 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 ServiceFabric. 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>
```

The error is due to the previous failed run leaving the application type and version provisioned in Service Fabric and running the script again will clash as it is the same version. The script itself will continue and overwrite this version however, to avoid seeing this error, you can navigate to Service Fabric explorer and manually unprovision the new version of the application before re-running the script. However you cannot roll back to previous versions if you unprovision the application. You can do this by navigating to the **Cluster** > **Applications** > **IC3.FabricType** node and click **Unprovision**.

Upgrade the Portal

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

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

Apply Windows Updates

This section details how to manage your Windows Updates on the servers running iC3.

To manage Windows updates for iC3 you need to install the Service Fabric Patch Orchestration application into the Service Fabric Cluster

https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-patch-orchestration-application

BeyondTrust recommends you use the Service Fabric Patch Orchestration application as it ensures that the updates only take one node of the cluster offline at a time.

Hardware Sizes

Microsoft only support five node Service Fabric Cluster deployments for production environments, but iC3 supports up to 250,000 endpoints on a three or five node configuration.

BeyondTrust Specifications

During the performance testing we hosted the iC3 cluster on the following specifications of virtual machines:

- 4 Core CPU @ 2.40GHz
- 16 GB RAM
- 100 GB HDD
- Windows Server 2016 R2 / 2016

Our database server had the following specification:

- 4 CPUs @ 2.40GHz
- 16 GB RAM
- 150 GB HDD
- Microsoft SQL Server R2 / 2016

With these specifications we were able to scale our environment to support 250,000 endpoints.

Microsoft Specifications

Microsoft recommend the following specifications for a Service Fabric Cluster:

- 4 core CPU
- 16GB RAM
- Windows Server 2012 R2 / 2016

https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-cluster-standalone-deployment-preparation

Enterprise 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 Enterprise Reporting is the only application running on the database server.

Managed Computers	CPU	Memory	Database
10,000	2	12 GB	67.5 GB
25,000	4	16 GB	168.75 GB
50,000	6	16 GB	337.5 GB
75,000	6	22 GB	506.25 GB
100,000	8	24 GB	675 GB
150,000	8	24 GB	1012.5 GB
200,000	8	32 GB	1350 GB
250,000	8	32 GB	1687.5 GB

iC3 Scripts

There are three PowerShell scripts that are supplied with iC3 to support your installation. The use of these is optional:

- "Deactivate Duplicate Agents" on page 53
- "Deactivate Inactive Agents" on page 54
- NodeDiagnosticsLogsDownload, see "Cluster Node Service Logs" on page 39

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 iC3. 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 iC3.

This script takes five parameters:

- client_id
- client_secret
- tenant_id
- cloudServiceDnsName
- platformApiPort

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

Example Script

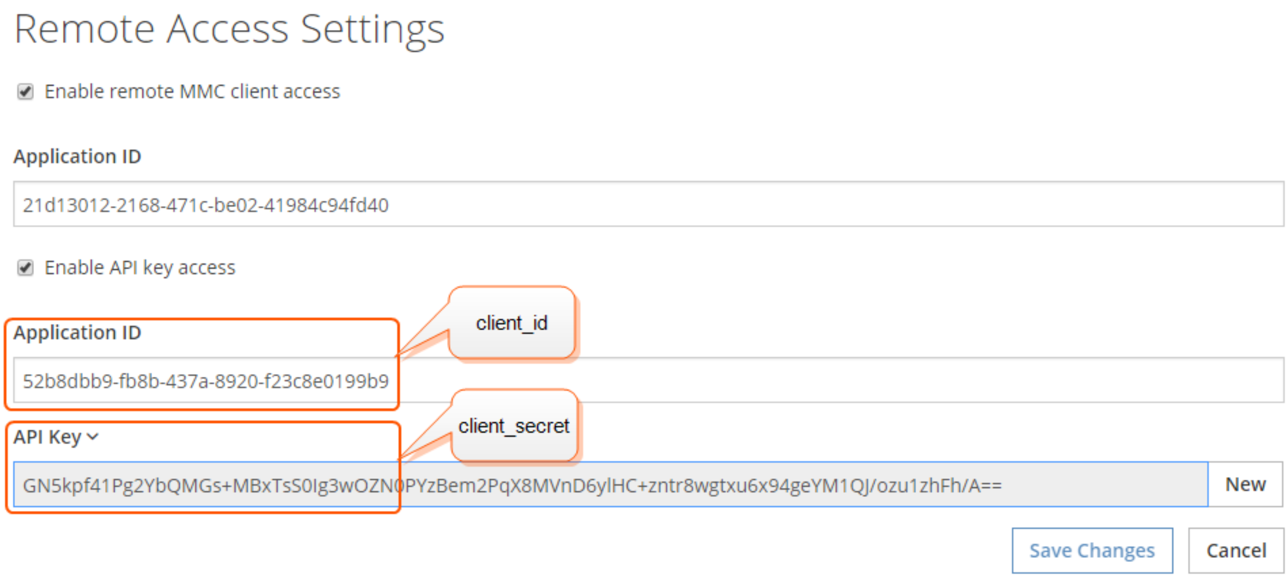
```
.\DeactivateDuplicateAgents.ps1 -client_id "<client_id>" -client_secret "<client_secret>" -tenant_id
"<tenant_id>" -cloudServiceDnsName "<cloudServiceDnsName>" -platformApiPort "<port number>"
```

client_id

This is the **Application ID** that is below the **Enable API key** access check box in the **Remove Access Settings** page in iC3.

client_secret

This is the **API Key** in the iC3 **Settings** page.



Remote Access Settings

☑ Enable remote MMC client access

Application ID

21d13012-2168-471c-be02-41984c94fd40

☑ Enable API key access

Application ID

52b8dbb9-fb8b-437a-8920-f23c8e0199b9

API Key

GN5kpf41Pg2YbQMGs+MBxTsS0Ig3wOZN0PYzBem2PqX8MVnD6ylHC+zntr8wgtxu6x94geYM1QJ/ozu1zhFh/A==

tenant_id

- `TenantID`, see "Microsoft Azure AD Authentication" on page 11 for instructions on getting this GUID for Microsoft Azure authentication. For Windows Directory and LDAPS the GUID is generated by the deployment tool and you should have a note of it already.

cloudServiceDnsName

This is your iC3 URL. Do not included the `https://` or the port when entering, for example `ic3.avecto.com`.

platformApiPort

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

Deactivate Inactive Agents

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

Description

When running, the script states that it's retrieving a list of Agents that have not connected for the defined number of days (**inactiveDays**) since a date and time. The date and time will be the date of the system minus the number set for **inactiveDays**. It then details how many agents have been identified and confirms that it will request to deactivate a specified number of agents. The script pauses for five minutes before it deactivates the agents to ensure that other tasks aren't running. The script will confirm the number of agents that it has deactivated. On deactivation, the Authorization Status of the agent will change to 'Deactivated'. You can view the Authorization Status of an agent in the Computer Details page in iC3.

This script takes six parameters:

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

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

Example Script

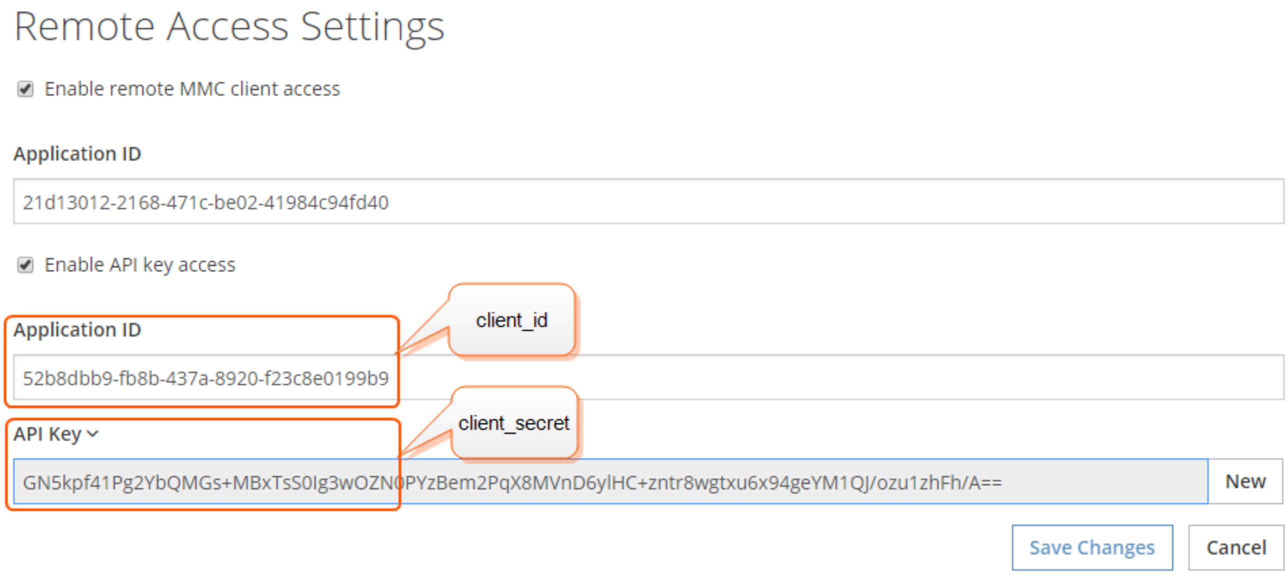
```
.\DeactivateNonActiveAgents.ps1 -client_id "<client_id>" -client_secret "<client_secret>" -tenant_id
"<tenant_id>" -cloudServiceDnsName "<cloudServiceDnsName>" -inactiveDays "<inactiveDays>" -
platformApiPort "<port number>"
```

client_id

This is the **Application ID** that is below the **Enable API key** access check box in the **Remove Access Settings** page in iC3.

client_secret

This is the **API Key** in the iC3 **Settings** page.



Remote Access Settings

☑ Enable remote MMC client access

Application ID

21d13012-2168-471c-be02-41984c94fd40

☑ Enable API key access

Application ID

52b8dbb9-fb8b-437a-8920-f23c8e0199b9

API Key

GN5kpf41Pg2YbQMGs+MBxTsS0Ig3wOZN0PYzBem2PqX8MVnD6ylHC+zntr8wgtxu6x94geYM1QJ/ozu1zhFh/A==

tenant_id

- `TenantID`, see "Microsoft Azure AD Authentication" on page 11 for instructions on getting this GUID for Microsoft Azure authentication. For Windows Directory and LDAPS this is generated by the deployment tool and you should have made a note of it already.

cloudServiceDnsName

This is your iC3 URL. Do not included the `https://` or the port when entering, for example `test.ic3.avecto.com`.

inactiveDays

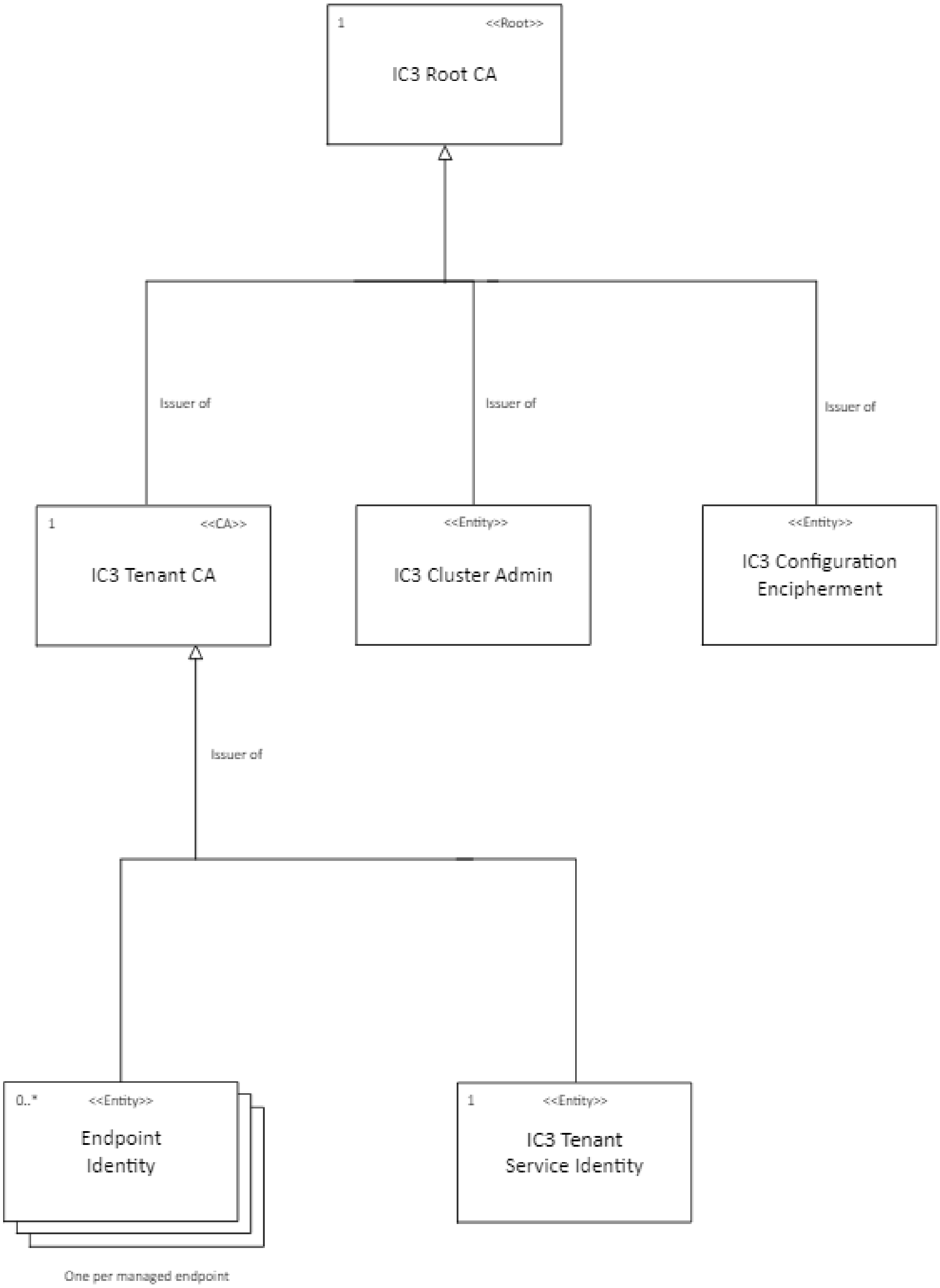
This is the number of days the tenant has been inactive for and has to be a minimum of 15.

platformApiPort

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

iC3 Certificate Chain

iC3 uses certificate-based security to ensure identity and communications security. The following section describes 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 iC3 deployment tool are desired.


1
<<Root>>
IC3 Root CA
Issuer of
Issuer of
Issuer of
1
<<CA>>
IC3 Tenant CA
<<Entity>>
IC3 Cluster Admin
<<Entity>>
IC3 Configuration Encipherment
Issuer of
0..*
<<Entity>>
Endpoint Identity
1
<<Entity>>
IC3 Tenant Service Identity
One per managed endpoint