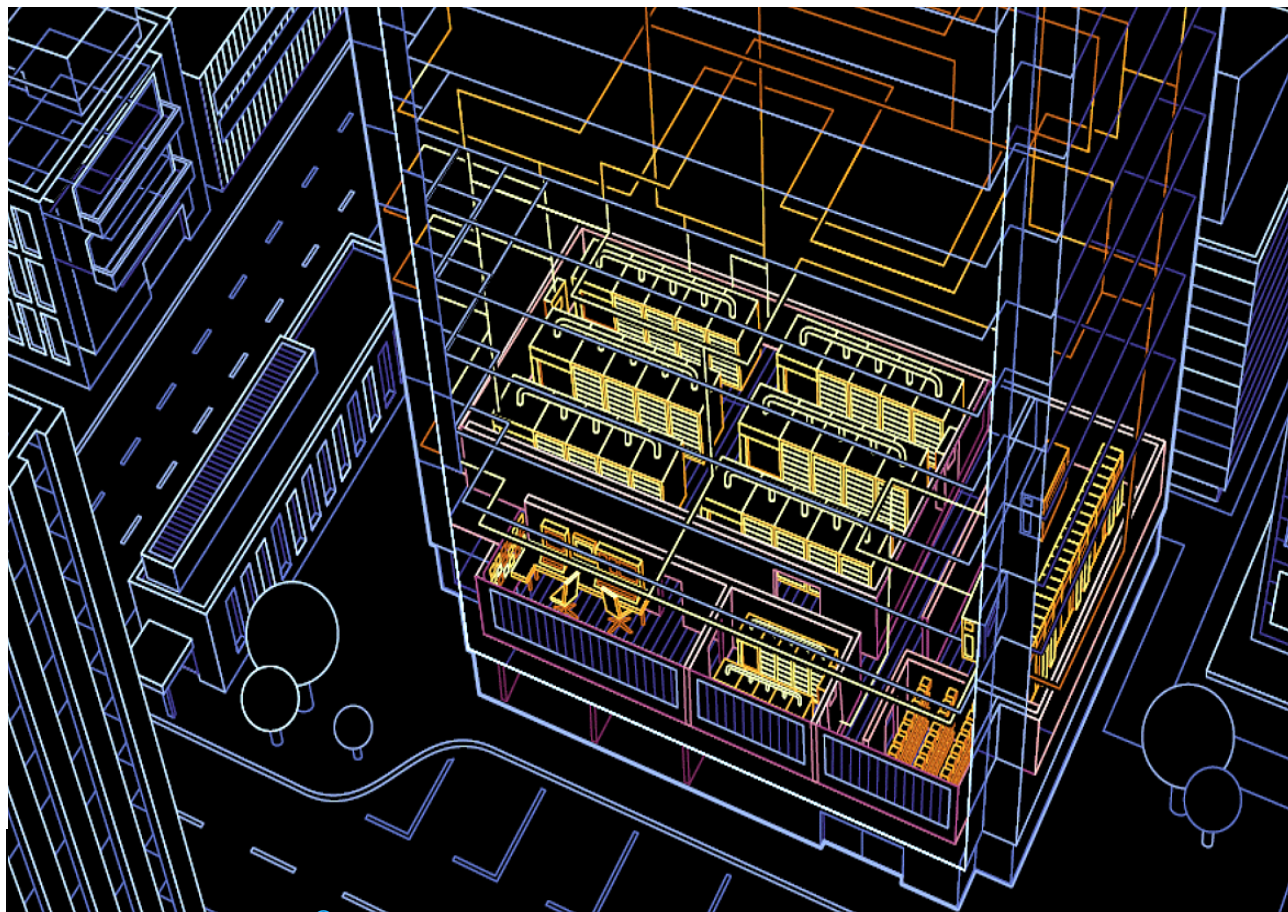




Decathlon® for Data Centers

Intel DCM Integration
User Manual

System Version 6.0

Power and productivity
for a better world™



Decathlon® for Data Centers

Intel DCM Integration User Manual

System Version 6.0

NOTICE

This document contains information about one or more ABB products and may include a description of or a reference to one or more standards that may be generally relevant to the ABB products. The presence of any such description of a standard or reference to a standard is not a representation that all of the ABB products referenced in this document support all of the features of the described or referenced standard. In order to determine the specific features supported by a particular ABB product, the reader should consult the product specifications for the particular ABB product.

ABB may have one or more patents or pending patent applications protecting the intellectual property in the ABB products described in this document.

The information in this document is subject to change without notice and should not be construed as a commitment by ABB. ABB assumes no responsibility for any errors that may appear in this document.

Products described or referenced in this document are designed to be connected, and to communicate information and data via a secure network. It is the sole responsibility of the system/product owner to provide and continuously ensure a secure connection between the product and the system network and/or any other networks that may be connected.

The system/product owners must establish and maintain appropriate measures, including, but not limited to, the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, and so on, to protect the system, its products and networks, against security breaches, unauthorized access, interference, intrusion, leakage, and/or theft of data or information.

ABB verifies the function of released products and updates. However system/product owners are ultimately responsible to ensure that any system update (including but not limited to code changes, configuration file changes, third-party software updates or patches, hardware change out, and so on) is compatible with the security measures implemented. The system/product owners must verify that the system and associated products function as expected in the environment they are deployed.

In no event shall ABB be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB be liable for incidental or consequential damages arising from use of any software or hardware described in this document.

This document and parts thereof must not be reproduced or copied without written permission from ABB, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license. This product meets the requirements specified in EMC Directive 2004/108/EC and in Low Voltage Directive 2006/95/EC.

TRADEMARKS

All rights to copyrights, registered trademarks, and trademarks reside with their respective owners.

Copyright © 2003-2016 by ABB.
All rights reserved.

Release: November 2016
Document number: 2PAA115263-600 A

Table of Contents

About this User Manual

User Manual Conventions	5
Warning, Caution, Information, and Tip Icons	5
Terminology	6

Section 1 - Overview

Section 2 - Installation and Configuration

Installing Intel Data Center Manager	9
Installation Steps	9
Post Installation Step	9
Installing the Intel DCM Integration	10
Overview	10
Installation Steps	10
Post-Installation Configuration	10
Time Synchronization	26

Section 3 - Maintenance

Backup and Restore Procedures	27
Import and Export	27
Server node creation using the Bulk data manager	28

Section 4 - Client Certificate Authentication

Certificate Creation or Identification	31
Application Server Certificate Installation	31
Installing a user certificate on a client node	32

- Intel DCM Server Certificate Configuration 40
 - Installing a client certificate on the server node 41
- Application Server Configuration of the Intel DCM Integration Service 44
 - Intel DCM Integration Client Certificate Authentication Diagnostics 46
- Appendix A - Intel® Data Center Manager Installation**
 - Prerequisites 49
 - Computer Hardware..... 49
 - Operating System..... 51
 - Installation Steps 51
 - Post Installation Steps 61
 - IntelDCMConfigUtil Configuration 62
 - IntelDCMConfigUtil Usage..... 62
 - IntelDCMConfigUtil Command Line Reference..... 63
 - IntelDCMConfigUtil Command Line Examples 64
- Appendix B - Intel DCM Integration 6.0.1 Installation**
 - Installation Steps 65
- Appendix C - Intel DCM Object Types**
 - IntelDCMServer 71
 - Properties 72
 - Alarms 75
 - Views 75
 - IntelDCMServerBasic 78
 - Properties 79
 - Alarms 81
 - Views 81
- Appendix D - Troubleshooting**
 - Using the Service Status Object 85
 - Using the Intel® Data Center Manager console 89
 - Communication between Intel DCM Connectivity Node and Intel DCM Server node.. 91

Inlet temperature not being reported for some HP servers91

Appendix E - Performance and Capacity

Number of supported Server nodes93

Time to create & establish servers.....93

Appendix F - Online/Offline Configuration Changes

Appendix G - Exporting a Certificate to a File

Revision History

Updates in Revision A.....107

About this User Manual



Any security measures described in this User Manual, for example, for user access, password security, network security, firewalls, virus protection, etc., represent possible steps that a user of a Decathlon for Data Centers system may want to consider based on a risk assessment for a particular application and installation. This risk assessment, as well as the proper implementation, configuration, installation, operation, administration, and maintenance of all relevant security related equipment, software, and procedures, are the responsibility of the engineering team.

This user manual contains information about the Intel DCM Integration. It is recommended that you attend the applicable training courses offered by ABB.

User Manual Conventions

Microsoft Windows conventions are normally used for the standard presentation of material when entering text, key sequences, prompts, messages, menu items, screen elements, etc.

Warning, Caution, Information, and Tip Icons

This User Manual includes Warning, Caution, and Information where appropriate to point out safety related or other important information. It also includes Tip to point out useful hints to the reader. The corresponding symbols should be interpreted as follows:



Electrical warning icon indicates the presence of a hazard that could result in *electrical shock*.

- 

Warning icon indicates the presence of a hazard that could result in *personal injury*.
- 

Caution icon indicates important information or warning related to the concept discussed in the text. It might indicate the presence of a hazard that could result in *corruption of software or damage to equipment/property*.
- 

Information icon alerts the reader to pertinent facts and conditions.
- 

Tip icon indicates advice on, for example, how to design your project or how to use a certain function

Although Warning hazards are related to personal injury, and Caution hazards are associated with equipment or property damage, it should be understood that operation of damaged equipment could, under certain operational conditions, result in degraded process performance leading to personal injury or death. Therefore, fully comply with all Warning and Caution notices.

Terminology

Table 1 lists the terms and definitions used in this user manual.

Table 1. Terminology

Term/Acronym	Description
PPA	Process Portal A
DCIM	Data Center Infrastructure Management
DCM	Data Center Management
BMC	Baseboard Management Controller
IPMI	Intelligent Platform Management Interface

Section 1 Overview

ABB's Intel DCM Integration package provides the functionality required for integrating the Intel® Data Center Manager product into Decathlon for Data Centers.

It provides the ability from within Decathlon for Data Centers to access the status of servers in a data center.

The power of Decathlon for Data Centers can now be brought to bear on this additional facet of the data center runtime environment.

Server power, temperature and airflow, where supported, are all made available for use in monitoring, as well as inputs to advanced level functionality like aggregation, alarming, historizing, analysis, condition monitoring, reporting etc.

The Intel DCM Integration aspect system uses the 800xA OPC Framework together with specifically developed object types to provide a simple yet comprehensive solution.

The integration offers a single point of configuration where the BMC address for each server is the only information that is required to associate an Intel DCM Server object with a physical server.

It can handle up to 5,000 servers per Decathlon for Data Center's system.

The rest of this document contains the instructions to install, configure and use the Intel DCM Integration.

Appendices are used to lessen the complexity of the main document and when the information is optional or an advanced topic.

Prior to installation, you should decide on the security required between the Intel DCM Integration and the Intel Data Center Manager package as this determines some of the installation and configuration.

You need to separately configure the communication channel security and the authentication/authorization. You need to configure both server and client to use the same settings for both of these for the integration to work successfully.

For the most secure system, the following are recommend:

- https/TLS for the communication channel. (The other option is to use http). This encrypts the channel and provide a highest level of security.
- Client Certificate Authorization for user authorization. (The other option is to use *Anonymous*).

This ensure that only known and authorized clients like the Intel DCM Integration, are able to connect to the Intel Data Center Manager server.

Configuring client certificate authentication is complex and it is suggested that you initially use *Anonymous* until you have the system installed, configured and working before switching to use certificates. You can do this after the system is working.

The following are the high level steps required to get a working system:

- Install Intel Data Center Manager. Refer to [Section 2, Installation and Configuration](#) and [Appendix A, Intel® Data Center Manager Installation](#).
- Install the Intel DCM Integration. Refer to [Section 2, Installation and Configuration](#) and [Appendix B, Intel DCM Integration 6.0.1 Installation](#).
- Configure the Intel DCM Integration. Refer to [Post-Installation Configuration](#) for the Intel DCM Integration in section 2).

For setting up client certificate authorization, refer to [Section 4, Client Certificate Authentication](#). This outlines the steps for both clients and server.

[Section 3, Maintenance](#) describes backup & restore and import & export processes that you may require during operation.

[Appendix A, Intel® Data Center Manager Installation](#) & [Appendix B, Intel DCM Integration 6.0.1 Installation](#) cover the detailed installation instruction. Other appendices cover an explanation of the object types used in the integration, the performance & capacity numbers and a troubleshooting section to help diagnose problems.

Section 2 Installation and Configuration

As the name suggests the Decathlon for Data Center's Intel DCM Integration relies on a separate Intel® Data Center Manager installation for operation.

Our distribution includes installation packages for both Intel® Data Center Manager, and the ABB developed Intel DCM Integration.

The Intel® Data Center Manager is a package produced by Intel and redistributed by ABB.

Installing Intel Data Center Manager

The Intel® Data Center Manager (DCM) by Intel Corporation is typically installed prior to installing the Intel DCM Integration though it can be installed afterwards.

The Intel® Data Center Manager installation is distributed as a Windows Installer (.msi) package.

For performance reasons Intel Data Center Manager is installed on its own dedicated server computer and that server must comply with the minimum hardware requirements set out in Intel Data Center Manager Installation appendix.

Installation Steps

Follow the direction for installing the Intel® Data Center Manager as detailed in [Appendix A, Intel® Data Center Manager Installation](#)

Post Installation Step

There will be post installation steps if client certificate authentication is to be used for user authorization/authentication.

Refer to [Section 4, Client Certificate Authentication](#) for the steps required on the server to support this.

Installing the Intel DCM Integration

Overview

The following are the minimum software required to install the Intel DCM Integration package. Specific software may vary depending on project requirements:

- Operating System: Windows 8 or 8.1 or Windows 2012 Server R2 (or later) (as required by System 800xA)
- Microsoft Office (as required by System 800xA)
- System 800xA 6.0.1, 6.0.2, & 6.0.3
- DCIMLib 6.0-0 or above



Intel DCM Integration 6.0.1 can also be installed on top of an existing Decathlon for Data Center v6.0.1 system.

The Decathlon for Data Centers Intel DCM Integration package is distributed as a Windows Installer (.msi) package.



For performance reasons it is recommended that the Intel DCM Integration service should be installed on its own dedicated 800xA Application Server.

Installation Steps

Follow the direction for installing the Intel DCM Integration as detailed in [Appendix B, Intel DCM Integration 6.0.1 Installation](#).

Post-Installation Configuration

The following section details the steps required after installation to setup and configure the Intel DCM Integration.

Load the System Extension

The system extension for the Intel DCM Integration needs to be manually loaded after the installation completes.

1. Start the 800xA Configuration Wizard.
Select '**System Administration**', select the system and then '**System Extension Load**'. In the left hand pane select **Intel DCM Integration Extension**, and select '>' and **Next** to complete the operation.

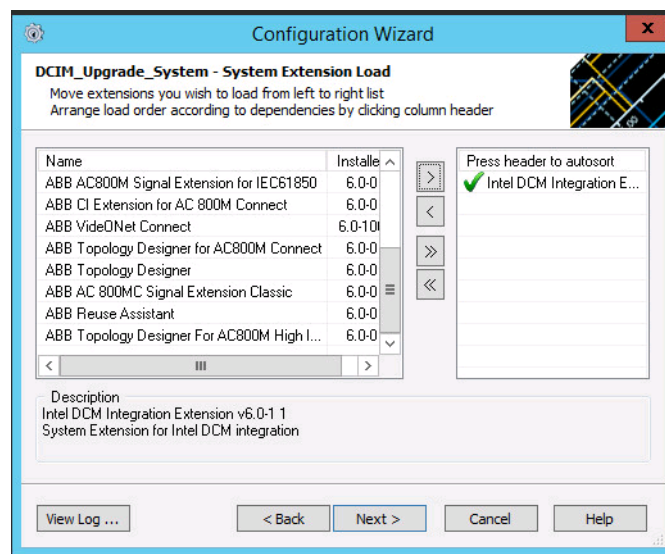


Figure 1. 800xA Configuration Wizard

2. Click **Finish**.

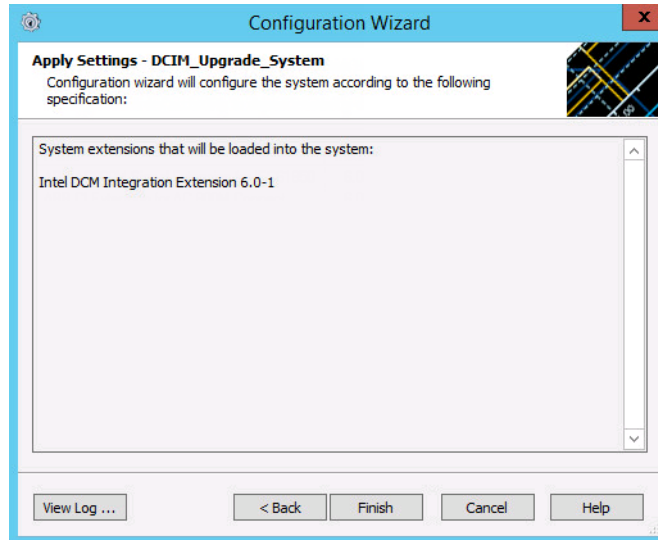


Figure 2. Complete System Extension loading

Figure 3 shows the loaded Intel DCM Integration Extension in PPA.

System Extensions	9/12/2016 11:18:...	800xAService	This ...	False	System Extensi...	1
System Settings	8/17/2016 3:53:4...	ABB 800xA Base		False	System Settings	1

DCIM_Upgrade_System:System Extension						
SystemExtensions Identification						
Name	Version	Build number	Description	Installed on this node	Successf	
ABB Engineering Base	6.0-0	2	This system extension provides a special configuration of ...	X	X	
Decathlon for Data Centers Core	6.0-1	0	ABB Decathlon for Data Centers Core System Extension	X	X	
ABB Inform IT Scheduler	6.0-0	1	Service and standard plug-ins for scheduling jobs in Indus...	X	X	
ABB Function Designer	6.0-0	3	ABB Function Designer is the engineering portal for plant...	X	X	
ABB APC System Extension	3.1-0	40	ABB APC System Extension	X	X	
Intel DCM Integration Extension	6.0-1	1	System Extension for Intel DCM integration	X	X	
ABB 800xA Base	6.0-100	222	ABB 800xA Base	X	X	
ABB APC Runtime FD Extension	3.1-0	40	This extension needs to be loaded in case the MPC applic...	X	X	
ABB Signal Extension for AC800M Connect	6.0-0	8	ABB Signal Extension for AC800M Connect provides the C...	X	X	
AC800M Connect	6.0-0	22000	AC800M Connect gives you controller integration to AC8...	X	X	
ABB Inform IT Calculations	6.0-0	0	Create, configure and execute calculation aspects.	X	X	
ABB DM & PM Application	6.0-0	2	ABB Document Manager (DM) provides functionality for b...	X	X	
ABB SFC Viewer	6.0-0	1	This system extension loads the SFC Viewer to the system	X	X	
ABB Central Licensing System	6.0-1	54	ABB Central Licensing System Extension	X	X	
ABB Function Designer for AC800M Connect	6.0-0	14	ABB Function Designer for AC800M Connect. This syste...	X	X	

III						
Name	Version	Build number	Description	Installed on this node	Successfully loaded	
Intel DCM Integration Extension	6.0-1	1	System Extension for Intel DCM integration	X	X	

Figure 3. Intel DCM Integration Extension loaded in PPA

For more information, refer to *Adding System Extension* section of *System 800xA 6.0 Post Installation (3BUA000156*)*.

Create and configure the Service Group and Service Provider

The Intel DCM Monitor Service is created by the product installer. To use the Intel DCM Service, you will need to configure both a Service Group and a Service Provider.

Create the Service Group.

1. Navigate to **Service Structure > IntelDCMMonitor, Service**.
2. Right-click on the object and select **New Object...**

3. Select **Service Group**, and enter a name, such as **Intel_DCM_Monitor_SG**.
4. Click **Create**.

Configure the Service Group. The **Special Configuration** tab has the configuration for communicating with the Intel DCM Manager Web service.

There are fields to setup the URL to the web service, whether TLS will be used (http or https), the authentication scheme to be used and the interval at which real-time data is retrieved.

When *Anonymous* is used for the authentication scheme there is no further setup required on the client or server side.

Selecting *Certificate* indicates the use of Client Certificate Authorization.

Refer to [Section 4, Client Certificate Authentication](#) for the steps to install the certificates and configure the field in this dialog on the client(s).

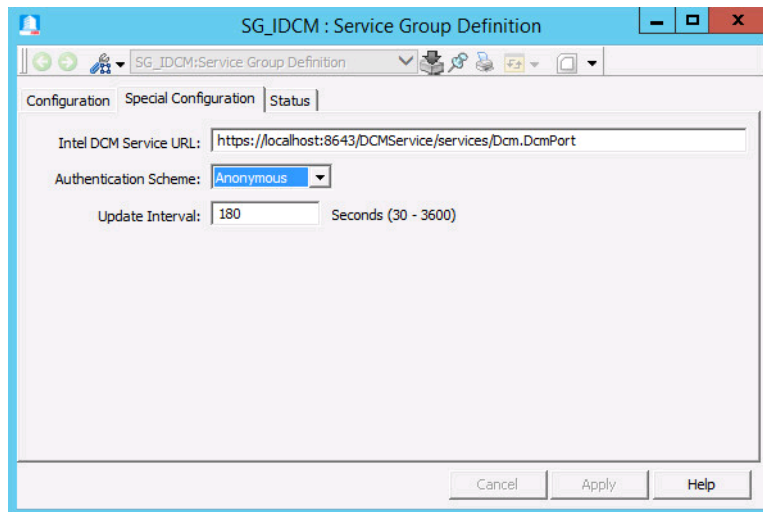


Figure 4. Special Configuration tab



The format of the URL should match the installation of the Intel Data Center Manager TLS/https option. Typically TLS/https will be enabled and the first option listed below for the URL format must be used.

Intel DCM Service URL:

This has the format:

- Using TLS/https:
<https://ServerIdentifier:8643/DCMService/services/Dcm.DcmPort>
- No TLS/http:
<http://ServerIdentifier:8688/DCMService/services/Dcm.DcmPort>

Where *ServerIdentifier* is the IP address or URI of the server where the Intel Data Center Manager was installed.

This may also be a node identifier if this is defined in the hosts ini file in the C:\Windows\System32\drivers\etc directory.

The port numbers (8643 or 8688) are the defaults for the Intel Data Center Manager. These will need to be changed to match those specified during the Intel Data Center Manager configuration if necessary.

Authentication Scheme:

- Either Anonymous or Certificate. This setting needs to be identical to the setting configured in the Intel Data Center Manager system.

Refer [Section 4, Client Certificate Authentication](#) to configure the security authentication.

Update Interval:

The Update Interval is the period the Intel DCM Integration reads real-time information for configured servers.

The real-time data changes only at the granularity rate setup when the Intel Data Center Manager was installed.

To ensure that changes are picked up in a timely way we recommend that the Update Interval be set to half the configured granularity.

The following are the recommended Update Interval providing that the granularity was set to the recommendations as specified in [Appendix A, Intel® Data Center Manager Installation](#).

- <1000 servers: 30 seconds (this is the minimum allowed)
- 1001-5000 servers: 90 seconds

- 5001-10000 servers: 180 seconds

Create the Service Provider.

1. Navigate to **Service Structure > IntelDCMMonitor, Service > Intel_DCM_Monitor_SG** (or the name of the group created in the previous step).
2. Right-click on the object and select **New Object....**
3. Select Service Provider, and enter a name, such as **Intel_DCM_Monitor_SP**.
4. Click **Create**.
5. On the **Configuration** tab open the Node list box and select the computer where the Intel DCM Integration was installed. Click **Apply** to complete the configuration.

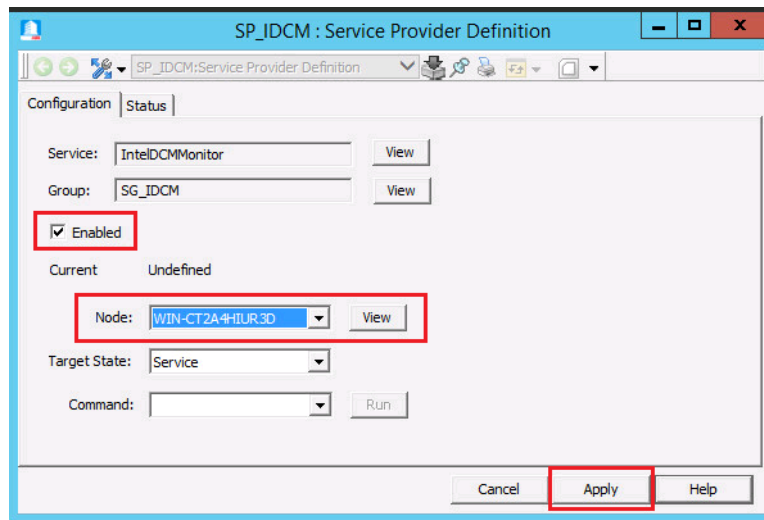


Figure 5. Configuration tab



The Application Server name where the **IntelDCMMonitor** Service was installed will need to be selected from the Node drop-down in the Service Provider object.



The Enabled check boxes for both the Service Group and Service Provider need to be checked for the service to be started as indicated by the 'Service' state. Once the service is enabled and in the Service state, the system will create a Server Status Object as a child of the Service Provider, which can be used to monitor the internal health of the service. The status object is described in more detail in Appendix D.



The Service Provider should be disabled (in the Undefined state) before creating the Intel DCM Server Network as described in the next section.

Creating the Intel DCM Server Network.

1. Navigate to the **Control Structure > Root**.
2. Right click and select **New Object...**
3. Open the 'Intel DCM Object Types' and select **IntelDCMServerNetwork**. Enter a name such as **Intel_DCM_Network**.
4. Click **Create**.

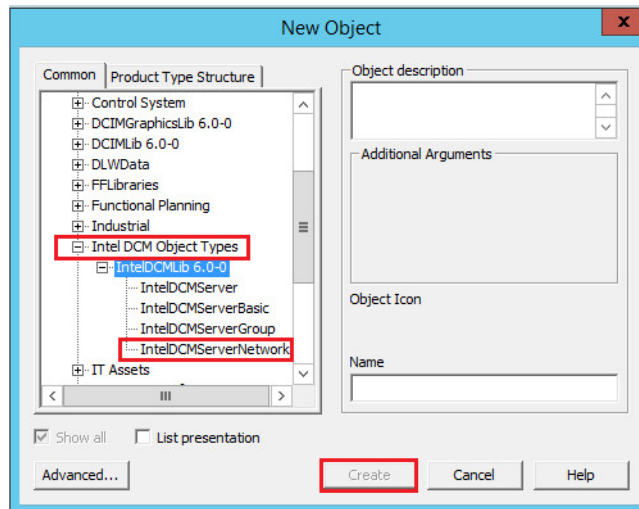


Figure 6. New Object

5. Select the **Generic Data Source Definition** aspect in the just created object. In the Service Group list box, select **Service Group** (see section [Create the Service Group](#)), and select **Apply** to complete the configuration.

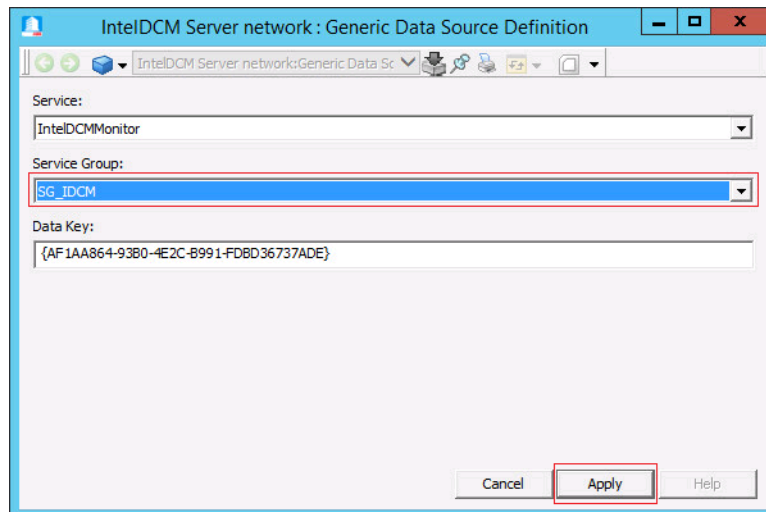


Figure 7. Generic Data

Creating Server Groups. An **IntelDCMServerGroup** object represents a logical grouping of servers that share the same BMC username and password. All servers with the same BMC credentials should be created under the same Server Group.

1. Navigate to the **Control Structure > IntelDCMServerNetwork** object created above.
2. Right click and select **New Object...**

3. Select **IntelDCMServerGroup** and enter a name, such as **Intel_DCM_SG_1**.

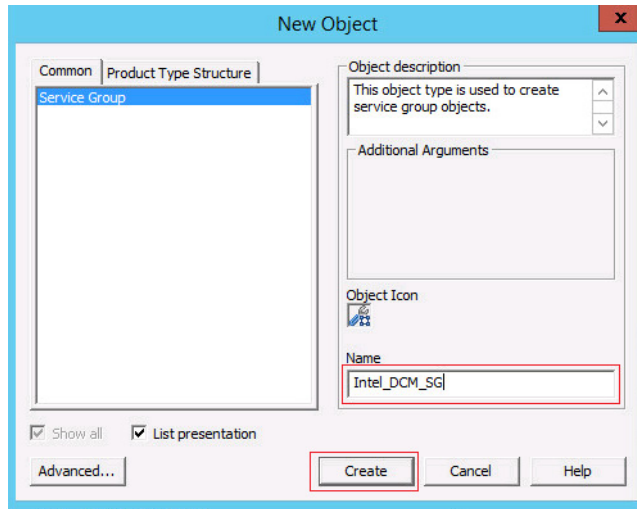


Figure 8. Product Type Structure tab

4. Enter the username and password and select **Apply** to complete the process. Repeat steps 1 to 4 to create other server groups as required. In most data centers BMC accounts will have been setup to enhance security. However this can be left blank if no BMC accounts have been created.

Figure 9. DCM Server Group Configuration

- Repeat steps 1 to 4 to create other server groups as required.



When the username and password are changed, the IPMIMonitor service must be restarted for the change to take effect. (Navigate to the **Service Structure > IntelDCMMonitor > Intel_DCM_Monitor_SG > Intel_DCM_Monitor_SP**. Deselect the **Enabled** checkbox and **Apply**, wait for the state to go into 'Undefined', then select the **Enabled** checkbox and **Apply**).

The Username and Password can be reset to empty strings after being previously set, by deleting all the characters from the Username field and selecting **Apply**.

Creating Intel DCM Servers

Intel DCM Servers objects represent actual physical servers. The description, definition and use of these object types is contained in [Appendix C, Intel DCM Object Types](#)

- Navigate to the **IntelDCMServerGroup** into which you want to create server (for example **Control Structure > Intel DCM Network, IntelDCMServerNetwork > Intel DCM SG, IntelDCMServerGroup**).

2. Right click and select **New Object...**
3. Select **IntelDCMServer** or **IntelDCMServerBasic**, and enter a name (e.g. Server 1).



To select a user-defined server object type, select the **Show All** check box to view other object types.

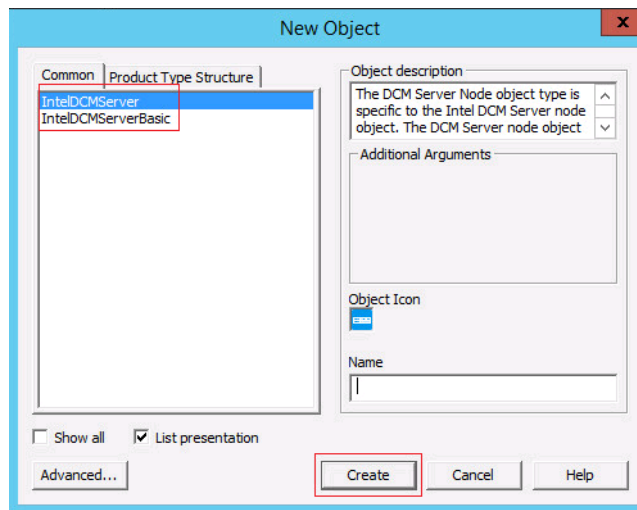


Figure 10. New Object

4. Click **Create**.

5. Navigate to the **DCM Server Node Configuration** aspect of the just created object. Enter the BMC address in the value field and select **Apply** to complete the configuration.

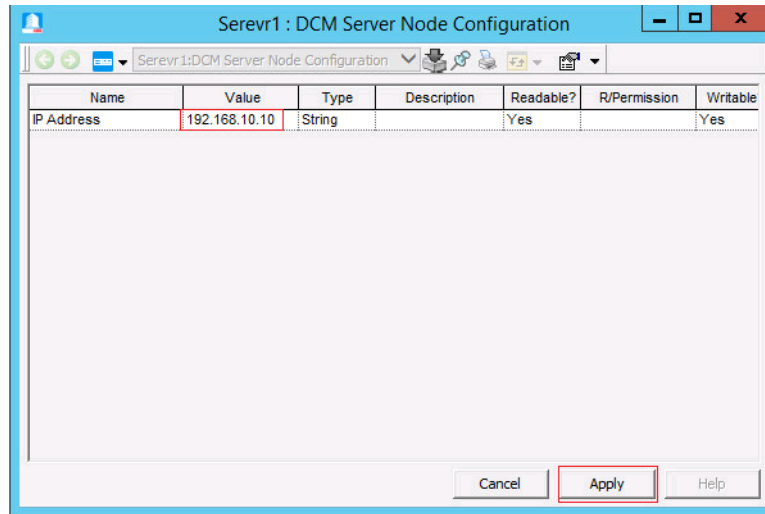


Figure 11. DCM Server Node Configuration

6. Navigate to the faceplate (i.e. the '**Detailed View**' aspect) for the newly added server. Intel DCM will establish connection to the server, which will take some time. 800xA displays and clients will show the real-time values for the server after this startup period.



It is possible to create the Intel DCM Server objects and/or configure the BMC IP address using the 800xA Bulk Data Manager.



There is a delay after the server is established and before the initial Real-time values are received. It can take up to the granularity period setup during the Intel DCM Manager installation for the initial values to be shown.

Thereafter values will change no faster than the granularity rate.

Unit Conversion

Intel Data Center Manager returns real-time server information in a fixed set of units (i.e. temperature always in Celsius, power in Watts etc.). The Intel DCM Integration allows for units to be converted. The unit selection impact all servers (i.e. the selection is global and not per server).

Unit conversion is done in two steps: select the unit conversion and then select/modify the text representing the unit in the display.

1. Navigate to the **Service Structure > IntelDCMMonitor, Service Object** and select the **Special Configuration** tab.

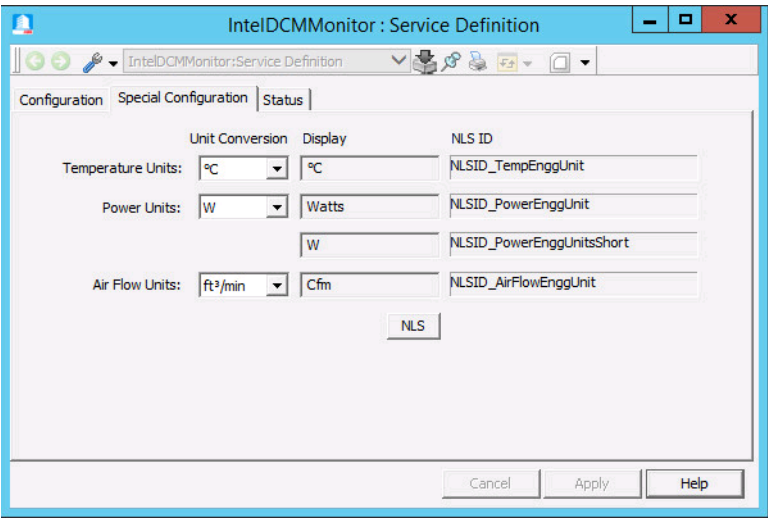


Figure 12. Service Structure, Special configuration tab

2. To select the unit conversion for the unit to be changed e.g. for temperature unit the list box presents choices of °C (degrees Celsius) or °F (degrees Fahrenheit).

3. Selecting the NLS button will bring up the NLS Resource Manager.

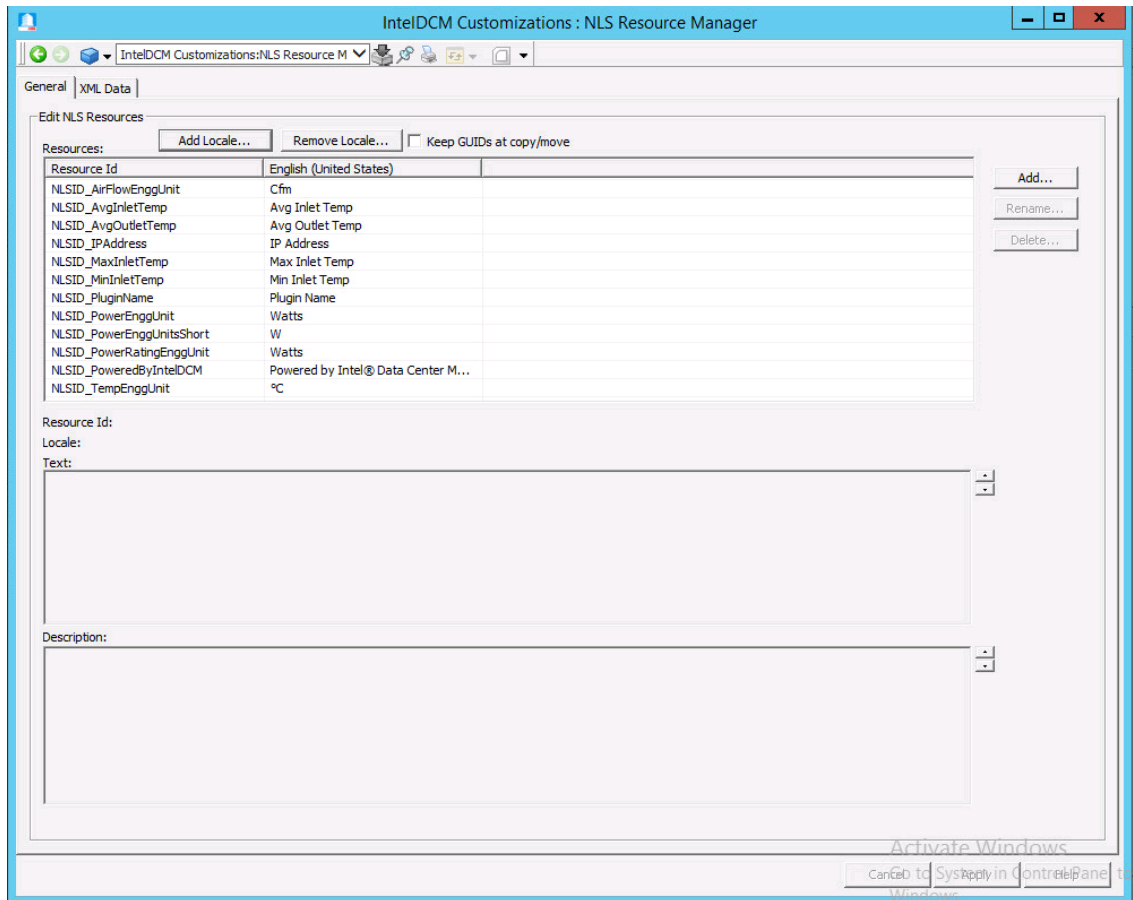


Figure 13. Intel DCM Customization

Select the resource Id to be modified and update it in the Text field. Selecting **Apply** will complete the change. Close the NLS Resource Manager window.



The **IntelDCMMonitor** Service needs to be restarted before the modified unit conversion settings take effect.

User Rights and Security

For more information on User Rights and Security, refer to *System 800xA Administration and Security (3BSE037410*)*.

Windows Firewall Exceptions for exe and ports

The *DCMIPMIService.exe* must be included in the Windows Firewall exception list on the Intel DCM connectivity node.

The ports that are in use for the Intel DCM Server must be included in the TCP port exception list of the Windows Firewall on the respective nodes. For example: If Intel DCM is configured to run with HTTPS on port **8643**, then this port must be included in the Firewall exception list on the Intel DCM Server node.

On the Intel DCM server node allow outgoing requests on UDP port 623 for DcmServer.exe.

On the Intel DCM server node allow incoming requests on HTTPS ports 8643 for tomcat6.exe.

On the 800xA Application Server node that runs Intel DCM integration service allow outgoing requests to HTTPS port 8643 for DCMIPMIService.exe.

Time Synchronization

All computers in a Decathlon for Data Centers system must have the same time. This includes the node running the Intel Data Center Manager.

Time synchronization is required for the correct operation of the system and to ensure that data is consistent across the system.

For information on configuring time synchronization, refer to *System 800xA Network Operations manual (3BSE034463*)*.

Section 3 Maintenance

Backup and Restore Procedures

Backup is used within System 800xA to copy the configuration of an entire system, so that it can be restored on another system. The Backup and Restore procedure must be performed in an order to save and restore a complete 800xA system including the Intel DCM Integration configuration data like Intel DCM Server Network, Intel DCM Server Group and Intel DCM Server node objects. 800xA backup and restore utility is used to save the Aspect directory and other System 800xA information.

For more information on Backup and Restore functions, refer to *System 800xA Maintenance (3BSE046784*)*.

Import and Export

The Import/Export tool allows the user to move applications (i.e. import and export data) to and from any 800xA System. The data is saved as objects and aspects in archive files (.afw). The Import/Export tool allows you to store and restore objects, aspects, and entities. It is also possible to view the contents of an archive file. For more information on Import/Export, refer to *System 800xA Maintenance (3BSE046784*)*.



After Importing the Intel DCM Integration configuration data like Intel DCM Server Network, Intel DCM Server Group and Intel DCM Server node objects, the DCMIPMIService.exe must be restarted.

Server node creation using the Bulk data manager

The following care must be taken while creating Intel DCM Server nodes using the Bulk Data Manager:

1. Create the nodes without specifying the IP of the Intel DCM Server node.
2. Modify the nodes by specifying the IP of the Intel DCM Server node.

By following above steps, the update of the latest object type is done without affecting the already configured objects.

Section 4 Client Certificate Authentication

Intel DCM Integration supports client certificate authentication in addition to anonymous connections (no authentication). Client certificate authentication requires more effort to setup than the authentication for the anonymous connections, but provides the additional assurance that only authorized Decathlon for Data Centers clients/users are able to connect to the Intel Data Center Manager server. Client certificate authentication, together with TLS/https, provides a high level of security by both securing the communication channel and ensuring that only valid recognized clients are able to connect.

Client certificate authentication requires the installation of the same certificate on both the client (the Application Server running the Intel DCM Integration) and server (the Intel DCM server collecting the data). To install, follow the below steps:

1. [Certificate Creation or Identification](#): An appropriate certificate may need to be obtained from an appropriate issuing authority, or may be installed with the user account (in that case, it needs to be exported for installation on the server).
2. [Application Server Certificate Installation](#) (if obtained from an issuing authority)
3. [Intel DCM Server Certificate Configuration](#)
4. [Application Server Configuration of the Intel DCM Integration Service](#)

Client certificates are stored in the Windows operating system, either in the personal certificate store of the windows user, or in the Local Computer store. Server certificates are stored within the Tomcat server used by the Intel DCM software service. One or more certificates may be used, depending on the authentication

approach implemented. [Table 2](#) shows the authentication approach.

Table 2. Authentication Approach

Authentication Approach	Certificate usage	Client Certificate Storage	Server Certificate Configuration	Comments
Anonymous	None	None	None	No secure access to Intel DCM service
Role-based	Shared; application-specific	User (personal); installation using each account	Single certificate (+ authentication chain)	Possible to limit users on client
Role-based	Shared; application-specific	Local Machine); installation using administrator	Single certificate (+ authentication chain)	All users on client have access
User-based	Per-user; not required to be application-specific	User (personal); installation using each account	Per-user certificate (+ authentication chain)	Can restrict access to specific users

A security assessment should be conducted to determine the appropriate authentication approach for each installation. User-based authentication provides granular access control on the server, and may be able to leverage existing domain certificates, but may require additional client setup if an application-specific certificate is used. Typically, only the account which runs the Intel DCM Integration service is required to be authenticated with, although other users may be granted access for diagnostics purposes. Role-based security may be sufficient for most security needs.



There are multiple ways to work with certificates on Windows. For consistency reason this guide uses the Microsoft Management Console (MMC) for managing certificates on client (Application Server) nodes.

Certificate Creation or Identification

A certificate used on an Intel DCM client should be obtained from an appropriate Certificate Authority (CA). The certificate is installed on both the client and server, and the certificate format must be compatible with the Java keytool that is used to install client certificates on the Intel DCM server. The certificate should be digitally encoded (DER) and must have PKCS12 (PFX) format.



BASE64 encoding (PEM) is not supported.

For user-based authentication, it is possible to use a certificate created for the client user account (e.g. a certificate assigned to a corporate Windows Domain account). If available, this certificate must be exported from its store to a file to be used for installation on Intel DCM Server. Refer to [Appendix G, Exporting a Certificate to a File](#) to know the procedure for accessing this type of certificate.

For user- or role-based authentication, a certificate for this application may need to be created and installed.

If the certificate is not a root or self-signed certificate, any one of the following conditions should be met:

- The certificate file must include the entire certificate chain (including the root certificate).
- The certificate chain must be made available in a separate file.

Each certificate location has a number of stores, but the Intel DCM Integration feature uses the Personal store (also known as “My”) to search for certificates, and searches for the certificate in the configured store using the common name field (CN).

Application Server Certificate Installation

The client certificate(s) must be installed in the “My” (Personal) certificate store of either Current User or Local Machine location on the Intel DCM Integration service Application Node. If the Current User location is used, you must log in as each user account that is expected to use Intel DCM in order to install the appropriate certificate. Depending on the Authentication Scheme used, you may be installing

the same certificate to multiple accounts, or you may be installing a certificate unique to each user.



The user account that runs Decathlon for Data Centers Intel DCM Integration service must have access to the appropriate certificate on the Application Server node in order to successfully authenticate with Intel DCM server.

Installing a user certificate on a client node

This option is used when a certificate is obtained from a certificate authority (or if a certificate was exported from another node and was not previously installed on the Application Server node).

The certificate must be digitally encoded (DER) and must be in PKCS12 format.

To install a user certificate on a client node, do the following steps:

1. Start the MMC console (type MMC in the Windows Search Bar, click **File** and select **Add / Remove Snap-ins**. Select **Certificates** and click **Add >**).

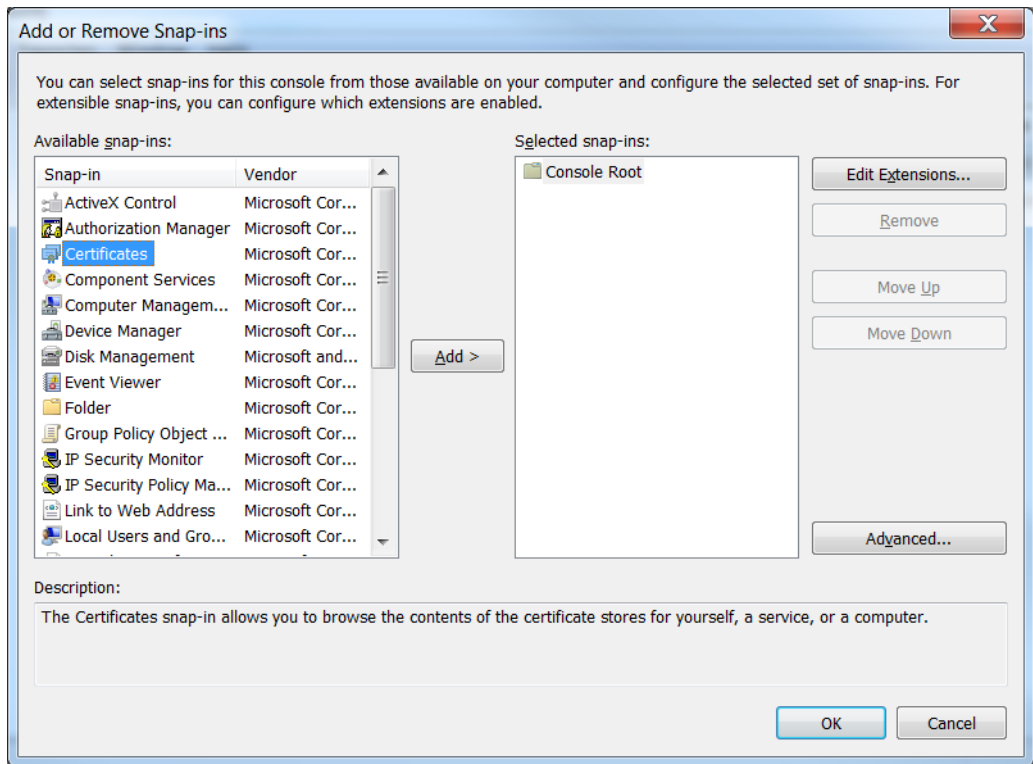


Figure 14. Add or Remove snap-ins

2. Select **My user account** for the Current User store location or **Computer account** for the Local Machine store location and click **OK**.

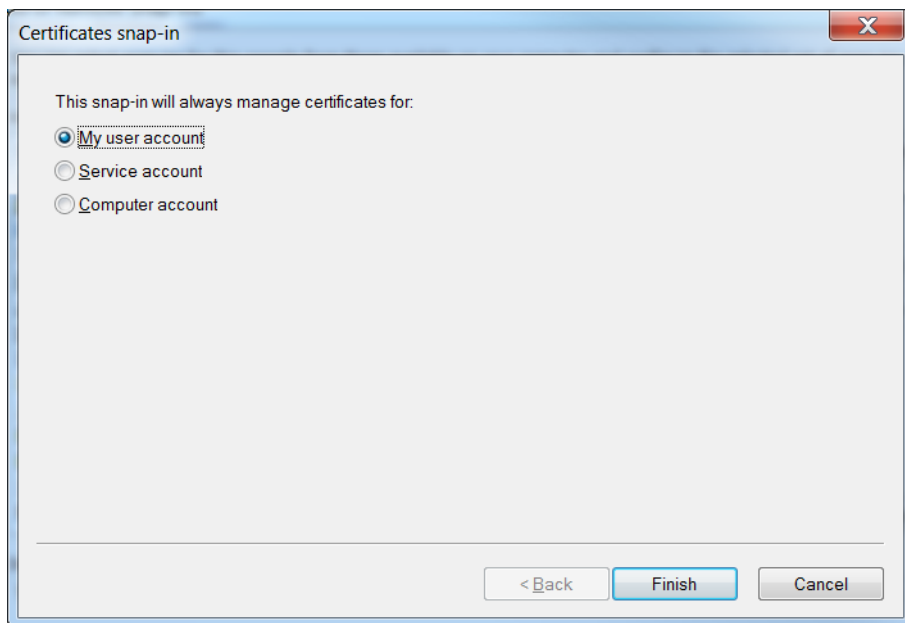


Figure 15. Certificate snap - ins

3. Navigate to Certificates > Current User (or Certificates (Local Computer))/Personal/Certificates (if no certificates are currently installed in the store, the last path node (Certificates) will not be present).

4. In the **Actions** pane, click **More Actions/All tasks/Import**.

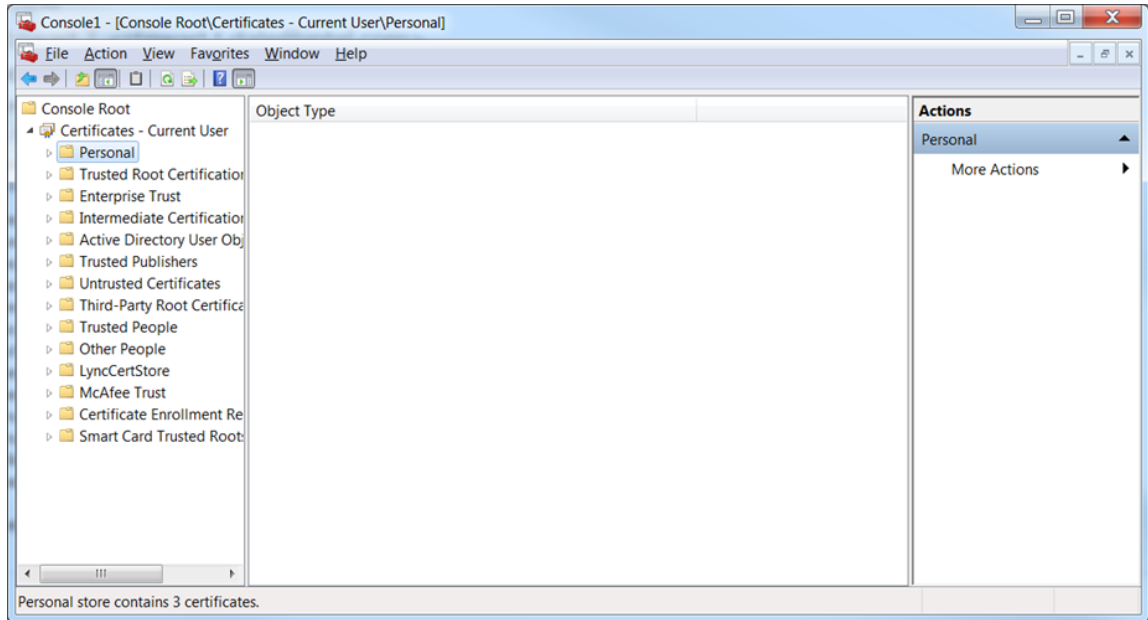


Figure 16. Console

5. Click **Next**.



Figure 17. Certificate Import Wizard

6. Click **Browse** and enter '*.*', '*.p12' or '*.pfx' as the file filter. Navigate to and select the client certificate file.

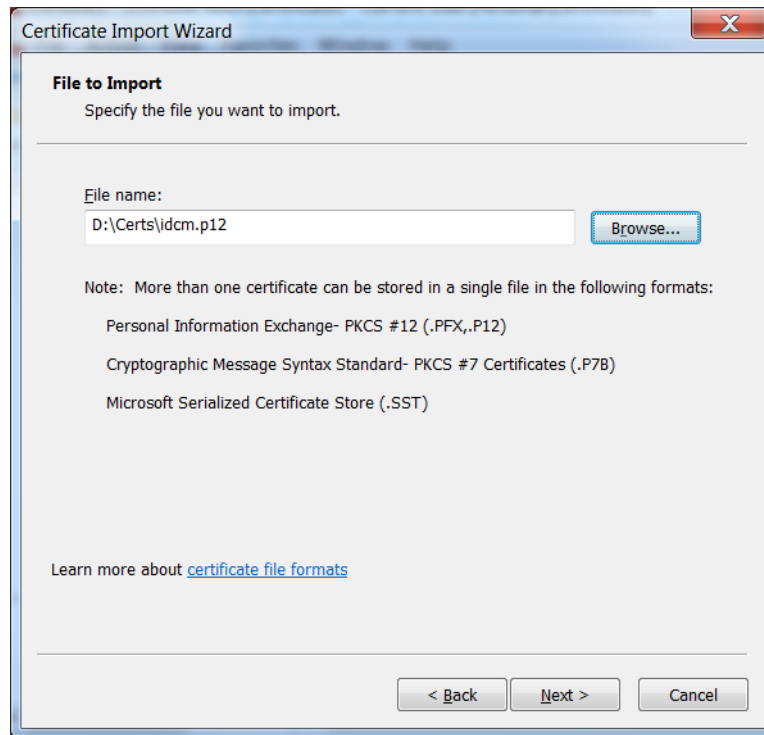


Figure 18. Certificate Import Wizard

7. Enter the key store password (select **Mark this key as exportable**, if the certificate is exported in the future), and click **Next**.

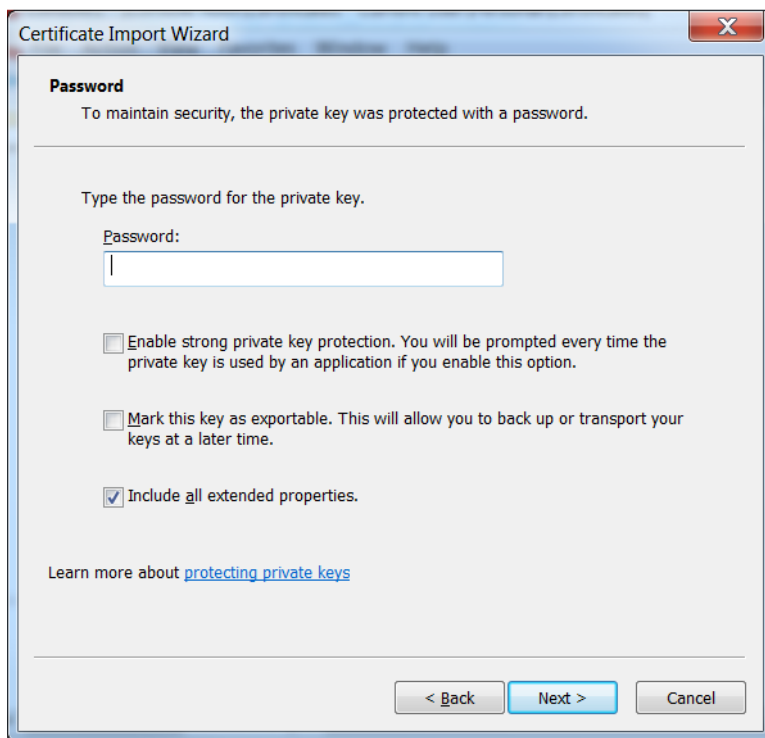


Figure 19. Certificate Import Wizard

8. Click **Next**, and accept **Personal** as the store name.

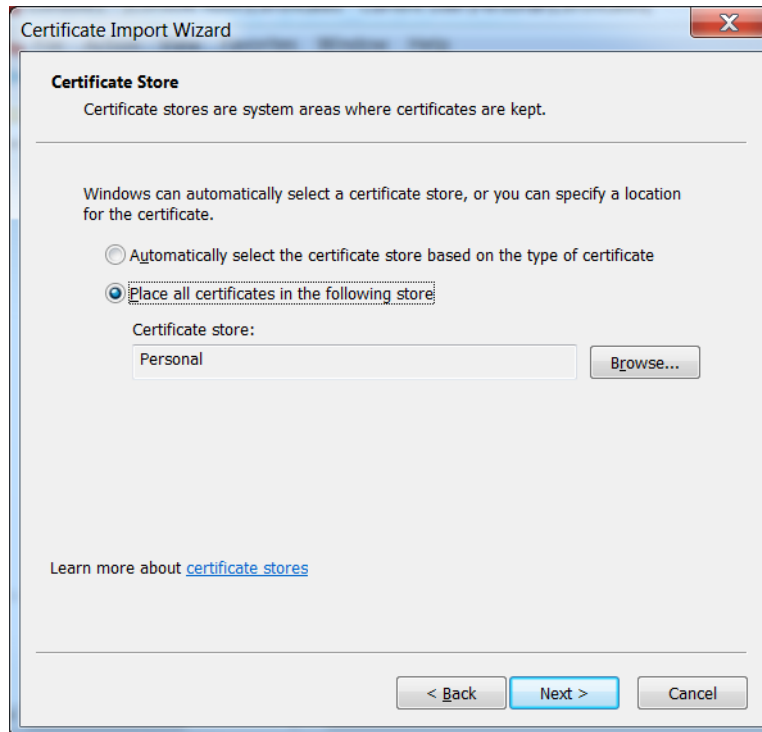


Figure 20. Certificate Import Wizard

9. Click **Finish**. The certificate should be visible in the selected store.

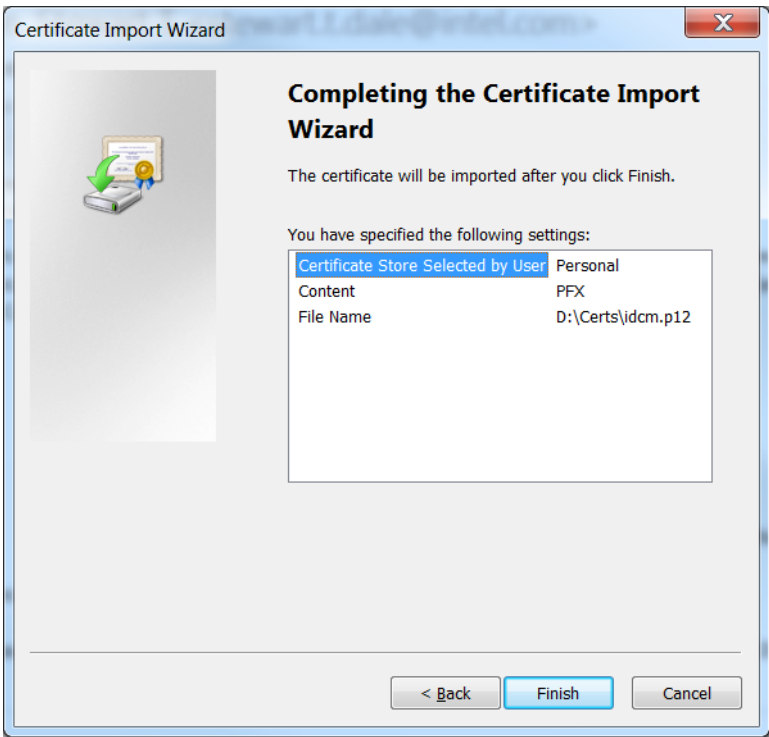


Figure 21. Certificate Import Wizard

Also see <https://technet.microsoft.com/en-ca/library/cc754489.aspx> and <https://technet.microsoft.com/en-us/library/cc771377.aspx> for more details.

Intel DCM Server Certificate Configuration

The Intel DCM Server uses the Tomcat Java Key Store (JKS) key store format. The Java keytool utility (distributed with JRE or JDK packages) should be used to maintain the Tomcat key store. The keytool can work with JKS or PKCS12 (PFX) certificate formats, and can be used to create the PKCS12 format certificate required for installation on the client node.

To install the PKCS12 client certificate and its certificate chain on the Intel DCM server, do the following steps:

1. [Convert PKCS12 keystore to JKS format to be used in Tomcat keystore](#) - The key store containing the certificate and its certificate chain must be converted to JKS format using the Java keytool.
The certificate chain must be imported to the Intel DCM (Tomcat) key store. A single chain may sign more than one client certificate. Typically a chain matches a CA and signs all the certificates issued by that CA.
2. [Load the client certificate into the Tomcat keystore](#) - The client certificate must be imported into the Intel DCM (Tomcat) key store.
3. [Enable Intel DCM client certificate authentication](#).

These steps must be repeated for each client certificate that is expected to use the Intel DCM server instance.

Installing a client certificate on the server node

Login to the Intel DCM server using an administrative account. Open command prompt and change current directory to the one containing Tomcat key store, i.e by executing the following command:

```
C:\Users\{logged in user}> cd "C:\Program  
Files\Intel\DataCenterManager"
```

The tool used to create and manipulate is the Java keytool. It is distributed with JRE that is required to run Tomcat (the servlet container used by Intel DCM). The keytool is found in %JRE_HOME%\bin (or %JAVA_HOME%\bin). Typically this location is not included in the %PATH%.

For convenience purpose, a temporary environment variable can be set as follows, (in command prompt): set JRE_HOME="C:\Program Files\Java\jre1.8.0_65"

(use the path to your JRE version). The setting can be tested using echo command. Figure 22 shows the command prompt.

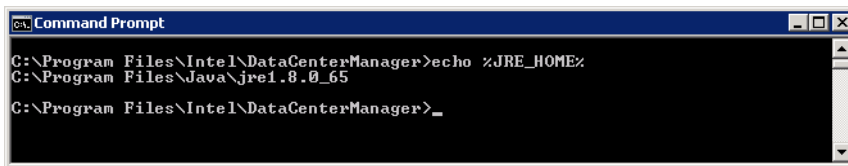


Figure 22. Command Prompt

Convert PKCS12 keystore to JKS format to be used in Tomcat keystore

The file containing the client certificate must be converted from PKCS12 to JKS format to be used with Tomcat, using the following command:

```
%JRE_HOME%\bin\keytool.exe -importkeystore -alias wsclient -  
srckeystore D:\temp\certs\idcm.pfx -srcstoretype PKCS12 -  
destalias <user name> -destkeystore D:\temp\certs\idcm.jks -  
deststoretype JKS
```

In this example, the alias “wsclient” is used as a friendly certificate name. If multiple user certificates are loaded, distinct aliases are required. The idcm.pfx and idcm.jks file names are examples, and should be substituted with the appropriate names (e.g. use file names describing the users when multiple certificates are imported). The file extension “pfx” is not mandatory (P12, crt or cer also can be used), but it helps to remember the key store format.

After the store format is converted, the certificate can be imported to the Tomcat keystore. The password assigned during the certificate creation (or export) is required and will be prompted (every keytool action requires the key store password).

Load the client certificate into the Tomcat keystore

Export the client certificate and the chain from the new key store and import both the certificate chain and the certificate into the Tomcat key store:

```
%JRE_HOME%\bin\keytool.exe -exportcert -alias <user name> -
keystore D:\temp\certs\idcm.jks -file d:\temp\certs\idcm.crt
%JRE_HOME%\bin\keytool.exe -import -alias <chain name> -
keystore keystore.ssl -trustcacerts -file D:\temp\certs\idcm-
chain.crt
```

The idcm-chain.crt is either the certificate chain file obtained from the CA or the same as idcm.jks if the certificate was exported with the entire path.

```
%JRE_HOME%\bin\keytool.exe -importcert -alias <user name> -
keystore keystore.ssl -file D:\temp\certs\idcm.crt
```

The alias may be set to a GUID. To see the actual aliases, use the following command:

```
"%JRE_HOME%\bin\keytool" -v -list -keystore
c:\software\cert\idcm.jks
```



After the important command executes, following question is asked “Trust this certificate? [no]:

At this point answer “yes” and enter.

Also see <https://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html> for more details.

Enable Intel DCM client certificate authentication

Modify the Tomcat server.xml configuration file (the default location is C:\Program Files\Intel\DatacenterManager\external\apache-tomcat\conf\server.xml) to enable certificate authentication by adding the truststoreFile attribute to the Connector element and setting the clientAuth attribute to “true” (as shown in **underline**):

```
<Connector protocol="org.apache.coyote.http11.Http11Protocol"
port="8643"
minSpareThreads="5" maxSpareThreads="75"
enableLookups="true" disableUploadTimeout="true"
acceptCount="100" maxThreads="200" scheme="https"
secure="true" SSLEnabled="true"
keystoreFile="C:\Program
Files\Intel\DataCenterManager\keystore.ssl"
keystorePass="<pwd>"
truststoreFile="C:\Program
Files\Intel\DataCenterManager\keystore.ssl"
truststorePass="<pwd>"
```

```
clientAuth="true" sslProtocol="TLS"  
protocols="TLSv1,TLSv1.1,TLSv1.2"/>
```

where <pwd> is a placeholder for the actual key store password. Tomcat will authenticate trusted certificates only, therefore the truststoreFile attribute is required. The clientAuth = “true” attribute enables certificate authentication for all of Tomcat. This includes the root location and all the web applications.



The Intel(R) DCM Service must be restarted from the service control panel in order for the changes to take effect.

Application Server Configuration of the Intel DCM Integration Service

To configure the Intel DCM Integration service to use client certificate authentication, set the Authentication Scheme to *Certificate*. That will enable and display the certificate store location and the certificate name edit controls. Select

User to set the certificate store location to Current User. Type the common name (CN) of the certificate into the Name edit control.

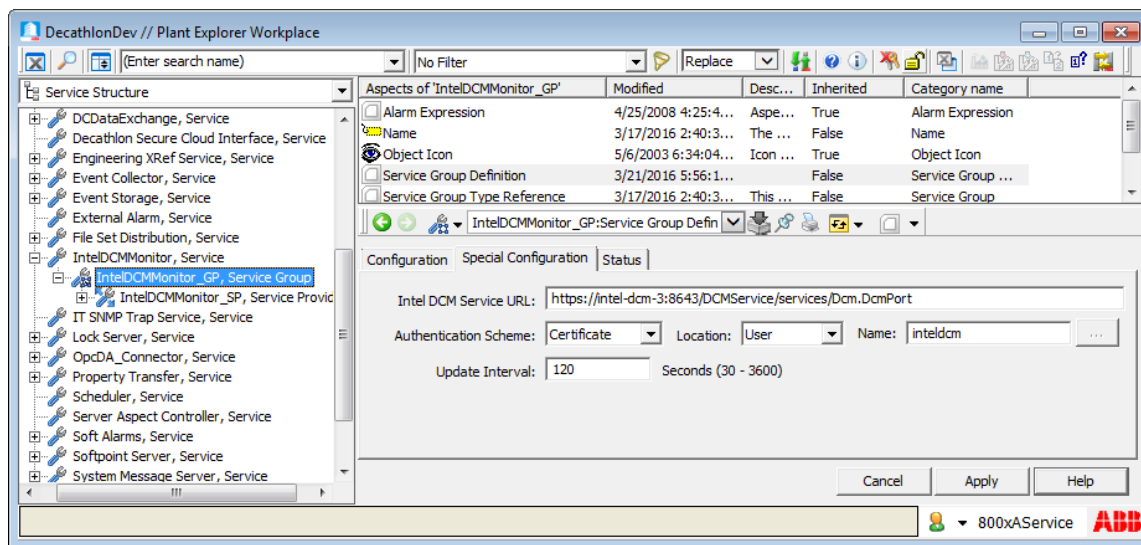


Figure 23. DecathlonDev - Plant Explorer Workplace

The “...” button is not available for this store location as the user configuring the service may be different than the user account that runs the 800xA services, and it is likely that each account has different certificates that are private to each account. When using the User location, the certificate name and certificate settings are validated when the service starts.

Selecting *Computer* sets the certificate location to Local Machine. Type the common name (CN) of the certificate into the Name edit control or use the “...” button to select a certificate name interactively. When using the Computer location,

the certificate is available to all the users and validation is performed when the **Apply** button is clicked.

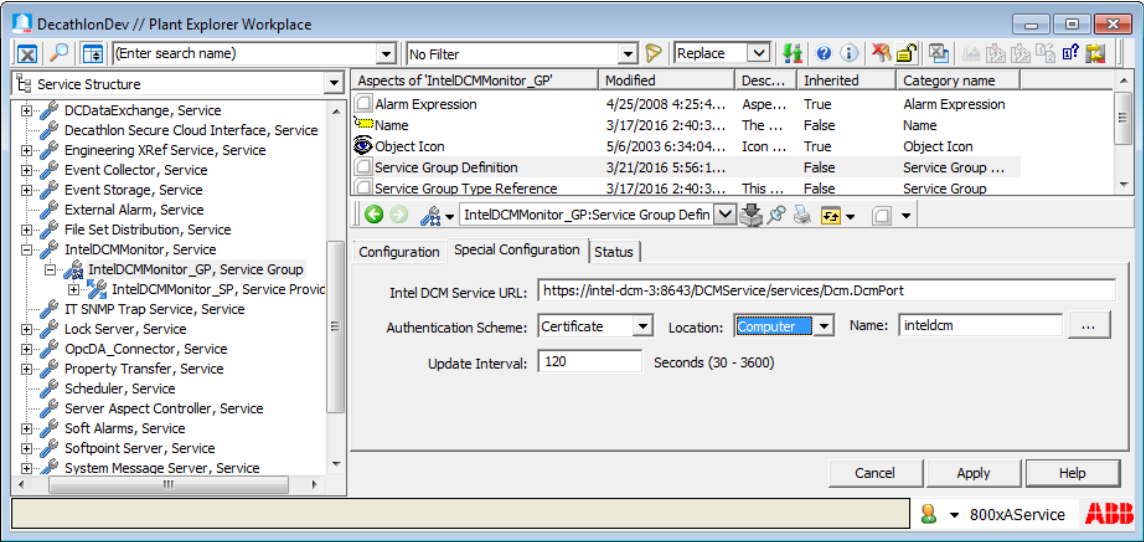


Figure 24. DecathlonDev - Plant Explorer Workplace

Intel DCM Integration Client Certificate Authentication Diagnostics

When the Intel DCM Integration service starts the CONN_Authentication property on the Service Status object indicates the authentication scheme used. Currently

supported schemes are *Anonymous* and *Certificate*. For the Certificate scheme the certificate status is also included.

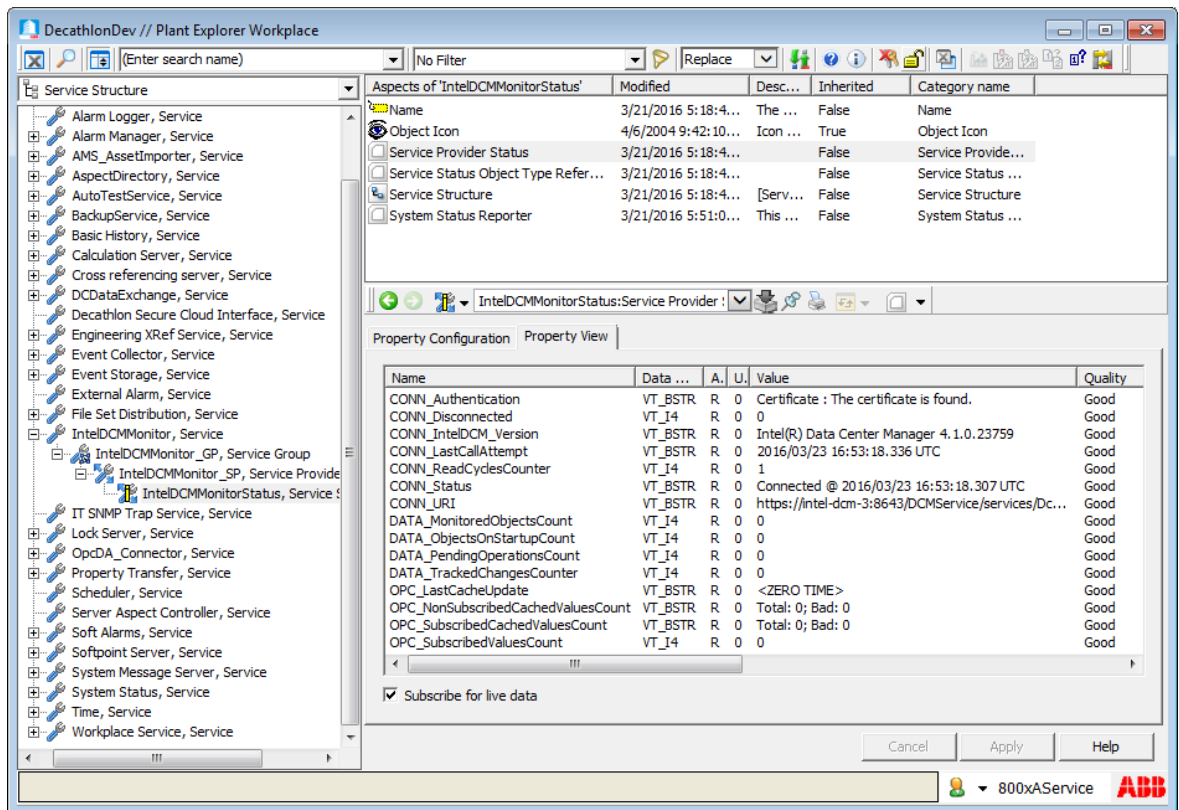


Figure 25. DecathlonDev - Plant Explorer Workplace

If the certificate lookup is successful, *Certificate: The certificate is found* status is displayed. Otherwise, the message *Certificate: Failed to find the certificate in the store* status is displayed.

Appendix A Intel® Data Center Manager Installation

The Decathlon for Data Center's Intel DCM Integration 6.0.1 release was developed and tested against Intel® Data Center Manager 4.2.

Prerequisites

Intel Data Center Manager needs to run on a dedicated server. The hardware and software requirements are detailed in this section.

Computer Hardware

The server, required to run the Intel Data Center Manager, needs to be sized correctly. An undersized servers may result in the real-time server information being returned slower than the requested update rate and may also result in time errors within Decathlon with servers faceplates showing bad quality data.

Figure 26 shows the relationship between the number of monitored servers and the size of the system required.

		Computer Sizing			
		Small	Medium	Large	X-Large
# of monitored servers	Up to 500	Ideal	Oversized	Oversized	Oversized
	Up to 1,000	Ideal	Oversized	Oversized	Oversized
	Up to 2,500	Unsuitable	Ideal	Oversized	Oversized
	Up to 5,000	Unsuitable	Unsuitable	Ideal	Oversized
	Up to 7,500	Unsuitable	Unsuitable	Ideal	Oversized
	Up to 10,000	Unsuitable	Unsuitable	Unsuitable	Ideal

Figure 26. Computer Sizing

The green **Ideal** and yellow **Oversized** cells indicate the computer size that will perform successfully for the number of monitored servers.

The green cells indicate a computer size that it correctly sized.

For example, for 7000 servers a **Large** size would meet the minimum performance requirements without being oversized.

The size indicated in the table translates to the following minimum HW requirements:

- Small: 1 CPU with 2 cores, 4GB RAM
- Medium: 1 CPU with 4 cores, 8GB RAM
- Large: 2 CPUs each with 4 cores, 12GB RAM
- X-Large: 2 CPUs each with 8 cores, 16GB RAM

The hard drive will need a minimum of 120 GB of free space for use by Intel Data Center Manager i.e. after the OS is installed but before Intel Data Center Manager is installed.

Operating System

Windows Server 2012 R2 is the prerequisite operating system for Intel Data Center Manager.

Installation Steps

1. Double click on the **Intel(R)_Data_Center_Manager.exe**. Click **Next** to proceed to the Intel Data Center Manager EULA.

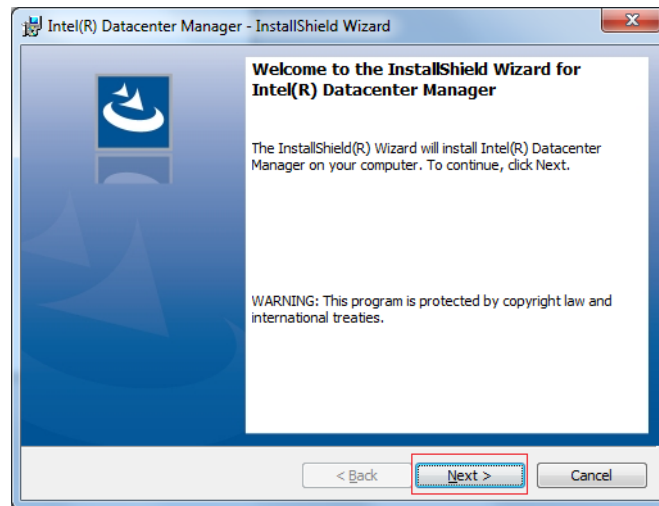


Figure 27. InstallShield Wizard

2. Read through the EULA, select the acceptance button then click **Next** to proceed to the **Customer Information** screen.

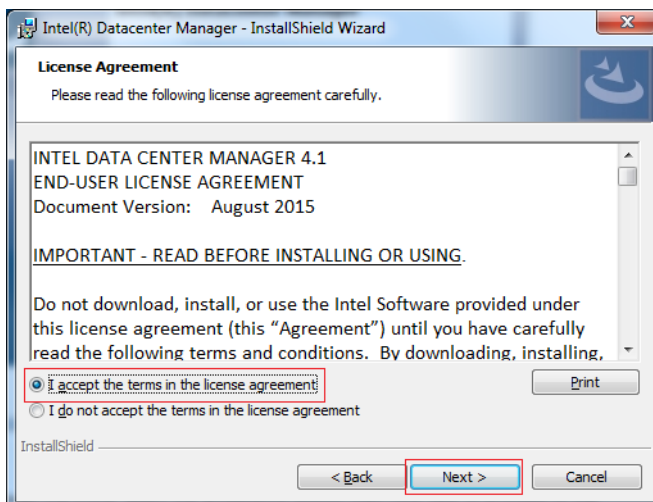


Figure 28. Licence Agreement

3. Add customer details and select **Next** to proceed to the **Custom Setup** page.

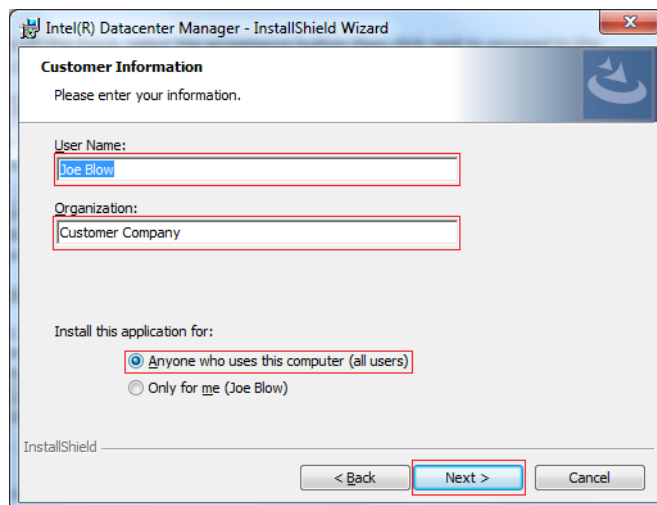


Figure 29. Customer Information tab

4. On the **Custom Setup** page select '**Reference UI**' and deselect '**Samples**' checkboxes. Select **Next** to proceed to the **Destination Folder**. The reference UI option installs the console app.

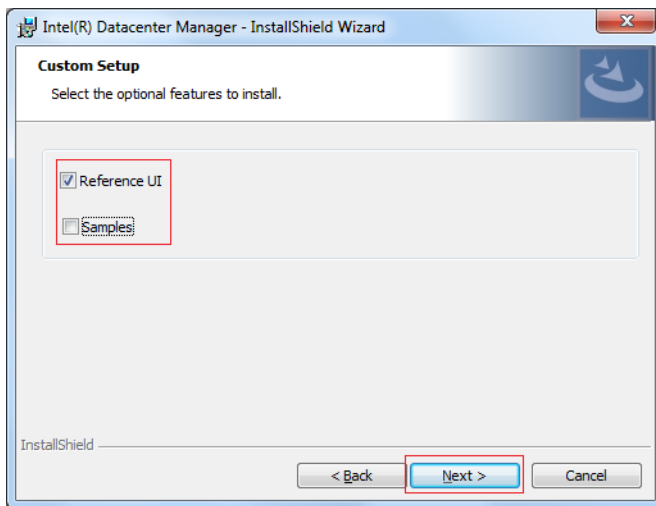


Figure 30. Custom Setup

5. Use the default destination folder. Select **Next** to proceed to the SNMP & RMI setup page.

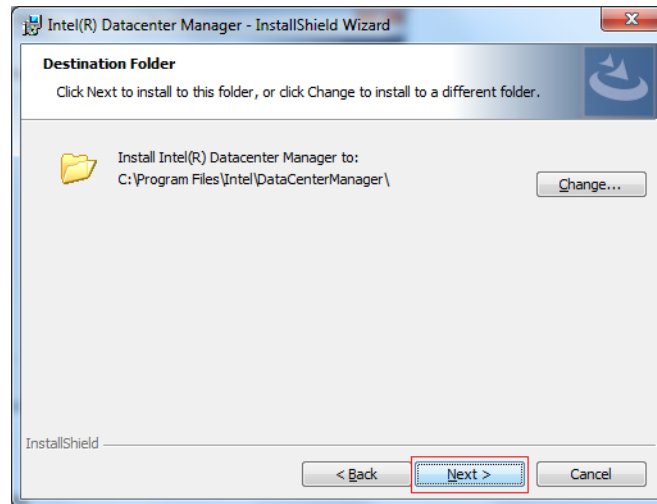


Figure 31. Destination Folder

6. Accept the defaults for SNMP and RMI. Select **Next** to proceed to the DCM Web configuration page.

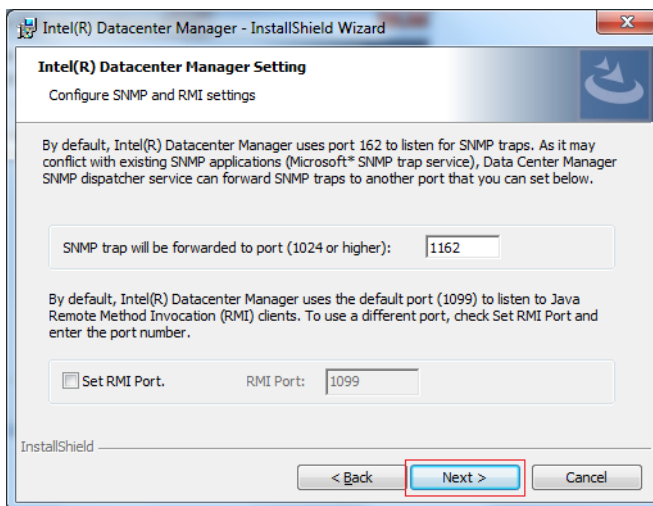


Figure 32. SNMP and RMI Settings

7. Select the 'Use TLS' checkbox to configure the use of TLS in accessing the web services.



It is recommended that TLS be used to increase the security of the system.

Accept the defaults for the port address unless a conflict has been identified.

Select **Next** to proceed to the sample frequency page.

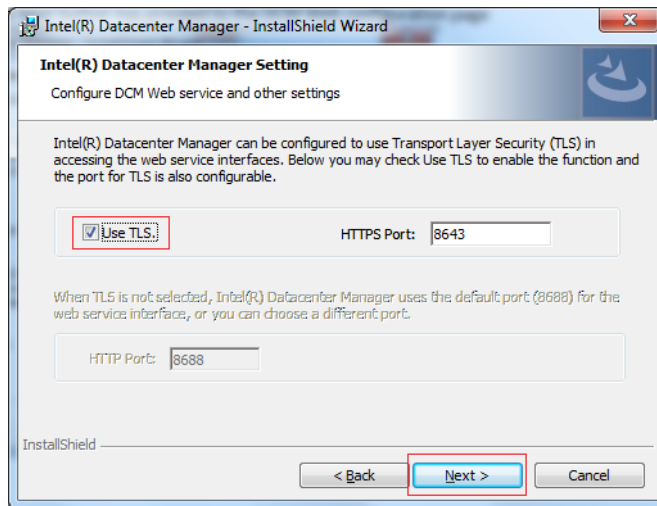


Figure 33. DCM Web service setting

8. The sample rate and the granularity period for the power and temperature are set in the next dialog.



Specifying numbers lower the Intel recommendations may cause the Intel Data Center system to be overloaded and result in a loss of real-time data.

Select **Next** to move to the keystore settings.

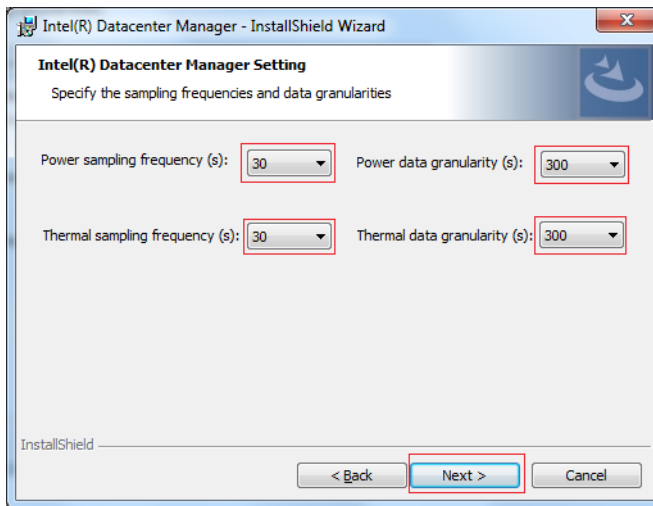


Figure 34. Sampling frequency setting

Granularity:

The minimum setting depends on the number of servers to be monitored.

The minimum recommended granularity as specified by Intel is as follows:

- <1000 nodes: 30 seconds
- 1001-5000: 180 seconds
- 5001-10000: 360 seconds

We recommend that you set both power and temperature to the same Intel recommended granularity

Sampling Frequency

We recommend that you set both sampling frequencies to a half or a third of the granularity as defined above.

For example for a granularity of 180 seconds the sampling rate should be set 60 or 90 seconds.



There is a single granularity and associated sampling frequency for all devices and it should be set to accommodate the slowest device being monitored.

9. Fill in the customer information and choose a TLS Keystore password. The passwords must be greater than 6 character long. Select **Next** to proceed to the PostgreSQL setup page.

The image shows a screenshot of the 'Intel(R) Datacenter Manager - InstallShield Wizard' window. The title bar includes the Intel logo and the text 'Intel(R) Datacenter Manager - InstallShield Wizard'. The main window has a header 'Intel(R) Datacenter Manager Setting' and a sub-header 'Configure keystore setting'. Below this, a message states: 'Intel(R) Datacenter Manager will use keystore. Please give the keystore password and enter the fields of the distinguished name for the certificate.' There are two password fields: 'TLS Keystore Password:' and 'Verify Password:', both containing six dots. Below these is a section titled 'The fields of the distinguished name for the certificate.' which contains six text input fields: 'Your Name:' (Joe Blow), 'Organization Unit:' (Data Center), 'Organization Name:' (MYCOMPANY), 'Locality Name:' (MYADDRESS), 'State Name:' (MYSTATE), and 'Two-letter Country Code:' (US). At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red rectangle.

Figure 35. Keystore setting

10. Configure the username and password for the PostgreSQL database. We strongly recommend you accept the defaults for the port and data directory. Select **Next** to go to the installation screen.

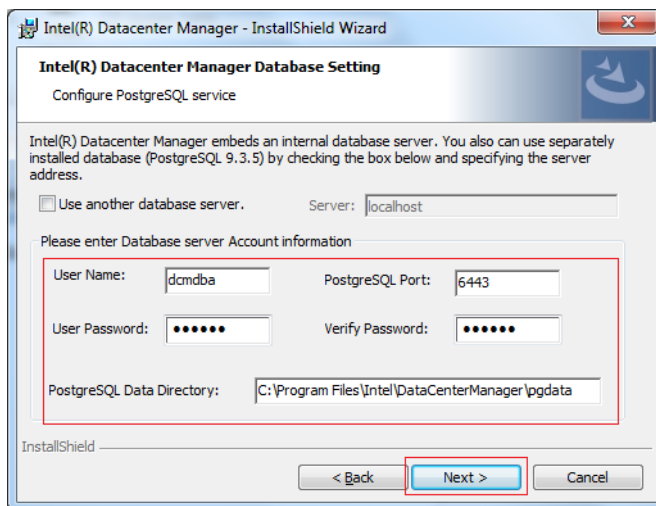


Figure 36. PostgreSQL service

11. Select **Install** to complete the installation.

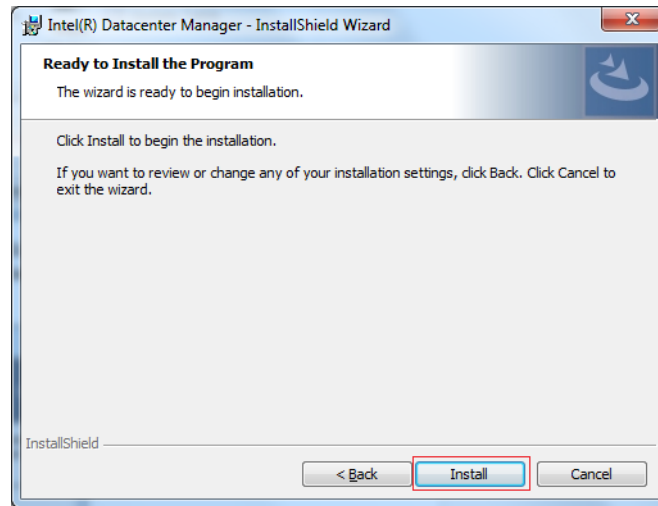


Figure 37. Intel DCM, Install Program



It is essential that Operating System patches are applied to the Decathlon for Data Center system as part of ongoing maintenance. The patches should also be applied to the node running the Intel Data Center Manager server.

Post Installation Steps

Intel DCM is shipped with some default settings which are not suitable for a large installation when used with the ABB Intel DCM Integration product. The IntelDCMConfigUtil.exe utility is used to modify the default settings in the Intel DCM integration after the Intel DCM server is installed.

The utility is available in the bin folder of the Intel DCM Integration install directory, and is run from a command prompt.



The tool must run from any of the 800xA node as it is part of the Intel DCM integration installation.

IntelDCMConfigUtil Configuration

The utility is configured to use the **HTTPS** protocol with **anonymous** authentication.

Special communications configurations (such as authentication methods) can be modified in the app config file “IntelDCMConfigUtil.exe.config” in consultation with Decathlon for Data Centers technical support if required. Typical configuration settings can be made from the command-line (for example, a command-line option exists for using an alternate URI).

IntelDCMConfigUtil Usage

For post-installation, execute the following command-line (use the server name for your Intel DCM server instead of “idcm”):

```
IntelDCMConfigUtil -uri  
https://idcm:8643/DCMService/services/Dcm.DcmPort/ -dbset
```

The tool will display status and current settings after it is run, as shown in the figure:

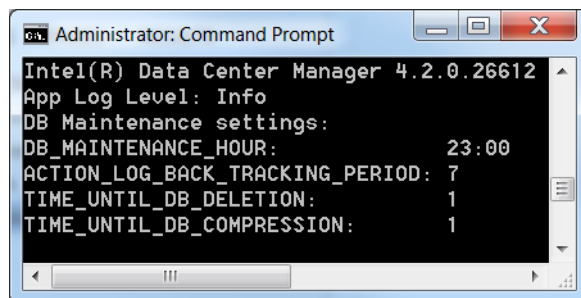


Figure 38. IntelDCMConfigUtil Command

By using the options described in the following section, the utility can be used to display current Intel DCM global properties, and can also be used to update App Log Level, DB_MAINTENANCE_HOUR, TIME_UNTIL_DB_DELETION and TIME_UNTIL_DB_COMPRESSION.

The settings are displayed after modifications are applied.

IntelDCMConfigUtil Command Line Reference

The utility supports the following list of command line arguments that control its execution (the arguments can be specified in any order).

Table 3. List of Command Line Arguments

Command line Arguments	Description
-h	Displays the usage message. This argument overrides any other if used in any combination of arguments.
-display	Displays current settings of the default Intel DCM instance. This argument is implied when the “-uri” argument is used.
-dbset	Sets TIME_UNTIL_DB_DELETION to 1 and TIME_UNTIL_DB_COMPRESSION to 1. This argument could be combined with any other except “-h”. It will have no effect if combined with both “-dbdel” and “-dbcom”.
-uri <address>	Specifies Intel DCM web service URI. The address value must include protocol (http or https), host name, port number (if different from default 80 for http and 443 for https) and the rest of the path (if any). For example, https://idcm:8443/DCMService/services/Dcm.DcmPort/
-dbmts <start time>	Sets Intel DCM database maintenance cycle start time in the Intel DCM server's local time zone. The start time value is a string specifying hours (using 24 hour clock) and minutes: For example, 22:30. Don't enter quotation marks around the value.
-dbdel <integral value>	Sets number of days before the database is purged. The minimum value is 1. The maximum should not exceed 365 as it will lead to significant database growth. The recommended value to be used with Decathlon for Datacenters Intel DCM Integration is 1.
-dbcom <integral value>	Sets the number of days before the database is compressed to the specified value. The recommended value to be used with Decathlon for Datacenters Intel DCM Integration is 1.
-log <Debug or Info>	Sets Intel DCM App Log Level to the specified value. The recommended value used with Decathlon for Datacenters Intel DCM Integration is the default, Info.

IntelDCMConfigUtil Command Line Examples

```
IntelDCMConfigUtil -uri  
https://idcm:8643/DCMService/services/Dcm.DcmPort/
```

Displays current settings.

```
IntelDCMConfigUtil -uri  
https://idcm:8643/DCMService/services/Dcm.DcmPort/ -dbset
```

Sets default values for TIME_UNTIL_DB_DELETION (1) and
TIME_UNTIL_DB_COMPRESSION (1).

```
IntelDCMConfigUtil -uri  
https://idcm:8643/DCMService/services/Dcm.DcmPort/ -dbmts  
22:30
```

Sets DB maintenance start to 10:30pm (server local time).

```
IntelDCMConfigUtil -uri  
https://idcm:8643/DCMService/services/Dcm.DcmPort/ -dbdel 50  
-dbcom 3
```

Sets TIME_UNTIL_DB_DELETION to 50 and
TIME_UNTIL_DB_COMPRESSION to 3.

```
IntelDCMConfigUtil -uri  
https://idcm:8643/DCMService/services/Dcm.DcmPort/ -log Debug
```

Sets Intel DCM logging level to Debug.

Appendix B Intel DCM Integration 6.0.1 Installation

This product needs to be installed on all nodes of the 800xA system, and has two installation options. The “Complete” option needs to be installed on an 800xA application server. The “Client” option needs to be installed on all 800xA nodes. The Application Server should be installed first.

Installation Steps

1. Log into the 800xA Node using the 800xA installation account (typically “800xAInstaller”).

2. Double click **Intel DCM Installation** package, ABB IntelDCMSetup.msi. Select **Next** to move to the license agreement dialog box.

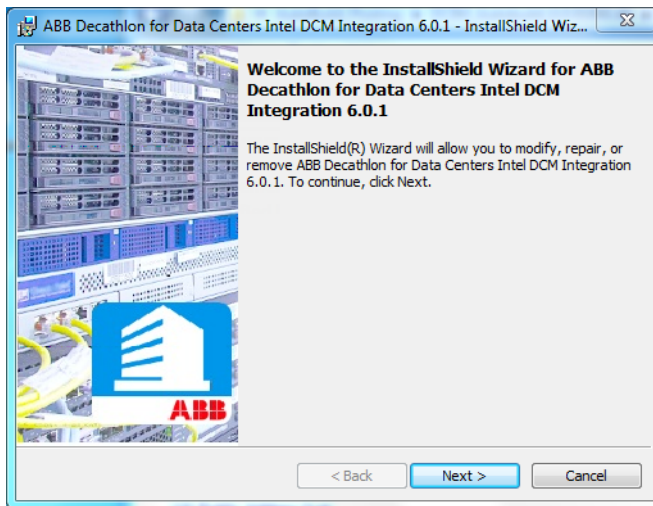


Figure 39. Intel DCM Integration Installation welcome

3. Review the EULA and after selecting the button to accept the terms click **Next**.



Figure 40. End User License Agreement

4. Accept the default destination folder. Select **Next** to advance to the screen.
5. On the **Setup Type** page select the **Installation** option for the current node.
 - The '**Complete**' option is installed on the designated Application Server node and installs all the Server and Client software that the node and system requires to run the Intel DCM Service and act as a Decathlon client.
 - Use the '**Client**' option during the installation of all other nodes.

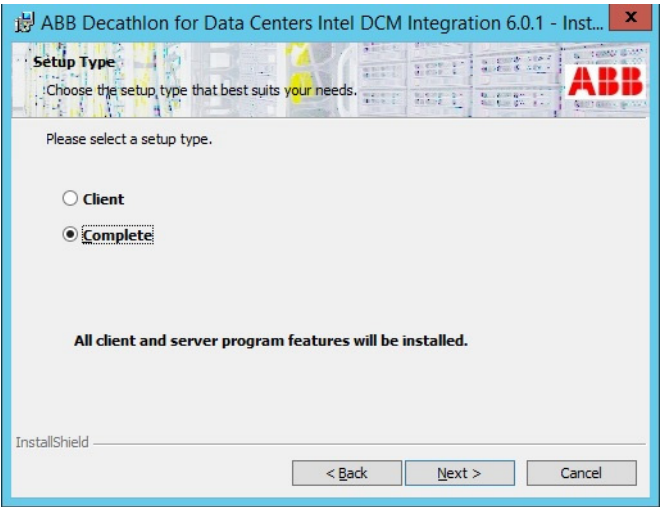


Figure 41. Setup Type

6. Select **Install** to start the installation and **Finish** to complete.

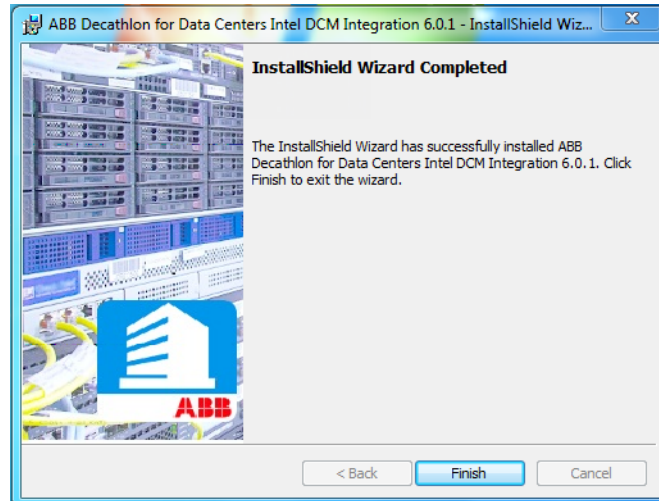


Figure 42. Setup Complete

Appendix C Intel DCM Object Types

This section contains an overview of the object types developed for use within the integration. The Intel DCM Library User Manual should be consulted for more detailed information on configuration and customization.

Intel DCM Integration selects the appropriate Intel Data Center Manager plugin when establishing communications with a specific server. This determination is done by the Intel Data Center Manager software by probing the IPMI port on the server.

Two object types were defined to encapsulate the properties available in the different Intel Data Center Manager plugins:

- ‘IntelDCMServerBasic’ provides power and inlet temperature and is supported by all plugins.
- ‘IntelDCMServer’ provides outlet temperature and airflow in addition to the properties provided by IntelDCMServerBasic. Only certain Intel Data Center Manager plugins support these additional properties.

Both the object types include the following:

- Log configuration - For logging the short term or the log term history of the tags. Enable or disable the logging if not required.
- Trend - To monitor the trend of particular properties.

IntelDCMServer

The IntelDCMServer object type represents a typical physical server.

IntelDCMServer objects are powered devices. Power may be single-sourced or dual-sourced. Intel DCM Server configurable physical attributes include dimension information, and mounting position within a rack object.

Servers are able to measure power consumption and read temperature data from integrated sensors, but must support a protocol such as IPMI over LAN to provide external communications. IPMI access is typically provided independent of the operating system by a base board management controller (BMC) at the hardware level.

This object type supports the same properties as the IntelDCMServerBasic object type with the addition of Outlet Temperature and Airflow.

Intel Data Center Manager collects the IPMI data from the physical server nodes. In the Intel DCM Integration product we use the Intel Data Center Manager web service to collect the server node's real-time IPMI properties in a System 800xA object instance.

Properties

The IntelDCMServer object type properties are described in the tables below.

Table 4. IntelDCMServer - Real Time Properties

Property ID	Type	R/W/C	Eng Units/States	Default Range	Log	Description
maxInlet Temp	Real	R	Variable(°C /Fahrenheit)	0-100		The maximum temperature for any single node within the specified entity.
avgInlet Temp	Real	R	Variable(°C /Fahrenheit)	0-100		The average temperature for any single node within the specified entity.
minInlet Temp	Real	R	Variable(°C /Fahrenheit)	0-100		The minimum temperature for any single node within the specified entity.

Table 4. IntelDCMServer - Real Time Properties

Property ID	Type	R/W/C	Eng Units/States	Default Range	Log	Description
power	Real	R	Watts	0-1500		The power property represent either the Instantaneous Power (INS_PWR) or Average_Power(AVG_PWR) depending upon the plugin supported by the server node. The instantaneous power(INS_PWR) is the consumption of a specific server. The AVG_PWR is the average power consumption of server. In a situation where both INS_PWR and AVG_PWR are supported by the plugin the INS_PWR will be returned.
avgOutlet Temp	Real	R	Variable (°C /Fahrenheit)	0-100		The weighted average outlet temperature with respect to airflow for any single node within the specified entity.
airFlow	Real	R	CFM			The average airflow going through the node.
plugin	String	R				Plugin name used by Intel DCM for integrating server IPMI data.

Table 5. IntelDCMServer - Configuration Properties

Property ID	Type	Default Value	Write Permission	Description
assetTag	String	-	Configure	Asset identifier
serialNum	String	-	Configure	Device serial number
totalUHeight	Integer	0	Configure	Total number of units occupied within rack
rackUPosition	Integer	0	Configure	Rack unit number – position within rack
modelNum	String	-	Configure	Device model number
manufacturer	String	-	Configure	Device manufacturer's name
airflowType	String	-	Configure	Description of airflow (e.g. Front to Back)
mountingType	String	-	Configure	Description of mounting type (e.g. Rack 19 Inch)
powerSources Total	Integer	0	Configure	Number of power sources supported
powerSources Required	Integer	0	Configure	Number of connected power sources required to operate
powerRating	Real	0	Configure	Power rating for device model
powerType	String	-	Configure	Description of power type (e.g. Single Phase)
width	Real	0	Configure	Width of the Server
depth	Real	0	Configure	Depth of the Server
height	Real	0	Configure	Height of the Server
externalID	String	-	Configure	Unique identifier used by AMS Import Tool
externalKey	String	-	Configure	Unique identifier used by AMS data synchronization (optional)

Table 5. IntelDCMServer - Configuration Properties

Property ID	Type	Default Value	Write Permission	Description
TotalUHeight EnggUnit	String	U	Configure	TotalUHeight Engineering Unit
RackUPosition EnggUnit	String	U	Configure	RackUPosition Engineering Unit
WidthEnggUnit	String	mm	Configure	Width Engineering Unit
DepthEngg Unit	String	mm	Configure	Depth Engineering Unit
HeightEngg Unit	String	mm	Configure	Height Engineering Unit
TempMax	Real	100.000000	Configure	Temp Max Value
TempMin	Real	0.000000	Configure	Temp Min Value
PowerMax	Real	1500.000000	Configure	Power Max Value
PowerMin	Real	0.000000	Configure	Power Min Value

Alarms

There are no default alarms for IntelDCMServer object type.

Views

Faceplate

The DCM Server node object type has a faceplate with **Overview** tab and tabs displaying configuration information.

- Overview. Provides indicators for these properties: Temp, power and Airflow.
- Attributes. Provides air FlowType, power config properties, and a section with physical attributes including dimension.

- Vendor Info. Provides static information such as make, model, serial number, assetTag, Plugin name, IP address.

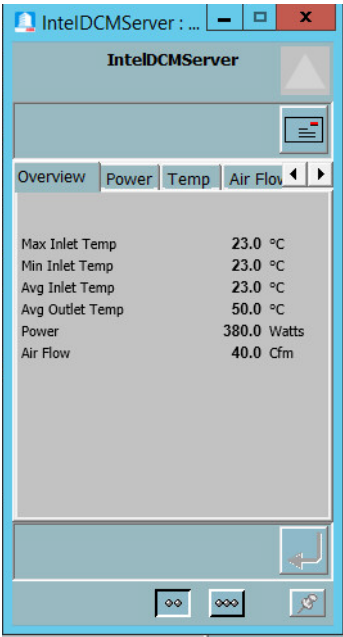


Figure 43. IntelDCMServer Overview

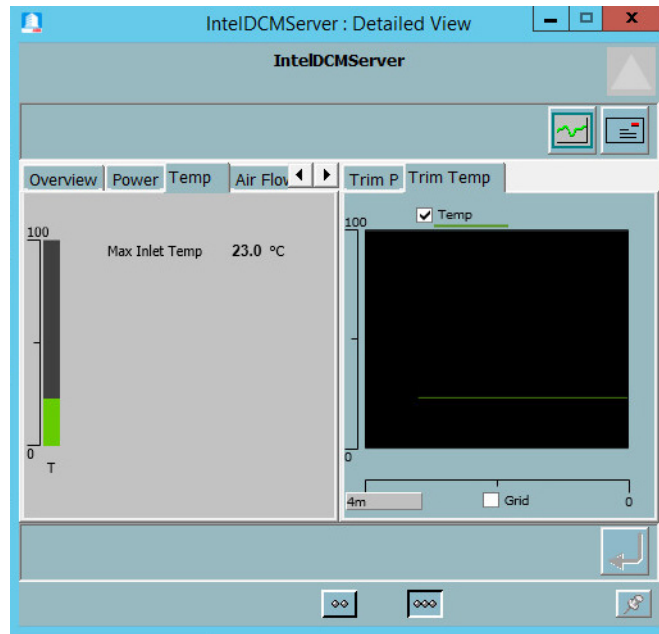


Figure 44. IntelDCMServer Temperature

Graphic Elements

The IntelDCMServer object type includes graphical elements corresponding to faceplate elements. Examples of Display Elements are shown below.



Figure 45. Display Element Power and Display Element Power with Bar

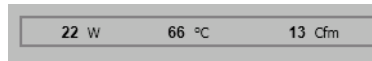


Figure 46. Display Element DCMServer Front View

IntelDCMServerBasic

The IntelDCMServerBasic object type represents a typical physical server.

IntelDCMServerBasic objects are powered devices. Power may be single-sourced or dual-sourced. IntelDCMServerBasic configurable physical attributes include dimension information, and mounting position within a rack object.

Servers are able to measure power consumption and read temperature data from integrated sensors, but must support a protocol such as IPMI over LAN to provide external communications. IPMI access is typically provided independent of the operating system by a base board management controller (BMC) at the hardware level.

This object type supports the same properties as the IntelDCMServer object type but without Outlet Temperature and Airflow.

Intel Data Center Manager collects the IPMI data from physical server nodes. In the Intel DCM Integration product we use the Intel Data Center Manager web service to collect the server node's real-time IPMI properties in a System 800xA object instance.

Properties

The IntelDCMServerBasic object type properties are described in the table below.

Table 6. IntelDCMServerBasic - Real Time Properties

Property ID	Type	R/W/C	Eng Units/States	Default Range	Log	Description
maxInlet Temp	Real	R	Variable(°C /Fahrenheit)	0-100		The maximum temperature for any single node within the specified entity.
avgInlet Temp	Real	R	Variable(°C /Fahrenheit)	0-100		The average temperature for any single node within the specified entity.
minInlet Temp	Real	R	Variable(°C /Fahrenheit)	0-100		The minimum temperature for any single node within the specified entity.
power	Real	R	watts	0-1500		The power property represent either the Instantaneous Power (INS_PWR) or Average_Power(AVG_PWR) depending upon the plugin supported by the server node. The instantaneous power(INS_PWR) is the consumption of a server. The AVG_PWR is the average power consumption of server. In a situation where both INS_PWR and AVG_PWR are supported by the plugin the INS_PWR will be returned.
plugin	String	R				Plugin name used by Intel DCM for integrating server IPMI data.

Table 7. IntelDCMServerBasic - Configuration Properties

Property ID	Type	Default Value	Write Permission	Description
assetTag	String	-	Configure	Asset identifier
serialNum	String	-	Configure	Device serial number
totalUHeight	Integer	0	Configure	Total number of units occupied within rack
rackUPosition	Integer	0	Configure	Rack unit number – position within rack
modelNum	String	-	Configure	Device model number
manufacturer	String	-	Configure	Device manufacturer's name
mountingType	String	-	Configure	Description of mounting type (e.g. Rack 19 Inch)
powerSources Total	Integer	0	Configure	Number of power sources supported
powerSources Required	Integer	0	Configure	Number of connected power sources required to operate
powerRating	Real	0	Configure	Power rating for device model
powerType	String	-	Configure	Description of power type (e.g. Single Phase)
width	Real	0	Configure	Width of the Server
depth	Real	0	Configure	Depth of the Server
height	Real	0	Configure	Height of the Server
externalID	String	-	Configure	Unique identifier used by AMS Import Tool.
externalKey	String	-	Configure	Unique identifier used by AMS data synchronization (optional)
TotalUHeightEngg Unit	String	U	Configure	TotalUHeight Engineering Unit

Table 7. IntelDCMServerBasic - Configuration Properties

Property ID	Type	Default Value	Write Permission	Description
RackUPositionEnggUnit	String	U	Configure	RackUPosition Engineering Unit
WidthEnggUnit	String	mm	Configure	Width Engineering Unit
DepthEnggUnit	String	mm	Configure	Depth Engineering Unit
HeightEnggUnit	String	mm	Configure	Height Engineering Unit
TempMax	Real	100.000000	Configure	Temp Max Value
TempMin	Real	0.000000	Configure	Temp Min Value
PowerMax	Real	1500.000000	Configure	Power Max Value
PowerMin	Real	0.000000	Configure	Power Min Value

Alarms

No alarms for IntelDCMServerBasic object type.

Views

Faceplate

The IntelDCMServerBasic node object type has a simple faceplate with **Overview** tab and tabs displaying configuration information.

- Overview. Provides indicators for these properties: Temp, power and Airflow.
- Attributes. Provides power config properties, and a section with physical attributes including dimension.

- Vendor Info. Provides static information such as make, model, serial number, assetTag, Plugin name, IP address.

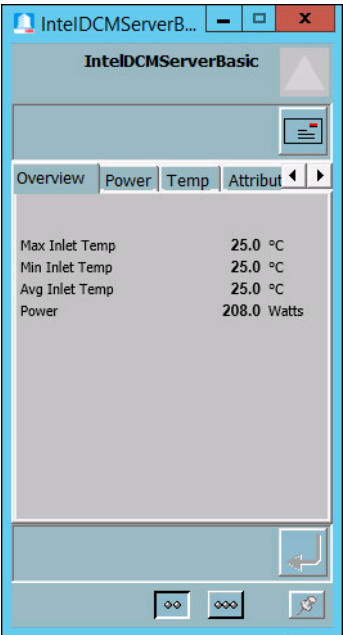


Figure 47. IntelDCMServerBasic Overview

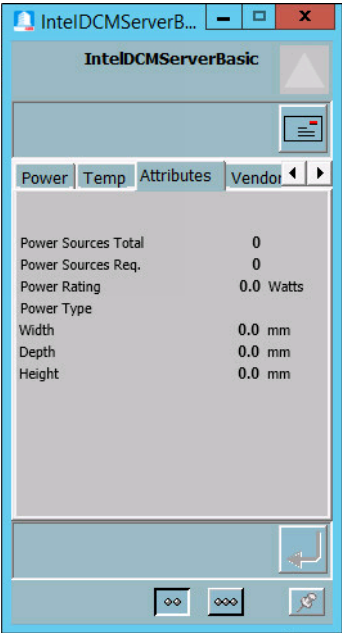


Figure 48. IntelDCMServerBasic Attributes

Graphic Elements

The IntelDCMServerBasic node object type includes graphical elements corresponding to faceplate elements. Examples of Display Elements are shown below.

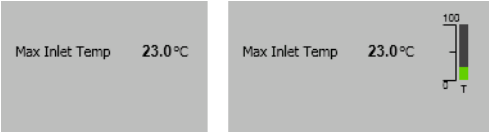


Figure 49. Display Element Temp and Display Element Temp with Bar



Figure 50. Display Element Front View

Appendix D Troubleshooting

Using the Service Status Object

The IPMI Service provides a number of diagnostic properties that can aid in investigating issues with the service.

The Service Status object is found under the **IPMIService > Intel_DCM_Service_SG > Intel_DCM_Service_SP** and is created when the service is first enabled.

(The Service Group and Service Provider names are entered during the post installation steps and may be different from what is shown above)

The properties on the **Property View** tab are updated in real-time and provide a view into the service.

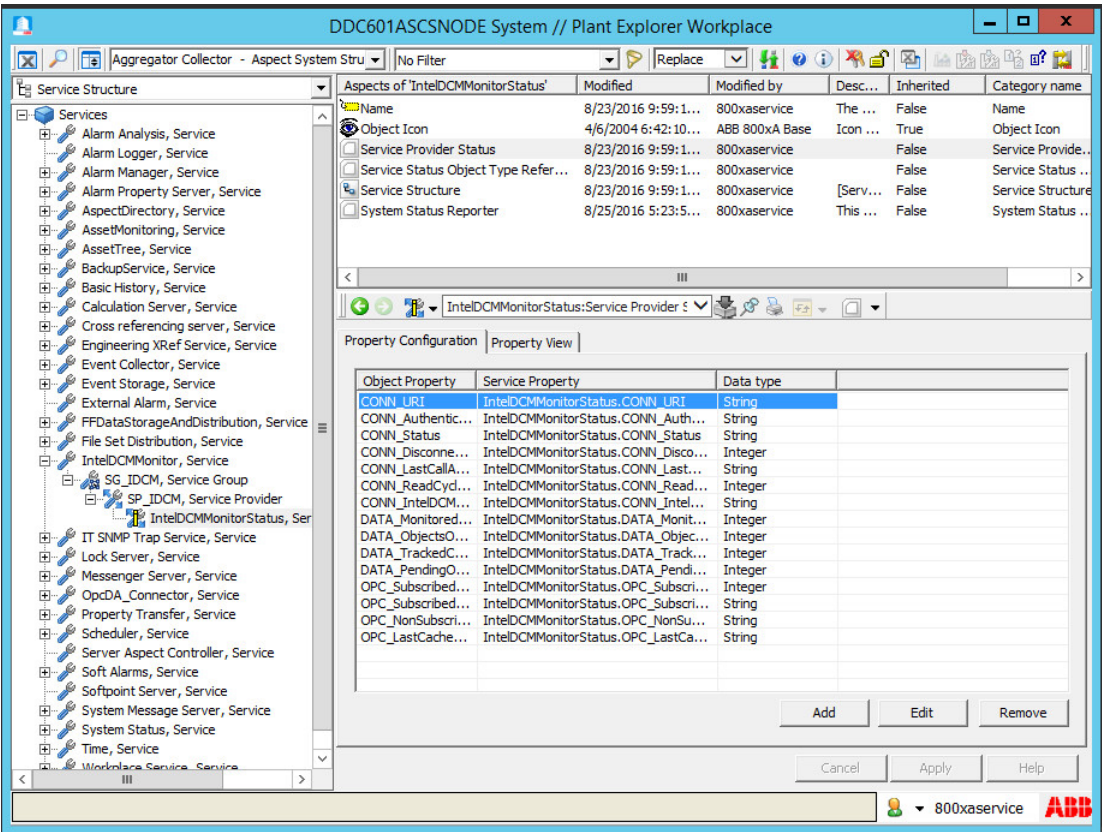


Figure 51. Service Status tab

CONN_IntelDCM_Version

The product version of the connected Intel Data Center Manager.

CONN_LastCallAttempt

The timestamp of the last call made to the Intel Data Center Manager. This could be the result of establishing a server group, establish a server, reading server real-time data etc.

CONN_ReadCyclesCounter

Indefinitely increasing count of the read requests to Intel Data Center Manager. This counter is reset when the IntelDCMMonitor service is restarted. This counter increases whether connected to Intel Data Center Manager or not and provides an indication into the health of the service.

CONN_Disconnected

This indicates if the intel DCM integration service on the connectivity node is connected with the Intel DCM server node.

CONN_URI

The Intel DCM Service URL used to connect to the Intel Data Center Manager. This is the URL as configured in the IntelDCMMonitor > IntelDCMServiceGroup in the Service Structure.

DATA_MonitoredObjectsCount

A current count of the number of server objects under all Intel DCM Server Groups under the Intel DCM Service Network object in the Control structure. This takes into account any additions or deletions of server objects since service startup. If no objects were added or deleted it will be the same as DATA_ObjectsOnStartupCount.

DATA_ObjectOnStartupCount

A count of server objects found when the IntelDCMMonitor service was first started. This includes all server objects under all Intel DCM Server Groups under the Intel DCM Service Network object in the Control structure.

DATA_PendingOperationsCount

This shows internal pending operations that are queued for processing by the service.

This counter could include the number of tracked changes that have yet to be processed: The count will be non-zero during bulk operations before they are processed, or in situations where there is a problem communicating with the server or the Intel Data Center Manager service.

DATA_TrackedChangesCounter

An increasing count that tracks changes (additions, deletions, updates) of server object instances. This counter is reset to zero on a service restart.

OPC_LastCacheUpdate

Timestamp when the value cache was last updated after a read to Intel Data Center Manager.

OPC_NonSubscribedCachedValuesCount

The number of properties with cached values which have never been subscribed to by clients at any time since the service was started. The counter consists of two parts: 'Total' indicates the number of properties with cached values. 'Bad' indicates the number of cached values which are currently bad quality.

Over time, it is likely that values in the nonsubscribed cache will move to the subscribed cache as clients access additional server properties for the first time (counted by OPC_SubscribedCachedValues).

OPC_SubscribedCachedValuesCount

The number of properties with cached values which have been subscribed to by clients currently or at any time since the service was started. The counter consists of two parts: 'Total' indicates the number of properties which have been subscribed to with cached values. 'Bad' indicates the number of cached values which are currently bad quality.

The total cached value count will be different than OPC_SubscribedValuesCount (which provides an indication of current client activity).

CONN_Authentication

The value indicates the type of client authentication schema. Currently the feature supports *Anonymous* and *Certificate* authentication.

In case of certificate authentication the status also indicates whether or not the certificate was found in the specified store location. The authentication cannot be successfully completed unless the specified certificate is located in the specified store location.

CONN_Status

The value indicates whether the connection is established or not.

Using the Intel® Data Center Manager console

The Intel Data Center Manager console web application may be used to investigate issues or to conduct tests with server connectivity.

To launch the console, enter one of the following URLs into a browser:

- Using TLS: <https://ServerAddress:8643/DataCenterManager>
- No TLS: <http://ServerAddress:8688/DataCenterManager>

Where *ServerAddress* is the IP address of the server where the Intel Data Center Manager was installed. This may also be a node identifier if this is defined in the hosts ini file in the C:\Windows\System32\drivers\etc directory.

The following screen will be shown.

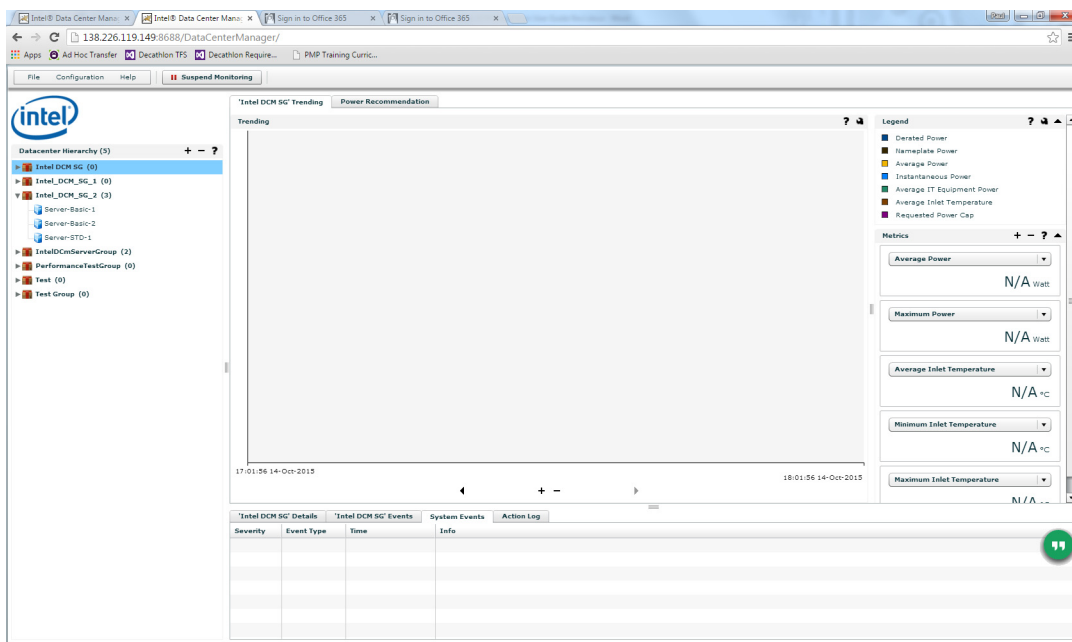


Figure 52. Intel Data Center Manager console

The Data Center Hierarchy should show the 'Server Group's that were created under the **Control Structure > IntelDCMNetwork** object.

A list of servers as entered in Decathlon under each IntelDCMServerGroup should be shown in the corresponding Server Group in the Intel Data Center Manager console.

After selecting the Server Group and Server, metrics for the server will be shown in the main area, and details about the server will be shown at the bottom of the screen.

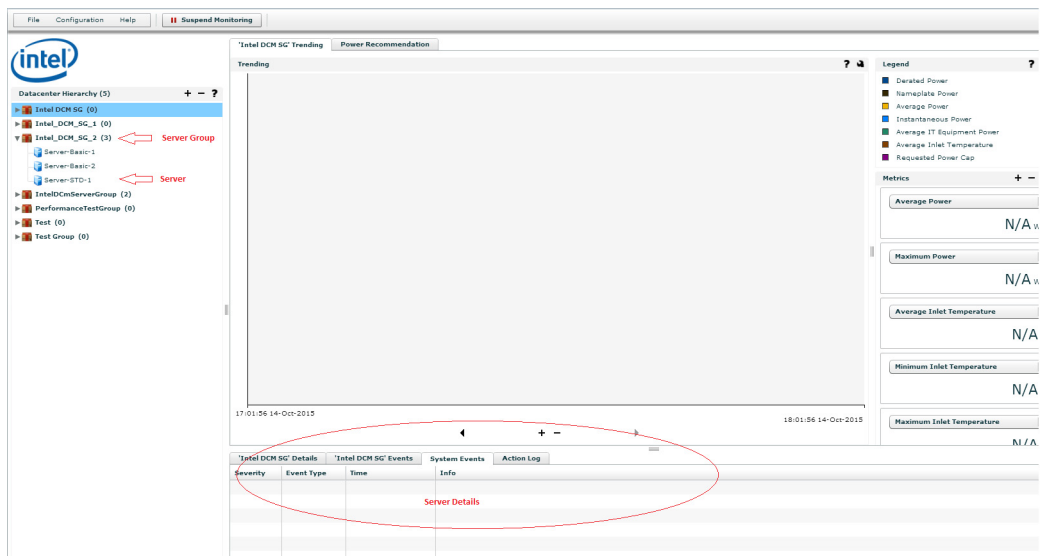


Figure 53. Server details

Communication between Intel DCM Connectivity Node and Intel DCM Server node

If there is an issue between the Connectivity Node and the Intel DCM Server node, do the following checks:

- Check if the Connectivity Node can ping the Intel DCM Server node.
- Check if the Connectivity Node is connected to the Intel DCM Server on port specified in the Intel DCM Service URL filed of the Service Group special configuration using the following command: telnet Serverhostname 8643

A blank window is displayed if the Connectivity Node is connected to the Intel DCM Server. An error message is displayed if the Connectivity Node is not connected to the Intel DCM Server.

Alternatively, the connection to the Intel DCM Server can also be tested using the Intel DCM console in the browser. Please check the following link:
<https://Serverhostname:8643/DataCenterManager/>

Inlet temperature not being reported for some HP servers

There may be Intel Server objects within Decathlon connected to older HP servers that are not showing inlet temperature. In these specific cases it is possible to modify the configuration of Intel Data Center Manager to show this data.

To modify the configuration of Intel Data Center Manager, do the following steps:

1. Log onto the node where the Intel Data Center Manager software is installed using the Administrator account.
2. Navigate to the C:\Program Files\Intel\DataCenterManager\bin\plugins directory and open the **IpmiSensorConfig.xml** file account using a text editor e.g. notepad.exe.
3. Under the **IpmiThermalSensorList** section find the section that looks like the section below and add the bolded text:

```
<IpmiThermalSensorList>
<IpmiThermalSensor name = "fp_ambient_temp" />
<IpmiThermalSensor name = "ambient temp" />
<IpmiThermalSensor name = "inlet temp" />
```

```
<IpmiThermalSensor name = "inlet amb temp"/>
<IpmiThermalSensor name = "system amb temp"/>
<IpmiThermalSensor name = "/sys/t_amb"/>
<IpmiThermalSensor name = "domain a fp temp"/>
<IpmiThermalSensor name = "temp 1"/>
```

4. Restart the Intel Data Center Services (Open the Service application (services.msc)), find the **Intel(R) DCM** service, right-click and select **Restart**.

Appendix E Performance and Capacity

Number of supported Server nodes

This release supports monitoring of up to 5000 servers. This assumes the granularity and sample frequency are set according to the number of servers being monitored as described in [Appendix A, Intel® Data Center Manager Installation](#).

Time to create & establish servers

The time to establish servers and receive the real-time data depends whether the servers have been established with Intel Data Center Manager before or if this is the first time they are being created.

The initial creation and establishing of servers is time consuming. **It takes about 18 minutes per 1000 servers.** (This mean about 90 minutes for 5000 servers in a clean system). The initial values for the servers will be shown in Decathlon at the end of the creation process i.e. after 90 minutes for 5000 servers.

Once servers have been established with Intel Data Center Manager it is able to return real-time values much quicker given that the server has already been created.

This situation would happen the servers had been created and then Decathlon or the Intel DCM Integration service was restarted.

The time taken to receive the initial values is around 1 second per 10 servers. For example, for 3000 servers it will take around 300 seconds (5 minutes) to get the initial update of values.

Appendix F Online/Offline Configuration Changes

The Intel DCM Integration tracks the addition and modification of servers and automatically handles the establishing and updating the servers without further action. When the specific changes listed below are made, the Intel DCM Integration Service (IntelDCMMonitor) needs to be restarted to process the changes. These are detailed in the table below.

[Table 8](#) shows the instance when Intel DCM Integration Service is to be restarted.

Table 8. IntelDCMMonitor - Instances to restart

Operation	Details	Behavior
Insert	Insert of the Intel DCM Server node from some other structure to control structure under the specific Intel DCM Server Group	In this case, Intel DCM Integration Service needs to be restarted. Alternatively, one can just re-apply the IP of the inserted Intel DCM server node after the insert operation is done and Runtime data will start updating without restart of the service.
DragDrop	Drag the intel DCM server node from one particular hierarchy which is not part of the Intel DCM server network and drop this node under the Intel DCM server group which is already part of the Intel DCM server network	In this case, Intel DCM Integration Service needs to be restarted. Alternatively, one can just re-apply the IP of the Intel DCM server node after the drag drop and the runtime data will start updating without restart of the service.

Table 8. IntelDCMMonitor - Instances to restart

Operation	Details	Behavior
CutPaste	Cut the Intel DCM server node from one particular hierarchy which is not part of the Intel DCM server network and paste this node under the Intel DCM server group which is already part of the Intel DCM server network.	In this case, Intel DCM Integration Service needs to be restarted. Alternatively, one can just re-apply the IP of the Intel DCM server node after the paste operation and the runtime data will start updating without restart of the service.
Import	An import of Intel DCM Server objects that had previously been exported using the 800xA Import/Export tool.	The Intel DCM Integration must be restarted.

To restart the Intel DCM Integration Service do the following steps:

1. Navigate to the **Service Structure > IntelDCMMonitor > Intel_DCM_Monitor_SG > Intel_DCM_Monitor_SP**.



The names of the service group (SG) and service provider (SP) are created during the configuration phase and may be different from those detailed above.

2. Deselect **Enabled** checkbox and click **Apply**.
3. Wait for the state to go into **Undefined**, then select **Enabled** checkbox and click **Apply**.

Appendix G Exporting a Certificate to a File

This process is used when a certificate to be used for Intel DCM Integration client authentication exists on one of nodes in the Windows system certificate store.

The certificate has to be exported from the store to a disk file and use for installation on the Intel DCM server, after logging in as the owning user.

To export a certificate to a file, follow the below steps:

1. Start the MMC console (type MMC in Search Bar, click **File** and select **Add / Remove Snap-ins**. Select **Certificates** and click **Add**.

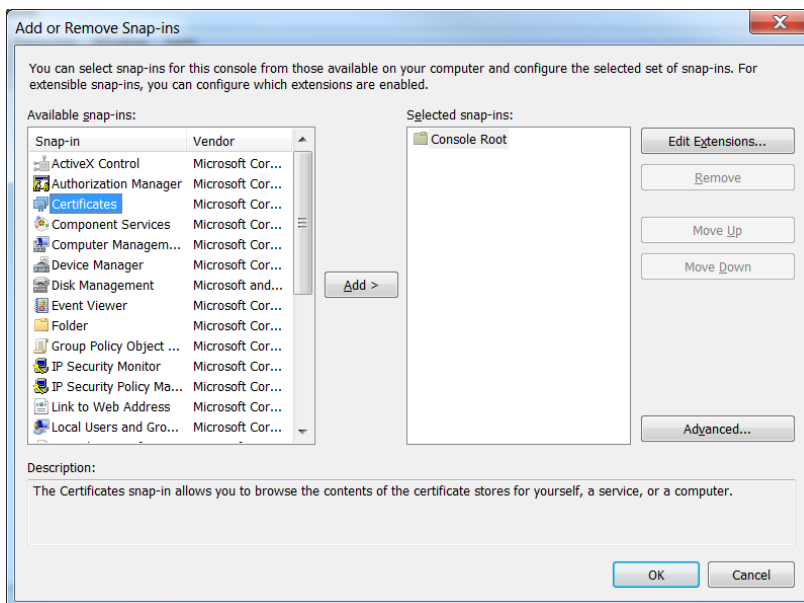


Figure 54. Add / Remove Snap - ins

2. Select **My user account** for the Current User store location (or **Computer account** for Local Machine store location) and click **Finish**.

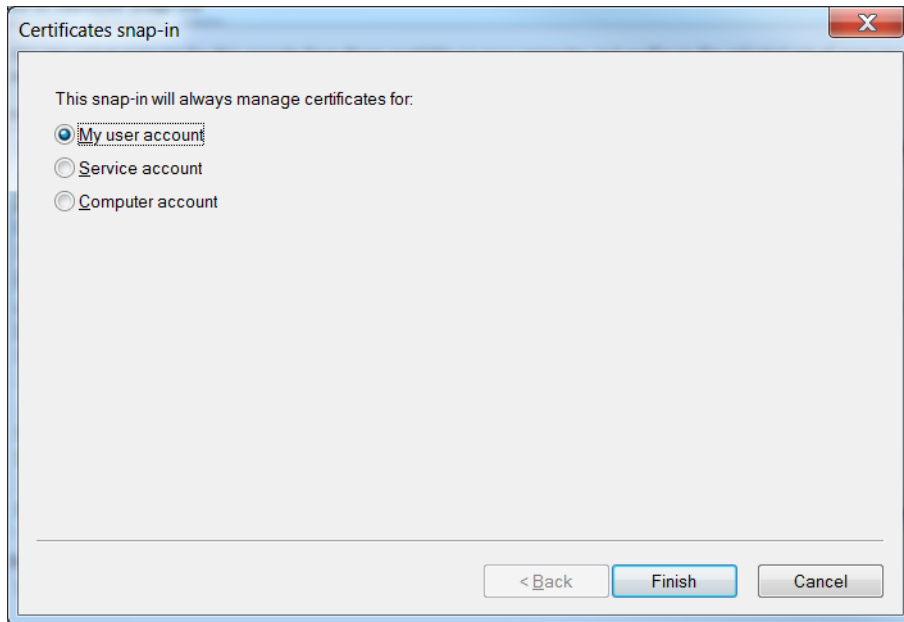


Figure 55. Certificate snap - ins

3. Navigate to Certificates > Current User (or Certificates (Local Computer))/Personal/Certificates and select the required certificate.

4. Right-click and select All Tasks/Export.

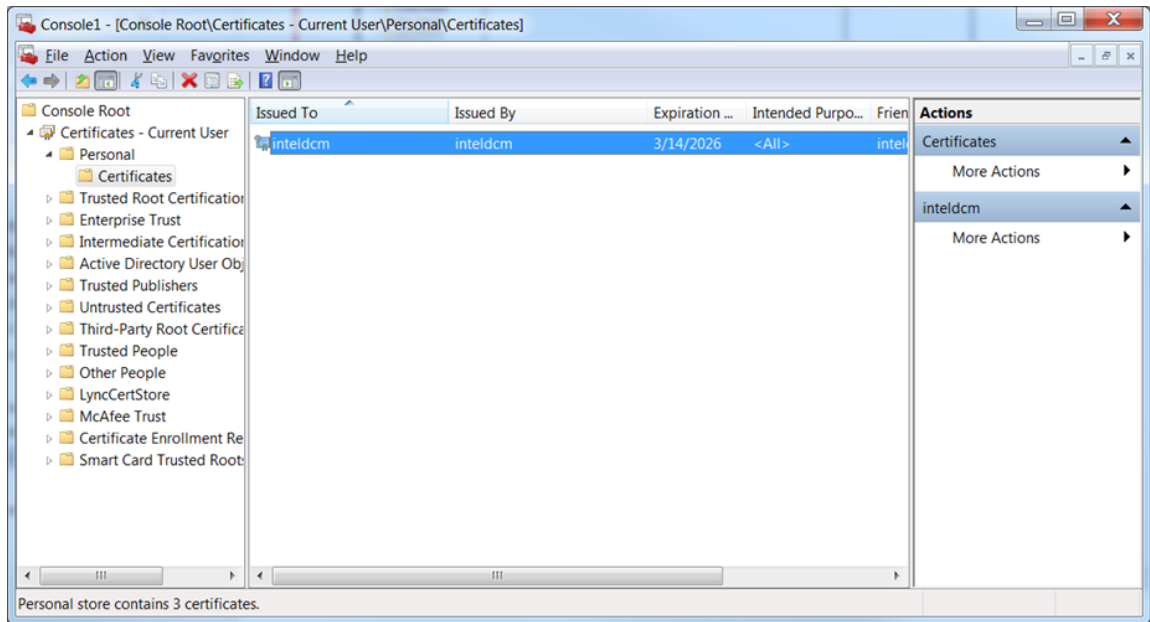


Figure 56. Console

5. Click **Next**.

Figure 57. Certificate Export Wizard

6. Select **Yes, export the private key** and select **Next**.

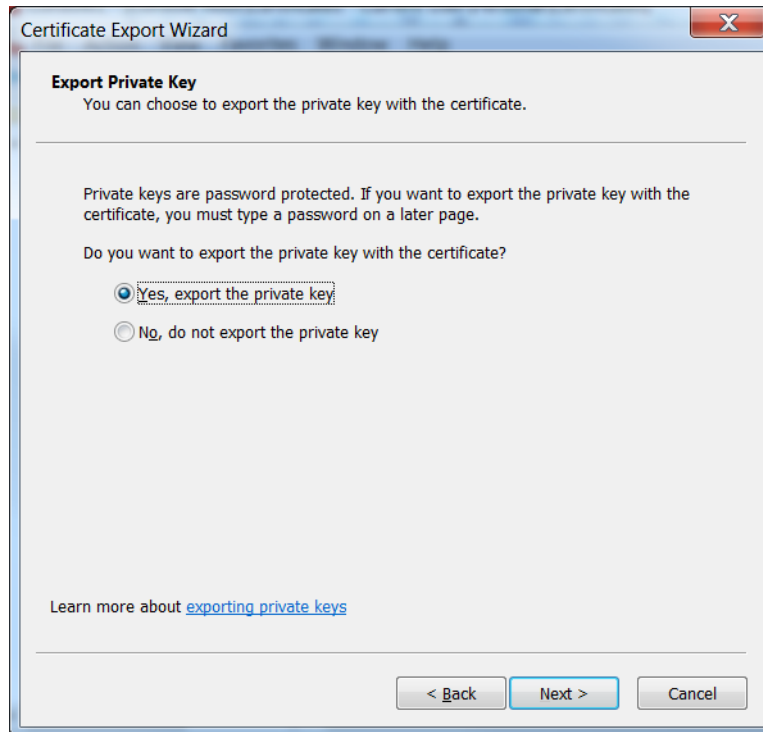


Figure 58. Certificate Export Wizard



The option will be available only if the certificate was installed with the option of being an exportable key.

7. Accept the default format **PKCS#12**, check **Include all certificates in the certification path if possible** and click **Next**.

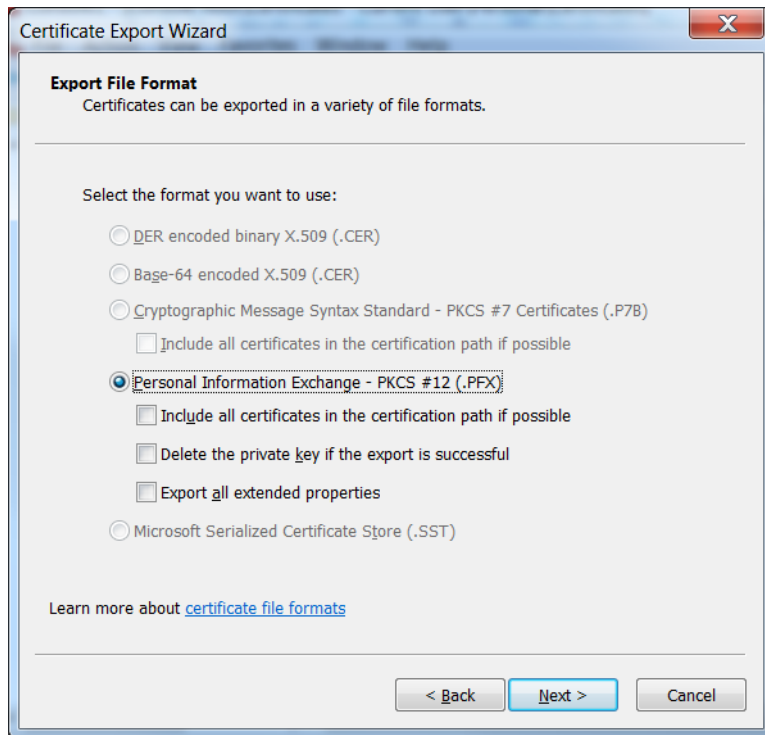


Figure 59. Certificate Export Wizard

8. Enter and confirm a password for the certificate. This is needed to install the certificate on other nodes.

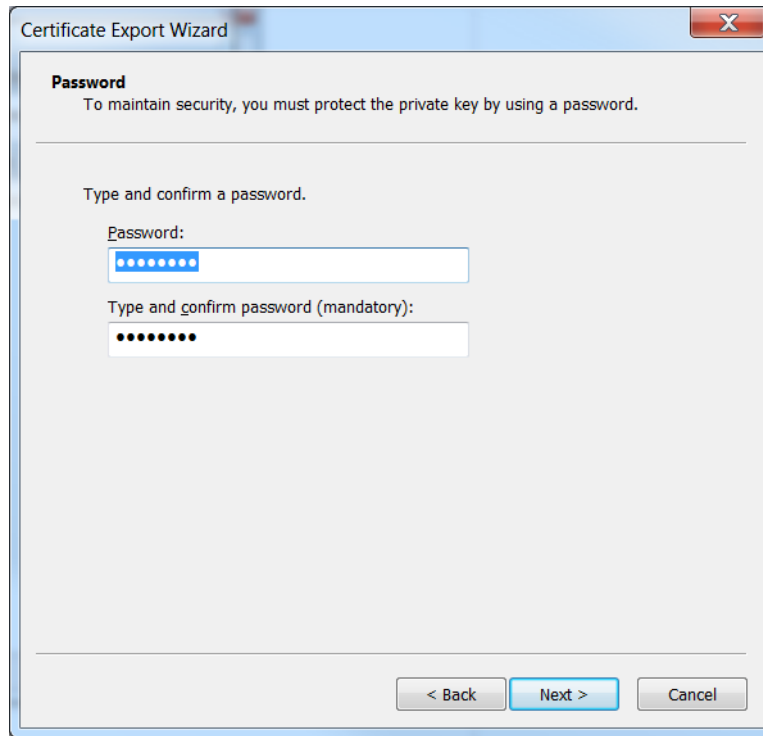


Figure 60. Certificate Export Wizard - Password

9. Type in the name of the file that contains the exported certificate and click **Next**.

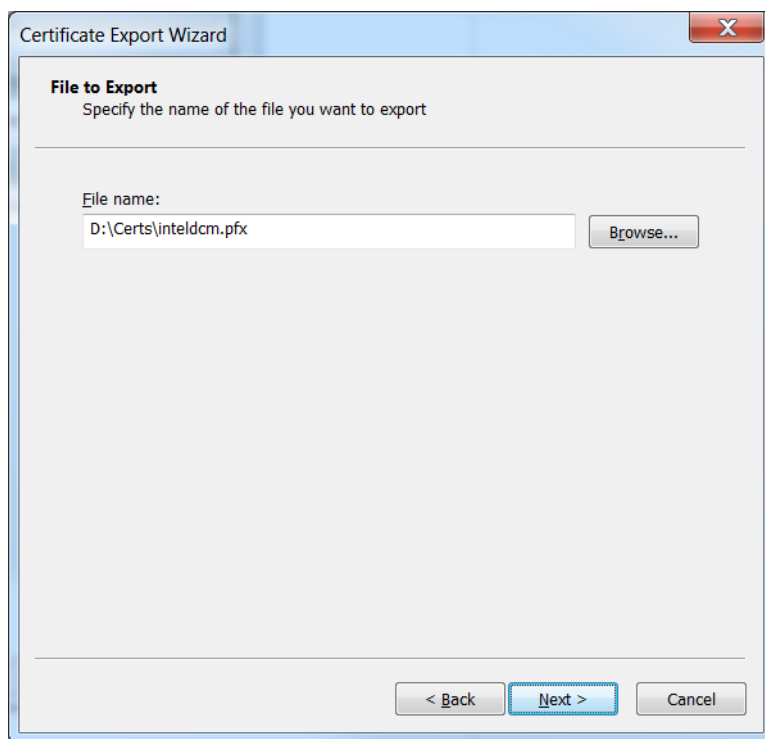


Figure 61. Certificate Export Wizard - File to export

10. Click **Finish**.

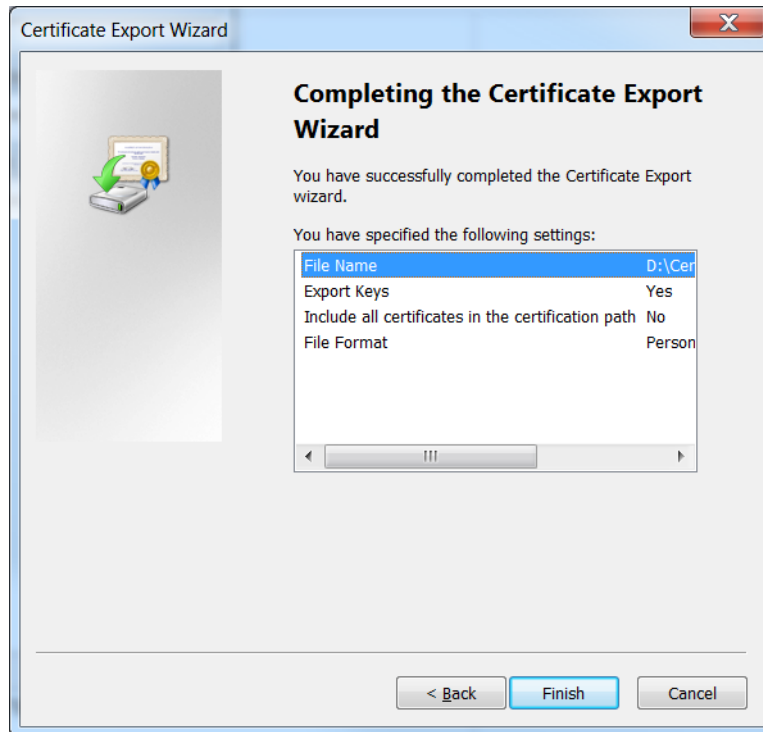


Figure 62. Certificate Export Wizard - Complete

Also see <https://technet.microsoft.com/en-ca/library/cc754329.aspx> and <https://technet.microsoft.com/en-us/library/cc730988.aspx> for more details.

Revision History

This section provides information on the revision history of this User Manual.

The following table lists the revision history of this User Manual.

Revision Index	Description	Date
-	First version published for Intel DCM Integration	November 2016
A	Published for DDC SV 60 Intel DCM Integration	December 2016

Updates in Revision A

The following table shows the updates made in this revision.

Updated Section/Sub-section	Description of Update
Section 2 Installation and Configuration	The Installing the Intel DCM Integration > Overview subsection is modified with the required software to install the Intel DCM Integration package.

Contact us

For more information please contact:

NA Regional Data Center Hub

ABB Inc.

Process Automation
125 East County Line Road
Warminster, PA 18974
USA
Phone: +1 215 674 6001

Asia, Middle East & Africa Regional Data Center Hub

ABB Pte. Ltd.

2 Ayer Rajah Crescent
Singapore 139935
SINGAPORE
Phone: +65 6776 5711

ABB AB, Control Technologies

Tvärleden 2, SE -721 59 Västerås
Sweden
Phone: +46 70 303 70 50

www.abb.com/datacenters

Copyright © 2016 ABB.
All rights reserved.

2PAA115263-600 A

Power and productivity
for a better world™

