
VERSION 3.0

Advanced Services

My Control System - Data Collector User manual





VERSION 3.0

Advanced Services

My Control System - Data Collector User manual

Document Number: 2PAA120980D3000

Document Revision: P

Release: March 2025

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 are 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 include all the features of the described or referenced standard. In order to determine the specific features included in a particular ABB product, the product specifications for the particular ABB product apply.

The buyer acknowledges the proprietary and confidential nature of the information contained in this document and agrees that all rights to and concerning the information contained in this document remain vested in ABB, in particular regarding to any intellectual property rights. Nothing contained herein shall oblige ABB to furnish any specific information to the buyer.

The information in this document is subject to change without notice and should not be construed as a binding declaration of ABB. ABB assumes no responsibility for any errors or omissions in this document.

Products described or referenced in this document are designed to be connected with networks and provide information and data through network interfaces. The products must be connected to a secure network. It is the sole responsibility of the buyer of the products to provide and continuously ensure a secure connection between the product and the system network and/or any other networks that may be connected to the product. In no event ABB is liable for the security of the network used by buyer.

The buyer of the product 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 these products, the network, its system, and interfaces against security breaches, unauthorized access, interference, intrusion, leakage, and/or theft of data or information. Any liability of ABB in this regard is excluded.

ABB may perform functionality testing on the products and may release updates. However, it is the sole responsibility of the buyer of the product to ensure that any product updates or other major system updates (included but not limited to code changes, configuration file changes, thirdparty software updates or patches, hardware change out, and so on) are compatible with the security measures implemented. The buyer of the product must verify that the system and associated products function as expected in the environment in which they are deployed. ABB has no obligations in this regard.

In no event shall ABB be liable for any damages inclusive but not limited to indirect, special, incidental or consequential damages of any nature or kind whatsoever arising from the use of this document, nor shall ABB be liable for any damages inclusive but not limited to indirect, special, incidental or consequential damages arising from the use of any software or hardware described in this document.

This document and parts thereof must be kept confidential and must not be reproduced or copied without the prior written permission from ABB, and the contents thereof must not be disclosed or made available to any third party nor used for any unauthorized purpose.

The software or hardware described in this document may be 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 2014/30/EU and in Low Voltage Directive 2014/35/EU.



The crossed-out wheeled bin symbol on the product and accompanying documents means that used electrical and electronic equipment (WEEE) should not be mixed with general household waste. If you wish to discard electrical and electronic equipment (EEE), please contact your dealer or supplier for further information.

Disposing of this product correctly will help save valuable resources and prevent any potential negative effects on human health and the environment, which could otherwise arise from inappropriate waste handling.

Table of Contents

About this user manual

User Manual Conventions	8
Warning, Caution, Information, and Tip Icons	8
Terminology	9
Release Information	9
Reference Documents	9

1 Introduction

1.1 Scope and Software Versions	10
1.2 Supported Systems and Versions	11
1.3 Compatibility	13

2 Prerequisites

2.1 Common Prerequisites	14
2.2 System 800xA	19
2.2.1 In Domain:	20
2.2.2 In Workgroup:	21
2.3 Freelance System	22
2.4 S+ Operations	24
2.5 Harmony controllers	24
2.6 Advant Master controllers with System 800xA HMI	25
2.7 Melody Rack controllers	25
2.8 Advant MOD 300	25
2.9 Procontrol P13 controllers	25
2.10 QCS with System 800xA HMI	26
2.11 Non-ABB System (Security Data collection)	26
2.12 VMware Server Health Data	26
2.13 ABB cyber security guidelines	27
2.14 Effects on cyber security policies	27

3 Setup and Maintenance

3.1 Installing MCS-DC	28
3.1.1 Manual Installation	28
3.1.2 Installation via System 800xA system installer	31
3.2 Updating to a New Version	33

3.3	Uninstalling MCS-DC	36
3.3.1	Manual Uninstallation	37
3.3.2	Uninstallation via System 800xA system installer	39
4	Data Collection	
4.1	Basic Mode Data Collection	41
4.1.1	Language and System Selection	42
4.1.2	Input Configuration	45
4.1.3	Scan, Agent Deployment and Collection	59
4.2	Advanced Mode Data Collection	61
4.2.1	Language and System Selection	63
4.2.2	System 800xA	65
4.2.3	Freelance	69
4.2.4	S+ Operations	72
4.2.5	AC 800M	73
4.2.6	AC 70, 110, 160	76
4.2.7	Freelance	78
4.2.8	AC 410, 450, MP, SG 400	78
4.2.9	Melody Rack	79
4.2.10	MOD 300	80
4.2.11	Harmony	80
4.2.12	Procontrol	86
4.2.13	QCS	89
4.2.14	ESXi	89
4.2.15	Non-ABB Systems	92
4.2.16	S+ Historian in 800xA or third party HMI environment	93
4.2.17	Scan, Agent Deployment and Data Collection	94
4.3	Periodic Collection Configuration	99
5	Post Collection	
5.1	Collection file merging	107
5.2	Limitations in data file merging	110
5.3	Report Generation from MyABB and uploading data file to ServIS	111
6	Troubleshooting	
6.1	Node scan failed	112
6.2	Agent deployment failed	112
6.3	Error message when .NET Framework is missing in the launch node	112
6.4	WMI access denied or failed to connect remote node	113
6.5	WMI DCOM access denied	113
6.6	CBA online builder cannot print application which is using RTA board	113

6.7	Connection with ICI module failed	114
6.8	Invalid certificates cause the data collection window to hang.	115
Appendix A How to change the default port number		
A.1	Basic Mode	117
A.2	Advanced Mode	118
Appendix B Configuring Secured Communication		
B.1	Selection of Server Certificate	120
B.2	Selection of Client Certificate	122
Appendix C Procontrol P13 source file (.csv) separators		
Appendix D System configuration export		
D.1	Freelance System	126
D.2	Advant MOD 300	128
D.3	AC100 System	129
D.4	Melody Rack	134
D.4.1	Melody Island Devices File	134
D.4.2	Melody CSE_Conf File	144
D.4.3	Asset structure export	145
Appendix E SHA256 Hash verification		
Appendix F Testing the WMI health of a computer		
F.1	Health check of WMI query within the local node	150
Appendix G Prerequisite tool		
Appendix H Procontrol P14 system configuration file		
Appendix I The Microsoft Defender SmartScreen		
Appendix J How to enable Windows administrative share access		
Appendix K How to check firewall settings for WMI		
Appendix L How to determine which .NET Framework versions are installed		
Revision History		171

About this user manual



Any security measures described in this user manual, for example, for user access, password security, network security, firewalls, virus protection, and so on, represent possible steps that a user of a 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 user of the system.

This user manual describes the data collection process using MCS-DC product on various ABB control systems.

User Manual Conventions

Microsoft Windows conventions as defined in the *Microsoft Writing Style Guide* are normally used for the standard presentation of material when entering text, key sequences, prompts, messages, menu items, screen elements, and so on.

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*.



Required action icon indicates actions that are required for the product or system to function as intended.



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

A complete and comprehensive list of terms is included in *System 800xA Terminology and Acronyms (3BSE089190*)*. The listing includes terms and definitions that apply to the System 800xA where the usage is different from commonly accepted industry standard definitions.

Table: Terminology

Term/Acronym	Description
CSM	Control System Monitoring
MCS-DC	My Control System - Data Collector
MCS-FW	My Control System - Forwarder

Release Information

Before using MCS-DC it is highly recommended to read the End User License Agreement, the Release Notes and this user manual. Should you need to report problems, always mention the version that you are using.

Reference Documents

Document Kind	Title Document No
My Control System (on- premise) – Installation and Configuration Manual	2PAA121208
My Control System – Forwarder – user manual	7PAA001522
My Control System (on- premise) – Hardening Guide	7PAA002031
Digital Service Products Lifecycle Plan	7PAA005206

1 Introduction

My Control System - Data Collector (in the following referred to as MCS-DC) is used to collect Performance, Lifecycle, Software and Security data from ABB's major control systems: System 800xA, Freelance and Symphony Plus. A complete list of systems, system versions and system combinations is available in [Table 1.2](#).

The collected data is bundled and encrypted into a file (.zip). This file shall be uploaded to My Control System (MCS) for further analysis and report generation, such as Benchmark report, Fingerprint report, etc. Additionally, the lifecycle information on this collection file can be uploaded to ServIS from MCS for Installed Base Management (by the local ABB installed base manager).

Download the latest version of MCS-DC from My Control System (MCS) portal or ABB library. Optionally, users can verify the authenticity of the downloaded package using its Hash value provided with the package. Refer [Appendix E, SHA256 Hash verification](#) for more details on Hash verification.

1.1 Scope and Software Versions

This user manual describes the data collection process for the various systems supported by this version of MCS-DC.

1.2 Supported Systems and Versions

Supported system versions for data collection are listed below.

Table 1.1: Supported Systems

Control System	Supported Major Versions	Supported Roll-up Versions
Freelance	<ul style="list-style-type: none"> – V8.1, V8.2 – V9.1, V9.1 SP1 – V9.2, V9.2 SP1, V9.2 SP2 – Freelance 2013, Freelance 2013 SP1 – Freelance 2016, Freelance 2016 SP1 – Freelance 2019, Freelance 2019 SP1 – Freelance 2019 SP1 FP1 – Freelance 2024 	<ul style="list-style-type: none"> – V9.2.01 – Freelance 2013 SP1 RU1, Freelance 2013 SP1 RU2, Freelance 2013 SP1 RU3, Freelance 2013 SP1 RU4, Freelance 2013 SP1 RU5, Freelance 2013 SP1 RU6 – Freelance 2016 SP1 RU1, Freelance 2016 SP1 RU2, Freelance 2016 SP1 RU3, Freelance 2016 SP1 RU4, Freelance 2016 SP1 RU5, Freelance 2016 SP1 RU6, Freelance 2016 SP1 RU7 – Freelance 2019 SP1 RU1, Freelance 2019 SP1 RU2, Freelance 2019 SP1 RU3, Freelance 2019 SP1 FP1 RU01, Freelance 2019 SP1 FP1 RU02, Freelance 2019 SP1 FP1 RU03
Advant controllers	<ul style="list-style-type: none"> – AC 450, AC 410, MP 200/1, Safeguard 415, MG 230/1, AC 160, AC 110, AC 70, 450 RMC, MOD300 – Advant Master Communication interfaces: CI520, CI522, CI541, AF100, CI810, CI820, PBS, PU535, CI532, CI535, CI570, CS513, CI510, CI610, CI615, CI810, CI820, CI626, CI627, CI630, CI631, CI830, CI671 	
Melody Rack controllers	<p>Melody Composer 4.0 to 7.x</p> <p>S+ Engineering (for Melody) 1.0.0, 1.0.1, 1.0.2, 1.1.0, 1.1.1, 1.1.2, 1.1.3, 1.4, 1.4.1, 2.0</p>	
Harmony Rack controllers (LCS only)	<ul style="list-style-type: none"> – S+ Engineering 1.0 to 2.4 SP2 – Harmony Composer 5.1, 6.0 till 7.2 	

Table 1.1: Supported Systems
(Continued)

Control System	Supported Major Versions	Supported Roll-up Versions
Harmony Rack/ Symphony Din controllers (For Performance collection)	<ul style="list-style-type: none"> – HAPI 3.1.0.15 to 4.3.0.8 and Control API 5.x.x.x. For Performance collection, Composer Harmony version is not relevant. It depends only on HAPI version. – Scan through the bridge modules IIT03 (firmware version B4 and above only)/IIT13/IEB800 is supported. – To scan a network via the bridge module IIT, the minimum firmware version of IIT must be B04. – To scan the network through an IEB bridge, it is suggested to start the data collection from the PN800 network. The bridge module IPT800 require a minimum firmware version B.0 or higher. 	
S+ Operations HMI	<ul style="list-style-type: none"> – 2.0.0 to 2.0.6, 2.1.0 to 2.1.2, 2.1.2.3, 2.2, 3.3.1, 3.3.2 (Yoda2) 	
System 800xA	<ul style="list-style-type: none"> – SV4.1 Rev M – SV5.0, SV5.0 SP1, SV5.0 SP1a, SV5.0 SP2 to SV5.0 SP2 Rev E – SV5.1 to SV5.1 FP4 Rev E – 6.0, 6.0.1, 6.0.2, 6.0.3, 6.0.3.1, 6.0.3.2, 6.0.3.3, 6.0.3.4 – 6.1, 6.1.0.1, 6.1.1, 6.1.1.1, 6.1.1.2, 6.2, 7.0 	<ul style="list-style-type: none"> – SV5.1 Rev D Roll-up 5, SV5.1 Rev E Roll-up 2, SV5.1 FP4 Rev D Roll-up 4, SV5.1 FP4 Rev D Roll-up 5, SV5.1 FP4 Rev E Roll-up 3, SV5.1 FP4 Rev E Roll-up 4, 6.0.3.3 Rev B – 6.0.1 Roll-up 1, 6.0.3 Rollup1, 6.0.3 Roll-up 2, 6.0.3 Roll-up 3, 6.0.3 Roll-up 4, 6.0.3.3 Rev B – 6.1 Roll-up 1
QCS with System 800xA HMI	<ul style="list-style-type: none"> – 5.0 SP2, SV 5.1 to 5.1 FP4 Rev E, 6.0, 6.0.1, 6.0.2, 6.0.3, 6.0.3.1, 6.0.3.2, 6.0.3.3, 6.0.3.3 Rev B, 6.1, 6.1.0.1, 6.1.1, 6.1 SP2, 6.1 SP3 RU1, 6.1 SP4, 6.2 	
Non-ABB Systems (Cyber security data only)	<ul style="list-style-type: none"> – All Windows Operating systems with .NET Framework version 3.5 SP1 or above installed. 	
ESXi	<ul style="list-style-type: none"> – 6.0, 6.7, 7.0, 8.0 U2 	

1.3 Compatibility

MCS-DC 3.0 or newer versions are compatible with MCS-FW version 1.9 and above. These are not backward compatible. MCS-FW 1.9 is compatible with MCS (on-premise) v6.9 and newer versions. Refer to the Digital Service Products Lifecycle Plan [Section Reference Documents on page 9](#).

2 Prerequisites

Prerequisites for data collection are described in this section.



The verification of data collection prerequisites and some configuration settings may differ based on the Operating System that is installed on a given node. In this user manual we will refer to “legacy” and “modern” Operating System versions where “legacy” are Windows XP and Windows Server 2003, “modern” are Windows 10 and Windows Server 2012 or above, etc.

2.1 Common Prerequisites

These prerequisites are applicable to all Systems and System combinations. Prerequisites specific to each system family are described in respective chapters.

- Based on the HMI system and the controllers that must be collected, the MCS-DC launch node may vary. Details are described in respective section.
- The data collection user must have administrator rights. For a Domain network, the user must also be a member of the domain administrator group.
- The recommended screen resolution is 1920x1200 (Height 1920, Width 1200)
- If the control system is running in a Windows workgroup, and if the **User Access Control Remote Restrictions** are enabled on the nodes in the network, it is mandatory to use the **built-in administrator** account for data collection. If any other administrator account is to be used instead of the built-in administrator account, it is required to disable the UAC remote restrictions on all nodes, before deploying the data collector agent. Once the agent is deployed, UAC remote restrictions can be enabled back (if this was the original state). UAC remote restrictions can be disabled/enabled using MCS-DC Prerequisite tool. Refer to [Appendix G, Prerequisite tool](#) for more details. Run the prerequisite tool in every node in the workgroup network and make the nodes ready for data collection.
- MCS-DC uses port number 23571 as default. Should you need to use a different port, refer to [Appendix A, How to change the default port number](#) of this document. If MCS-DC detects that the port that is chosen is already in use, a notification is shown, asking to change the port number.
- The node where MCS-DC is deployed must be reachable by IP Address from any other node part of data collection.

2 Prerequisites

2.1 Common Prerequisites

- Enable file and Printer sharing.
 - The procedure to **“Enable file and Printer sharing”** is different for legacy and modern operating systems.
For modern operating systems, in allowed programs section under firewall settings, click on change settings to enable the File and Printer sharing service for all networks (Domain, Public and Private).

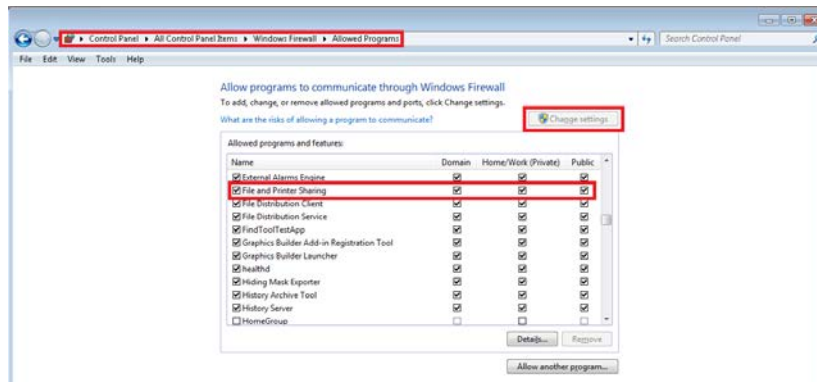


Figure 2.1: File and Print sharing

- In case of Windows XP, open Windows Firewall exceptions in the Control Panel and enable “File and Printer Sharing”.

2 Prerequisites

2.1 Common Prerequisites

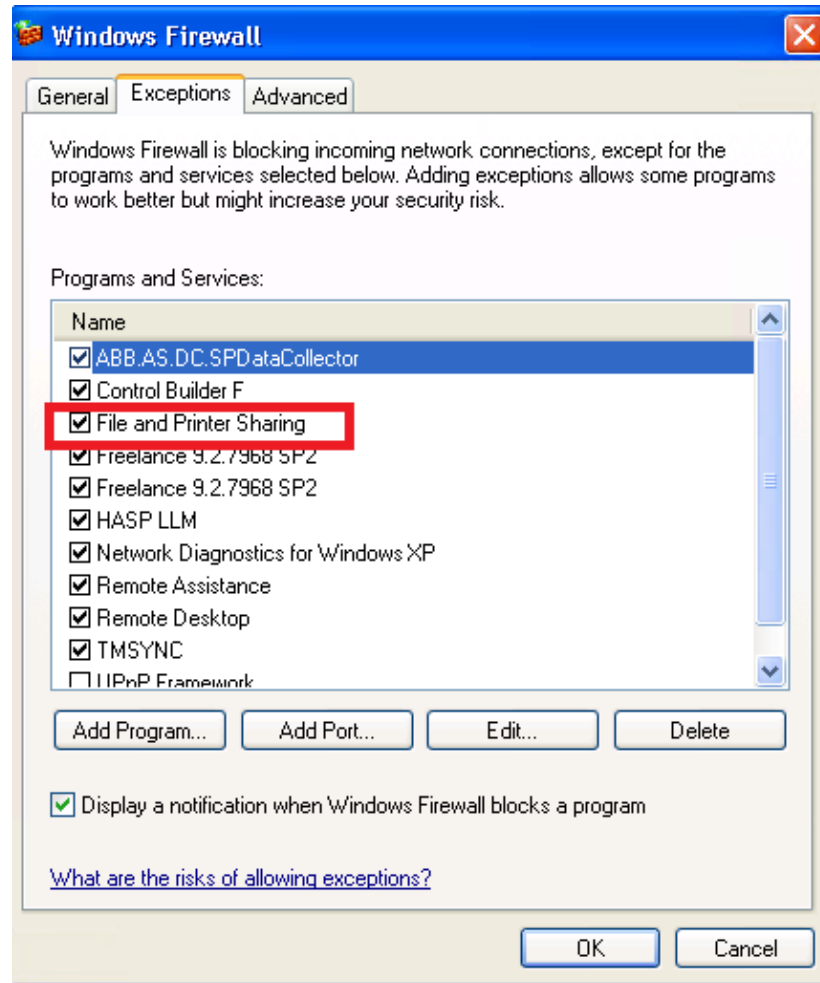


Figure 2.2: File and printer sharing for Windows XP

2 Prerequisites

2.1 Common Prerequisites

- Enable **Windows Management Instrumentation (WMI)**.

The procedure to enable “Windows Management Instrumentation (WMI)” is different for legacy and modern operating systems.

- For modern operating systems, in allowed programs section under firewall settings, click on change settings to enable the File and Printer sharing service for all networks (Domain, Public and Private). Refer to [Appendix K, How to check firewall settings for WMI](#) for more details.

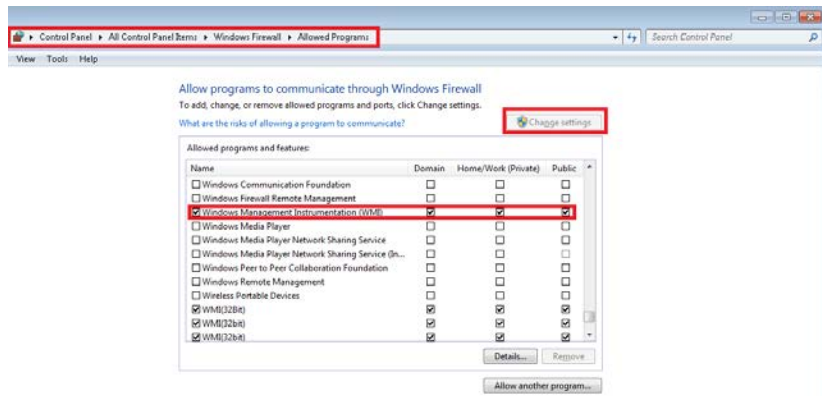


Figure 2.3: Windows Management Instrument (WMI)

- In case of Windows XP, go to *Administrative Tool* → *Computer Management* → *Services and Applications* → *WMI control*. Right click on WMI control and select the tab *Security*. Add the logged in administrator user if not present in *Group or usernames* section. Enable the *Remote enable* permission for the user and click *OK*. For allowing WMI through firewall, execute the command ***“netsh firewall set service RemoteAdmin enable”*** in a command prompt.

2 Prerequisites

2.1 Common Prerequisites

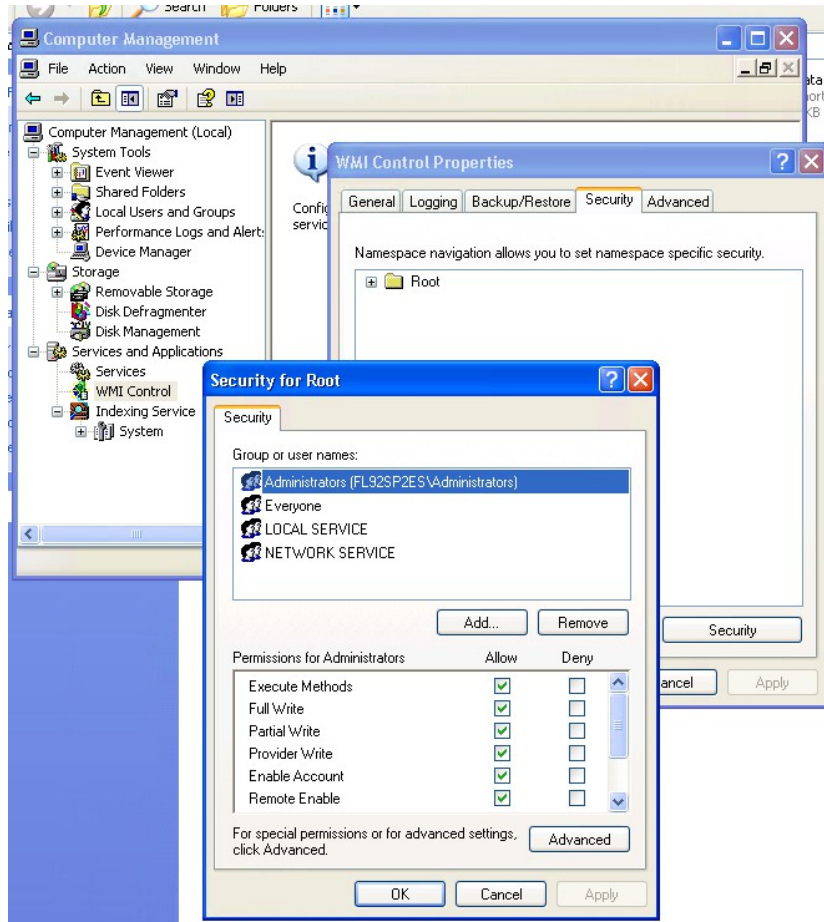


Figure 2.4: WMI for Windows XP

- Turn on Network Discovery.

As shown in figure, enable network discovery for Domain and Private network profiles.

Allow apps to communicate through Windows Defender Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Change settings

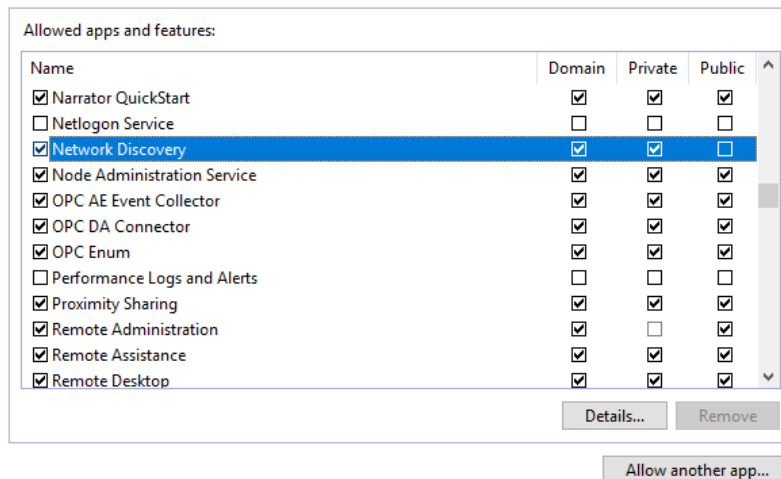


Figure 2.5: Turn on Network Discovery



It is important to revert all the changes made as part of prerequisite settings, after completing the data collection.



A tool is created for System 800xA and Freelance that checks whether prerequisites are met on each node and assists the user in installing them, if they aren't. Changes can be rolled back using the tool after data collection. Refer to [Appendix G, Prerequisite tool](#) for more details.

2.2 System 800xA

Refer to [Section 2.1, Common Prerequisites](#) for common prerequisites applicable to all system families. The following sections describe the prerequisites specific to System 800xA.

2.2.1 In Domain:

- Microsoft®.NET Framework 1.1 or above.

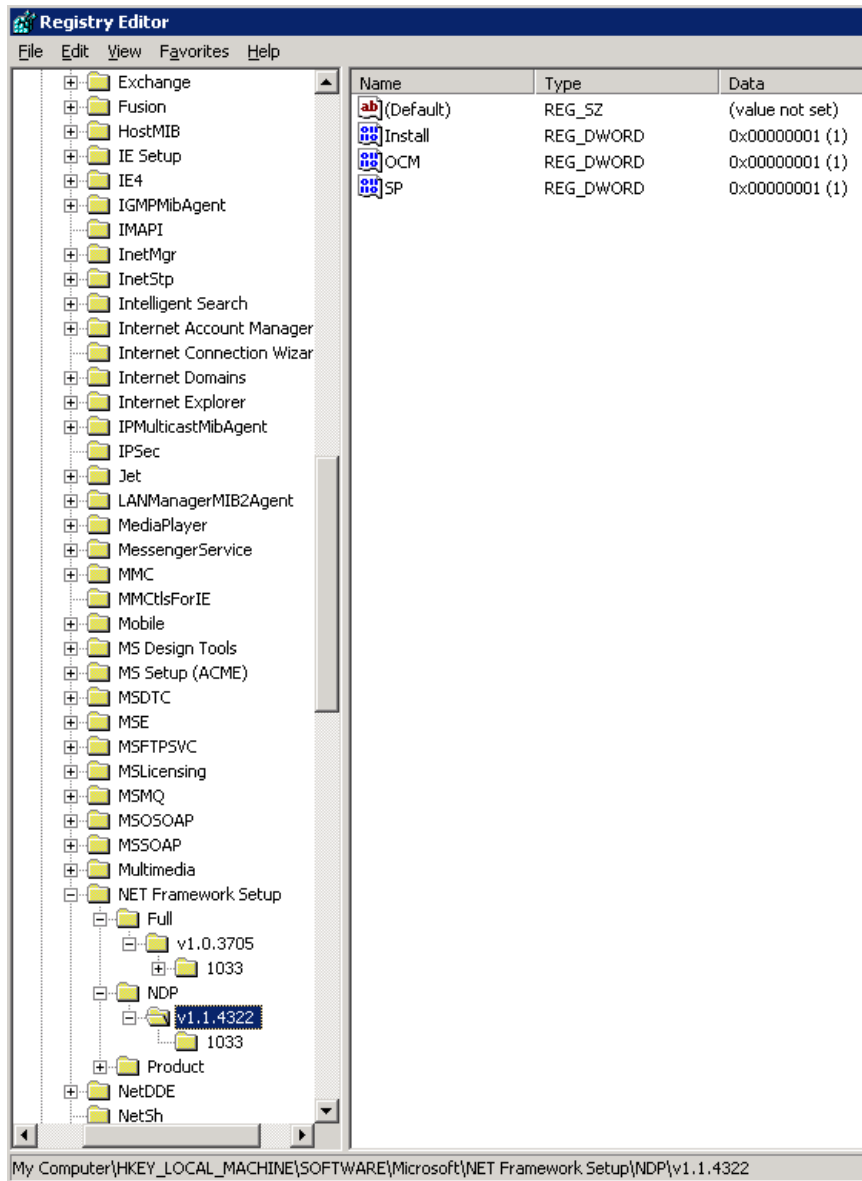


Figure 2.6: .NET Framework 1.1

- User accounts and passwords with administrative rights are required for all 800xA computers.
- User account must be part of IndustrialITUser group for System 800xA version lower than 6.2. For the versions 6.2 and above, user must be part of user group in which System 800xA users are configured.
- The launch node of MCS-DC must be part of a running System 800xA.
- MCS-DC will not collect data on nodes that have installed HP disk driver version 6.26.0.64 (hpcisss2.sys) or lower.
- Make sure to revert all the changes done as part of the prerequisite settings after completing the data collection.

2.2.2 In Workgroup:

- Microsoft®.NET Framework 1.1 or above

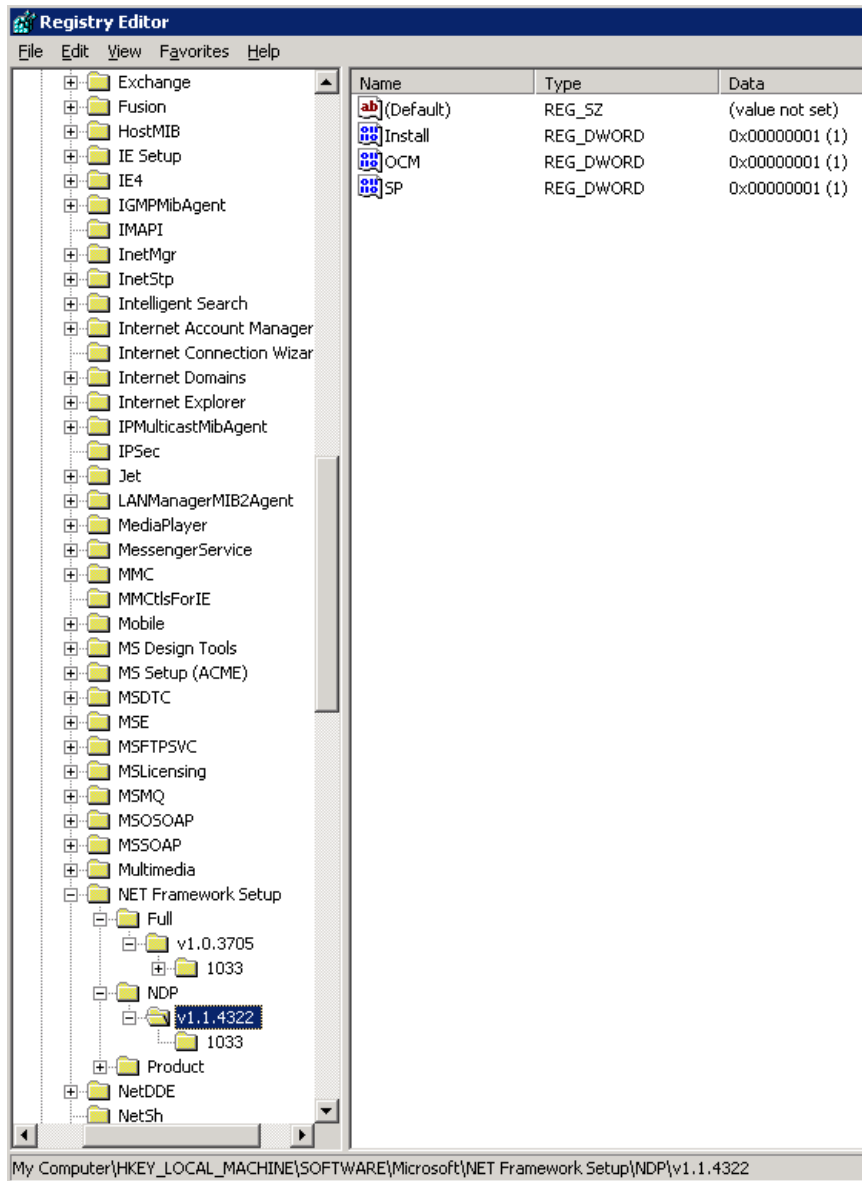


Figure 2.7: .NET 1.1 or above

- UAC Remote restrictions must be disabled on all nodes in the workgroup network. UAC remote restrictions can be disabled/enabled using MCS-DC Prerequisite tool. Refer to [Appendix G, Prerequisite tool](#) for more details.
- User accounts and passwords with administrative rights are required for all 800xA computers.
- User account must be part of IndustrialITUser group for System 800xA version lower than 6.2. For the versions 6.2 and above, user must be part of 800xA user group.
- The node that runs this collection tool must be a part of running System 800xA.
- MCS-DC will not collect data on the nodes which has HP disk driver version of 6.26.0.64 (hpciss2.sys) or lower.

- It is important to revert all the changes made as part of prerequisite settings, after completing the data collection.



Basic mode data collection is not supported for System 800xA in Windows workgroup network.

2.3 Freelance System

Refer to [Section 2.1, Common Prerequisites](#) for common prerequisites applicable to all system families. The following are the prerequisites for freelance data collection. The prerequisite tool described in [Appendix G, Prerequisite tool](#) shall be used to check and install the prerequisites mentioned below, in each Freelance node in the network. Once data collection is complete, the tool can be used to roll back changes.

- Microsoft®.NET Framework 2.0 Service Pack 1 or above. Installed .NET version can be checked under the path HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NETFramework Setup\NDP\v2.xx\Full.

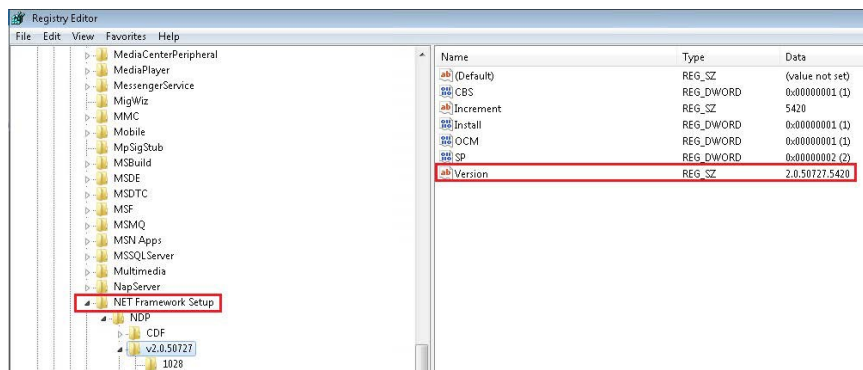


Figure 2.8: .NET Framework version

- Start Windows Services application and verify that the Service "Server" is running. It must be running, and its startup time must be automatic. Refer [Section J, How to enable Windows administrative share access](#) for more details.

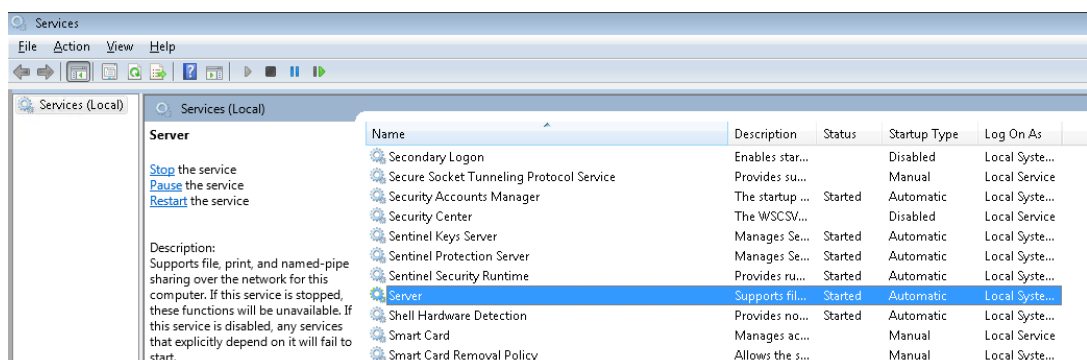


Figure 2.9: "Server" running in Windows services

- Disable User Account Control Remote Access Restrictions. In order to disable the UAC remote access restrictions, create a new registry key LocalAccountTokenFilterPolicy of DWORD type the path HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
 \CurrentVersion\Policies\system\LocalAccountTokenFilterPolicy and provide the value as 1. This setting can be reverted once the data collection completes.
- If Freelance client nodes have Windows XP and are in a workgroup, then do the following registry settings in those nodes:
 1. Open registry by running the command regedit.exe
 2. Expand HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control.
 3. Select Lsa.
 4. Change the value for the forcequest DWORD to 0:
- User accounts and passwords with administrative rights are required for all Freelance computers. Enter the user credentials in computer name\ Username format.
- Launch MCS-DC on Freelance engineering client. If MCS-DC is launched on any other Freelance computer, then Freelance Engineering client will be skipped.
- MCS-DC will not collect data on nodes that have installed HP disk driver version 6.26.0.64 (hpcisss2.sys) or lower.
- Make sure to revert all the changes done as part of the prerequisite settings after completing the data collection.



Make sure that no external GPS clock is connected to the Freelance system for time synchronization. In rare cases, it is observed that the precision of the time signal changes during system scan, it may be prudent not to collect performance data in this case.

2.4 S+ Operations

Refer to [Section 2.1, Common Prerequisites](#) for common prerequisites applicable to all system families. The following software is required for installation and operation of S+ Operations Data Collector.

- .NET Framework 4.0 and above.

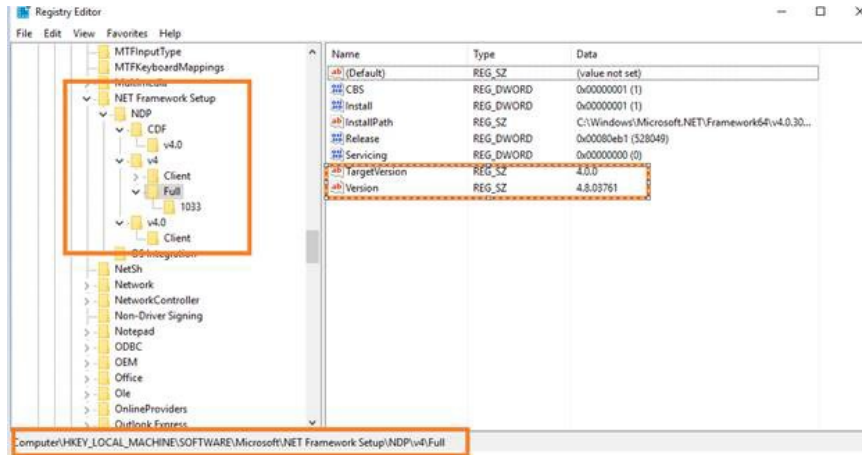


Figure 2.10: .NET Framework 4.0 and above

- Enable administrator share access in windows. To enable the administrator share access refer [Section J, How to enable Windows administrative share access](#).
- It is important to revert all the changes made as part of prerequisite settings after completing the data collection.

2.5 Harmony controllers

- MCS-DC must be launched on a node that can reach the Control Network; the suggestion is to execute it in S+ Engineering Servers, or S+ Engineering Clients.
- HAPI is installed and can connect to configured ICI (IET800). IET800 is mutually exclusive for MCS-DC for the duration of data collection (MCS-DC connects to IET800 in exclusive mode).
- MCS-DC launching node must have .NET Framework 4.5.2 or above.
- Microsoft Visual C++ 2012 Redistributable(x86) -11.61030 or C++ 2015 Redistributable(x86) -14.26.29910 is installed.
- HAPI is licensed based on version being installed/used.
- To collect Lifecycle information browsing a Composer Harmony project (*.epb file) data collection must be necessarily done on Composer Harmony's (S+ Engineering) node.

2.6 Advant Master controllers with System 800xA HMI

- Microsoft® .NET Framework 2.0 Service Pack 1 or above.
- Online Builder must not be running and should not be started while data collection is in progress. This is valid for all the system variants.



Starting the Online Builder during execution of MCS-DC will result in incomplete data collection.



In case selected target node does not have Microsoft® .NET Framework 2.0 Service Pack 1 or higher, select another node, possibly non-critical for plant operation. There is a rare possibility and low risk of application conflicts because of two different versions of Microsoft® .NET Framework running in the same node. Once you choose the node, download and install the Microsoft® .NET Framework 2.0 Service Pack 1 on this node and run the MCS-DC tool.

- The .NET Framework version of the MCS-DC launch node must be same or lower than the .NET Framework version installed on the data collection nodes. Data collection will fail for the nodes with higher .NET Framework version.



In the event that the controller load exceeds 80% or the controller has been locked by another user, MCS-DC will skip the data collection from the Advant Master controller.

2.7 Melody Rack controllers

- Microsoft® .NET Framework 3.5 SP1 or above.

2.8 Advant MOD 300

- Exported System or Project configuration file is an important prerequisite to collect lifecycle data for MOD 300 System.
- Microsoft® .NET Framework 2.0 Service Pack 1 or above is required for the MCS-DC to run. This is not supplied with the MCS-DC package. User is requested to download it from the Microsoft website.
- The MOD API must be installed in the MCS-DC launch node.

2.9 Procontrol P13 controllers

- Microsoft® .NET Framework 2.0 Service Pack 1 or above is required for the MCS-DC to run. This is not supplied with the MCS-DC package. User is requested to download it from the Microsoft website.
- Exported System or Project configuration file is an important prerequisite to collect lifecycle data for Procontrol P13 hardware. Please note, in the exported P13 Source file (.CSV), the text separator must be double quotes (") and the field separator should be comma (.). For more details refer Appendix C.

2.10 QCS with System 800xA HMI

- Microsoft® .NET Framework 2.0 Service Pack 1 or above is required for the MCS-DC to run. This is not supplied with the MCS-DC package. User is requested to download it from the Microsoft website.
- Latest config.xml file from QCS connectivity server.

2.11 Non-ABB System (Security Data collection)

- Microsoft® .NET Framework 3.5 Service Pack 1 or above is required for Non-ABB security data collection. This is not supplied with the MCS-DC package. User is requested to download it from the Microsoft website.
- Make sure Windows Management Instrumentation (WMI) service is running in Windows services list. If not, start it.
- Enable Windows Management Instrumentation (WMI) in Windows firewall exemption list on all the nodes.

2.12 VMware Server Health Data

- In order to collect VMware server health data, VMware performance counters must be enabled in each VMware server. These counters are about VM memory and VM processor. These counters are usually enabled, but it is suggested to check that they are really available.

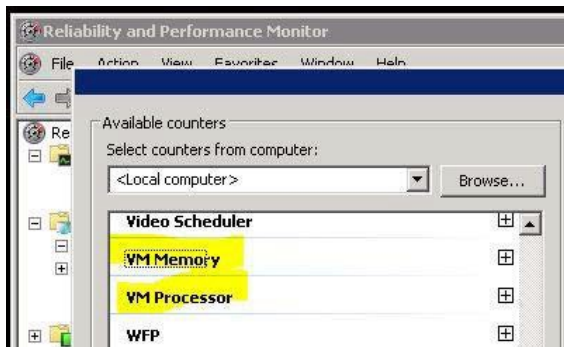


Figure 2.11: VM Performance Counters



It has been observed that, at times, VMware provides inconsistent results. To overcome this, MCS-DC has a data collection retry option that can be enabled to guarantee that a certain number of retries is performed. Select settings (gear icon in the top-right corner of the screen) and select "Collection Retry" tab.

The number of retries can be selected to be between one and six; in addition, a time-interval between retries can be selected too (minimum thirty seconds, maximum two minutes).

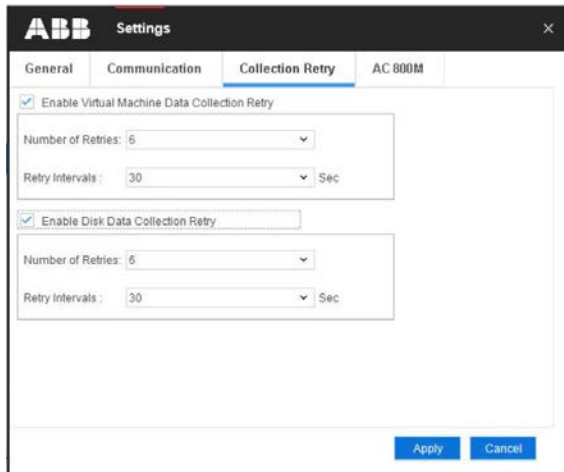


Figure 2.12: Collection Retry

2.13 ABB cyber security guidelines

Below suggestions are provided to comply with ABB cyber security guidelines:

- For complying with ABB minimum cyber security guidelines, it is recommended to launch MCS-DC on a less privileged node, run as administrator and provide required credentials to access other computers on the network.
- It is recommended to use the secured communication for data collection. Refer to [Appendix B, Configuring Secured Communication](#) for details on secured communication configuration.
- It is recommended to use TLS versions 1.2 or above on the MCS-DC launch node. If the recommended TLS version is not supported or available on the launch node, please find a suitable launch node before running MCS- DC to make communication secure.
- User will be warned and acknowledgment will be required to proceed with data collection when TLS version is less than 1.2 or weaker cyber suits are found on the launch node.
- It is recommended to have an Anti-virus installed on the node where MCS- DC is launched.

2.14 Effects on cyber security policies

MCS-DC execution may trigger cyber security warnings. Examples of this are:

- Executing the tool could trigger alarms in network anomaly detection systems. An allow-listing solution could block execution of the tool
- Refer to the documentation of the cyber security solution(s) or consult the service organization which implemented the cyber security solution(s) to determine the possible impact and possible measurement(s) to be taken to overcome any negative impact when operating the tool.
- All needed services, user rights and needed open ports are documented in [Section 2, Prerequisites](#) and [Section 4, Data Collection](#) in this user manual.

3 Setup and Maintenance

The procedure for installing, updating, and removing the MCS-DC is described in this section.

Download the latest version of MCS-DC from ABB library. Optionally, users can verify the authenticity of the downloaded package using its hash value provided with the package. For more details on hash verification, refer to [Appendix E, SHA256 Hash verification](#).

3.1 Installing MCS-DC

MCS-DC can be installed manually or via System 800xA system installer.



If MCS-DC is installed via System 800xA system installer, update to a newer version is possible only via a newer version of system installer. The same applies to uninstalling MCS-DC.



Ensure that all the prerequisites mentioned in [Section 2, Prerequisites](#), are met before installing.

3.1.1 Manual Installation

Execute the following steps to install the MCS-DC manually:

1. Copy the downloaded package to the computer node where MCS-DC is to be installed and unzip the package.
2. Right click on **ABB.MCSDDataCollector.Installation** and run it as **Administrator**.

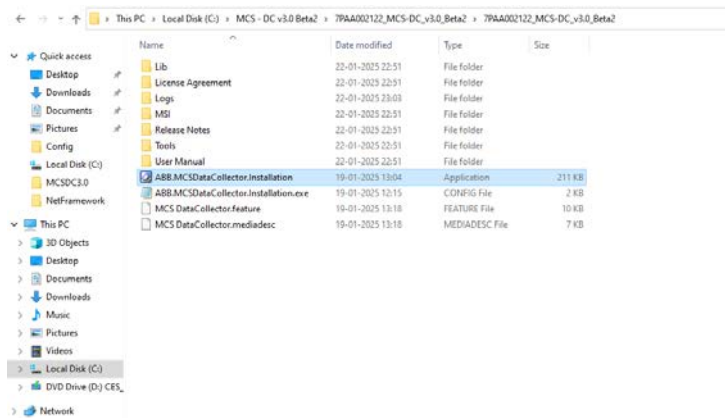


Figure 3.1: MCS-DC installation package

3 Setup and Maintenance

3.1 Installing MCS-DC

3. Starting with version 2.10, MCS-DC supports data collection from Japanese language systems. Select the applicable language on the installation wizard and click **Next**, as shown in **Figure 3.2**.

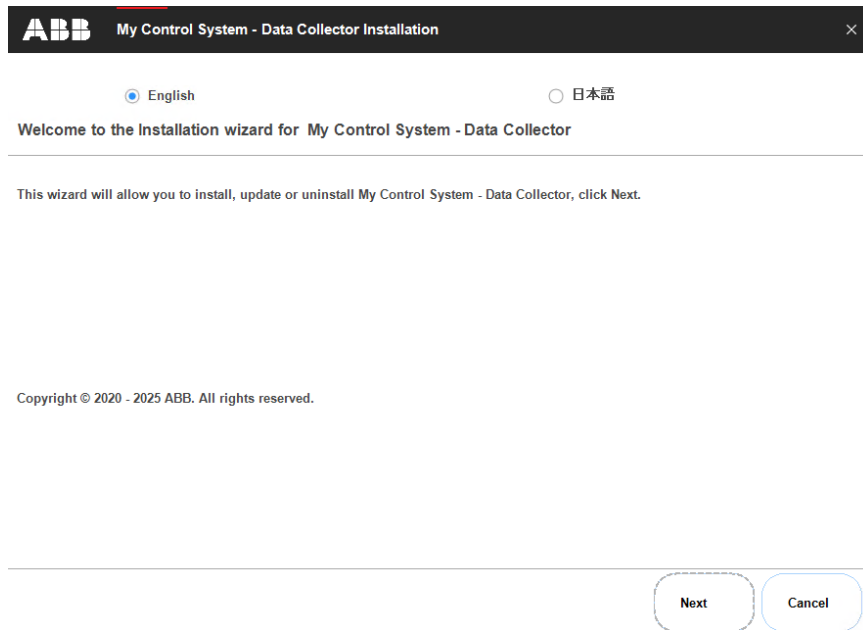


Figure 3.2: MCS-DC Installation Wizard

4. Select **Install** option and click **Next**, as shown in **Figure 3.3**.

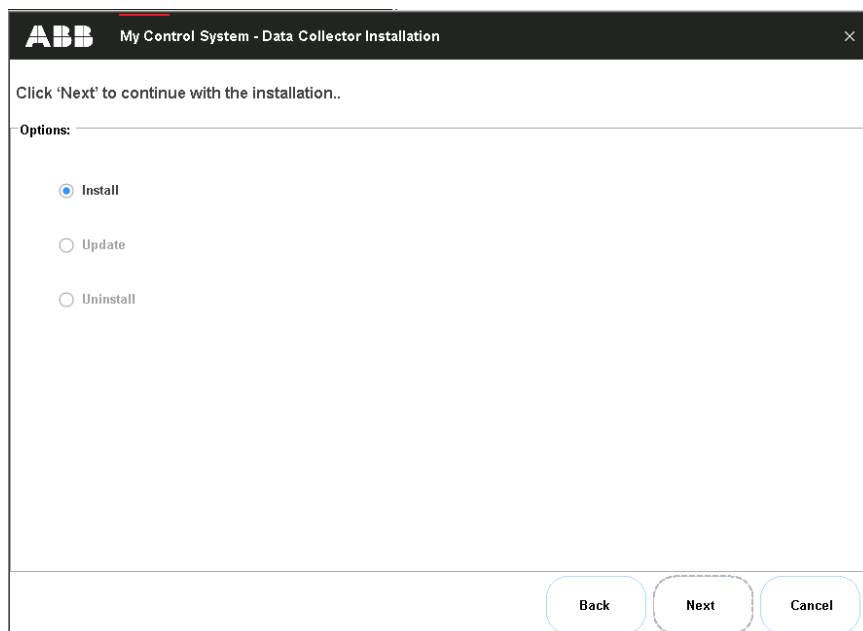


Figure 3.3: MCS-DC Installation

5. Version information will appear on the screen. Click **Next** to continue.

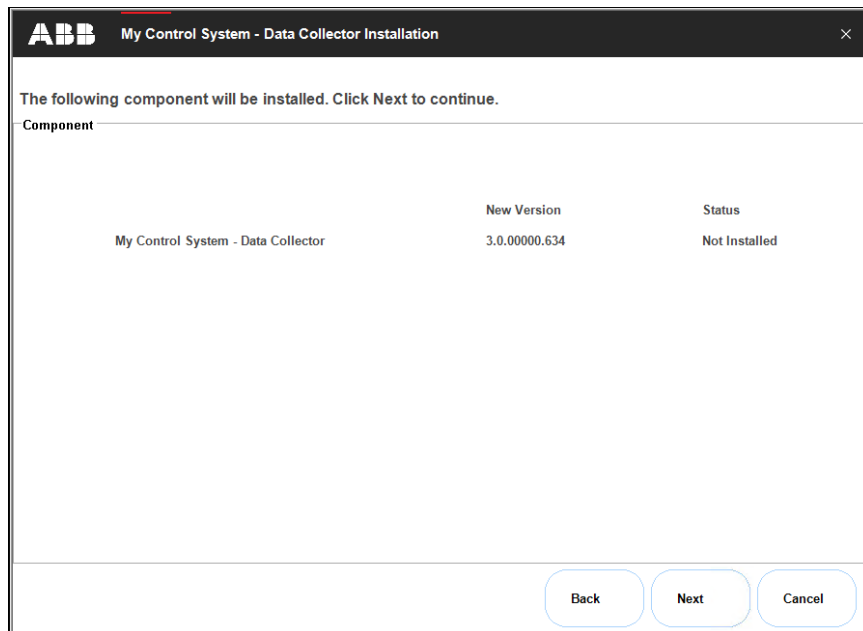


Figure 3.4: Version details

6. Installation begins. Once completed, click **Finish** to exit the wizard.

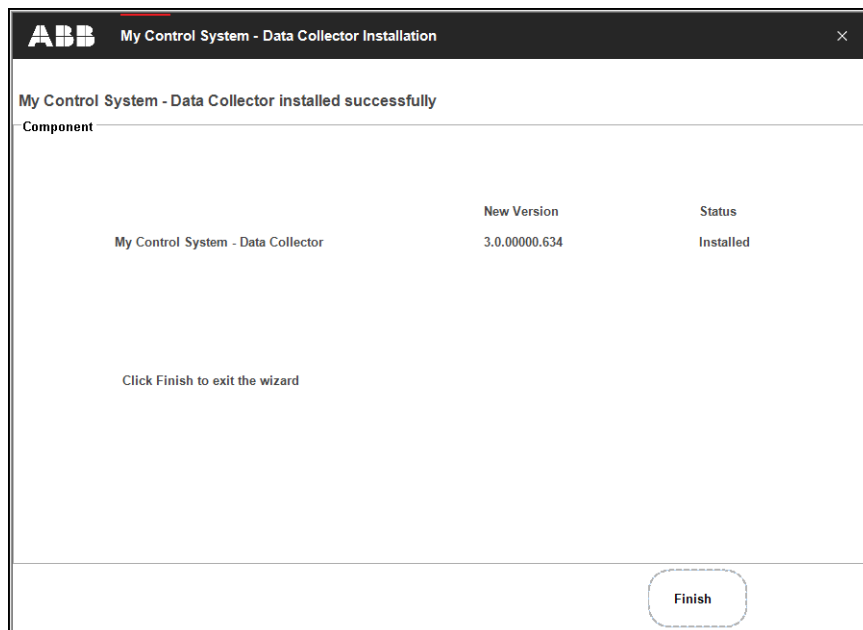


Figure 3.5: Installation completed

7. Proceed with the data collection as described in [Section 4, Data Collection](#).

3.1.2 Installation via System 800xA system installer

Alternatively, the System 800xA users shall utilize the system installer functionality to install the MCS data collector. MCS Collectors and Forwarder are integrated into the System 800xA media since version 7.0. To install MCS-DC using the system installer, follow the steps below.

1. In 800xA system installer, select the system function **MCS Data Collector** under **Lifecycle Service** and click **OK**.

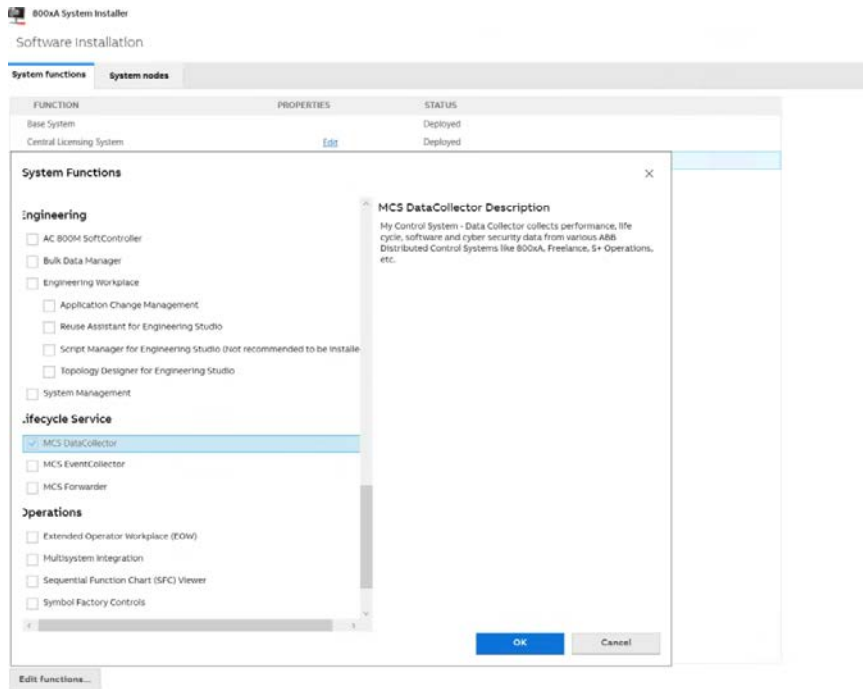


Figure 3.6: Select the system function MCS Data Collector.

3 Setup and Maintenance

3.1 Installing MCS-DC

2. As shown in **Figure 3.7** as soon as it is added to the list of system functions, the **MCS Data Collector** will appear as deployed even before it is deployed. Ignore this status and proceed to the next step.

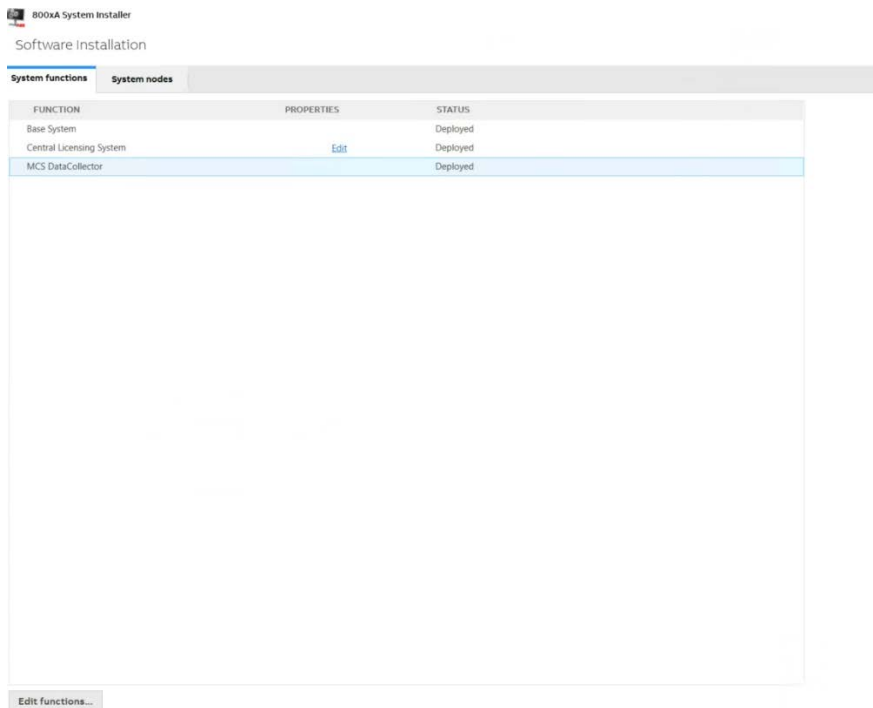


Figure 3.7: System functions list

3. Under **System nodes** tab, select a node with client node role, where MCS-DC is to be installed. Click on **Allocate function** and select the **MCS Data Collector** as shown in **Figure 3.8**. Click **OK**.

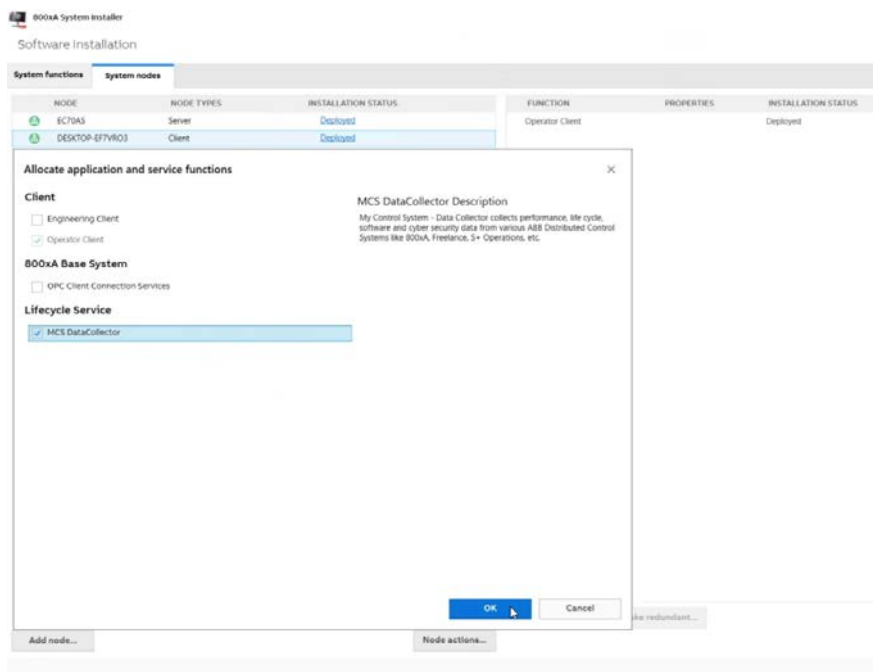


Figure 3.8: Node function

4. Install MCS-DC by clicking on the **Deploy system** button.

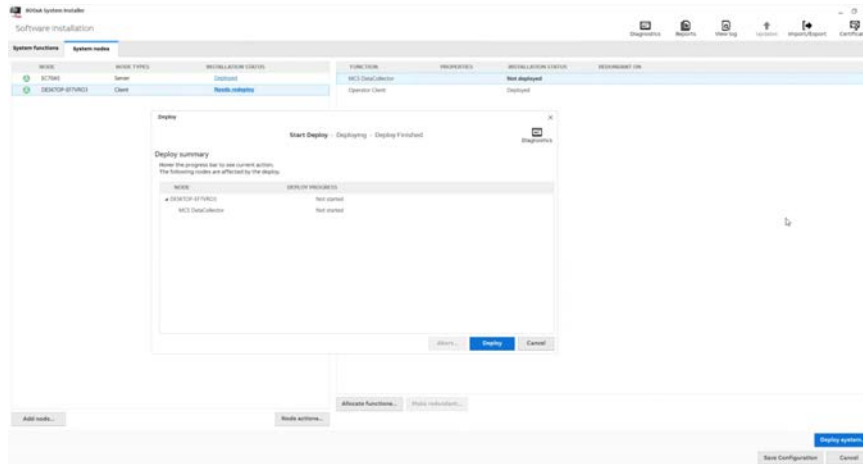


Figure 3.9: Deploy system

3.2 Updating to a New Version

This section describes the procedure for updating the MCS-DC.



If MCS-DC was installed via System 800xA system installer, follow the standard update procedure of system installer for updating the MCS-DC. Manual update (procedure mentioned below), is not possible if the previous installation was done via system installer.



Ensure that any running instance of MCS-DC must be closed prior to the update and the data collection is not scheduled to run during the update process.

3 Setup and Maintenance

3.2 Updating to a New Version

1. Copy the MCS-DC package into the local disk (hard disk drive partition for Operating System) of the system where the MCS-DC has to be installed. Unzip the package.
2. Find the MCS-DC installation file ABB.MCS-DC. Installation in MCS-DC folder, right click and run it as **Administrator**. ABB MCS-DC Installation Wizard opens, select **Update** and click **Next** to continue.

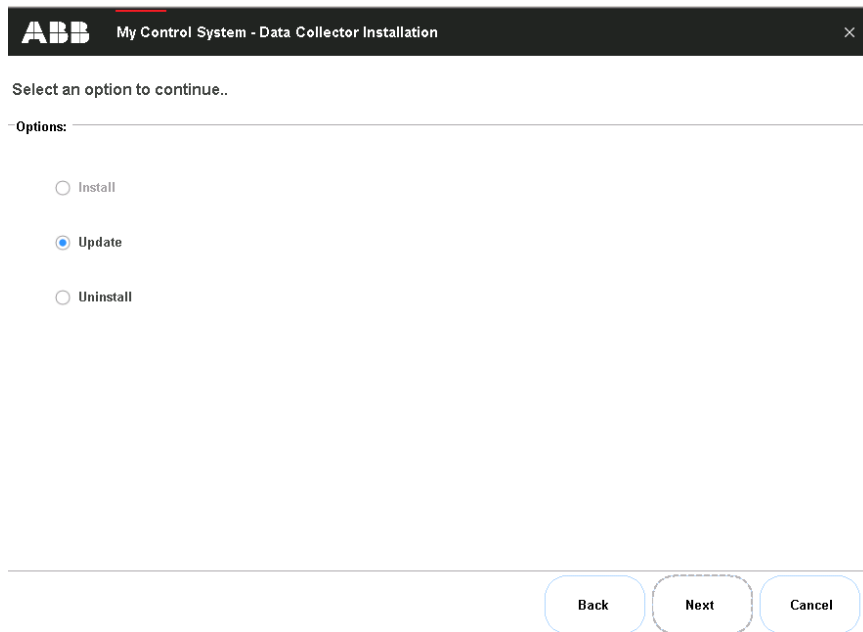


Figure 3.10: ABB MCS-DC Installation Wizard

If periodic data collection is configured and running, user will be notified that the data collector service will be stopped to continue with the update process.



Update is not possible if data collection is scheduled to run within an hour during the update. This will be notified to the user and the update window will be closed.

3 Setup and Maintenance

3.2 Updating to a New Version

3. New and installed version will appear on the screen. Click **Next** to continue.

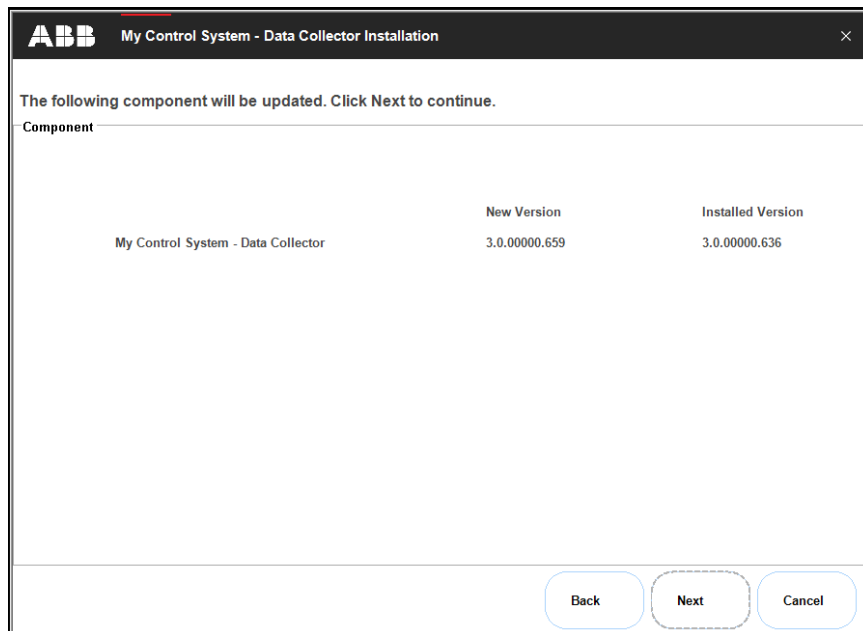


Figure 3.11: New and installed version

4. Update begins. Once the update is completed click **Next** to continue.

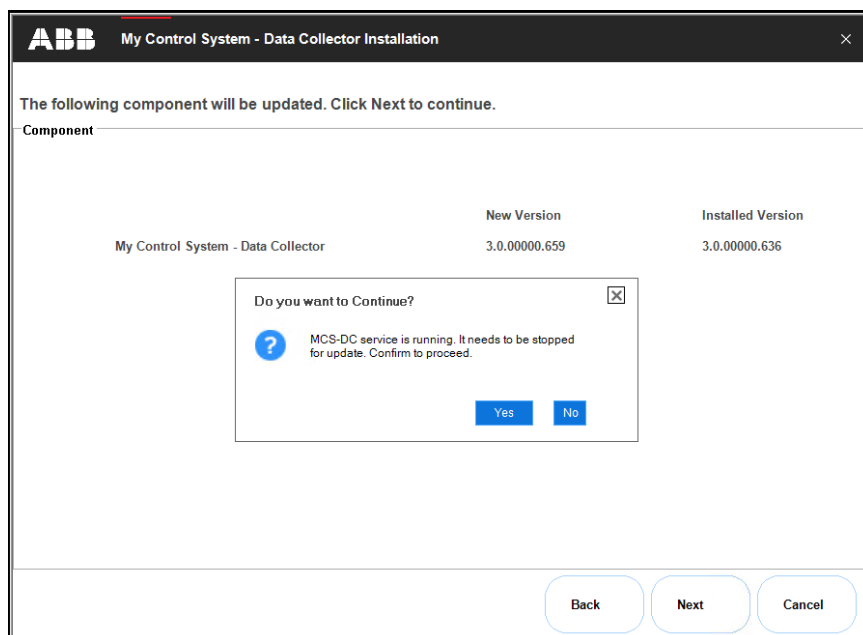


Figure 3.12: Update in progress

5. Upon completion, the update status will be displayed. Click **Finish** to close the update window.

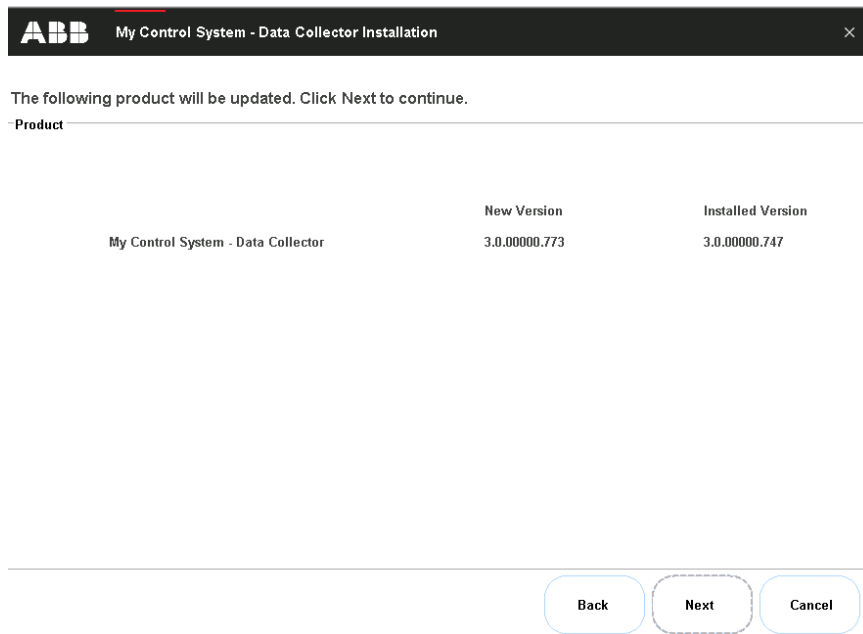


Figure 3.13: Update successful

3.3 Uninstalling MCS-DC

This section describes the procedure for uninstalling the MCS-DC manually or via System 800xA system installer.



MCS-DC should only be uninstalled through the MCS-DC installation wizard. It shall not be uninstalled from Windows Add/Remove programs

3.3.1 Manual Uninstallation

1. Launch the MCS-DC Installation Wizard (refer to **Step 1** to **Step 3** of **Section 3.1, Installing MCS-DC**). Click **Next** to continue.
2. Select the language and click **Next**, to continue.

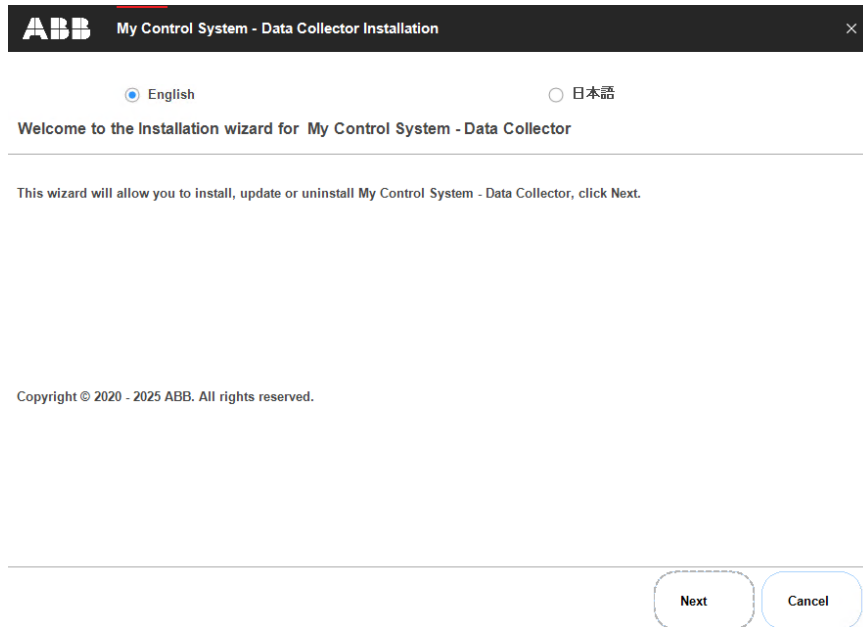


Figure 3.14: Select the language

3. Select **Uninstall** option and click **Next**, as shown in **Figure 3.15**.

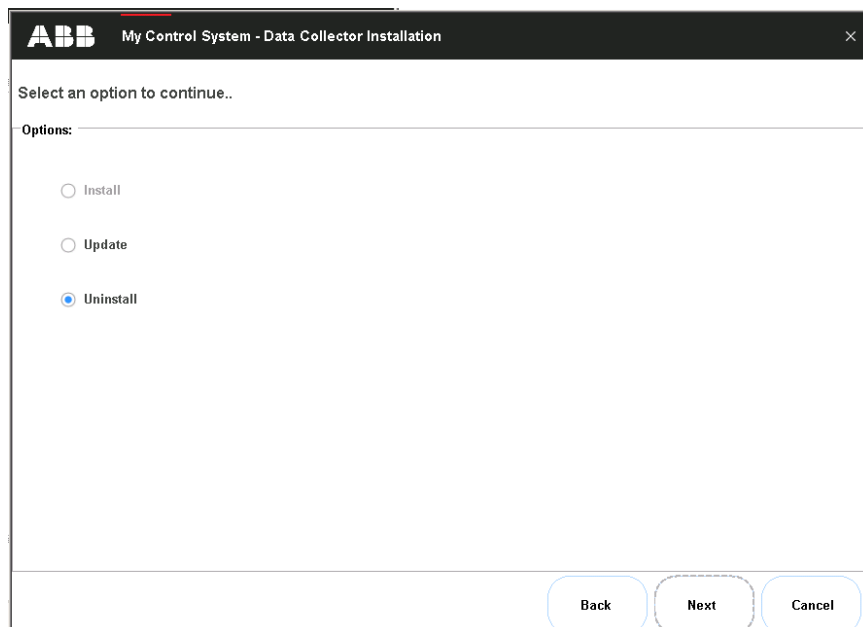
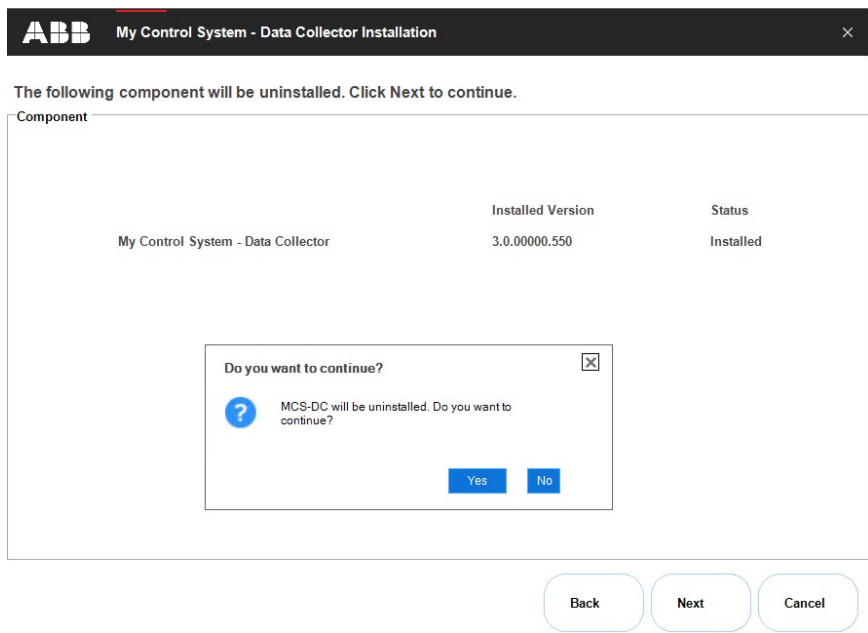


Figure 3.15: Install Shield Wizard

4. A confirmation window appears. Click **Yes** to continue.



5. Uninstallation begins. Click **Finish** to complete the uninstallation, as shown in **Figure 3.16**.

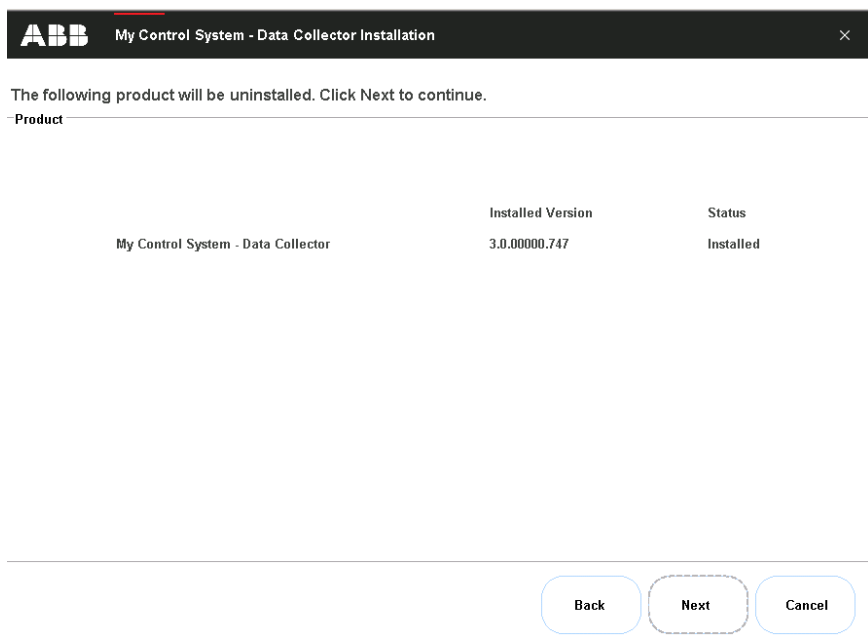


Figure 3.16: Uninstallation completed

3.3.2 Uninstallation via System 800xA system installer

If MCS-DC was installed via System 800xA system installer, it can only be uninstalled via system installer. Follow the procedure below.

1. Select **System nodes** tab in system installer and right click on MCS Data Collector. Select **Manually remove** option as shown in figure.

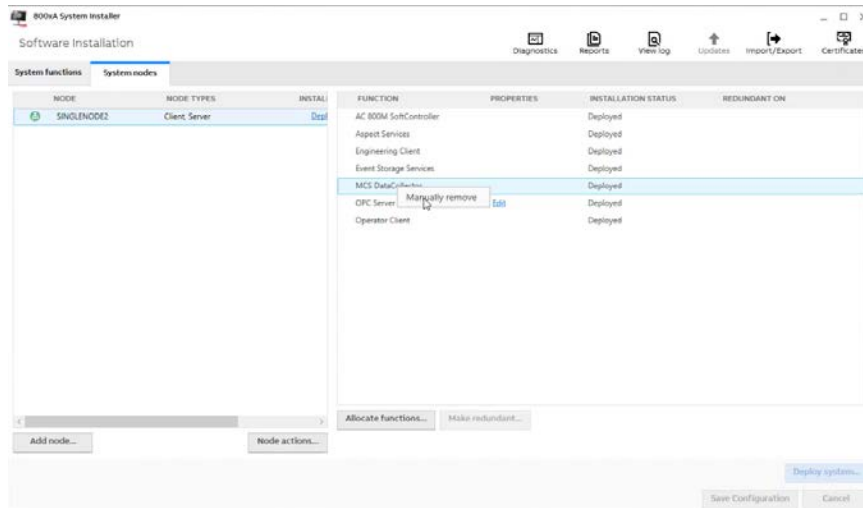


Figure 3.17: Remove from system nodes

2. Click **Continue** in the next two screens and then click **Finish**.

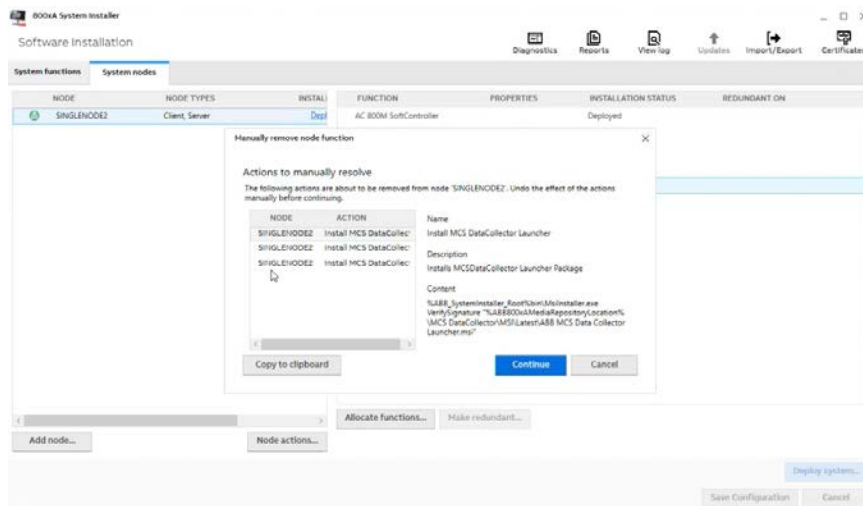


Figure 3.18: Actions to manually resolve

3 Setup and Maintenance

3.3 Uninstalling MCS-DC

3. Repeat the steps above after selecting the tab **System functions**.

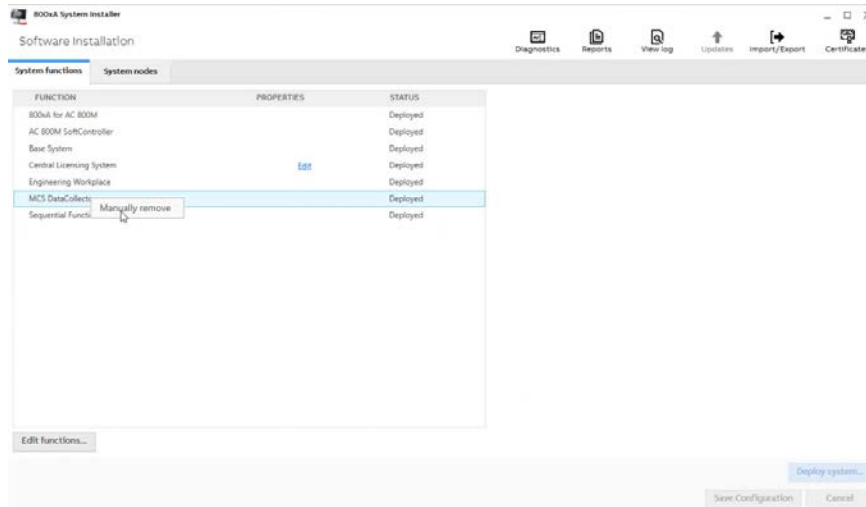


Figure 3.19: Remove from system functions

4. Close the system installer and run **ABB.MCSDataCollector.Installation.exe** from **C:\ProgramData\ABB Control Systems\LMR\MCS DataCollector**. Follow the instructions on the installation wizard to complete the uninstallation.

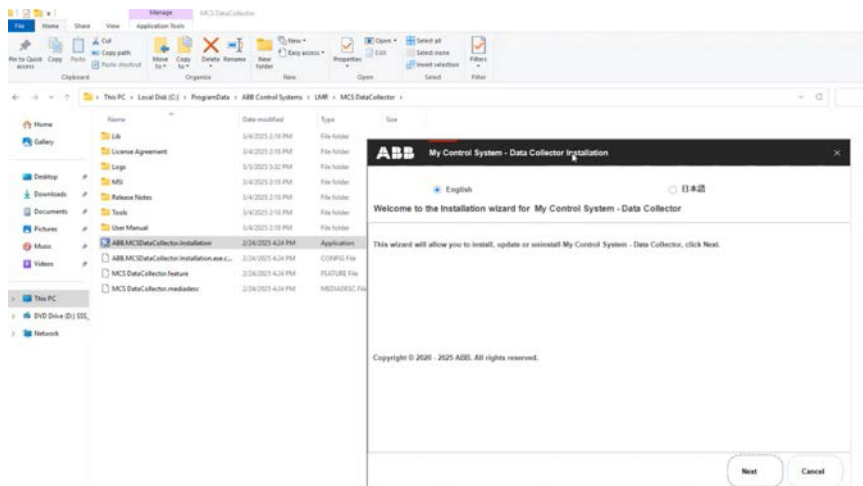


Figure 3.20: Uninstall wizard

4 Data Collection

Upon successful installation, the MCS-DC launcher can be located in *C:\Program Files (x86)\ABB\Service Products\DataCollector*.

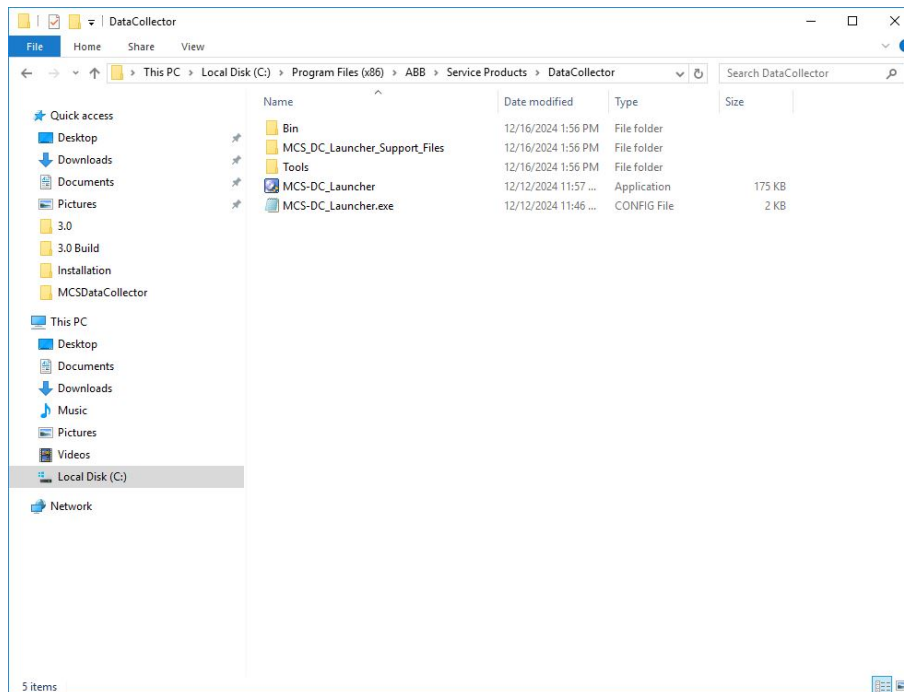


Figure 4.1: MCS-DC Launcher

MCS-DC has two modes of operation

- Basic mode
- Advanced mode

4.1 Basic Mode Data Collection

This mode is intended for users who prefer ease of use and minimal user interaction. In this mode, MCS-DC identifies the HMI and controller systems automatically. User will not have much of the customizable options (like choosing only performance data or lifecycle data, choosing only specific nodes for data collection, etc.). If the system could not be identified automatically, users have option to switch the collection mode from basic to advanced.



Basic mode is not supported for System 800xA in Windows workgroup network. Users are prompted to switch to **Advanced mode** data collection. Besides, for System 800xA in workgroup network, periodic data collection will be enabled by default. However, the instant collection feature allows users to override periodic collection and collect data on demand. Refer to [Section 4.3, Periodic Collection Configuration](#) for further details.

Depending on the HMI/Controller, MCS-DC launch nodes may vary. Refer to the respective sections for more details.

4.1.1 Language and System Selection

Follow the steps below, to start the data collector and select the language and the System.

1. Double-click the **MCS-DC_Launcher.exe**, to launch the tool.



If a Microsoft Defender SmartScreen popup appears when MCS-DC is being launched, click Run and continue. Refer to [Appendix I, The Microsoft Defender SmartScreen](#) for more details.



In the event that the release date of MCS-DC is 180 days older than the launch date, the user will be notified that there is a newer version available in the ABB library. Nevertheless, the user will not be prevented from launching the product and collecting data.

2. MCS-DC tool runs the below checks on the launch node. The green tick marks refer to successful checks, and a red cross mark indicate the failed ones. User must fix the issue and re-launch the MCS-DC tool.
 - .NET Framework version check

If the .NET Framework version is 1.1 or above, then this check is passed and the latest version of MCS-DC will be launched for data collection.

If the .NET Framework version is lower than 1.1, then this check is failed and MCS-DC version 1.9.x will be launched for data collection. Please refer MCS-DC 1.9.x user manual for data collection procedure.
 - Prerequisites check

Below prerequisites are validated. User can proceed for data collection only if these checks are passed.

 - User privileges check, checks if the MCS-DC is launched in the user account with administrator privileges.
 - System drive launch check, MCS-DC tool must be launched only from the local disk drive of the launch node.
 - Required disk space check, free disk space of at least 500 MB must be available on the disk drive from which the MCS-DC is launched.

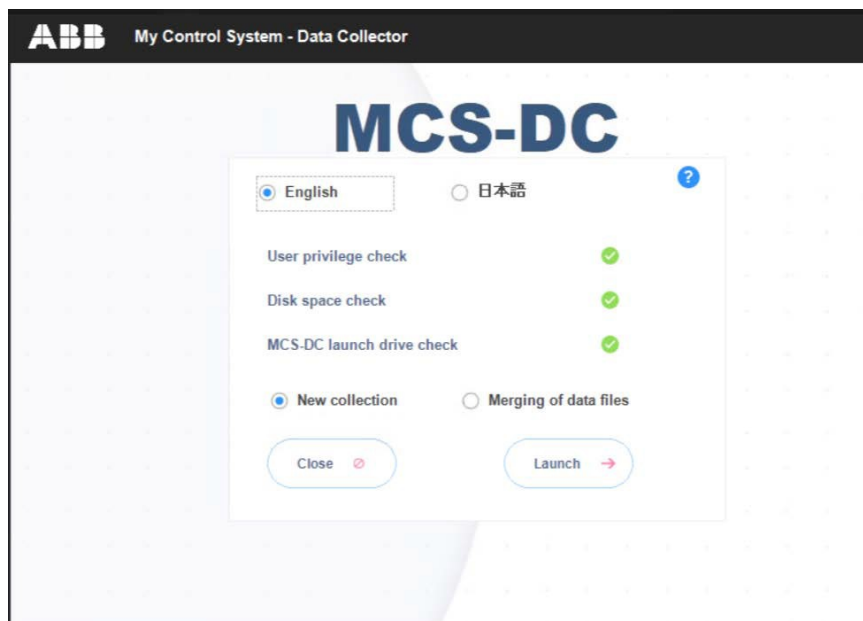


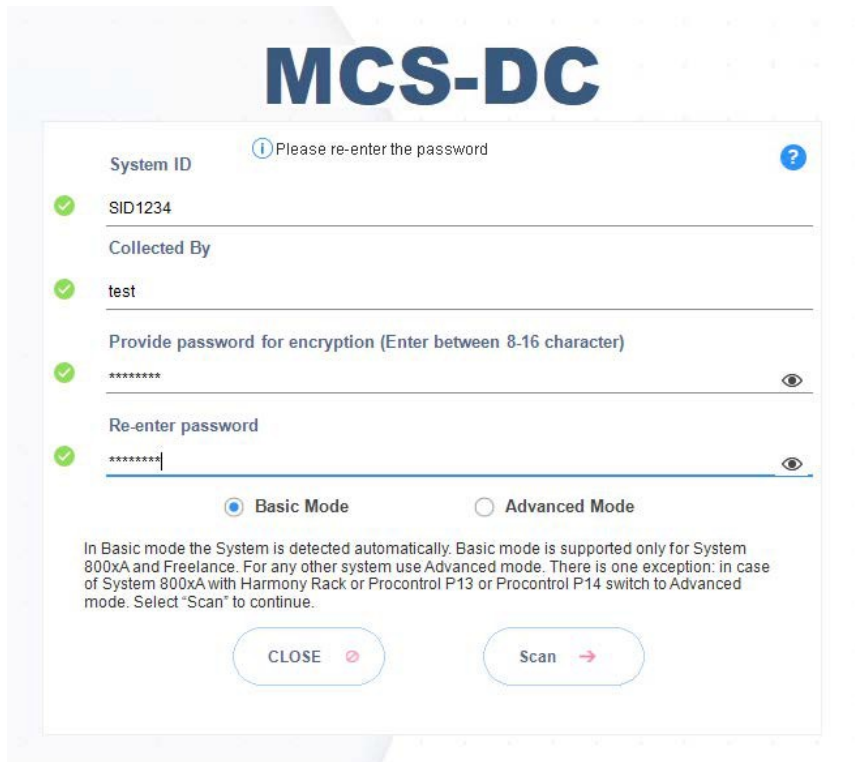
Figure 4.2: .NET Framework version check and Prerequisite check status

3. Starting with version 2.10, MCS-DC supports data collection from Japanese language systems. Click on the Launch button after selecting the preferred language.

4 Data Collection

4.1 Basic Mode Data Collection

4. Provide the System ID, full name of the user (Collected by) and password. Note that special characters are not allowed in the '**Collected by**' field. The password will be used for encrypting collected data and create system data file. Decryption of the collected data is possible only at 3 places, namely, My Control System web, My Control System On-premise and My Control System Portable. To use the system data file at My Control System Portable, the user needs to enter the same password, which is entered here, to decrypt the data. So, remember this password. Once all the required inputs are provided, select Basic Mode (default selection). Upon clicking on the **Scan** button, validation of System ID and Collected by fields are executed. Tick mark appears if validation succeeds and cross marks appear when validation fails against respective fields. Correct the errors and click on the **Scan** button to proceed further.



The screenshot shows the 'MCS-DC' (My Control System Data Collection) interface. It features a form with the following fields and elements:

- System ID:** A text input field containing 'SID1234' with a green checkmark icon on the left and a blue question mark icon on the right. Above the field is a message: 'Please re-enter the password'.
- Collected By:** A text input field containing 'test' with a green checkmark icon on the left.
- Provide password for encryption (Enter between 8-16 character):** A password input field with masked characters '*****' and a green checkmark icon on the left. An eye icon is on the right to toggle visibility.
- Re-enter password:** A password input field with masked characters '*****' and a green checkmark icon on the left. An eye icon is on the right to toggle visibility.
- Mode Selection:** Two radio buttons: 'Basic Mode' (selected) and 'Advanced Mode'.
- Instructions:** A paragraph of text explaining the modes: 'In Basic mode the System is detected automatically. Basic mode is supported only for System 800xA and Freelance. For any other system use Advanced mode. There is one exception: in case of System 800xA with Harmony Rack or Procontrol P13 or Procontrol P14 switch to Advanced mode. Select "Scan" to continue.'
- Buttons:** 'CLOSE' with a red 'X' icon and 'Scan' with a red arrow icon.

Figure 4.3: User Credentials

4 Data Collection

4.1 Basic Mode Data Collection

5. Click Scan button to start the system scan. This results in the identification of the HMI, the controller and the system version etc. A progress bar is shown to indicate the scan status. This operation may take a few minutes to complete, as it depends on the size of the system.

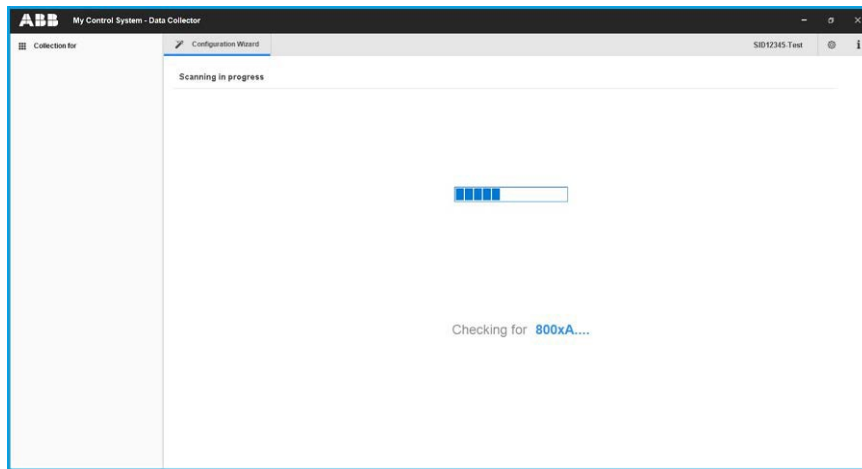


Figure 4.4: System Scan

6. After the scan is successfully completed, details of HMI, controllers and system version are displayed.

4.1.2 Input Configuration

System 800xA

For 800xA HMI data collection, MCS-DC can be launched on any 800xA node. Depending on the connects, below are the launch nodes for various connects.



Basic mode is not supported for 800xA HMI with Harmony Rack controllers and 800xA HMI with Procontrol P13/P14 controllers.

- 800xA HMI with AC 800M controllers:
Any 800xA node
- 800xA HMI with AC 70, 110, 160 controllers:
Any 800xA node
- 800xA HMI with Freelance controllers:
Any 800xA node
- 800xA HMI with AC 410, 450, MP, SG 400 controllers:
Any 800xA node
- 800xA HMI with Melody Rack controllers:
Any 800xA node which is part of Onet network. Additionally, CSE_Config has to be synchronized in all the 800xA nodes
- 800xA HMI with MOD 300 controllers:
Any 800xA node
- 800xA HMI with QCS controllers:
Any 800xA node with QCS connect



The procedure to export system configuration files that are required for data collection can be found in [Appendix D, System configuration export](#).

1. Clicking on the **Continue** button will take to Configuration Wizard where the user needs to provide necessary input parameters required for data collection. The first input screen is IP range input for the nodes that are not part of Node Admin structure of 800xA.

Users can switch the collection mode from basic to advanced, by clicking 'Switch to Advanced mode' button.

2. All HMI and controller nodes will be detected by MCS-DC from Node Admin Structure and their respective IP's will be read automatically. Enter only the range of IP's related to other computers for which MCS-DC needs to collect data and are not part of the Node Admin structure. This is only an optional input. If there are no IT assets, other than HMI and Controller nodes, user can proceed without providing IP range.

Figure 4.5: IP range Input

3. Provide the IP range and click on **Add** button. User can provide multiple ranges too. Larger the range of IP's, more time will be taken by MCS-DC to complete the node scan. Hence, it is better to provide specific range related to required computers. For these nodes, lifecycle and security data can be collected.

Figure 4.6: IP Details

4 Data Collection

4.1 Basic Mode Data Collection

4. If a wrong IP range is added, there is option to remove that. To remove, select the added IP range by clicking on it and then click on the **Remove** button. For these nodes, lifecycle and security data can be collected.

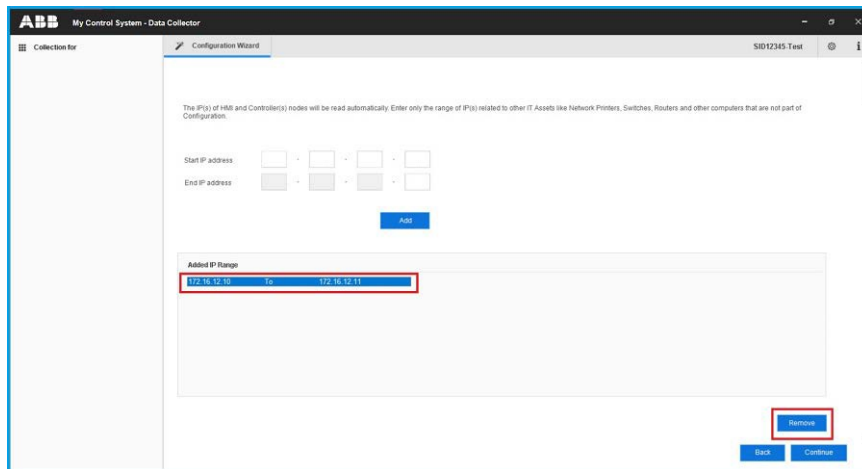


Figure 4.7: IP Range Input

5. Click on the **Continue** button to proceed. There is option to go back to the previous window in each step of the configuration.
6. Next input is User Credentials. As appropriate, provide the Username and Password in the format 'domain name\username' or '.\username', depending on the type of network (domain or Workgroup) used. Alternatively, select a user account from the drop-down list that has the necessary privileges for data collection. The required user privileges are outlined in [Section 2.2, System 800xA](#). Click the Add button.

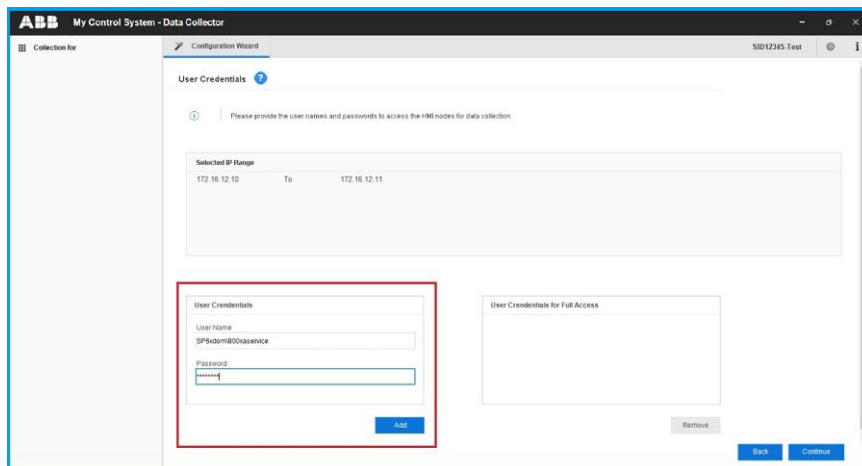


Figure 4.8: User Credentials

4 Data Collection

4.1 Basic Mode Data Collection

7. There is option to remove the added credentials. To remove, select the added credential and click on the **Remove** button.

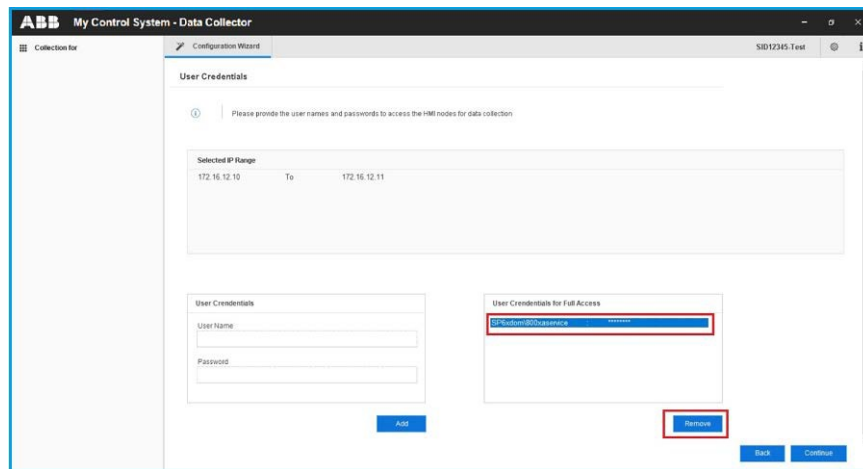


Figure 4.9: User Credentials

8. If the System 800xA is configured with AC 800M no input settings are needed for collecting performance and lifecycle data from AC 800M controllers. Controller crash files are collected from both primary and backup Connectivity Servers; the maximum size of files that are collected can be selected. Click on settings (the gear icon in the top right corner) and select the tab AC 800M. From drop down menu, select the maximum size for the collection file.

Crash file collection is enabled by default with a maximum file size of 15 MB. Other possible choices are 5, 10, or 20 MB maximum. File collection can be disabled by unchecking the provided checkbox.

By default, AC 800M controller data is collected by MCS-DC using AfwOPCDASurrogate service. As this is a licensed service, if the license is not present in the system, an error message will be displayed in all HMI nodes. Alternatively, users may choose ABB.AfwOpcDaServer service instead, by selecting the drop-down menu shown below.

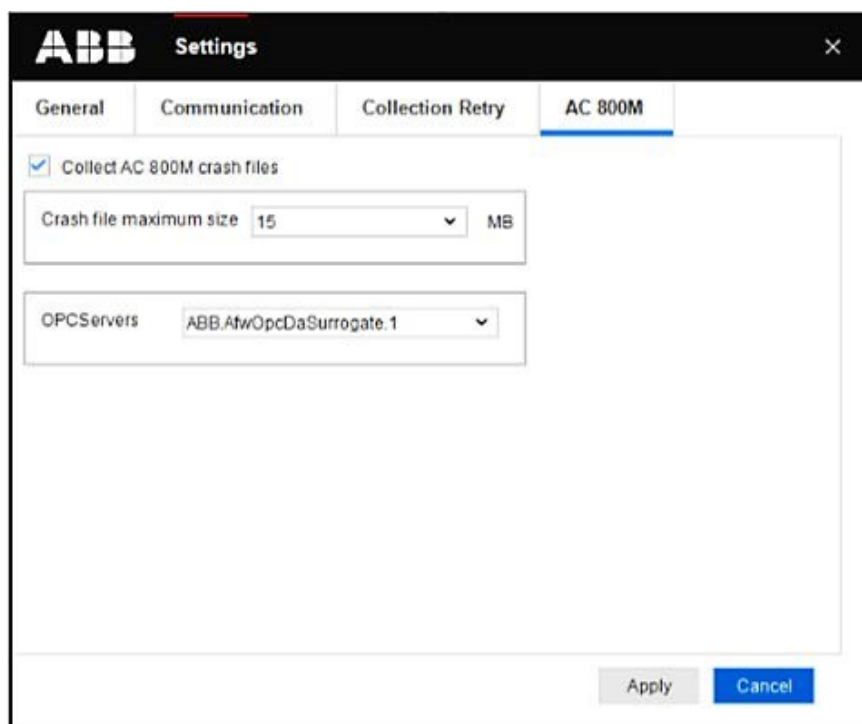


Figure 4.10: Crash File Collection Settings

4 Data Collection

4.1 Basic Mode Data Collection

9. If the System 800xA is configured with AC 70, 110, 160 connect, the below input screen for AC 70, 110, 160 appears. Click the **Browse** button to select the AC 70, 110, 160 project export folders. Once the project export folder is selected, all the available project export (.BAX) files are listed under Available section. The most recent export (.BAX) file is auto selected and is listed under Selected section. There are options to move the export files from Selected section to Available section and vice versa. Move the required export files to Selected section and click Continue to proceed (Refer to [Appendix D, System configuration export](#) for exporting system configuration files.).

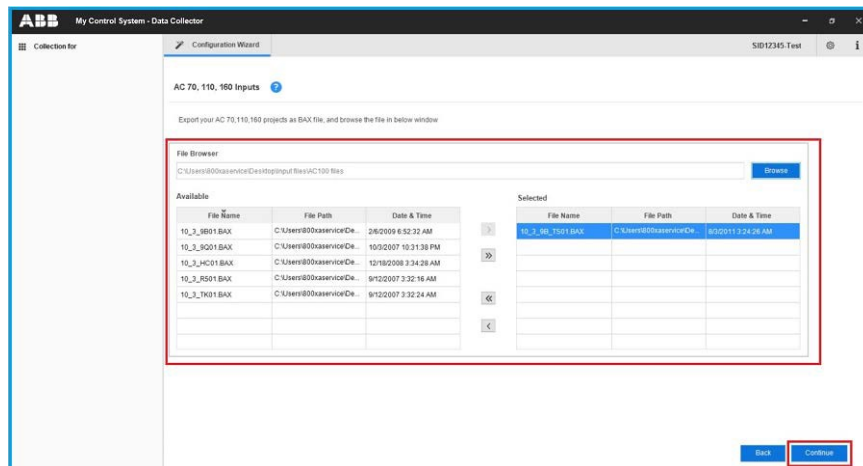


Figure 4.11: AC 70, 110, 160 Inputs

10. If the System 800xA is configured with Freelance connect, the below input screen for Freelance appears. Click on the **Browse** button to select the Freelance project export folder. Once the project export folder is selected, all the available project export (.csv/.csvs) files are listed under Available section. The most recent export (.csv/.csvs) file is auto selected and is listed under Selected section. There are options to move the export files from Selected section to Available section and vice versa. Move the required export files to Selected section. If the selected project export file type is .csvs, project export file decryption key has to be provided in the decryption key field (refer to [Appendix D, System configuration export](#) for exporting system configuration files).

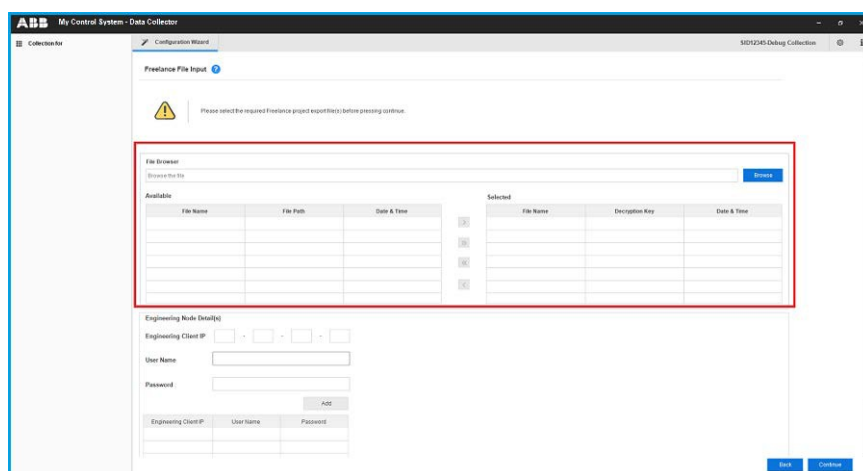


Figure 4.12: Freelance Input

4 Data Collection

4.1 Basic Mode Data Collection

11. Engineering node IP: Scroll down the screen to enter the Engineering client node IP, user credentials and click Add.

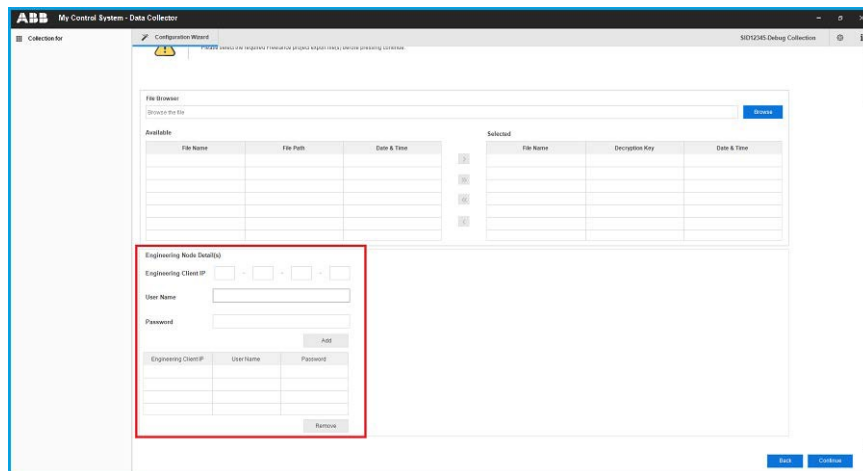


Figure 4.13: Engineering node IP

4 Data Collection

4.1 Basic Mode Data Collection

12. If the System 800xA is configured with Melody Rack connect, the below input screen for Melody Rack appears. Provide the below inputs and click Continue to proceed (refer to [Appendix D, System configuration export](#) export for exporting system configuration files).
 - a. QCS controllers:
Melody Island Devices: Click the **Browse** button to select the Melody Island Devices Export file. Ensure to export the latest melody Island deice file that is synced with the latest hardware structure.
 - b. CSE_Conf File
Click the **Browse** button to select the Current CSE_Conf File
 - c. Asset Export Folder
Click the **Browse** button to select the Asset Export Folder
 - d. Composer Melody node IP Address
Enter the IP Address of S+ Engineering Server, where Composer Melody is installed.
 - e. UserName
Provide the Composer Melody node username
 - f. Password
Provide the Composer Melody node password

The screenshot shows the 'ABB My Control System - Data Collector' window. The 'Configuration Wizard' tab is active, and the 'Melody Rack' section is selected. A red rectangular box highlights the input fields for the Melody Rack configuration. The fields are: 'Melody Island Devices' with a 'Browse' button, 'CSE_Conf File' with a 'Browse' button, 'Asset export folder' with a 'Browse' button, 'Engineering Server' with a numeric IP address field (172.16.4.20), 'UserName' with a text field (Administrator), and 'Password' with a password field. At the bottom right of the window are 'Back' and 'Continue' buttons.

Figure 4.14: Melody Rack

4 Data Collection

4.1 Basic Mode Data Collection

13. If the System 800xA is configured with MOD 300 connect, the below input screen for MOD 300 appears. Click the **Browse** button to select the latest ATF file, taken from AdvaBuild engineering node. Click **Continue** to proceed (refer to [Appendix D, System configuration export](#) export for exporting system configuration files).

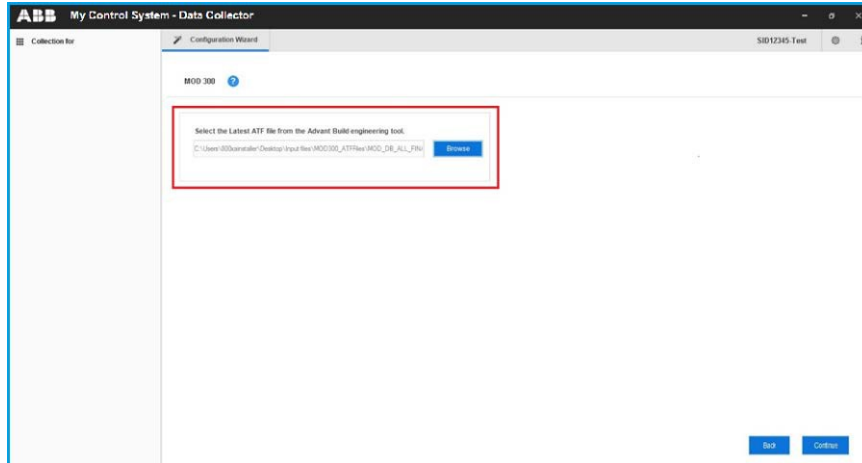


Figure 4.15: MOD 300

14. If the System 800xA is configured with QCS connect, the below input screen for QCS appears. Select the relevant QCS version in the **QCS Version** drop-down list. The correct version should already have been identified, if MCS-DC is running on a computer that has the QCS software installed. Verify the identified QCS version.

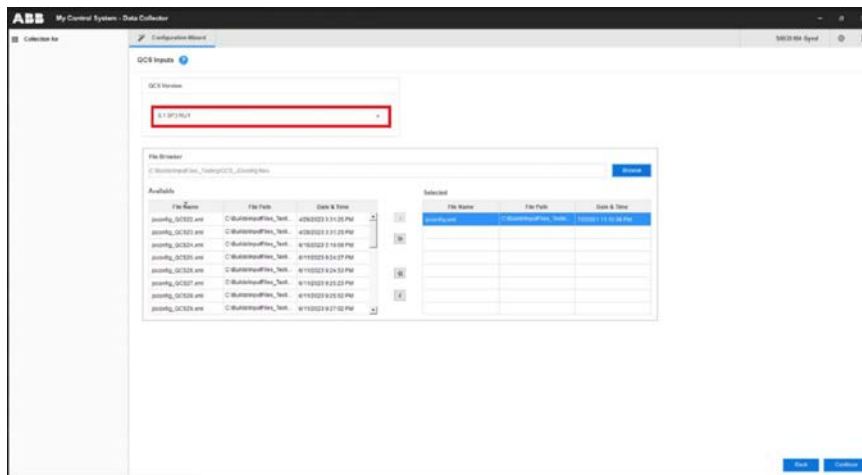


Figure 4.16: Configuration Wizard

4 Data Collection

4.1 Basic Mode Data Collection

15. Click on the Browse button to select the QCS folder where the latest joconfig.xml files are stored. The joconfig.xml files will be available in the project directory of the QCS Connectivity Server, which is usually “C:\Program Files (x86)\ABB Industrial IT\Quality Control Solutions\Engineer IT\JOCONFIG \Projects”. There will be subdirectories for the different builds that have been created on that QCS system. Select the directory with the most recent build that has been deployed to build the system. Once the folder is selected, all the available joconfig.xml files will be listed under Available section. The files can be moved from the Selected section to the Available section and vice versa. Move the required files to the Selected section. Click Continue to proceed.

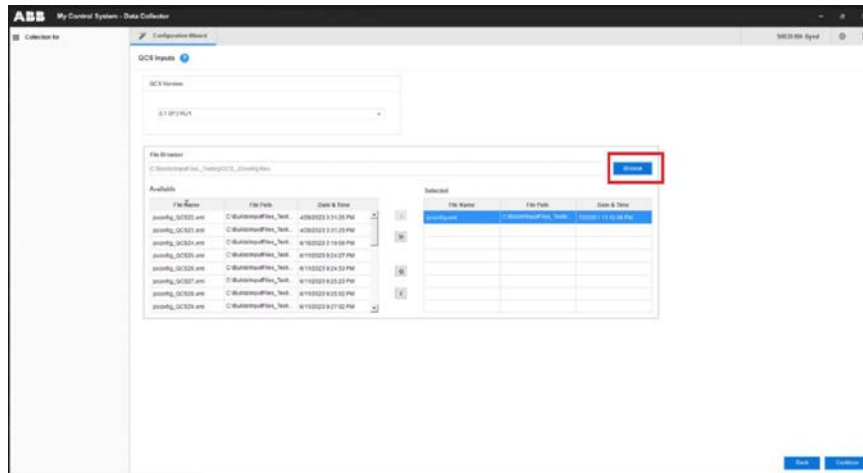


Figure 4.17: Browse option to browse joconfig.xml

16. Once all HMI and connect inputs are provided, it is required to acknowledge that all the prerequisites for data collection, are met. For this, click the tab Prerequisites and confirm each prerequisite by checking the checkbox against them. Please note, this is only an acknowledgment that user has verified all the prerequisites for proceeding with data collection. For more details, refer to [Section 2, Prerequisites](#).

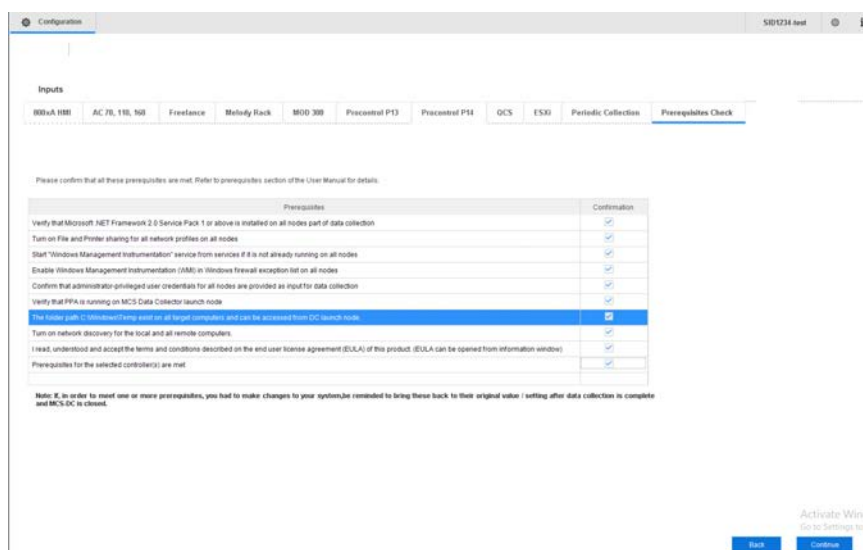


Figure 4.18: Prerequisites acknowledgement

17. Click on the **Continue** button to proceed with the node scan. Refer to [Section 4.1.3, Scan, Agent Deployment and Collection](#).

Freelance

Freelance HMI data collection is supported with Freelance controllers only. Below are the supported data categories.

1. Clicking on the **Continue** button will take to Configuration wizard where the user needs to provide necessary input parameters required for data collection. The first input screen is Freelance File Input.

Users can switch the collection mode from basic to advanced, by clicking 'Switch to Advanced mode' button.

2. Click the **Browse** button to select the Freelance project export folder. Once the project export folder is selected, all the available project export (.csv/.csvs) files are listed under Available section. The most recent export (.csv/.csvs) file is auto selected and is listed under Selected section. There are options to move the export files from Selected section to Available section and vice versa. Move the required export files to Selected section and click on **Continue** to proceed. If the selected project export file type is .csvs, project export file decryption key has to be provided in the decryption key field (refer to [Appendix D, System configuration export](#) for exporting system configuration files).

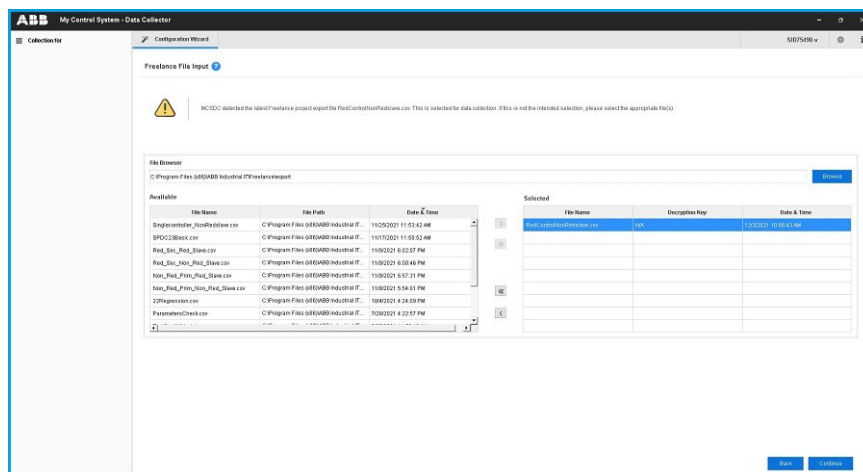


Figure 4.19: IP Range Input

4 Data Collection

4.1 Basic Mode Data Collection

3. All HMI and controller nodes will be detected by MCS-DC from the .csv/.csvs file of the customer's project and their respective IP's will be read automatically. Enter only the range of IP's related to other computers, where MCS-DC needs to collect data. This is only an optional input. If there are no IT assets, other than HMI and Controller nodes, user can proceed without providing IP range.

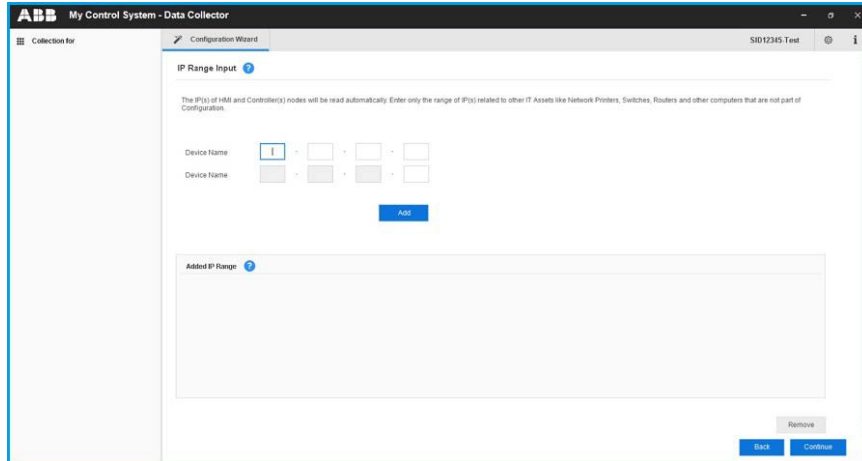


Figure 4.20: IP Range Input

4. Provide the IP range and click on **Add** button. User can provide multiple ranges too. Larger the range of IP's, more time will be taken by MCS-DC to complete the node scan. Hence, it is better to provide specific range related to required computers.

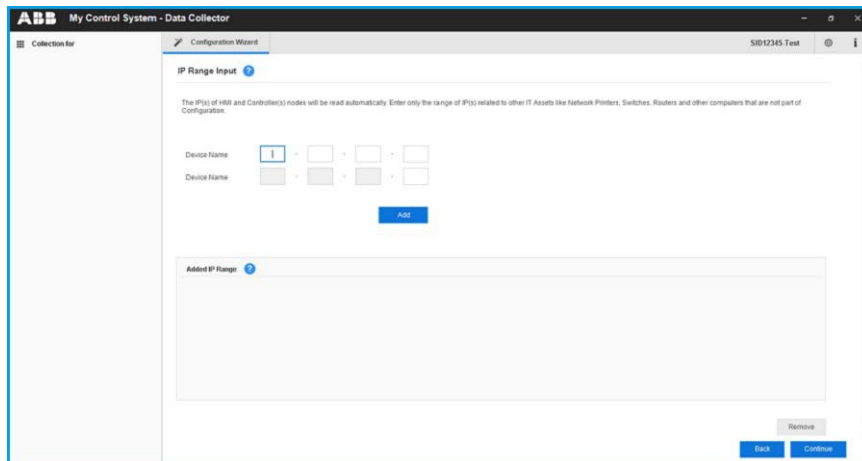


Figure 4.21: IP Range

4 Data Collection

4.1 Basic Mode Data Collection

5. If a wrong IP range is added, there is option to remove that. To remove, select the added IP range by clicking on it and then click on the **Remove** button.

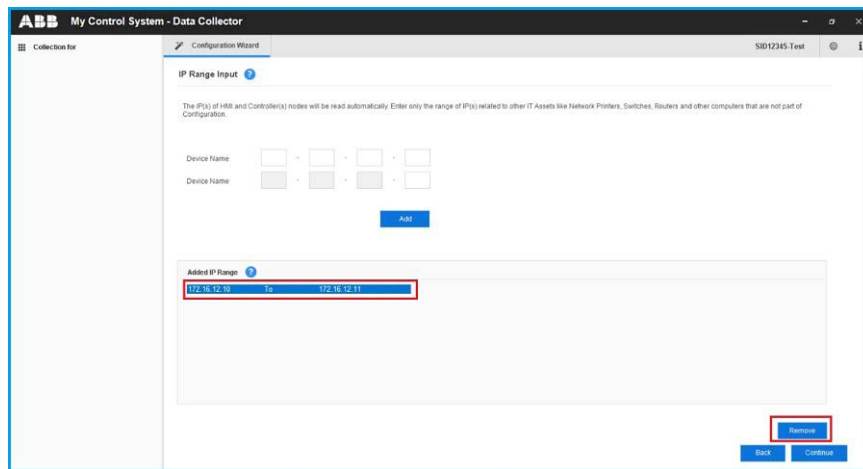


Figure 4.22: Remove IP Option

6. Click on the **Continue** button to proceed. There is an option to go back to the previous window in each step of the configuration.
7. Next input is user credential. Provide username and password in the format 'computer name\username'. Alternatively, select a user account from the drop-down list that has the necessary privileges for data collection. The required user privileges are outlined in [Section 2.3, Freelance System](#). Click the Add button.

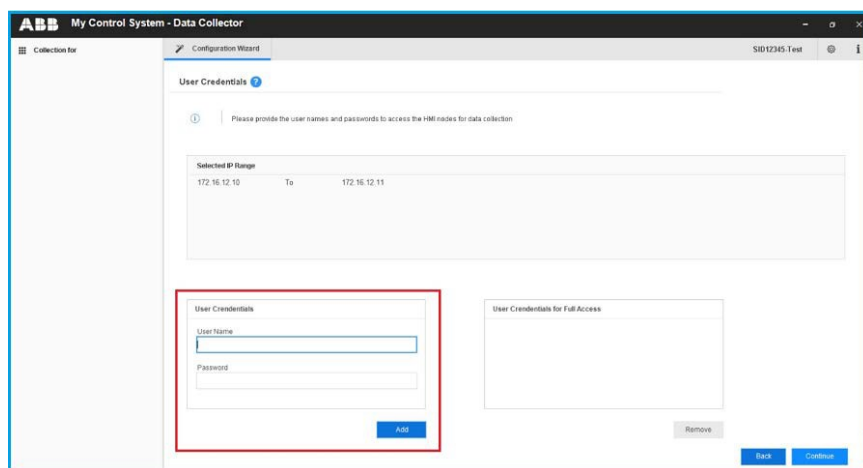


Figure 4.23: Freelance Folder

4 Data Collection

4.1 Basic Mode Data Collection

- There is option to remove the added credentials. To remove, select the added credential and click on the **Remove** button.

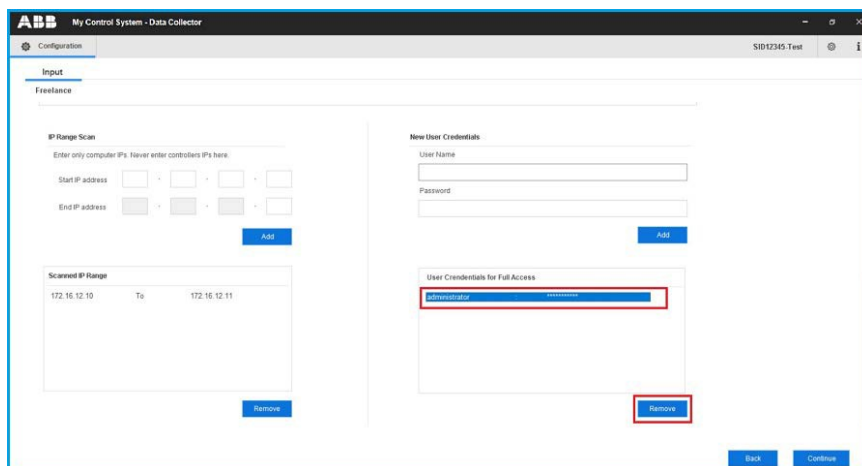


Figure 4.24: Remove Credentials

- Once all HMI and connect inputs are provided, it is required to acknowledge that all the prerequisites for data collection, are met. For this, click the tab Prerequisites and confirm each prerequisite by checking the checkbox against them. Please note, this is only an acknowledgment that user has verified all the prerequisites for proceeding with data collection. For more details, refer to [Section 2, Prerequisites](#).

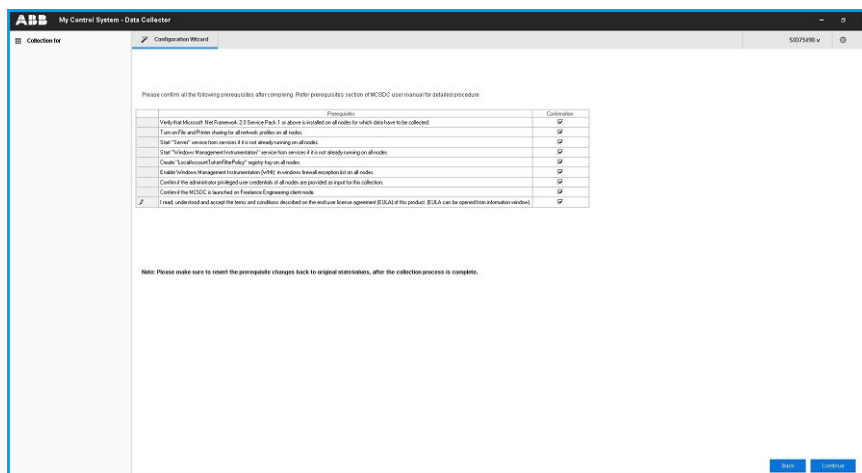


Figure 4.25: Configuration wizard

- Click on the **Continue** button to proceed with the node scan. Refer to [Section 4.1.3, Scan, Agent Deployment and Collection](#).

4.1.3 Scan, Agent Deployment and Collection

The scanning, agent deployment, and collection are described in this section.

- 1. Progress bar is shown to indicate the scanning progress.

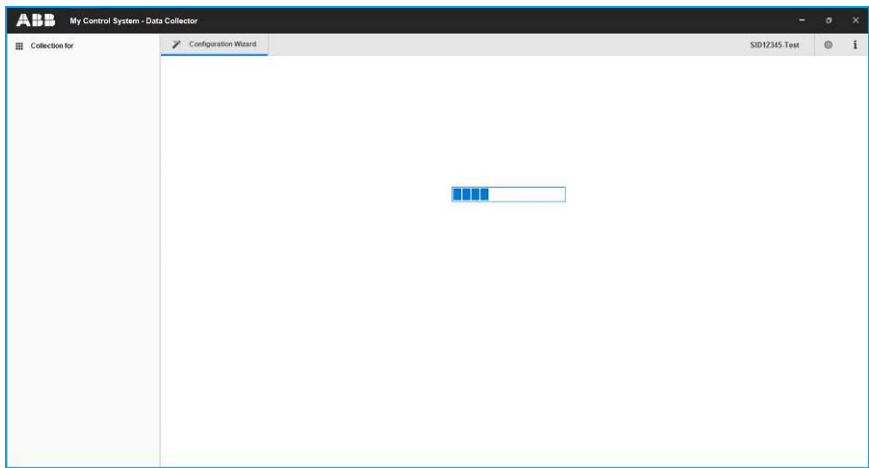


Figure 4.26: Progress

- 2. Once the scanning is complete, all the available HMI and controller nodes are listed. If the HMI nodes are fully accessible, it is shown as Yes in Full Access field. If the nodes are not fully accessible, it is shown as No in Full Access field. This may be due to issues such as invalid user credentials, IP not reachable, network issues, etc. For not accessible nodes, possible reasons for non-accessibility will be provided in the remarks field. User can fix the issue and perform a re-scan. To do a re-scan, click on the **Back** button and repeat the scan. There is an option to add new credentials by clicking on the **Add Credentials** button. When a new credential is added, failed nodes are re-scanned. To proceed with data collection, click on the **Continue** button.

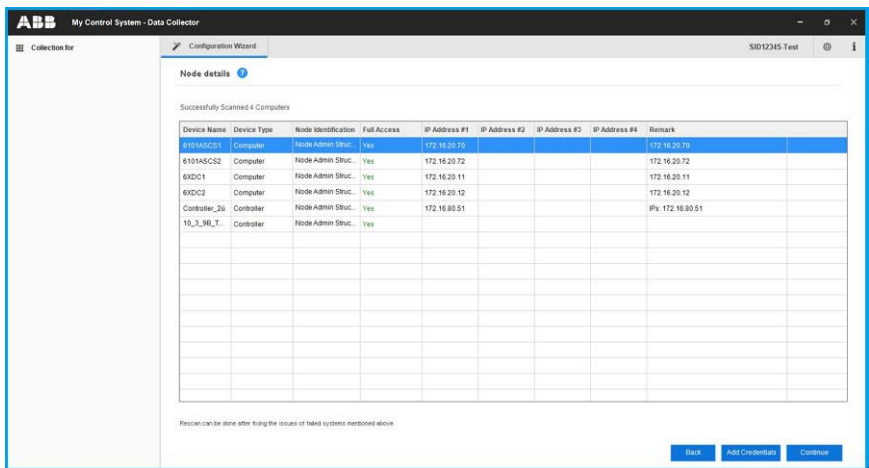


Figure 4.27: Node Details

4 Data Collection

4.1 Basic Mode Data Collection

- Collection screen appears, and data collection is started. Data collection progress is shown in the progress bar. During the data collection if the user wants to cancel the data collection process, click on the **Cancel** button.

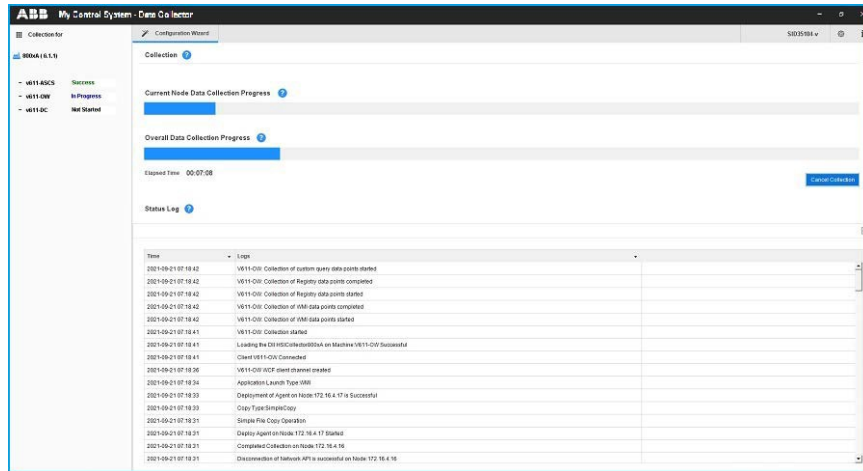


Figure 4.28: Data Collection

- Node wise progress update is shown on the left pane. Below are the available states based on the node status color code:

Grey: Indicates the data that is yet to be collected in the node.

Blue: Indicates that the data is currently getting collected in the node.

Green: Indicates the data is successfully collected in the node.

Red: Indicates the data collection is failed in the node.

- Once the data collection is completed, the collection file is created and stored under output folder (inside the MCS-DC folder). This file can be viewed by clicking on the **Click here for collection file** button.

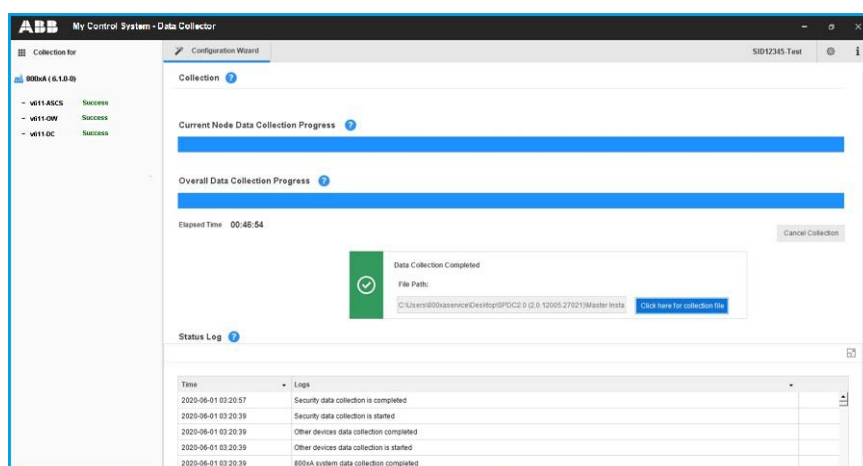


Figure 4.29: View Collection

6. When the user clicks the **Click here for collection file** button, the collection file folder opens.

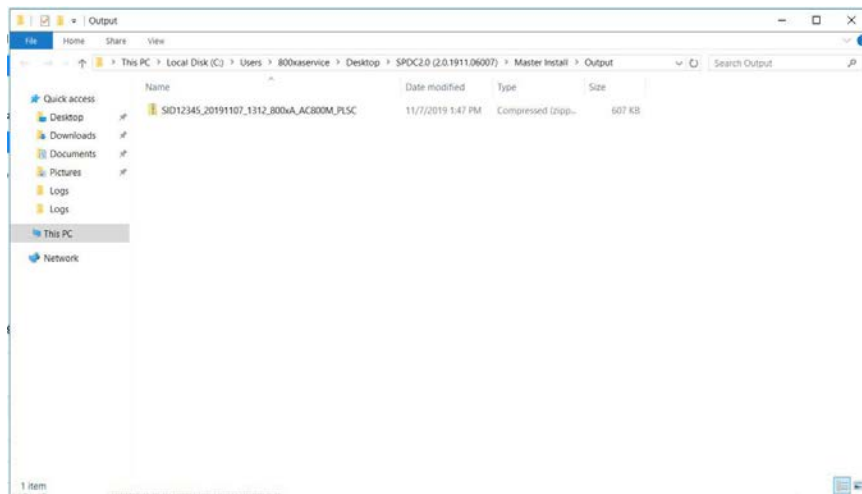


Figure 4.30: Collection Folder

4.2 Advanced Mode Data Collection

This mode is intended for expert users who prefer complete control on the data collection process with respect to selecting the systems, nodes, data category (like performance or Lifecycle), etc. In this mode, user will have opportunity to fix the issues, reported by MCS-DC during node scanning and data collection and then will be able to re-scan or re-collect the failed nodes. Detailed logs and progress updates will be provided by MCS-DC during scanning and data collection.

Depending on the HMI/Controller, MCS-DC launch nodes may vary. Refer to the respective section for more details.

Following are the HMI systems and the data categories supported by MCS-DC.

Table 4.1: HMI and data categories

HMI Systems	Performance	Lifecycle	Software	Security
System 800xA	✓	✓	✓	✓
Freelance	✓	✓		✓
S+ Operations	✓	✓		✓
Non-ABB Systems				✓

Following are the controllers and the data categories supported by MCS-DC.

Table 4.2: Controllers and data categories

Controllers	Performance	Lifecycle
AC 800M	✓	✓
AC 800M PEC		✓
AC 70, 110, 160		✓
Freelance	✓	✓

Table 4.2: Controllers and data categories
(Continued)

Controllers	Performance	Lifecycle
AC410, 450, MP and SG400	✓	✓
Melody	✓	✓
Harmony	✓	✓
MOD300		✓
Procontrol		✓
QCS		✓

Following are the HMI and controller combinations supported by MCS-DC.

Table 4.3: HMI and controller combinations

	System 800xA	Freelance	S+ Operations	Non-ABB Systems
AC 800M	✓		✓	
AC 800M PEC	✓			
AC 70, 110, 160	✓			
Freelance	✓	✓		
AC410, 450, MP and SG400	✓			
Melody	✓		✓	
Harmony	✓ ⁽¹⁾		✓	
MOD300	✓			
Procontrol	✓		✓	
QCS	✓			

(1). If Harmony engineering node is not part of System 800xA node admin structure, HMI and controller data must be collected separately and to be merged. Refer to Section 4.1, Post Collection Procedure for more details.

Detailed instructions for configuring and collecting data in advanced mode is provided in the following sections.

4.2.1 Language and System Selection

1. Double-click the **MCS-DC_Launcher.exe**, to launch the tool.



If a Microsoft Defender Smart Screen popup appears when MCS-DC is being launched, click Run and continue. Refer to [Appendix I, The Microsoft Defender SmartScreen](#) for more details.



In the event that the release date of MCS-DC is 180 days older than the launch date, the user will be notified that there is a newer version available in the ABB library. Nevertheless, the user will not be prevented from launching the product and collecting data.

2. MCS-DC tool runs the below checks on the launch node. The green tick marks refer to successful checks, and a red cross mark indicate the failed ones. User must fix the issue and re-launch the MCS-DC tool.

- .NET Framework version check:

If the .NET Framework version is 1.1 or above, then this check is passed and the latest version of MCS-DC will be launched for data collection.

If the .NET Framework version is lower than 1.1, then this check is failed and MCS-DC version 1.9.x will be launched for data collection. Please refer MCS-DC 1.9.x user manual for data collection procedure.

- Prerequisites check:

Below prerequisites are validated. User can proceed for data collection only if these checks are passed.

- User privileges check, checks if the MCS-DC is launched in the user account with administrator privileges.
- System drive launch check, MCS-DC tool must be launched only from the local disk drive of the launch node.
- Required disk space check, free disk space of at least 500 MB must be available on the disk drive from which the MCS-DC is launched.

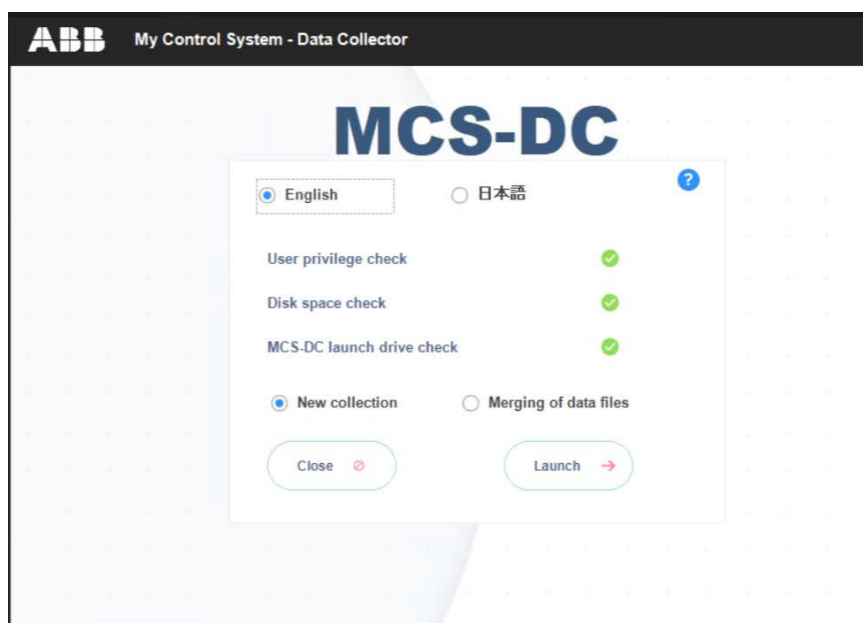
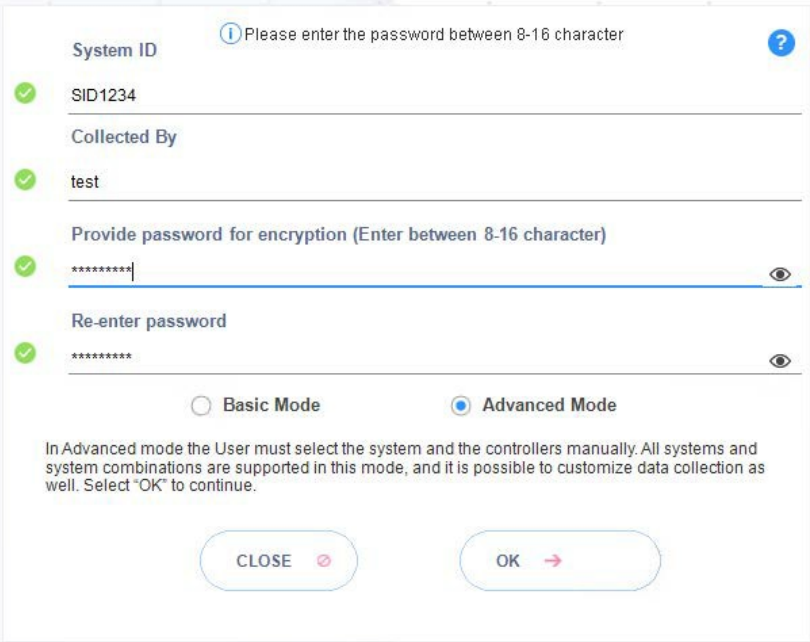


Figure 4.31: .NET Framework version check and Prerequisite check status

4 Data Collection

4.2 Advanced Mode Data Collection

3. Starting with version 2.10, MCS-DC supports data collection from Japanese language systems. Click on the Launch button after selecting the preferred language.
4. Provide the System ID, full name (Collected by) of the user and password. Note that special characters are not allowed in the '**Collected by**' field. The password will be used for encrypting collected data and create system data file. Decryption of the collected data is possible only at 3 places, namely, My Control System web, My Control System On-premise and My Control System Portable. To use the system data file at My Control System Portable, the user needs to enter the same password, which is entered here, to decrypt the data. So, remember this password. Once all the required inputs are provided, select Advanced Mode. Upon clicking on the **OK** button, validation of System ID and Collected by fields are executed. Tick mark appears if validation succeeds and cross marks appear when validation fails against respective fields. Correct the errors and click on the **OK** button to proceed further.



The image shows a screenshot of the MCS-DC application interface. At the top, the text 'MCS-DC' is displayed in a large, bold, blue font. Below this, there is a form titled 'User Credentials'. The form contains several input fields, each with a green checkmark icon to its left, indicating successful validation. The fields are: 'System ID' with the value 'SID1234', 'Collected By' with the value 'test', 'Provide password for encryption (Enter between 8-16 character)' with a masked password '*****', and 'Re-enter password' with a masked password '*****'. Above the 'System ID' field, there is a blue information icon and a message: 'Please enter the password between 8-16 character'. Below the password fields, there are two radio buttons: 'Basic Mode' and 'Advanced Mode'. The 'Advanced Mode' radio button is selected. Below the radio buttons, there is a paragraph of text: 'In Advanced mode the User must select the system and the controllers manually. All systems and system combinations are supported in this mode, and it is possible to customize data collection as well. Select "OK" to continue.' At the bottom of the form, there are two buttons: 'CLOSE' with a red 'X' icon and 'OK' with a red arrow icon.

Figure 4.32: User Credentials

4 Data Collection

4.2 Advanced Mode Data Collection

5. Configuration screen appears. User needs to select applicable HMI/controllers and data category (like Performance, Lifecycle, etc.) on this screen. Supported HMIs are listed on the left half of the screen. When an HMI selection changes, the related applicable controllers appear on the right half of the screen. Default selection of HMI is 800xA. To change the selection, click on the name of the HMI. Selected HMI is highlighted in Blue.

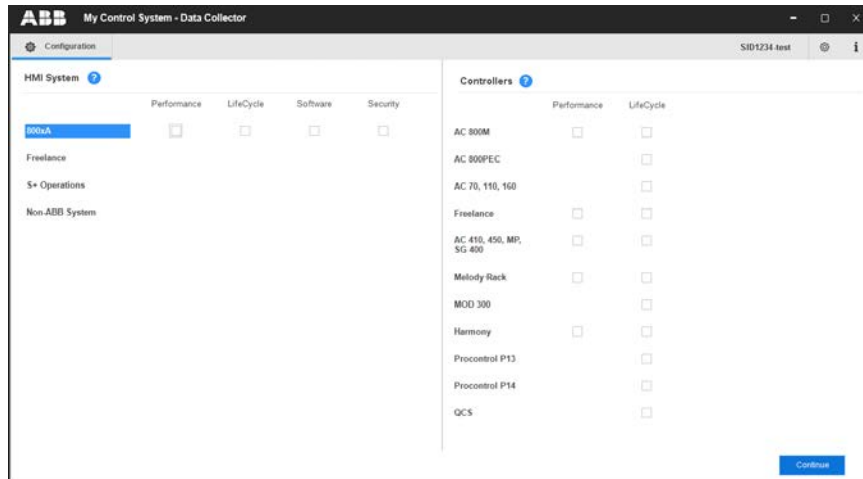


Figure 4.33: HMI and Controller Selection

4.2.2 System 800xA

Depending on the HMI/Controller, MCS-DC launch nodes may vary. For 800xA HMI data collection, the MCS-DC tool can be launched on any 800xA node. Configure the HMI data collection as follows, and then refer to [Section 4.2.5, AC 800M](#) till [Section 4.2.11, Harmony](#) for the connected controller data collection configuration.



If Harmony engineering node is not part of System 800xA node admin structure, HMI and controller data must be collected separately and to be merged. Refer to Section 4.1, Post Collection Procedure for more details.

4 Data Collection

4.2 Advanced Mode Data Collection

1. In the configuration screen select System 800xA, connected controllers and the data category (like Performance, Lifecycle, etc.). Click **Continue** button to proceed.



Select Security option only when it is needed as it will take significantly longer time for data collection.

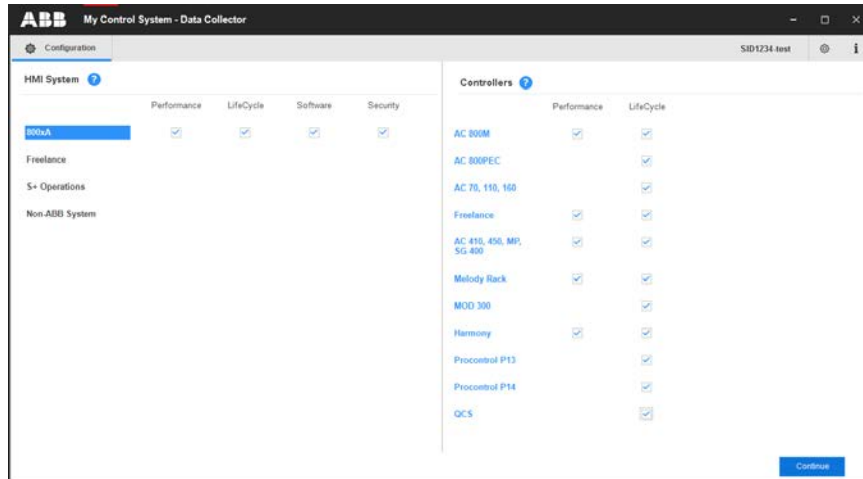


Figure 4.34: HMI and Controller Selection



If System 800xA is configured in Windows workgroup network, periodic data collection will be enabled by default. However, the instant collection feature, allows users to override periodic collection and collect data on demand. Refer to [Section 4.3, Periodic Collection Configuration](#) for further configuration.

4 Data Collection

4.2 Advanced Mode Data Collection

2. Input configuration screen appears. Required inputs may vary based on the HMI, controller and data categories, selected in the previous step. 800xA nodes that are part of Node Admin Structure of System 800xA will be automatically detected and collected by MCS- DC. If there are any non-800xA computers that are connected to System 800xA (for example Melody engineering node), user shall enter the IP range of these computers in the IP Range Scan input. This is an optional input. If no IP range is entered, then MCS-DC will collect only 800xA HMI nodes.

Figure 4.35: 800xA HMI Inputs

Click **Add** button to add the non-800xA nodes entered the IP Range Scan field. Provide the Username and Password of an Administrator user that can access to all the nodes part of data collection. For nodes in Domain network, the username must be provided in the format of “domain name \ username”.

3. Parallel data collection of client computers: Normally, data is collected serially one computer node at a time in order to reduce the network load. It is, however, possible to collect data simultaneously from multiple client computers to save time. This may, however, result in an increase in the total load on the system, which may impair its performance. Due to this, parallel collection is not recommended during critical plant operations. To execute parallel collection, enable the checkbox "Enable parallel collection of client nodes". Note that this is an optional setting.

Parallel data collection is not applicable to server nodes. When the checkbox is enabled, server nodes will be collected sequentially, followed by client nodes in parallel. At most 5 client nodes data will be collected simultaneously.



Parallel collection for 800xA clients will not work if the installed Operating System is Server Operating System.

4 Data Collection

4.2 Advanced Mode Data Collection

- There are several reachability checks are performed during scan. They include but limited to, Ping, Network file copy, WCF communication check, etc. Normally these checks should take only a couple of minutes. However, for slower computers or computers with some performance issues, these may take more time. In some cases, reachability checks may hang if there is no response from OS API calls of the remote computer. So, this time out configuration will help data collector, not to wait for completing the reachability checks, indefinitely. Choose the value wisely as per the system performance levels. For slower systems increase the timeout value. If you are not sure, the default value of 3 minutes should work for most systems.

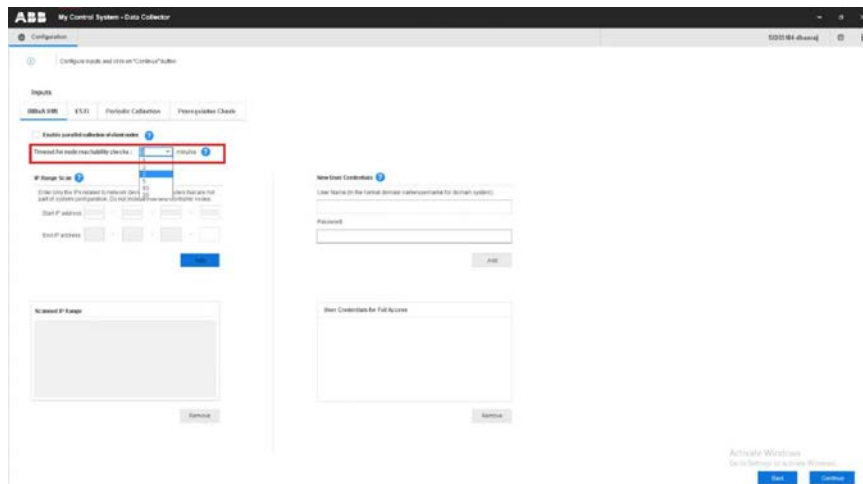


Figure 4.36: Timeout for node reachability check

- Proceed to section 4.2.2.2 for controller data collection configuration.
- After configuring the controller data collection parameters, select the Prerequisites tab and confirm all the listed prerequisites. Please note that this is just a manual acknowledgment that all the prerequisites as listed in Section 2, Prerequisites of this user manual have been met. It is up to the user to have implemented these in all the computers as part of data collection.

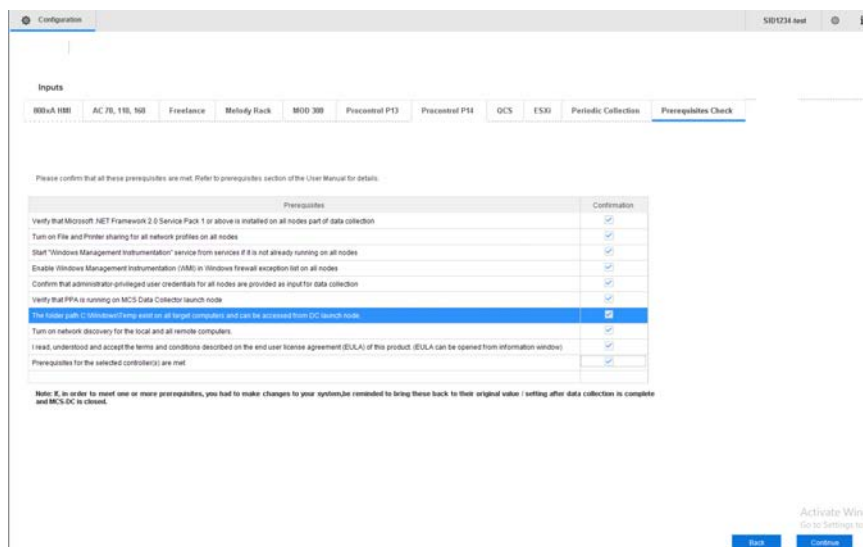


Figure 4.37: Prerequisites Check

7. Click the **Continue** button to proceed to collection screen.

4.2.3 Freelance

For Freelance HMI and controller data collection, the MCS-DC tool shall be installed and launched on Freelance engineering node. Configure the HMI data collection as follows, and then refer to [Section 4.2.7, Freelance](#) for Freelance controller data collection configuration.

1. In the configuration screen select **Freelance**, connected controllers and the data category (like Performance, Lifecycle, etc.). Click **Continue** button to proceed.

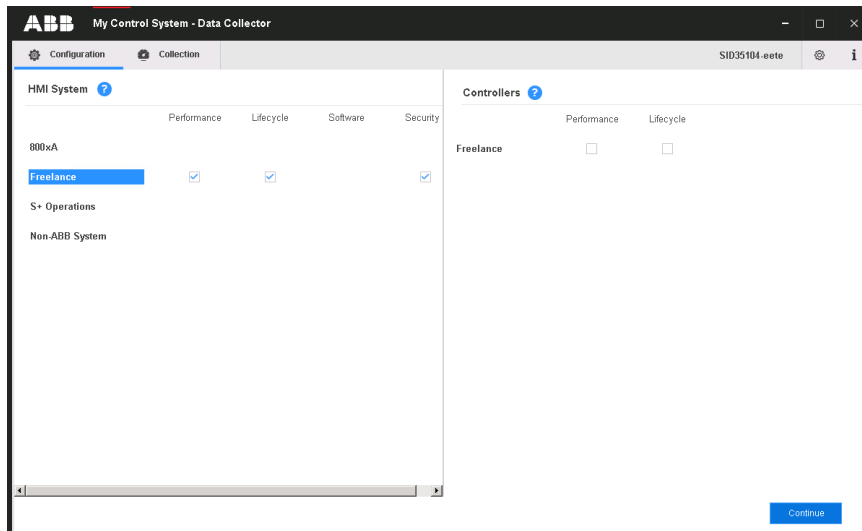


Figure 4.38: Freelance HMI data collection configuration

2. Click on the Browse button to select the Freelance project export folder. Once the project export folder is selected, all the available project export (.csv/.csvs) files are listed under Available section. The most recent export (.csv/.csvs) file is auto selected and is listed under Selected section. There are options to move the export files from Selected section to Available section and vice versa. Move the required export files to Selected section. If the selected project export file type is .csvs, project export file decryption key has to be provided in the decryption key field (refer to Appendix D, System configuration export for exporting system configuration files).

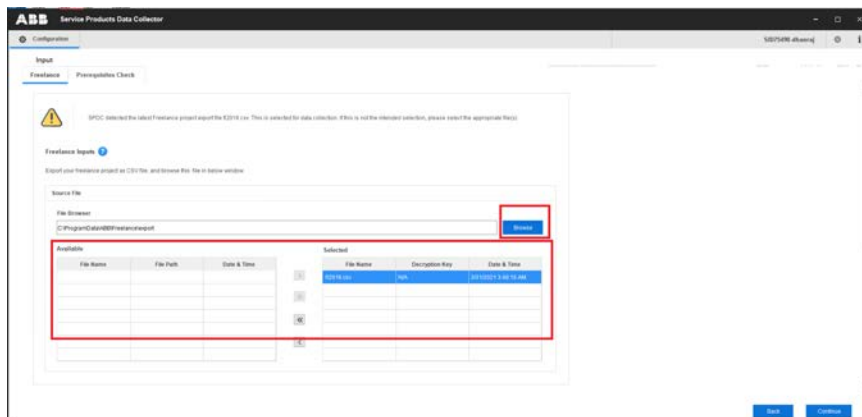


Figure 4.39: Project folder

4 Data Collection

4.2 Advanced Mode Data Collection

3. IP Range: Freelance nodes that are part of the .csv/.csvs file from the project are detected automatically by the Data Collector, so these must not be entered. However, if there are any computers that are connected to the Freelance system that you want to be part of data collection, this is where their IP addresses must be entered, so this is an optional input. If nothing is entered, Data Collector will collect only Freelance nodes.

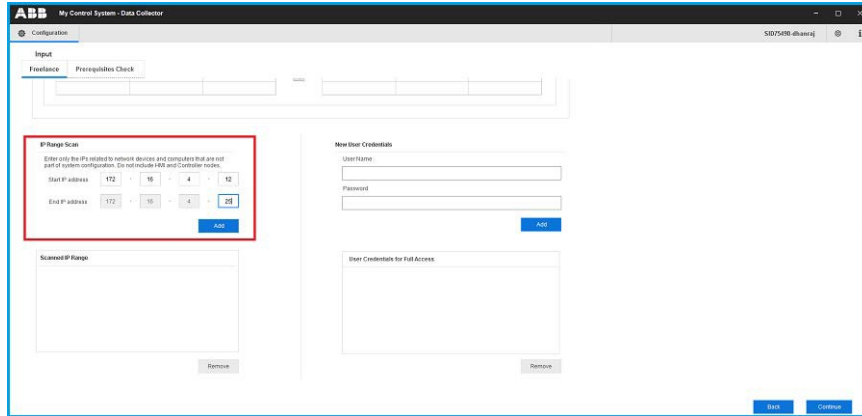


Figure 4.40: HMI nodes

Enter the IP range and select the Add button; it is possible to enter multiple IP ranges, if needed. The greater the range, the more time it will take to complete the node scan, so be careful here and enter only the ranges that are strictly necessary. If an incorrect range is added, it can be removed using Remove button.

4. Next input is user credentials. Provide username and password of administrative user to access all the HMI nodes for data collection. Click on the Add button. Please note, for nodes in domain network, username should be provided in the format of "PC Name\User". User Credentials must have administrator privileges in order to be able to access to all the nodes part of the Freelance system. Use Remove button to remove incorrect credentials.

4 Data Collection

4.2 Advanced Mode Data Collection

5. All prerequisites for data collection must be confirmed before proceeding to the collection screen. To do this, select the Prerequisites tab and confirm each of these individually. Please note that this is just a manual acknowledgment that all the prerequisites as listed in Section 2, Prerequisites of this user manual have been met. It is up to the user to have implemented these in all the computers as part of data collection.

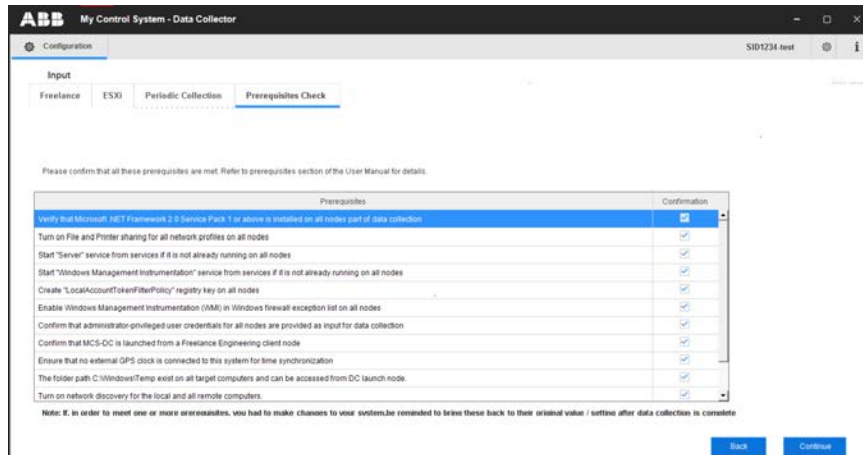


Figure 4.41: Prerequisites

Click on the Continue button to proceed to collection screen.

4.2.4 S+ Operations

Depending on the HMI/Controller, MCS-DC launch nodes may vary. For S+ Operations HMI data collection, the MCS-DC tool can be launched on any S+ Operations node, or on any engineering/client nodes which is connected in the same network as S+ Operations nodes. Refer to [Section 4.2.5, AC 800M](#), [Section 4.2.11, Harmony](#) and [Section 4.2.9, Melody Rack](#) for the connected controller data collection configuration and to determine the launch node. Supported controllers are Harmony, Melody and AC 800M.

1. Under S+ Operations HMI tab, IP range scan input: Enter IP range of all the nodes for which data collection has to be done. Data collection will be done only for the nodes for which the IP address is entered here.

The screenshot shows the 'My Control System - Data Collector' application window. The 'Configuration' tab is active, and the 'S+ Operations HMI' sub-tab is selected. The 'IP Range Scan' section is visible, containing a message: 'Enter only computer IPs. Never enter controllers IPs here.' Below this, there are input fields for 'Start IP address' and 'End IP address', each with a dropdown for the octet and a '+' button. An 'Add' button is positioned below these fields. To the right, the 'New User Credentials' section is visible, with fields for 'User Name' (containing 'S110PMSPOUSER1') and 'Password' (containing 'password'). An 'Add' button is also present here. At the bottom right, there are 'Back' and 'Continue' buttons.

Figure 4.42: IP Range Scan

2. Provide the IP range and click on **Add** button. User can provide multiple ranges. If a wrong IP range is added, use **Remove** button to remove it.

This screenshot is identical to Figure 4.42, showing the 'IP Range Scan' section of the 'My Control System - Data Collector' application. It highlights the 'Add' button located below the 'Start IP address' and 'End IP address' input fields, which is used to add the specified IP range to the 'Scanned IP Range' list.

Figure 4.43: ADD IP Range

3. Proceed to [Section 4.2.5, AC 800M](#) or [Section 4.2.11, Harmony](#) or [Section 4.2.9, Melody Rack](#) depending on the connected controller for the controller data collection configuration.

4 Data Collection

4.2 Advanced Mode Data Collection

- After configuring the controller data collection parameters, select the Prerequisites tab and confirm all the listed prerequisites. Please note that this is just a manual acknowledgment that all the prerequisites as listed in Section 2, Prerequisites of this user manual have been met. It is up to the user to have implemented these in all the computers as part of data collection.

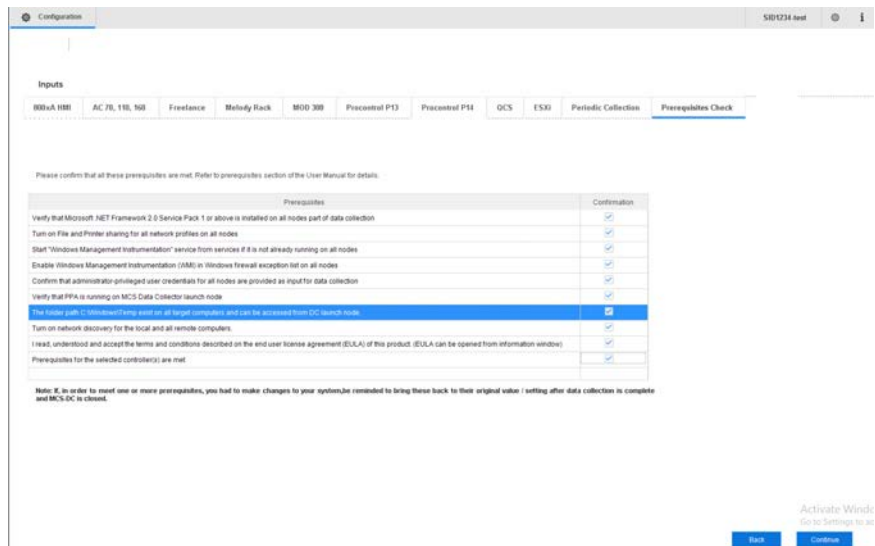


Figure 4.44: Prerequisite Check

- Click the **Continue** button to proceed to collection screen.

4.2.5 AC 800M



By default, AC 800M controller data is collected by MCS-DC using AfwOPCDASurrogate service. As this is a licensed service, if the license is not present in the system, an error message will be displayed in all HMI nodes. Alternatively, users may choose ABB.AfwOpcDaServer service instead. Click on settings (the gear icon in the top right corner) and select the tab AC 800M. From drop down menu, select the service.

AC 800M data can be collected along with System 800xA and S+ Operations HMI data. For System 800xA with AC 800M controller data collection, the MCS-DC tool can be launched on any 800xA node. No input settings are needed for collecting performance and lifecycle data from AC 800M controllers if the HMI is System 800xA. Configuration details of System 800xA HMI data collection is described in [Section 4.2.2, System 800xA](#)

4 Data Collection

4.2 Advanced Mode Data Collection

If the HMI is S+ Operations, follow the steps below to collect AC 800M controller data.

1. Click on **AC 800M** tab to provide input for AC 800M controllers data collection.

The screenshot shows the 'ABB My Control System - Data Collector' application window. The 'Configuration' tab is active, and the 'AC 800M' sub-tab is selected. The interface includes a progress bar at the top with steps: S+ Operations HMI, Prerequisites Check, Periodic Collection, and AC 800M. Below the progress bar, the 'AC 800M inputs' section contains two main areas. The first area, 'AC 800M Engineering Client', has input fields for 'AC 800M Engineering Client IP' (containing '172.16.4.50'), 'User Name' (containing 'S1MHDGSP0User1'), and 'Password' (with a masked input and a 'Get AC 800M Project' button). The second area, 'AC 800M project', includes a 'Browse for project folder' button and a 'Select project' dropdown menu. A warning message states: 'AC800M or S+ Operations with AC800M is not supported in current build, so system could not be detected automatically. Hence basic user mode cannot be used for this system. Collect data using Advanced user mode, after restarting MCSDC.' At the bottom right, there are 'Back' and 'Continue' buttons.

Figure 4.45: AC 800M Data Collection Input

Provide the below inputs if the MCS-DC is not launched on an AC 800 M engineering node.

- AC 800M Engineering Client: Below inputs must be provided if the MCS-DC is not launched on an AC 800 M engineering node. Provide the inputs and click on **Get AC 800 M Project** button.
 - a. Provide AC 800M engineering client IP
 - b. Provide username of a user account of the engineering client with administrative right
 - c. Provide password of the user account
- AC 800M Project:
 - a. Browse For AC 800M Project Folder by clicking Browse button.
 - b. Select the required AC 800M project from the drop-down list.

4 Data Collection

4.2 Advanced Mode Data Collection

2. Input AC 800M Project: If the MCS-DC is launched on an AC 800 M engineering Client, the recent Project and the Project folder is autopopulated. User can select the inputs as required.
 - Browse For Project Folder Browse the AC 800 M Project
 - Select Project
Select the required AC 800 M project

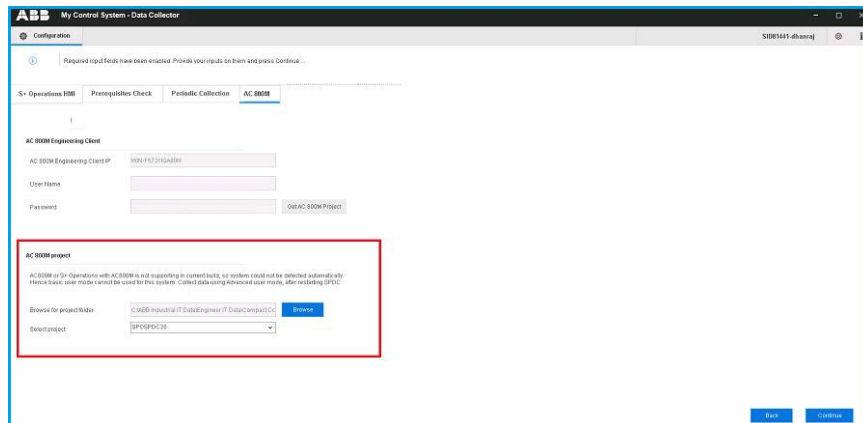


Figure 4.46: Browse and Select AC 800M Project

Controller crash files (logs) will be collected from primary as well as redundant AC 800M connectivity server, for which, users can set the maximum size of the collection file. Click on settings (the gear icon in the top right corner) and select the tab AC 800M. From drop down menu, select the maximum size for the collection file. Crash file collection is enabled by default with a maximum file size of 15 MB. Crash file collection can be disabled by unchecking the provided checkbox.

Figure 4.47: Crash File Collection Settings

4.2.6 AC 70, 110, 160

Only lifecycle data collection is supported for AC 70, 110 and 160 controllers. Supported HMI is System 800xA. Configuration details of System 800xA HMI data collection is described in [Section 4.2.2, System 800xA](#)

After providing the required input for System 800xA HMI data collection, click **Continue** to provide the input for AC 70, 110, 160 controller data collection. Click the **Browse** button to select the AC 70/110/160 project export folder. After selecting the project export folder, find all the available project export (.BAX) files listed under the 'Available' section. The most recent export (.BAX) file will be auto selected and listed under 'Selected' section. There are options to move the export files from 'Selected' section to the 'Available' section and vice versa. Move the required export files to the 'Selected' section. (refer to [Appendix D, System configuration export](#) for exporting system configuration files).

4 Data Collection

4.2 Advanced Mode Data Collection

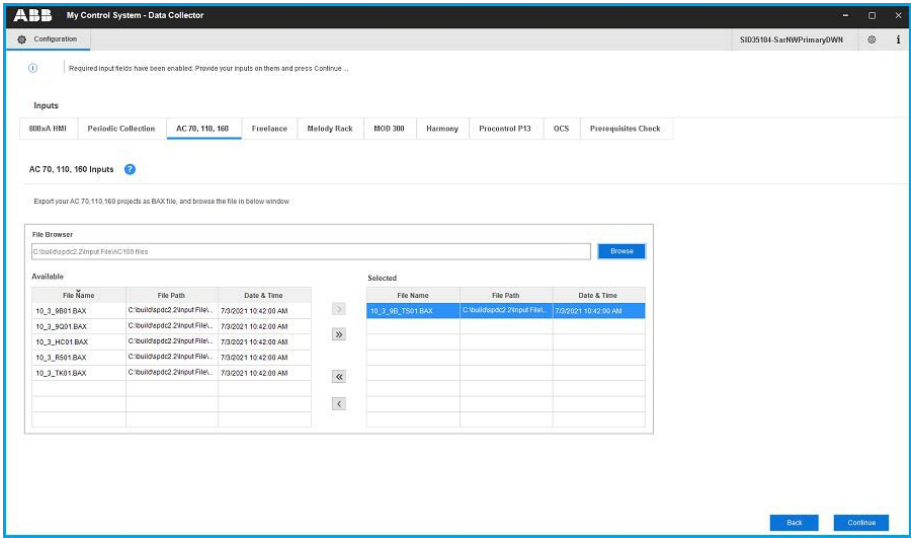


Figure 4.48: Browse Project Export Folder

Click **Continue** to proceed with the data collection.

4.2.7 Freelance

Freelance controller data can be collected along with System 800xA or Freelance HMI data. Freelance HMI with Freelance controller data collection is described in [Section 4.2.3, Freelance](#). If the connected HMI is System 800xA, follow the steps below.

1. Click on the **Browse** button to select the Freelance project export folder. Once the project export folder is selected, all the available project export (.csv/.csvs) files are listed under Available section. The most recent export (.csv/.csvs) file is auto selected and is listed under Selected section. There are options to move the export files from Selected section to Available section and vice versa. Move the required export files to Selected section. If the selected project export file type is .csvs, project export file decryption key has to be provided in the decryption key field (refer to [Appendix D, System configuration export](#) for exporting system configuration files).

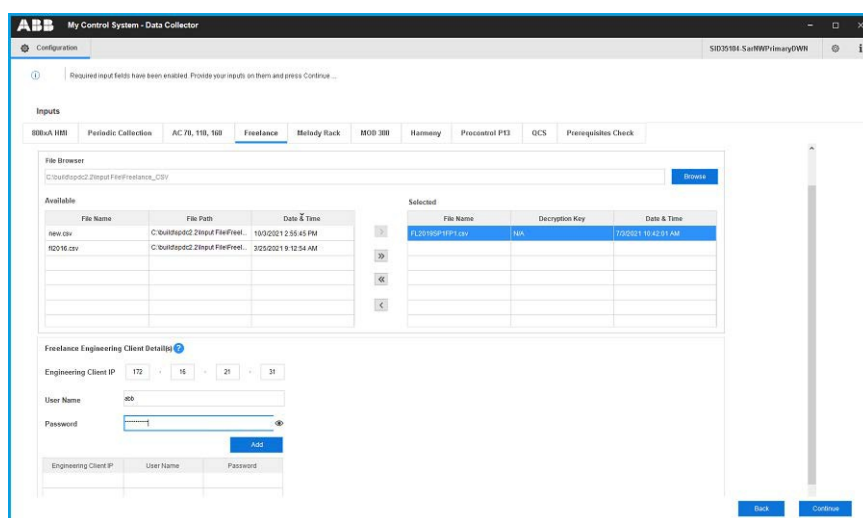


Figure 4.49: Select the Freelance project export folder

2. Engineering node IP: Scroll down the screen to enter the Engineering client node IP and the user credentials and click Add.

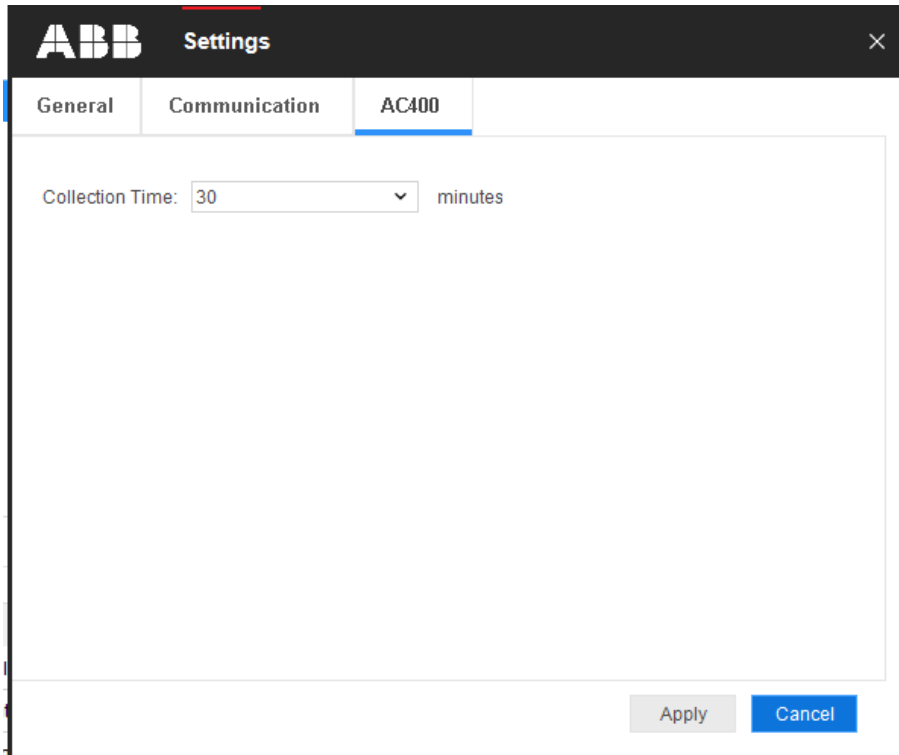
4.2.8 AC 410, 450, MP, SG 400

AC 410/450/MP/SG 400 controller data collection is described in this section. Supported HMI is System 800xA. Refer to [Section 4.2.2, System 800xA](#) for HMI data collection configuration.

Controller data collection happens in sequential manner, hence, collection duration per controller needs to be set. See the screenshot below. Minimum time interval that can be set between two controller collection is 2 minutes and maximum 30 minutes. Higher the duration, more data samples will be available for further calculations.

4 Data Collection

4.2 Advanced Mode Data Collection



The screenshot shows the ABB Settings application with the 'AC400' tab selected. Under the 'Collection Time' field, the value '30' is entered in the dropdown menu, followed by the unit 'minutes'. At the bottom right, there are 'Apply' and 'Cancel' buttons.

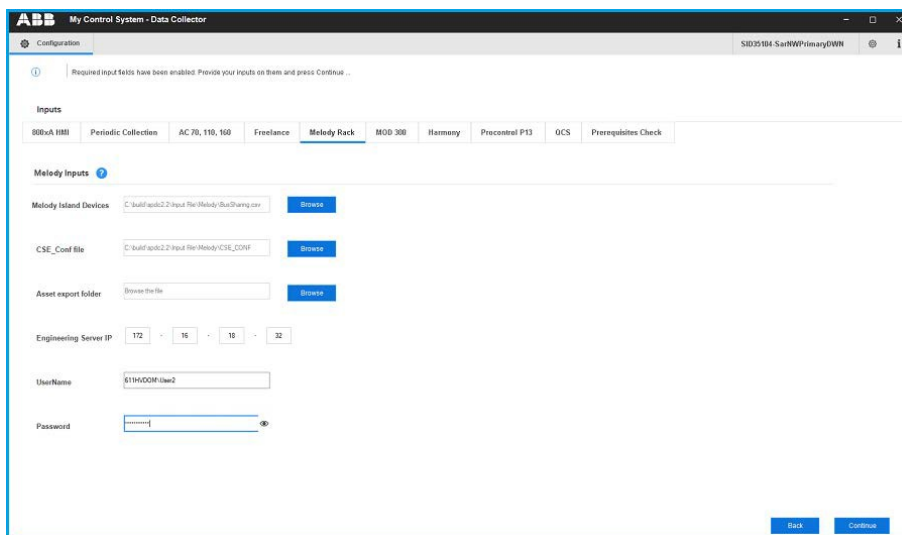
Figure 4.50: Collection Time Interval

4.2.9 Melody Rack



To collect Melody controller data, MCS-DC launch node must be part of Onet network.

Melody controller data can be collected along with System 800xA or S+ Operations HMI data. Based on the connected HMI, refer to [Section 4.2.2, System 800xA](#) or [Section 4.2.4, S+ Operations](#) for HMI data collection configuration. Provide the below inputs to proceed with Melody Rack data collection (refer to [Appendix D, System configuration export](#) for exporting system configuration files).



The screenshot shows the 'My Control System - Data Collector' configuration window. The 'Melody Rack' tab is selected under the 'Inputs' section. The 'Melody Inputs' section contains the following fields and buttons:

- Melody Island Devices:** C:\local\apoc2.2\input files\Melody\BusChangover [Browse]
- CSE_Conf file:** C:\local\apoc2.2\input files\Melody\CSE_CONF [Browse]
- Asset export folder:** [Browse the file] [Browse]
- Engineering Server IP:** 172.16.18.32
- UserName:** S11H000FUser2
- Password:** [Masked] [Show/Hide icon]

At the bottom right, there are 'Back' and 'Continue' buttons.

Figure 4.51: Melody Rack Tab

4 Data Collection

4.2 Advanced Mode Data Collection

1. Melody Island Devices:

Click the **Browse** button to select the Melody Island DevicesExport file. Ensure to export the latest melody Island device file that is synced with the latest hardware structure.

2. CSE_Conf File:

Click the **Browse** button to select the Current CSE_Conf File.

3. Asset Export Folder:

Click the **Browse** button to select the Asset Export Folder.

4. Composer Melody node IP Address:

Enter the IP Address of S+ Engineering Server, where Composer Melody is installed.

5. Username:

Provide the Composer Melody node username.

6. Password:

Provide the Composer Melody node server password

4.2.10 MOD 300

Click on **MOD 300** tab to provide input for MOD 300 controllers data collection. Click the **Browse** button to select the latest ATF file, taken from AdvaBuild engineering node. Click **Continue** to proceed (refer to [Appendix D, System configuration export](#) for exporting system configuration files).

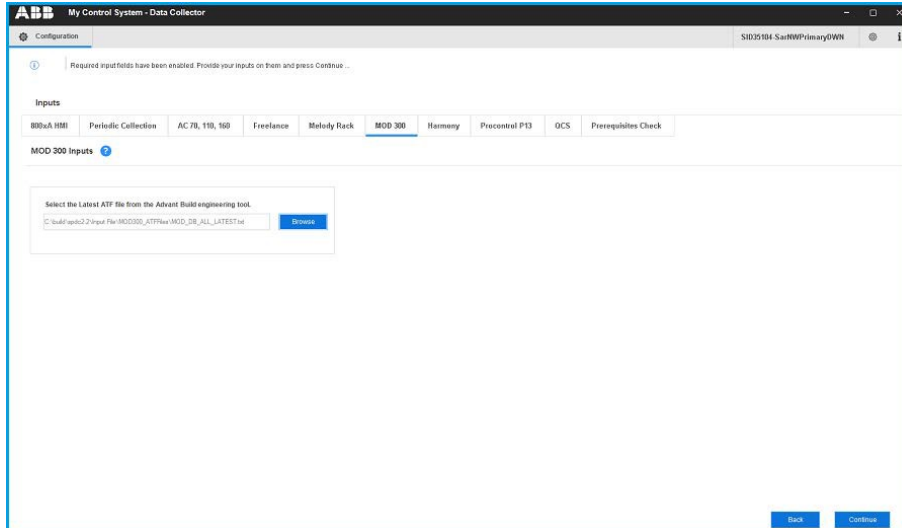


Figure 4.52: MOD300

4.2.11 Harmony

This section explains data collection from Harmony controllers.



If the HMI is System 800xA and the Harmony engineering node is not part of 800xA node admin structure, HMI and controller data must be collected separately and to be merged. Refer to [Section 5, Post Collection](#) for more details.

For 800xA with Harmony data collection, MCS-DC launch node shall be selected based on the following scenario.

- Lifecycle data (For Harmony Rack modules): Node in which Composer Harmony is installed (Harmony Composer project .ebp is present)
- Lifecycle data (For Symphony DIN): Any node which has HAPI installed and reachable through control network (recommended Composer Harmony node)
- Performance data: Any node which has HAPI installed and reachable through control network (recommended Composer Harmony node)

For S+ Operations HMI with Harmony Controllers, following nodes shall be used for data collection.

1. Performance and Lifecycle data: S+ Control Engineering node (Composer Harmony is present)
2. Performance data only: Recommended on S+ Control Engineering node or any node from where control network is reachable.

Follow the steps below to collect Harmony controller data.



In order to collect Harmony controller data, MCS-DC must have a dedicated connection to the ICI module. If this isn't the case, the controller collection may fail. Refer to [Section 6.7, Connection with ICI module failed](#) for the procedure to ensure this.

4 Data Collection

4.2 Advanced Mode Data Collection

1. Select the Harmony tab to provide input for Harmony controllers data collection.

ABB My Control System - Data Collector

Configuration SID25104 dhanraj

Required input fields have been enabled. Provide your inputs on them and press Continue...

Inputs

Harmony Periodic Collection

Harmony Inputs

General

Control Network Type ☒ INFI-NET ☐ PN800

Logical ICI

ICI Type ☒ ET/IC2 ☐ SPS / PN800

HAPI Licensed To

HAPI Request (ms)

IP Range Scan

Enter the Control Network IP's here

Start IP address:

End IP address:

Scan IP Range

Topology Scan

Scan All Loops ☒

Loops

Topology File

Data Collection

Data Collection Duration (min)

Time Interval Between Samples (sec)

Samples

LCS Data

Launch LCS Parser

LCS Input data file

Browse

Include Edited Modules ☐

Back Continue

Figure 4.53: Harmony Rack

- General
 - a. Controller Type: INFI-NET and PN800 control network types are supported for 800xA with Harmony data collection.
 - b. Logical ICI: Provide the ICI number configured by Harmony System Configuration Utility (hSysCfgU.exe) for connecting into control network.
 - c. ICI Type: This selection will be done automatically based on Control Network Type selection.
 - d. HAPI Licensed To: Keep the default input S+ Engineering, unless it is different.
 - e. HAPI Request (ms): Keep the default input.
- IP Scan Range - This input is applicable only if PN800 network type is selected. Provide the required Symphony DIN Controller IP range or IP of ENM module. Data collection will be done only modules which IP address falls within the specified scan range.
- Topology Scan
 - a. Scan All loops:
Check this Check Box to scan all loops
 - b. Loops: To Scan the specific loops, provide the loop numbers separated with comma (Example: 1, 5, 6)
 - c. Topology File: Provide Name of Harmony topology scan file
- Data Collection Duration (min): It is recommended to keep the default input. Please note that the minimum data collection duration which can be set is 6 minutes.
Time Interval Between Samples (sec): It is recommended to keep the default input. Please note that the minimum time interval duration which can be set is 30 seconds.
Samples: Samples are auto calculated based on the formula $\text{Samples} = \frac{\text{Data Collection Duration} \times 60}{\text{Time Interval Between Samples}}$. Please note that the minimum Samples

4 Data Collection

4.2 Advanced Mode Data Collection

which can be configured is 10. If a correct value is configured for Data Collection Duration (min) and Time Interval.

Near Samples field, a Green tick mark will appear. If wrong values are configured, a Red cross mark will appear.

2. Harmony controllers Performance Input, IP Scan Range: This input is applicable only if VPNI ICI Type is selected. Provide the required Symphony DIN Controller IP range or IP of ENM module. Data collection will be done only for the Controllers for which the IP address is entered here.
3. If a wrong IP range is added, there is an option to remove that. To remove incorrectly given IP range, select the IP range by clicking on it and then click on the **Remove** button.
4. Harmony INFI-NET network controller LCS Input data file: If the user already has a valid LCS input data file (.csv), click Browse button to select the file.

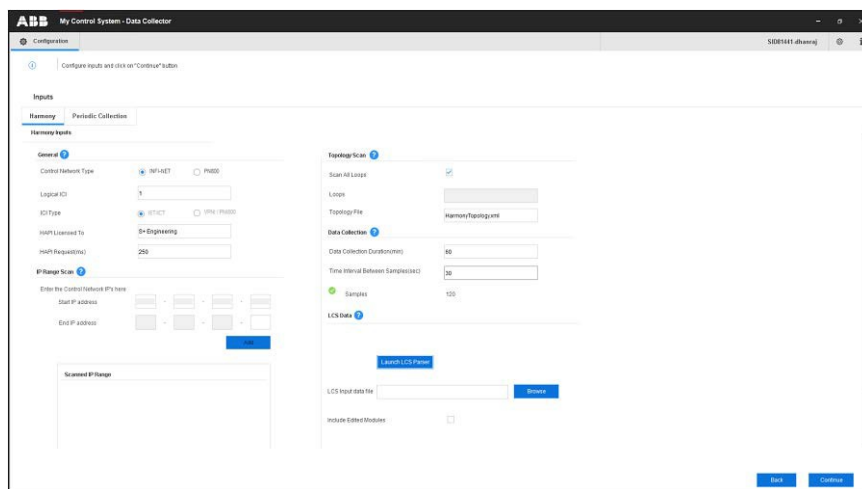


Figure 4.54: Harmony Rack

4 Data Collection

4.2 Advanced Mode Data Collection

5. INFI-NET network controllers LCS Input data file: For generating a new LCS Input data file, make sure that MCS-DC tool is launched in the S+ engineering node. Click on **Launch LCS Parser** button and follow the below procedure.
 - a. Click on **Open Project** button.

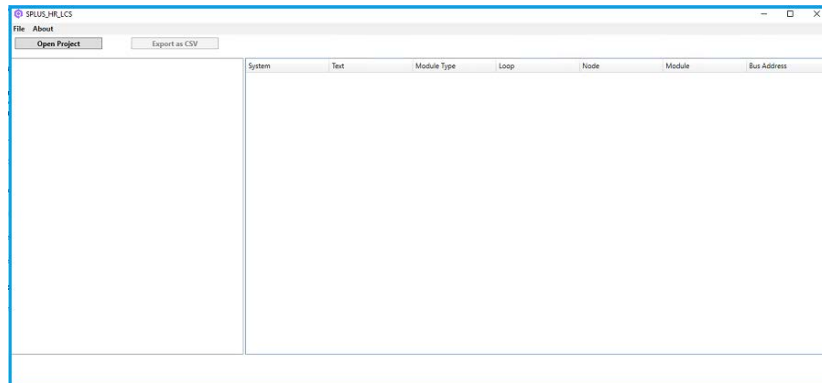


Figure 4.55: Open Project

- b. Browse and select the required project (.ebp) file, click **Open**.

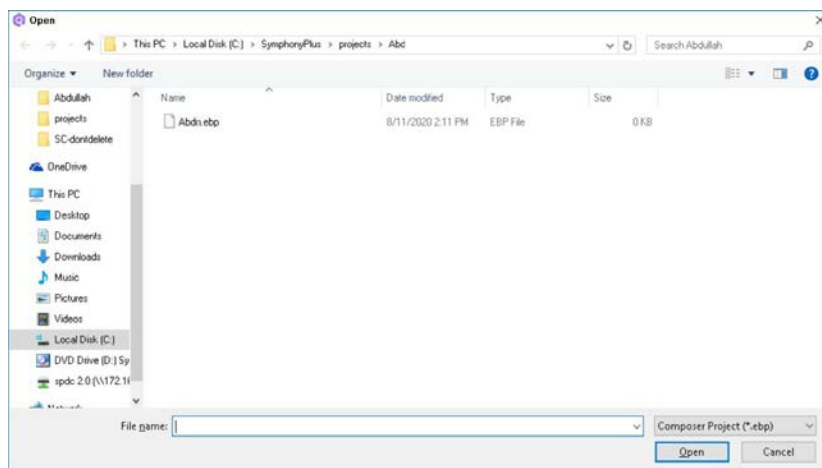


Figure 4.56: Open option

- c. The following window appears with a progress bar as highlighted in Figure, which indicates that the data collection process is in progress. Once the data collection process is completed. Click on **Export as CSV** button to generate a new LCS Input data file and save the file in PC.

NOTE: The data collection process may take some time based on the size of the project.

4 Data Collection

4.2 Advanced Mode Data Collection

System	Text	Module Type	Loop	Node	Module	Bus Address
HarmonyRack	Control Network1	INNISev	1	2		
HarmonyRack	Control Network1	INNPMax	1	2	0	
HarmonyRack	Control Network1	BRC410	1	2	2	
HarmonyRack	Control Network1	BRC410	1	2	3	
HarmonyRack	Control Network1	MFP02	1	2	4	
HarmonyRack	Control Network1	MFP02	1	2	5	
HarmonyRack	Control Network2	INNPMax	2	2		
HarmonyRack	Control Network2	INNPMax	2	2	0	
HarmonyRack	Control Network2	BRC410	2	2	3	
HarmonyRack	Control Network2	INNPMax	2	3	0	
HarmonyRack	Control Network2	BRC400	2	3	2	
HarmonyRack	Control Network2	BRC400	2	3	3	

Figure 4.57: Export as CSV

- d. A popup appears as a confirmation that the .csv file is exported successfully. Click **OK**.
- e. Click on the to **Browse** button to select the exported .csv file.

4.2.12 Procontrol

Configuration details of System 800xA HMI data collection is described in [Section 4.2.2, System 800xA](#). For P13 and P14 controllers, only lifecycle data collection is supported as described below.

1. After providing the required input for System 800xA HMI data collection, click **Continue** to provide the input for P13/P14 controller lifecycle data collection. Select Procontrol P13 or P14 tab. Click on **Browse** button to select the latest P13/P14 source file, taken from the engineering node. Refer to [Appendix C, Procontrol P13 source file \(.csv\) separators](#) / [Appendix H, Procontrol P14 system configuration file](#) for more details.

4 Data Collection

4.2 Advanced Mode Data Collection

2. Click **Parse** button, in case of P13. Contents of the P13 source file (.CSV) is displayed.

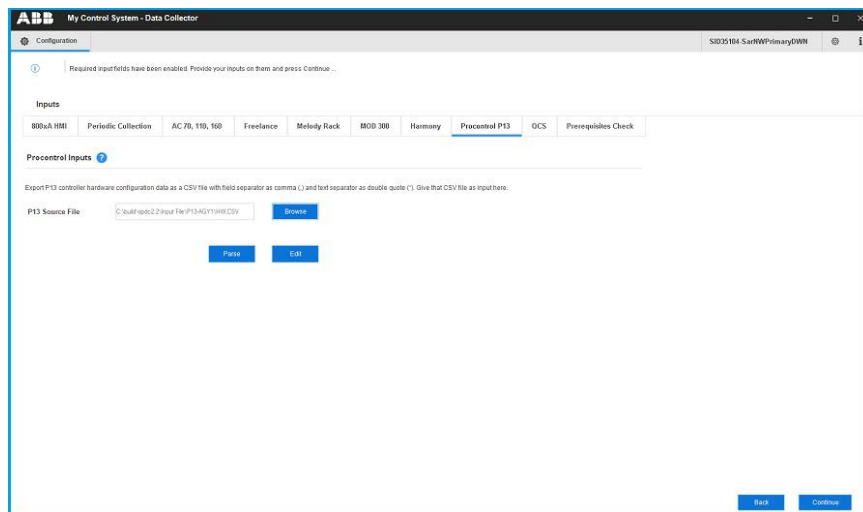


Figure 4.58: P13 Parse Button

In the case of P14, browse and select the exported log file as shown in figure. Click on the 'Validate' button to validate the file and then click on the 'Continue' button.

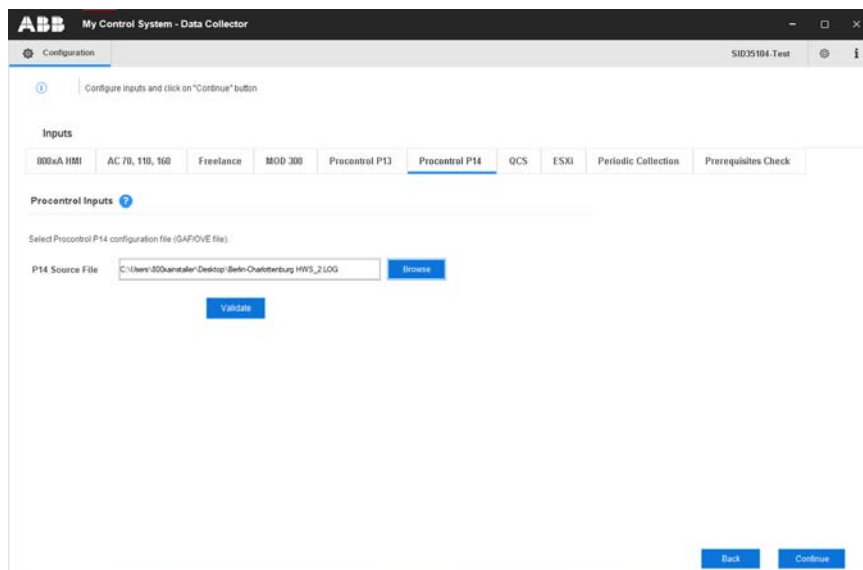


Figure 4.59: P14 Validate Button

- a. In the case of P13, for all the blank entries, select the exact module type and version from the drop-down box and click **OK**, if there are any blank entries while clicking OK, an error is thrown saying "The below devices are not having the mapping name". Select the exact module type and version to proceed further. If any modification is required, click Edit, to modify the parsed file. Click Continue to proceed.

4 Data Collection

4.2 Advanced Mode Data Collection

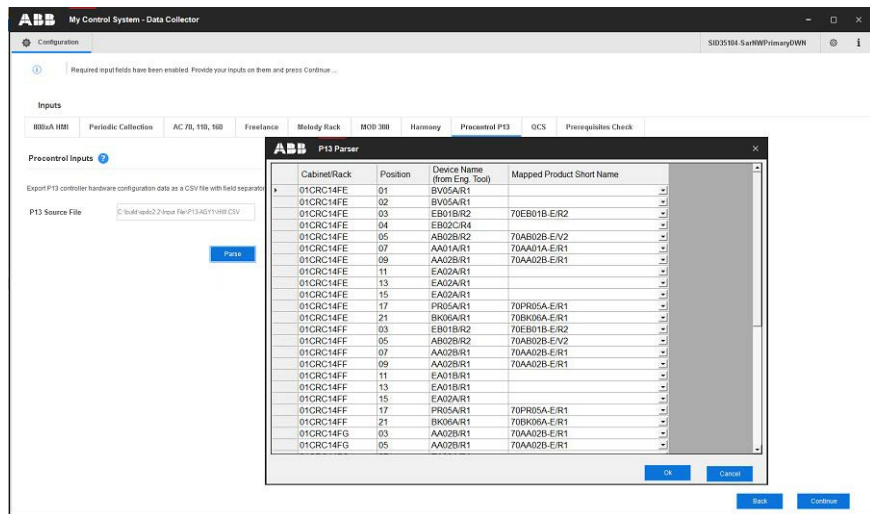


Figure 4.60: Mapped Product Short Name

4.2.13 QCS

Configuration details of System 800xA HMI data collection is described in [Section 4.2.2, System 800xA](#). For QCS controllers, only lifecycle data collection is supported as described below.

1. Click on the **Browse** button to select the QCS folder where the latest joconfig.xml files are stored. The joconfig.xml files will be available in the project directory of the QCS Connectivity Server, which is usually “C:\Program Files (x86)\ABB Industrial IT\Quality Control Solutions\Engineer IT\JOCONFIG\Projects”. There will be subdirectories for different builds that have been created on that QCS system. Select the directory with the most recent build that has been deployed to build the system. Once the folder is selected, all the available joconfig.xml files will be listed under Available section. The files can be moved from the Selected section to the **Available** section and vice versa. Move the required files to the **Selected** section. Click **Continue** to proceed.

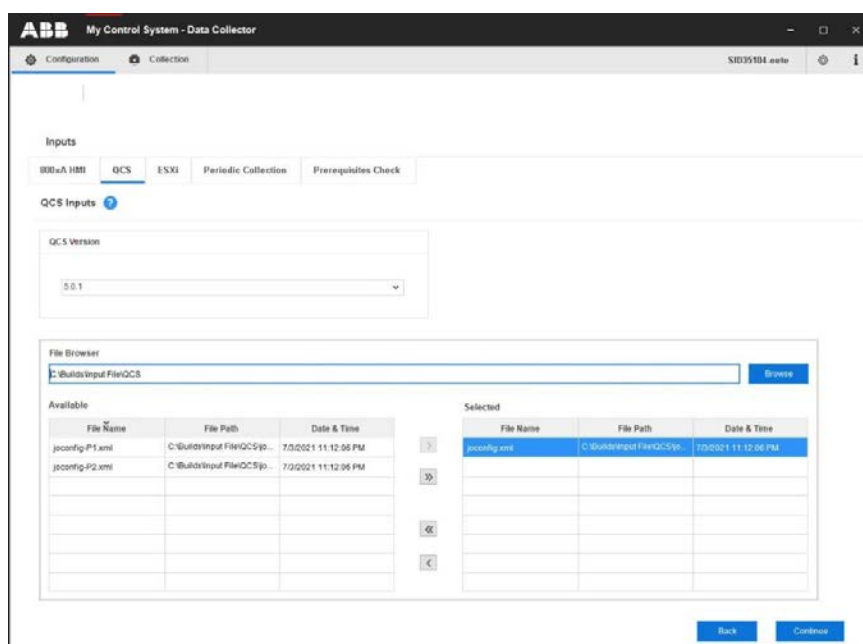


Figure 4.61: Select QCS version

2. Click the **Browse** button to select the and load the joconfig.xml of the correct build from the joconfig project directory. The latest joconfig.xml file will be available in the project directory of the QCS Connectivity Server, which is usually “C:\Program Files (x86)\ABB Industrial IT\Quality Control Solutions\Engineer IT\JOCONFIG\Projects”. There will be the subdirectories for the different builds that have been created on that QCS system. Select the directory with the most current build that has been deployed to build the system and browse to the joconfig.xml file in there. Click **Continue** to proceed.

4.2.14 ESXi

In this chapter there is a detailed explanation about how to collect ESXi host server health data with MCS-DC. ESXi's data collection is supported in both Basic and Advanced mode. Following are the input configuration for collecting ESXi performance data.

At least one HMI performance and/or lifecycle must be selected to enable ESXi data collection.

4 Data Collection

4.2 Advanced Mode Data Collection

The screenshot shows the 'ABB My Control System - Data Collector' window. The 'Configuration' tab is active, and the 'ESXi' sub-tab is selected under 'Input'. The 'Enable ESXi Data Collection' checkbox is checked. Below this, the 'ESXi inputs' section contains a form with the following fields: 'ESXi Server Name' (text input), 'ESXi server IP' (IP address input), 'Port Number' (text input with '443' entered), 'User Name' (text input), 'Password' (password input), and 'Computer IP to reach ESXi server' (IP address input). An 'Add' button is located below the form. Below the form is a table with columns: 'ESXi Server Name', 'ESXi server IP', 'Port Number', 'User Name', 'Password', and 'Compute'. The table is currently empty. A 'Remove' button is located at the bottom right of the table. At the bottom of the window are 'Back' and 'Continue' buttons.

Figure 4.62: ESXi Data Collection - Input Configuration

Enable ESXi data collection: Check this for enabling ESXi data collection.

ESXi Server Name: The name of the ESXi server that must be collected. To obtain the ESXi server name, log in to the ESXi server by using vSphere web client and click on Host under Navigator. Note that ESXi server name input is case-sensitive, so provide the name as appearing in the web portal. Refer to the image below.

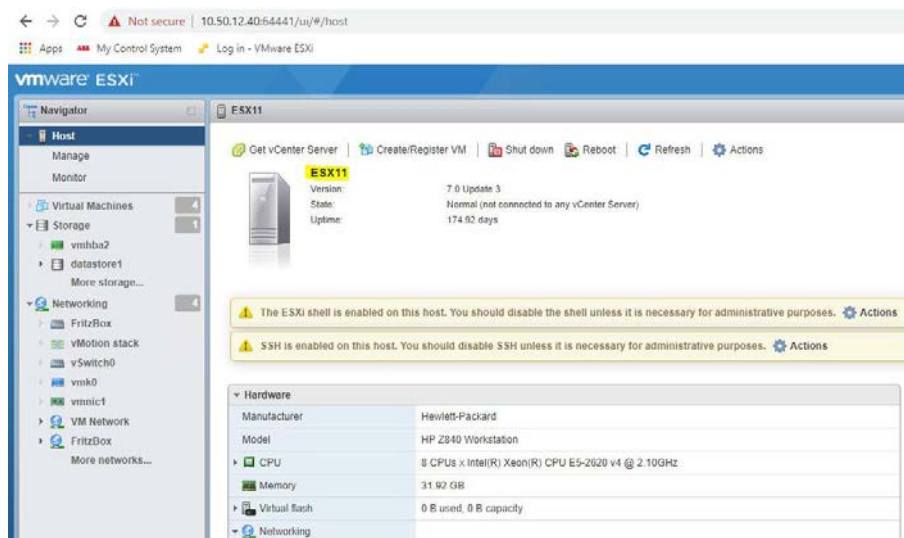


Figure 4.63: ESXi Server Name

ESXi Server IP: The IP Address of the ESXi Server that must be collected; make sure that the selected IP can be reached from at least one of the computers part of the system.

Port Number: The default port number is 443. Do not change this, unless the ESXi server has been configured to communicate though a different port number.

4 Data Collection

4.2 Advanced Mode Data Collection

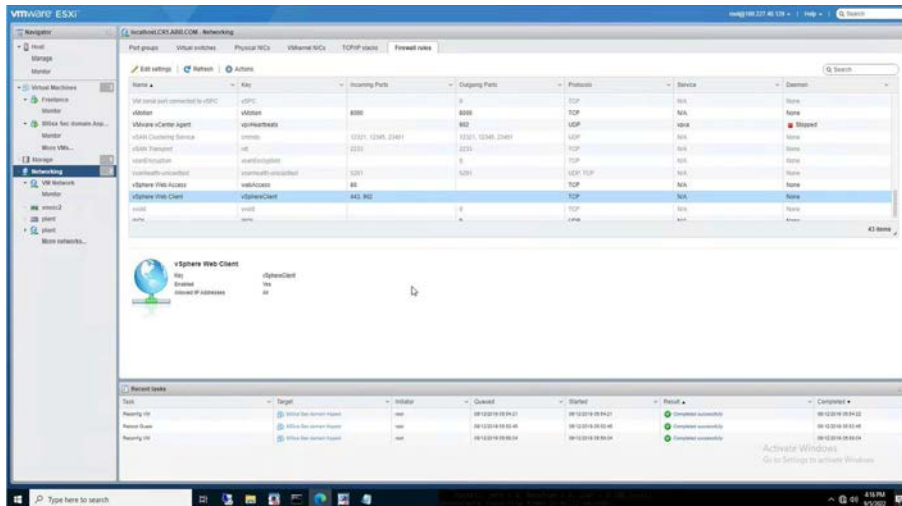


Figure 4.64: ESXi Access - Incoming Port

User credentials: The credentials needed to access the ESXi server in read-only mode. Note that, the username and password are case-sensitive. The scan will fail if the user access permission is higher than read-only.

Computer IP to reach ESXi server: The IP Address of the computer which has access to the ESXi sever. The ESXi data collection agent will be deployed in this computer, therefore it is mandatory that this computer is part of the system and is part of data collection. Please be aware that, if this computer is not reachable from the computer where MSC-DC is being executed, ESXi data collection can't be done. Add the IP Address of the computer, and then select the Add button. It is possible to add more than one ESXi server, one at a time. If an ESXi server has been added by mistake, it can be removed selecting it and then selecting the Remove button. Ensure that this computer is not removed from the collection by means of node customization on the collection screen.

Care must be taken for not using this computer as the reachable node for more than one ESXi server.



If the service SFCB (Small Footprint CIM Broker) is not running in the ESXi server, certain sensor data like processor temperature and fan speed, will not be collected.

4.2.15 Non-ABB Systems

Collection of cyber security fingerprint data from non-ABB windows based control system, is possible using MCS-DC. Follow the steps given below.

1. Click Non-ABB System on the left pane and select the checkbox Security. Click Continue.

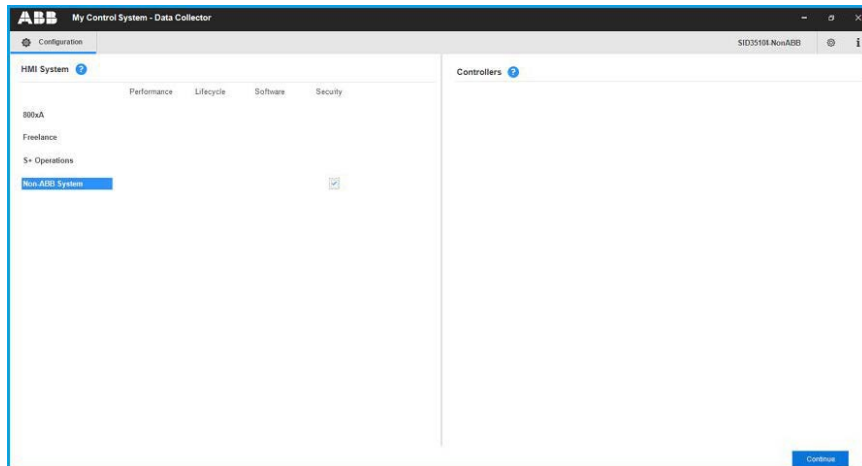


Figure 4.65: Non-ABB System

2. Under Non-ABB System tab, enter IP range of all the node for which data collection has to be done. Data collection will be done only for the node for which the IP address is entered here. After providing the IP range, click **Add**. User can provide multiple ranges too.
3. If a wrong IP range is added, there is option to remove that. To remove, select the added IP range by clicking on it and then click on the **Remove** button.
4. Next input is user credential. Provide the **Username** and **Password** of an administrator user to access all the HMI nodes for data collection. Alternatively, select an administrator user account from the drop-down list. Click the **Add** button. Please note, for nodes in domain network, username should be provided in the format domain name\username. To remove an added credential, use **Remove** button.

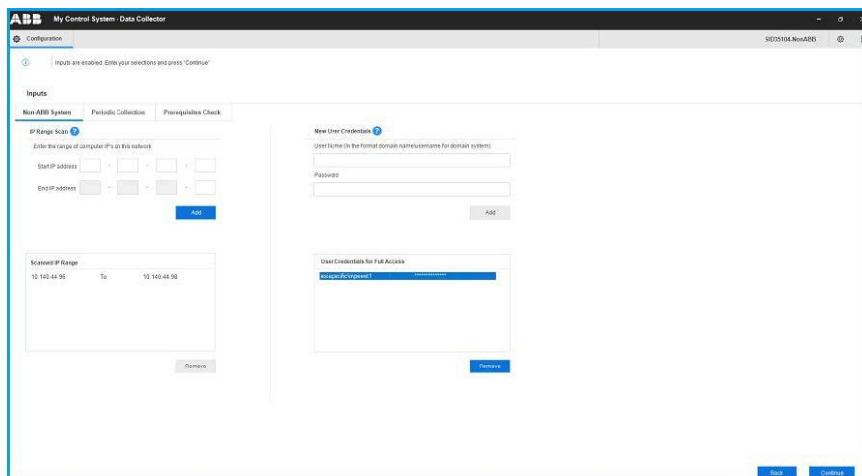


Figure 4.66: IP range and user credentials

4.2.16 S+ Historian in 800xA or third party HMI environment

Collection of S+ Historian data in 800xA or third party HMI environment is possible using MCS-DC. However, this cannot be achieved in a single step. The data must be collected in two instances and merged using MCS-DC's merge functionality described in [Section 5.1, Collection file merging Procedure](#). Follow the steps below to collect the S+ Historian data from the HMIs other than Symphony Plus.

1. Collect the HMI system data using the method described in previous sections (e.g. if the system is 800xA with connects, follow the [Section 4.2.2, System 800xA](#). If it is non-ABB Windows based control system, follow the [Section 4.2.15, Non-ABB Systems](#)).
2. For collecting S+ Historian data, HMI needs to be selected as S+ Operations. Follow the procedure to collect S+ Operations data mentioned in [Section 4.2.4, S+ Operations](#). Note that no controllers must be selected during this collection.
3. Follow the procedure mentioned in [Section 5.1, Collection file merging](#) to merge the data files generated in step 1 and step 2.

4.2.17 Scan, Agent Deployment and Data Collection

Follow the steps below to scan the network and identify the collectable nodes, deploy the collection agents and then to collect the data.

4 Data Collection

4.2 Advanced Mode Data Collection

1. Collection screen contains three parts. The top part contains command buttons for various actions by the user, progress bar and status message area. The middle part contains table for listing the list of HMI nodes and controllers that are part of data collection process and their respective status related to Scan, Agent deployment and Data collection operations. The bottom section contains the log messages.

When the collection screen first appears, only Scan button is enabled. Click on the **Scan** button to scan the available/reachable nodes for data collection.

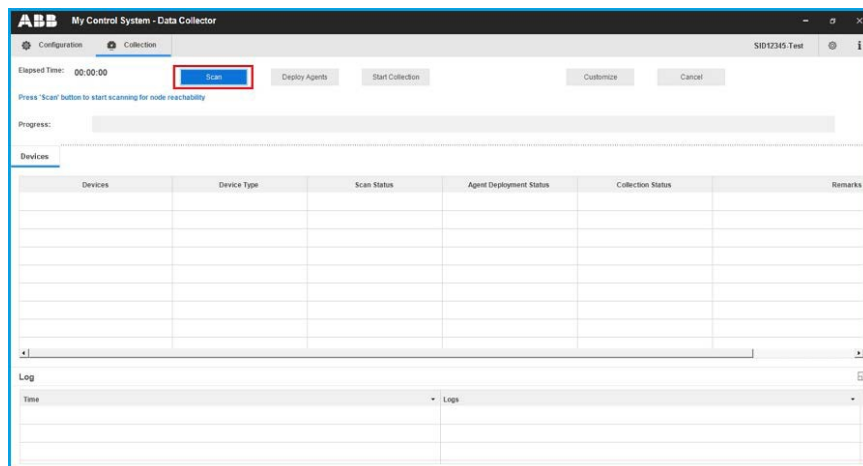


Figure 4.67: Scanning the Nodes

Computers and controllers that are accessible from the MCS-DC launch node, are listed on the first column of the table shown on this page. Their types are listed on the second column. Scan status are shown on the third column. If the node is accessible the status is “Success” in Green. If the node is not accessible the status is “Failed” in Red. However, if the accessibility status can't be checked at this point, then the status is “Not applicable” in Grey.

The possible reasons for the failed scans are indicated under the Remarks column. Furthermore, a message appears on the user interface prompting the user to either re-scan (partially or fully) or proceed with agent deployment. Users may fix the issue and re-scan the failed nodes by clicking the **Scan** button again. Remarks column also indicates the IP address used for accessing the nodes.

Once the scan completes, all the available nodes are listed. If the HMI nodes are accessible, it is shown as Success in Scan status field, if the nodes are not accessible, it is shown as Failed in Scan status field, this may be due to issues such as Network unreliable, IP not reachable, privileges issue over network, User rights not matching etc. If a node scan fails, a message appears on the user interface prompting the user to either re-scan (partially or fully) or proceed with agent deployment. Users may fix the issue and repeat the scan, click the **Scan** button to repeat the scan.

4 Data Collection

4.2 Advanced Mode Data Collection

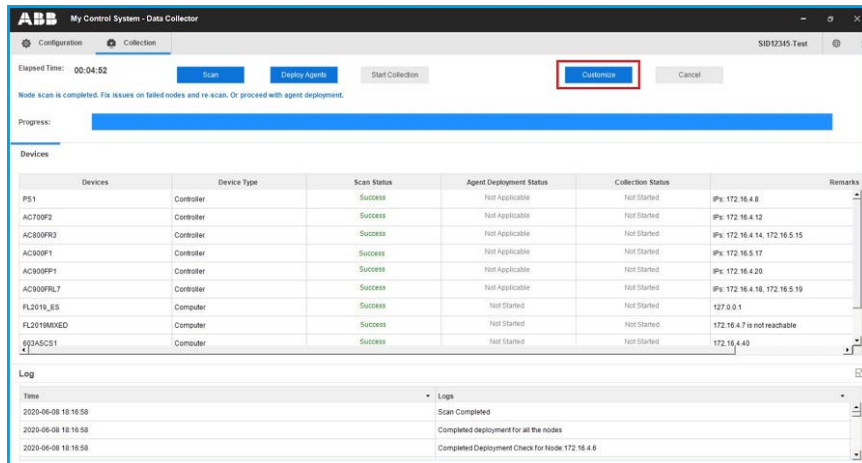


Figure 4.68: List of Nodes

2. User has an option to customize the Data collection nodes for Performance and Lifecycle data collection, to customize click on **Customize** button. All accessible HMI and controller nodes are listed. By default, all accessible HMI and controller nodes will be selected. User shall deselect the nodes that are not desired to be collected, by unchecking the respective checkboxes against the node names. Clicking on **OK** button will save the customization configuration and close the **Customize** window. Clicking on **Reset** button will reset the customization configuration. Please note, that controller customization is not available for this release.

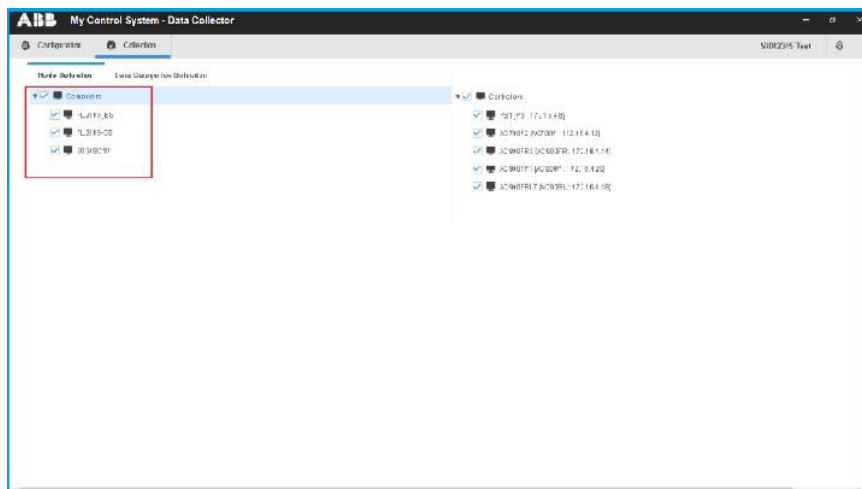


Figure 4.69: Customize Option

4 Data Collection

4.2 Advanced Mode Data Collection

3. Data category selection is possible for Performance data collection and partially for Lifecycle data collection. All the data categories are selected by default. User shall deselect the data categories that are not desired to be collected by unchecking the respective checkboxes against the data category names. Clicking on the **OK** button will save the customization configuration and close the customization window. Clicking on the **Reset** button will reset the customization configuration. Data categories customization is applicable only for HMI nodes, it is not applicable for controllers.

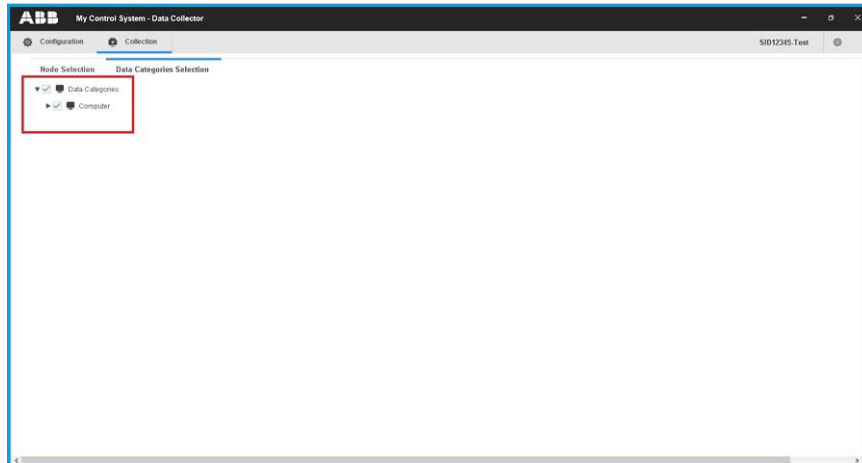


Figure 4.70: Select the Nodes

4. Click on the **Deploy Agents** button to deploy data collection agents on all the HMI nodes listed. MCS-DC performs data collection of HMI nodes through these data collection agents.

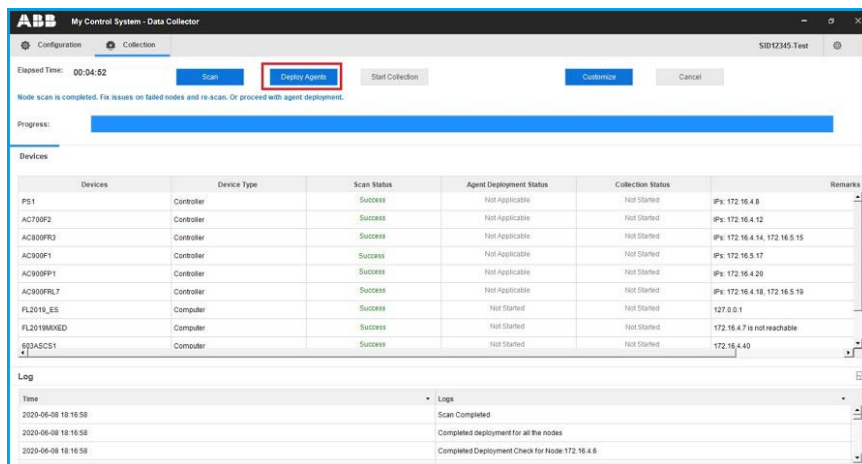


Figure 4.71: Deploy Agents

4 Data Collection

4.2 Advanced Mode Data Collection

5. Once the data collection agents are successfully deployed on the HMI nodes, Success status is shown under Agent Deployment Status column. If agent deployment fails for any node, same is indicated (similar to Scan status). At this point, Start Collection button will be enabled. Click the **Start Collection** button to start the data collection.

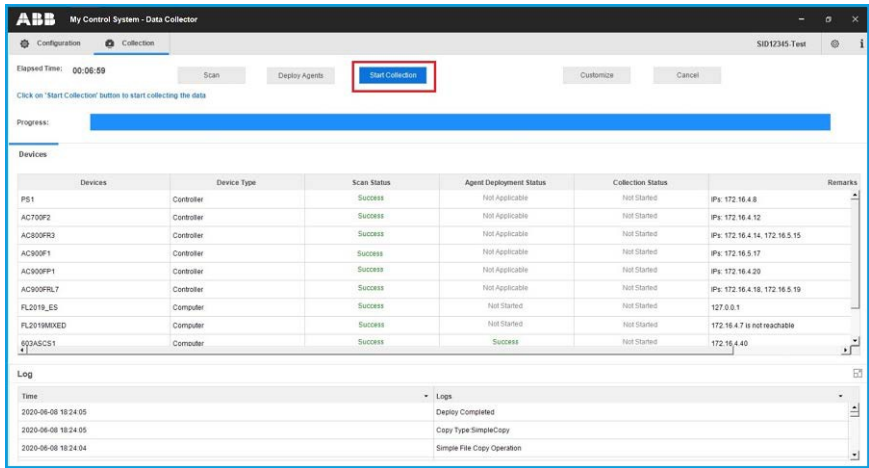


Figure 4.72: Agent Deployment Status

Data collection progress can be seen in the Collection Status column.

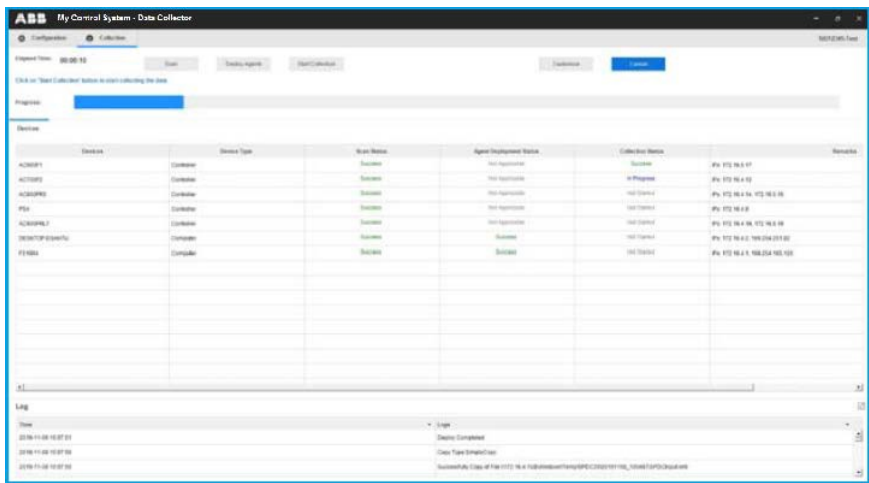


Figure 4.73: Data Collection Progress

Once the data collection is completed, result screen appears. Result screen contains three parts. The top part contains the command buttons for various user actions. The middle part the hardware tree information. The bottom part contains the collection statistics.

4 Data Collection

4.3 Periodic Collection Configuration

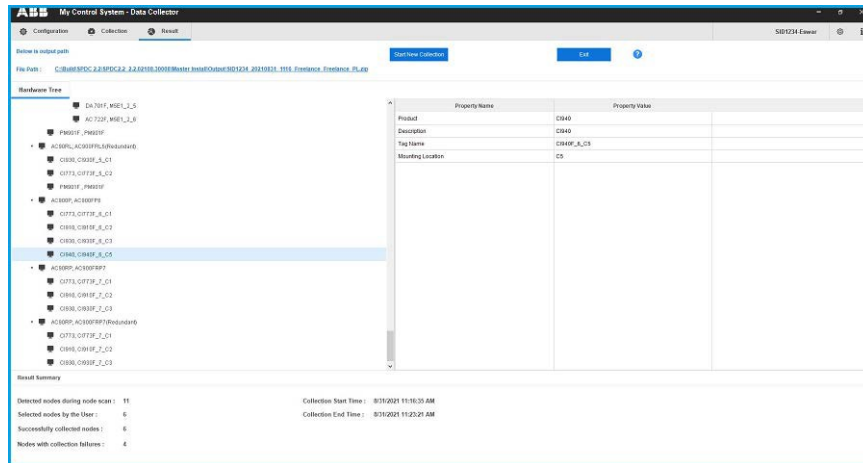


Figure 4.74: Collection File Path

Collection file will be created automatically once the collection is completed. Once the collection file is created, its file path appears on the screen. The collection file can be viewed by clicking on the file path.

6. Click the **Exit** button to close the MCS-DC application.

4.3 Periodic Collection Configuration

Scheduler functionality is implemented in MCS-DC to collect data periodically. Data collection is scheduled to run silently so that no manual intervention is required, once configured.



Note that a periodic data collection must **not** be scheduled in the following cases.

- Windows Maintenance (security update) is initiated.
- System 800xA is executing Aspect-System backup procedures.
- CSWP backup procedures are launching.
- 800xA Historian Server are providing local backups.
- DCS system nodes are down due to any other reasons.

4 Data Collection

4.3 Periodic Collection Configuration

1. Select the Periodic Collection tab after configuring the HMI and controller for data collection, as described in [Section 4.2, Advanced Mode Data Collection](#).

Figure 4.75: Scheduler Configuration

2. **Enable Periodic Data Collection** check-box enables the scheduler. Following are the configurable options:
 - **User Credentials:** To configure periodic data collection, an existing Windows user account can be used, or a new account must be created.
Following criteria must be met for the user account:
 - The user account should have local administrator and log on as a service rights on this computer (MCS-DC launch computer) as well as in the Aspect server. 'Log on as a service' privilege allows data collection services to start and run continuously, even if no users are logged on to the computer interactively.
 - If the user is a domain user, enter the username in the format **domain name\username**. If the system is in work group, provide the credentials as **.\username**.
 - User account must be part of IndustrialITUser group for System 800xA version lower than 6.2. For the versions 6.2 and above, user must be part of user group in which System 800xA users are configured.
 - Click on Validate button, to validate the credentials.
3. Under **Scheduler Configuration** following are the configuration options.
 - **Start Time:** Specify at what time the MCS Data Collection must start. Enter the start time in hours (0 - 23).
 - **Period Options:** User can choose to run the scheduler Daily, Weekly or Monthly. If Weekly is selected, select the day of the week from the drop-down menu. Select the start date, if Monthly is selected. Start Time is applicable for all three scheduler options.

4. MCS Forwarder Gateway Configuration: In order to send the collected data to target applications like CSM (Control System Monitoring) or MCS on-premise via MCS Forwarder, forwarder configuration needs to be done. A checkbox is provided to enable the Forwarder configuration. In the absence of an MCS-Forwarder node, this check box shall be disabled so that the collection files are saved in the output folder (local).



This version of MCS-DC supports MCS Forwarder version 1.8 and 1.9. MCS Forwarder is available in ABB Library and My Control System.



Before entering MCS Forwarder Gateway Configuration, make sure that the MCS Forwarder node is configured and running.

Provide IP address of the Forwarder node and port number, if the

.NET Framework version in the MCS-DC launch node is 3.5 or above. If the .NET Framework version is below 3.5, provide the destination folder path instead. These inputs are enabled automatically, based on the .NET Framework version installed in the MCS-DC launch node.

If the .NET Framework version of the MCS-DC launch node is below 3.5, follow the procedure below, to provide the destination (MCS Forwarder node) folder path:

- a. Folder on remote node (MCS Forwarder) must be set as shared.
- b. Map the remote folder in the MCS data collector launch node. It can be done either through command prompt or through windows UI. Command prompt method is given below.

Open command prompt in the MCS-DC launch node and type the following command.

net use <local drive name> <UNC path of remote node> /user:<UserName> <Password>

Refer to the below screenshot.

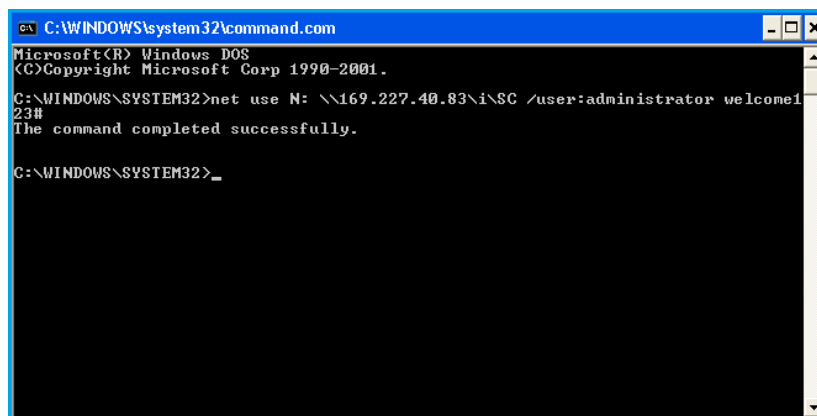


Figure 4.76: Map Network drive

- c. The above step will create a network shared drive in the MCS-DC launch node. Now provide the complete UNC path of the remote folder as destination folder path.

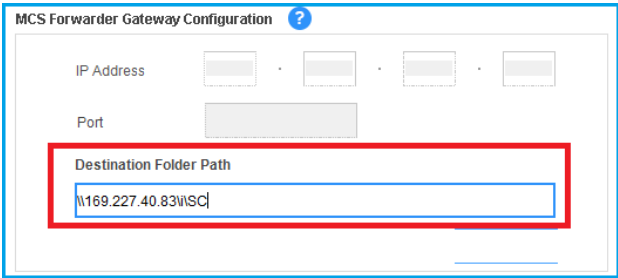


Figure 4.77: Complete UNC path of the remote folder

For more details on MCS Forwarder, refer **7PAA001522_A_EN_MCS Forwarder_user manual**. Provide **IP address**, **Port** and **Destination Folder Path** of the Forwarder node.

- 5. Enable secured communication if applicable. Refer appendix B for more details on secured communication configuration.
- 6. Alive event signals will be sent to MCS Forwarder during the time interval mentioned in this field. This verifies the communication health between MCS-DC and MCS-FW. Default value is 10 minutes.
- 7. After configuring the scheduler parameters, Click next to go to scan window. See fig below.



Scan window is slightly different for periodic data collection when compared with standalone data collection which is described in **Section 4.2.17, Scan, Agent Deployment and Data Collection**. Detailed information on common functionalities is provided in **Section 4.2.17, Scan, Agent Deployment and Data Collection**.

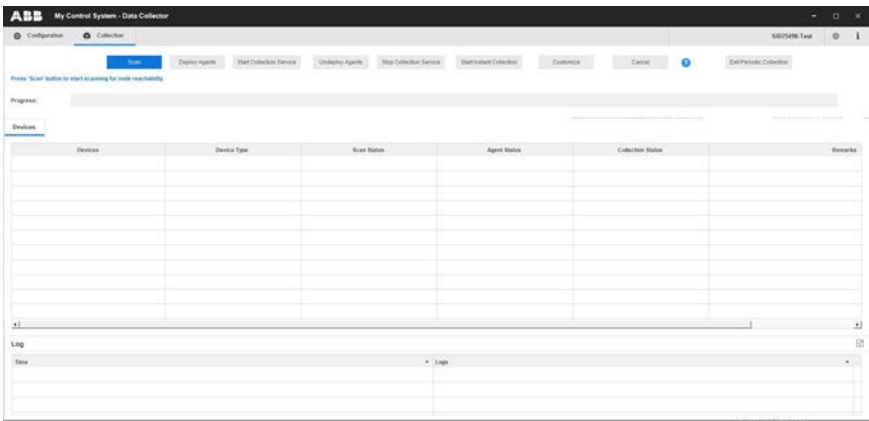


Figure 4.78: Node Scan

4 Data Collection

4.3 Periodic Collection Configuration

8. Click **Scan** button to initiate the control system node scan. Once the scan is completed, deploy button enables. See fig.

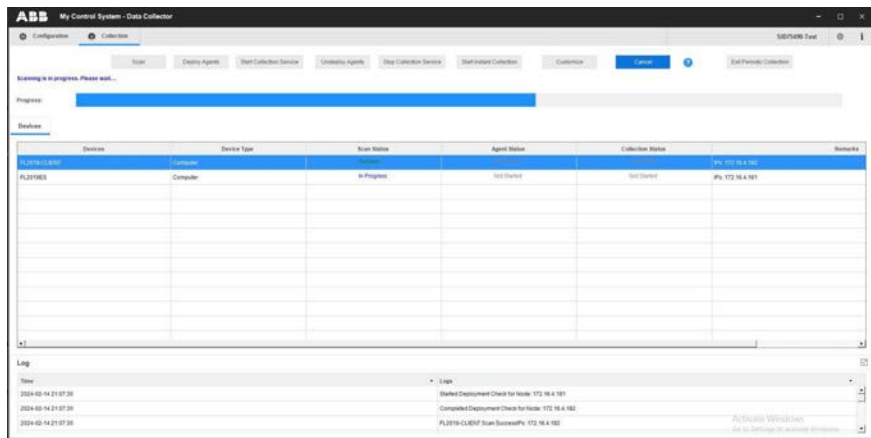


Figure 4.79: Node scan in progress

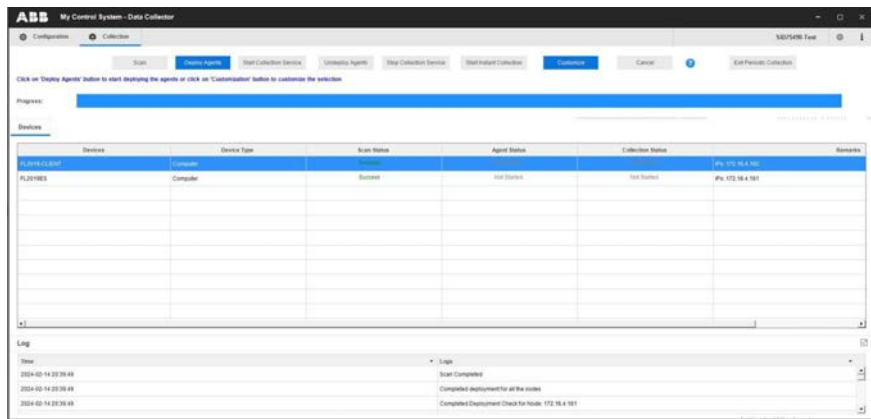


Figure 4.80: Deploy Agents

9. Click **Deploy Agent** button to deploy data collection agents to all the nodes. Refer [Section 6, Troubleshooting](#) if agent deployment fails.



User will be prompted whether to save the user credentials during agent deployment. If saved, user does not have to provide credentials when undeploying the agents.

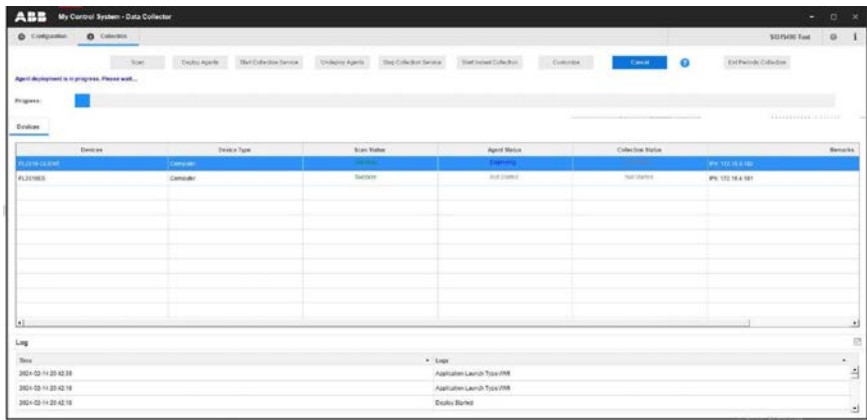


Figure 4.81: Agent deployment status

Figure 4.82: Agent service

Deploying the collection agents will create agent service (MCS.ABBDDataCollectorAgentSvc) in all the nodes earmarked for data collection, as Windows service. See fig.

10. After deploying the data collection agents, **Start Collection Service** button enables. See [Figure 4.83](#).

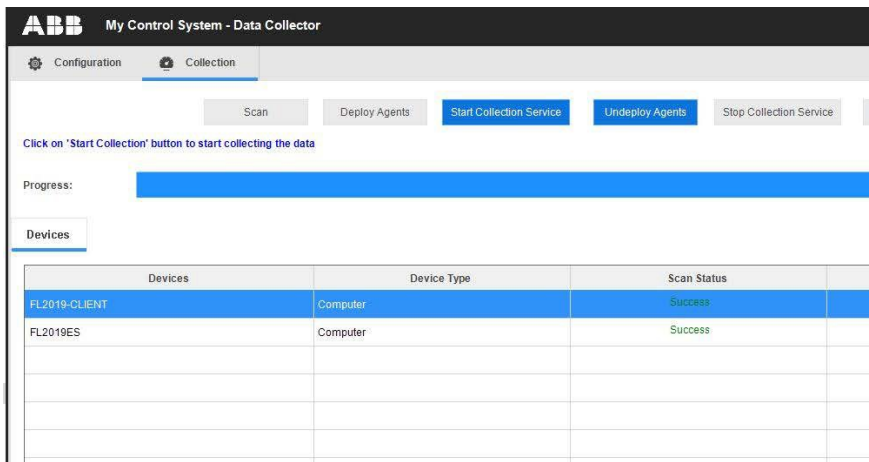


Figure 4.83: Start collection service

Click start collection service button to start the collection service.

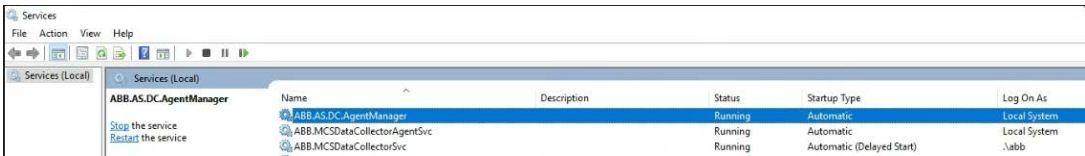


Figure 4.84: Agent Service

Agent services will start and periodically check with scheduler, if data collection is scheduled. The data collection starts based on the time set in the scheduler configuration.

Stop Collection Service button will become active once the collection starts. Collection can be stopped at any point in time by clicking this button. Upon clicking Stop Collection, data collector service in the launch node (ABB.MCSDDataCollectorsvc) will be stopped and therefor the collection.

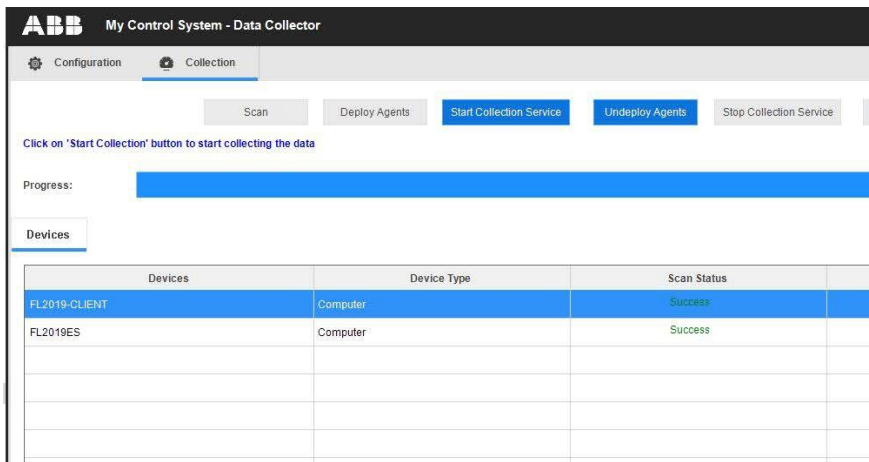


Figure 4.85: Stop collection service

Periodic collection needs to be stopped if the scheduler parameters need to be modified.

When exiting a periodic collection, it is mandatory to undeploy the agents. The **Undeploy Agents** button will stop the agent service in all the nodes and perform necessary cleanup of files, folders and services created as part of periodic collection execution.



From version 3.0 onwards, periodic collection configuration changes can be made without removing collection agents from network nodes. It is, however, necessary to stop the collection services prior to making such changes. Configuration changes will be synced to all remote agents, which may take a while depending on the network's size.



Configuration changes made to the HMI/Controller selection page will reset the prerequisite acknowledgement done previously. The user must reconfirm all prerequisites before proceeding.

To exit from periodic collection, click on **Exit Periodic Collection** button. This button will be enabled after un-deploying the agents.

At any point in time during collection, MCS-DC can be closed. When the tool is re-opened, it will show the collection progress.

Using **Start/Stop Instant Collection** button, users can override the scheduled time for data collection and start a collection immediately. In order to stop instant collection, click on the **Stop Instant Collection** button.

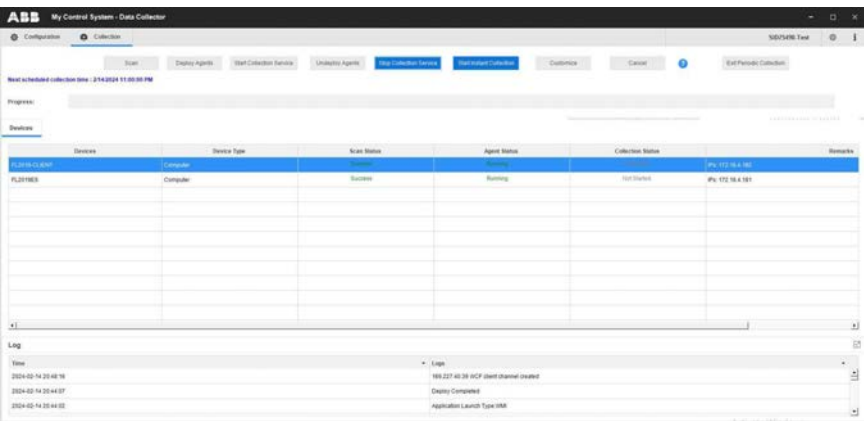


Figure 4.86: Start Instant Collection



Instant collection output file will not be forwarded to MCS-FW, rather it will be saved in *C:\Program Files (x86)\ABB\Service Products\DataCollector\Output* in the MCS-DC launch node.

5 Post Collection

Collection file name is structured in this way:

SID_RecDate_RecTime_HMISystemName_[ControllerSystemName]_DataCat
Mode[Part].zip

- SID: SID of System
- RecDate: Recording Date [YYYYMMDD]
- RecTime: Recording Time [HHMM]
- HMISystemNames: Refer [Figure 4.84](#)
- ControllerSystemNames: Refer [Figure 4.84](#)
- DataCat:
 - L- Lifecycle
 - P- Performance
 - S- Software
 - C- Cyber Security
- Mode:
 - A-Advanced mode
 - B-Basic mode
 - P-Periodic collection mode
 - M-System file merging
- Part - Denotes partial collection, as a result of node customization.

5.1 Collection file merging

For certain system families, it is not possible to collect data in single step. For example, 800xA with Harmony controller system. Harmony data which is collected from Harmony engineering node need not be an 800xA node, and to collect 800xA data, the MCS-DC should be launched in an 800xA node. In this case a two-step collection followed by data file merging is needed to generate a single collection file and therefore a single set of reports.

[Section 4.2.16, S+ Historian in 800xA or third party HMI environment](#) describes other examples where a single step data collection is not possible.

To merge two system data files follow the steps described below.

1. Double-click on the MCS-DC_Launcher.exe, to launch the tool. It is present inside the unzipped MCS-DC folder. Select the option Merging of data files and click the launch button.

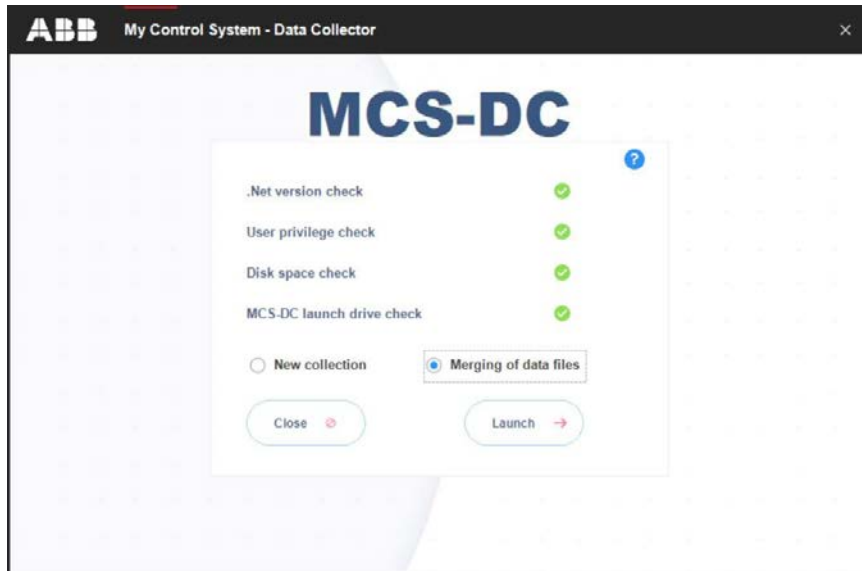


Figure 5.1: Merging of Data Files



If a Microsoft Defender SmartScreen popup appears when MCS-DC is being launched, click Run and continue. Refer to [Appendix I, The Microsoft Defender SmartScreen](#) for more details.

2. Provide the input data files by clicking respective browse buttons. Provide the decryption keys in the respective field. This is the encryption password provided as input during the respective collections. Click Continue.

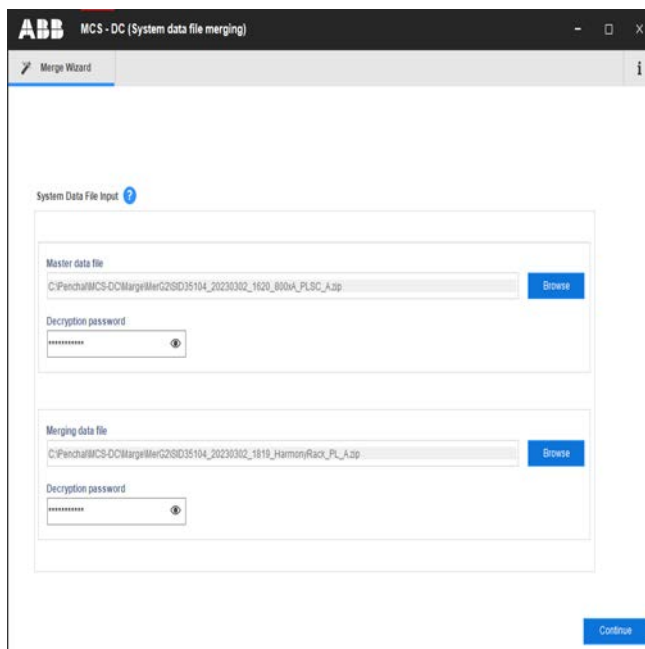


Figure 5.2: System Data File input

3. Select the systems\nodes to be merged from both the System data files. Ensure the following:
 - .NET Framework version 4.8.1 is installed in the computer where merging tool is launched.
 - Both system data files must belong to the same System ID.
 - Both system data files must have been collected with the same MCS- DC version.
 - The time gap between these two data collections must not exceed 90 days.
 - Minimum one system must be selected from each system data file for merging.
 - Same data file cannot be used twice as input files for merging.
 - Do not select more than one HMI system (800xA, Freelance or S+ operations).
 - If HMI system is part of one or both of system data files, selecting it from one of the files is mandatory.



It is important to note that when merging a System 800xA data file with S+ Historian data file, the master file must be the 800xA file. When merging a non-ABB system data file with S+ Historian data file, the non-ABB system data file must be selected as the master file and the S+ Historian data file must be the merging file.



In case of node level merging, collection files system version and collection types must be same.



It is strongly recommended that the data files collected using MCS-DC 2.9 or earlier versions, shall not be used for merging.

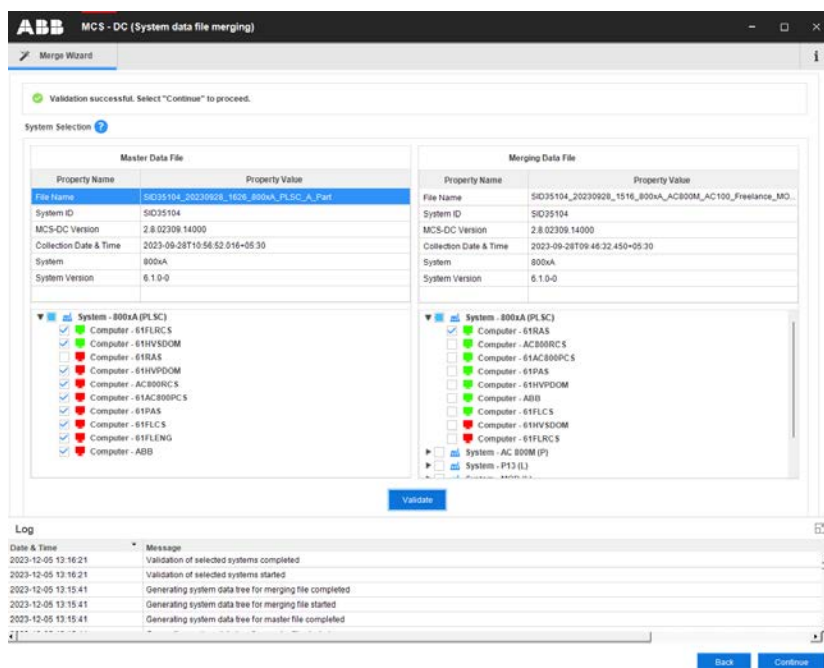


Figure 5.3: Validation

4. The failed nodes will appear in red and succeeded in green. Select the systems\nodes that are to be merged. After selecting required systems from both system data files, perform data validation by clicking on 'Validate' button. Refer to the log window for validation errors, if any. Clicking on 'Back' button will bring back the 'System Data File input' screen. Clicking on 'Continue' button will bring the 'Merging' screen, if data validation is successful.
5. Enter the full name of the user, as it will be shown in My Control System after the merged system data file has been uploaded. Enter an Encryption password with a length of 8 to 16 characters. Any combination of lower case, upper case, numeric and special characters is allowed. This password is used to encrypt the merged data.

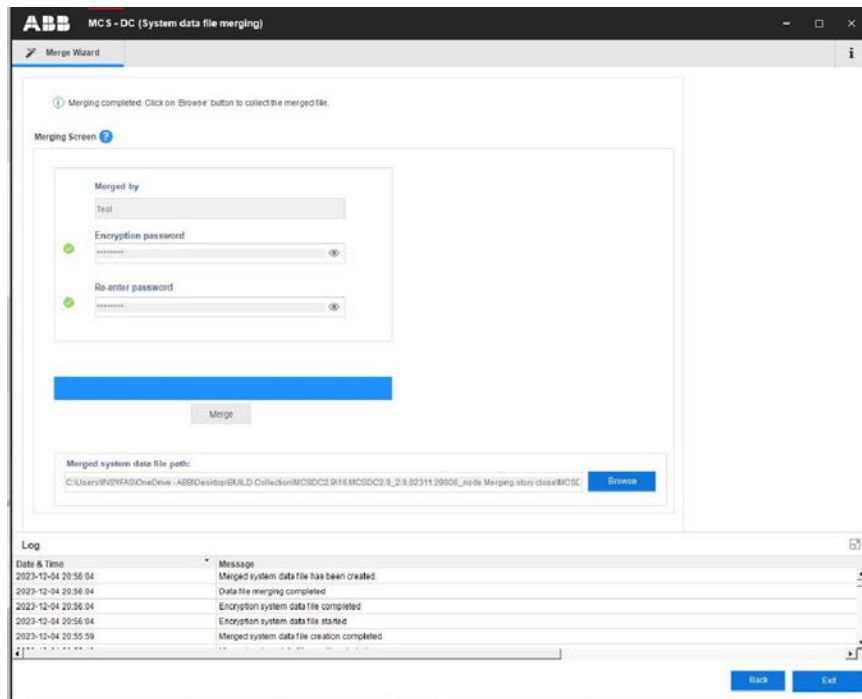


Figure 5.4: Merging Screen

6. Clicking on 'Merge' button will initiate the merging operation. Detailed logs will be shown on the log window. After successful completion, merged system data file will be created and the file path will be displayed. Click the button against the link, to find the merged data file.

Clicking on back button after successful merging operation, will bring the 'System data file input' screen and after failed merging operation, will bring the 'System selection' screen.

Click on Exit button to exit the application.



Merging functionality is not restricted to any system data file combinations. However, In order to maintain the accuracy and validity of the merged data file, users are expected to have proper understanding on valid system combinations.

5.2 Limitations in data file merging

Following are the restrictions in data file merging.

- Merging is not supported for Melody system collections.
- System level merging is supported for QCS system. (for e.g. System 800xA with QCS). However, QCS controller node level merging is not supported.

- Additional node's data which is collected as part of 800xA and Freelance system can only be merged for collections taken using MCS-DC 2.9 or above versions.

5.3 Report Generation from MyABB and uploading data file to ServIS

Collection file must be uploaded to myABB / My Control System to generate reports. Note that the upload of data to ServIS is restricted to specific ABB employees. Contact MCS product management for more details.

6 Troubleshooting

This section provides solution to common issues that may arise while using MCS-DC. Refer to the following sections for step-by-step instructions to resolve specific problems.

6.1 Node scan failed

If node scan failed, it may be due to inadequate user rights to access the remote node. To verify the access rights, do a simple file copy to the remote node from the launch node. Access the path \\<IP address of the remote node>\C\$\Windows\Temp from launch node and copy a small file. If the copy operation fails, user may not have sufficient rights to access the remote node. In workgroup systems, if the credential format .\username does not work, use computer name\Username format to enter the credentials.

6.2 Agent deployment failed

In very rare occasions during periodic data collection, data collector agent deployment may fail. In this case, stop and delete the Windows service ABB.MCSDataCollectorAgentSvc in remote nodes and deploy the agent from the launch node again. To delete the service, open Windows command prompt with administrative privilege and run the command "**sc delete ABB.MCSDataCollectorAgentSvc**" without quotes.

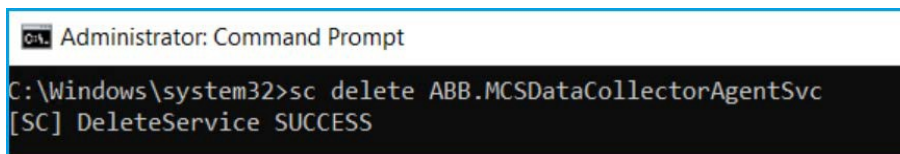


Figure 6.1: Delete service

6.3 Error message when .NET Framework is missing in the launch node

A certain, minimum .NET Framework version must be installed in the nodes as part of data collection. Refer to prerequisites section for more details. If MCS- DC is launched from a node where no .NET Framework is installed, or there is a version that is too old, an error message will pop up, as shown in the picture below.

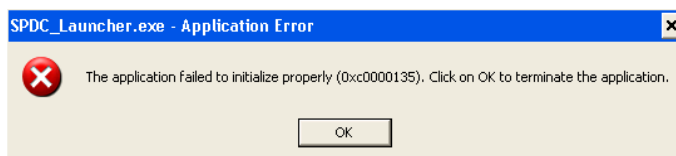


Figure 6.2: Error Message



For a complete list of .NET Framework versions compatible with each Operating System please consult your local IT department.

6.4 WMI access denied or failed to connect remote node

MCS-DC uses WMI API's to collect the data from configured nodes (local / remote) in the control system network. If WMI is not enabled in the firewall, MCS-DC will not be able to access the remote node and collect the data.

In case of WMI access denied error or failed to connect remote node error, check whether WMI traffic is blocked by the firewall. If the traffic is blocked, WMI needs to be enabled in the firewall. Refer to [Appendix K, How to check firewall settings for WMI](#) for more details.

6.5 WMI DCOM access denied

If an error event pertaining to elevated privileges for DCOM access appears in the local computer Windows event log, check whether the Windows security updates in that node are matching with other nodes in the network. If there is a mismatch, update all the network computers with the missing Windows security update. Such mismatch may cause WMI access denied error and the data collection from a remote computer will fail.

6.6 CBA online builder cannot print application which is using RTA board

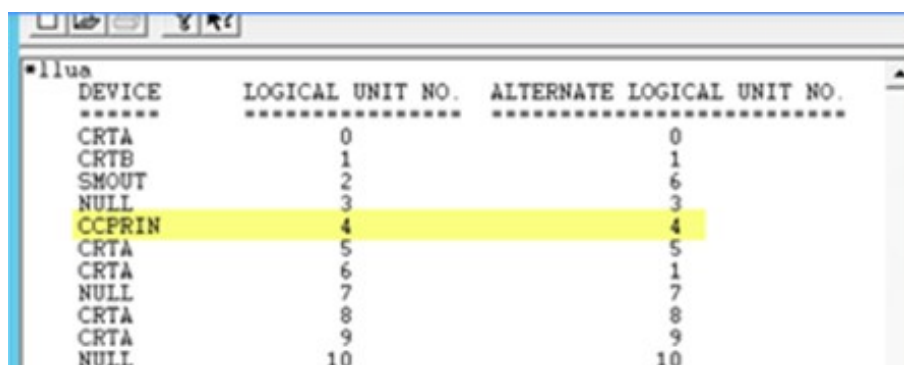
If a Masterbus 300 MCS-DC data collection is aborted of unknown reason, it is observed that the Control Builder A application can no longer be printed. To resolve this issue, follow the instruction below based on the configuration.

1. If redundant AC400 connectivity servers are used, restart one RTA unit at a time to solve the problem. Restart the first RTA board and verify that it is running again, then wait 5 minutes and perform the same action on the redundant RTA unit.
2. If a single RTA board is used, and it is not possible to restart the RTA unit, use the following workaround to correct the problem.

Start RTA Board Config in the concerned Connectivity Server and verify that Device CCPRIN has logical unit 4. To verify that the Logical Unit No 4 is allocated correctly, use the command LLUA.

See example below.

*LLUA



DEVICE	LOGICAL UNIT NO.	ALTERNATE LOGICAL UNIT NO.
CRTA	0	0
CRTB	1	1
SMOUT	2	6
NULL	3	3
CCPRIN	4	4
CRTA	5	5
CRTA	6	1
NULL	7	7
CRTA	8	8
CRTA	9	9
NULL	10	10

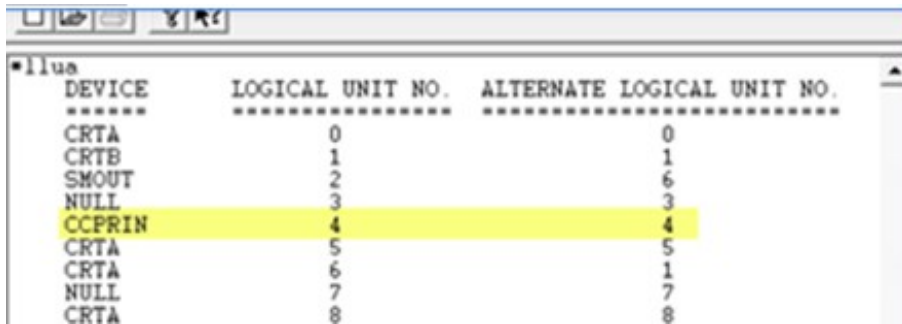
Listing of related documents

If CCPRIN is missing or doesn't have value 4, use the command ALU 4=CCPRIN to allocate logical unit 4 for CCPRIN

*ALU 4=CCPRIN

Verify that the Logical Unit No 4 is allocated correctly with the command LLUA.

*LLUA



DEVICE	LOGICAL UNIT NO.	ALTERNATE LOGICAL UNIT NO.
CRTA	0	0
CRTB	1	1
SMOUT	2	6
NULL	3	3
CCPRIN	4	4
CRTA	5	5
CRTA	6	1
NULL	7	7
CRTA	8	8

6.7 Connection with ICI module failed

A dedicated connection to ICI module is required to collect Harmony controller data. If this isn't the case, the controller collection may fail with an error message "ICI shared, other connection types not allowed". To avoid this situation, prior to the data collection, ensure that a healthy communication is established with the ICI module using S+ Control API ICI configuration utility. Refer to the screenshots below.

6 Troubleshooting

6.8 Invalid certificates cause the data collection window to hang.

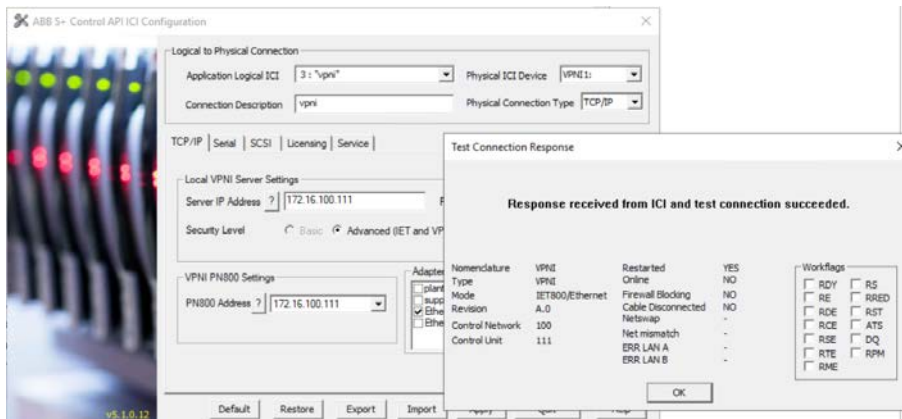
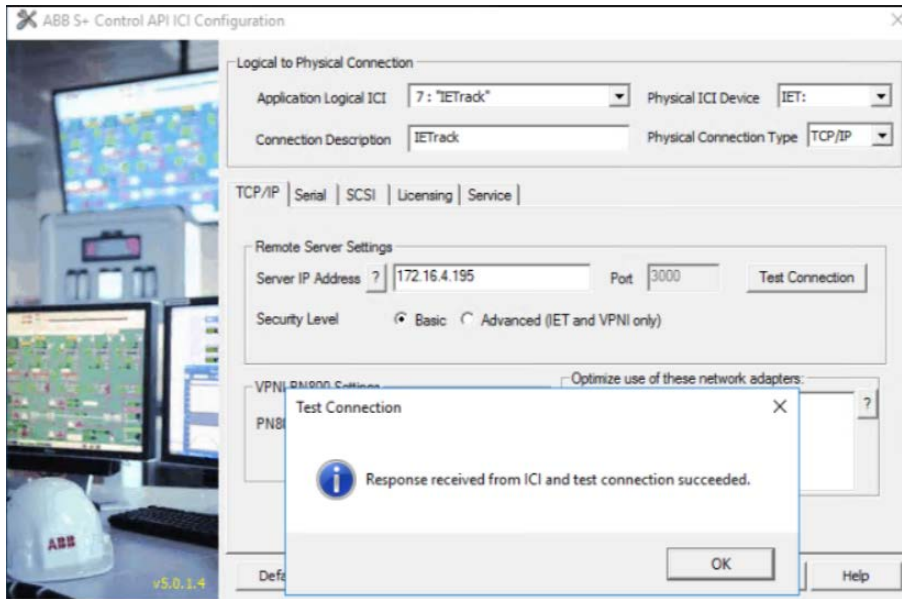


Figure 6.4: S+ Control API version above 5.0

Figure 6.3: S+ Control API version 5.0 and below

6.8 Invalid certificates cause the data collection window to hang.

An instant data collection may hang when secured communication is configured with invalid certificates. This results in no active controls, so the data collector cannot be stopped or exited. See the screenshot below.

6 Troubleshooting

6.8 Invalid certificates cause the data collection window to hang.

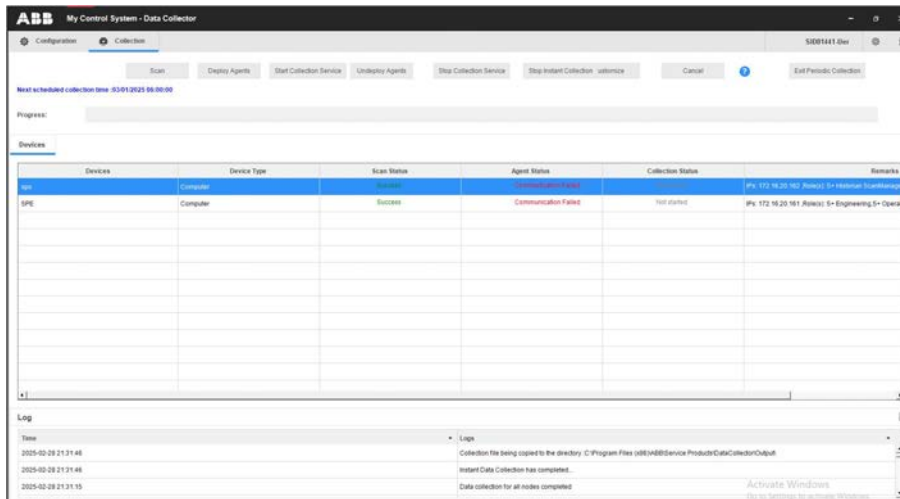


Figure 6.5: No controls are active

Follow these steps if such a situation arises.

1. Close the data collector window.
2. Open Windows services (type services.msc in the Run dialog box and press Enter) and stop the service ABB.MCSDDataCollectorSvc.

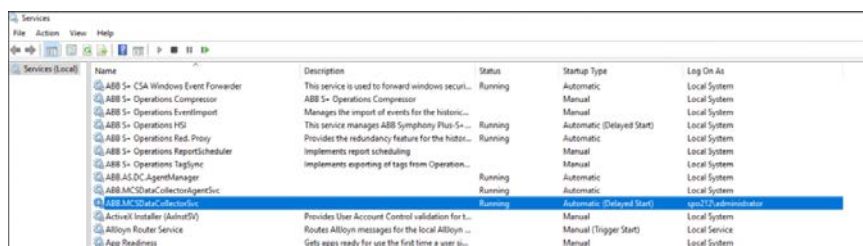


Figure 6.6: Stop the collector service

3. Start the data collector.



This situation is exceptional. Stopping services from Windows services list should not be performed under normal circumstances.

Appendix A How to change the default port number

MCS-DC uses port number 23571 as default. Should you need to use a different port, follow the instructions provided here. If MCS-DC detects that the port that is chosen is already in use, a notification is shown, asking to change the port number.

A.1 Basic Mode

1. In the Configuration screen click on the **settings** icon as highlighted in the below figure.

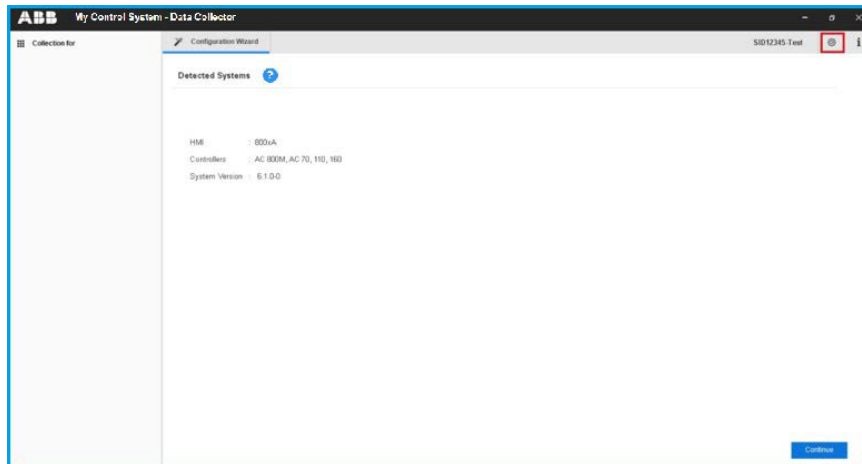


Figure A.1: Click On Settings Icon

2. As the settings screen appears, provide a new port number in the **Port Number** field.

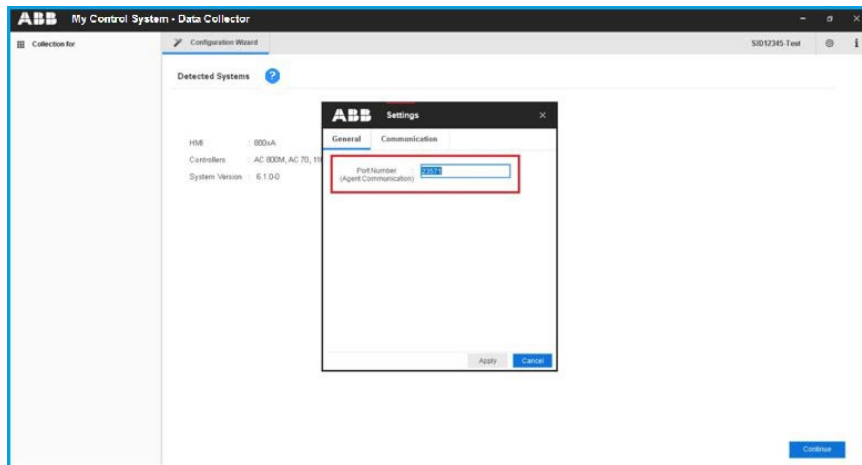


Figure A.2: Provide New Port Number

3. Click on **Apply** to save the changes.

A.2 Advanced Mode

1. In the Configuration screen click on the **settings** icon as highlighted in the below figure.

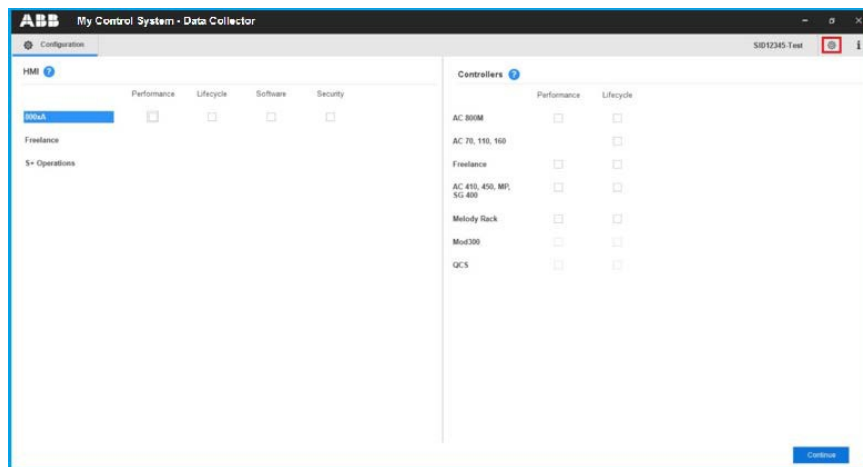


Figure A.3: Click on Settings Icon

2. Settings screen appears, provide a new port number in the **Port Number** field.

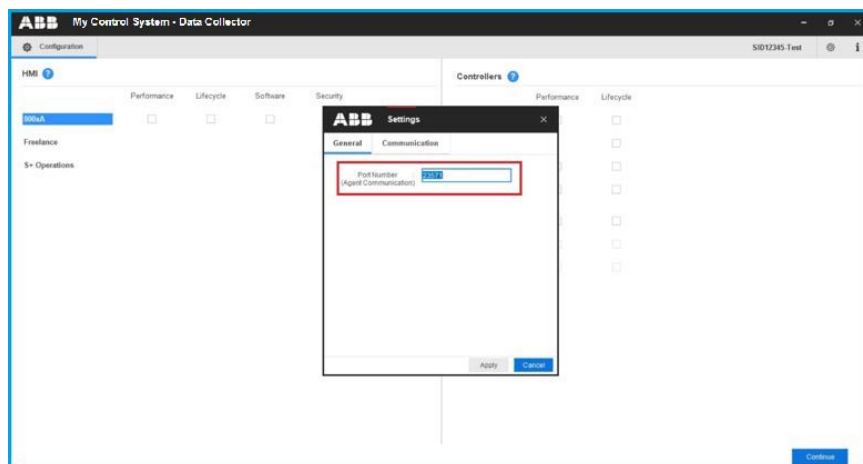


Figure A.4: Provide Port Number

3. Click on **Apply** to save the changes.

Appendix B Configuring Secured Communication

It is recommended to use the secured communication for data collection in order to maintain authentication, data protection and data integrity.

Please note, secured communication cannot be enabled if the .NET Framework version in the MCS-DC launch node is below 3.5. Please note, if secured communication is enabled in the MCS-DC tool, then all the computer nodes from which data collection has to be done should have a valid certificate for secured communication.

If the .NET Framework version on the MCS-DC launch node is above 3.5, MCS- DC tool does the below checks during the node scan.

- If secured communication is not enabled, a message is thrown during the node scan, saying “Secured communication is not enabled. It is recommended to use secured communication. Confirm to proceed without that”. User has a **Confirm** option to proceed with the node scan and **Cancel** option to abort the scan operation.
- If secured communication is enabled, user can proceed with the node scan.

Secured communication is established through digital certificates. As per the requirements, users can generate certificates in three different modes as mentioned below:

- Self-Signed Certificates
- Third Party Certificates
- Certificate Authority

Before proceeding with further steps for secured communication using certificates, user must obtain certificates from one of the above-mentioned modes or user should have a Certificate Authority Server configured and running.

Secured communication certificates should be installed in each node as mentioned below. Secured communication between MCS-DC launch node (server) and other nodes (client) in the network:

- Server certificate should be installed in MCS-DC launch node and client certificate should be installed in all the nodes in the network from where data need to be collected (including MCS-DC launch node).

Secured communication between MCS-FW (server) node and MCS-DC launch node (Client):

- Server certificate should be installed in MCS-FW node and client certificate should be installed in MCS-DC launch node.



Secured Communication is optional.



It is solely user's responsibility to obtain the certificates for secured communication.

B.1 Selection of Server Certificate

Refer the procedure below to select the installed certificates in MCS-DC launch node (Server) and all the client nodes in the network.

1. In the Configuration screen click on the **settings** icon as highlighted in the below figure.

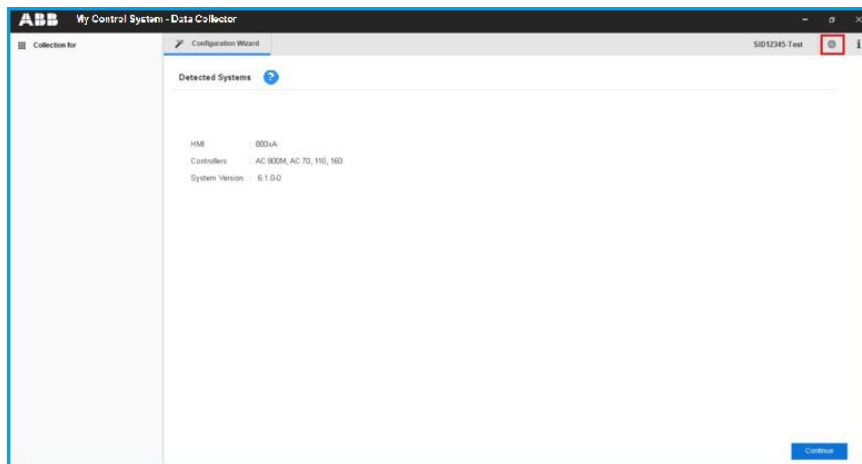


Figure B.1: Basic Mode

2. Settings screen appears, click on **General** tab. Enter the port number through which secured communication needs to be established.

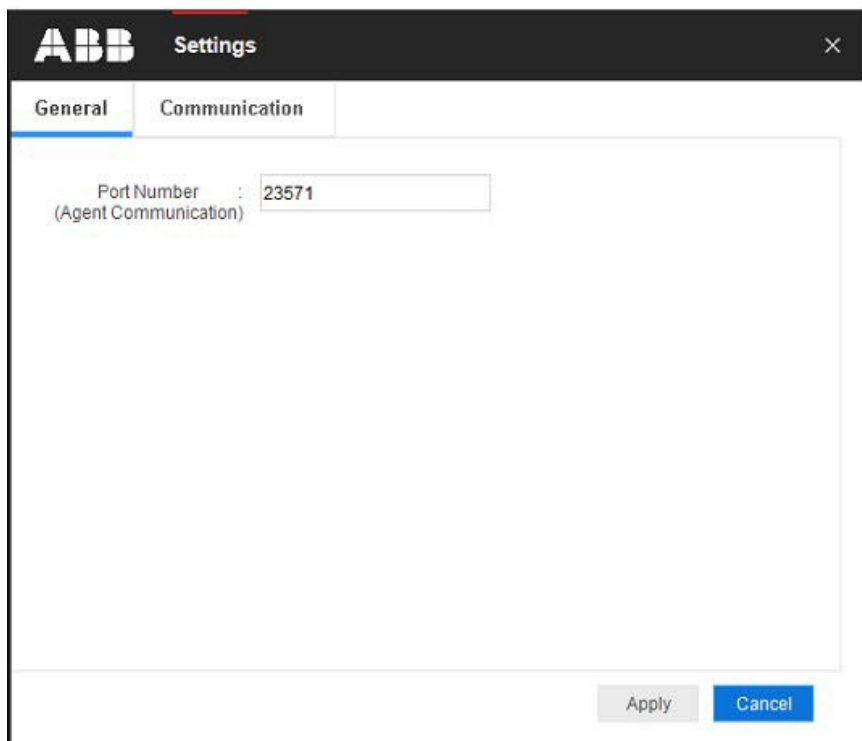


Figure B.2: Communication Port

- Settings screen appears, click on **Communication** tab.

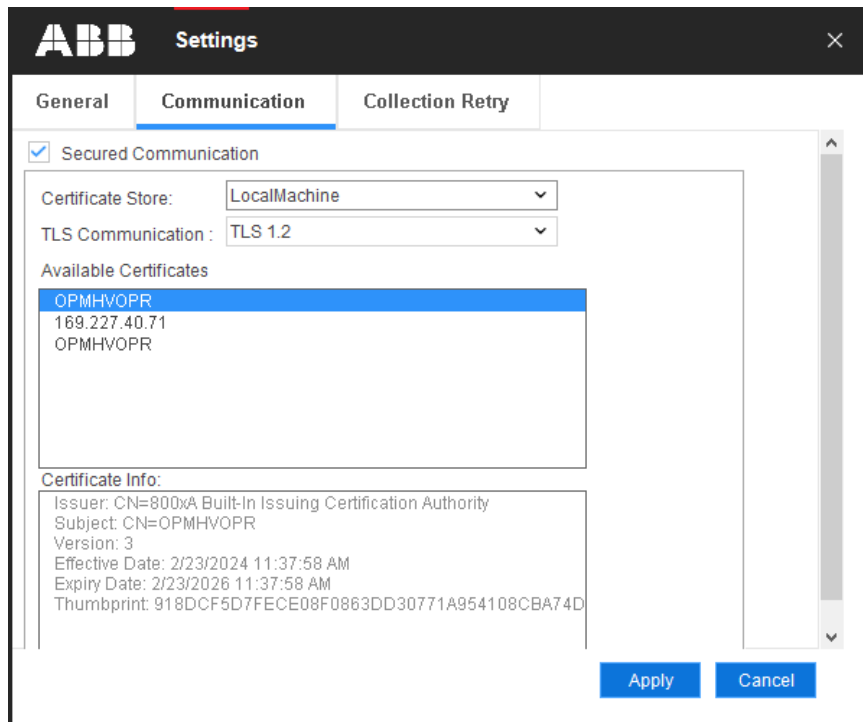


Figure B.3: Communication Tab

- Check the **Secured Communication** check-box. Select a relevant Certificate Store and TLS communication version. Selecting a Certificate Store shows available certificates in that store. Select a relevant certificate. Click **Apply** to save the changes. The IP address and port will be bound to the certificate automatically.

TLS version must be selected based on the installed .Net Framework version on a computer. Refer to the table below. It is important to note that not every TLS version is supported by all operating systems even if the corresponding .Net Framework version is present. For a complete list of TLS version support refer to Microsoft article

<https://learn.microsoft.com/en-us/windows/win32/secauthn/protocols-in-tls-ssl--schannel-ssp->



.NET Framework versions	TLS versions
3.5	1.0
4	1.0
4.5, 4.5.1	1.0 and 1.1
4.5.2, 4.6.1, 4.6.2, 4.7.1, 4.7.2 and 4.8	1.0, 1.1 and 1.2
4.8.1	1.0, 1.1, 1.2 and 1.3



If the same TLS version is not selected on both the client and server sides, secure communication will not work.



In basic mode, the highest TLS version is automatically selected on remote computers. Ensure that it matches with the TLS version selected on the host computer. If the highest TLS version is not compatible with the host computer operating system, switch the data collection to Advanced mode so that a lower TLS version shall be selected as desired.

B.2 Selection of Client Certificate

If the client certificate name is same as the name of the node where it is installed, the data collector agents will automatically detect the installed client certificate and use it for secured communication. If this is not the case, the user will have to select the Client Certificate in each node by following the procedure below.



If the HMI system is **S+ Operations**, before proceeding with the following steps, stop the service **ABB.MCSDDataCollectorAgentSVC** from the Windows services list in the node where client certificate is being selected. Once the client certificate has been selected, the service must be started again.

Run the utility **ABB.Services.UpdateClientCertificate** from the folder path *C:\Program Files (x86)\ABB\Service Products\DataCollector\Agent\Standalone\<Date>_<Time>* in the case of standalone data collection and *C:\Program Files (x86)\ABB\Service Products\DataCollector\Agent\Periodic* in the case of periodic data collection. This utility will be available only after deploying the collection agents to all the network nodes as part of data collection. After deploying the agents to all the nodes, go to each node and run the utility, select the certificate and then update configuration as mentioned in the figure below.

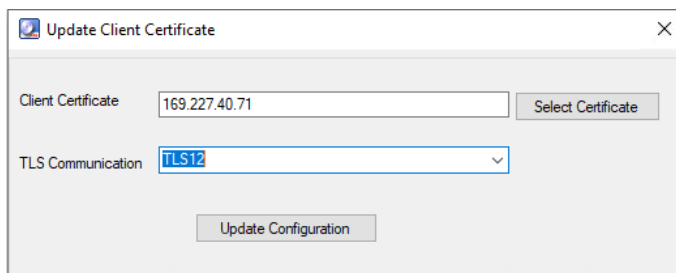


Figure B.4: Update Client Certificate

ABB Service Certificate Browser pop up appears, select option **Select Certificate from Local Store**.

Identify the intended client certificate and select it. Click OK.

B Configuring Secured Communication

B.2 Selection of Client Certificate

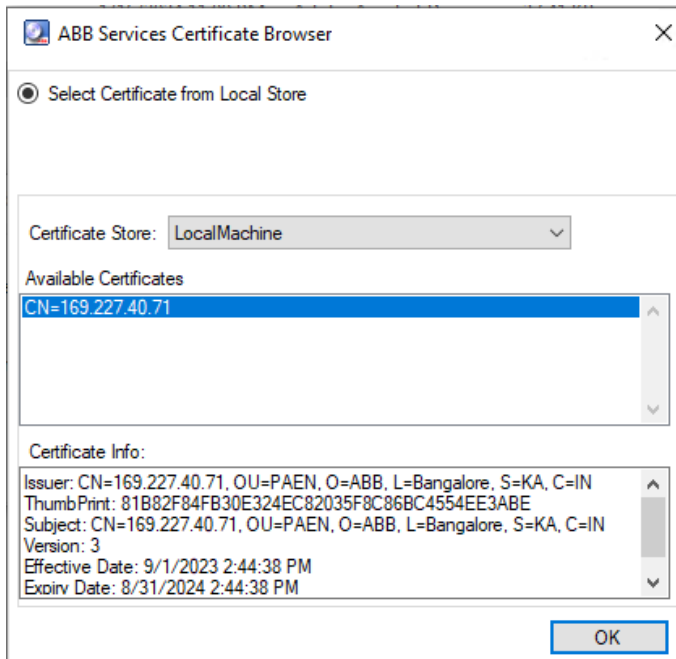


Figure B.5: Client Certificate



SSL agent communication might fail if 800xA configuration installs the License Service on a node where DC Agent is running with secure communication.

Appendix C Procontrol P13 source file (.csv) separators

The file location of P13 source file (.csv) is a mandatory input for P13 Lifecycle data collection. Please note that in the exported P13 source file the text separator must be double quotes ("), and the field separator must be a comma (,).

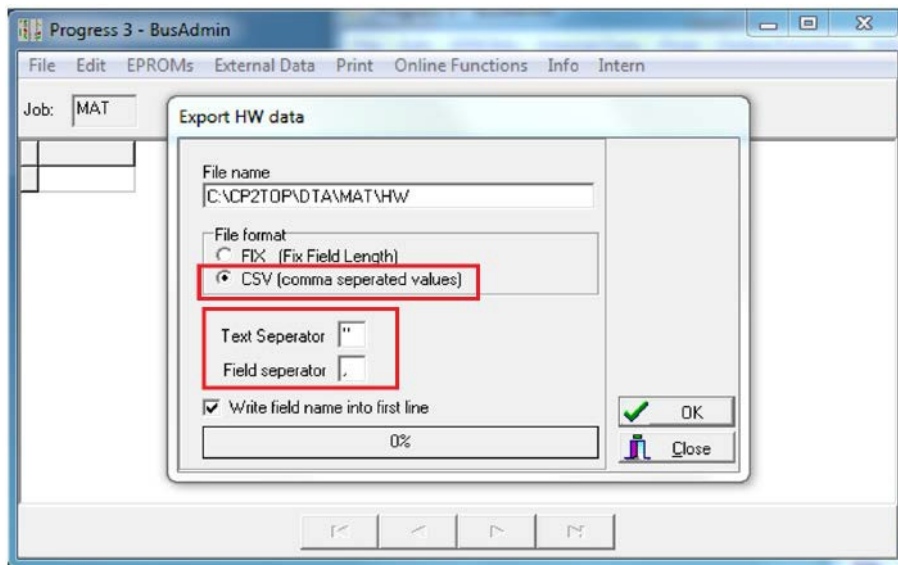


Figure C.1: Export HW data

Appendix D System configuration export

This section provides the procedure to export system configuration files that are required for data collection for various controller families.

D.1 Freelance System

This section provides a detailed explanation on how to export the Freelance system project configuration (structure) (file type *.csv or *.csvs), that is required for data collection.

1. In Configuration mode, select root node. Save project or any last changes done.

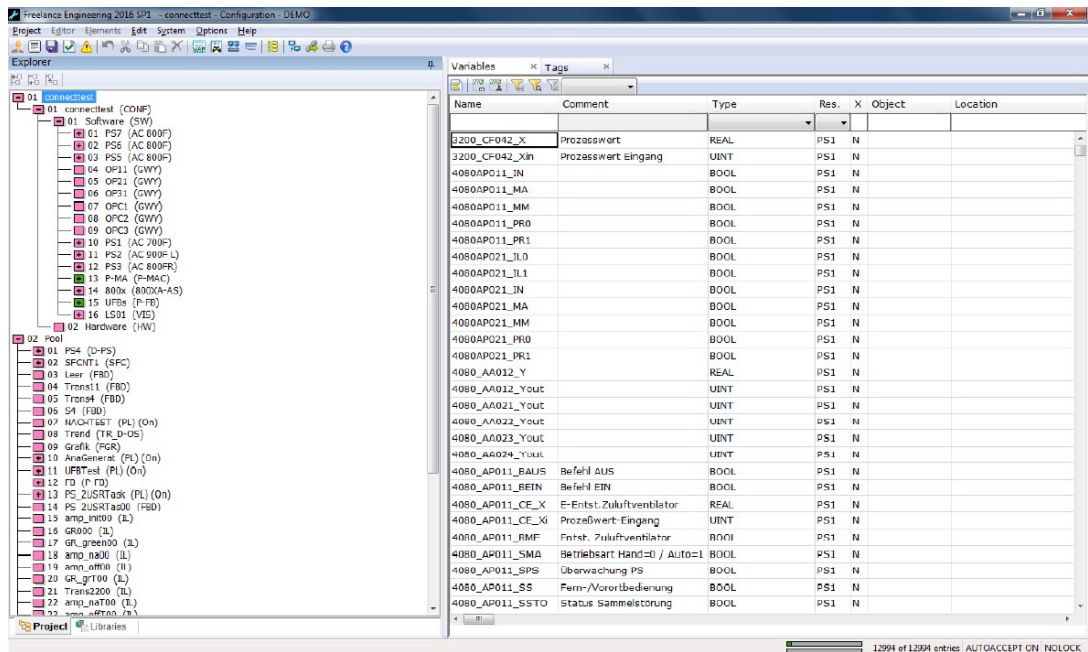


Figure D.1: Freelance Engineering 2016 sp1

2. Now from Project Tree Configuration mode go to menu item **Project > Project manager**. That brings to different window.

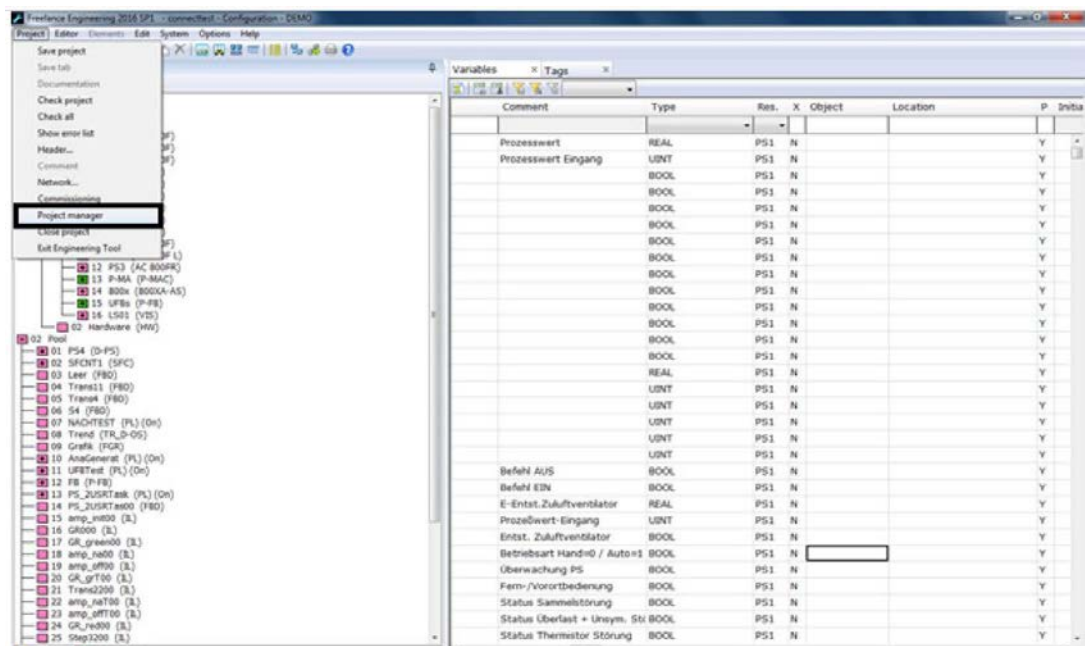


Figure D.2: Project Menu

D System configuration export

D.1 Freelance System

3. Under Manage project click on **Export** option.

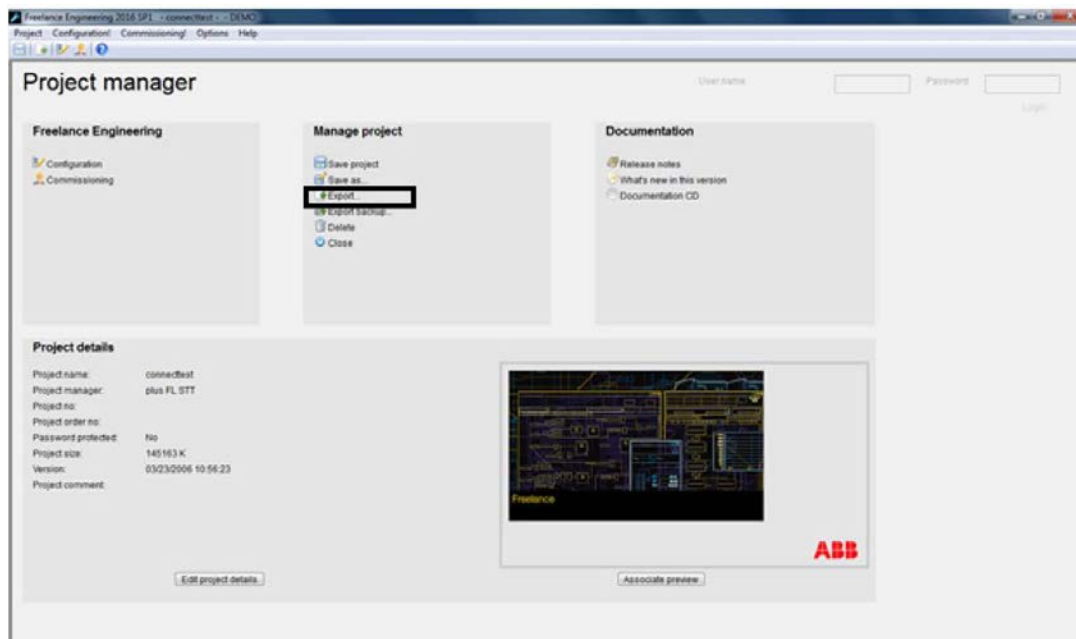


Figure D.3: Export option

4. Select the folder and file name for the backup .csv\ .csvs file to store.

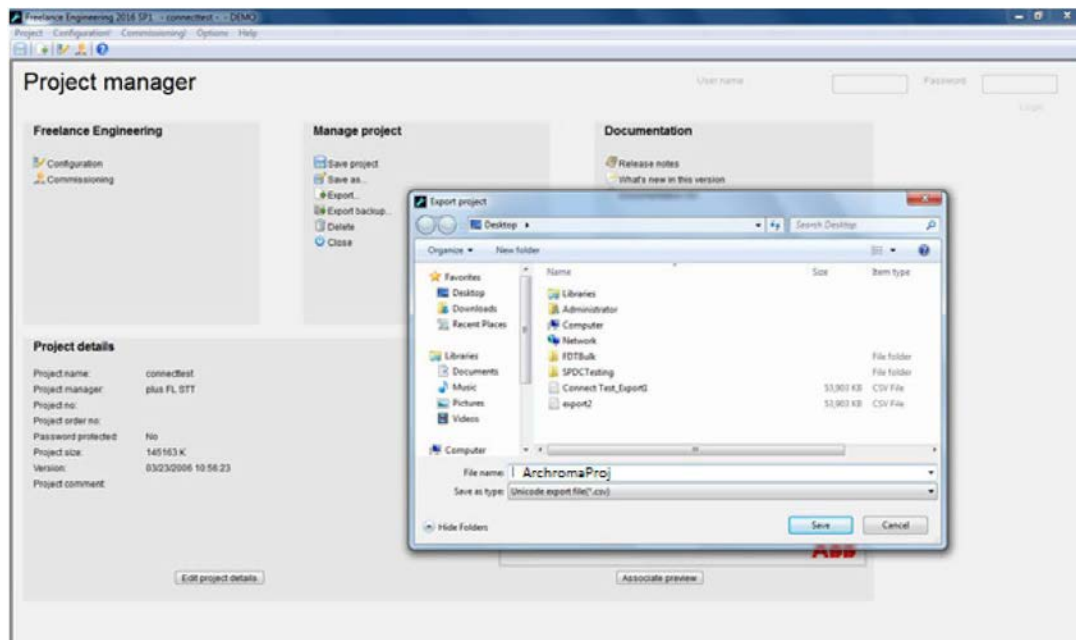


Figure D.4: Project manager tab

If the Project password is enabled in the freelance system, the export file type will be .csvs.

D.2 Advant MOD 300

This section provides the procedure about how to export the Advant MOD 300 System project configuration (structure) (ATF file) that is required for data collection.

1. Open **AdvaBuild Control Builder**.
2. Select and open the project.
3. To export project, go to menu **Object > Special Commands** and select **Save_ATF**.

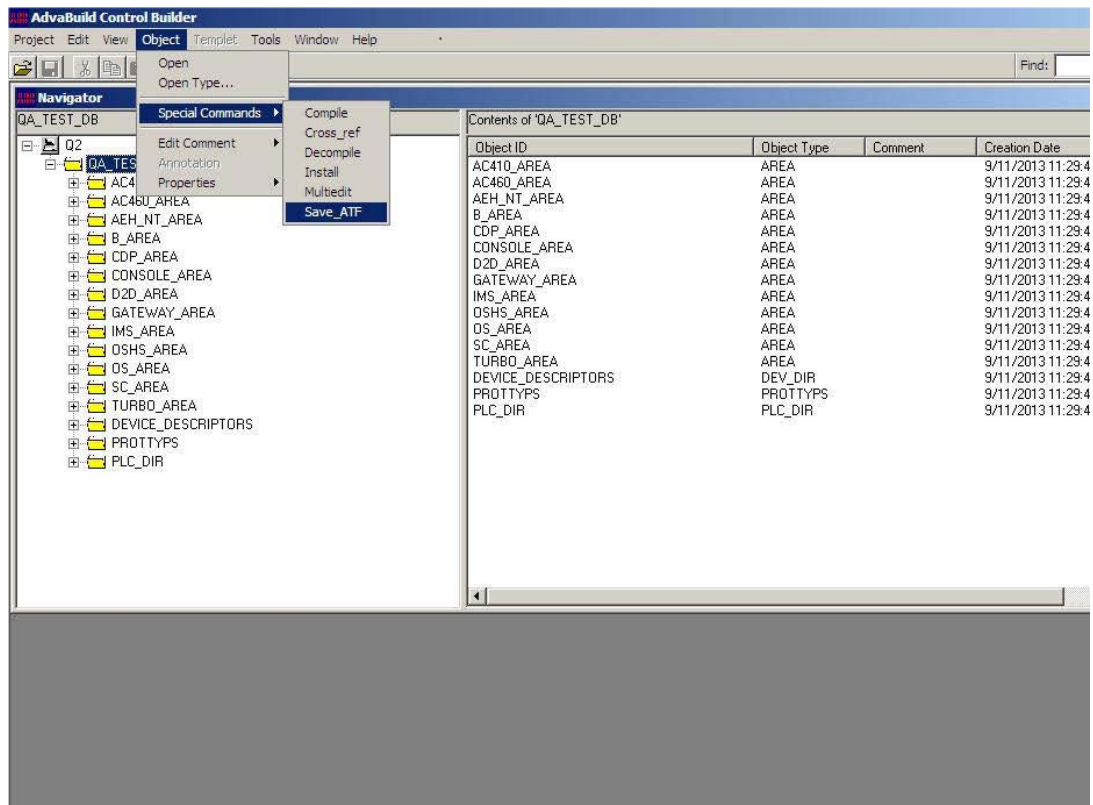


Figure D.5: Object Tab

4. This creates an ATF file. Save it, so that it is available for Installed Base Management.

D.3 AC100 System

Following is the procedure to extract the .bax file in a AC100 node:

1. Open application builder in AC100 node.
2. Select the desired controller node which is Online.

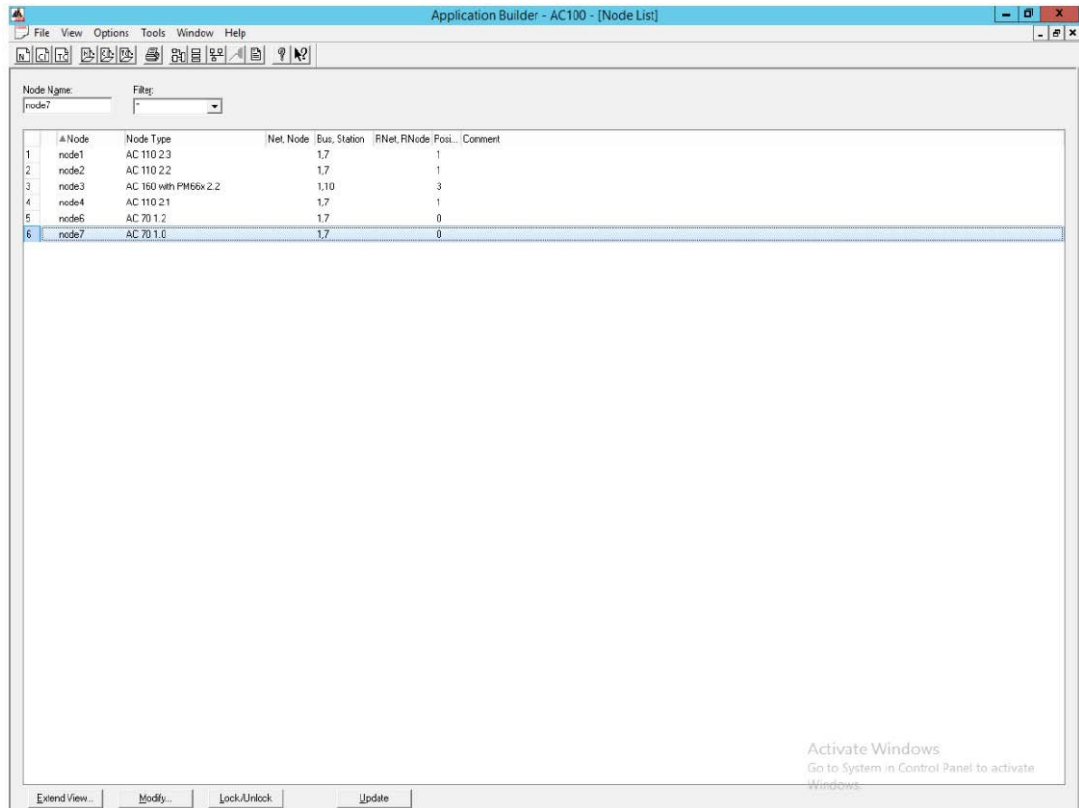


Figure D.6: Application Builder AC100

3. Right- click and open the function chart builder.

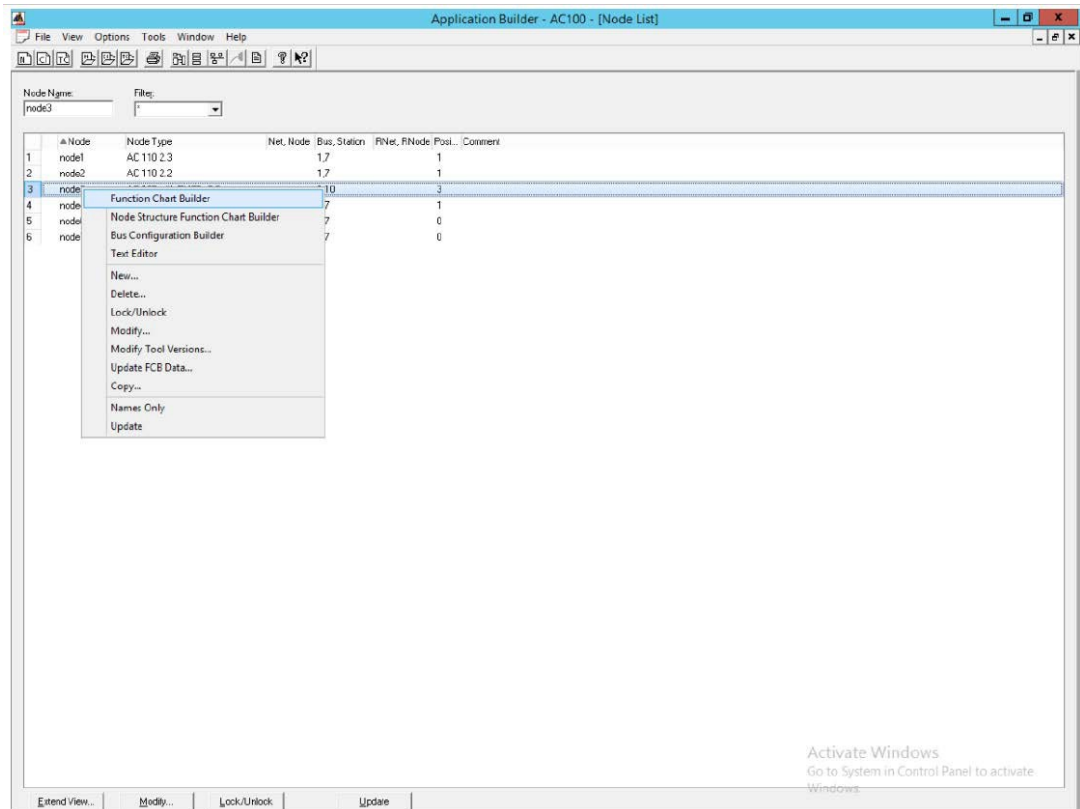


Figure D.7: Function Chart Builder

4. Once the function chart builder is opened, go to file and click on **generate source code**.

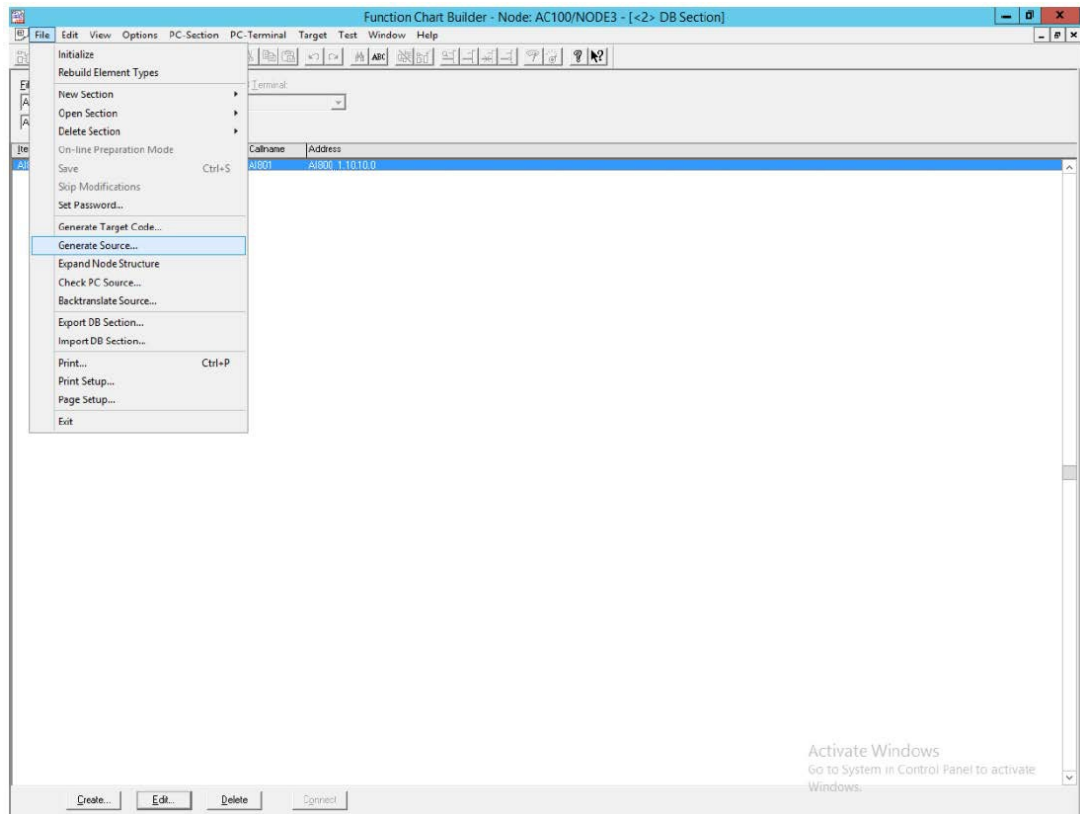


Figure D.8: Generate Source

D System configuration export

D.3 AC100 System

5. Enter the desired file name on the pop up which appears and click **OK**.

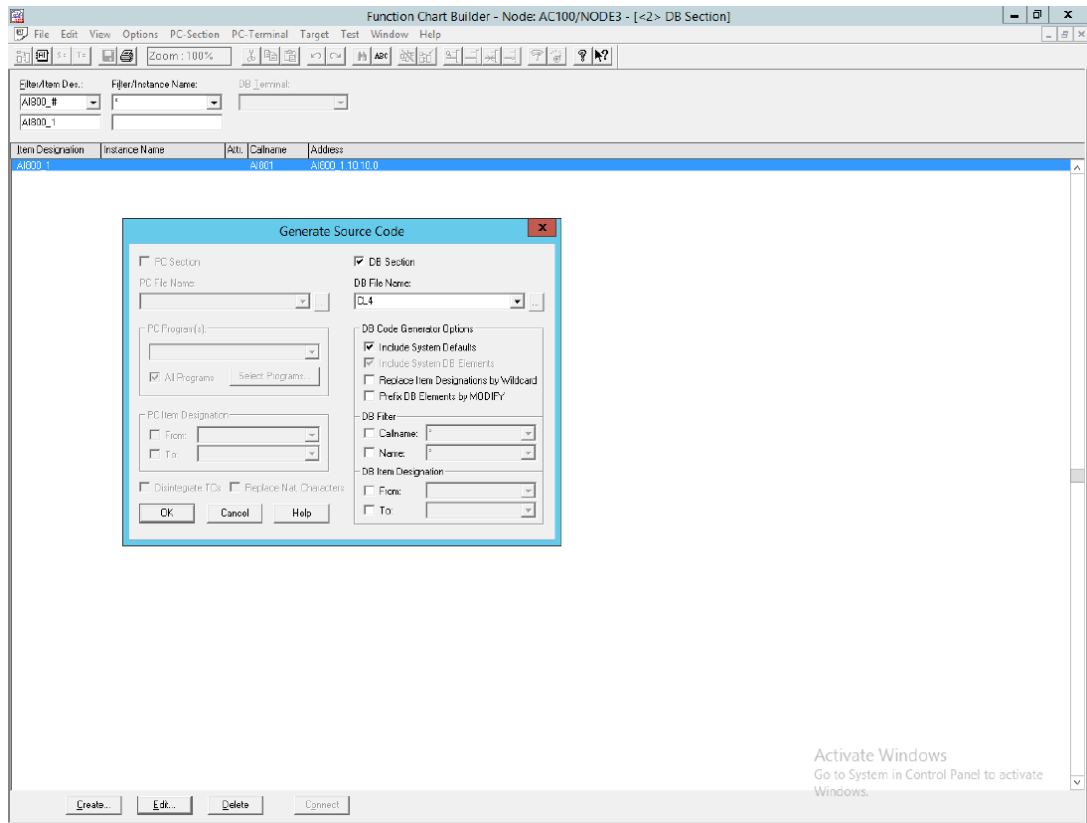


Figure D.9: Generate Source Code

6. The information of the nodes will be generated as DB source code. You will get a message that “DB source code generator finished successfully” in the function chart builder.

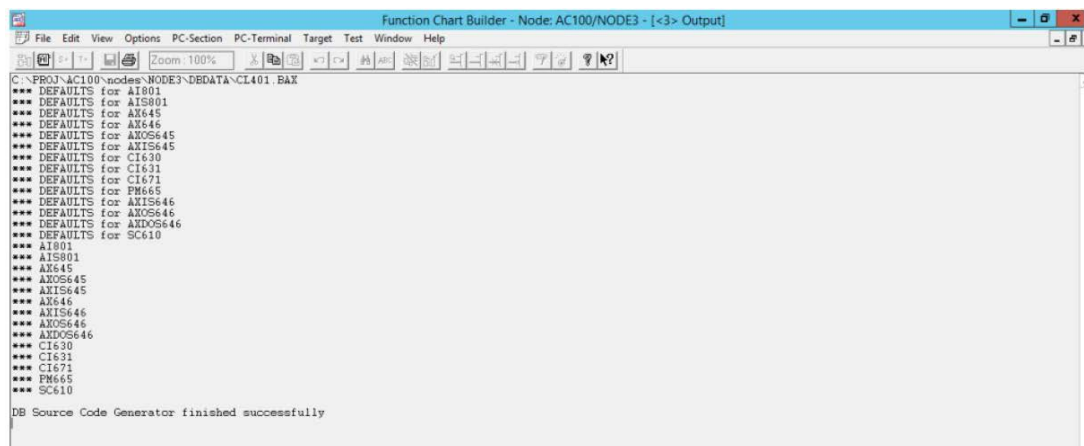


Figure D.10: Function Chart Builder - Node AC 100/NODE3

D System configuration export

D.3 AC100 System

7. This file will be saved in **C:\Proj\node\dbdata** as **.bax file**.

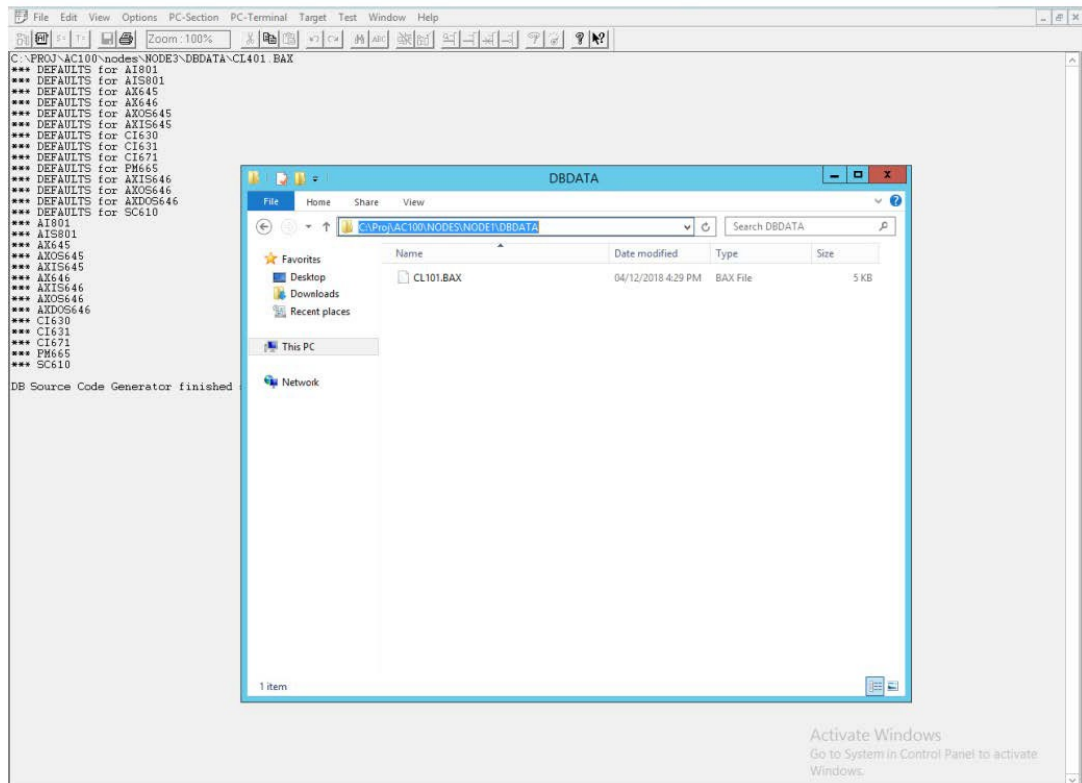


Figure D.11: Saved file path location

8. Figure shows the exported sample of .bax file with AC100 configuration details.

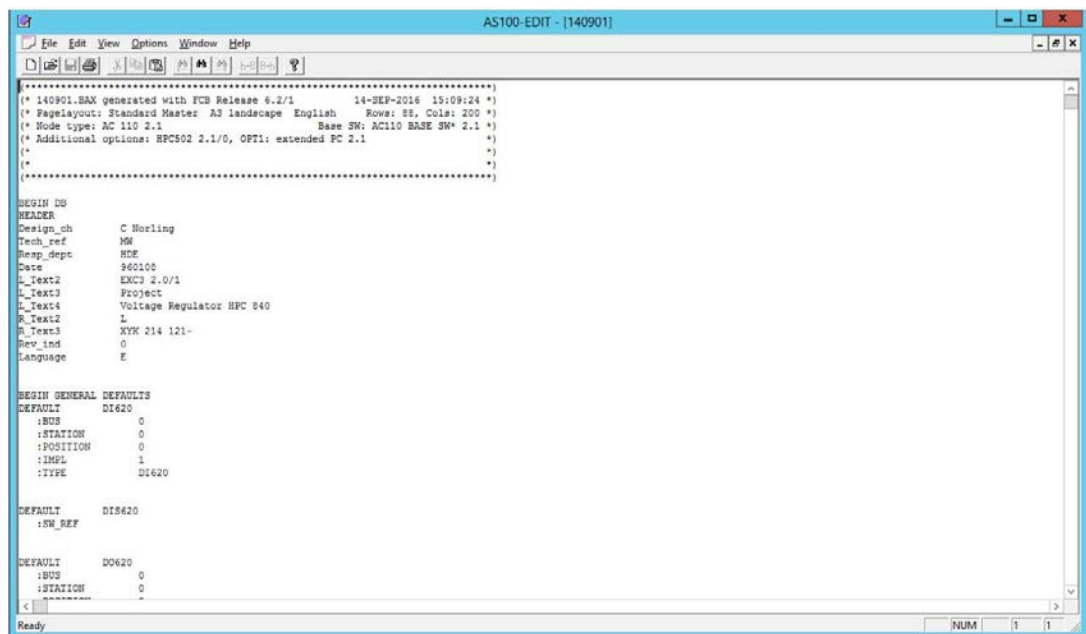


Figure D.12: Sample of .bax file with AC100 configuration

D.4 Melody Rack

This section describes various configuration files required for Melody control system data collection.

D.4.1 Melody Island Devices File

Procedure to obtain System Project Configuration or Melody Rack Island Devices file (file type *.csv with ';' delimiter)

Composer Melody Rack version 6.0 or later

Follow the procedure below if the Composer Melody rack version is 6.0 or later.

1. Open Composer and switch to **Project Structure** view.

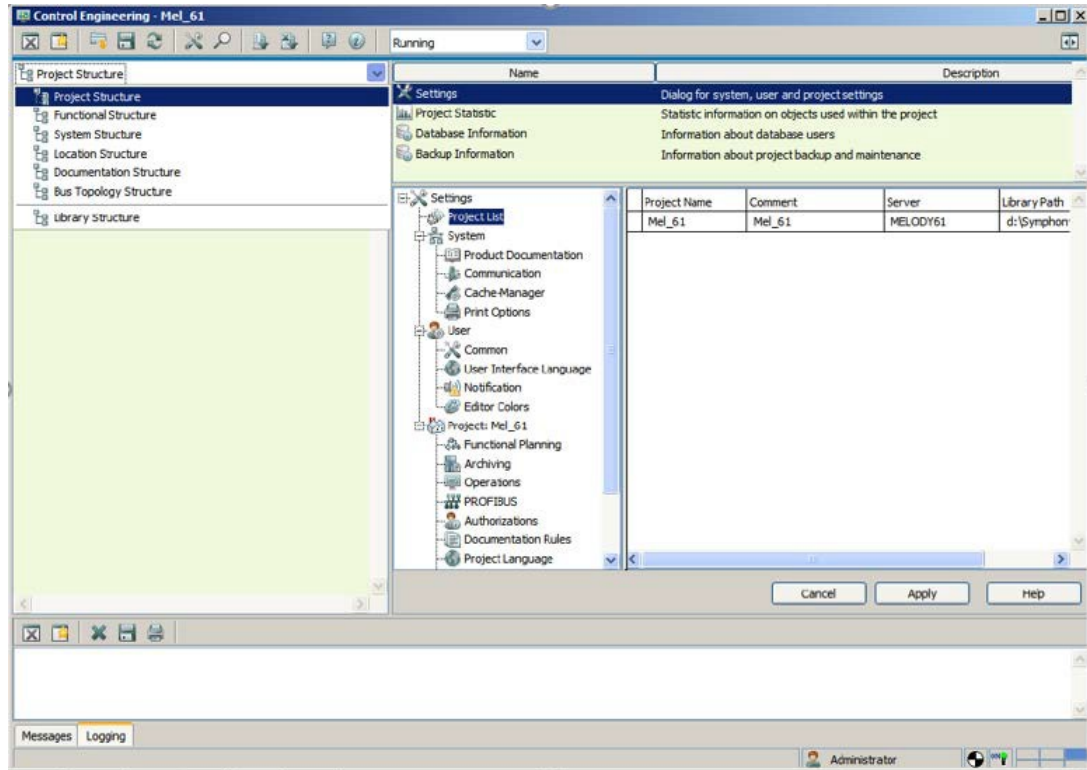


Figure D.13: Open Composer and switch to Project Structure view

2. Right-click on the project then select Open.

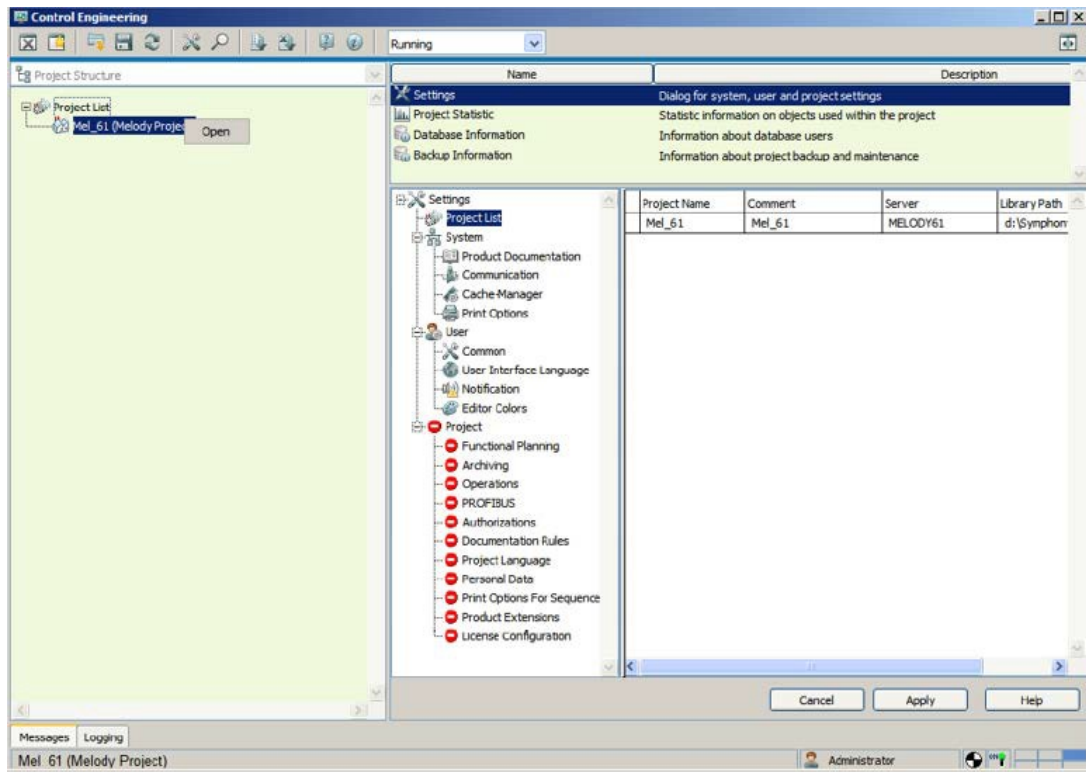


Figure D.14: Open the project

3. Select **Bus Topology Structure**.

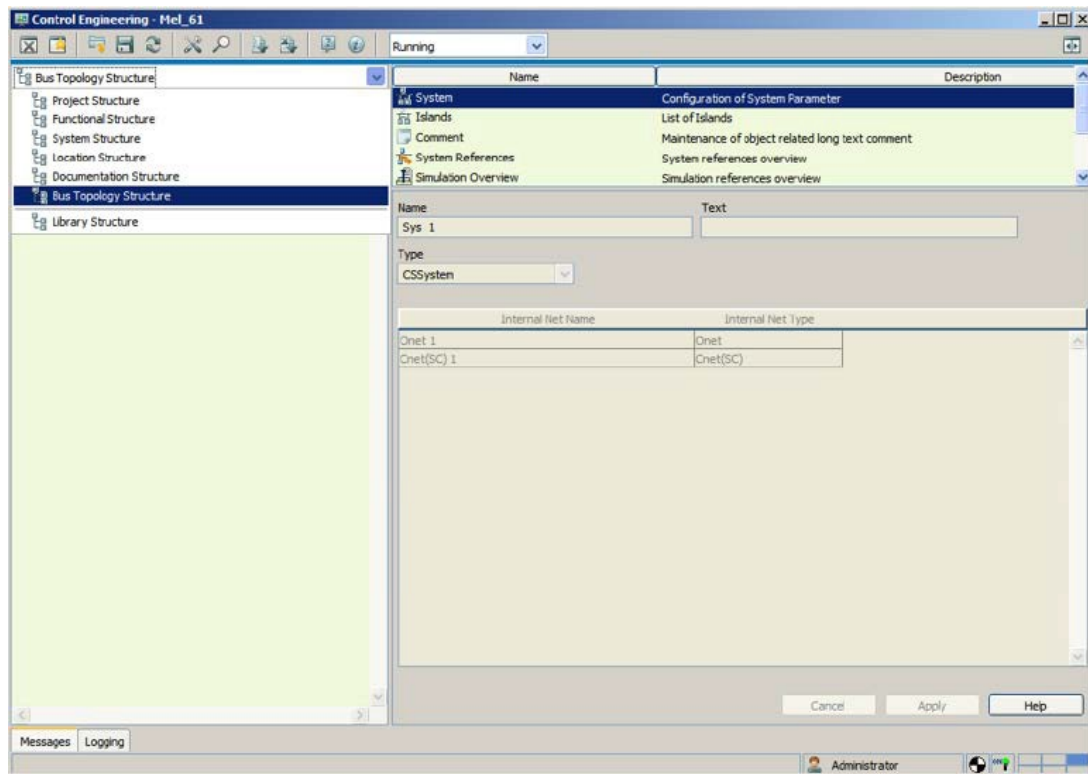


Figure D.15: Select Bus Topology Structure view

4. Right-click on the system and select **Export** then **Excel**.

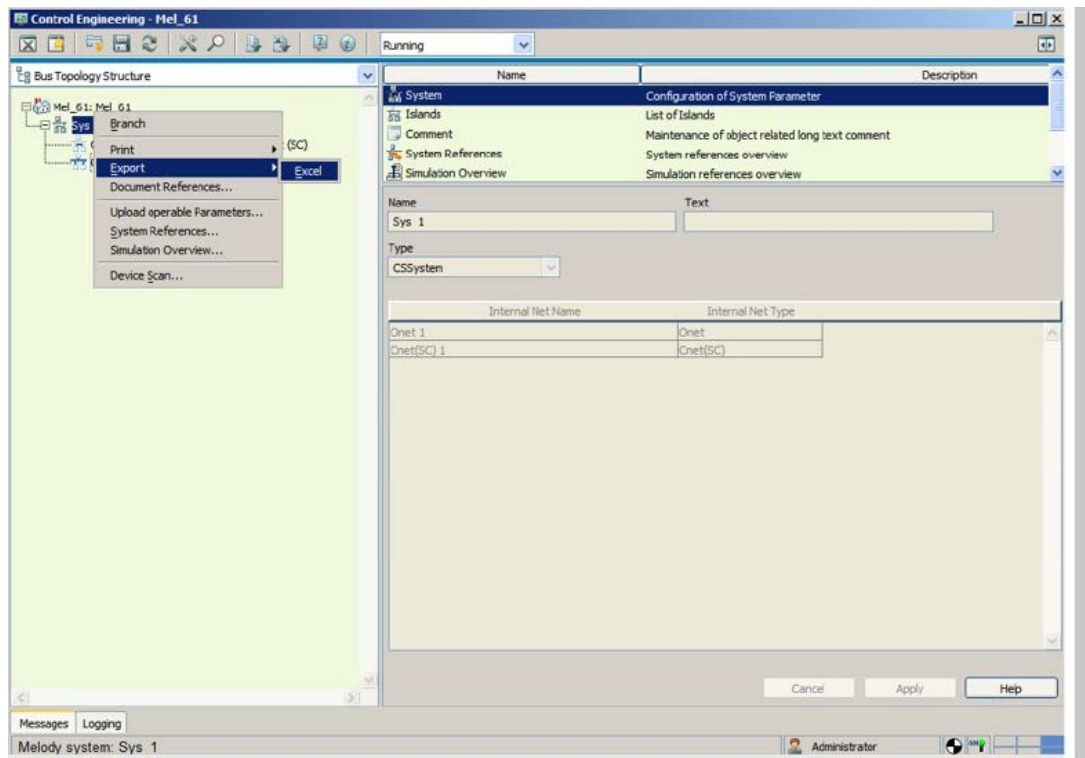


Figure D.16: Select Export to export in Excel

5. A window with multiple export format option opens. Select **CSV** option.

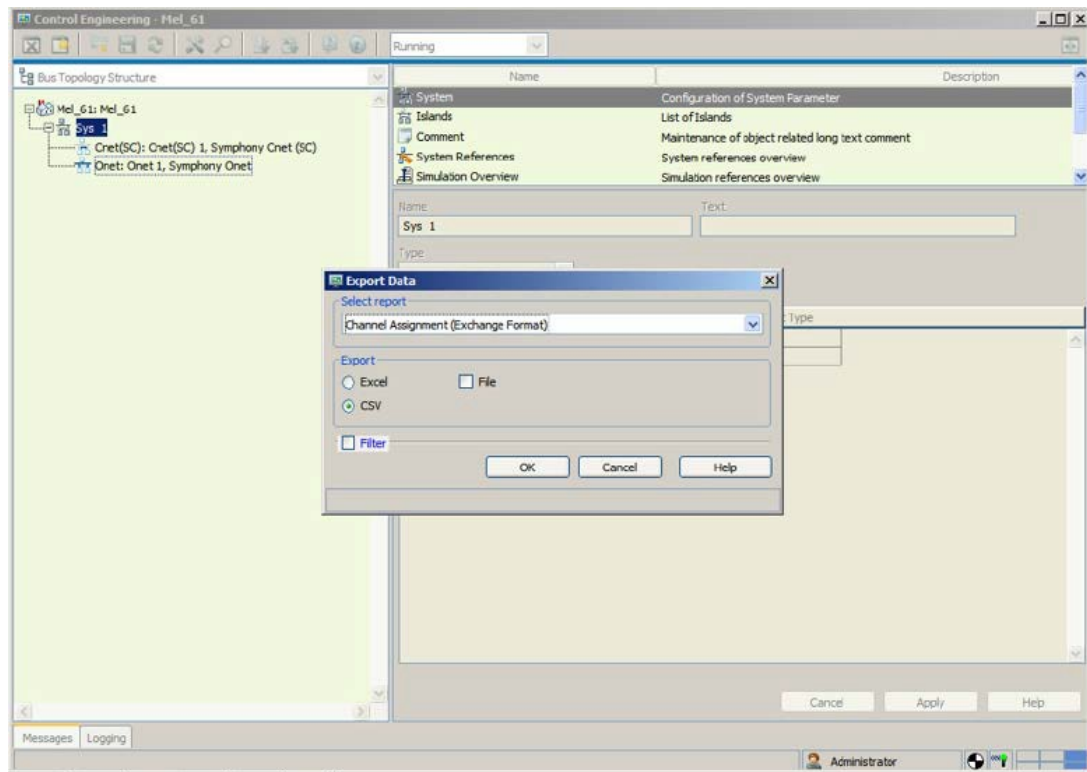


Figure D.17: Select CSV Option

6. Select **Bus Sharing Units** from **Select Report** drop down option and press **OK**.

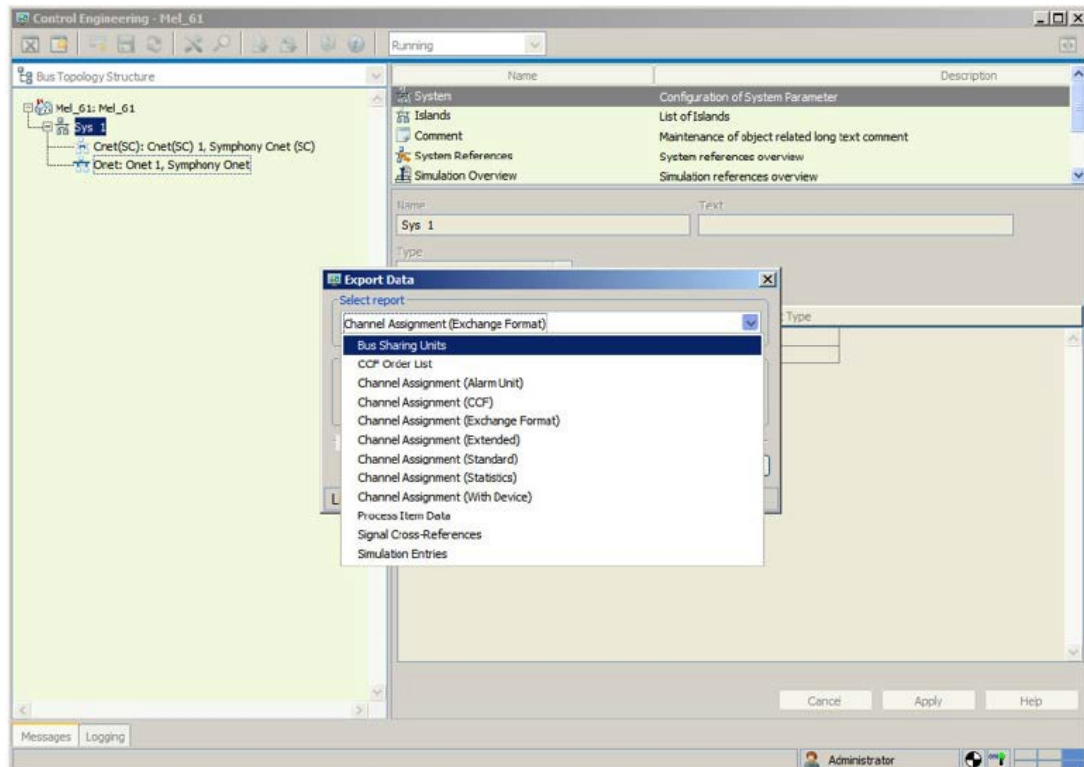


Figure D.18: Export Data Bus Sharing Units

7. This creates a **CSV** file. Once the CSV file is created, Save it.

Composer Melody Rack version 5.2 or earlier

Follow the procedure below if the Composer Melody rack version is 5.2 or earlier.

1. Open **Composer** and switch to **Project Structure** view.

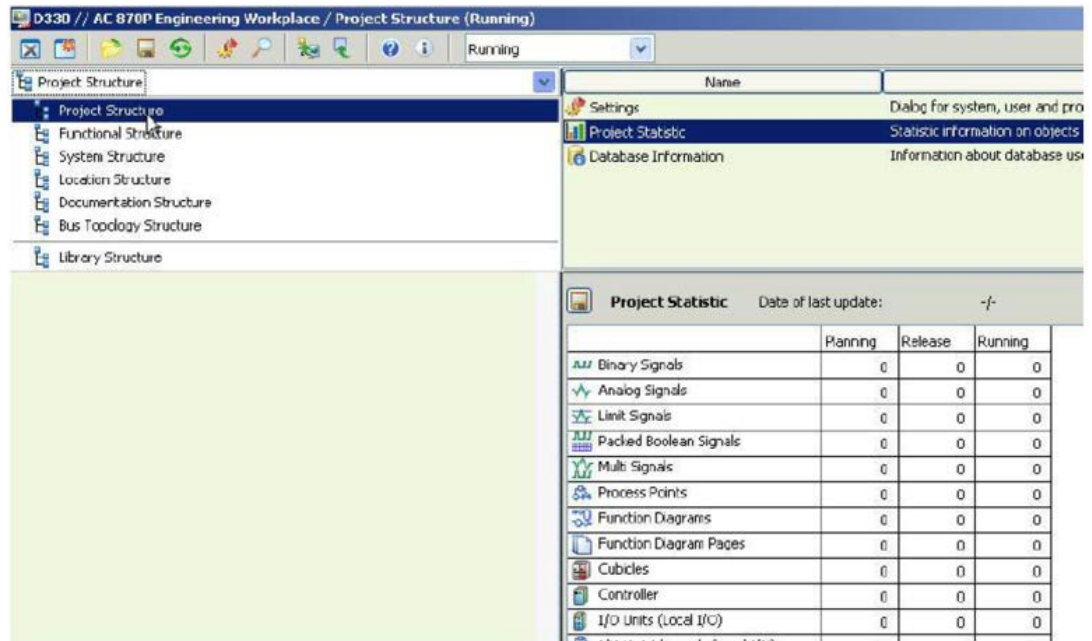


Figure D.19: Open Composer and switch to Project Structure view

2. Right-click on the **Project** then select **Open** to open customer's project.

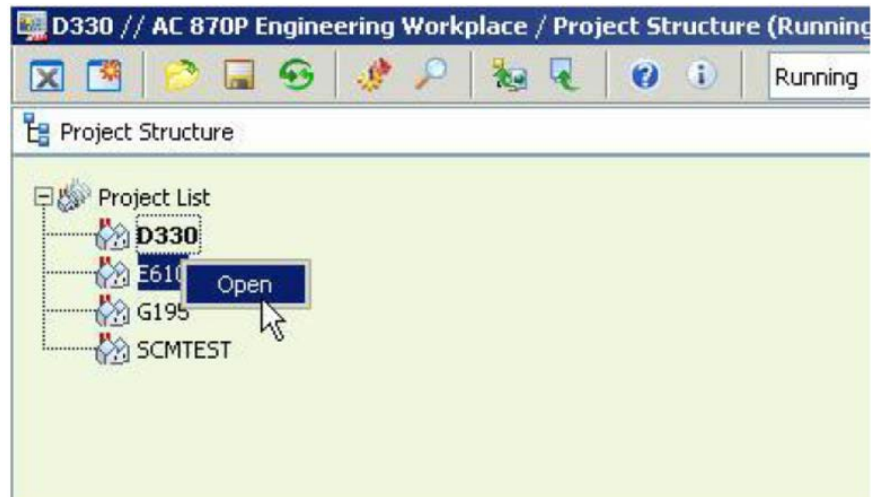


Figure D.20: Select Open to Open customer's project

3. If the project was already opened, the **Bus Topology Structure** view has to be selected.

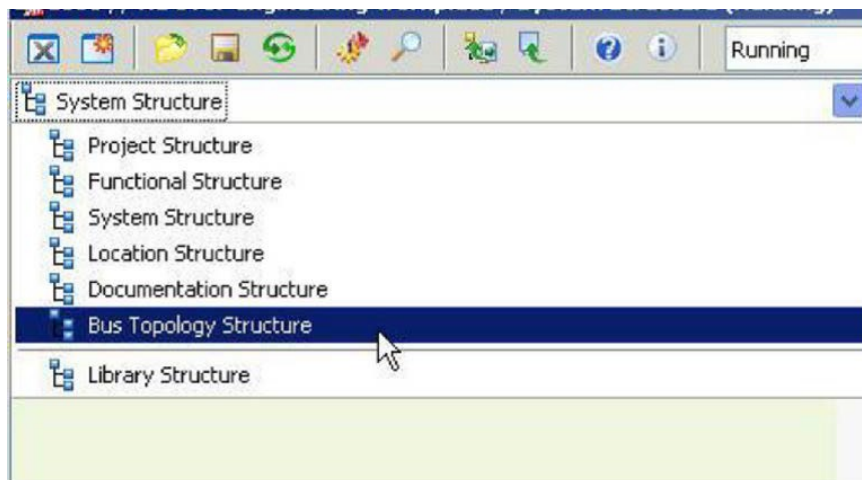


Figure D.21: Bus Topology Structure view

4. Right-click on the system and select Export then CSV.

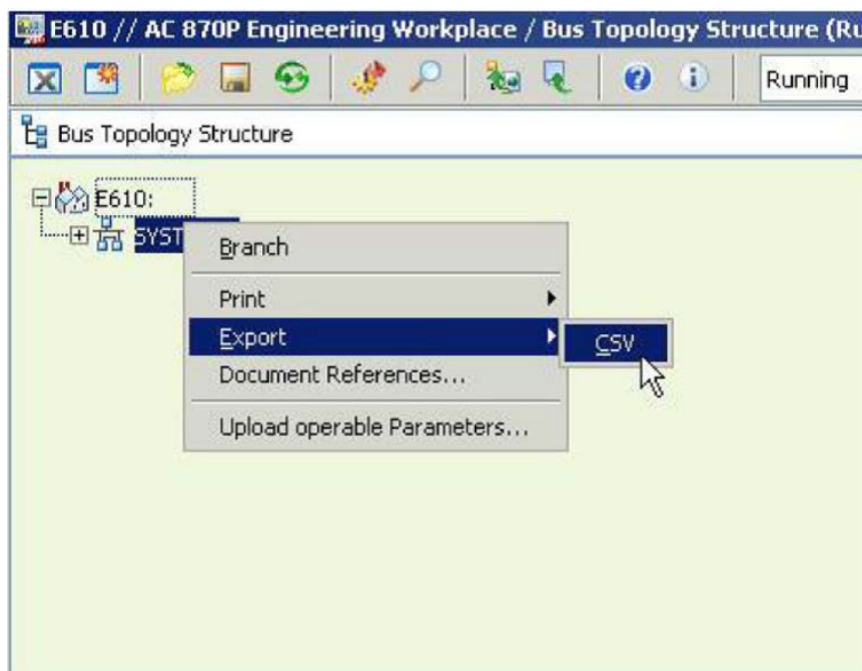


Figure D.22: How to export CSV

5. A window with multiple export format option opens. Select Excel for .csv.

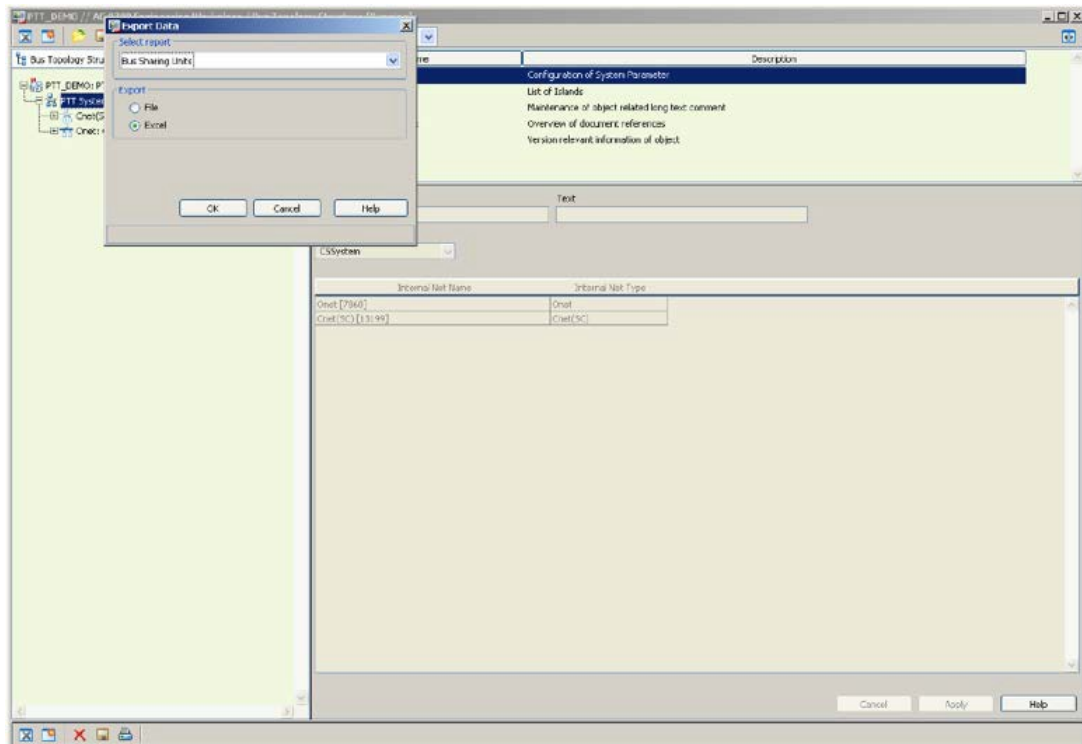


Figure D.23: .CSV file export option

6. A window opens where the Bus Sharing Units report needs to be chosen.

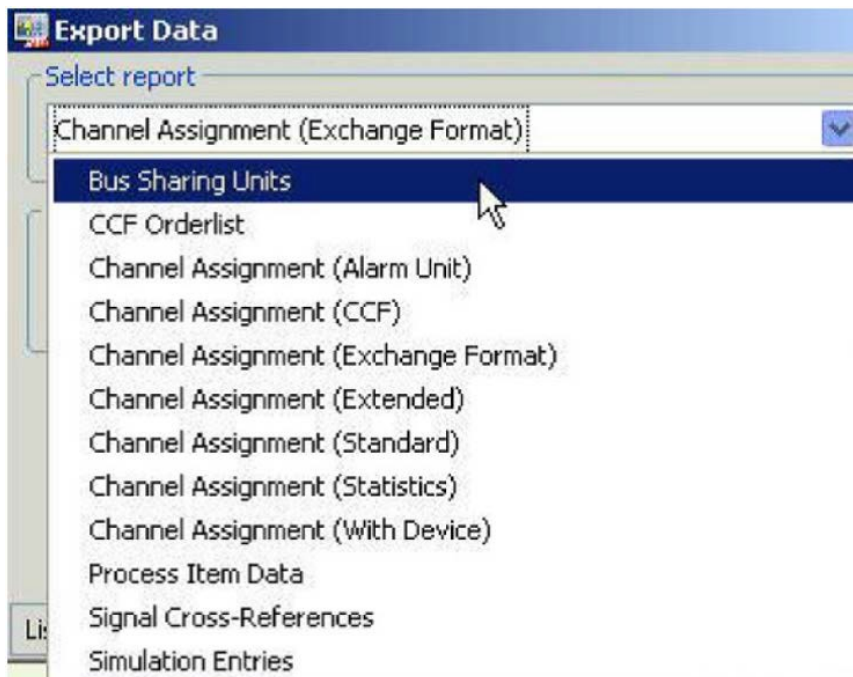


Figure D.24: Choose Bus Sharing Units report

7. Select **Excel** option for .csv. Provide desired path and file name to export the configuration.
8. This creates an .csv file. Once the .csv file is created, save it.

D.4.2 Melody CSE_Conf File

CSE_Conf file contains the EPC and IP addresses of all the modules part of the system. It must be exported from Composer Melody Rack too. It is stored in the below path.

C:\Program Files (x86)\ABB Symphony Plus\Engineering\Composer Melody Rack

Or in

C:\ProgramData\ABB Symphony Plus\Engineering\Composer Melody Rack



The folder **ProgramData** is hidden, choose Show hidden files option in Windows to view the files.

D.4.3 Asset structure export

1. Open Composer and switch to **Project Structure** view.

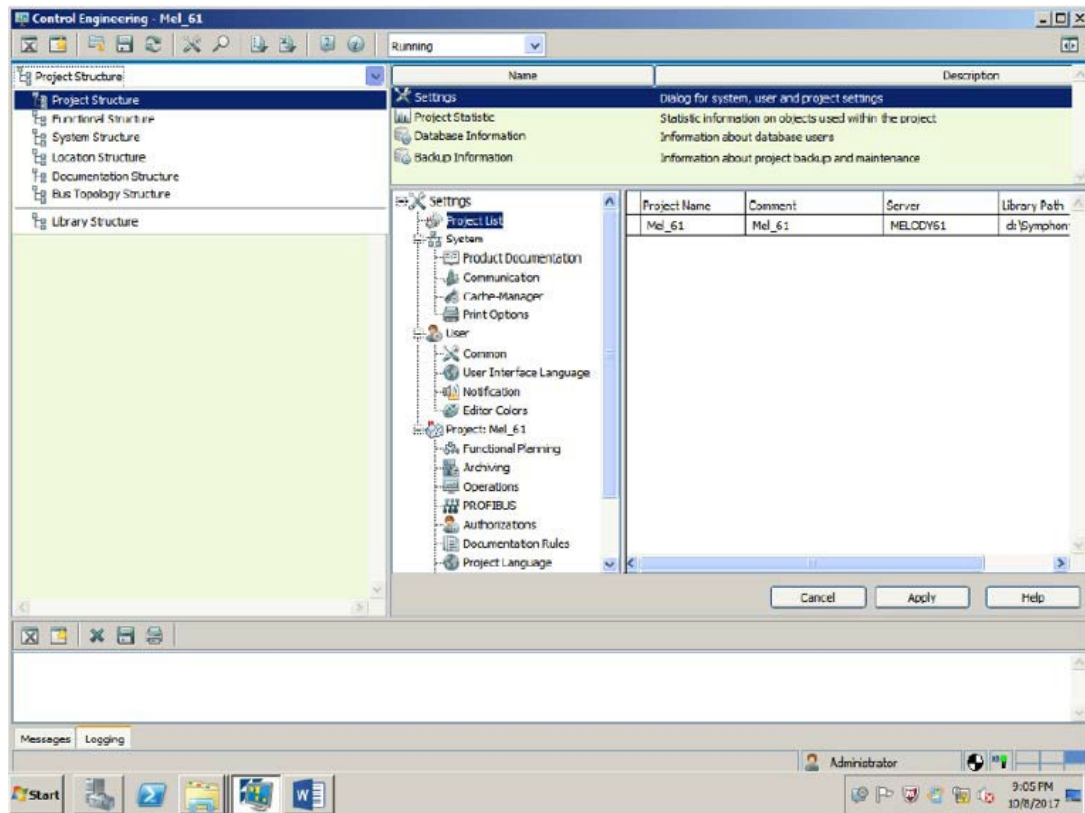


Figure D.25: Project Structure View

2. Click on **Settings**, to get the below window. Under Working Directory, select the location for saving the asset structure.

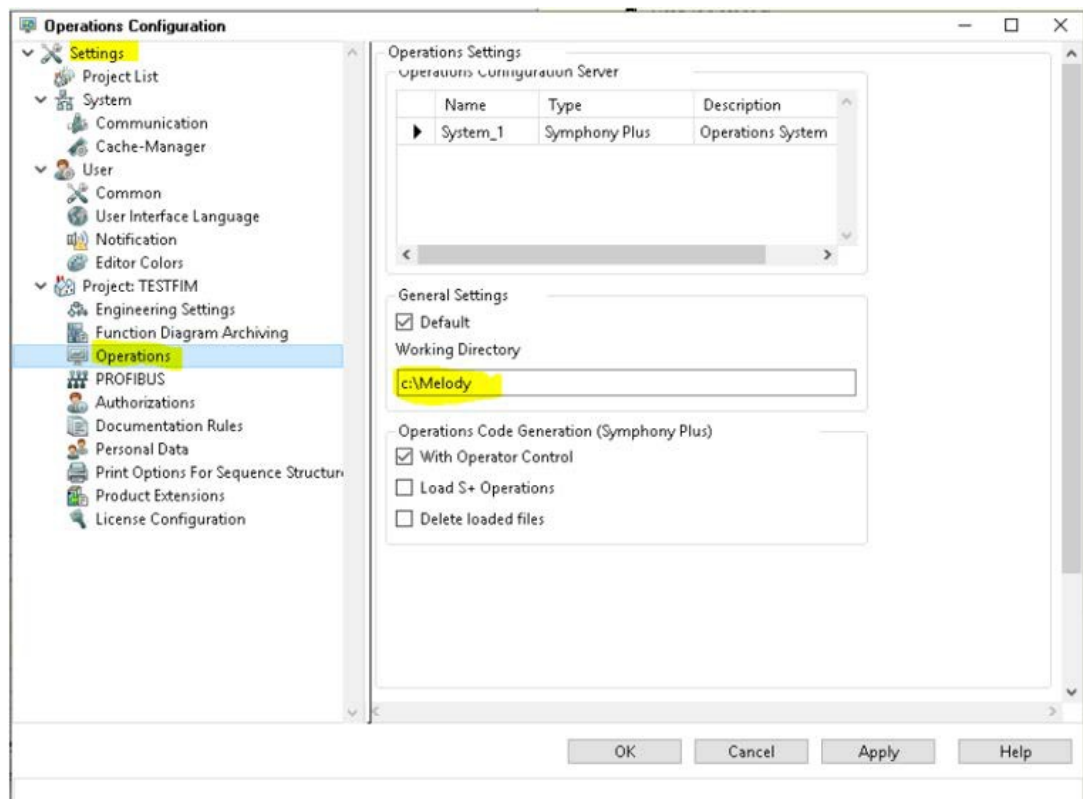


Figure D.26: Operations Configuration Window

3. Select system structure and click on **Export** to export the assets.

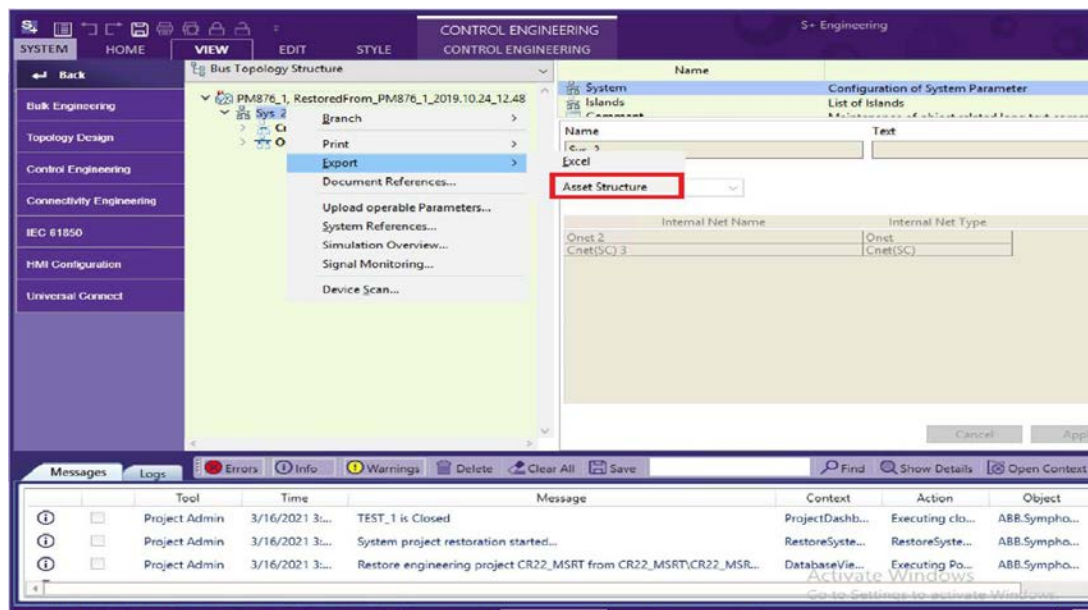


Figure D.27: Export the asset from system structure

4. Once exported, assets will appear as shown in the following image.














Name	Date modified
 Station EP204A09-Assets.xml	25/03/2019 14:41
 Station 01C05 (CMC60 102)-Assets.xml	25/03/2019 14:41
 Station 01G09 CMC70_103-Assets.xml	25/03/2019 14:41
 Station 04A09-Assets.xml	25/03/2019 14:41
 Station 06C09 S800 DPV1-Assets.xml	25/03/2019 14:41
 Station 08A09 PM877 Migra.-Assets.xml	25/03/2019 14:41
 Station 10A09 Turbotrol-Assets.xml	25/03/2019 14:41
 Station 11A09-Assets.xml	25/03/2019 14:41
 Station 13A (PM875-2 FW207)-Assets.xml	25/03/2019 14:41
 Station EP204C09-Assets.xml	25/03/2019 14:41
 WTM50A-Assets.xml	25/03/2019 14:41
 WTM50B-Assets.xml	25/03/2019 14:41
 WTM50C-Assets.xml	25/03/2019 14:41

Figure D.28: Exported Assets



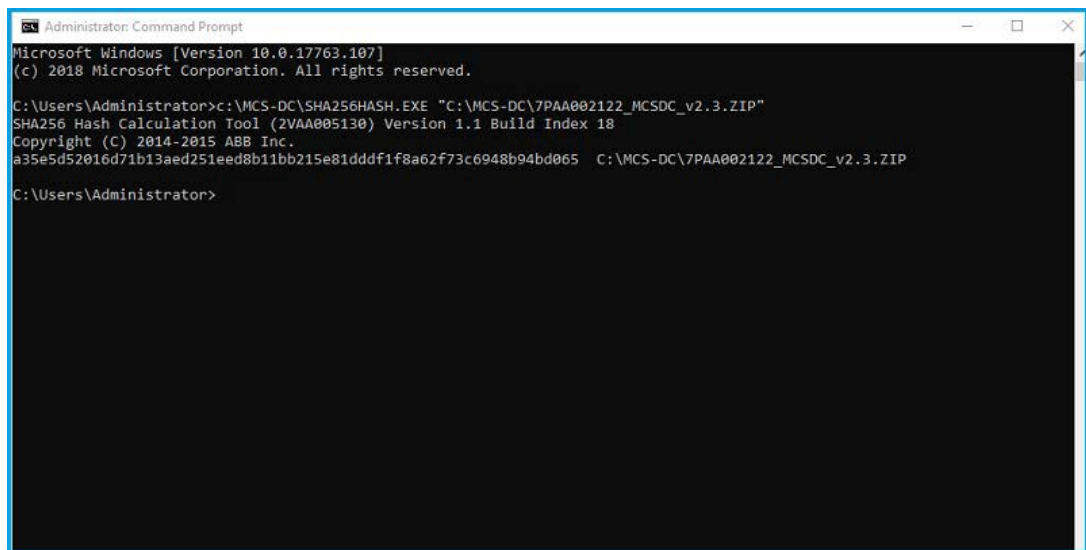
Asset structure export option is not available for Symphony Plus system in Composer version 7.0 SP1 and SP2.

Appendix E SHA256 Hash verification

ABB has created a tool (digitally signed) that can be used to calculate the SHA256 Hash. The tool, **2VAA005130.zip** (Symphony Plus SHA256 Hash Calculation Tool Version 1.1.0) can be downloaded from ABB library. This is by no means mandatory, it is an additional check that is up to the user.

To run the tool, perform the following steps:

1. Extract the file SHA256HASH.exe to the desired directory. In this case it is **C:\MCS-DC\SHA256HASH.EXE**
2. Copy the MCS-DC zip file downloaded from My Control System (MCS) portal or ABB library, to the desired directory. In this case it is **C:\MCS-DC\7PAA002122_MCSDC_v2.xx.ZIP**.
3. Click the Start button. In the Search box, type Command Prompt or cmd, and then press Enter, wait for the command prompt window to open.
4. Type the following command in the command prompt
C:\MCSDC\SHA256HASH.EXE "C:\MCS-DC\7PAA002122_MCSDC_v2.xx.ZIP" and press enter.
5. The tool will calculate the Hash and return the value to the screen followed by the name of the file that was hashed.



```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>c:\MCS-DC\SHA256HASH.EXE "C:\MCS-DC\7PAA002122_MCSDC_v2.3.ZIP"
SHA256 Hash Calculation Tool (2VAA005130) Version 1.1 Build Index 18
Copyright (C) 2014-2015 ABB Inc.
a35e5d52016d71b13aed251eed8b11bb215e81dddf1f8a62f73c6948b94bd065  C:\MCS-DC\7PAA002122_MCSDC_v2.3.ZIP
C:\Users\Administrator>

```

Figure E.1: Hash Check

6. Compare this Hash value with the one listed in the summary field of MCS- DC package, in ABB library. A matching value confirms that the downloaded package is identical to the source. If the values do not match, do the following.
 - Download the package again, repeat the steps.
 - If the problem persists, contact ABB Support Line (level 2).
7. Alternatively, users can compute SHA256 Hash value, using Windows power shell. Follow the link given below for Hash value calculation using Windows PowerShell:
<https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/get-filehash>.

Appendix F Testing the WMI health of a computer

Following procedure shall be executed to test the health of WMI queries within the local computer (MCS-DC launch node) as well as between local computer and remote computers.

F.1 Health check of WMI query within the local node

1. In MCS-DC launch node, Go to the system32 folder and select wbemtest.exe application. Hold Shift and Right-click, which brings up the "Run as different user" as shown in **Figure F.1**.

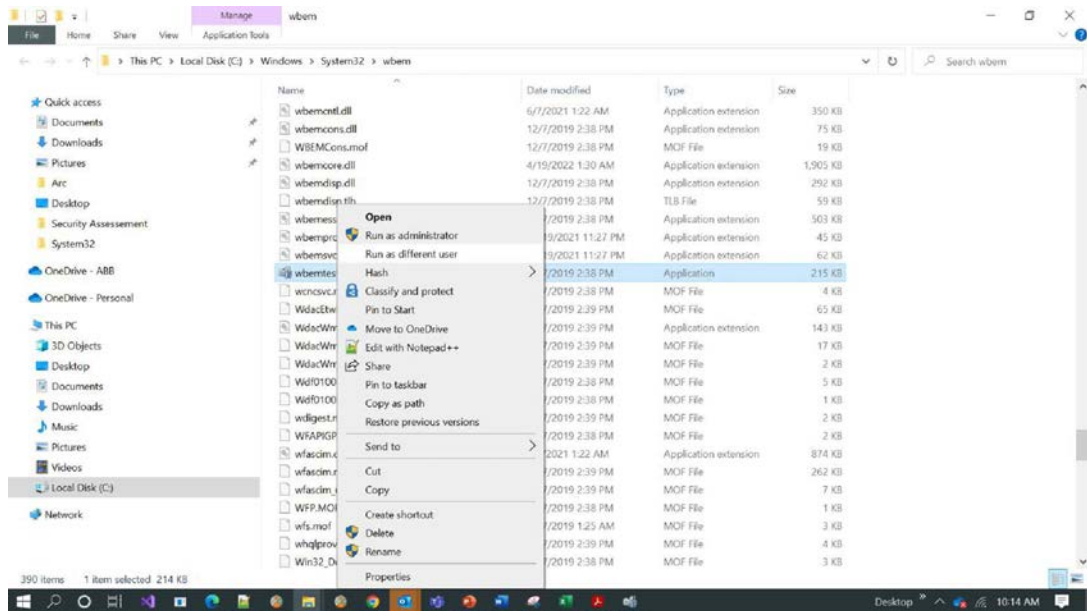


Figure F.1: System32 Folder

F Testing the WMI health of a computer
F.1 Health check of WMI query within the local node

2. Click on "Run as different user" option, which brings up the following screen. Provide the user credentials which were provided as input to MCS- DC for collecting data on this computer and click on **OK**.

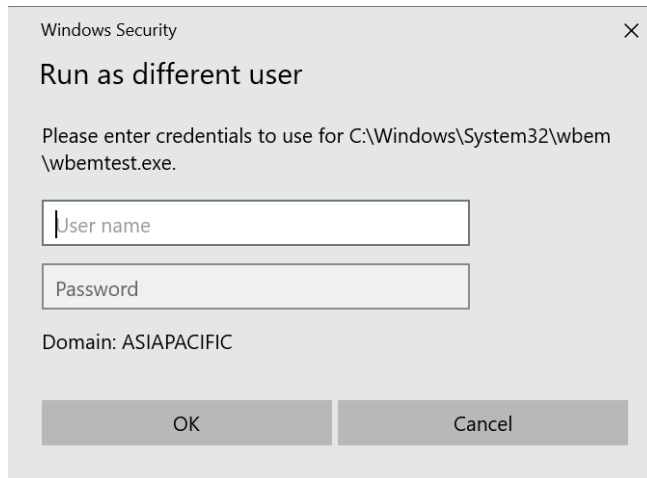


Figure F.2: Enter Credentials

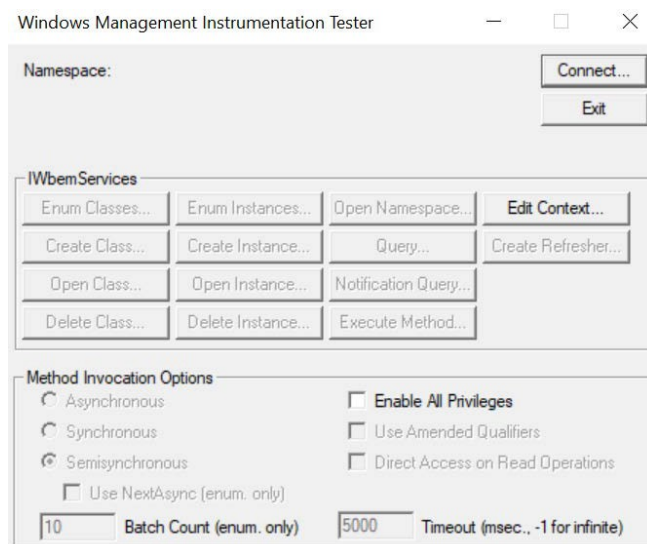


Figure F.3: Windows Management Instrumentation Tester

F Testing the WMI health of a computer
F.1 Health check of WMI query within the local node

3. Clicking on Connect brings up the following screen. To check the health of WMI query within the local node, click on the **Connect** button without entering any credentials. Health check of WMI query from local node to a remote node shall be done by entering the remote node IP address and access credentials.

The 'Connect' dialog box is shown with the following settings:

- Namespace:** root\cimv2
- Connection:** Using: IWbemLocator (Namespaces); Returning: IWbemServices; Completion: Synchronous
- Credentials:** User, Password, and Authority fields are empty.
- Locale:** Empty field.
- How to interpret empty password:** NULL (selected), Blank (unselected).
- Impersonation level:** Identify (unselected), Impersonate (selected), Delegate (unselected).
- Authentication level:** None (unselected), Packet (selected), Connection (unselected), Packet integrity (unselected), Call (unselected), Packet privacy (unselected).

Figure F.4: WMI query health check - Local computer

The 'Connect' dialog box is shown with the following settings:

- Namespace:** \\169.227.40.11\root\cimv2
- Connection:** Using: IWbemLocator (Namespaces); Returning: IWbemServices; Completion: Synchronous
- Credentials:** User: .\Administrator; Password: [masked]; Authority: Empty.
- Locale:** Empty field.
- How to interpret empty password:** NULL (selected), Blank (unselected).
- Impersonation level:** Identify (unselected), Impersonate (selected), Delegate (unselected).
- Authentication level:** None (unselected), Packet (selected), Connection (unselected), Packet integrity (unselected), Call (unselected), Packet privacy (unselected).

Figure F.5: WMI query health check - Remote computer

F Testing the WMI health of a computer
F.1 Health check of WMI query within the local node

4. Successful connect brings up the following Window.

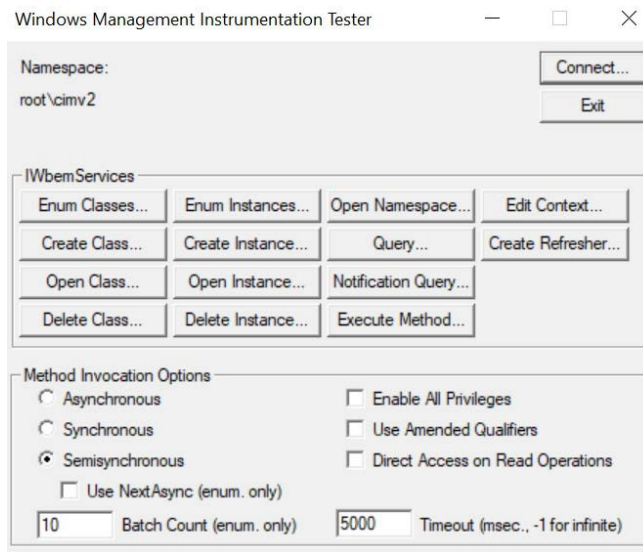


Figure F.6: Connection successful - Local

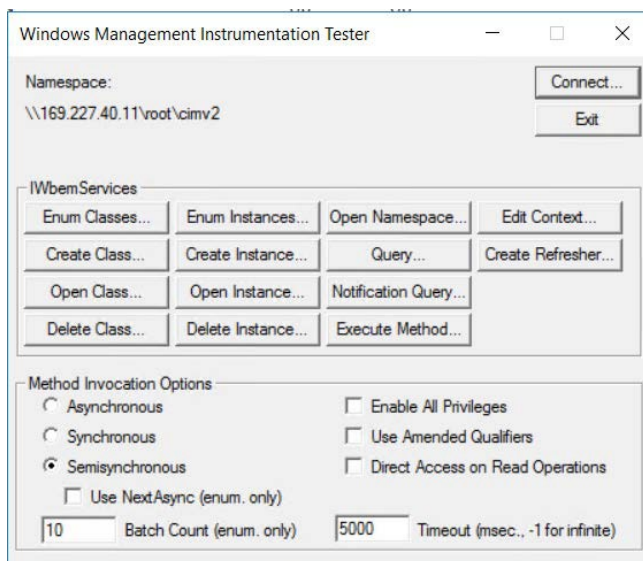


Figure F.7: Connection successful - Remote

5. Click on **Query** button in above screen brings up the following screen.

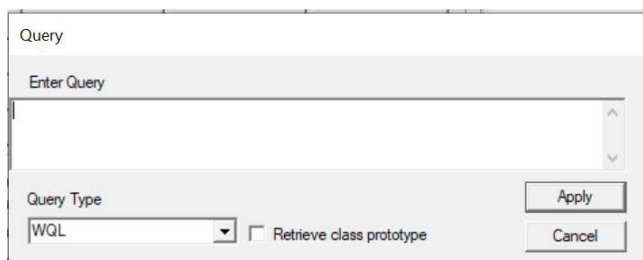


Figure F.8: Enter Query

F Testing the WMI health of a computer
F.1 Health check of WMI query within the local node

6. Enter the Following query in above screen and click on **Apply** button.
select * from Win32_OperatingSystem
7. Successful result of the above query bring the following screen.

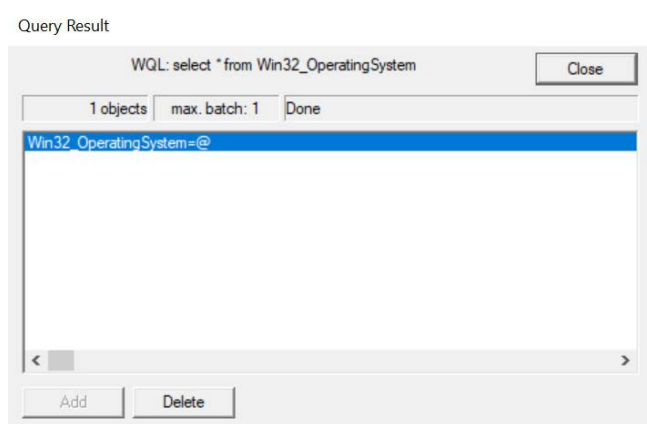


Figure F.9: Query Result

8. Double click on the object **Win32_OperatingSystem=@**. Properties of this object will be listed as shown in **Figure F.10**. For example, the property 'Caption' has a value 'Microsoft Windows 10 Enterprise'. The WMI query for this property is successful.

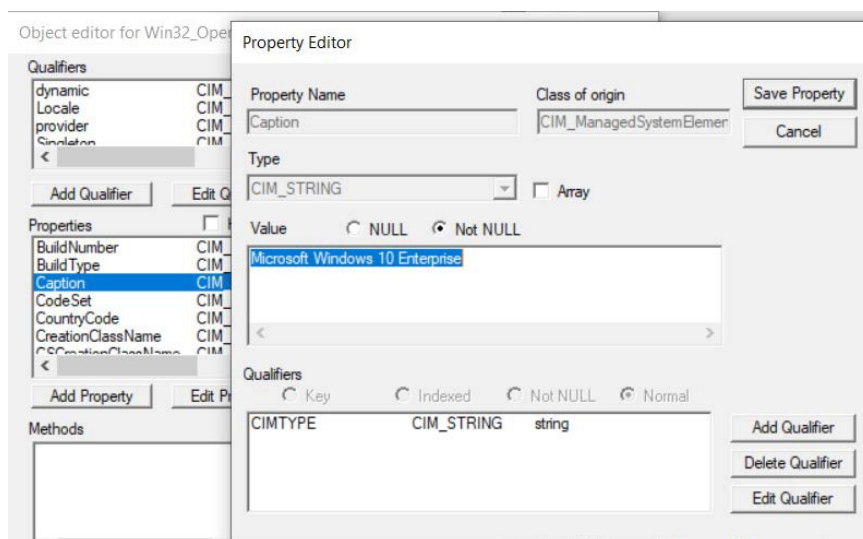


Figure F.10: WMI query - OS caption

Appendix G Prerequisite tool

The tool can be used for checking the prerequisites for data collection on each node of System 800xA and Freelance. Copy the 'Tools' folder from the MCS-DC package to the C:\Temp folder of each computer node in the network. Depending on the .Net Framework version installed on the launch node, run the tool by double-clicking **MCS-DC- Prerequisite_Tool.exe** from the following locations.

- .Net Framework version 4.8.1 and above: \Tools\Prerequisite\.NetFramework 4.8.1 and Above
- .Net Framework is lower than 4.8.1: \Tools\Prerequisite\.NetFramework 4.8 and Below.

Refer to the registry path in the screenshot below. The highlighted value (533320) indicates .Net Framework version 4.8.1. Values below or above this correspond to versions of the .Net Framework lower or higher than 4.8.1.

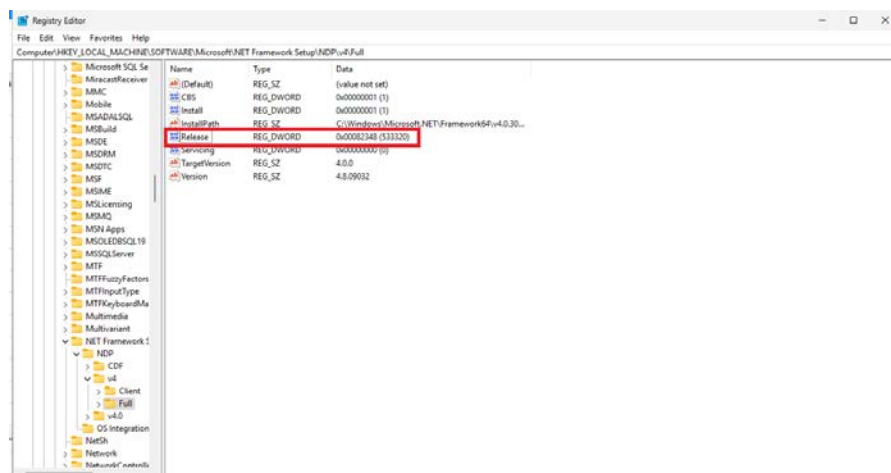


Figure G.1: .Net Framework version details in Windows registry

G Prerequisite tool

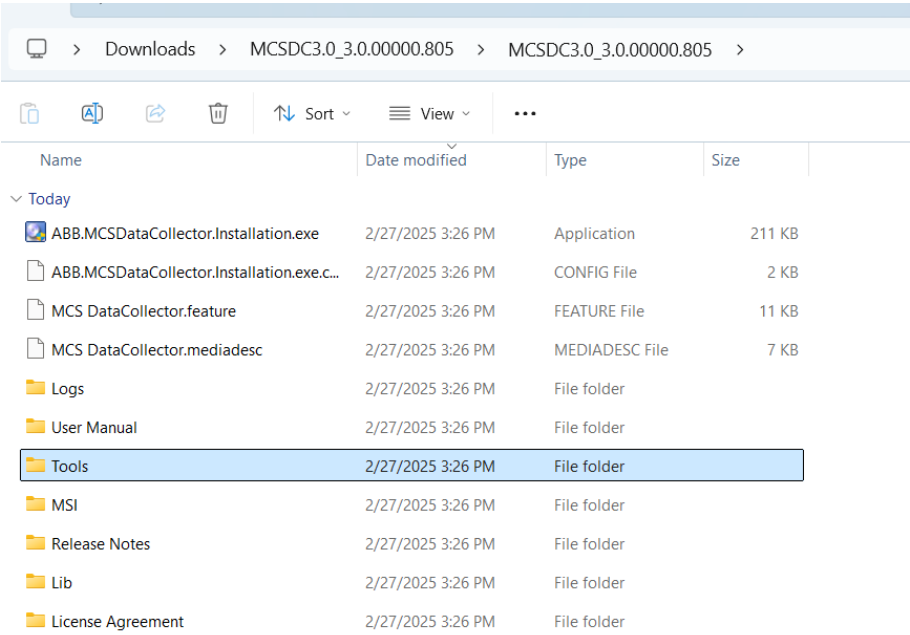


Figure G.2: Tools folder

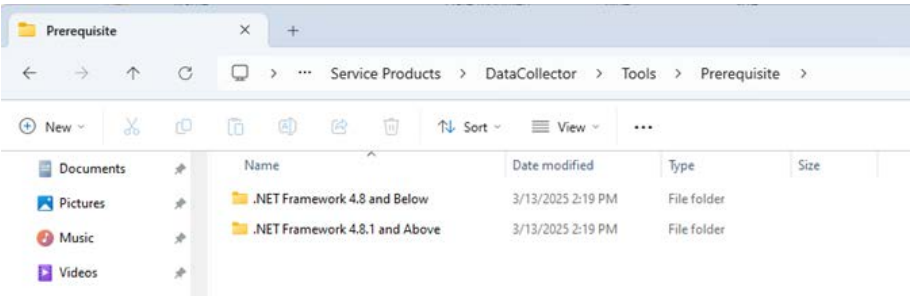


Figure G.3: MCS-DC_Prerequisite_Tool

Click the next button after selecting the system and Domain/Workgroup as applicable.

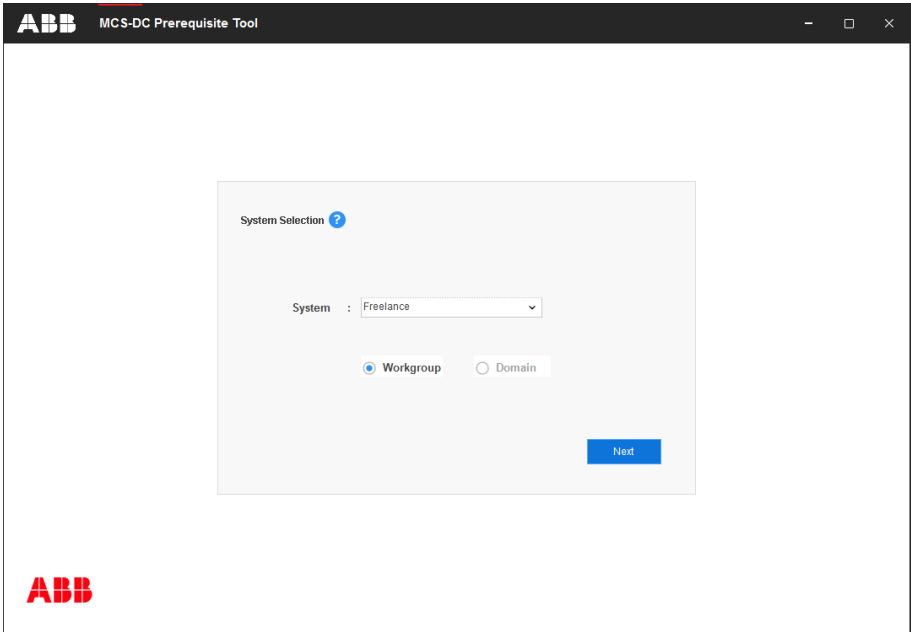


Figure G.4: System Selection

As shown below, the tool will check for the applicable prerequisites for the selected system and populate the results. All the available prerequisites in the node will be listed with a green tick, in the 'Original status' column.

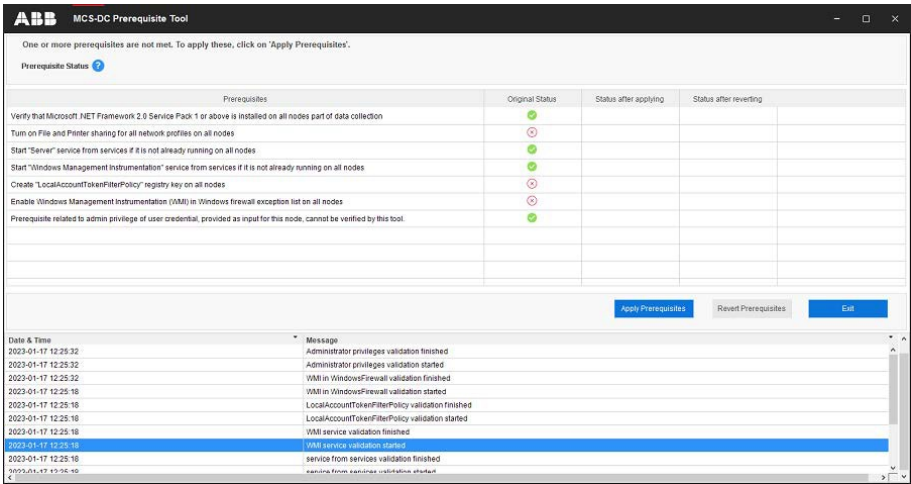


Figure G.5: Original status

Click on 'Apply prerequisite' button to apply the missing prerequisites. This must be repeated for all nodes from which the performance data is to be collected.



In Windows XP and Windows 2003 Server operating systems, this tool cannot identify/set 'File and Printer sharing' and 'WMI in Windows firewall' related prerequisites. Refer to [Section 2.1, Common Prerequisites](#) to set them manually. Ignore the status of these two prerequisites, shown by the tool. Rest of the prerequisites will work fine.

G Prerequisite tool

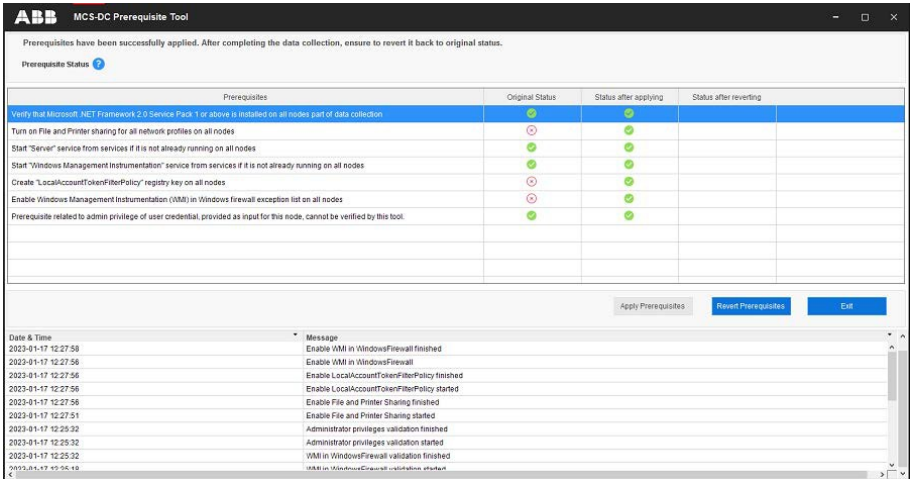


Figure G.6: Status after applying prerequisites

Now that all the prerequisites for data collection have been met, the node is ready for data collection.

Once the data has been collected, click the revert prerequisite button to revert the changes.

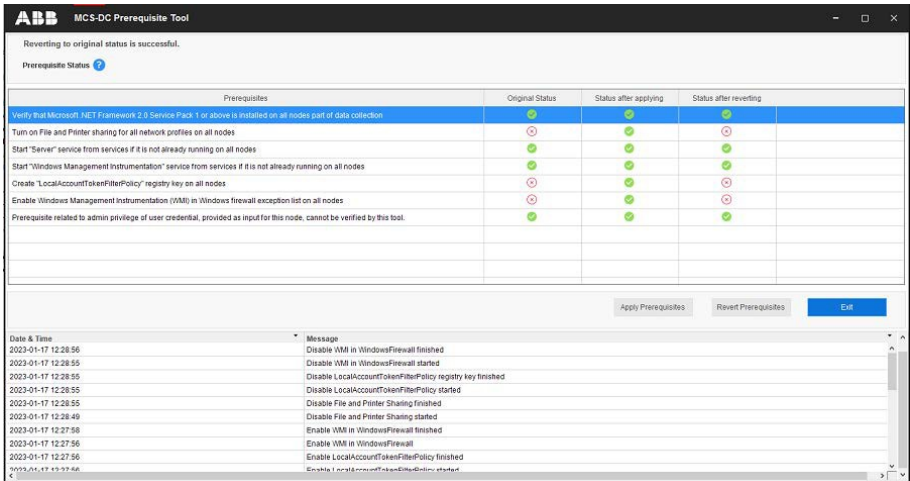


Figure G.7: Status after reverting prerequisites

After reverting the changes, ensure that the 'Status after reverting' column matches the 'Original status' column.



It is not possible to revert each change individually. A revert change command will revert all changes at once.



It is not possible to reverse prerequisite changes made with one version of MCS-DC with another version. Revert the changes using the same version of MCS-DC.

Appendix H Procontrol P14 system configuration file

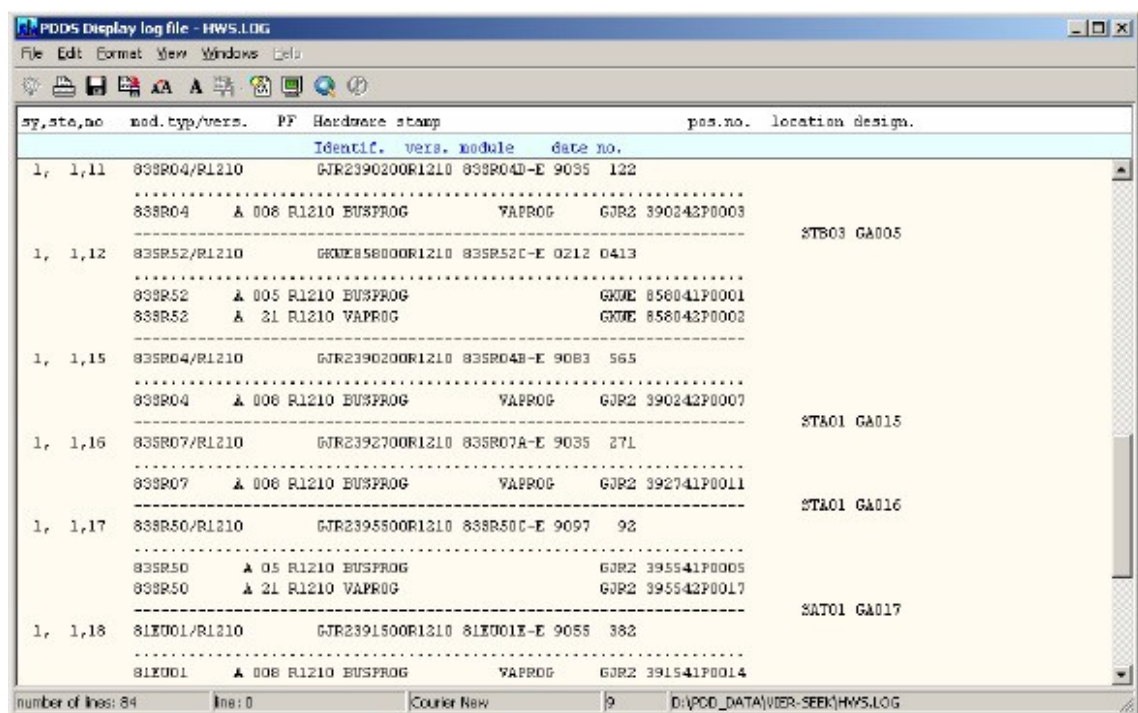
Figure 274 shows the exported log file(*) with Procontrol P14 PDDS (Programming, Diagnosis and Display System).

(*) English :

PROCONTROL configuration - Overall interrogation (OVE) with hardware stamp and software identification.

(*)German:

PROCONTROL Konfiguration - Gesamtabfrage (GAF) mit Hardwarestempel und Software-Identifikation. Run the tool.



sy	ste	no	mod. typ/vers.	PF	Hardware stamp	pas.no.	location	design.
					Identif. vers. module	date no.		
1,	1,11	83SR04/R1210			GJR2390200R1210 83SR04D-E 9035	122		
		83SR04	A 008 R1210	EUSPROG	VAPROG	GJR2 390243P0003		
							STB03	GA005
1,	1,12	83SR52/R1210			GJWE858000R1210 83SR52C-E 0212 0413			
		83SR52	A 005 R1210	EUSPROG		GJWE 858041P0001		
		83SR52	A 21 R1210	VAPROG		GJWE 858043P0002		
1,	1,15	83SR04/R1210			GJR2390200R1210 83SR04B-E 9083	565		
		83SR04	A 008 R1210	EUSPROG	VAPROG	GJR2 390243P0007		
							STA01	GA015
1,	1,16	83SR07/R1210			GJR2392700R1210 83SR07A-E 9035	271		
		83SR07	A 008 R1210	EUSPROG	VAPROG	GJR2 392741P0011		
							STA01	GA016
1,	1,17	83SR50/R1210			GJR2395500R1210 83SR50C-E 9097	92		
		83SR50	A 05 R1210	EUSPROG		GJR2 395541P0005		
		83SR50	A 21 R1210	VAPROG		GJR2 395542P0017		
							SAT01	GA017
1,	1,18	81EU01/R1210			GJR2391500R1210 81EU01E-E 9055	382		
		81EU01	A 008 R1210	EUSPROG	VAPROG	GJR2 391541P0014		

number of lines: 84 line: 0 Courier New 9 D:\PCD_DATA\WIER-SEK\HW5.LOG

Figure H.1: Example of exported configuration of Procontrol P14 System

Appendix I The Microsoft Defender SmartScreen

If Microsoft Defender smart screen is disabled in Windows 10 and Windows Server 2022, the following popup will appear when MCS-DC is run. To continue, click Run.

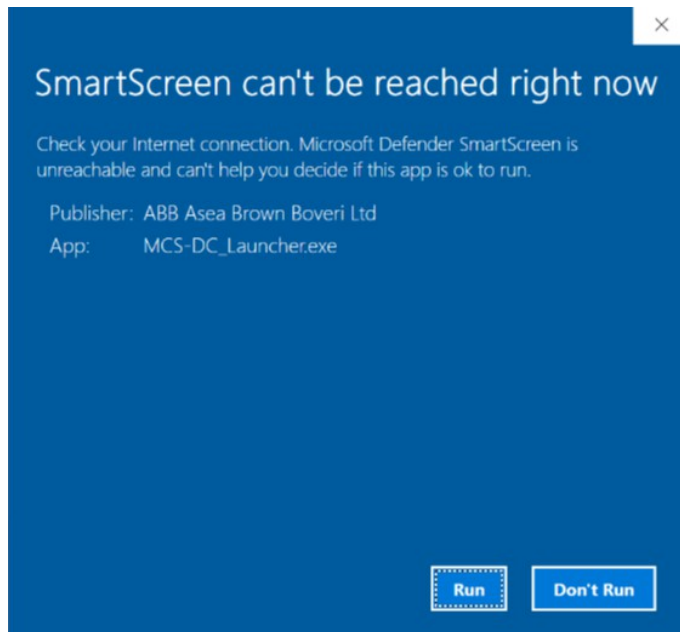


Figure I.1: SmartScreen related popup message

Appendix J How to enable Windows administrative share access

1. Login to the nodes in which Administrative Share has to enabled and open services window (type services.msc in the windows run command and click enter to open service window).
2. Under the list of services, identify the service name Server. The remote collection of process HMI fails when this service is disabled.
3. Double-click the server service to open the Server Properties.
4. Set the startup type to **Automatic**.
5. Click on Apply and then click on Start to bring the service to run state.
6. The status of the Server service changes to Started.

Appendix K How to check firewall settings for WMI

The below procedure is applicable for Windows Server 2016 Operating System, and may vary slightly for other Operating Systems. Enabling WMI is mandatory for all nodes from which the data is collected. This setting can be reverted once the data collection is complete.

1. In the Control Panel, click on **Windows Firewall**.

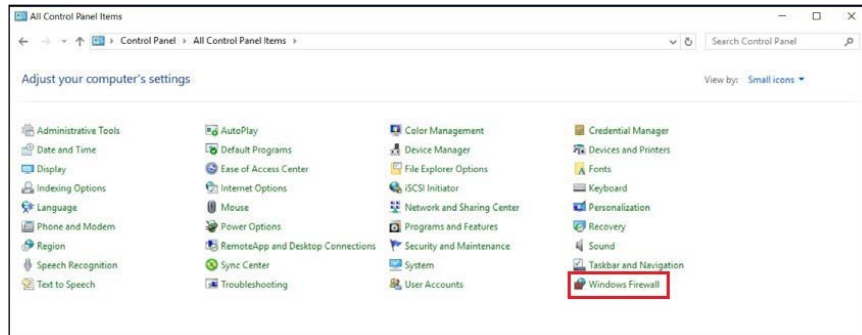


Figure K.1: Control Panel

2. Windows Firewall screen appears, click on **Advanced Settings**.



Figure K.2: Advanced Settings

K How to check firewall settings for WMI

3. Windows Firewall with Advanced Security screen appears. Select **Inbound Rules** option and check if **Windows Management Instrumentation (WMI- In)** rule is enabled. If the rule is enabled, WMI traffic is allowed by the Windows firewall, hence no further changes are required.

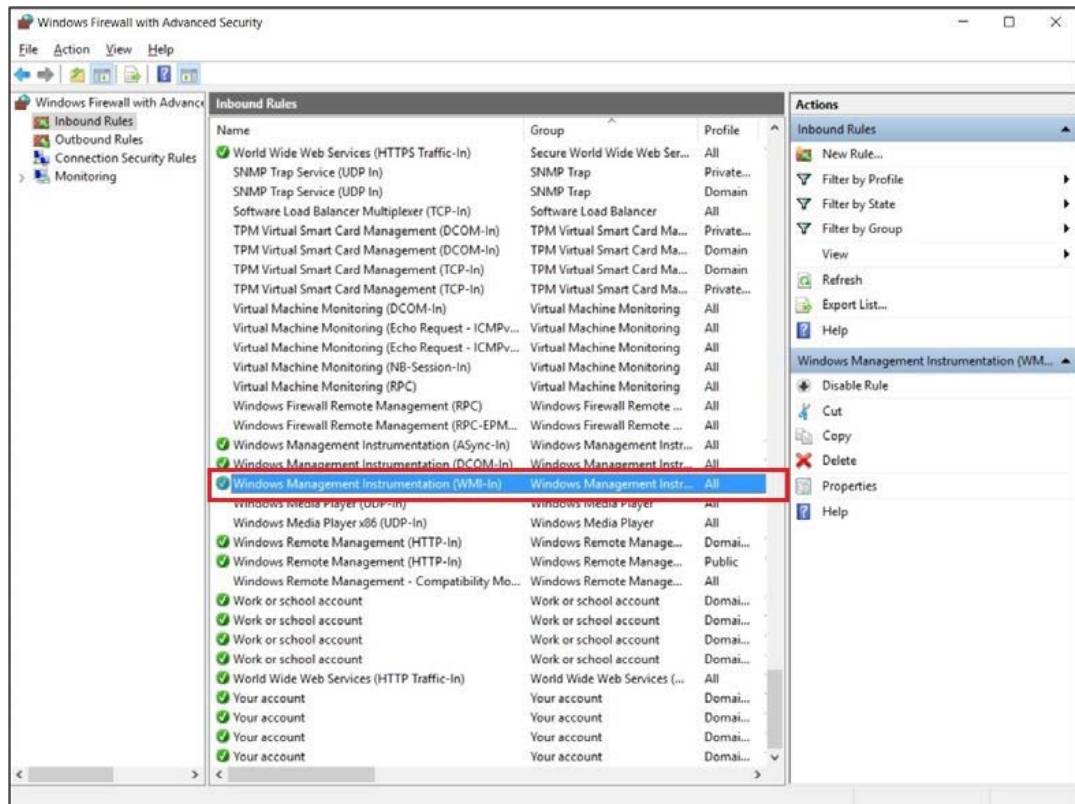


Figure K.3: Windows Firewall with Advanced Security Screen

K How to check firewall settings for WMI

4. In case, if rule is configured and not enabled in the inbound rules. Right-click on the **Windows Management Instrumentation (WMI-In)** and select **Enable Rule**.

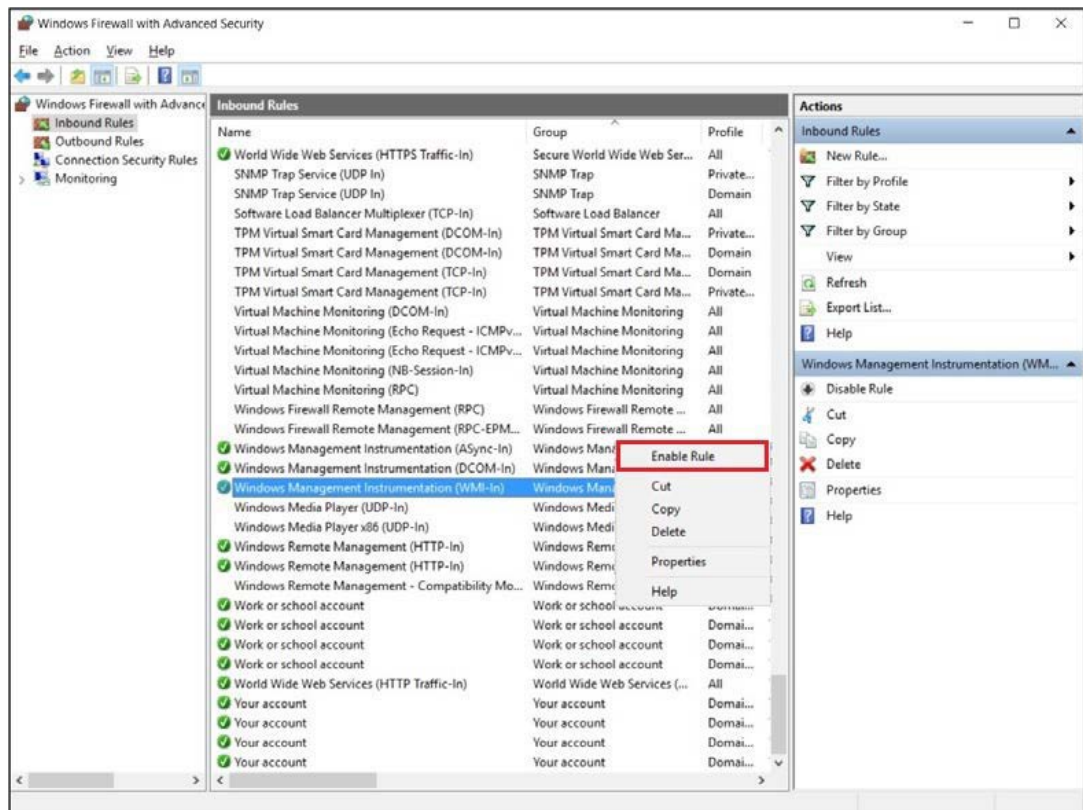


Figure K.4: Enable Rule

5. In case, if rule is not configured, right-click on the **Inbound Rules** and select **New Rule**.

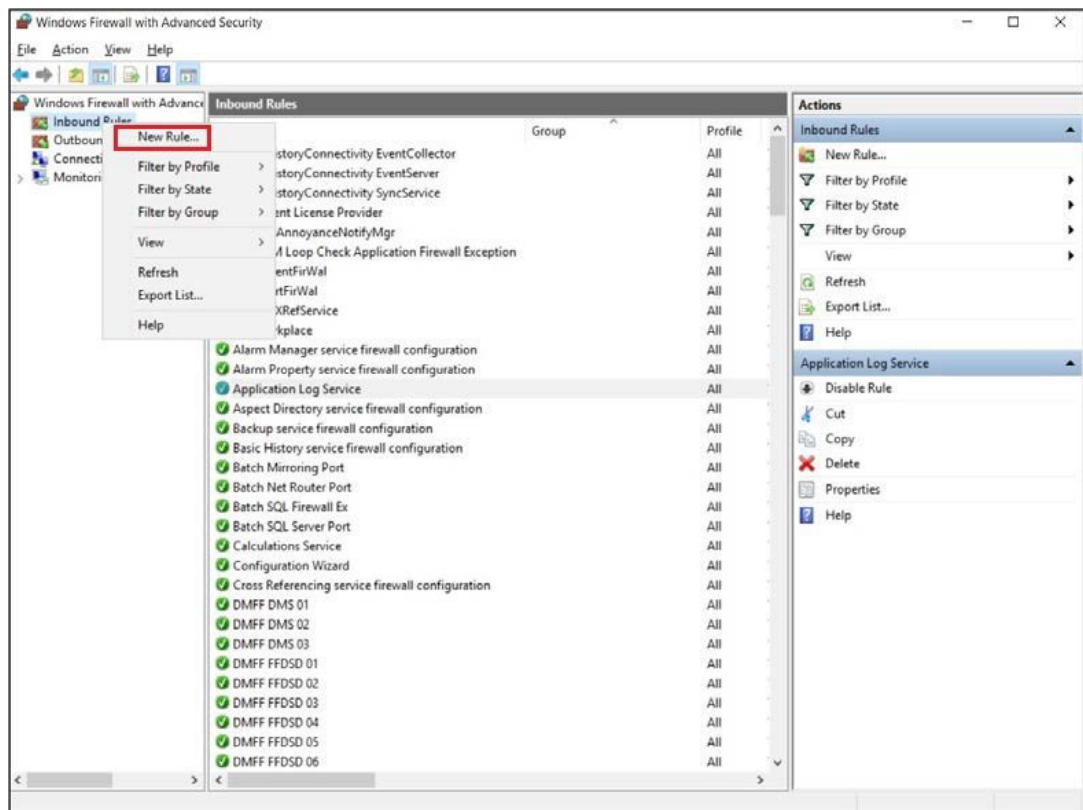


Figure K.5: New Rule

K How to check firewall settings for WMI

6. New Inbound Rule Wizard appears. In the New Inbound Rule Wizard, select **Predefined** option and select the **Windows Management Instrumentation (WMI-In)** rule and then click on **Next**.

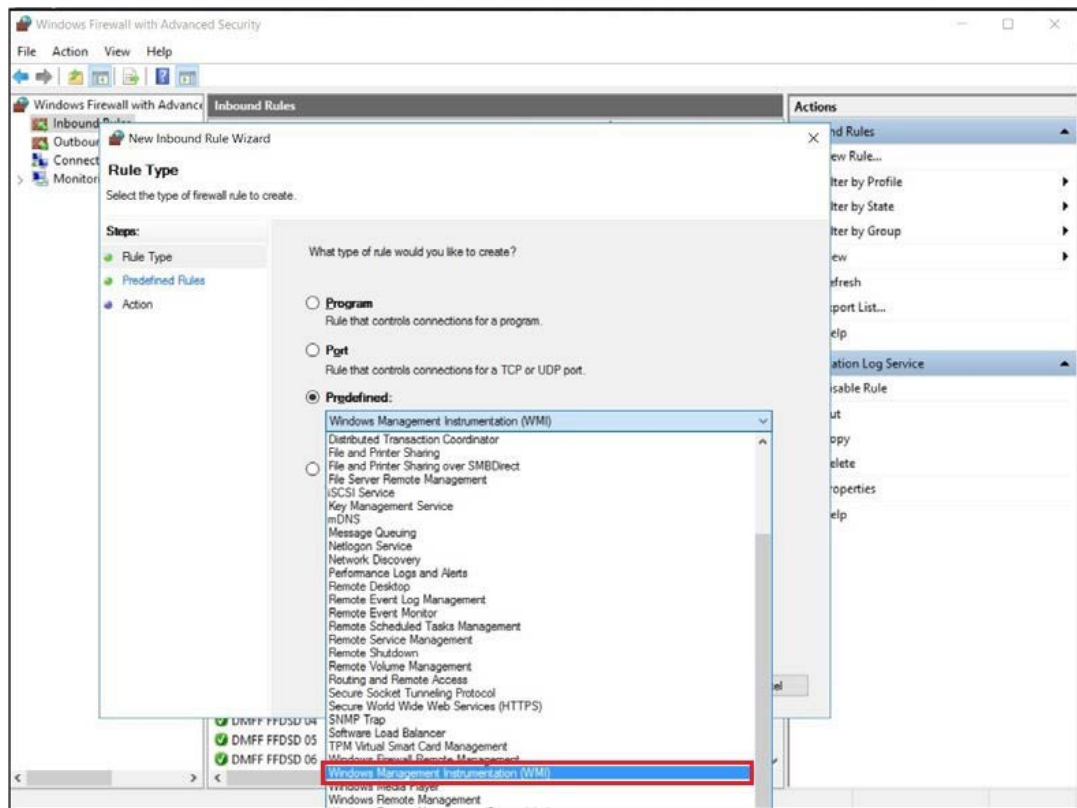


Figure K.6: Predefined Option

7. Select all the three rules in the Rules section and click on **Next**.

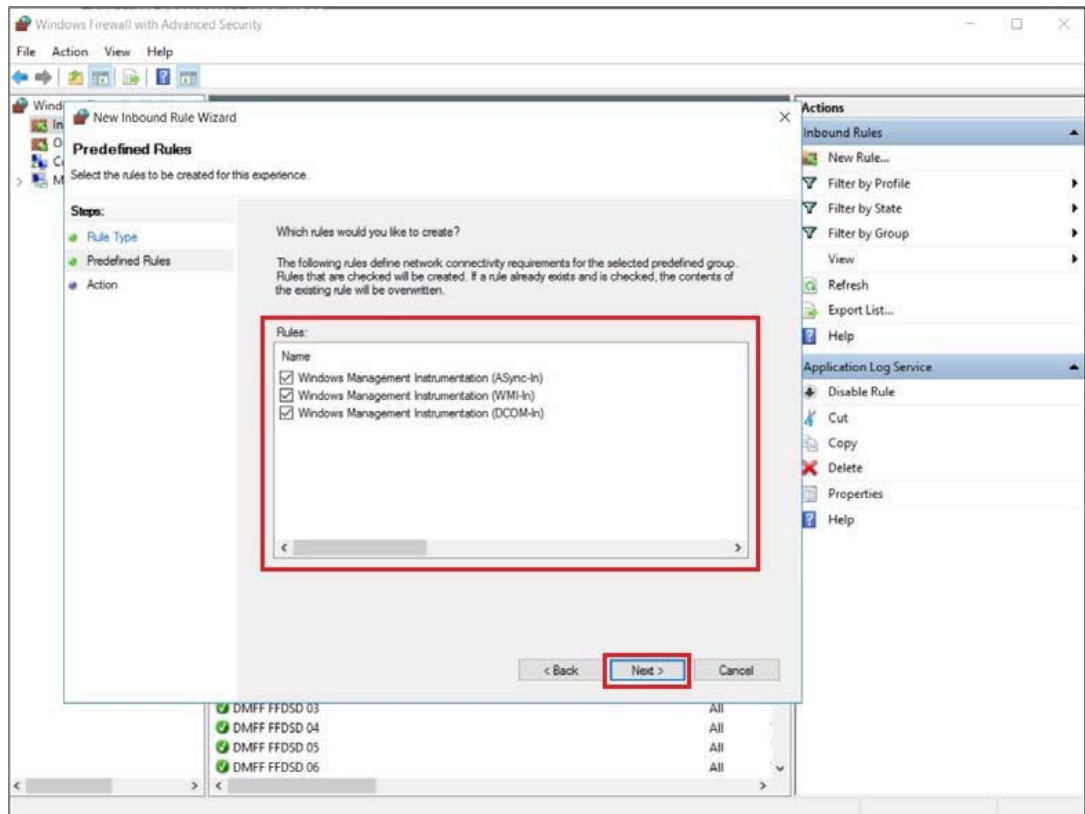


Figure K.7: Select All Rules

8. Select **Allow the connection** and click on **Finish**.

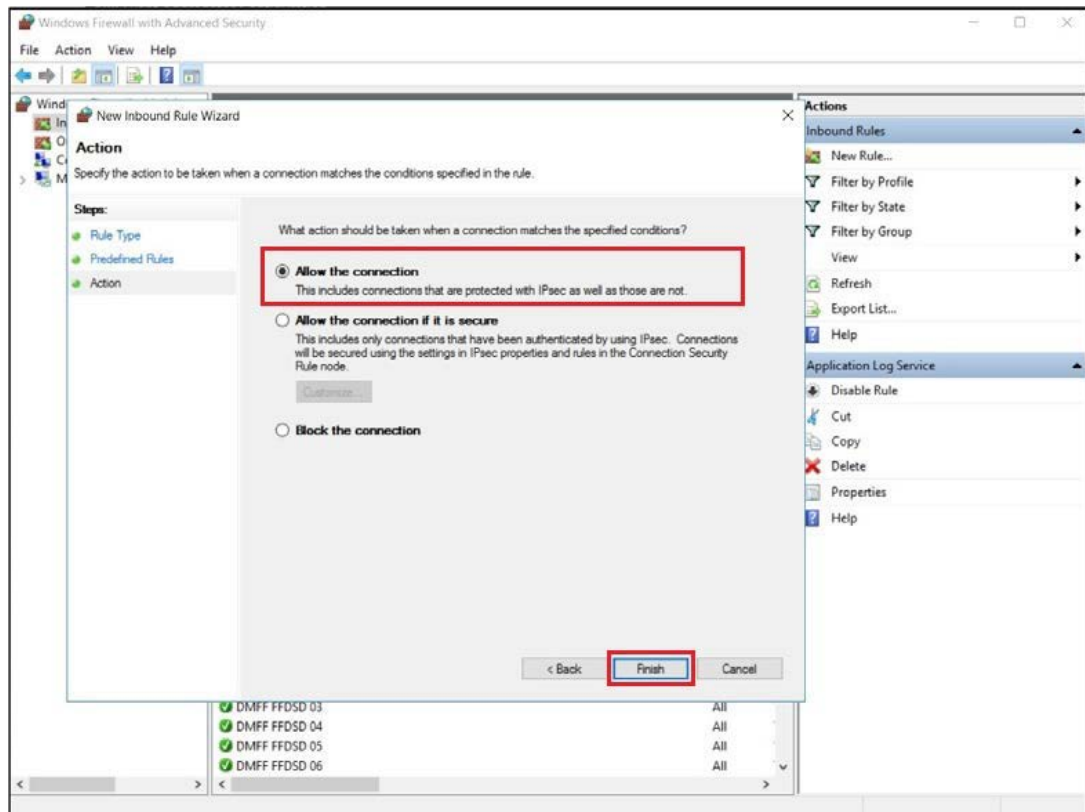


Figure K.8: Allow the Connection

K How to check firewall settings for WMI

9. After the collection of complete data, revert the changes. Select the options and click on **Disable Rule**.

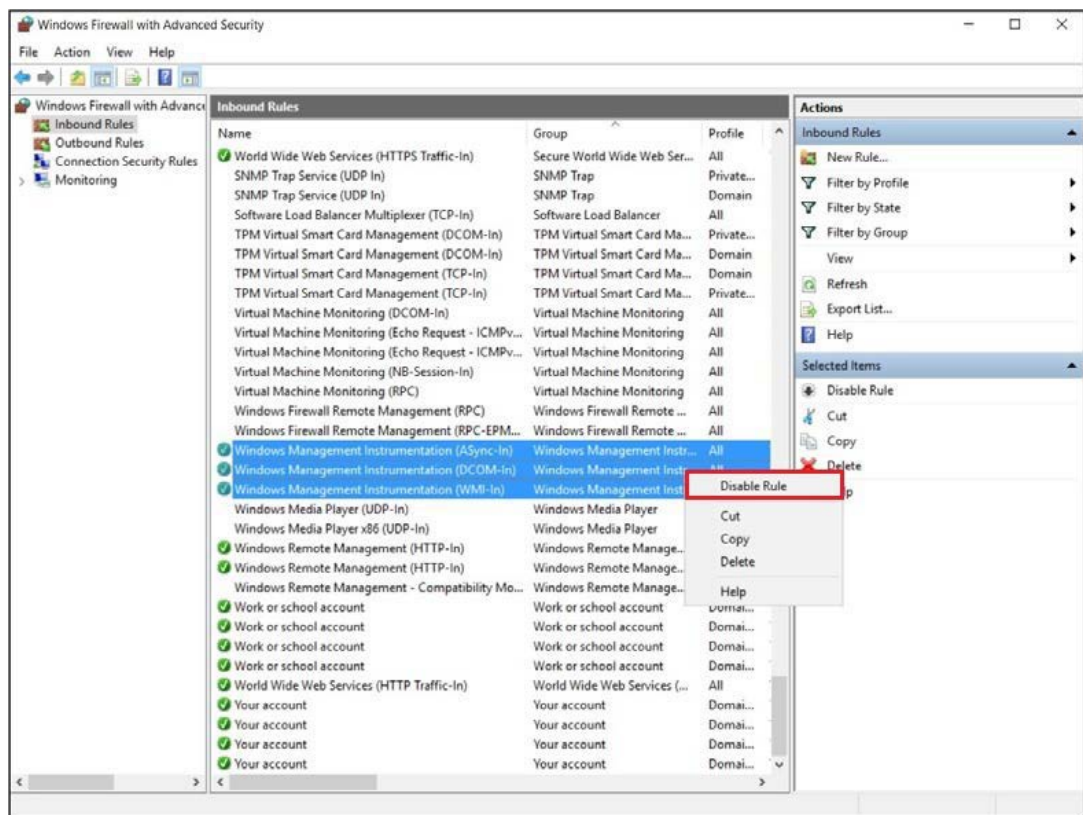


Figure K.9: Disable the Rule

Appendix L How to determine which .NET Framework versions are installed

For information about installed .Net Framework versions on a computer, refer to <https://learn.microsoft.com/en-us/dotnet/framework/install/how-to-determine-which-versions-are-installed>.

Revision History

This section provides information on the revision history of this user manual.

The revision index of this user manual is not related to the actual product revision. Please note, MCS-DC 2.0.0 and 2.0.1 are managed releases. It is released to selected users to get feedback on the product, as it is a new product.

Revision History

The following table lists the revision history of this user manual.

Revision Index	Description	Date
A	First version for MCS-DC 2.0.0 (Managed release)	September 2020
B	This version is for MCS-DC 2.0.1 (Managed release)	September 2020
C	This version is for MCS-DC 2.0.2	November 2020
D	This version is for MCS-DC 2.1	April 2021
E	This version is for MCS-DC 2.2	September 2021
F	This version is for MCS-DC 2.3	December 2021
G	This version is for MCS-DC 2.4	March 2022
H	This version is for MCS-DC 2.5	June 2022
I	This version is for MCS-DC 2.6	October 2022
J	This version is for MCS-DC 2.7	March 2023
K	This version is for MCS-DC 2.8	September 2023
L	This version is for MCS-DC 2.9	March 2024
M	This version is for MCS-DC 2.9.1	June 2024
N	This version is for MCS-DC 2.10	September 2024
P	This version is for MCS-DC 3.0	March 2025

Updated in Revision Index B

The following table shows the updates made in this Release for version 2.0.1.

Updated Section/Sub-section	Description of Update
Section 1.2	<ul style="list-style-type: none"> – Updated Support information for System 800xA – Added Support information for Advant Master controllers with System 800xA HMI – Added Support information for Melody Rack controllers – Added Support information for Harmony Rack controllers (LCS only) – Added Support information for S+ Operations HMI – Added support information for Freelance HMI versions Freelance 2019 SP1 FP1 and Freelance 2013 SP1 RU5.
Section 2	<ul style="list-style-type: none"> – Added Common Prerequisites – Updated Prerequisites for System 800xA – Added Prerequisites for S+ Operations HMI – Added Prerequisites for Harmony Rack – Added Prerequisites for Advant Master with System 800xA – Added Prerequisites for Melody Rack
Section 3	<ul style="list-style-type: none"> – Updated Basic Mode data collection process for 800xA HMI – Updated Basic Mode data collection process for Freelance HMI – Added subsection for Basic Mode data collection process for S+ Operations HMI – Updated Advanced Mode data collection process for System 800xA HMI – Updated Advanced Mode data collection process for Freelance HMI – Added Support information for Symphony DIN controllers with System 800xA HMI. – Added subsection for Advanced Mode data collection process for S+ Operations HMI. – Added support for Security data collection in S+ Operations system.
Section 4	<ul style="list-style-type: none"> – Updated Post collection procedure
Appendix	<ul style="list-style-type: none"> – Added Appendix A – Added Appendix B

Updated in Revision Index C

The following table shows the updates made in this Release for version 2.0.2.

Updated Section/Sub-section	Description of Update
Section 2	<ul style="list-style-type: none">– Added Prerequisites for Advant MOD 300– Added Prerequisites for Procontrol P13 controllers
Section 3	<ul style="list-style-type: none">– Updated Basic Mode data collection process for 800xA HMI– Updated Advanced Mode data collection process for 800xA HMI– Updated Advanced Mode data collection process for S+ Operations HMI
Appendix	<ul style="list-style-type: none">– Added Appendix C

Updated in Revision Index D

The following table shows the updates made in this Release for version 2.1.

Updated Section/Sub-section	Description of Update
Section 2	<ul style="list-style-type: none">– Added Prerequisites for QCS with 800xA HMI
Section 3	<ul style="list-style-type: none">– Updated Basic Mode data collection process for 800xA HMI– Updated Advanced Mode data collection process for 800xA HMI– Updated Advanced Mode data collection process for S+ Operations HMI
Appendix	<ul style="list-style-type: none">– Added Appendix D

Updated in Revision Index E

The following table shows the updates made in this Release for version 2.2.

Updated Section/Sub-section	Description of Update
Section 1	<ul style="list-style-type: none">– Supported Systems and Versions
Section 3	<ul style="list-style-type: none">– Data Collection process
Section 5	<ul style="list-style-type: none">– “chkdsk” issue is removed
Section 2	<ul style="list-style-type: none">– Modified .NET Framework version– Freelance prerequisite settings for Windows XP client nodes in workgroup
Section 5	<ul style="list-style-type: none">– Error when .NET Framework is missing in the launch node

Updated in Revision Index F

The following table shows the updates made in this Release for version 2.3.

Updated Section/Sub-section	Description of Update
Section 3	<ul style="list-style-type: none">– Periodic Data Collection– All Images– Product name change from SPDC to MSC Data collector
Section 5	<ul style="list-style-type: none">– Issue 1 Agent deployment failed added

Updated in Revision Index G

The following table shows the updates made in this Release for version 2.4.

Updated Section/Sub-section	Description of Update
Section 1.2	<ul style="list-style-type: none">– Supported Systems and Versions
Section 3.4.1	<ul style="list-style-type: none">– 800xA with Harmony data collection
Section 3.4.3	S+ Operations with Harmony data collection
Section 3.5	Periodic data collection improvements
Appendix E	Hash verification.

Updated in Revision Index H

The following table shows the updates made in this Release for version 2.5.

Updated Section/Sub-section	Description of Update
Section 2.13	<ul style="list-style-type: none">– Non-ABB System (Security Data collection).
Section 3.4.7	<ul style="list-style-type: none">– Security Data Collection from non-ABB Systems.– Support for QCS with System 800xA HMI version 6.1 SP2.
Section 1.2	<ul style="list-style-type: none">– Supported Systems and Versions.
Section 4	<ul style="list-style-type: none">– Change in collection file name.

Updated in Revision Index I

The following table shows the updates made in this Release for version 2.6.

Updated Section/Sub-section	Description of Update
Section 3.1	<ul style="list-style-type: none">– Switch option from Basic to Advanced mode data collection.
Section 3.3.1, Section 3.4.1	<ul style="list-style-type: none">– AC 800M crash file collection configuration.
Section 3.6	ESXi Data Collection

Updated Section/Sub-section	Description of Update
Section 4.1	Collection file merging
Appendix B.2	Secured communication - Client certificate selection procedure

Updated in Revision Index J

The following table shows the updates made in this Release for version 2.7.

Updated Section/Sub-section	Description of Update
Section 1.2	<ul style="list-style-type: none">– Supported Melody versions, Supported Harmony Composer & S+ Engineering versions, Supported HAPI versions, Supported S+ Operations Versions, Supported 800xA Versions and Support for Harmony Bridge modules.

Updated in Revision Index K

The following table shows the updates made in this Release for version 2.8.

Updated Section/Sub-section	Description of Update
Section 3.4.1	<ul style="list-style-type: none">– Parallel data collection of client computers.– AC 800M controller collection configuration.

Updated in Revision Index L

The following table shows the updates made in this Release for version 2.9.

Updated Section/Sub-section	Description of Update
Section 1.2	<ul style="list-style-type: none">– Supported Freelance versions.– Supported 800xA versions.
Section 3.1, 3.2	<ul style="list-style-type: none">– AC 800M crash file collection configuration.
Section 3.4.8	S+ Historian in 800xA or third party HMI environment.
Section 4.1	Collection file merging.
Appendix B	Secured communication.

Updated in Revision Index M

The following table shows the updates made in this Release for version 2.9.1

Updated Section/Sub-section	Description of Update
Section 2.8	<ul style="list-style-type: none">– Advant Master controller data collection prerequisite.–

Updated in Revision Index N

The following table shows the updates made in this Release for version 2.10

Updated Section/Sub-section	Description of Update
Section 1.2	<ul style="list-style-type: none">– Supported 800xA versions.– Supported QCS versions.– Supported Freelance versions.
Section 3.0	<ul style="list-style-type: none">– Support for Japanese language systems.

Updated in Revision Index P

The following table shows the updates made in this Release for version 3.0

Updated Section/Sub-section	Description of Update
Section 3	<ul style="list-style-type: none">– Setup and Maintenance.
Section 4	<ul style="list-style-type: none">– Data Collection.
Section 6	<ul style="list-style-type: none">– Troubleshooting.

