PROCESS AUTOMATION

My Control System - Data Collector
User Manual

PROCESS AUTOMATION

My Control System - Data Collector
User Manual

Document number: 2PAA120980 - 200
Document revision:L
Release: March 2024

Notice

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

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

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

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

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

ABB Ltd and its affiliates are not liable for damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

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

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

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

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license. This product meets the requirements specified in EMC Directive 2014/30/EU and in Low Voltage Directive 2014/35/EU.

Trademarks

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

Copyright©2024byABB.
All rights reserved.

Table of Contents

About This User Manual

General 9
Document Conventions 9
Warning, Caution, Information, and Tip Icons 9
Network Security Disclaimer 10
Terminology 10
Release Information 11

1 Introduction 13
1.1 Scope and Software Versions 13
1.2 Supported Systems and Versions 14
1.3 Compatibility 18

2 Prerequisites 19
2.1 Common Prerequisites 19
2.2 ABB cyber security guidelines 26
2.3 Effects on cyber security policies 27
2.4 System 800xA 28
2.4.1 In Domain: 28
2.4.2 In Workgroup: 32
2.5 Freelance System 37
2.6 S+ Operations 45
2.7 Harmony controllers 50
2.8 Advant Master controllers with System 800xA HMI 50
2.9 Melody Rack controllers 51
2.10 Advant MOD 300 51
2.11 Procontrol P13 controllers 51

2.12 QCS with System 800xA HMI 51
2.13 Non-ABB System (Security Data collection) 52
2.14 VMware Server Health Data 52

3 Data Collection Process 55
3.1 Basic Mode 55
3.2 Advanced Mode 56
3.3 Basic Mode Data Collection 56
3.3.1 Basic mode data collection for System 800xA 56
3.3.2 Basic mode data collection for Freelance 83
3.4 Advanced Mode Data Collection 101
3.4.1 Advanced Mode Data Collection Process for 800xA HMI 101
3.4.2 Advanced Mode Data Collection Process for Freelance HMI 145
3.4.3 Advanced mode data collection for S+ Operations with Harmony Controllers 162
3.4.4 Advanced mode data collection for S+ Operations with Melody Controllers 185
3.4.5 Advanced mode data collection for S+ Operations with AC800M Controllers 199
3.4.6 Advanced mode data collection for S+ Operations with Procontrol P13 214
3.4.7 Security Data Collection from non-ABB Systems 227
3.4.8 S+ Historian in 800xA or third party HMI environment 239
3.5 Periodic Data Collection 240
3.6 ESXi Data Collection 251

4 Post Collection Procedure 255
4.1 Collection file merging 255
4.2 Limitations in data file merging. 261
4.3 Report Generation from MyABB and uploading data file to ServIS. 261

5 Troubleshooting 263
5.1 Issue 1: Node scan failed 263
5.2 Issue 2: Agent deployment failed 263

5.3 Issue 3: Error message when .Net Framework is missing in the launch node264
5.4 Issue 4: Windows Firewall Settings for WMI 265
5.5 Issue 5: Enabling Windows Administrator Share Access for Freelance Data Collection.274
5.6 Issue 6: Disabling User Account Control 274

6 Additional Information 281
6.1 Listing of related documents 281

Appendix A How to change the default port number
A.1 Basic Mode 283
A.2 Advanced Mode 285

Appendix B Configuring Secured Communication
B.1 Selection of Server Certificate 288
B.2 Selection of Client Certificate 290
B.3 Binding the server certificate to an IP address and port 292

Appendix C Procontrol P13 source file (.csv) separators

Appendix D System configuration export
D.1 Freelance System 295
D.2 Advant MOD 300 299
D.3 AC100 System 300
D.4 Melody Rack 307
D.4.1 Composer Melody Rack version 6.0 or later 307
D.4.2 Asset structure export 313
D.4.3 Composer Melody Rack version 5.2 or earlier 317
D.4.4 Melody CSE_Conf File 323

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 327

Appendix G Prerequisite tool

Revision History **341**
Updated in Revision Index K 351

Index **353**

About This User Manual

General

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

Document Conventions

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

Warning, Caution, Information, and Tip Icons

This User Manual includes Warning, Caution, and Information where appropriate to point out safety related or other important information. It also includes Tip to point out useful hints to the reader. The different icon types found in this document are presented below:

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

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

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

Information icon alerts the reader to pertinent facts and conditions.

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

Although Warning hazards are related to personal injury, and Caution hazards are associated with equipment or property damage, it must 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.

Network Security Disclaimer

This product is designed to be connected to and to communicate information and data via a network interface, it is your sole responsibility to provide and continuously ensure a secure connection between the product and to your network or any other network (as the case may be). You shall establish and maintain any appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of anti-virus programs, etc) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB and its entities are not liable for damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

Terminology

A complete and comprehensive list of Terms is included in System *800xA System Guide Functional Description (3BSE038018*)*. The listing includes terms and definitions that apply to the 800xA System where the usage is different from commonly accepted industry standard definitions and definitions given in standard dictionaries such as Webster's Dictionary of Computer Terms. Terms that uniquely apply to this instruction are listed in the following table.

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.

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.

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 life cycle information on this collection file can be uploaded to ServIS from MCS by the local ABB installed base manager using SCX Tool for Installed Base Management, for the consolidation of installed base information on ServIS.

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 data collection process for the various systems that are supported by this version of MCS-DC.

1.2 Supported Systems and Versions

Supported systems version for Data Collection are listed below.

Table 1. Supported Sytems

Control System	Supported Major Versions	Supported Rollup Versions
Freelance	- 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	- V9.2.01 - Freelance 2013 SP1 RU1, Freelance 2013 SP1 RU2, Freelance 2013 SP1 RU3, Freelance 2013 SP1 RU4 Freelance 2013 SP1 RU5 - 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 2019 SP1 RU1 Freelance 2019 SP1 FP1 RU1 Freelance 2019 SP1 FP1 RU2 Freelance 2019 SP1 FP1 RU3

Table 1. Supported Sytems

Control System	Supported Major Versions	Supported Rollup Versions
Advant Master controllers	- Advant Master Controllers: AC 450, AC 410, MP 200/1, Safeguard 415, MG 230/1, AC 160, AC 110, AC 70, 450 RMC	
	- 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	- Melody Composer 4.0 to 7.x - 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	
Harmony Rack controllers (LCS only)	- S+ Engineering 1.0 to 2.4 - Harmony Composer 5.1, 6.0 till 7.2	

Table 1. Supported Sytems

Control System	Supported Major Versions	Supported Rollup Versions
Harmony Rack/ Symphony Din controllers (For Performance collection)	- 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/IIT13/IEB800 is supported. - To scan the network through an IEB bridge, it is suggested to start the data collection from the PN800 network. Data collection messages that traverse the bridge, require as minimum firmware version for the IPT800, B.0 or higher.	
S+ Operations HMI	- 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)	

Table 1. Supported Sytems

Control System	Supported Major Versions	Supported Rollup Versions
System 800xA	- 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 - 6.2	- SV5.1 Rev D Rollup 5, SV5.1 Rev E Rollup 2, SV5.1 FP4 Rev D Rollup 4, SV5.1 FP4 Rev D Rollup 5, SV5.1 FP4 Rev E Rollup 3, SV5.1 FP4 Rev E Rollup 4, 6.0.3.3 Rev B - 6.0.1 Rollup 1, 6.0.3 Rollup1, 6.0.3 Rollup 2, 6.0.3 Rollup 3, 6.0.3 Rollup 4, 6.0.3.3 Rev B - 6.1 Rollup 1
QCS with System 800xA HMI	- 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	
Non-ABB Systems (Cyber security data only)	- All Windows Operating systems with .Net framework version 3.5 SP1 or above installed.	
ESXi	- 6.0, 6.7, 7.0	

1.3 Compatibility

MCS-DC 2.5 or newer versions are compatible with MCS-FW version 1.4 and above. These are not backward compatible. MCS-FW 1.4 is compatible with MCS (on-premise) V5.6 and newer versions. Refer to the Digital Service Products Life cycle Plan[5] Section 6, Additional Information

2 Prerequisites

In this section are listed the prerequisites that must be met before starting data collection.

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.

- MCS-DC must be deployed in the node from which data collection must be launched. Based on the system and the controllers that must be collected, the suggested launch node may vary. Details are described in each system data collection process section.
- The User must have Administrator rights. For a Domain network, the User must also be a member of the Domain administrator group.
- The minimum screen resolution is 1280x800 (Height 1280, Width 800)

- Microsoft Windows User Access Control (UAC) must be disabled if the system is in work group network. Check if the UAC is disabled.

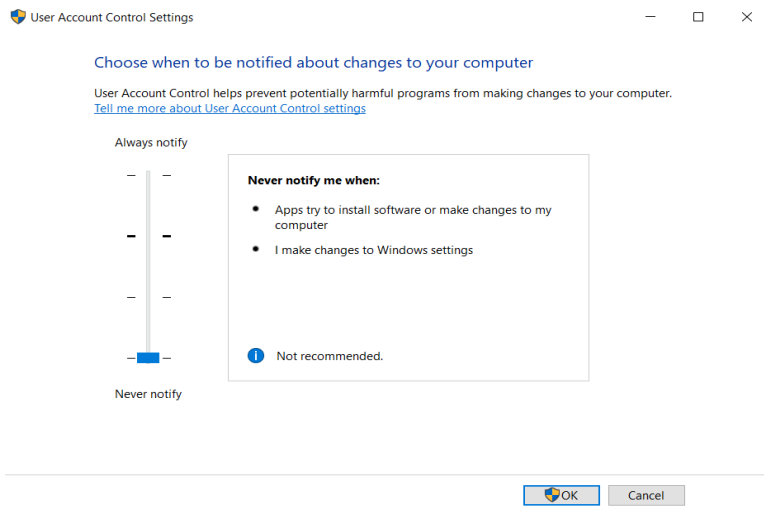

Figure 1. User account control settings (UAC)

- MCS-DC uses port number 23571 as default. Should you need to use a different port, refer to Appendix A 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.
- 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).

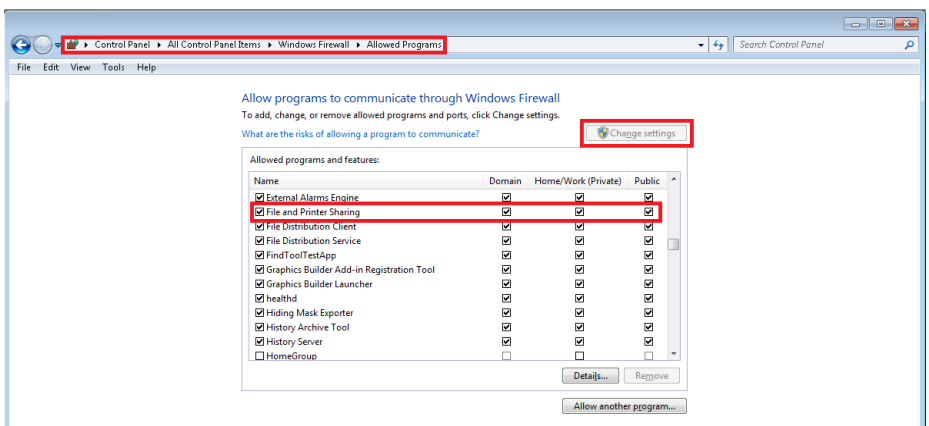

Figure 2. File and Print sharing

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

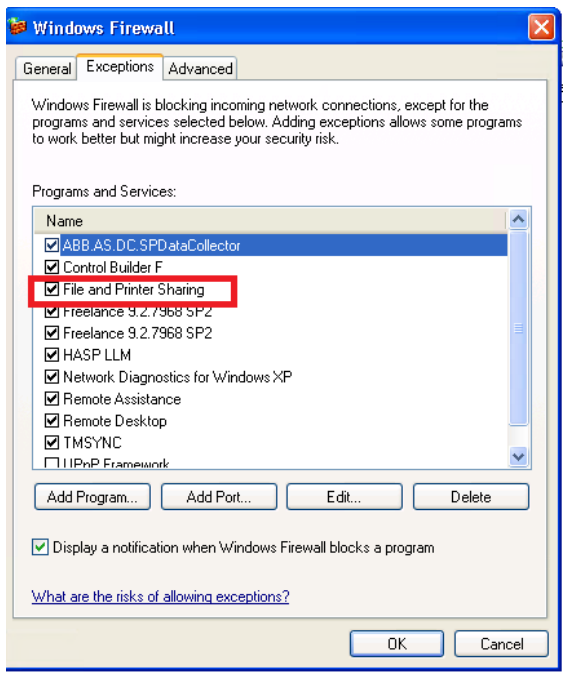

Figure 3. File and printer sharing for Windows XP

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

  The procedure to “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 Section 5, Troubleshooting for alternative method and troubleshooting.

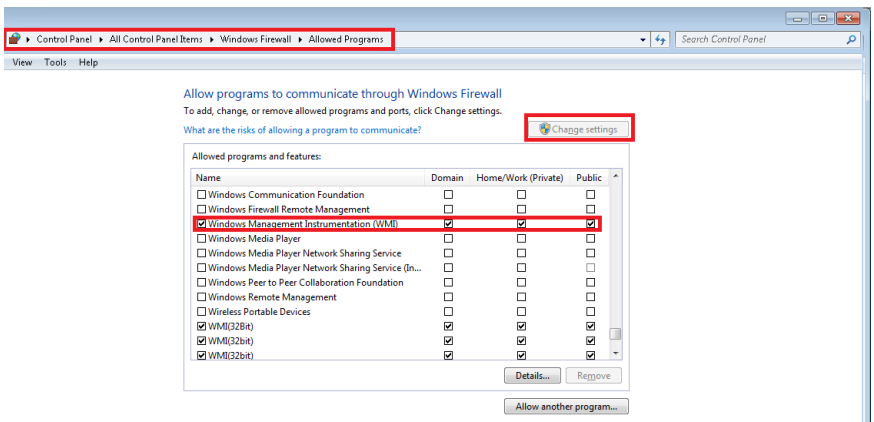

Figure 4. Windows Management Instrument (WMI)

- 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 user names 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.

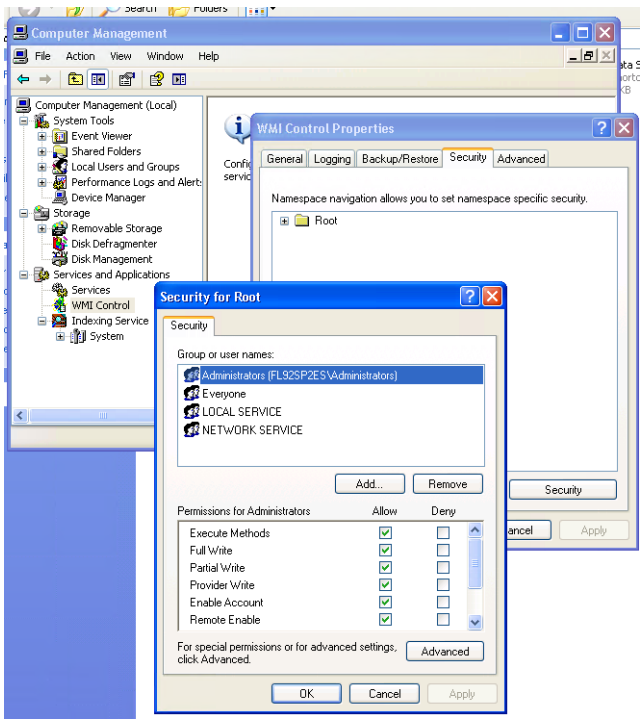

Figure 5. WMI for Windows XP

- Turn on Network Discovery.

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

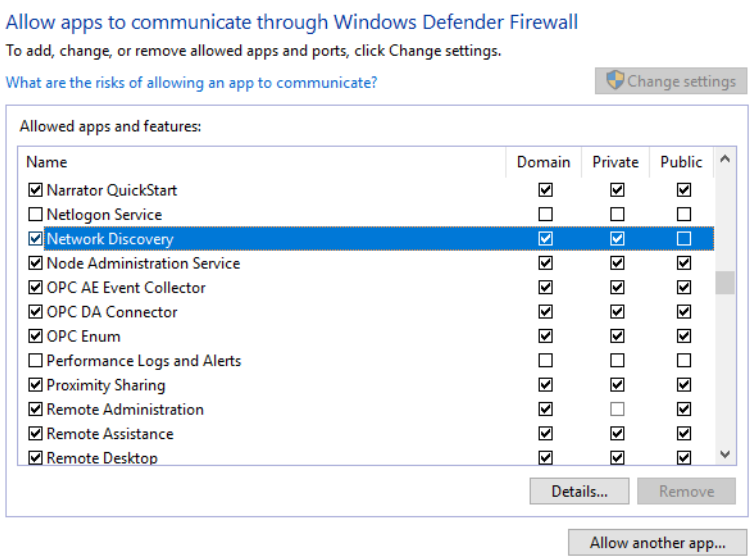

Figure 6. Turn on Network Discovery

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

2.2 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. Before launching the MCS-DC tool, it is mandatory to refer Appendix B for details on secured communication and to configure secured communication.
- 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.

2.3 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 3, Data Collection Process, in this user manual.

2.4 System 800xA

2.4.1 In Domain:

- Microsoft®.Net framework 1.1 or above.

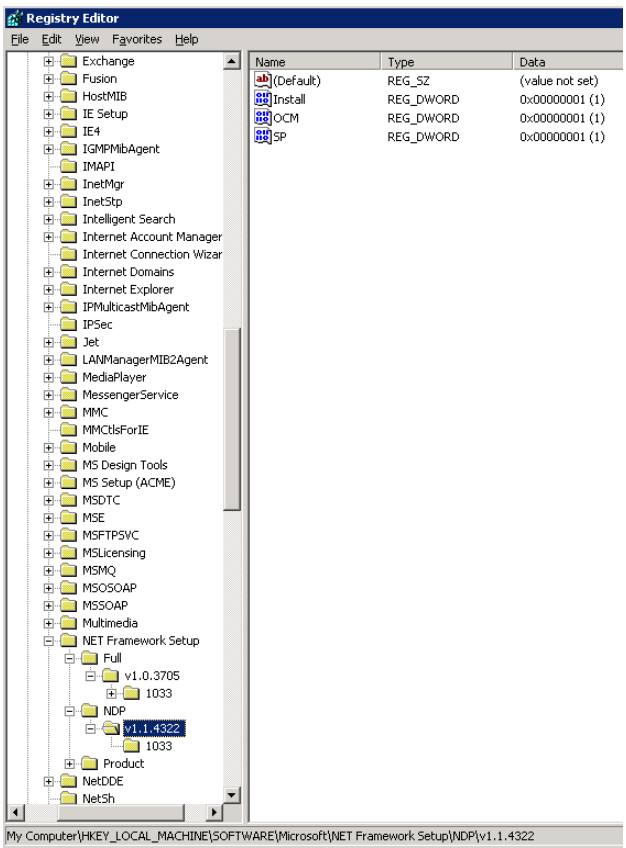

Figure 7. .Net framework 1.1

- Enable Windows Management Instrumentation (WMI).

  The procedure to enable **"Windows Management Instrumentation"** is different for old and new Operating Systems.

  - To enable WMI, go to Allow app through windows firewall in the firewall settings, click on change settings to enable the WMI for all networks (Domain, Public and Private). Refer Section 5, Troubleshooting for alternative method and troubleshooting.

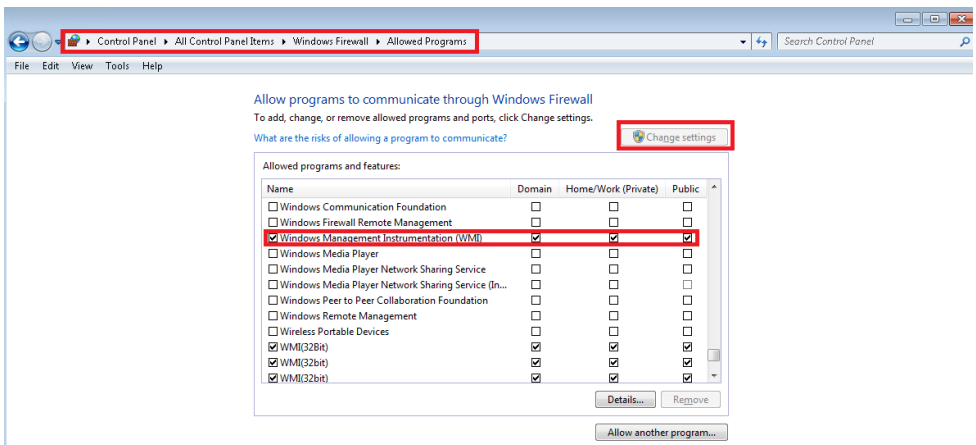

Figure 8. Windows management Instrument (WMI)

- 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 user names 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.

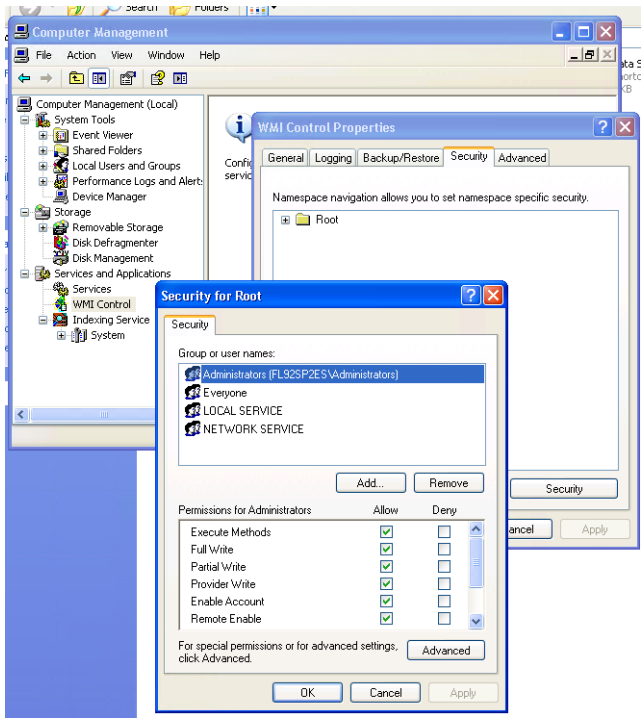

Figure 9. WMI for Windows XP

- Start “Windows Management Instrumentation” service from services if it is not already running on all nodes.

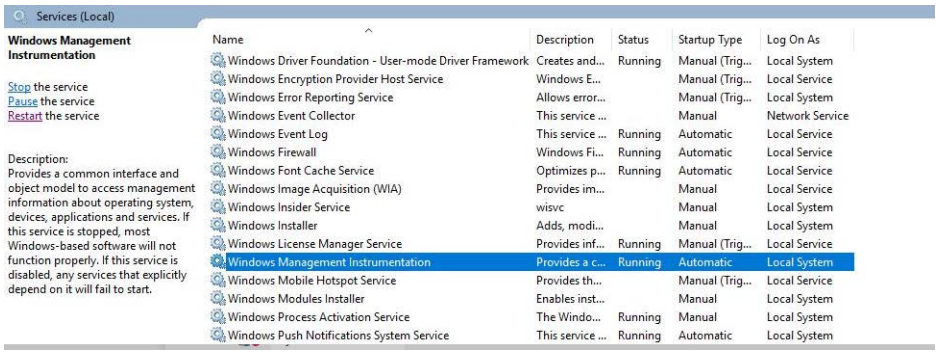

Figure 10. WMI running

- User accounts and passwords with administrative rights are required for all 800xA computers.
- The launch node of MCS-DC must be part of a running 800xA System.
- 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.

2.4.2 In Workgroup:

- Microsoft®.Net framework 1.1 or above

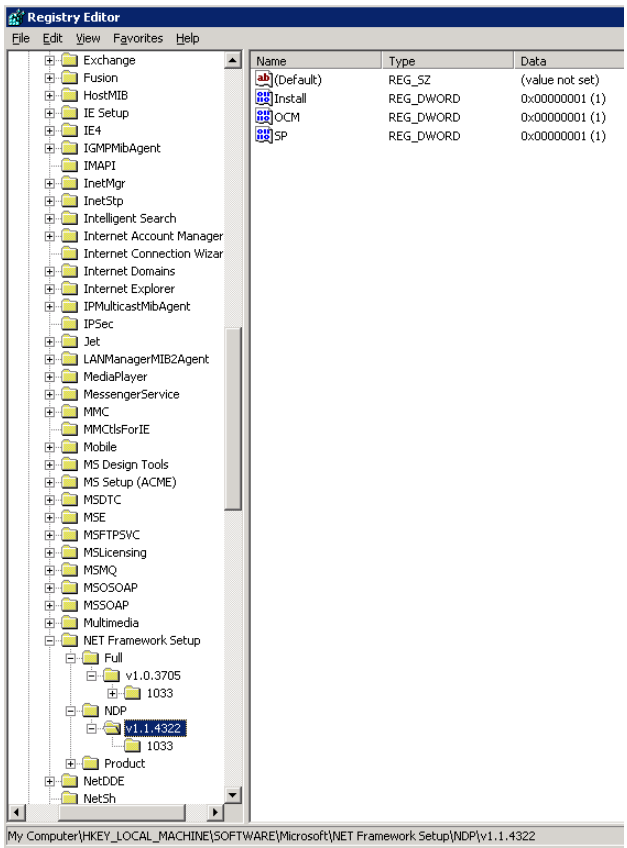

Figure 11. .Net 1.1 or above

- Start “Windows Management Instrumentation” service from services if it is not already running on all nodes.

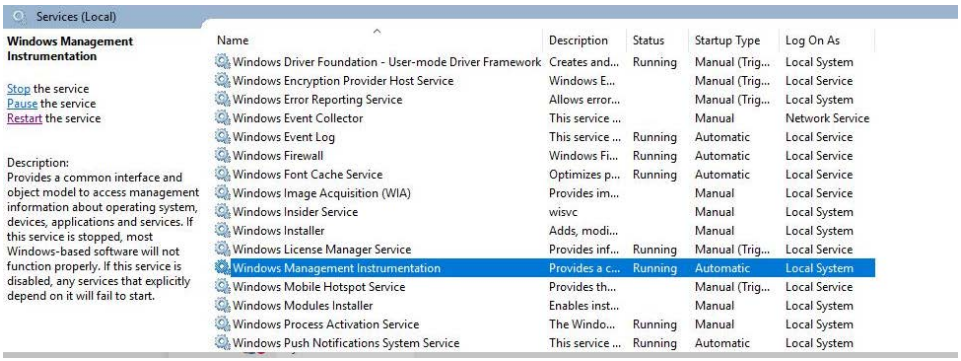

Figure 12. WMI Running

- Create a new registry key LocalAccountTokenFilterPolicy under 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. For detailed procedure on disabling UAC, Section 5, Troubleshooting.

- Enable Windows Management Instrumentation (WMI).

  The procedure to **“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 Section 5, Troubleshooting for alternative method and troubleshooting.

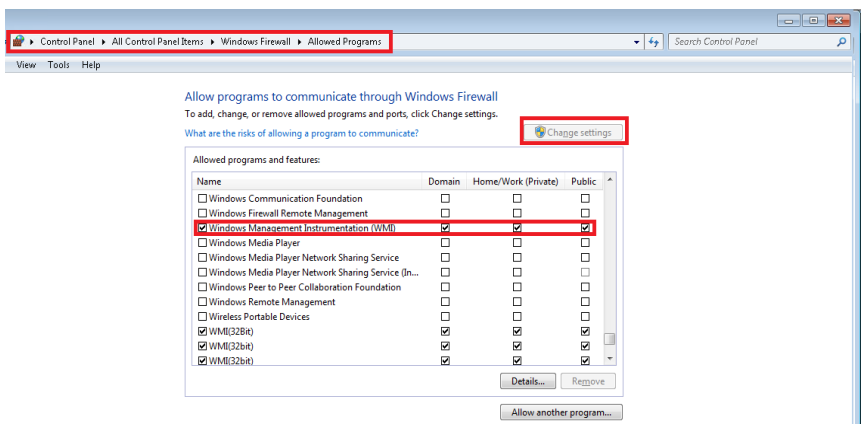

Figure 13. Enable Windows Management Instrumentation

- 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 user names 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.

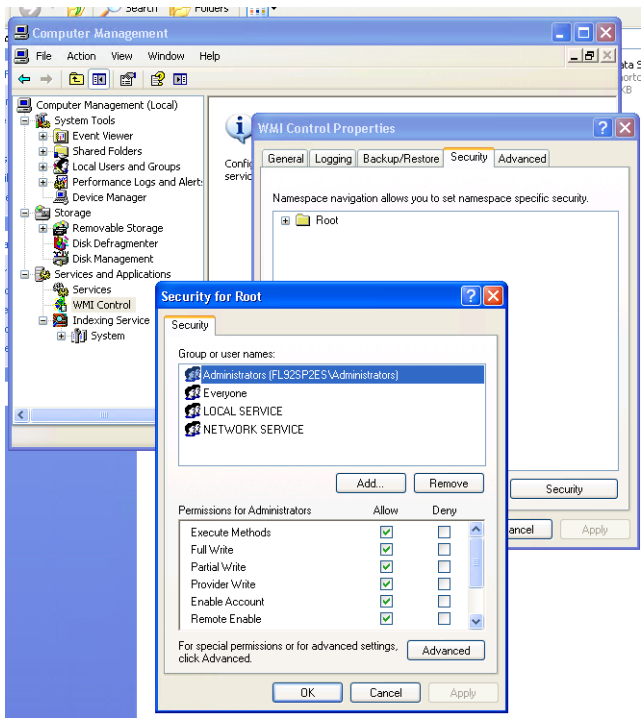

Figure 14. WMI for Windows XP

- User accounts and passwords with administrative rights are required for all 800xA computers.
- 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 (hpcisss2.sys) or lower.
- It is important to revert all the changes made as part of prerequisite settings, after completing the data collection.

2.5 Freelance System

- The following are the prerequisites for freelance data collection. In order to determine whether the pre-requisites are met on each computer node in the network, a tool was created that not only finds whether the pre-requisites are met, but also assists the user in installing them if they are not. With the help of the tool, changes can be reverted after data collection. The tool is described in more detail in Appendix G.

- 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.

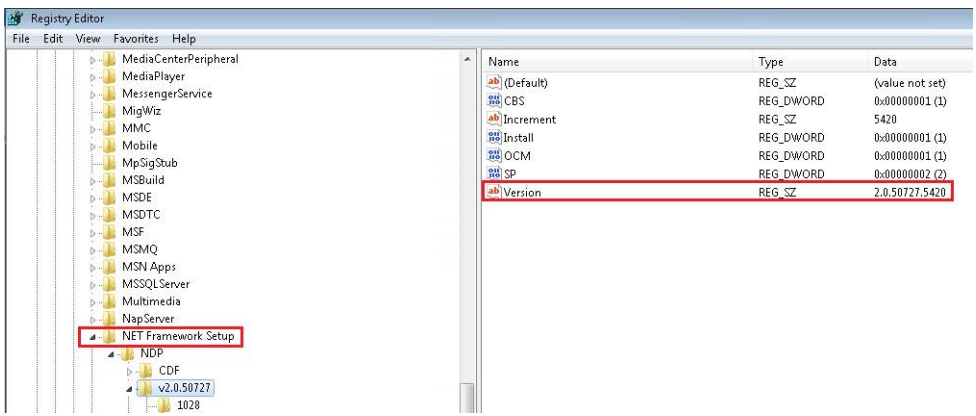

Figure 15. .Net Framework version

- 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).

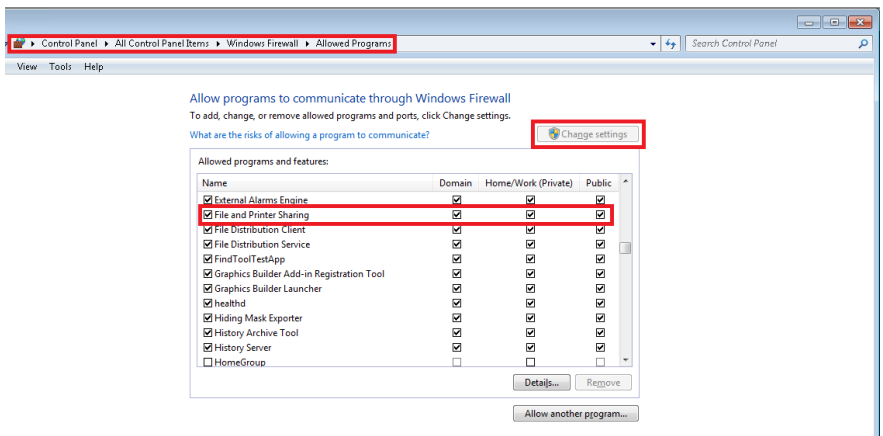

Figure 16. Enable file and printer sharing

- In case of Windows XP open the Windows Firewall exceptions from the Control Panel and enable File and Printer sharing.

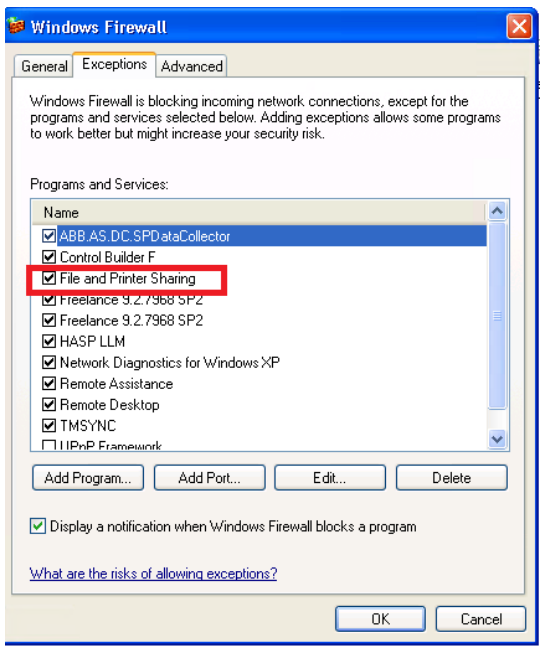

Figure 17. File and printer sharing for Windows XP

- 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 5.5, Troubleshooting Issue 2 for more details.

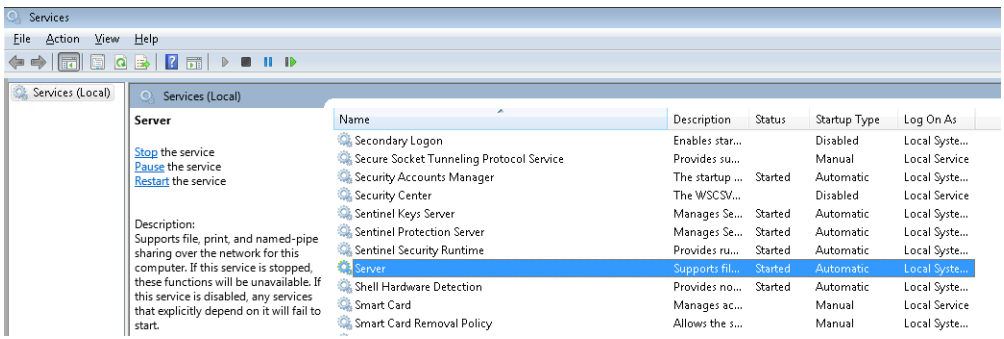

Figure 18. “Server” running in windows services

- Start “Windows Management Instrumentation” service from services if it is not already running on all nodes.
- Disable User Account Control. In order to disable the UAC completely 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. For detailed procedure on disabling UAC, refer Section 5, Troubleshooting.
- Enable Windows Management Instrumentation (WMI).

The procedure to enable **"Windows Management Instrumentation"** is different for old and new Operating Systems.

To enable WMI for new Operating Systems go to "Allowed Programs" in the Windows Firewall settings, and select change settings to enable the WMI for all networks (Domain, Public and Private). Refer to Section 5, Troubleshooting for an alternative method and for troubleshooting instructions.

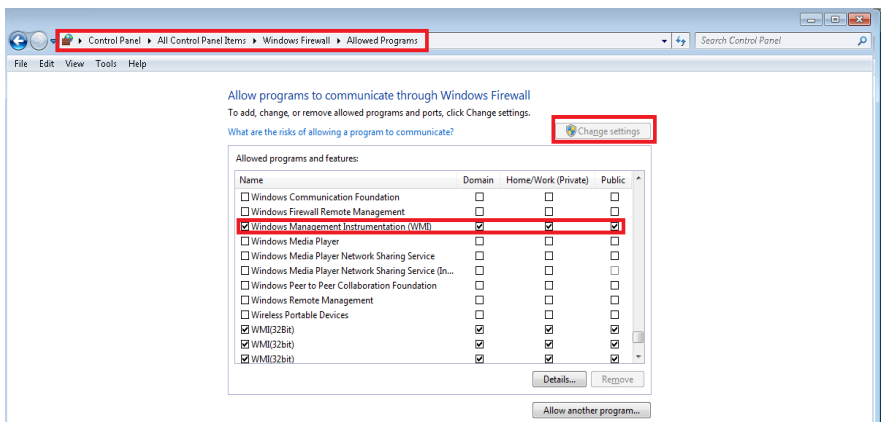

Figure 19. Enable Windows Management Instrumentation

- 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 user names 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.

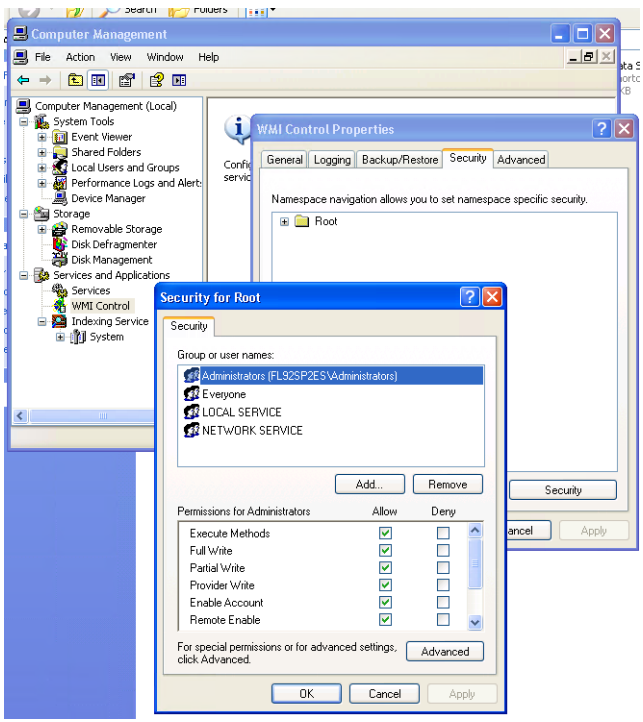

Figure 20. WMI for Windows XP

- Turn on Network Discovery.

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

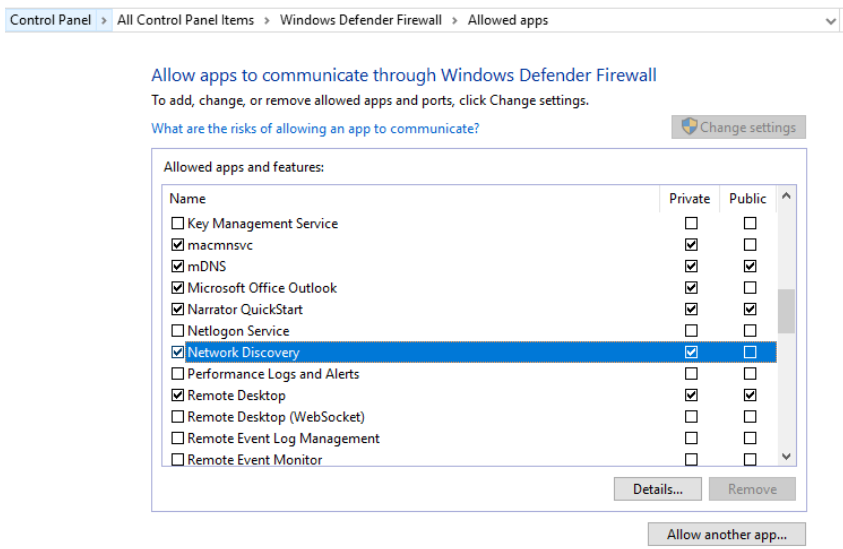

Figure 21. Turn on Network Discovery for Private profile

- 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 forceguest 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.

2.6 S+ Operations

The following software is required for installation and operation of S+ Operations Data Collector.

- .NET Framework 4.0 and above.

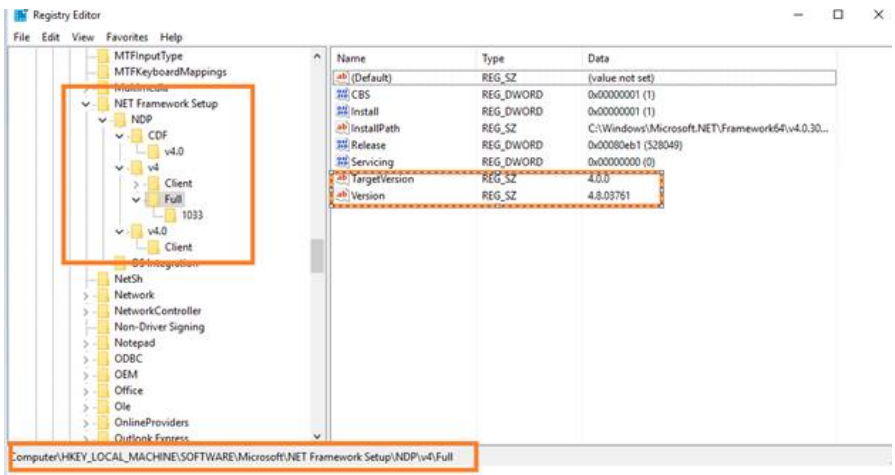

Figure 22. .Net Framework 4.0 and above

- Enable file and Printer sharing.

  The procedure to **“Enable file and Printer sharing”** is different for legacy and modern operating systems.

- For newer operating systems, Allow app through windows firewall in the firewall settings, click on change settings to enable the File and Printer sharing service for all networks (Domain, Public and Private).

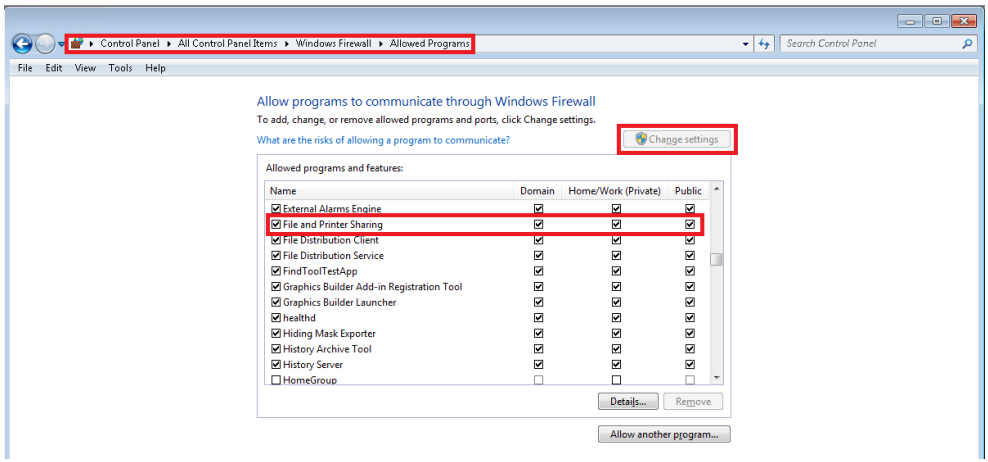

Figure 23. Allow File and Printer sharing

- In case of windows XP, open windows firewall exceptions in control panel and enable file and printer sharing.

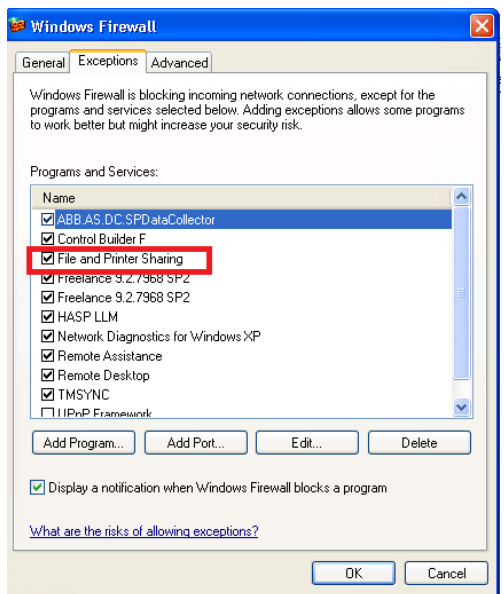

Figure 24. File and printer sharing for Windows XP

- Enable administrator share access in windows. To enable the administrator share access refer Section 5.5, Troubleshooting Issue 2.
- Enable Windows Management Instrumentation (WMI).

  The procedure to **“Windows Management Instrument”** 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 Section 5, Troubleshooting for alternative method and troubleshooting.

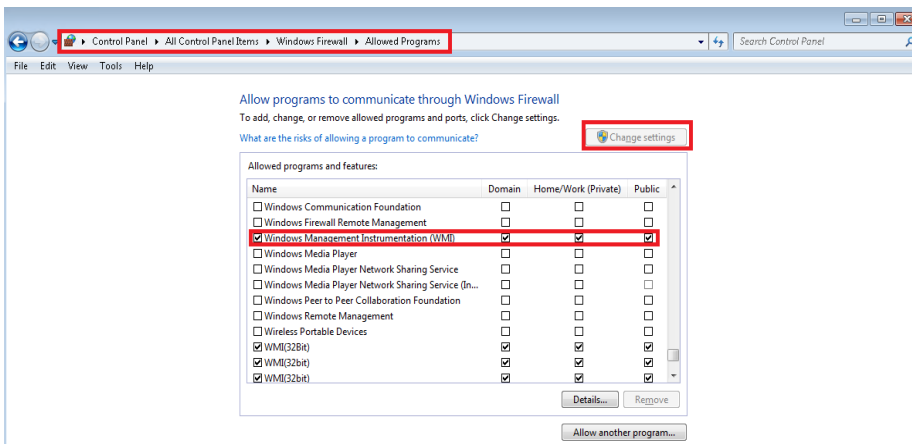

Figure 25. Enable Windows Management Instrument

- 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 user names 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.

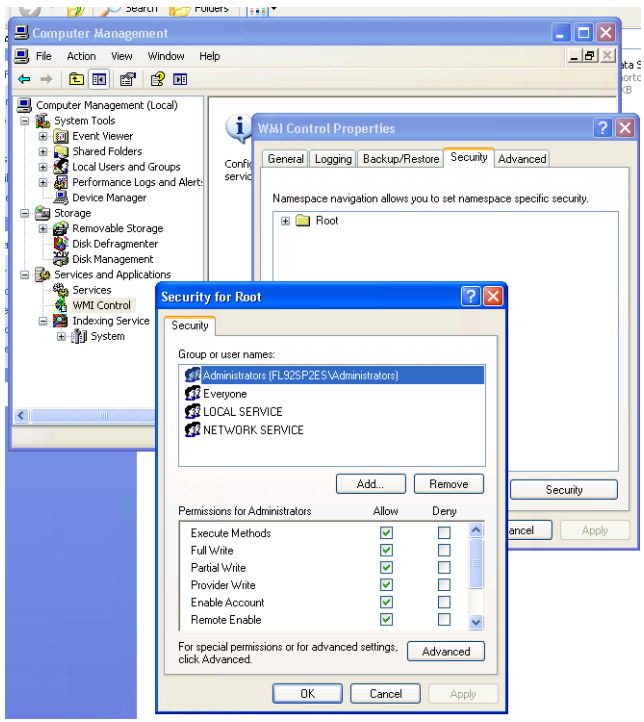

Figure 26. WMI for Windows XP

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

2.7 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.

2.8 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.

2.9 Melody Rack controllers

- Microsoft® .Net framework 3.5 SP1 or above.

2.10 Advant MOD 300

- Exported System or Project configuration file is an important prerequisite to collect life cycle 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.

2.11 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 life cycle 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.

2.12 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.

2.13 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.

2.14 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.

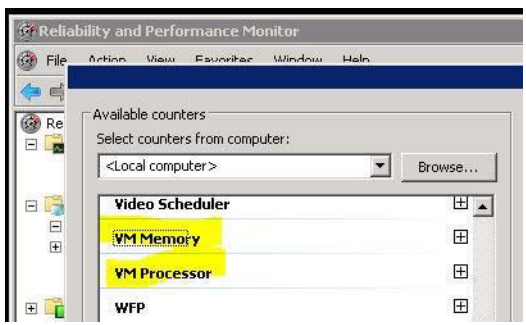

Figure 27. VM Performance Counters

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 on 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).

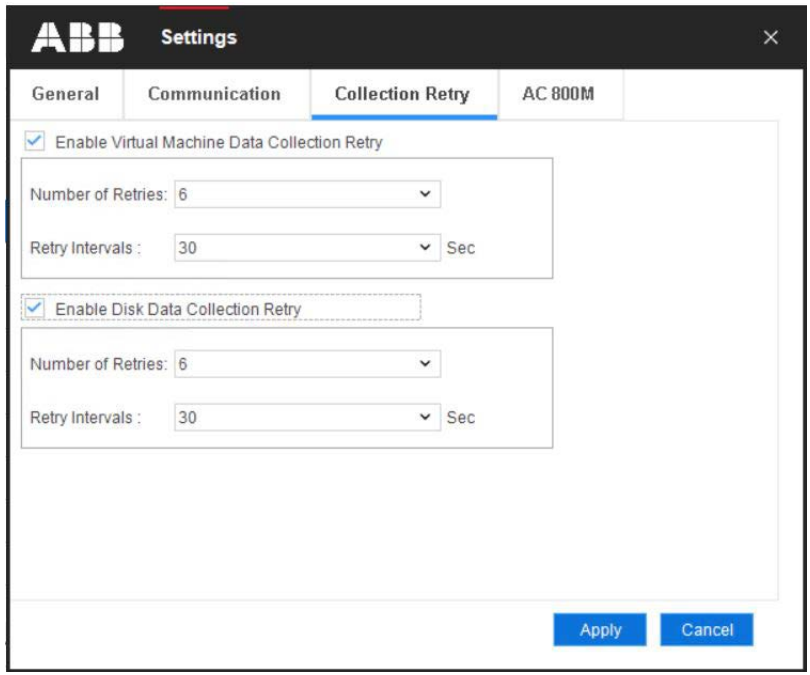

Figure 28. Collection Retry

3 Data Collection Process

MCS-DC has two modes of operation

- Basic mode
- Advanced mode

3.1 Basic Mode

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 life cycle 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.

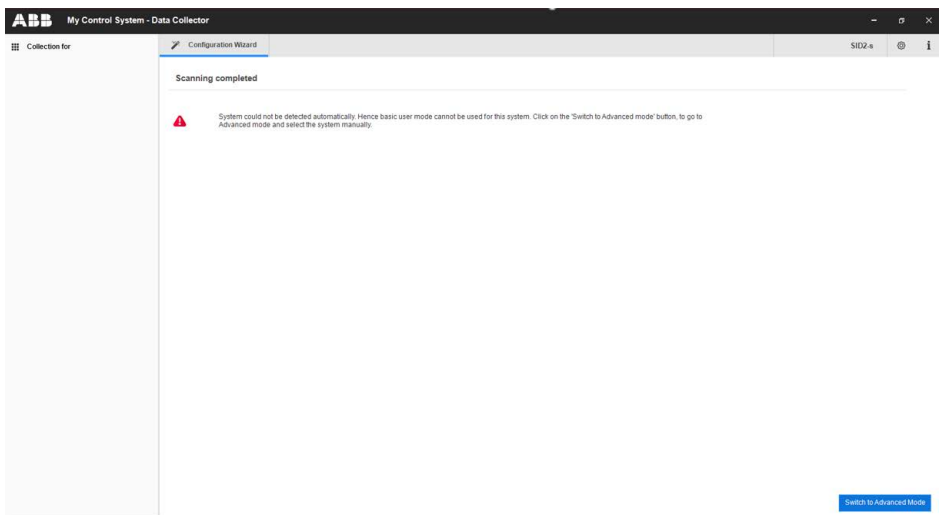

Figure 29. Switch to Advanced Mode

3.2 Advanced Mode

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 Life cycle), 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.

3.3 Basic Mode Data Collection

3.3.1 Basic mode data collection for System 800xA

1. Deploy MCS-DC in the hard drive (Operating System partition) of the node from which data collection must be executed. Depending on the HMI/Controller, MCS-DC launch nodes may vary. 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.Please note, basic mode is not supported for 800xA HMI with Harmony Rack controllers and 800xA HMI with Procontrol P13 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 contollers:

     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

2. Double-click the **MCS-DC_Launcher.exe**, to launch the tool. It is present inside the unzipped MCS-DC folder. The initial screen appears as shown in Figure 30. MCS-DC tool runs the below checks on the launch node. If the checks are passed, a Green tick mark is shown, click the **Launch** button to proceed for data collection. If the checks fail, a Red cross mark is shown, user has to fix the issue and launch the MCS-DC tool again.

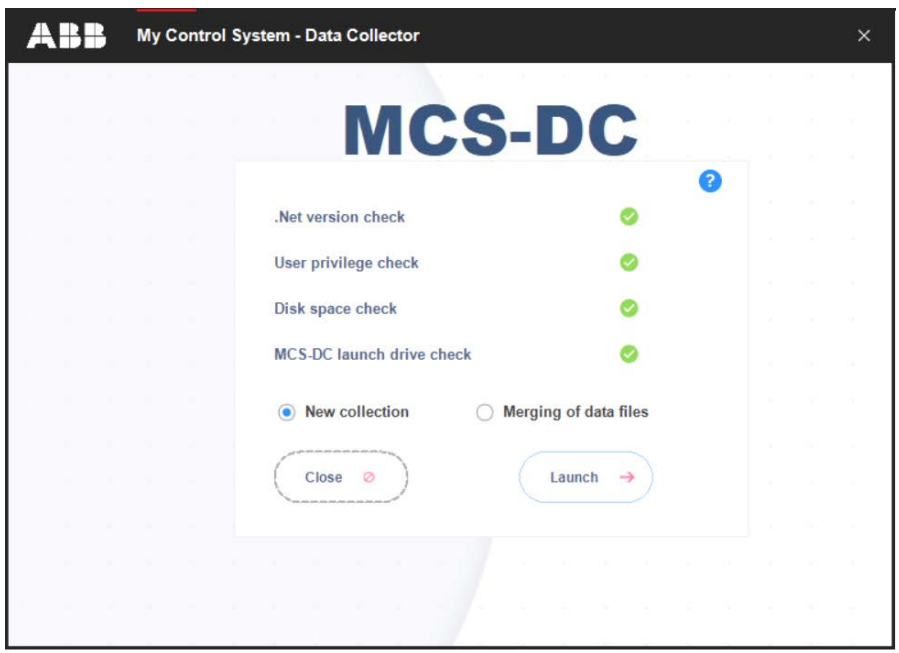

Figure 30. .NET Framework version check and Prerequisite check status

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.

- .NET Framework version check

  If the .NET Framework version is 1.1 or above, then this check is passed and MCS-DC 2.X version can be launched for data collection.

  If the .NET Framework version is lower than 1.1, then this check is failed and MCS-DC 2.X version cannot be launched for data collection, instead MCS-DC 1.9.x version 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.

  a) User privileges check, checks if the MCS-DC is launched in the user account with administrator privileges.

  b) System drive launch check, MCS-DC tool must be launched only from the local disk drive of the launch node.

  c) 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.

3. Provide the System ID of the 800xA system and your full name and provide Password for encryption. This 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.

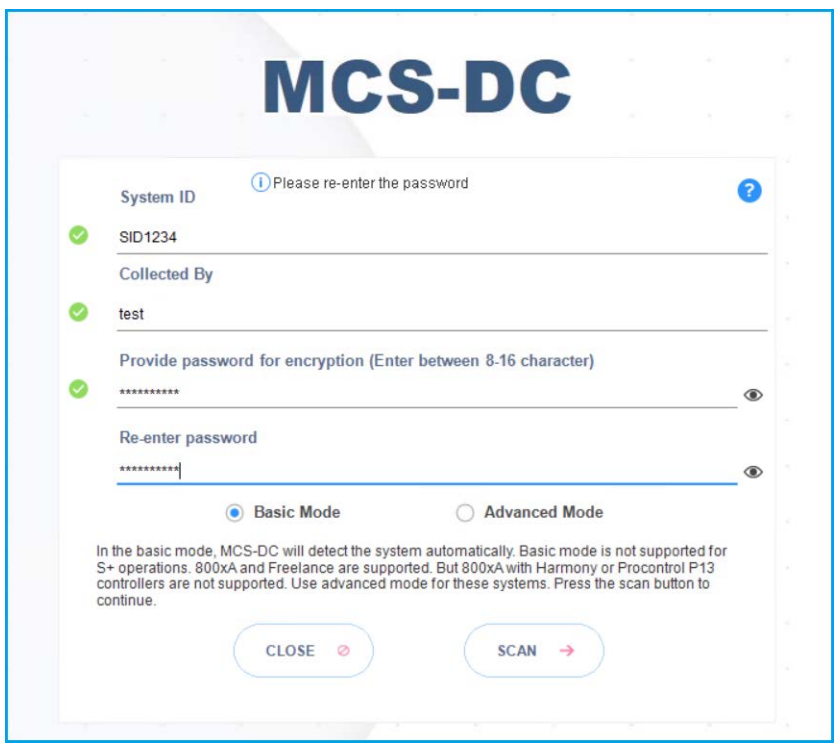

Figure 31. Provide System ID

4. Select Scan button to start the system scan. This results in the identification of the HMI, the controller and the 800xA System version. 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.

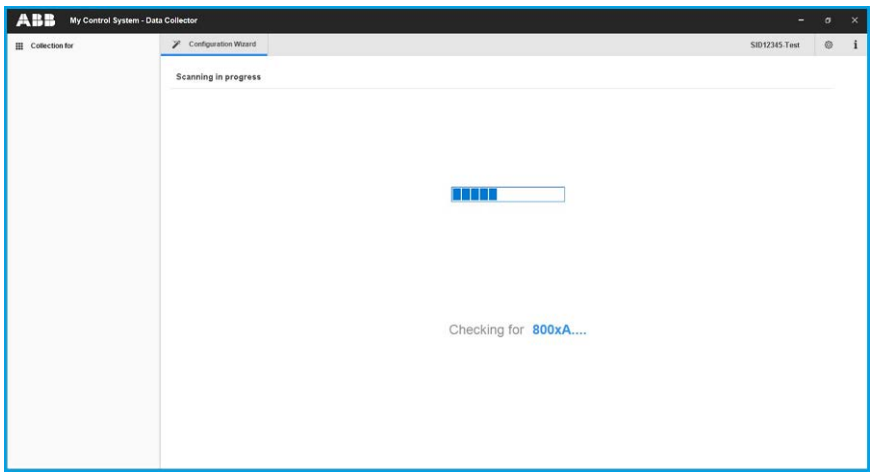

Figure 32. System Scan

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

   Below are the supported controllers related to 800xA HMI on this release:

   - AC 800M
   - AC 800PEC
   - AC 70, 110, 160
   - Freelance
   - AC 410, 450, MP, SG 400
   - Melody Rack
   - MOD 300
   - QCS

6. Below are the supported data category options for 800xA HMI:
   - Performance
   - Life cycle
   - Software
   - Security (Cyber security)

7. Below are the supported data category options for the controllers:
   - AC 800M:

     a) Performance

     b) Life cycle
   - AC 800PEC:

     a) Life cycle
   - AC 70, 110, 160:

     a) Life cycle
   - Freelance:

     a) Performance

     b) Life cycle
   - AC 410, 450, MP, SG 400:

     a) Performance

b) Life cycle

- Melody Rack

  a) Performance

  b) Life cycle

- MOD 300

  a) Life cycle

- QCS

  a) Life cycle

8. Refer below the required inputs for each system:

The procedure to export system configuration files can be found in Appendix D

- 800xA HMI:
  IP range (to scan and detect non-800xA nodes) Admin user credentials to access all computer nodes.
- AC 800M controller:

  No input settings are needed for collecting performance and life cycle data from AC800M 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 on the top right corner) and select the tab AC800M. 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 15MB. Other possible choices are 5, 10, or 20 MB maximum. File collection can be disabled by unchecking the provided check box.

  By default, AC800M 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.

  The collection of AC 800M lifecycle data from a system with a large number of control structure objects (for e.g a large number of redundant IO modules) may time out in certain rare cases. Users are advised to uncheck the option 'Collect redundant devices' in such cases and proceed with the collection process.

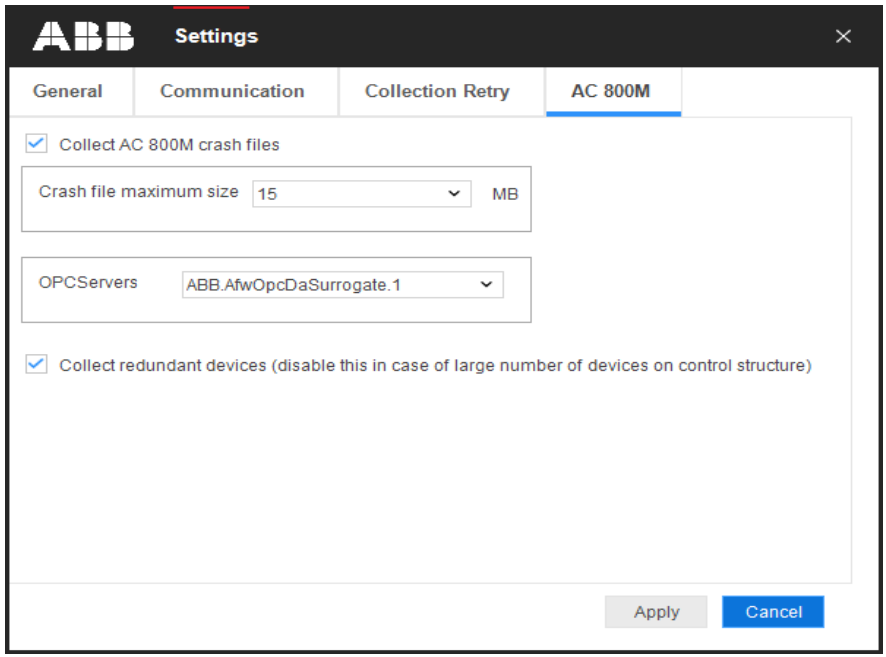

Figure 33. AC 800M data collection settings

- AC 70, 110, 160 Controllers:
  File location of customer project (.BAX file)
- Freelance Controller:
  File location of customer project (.csv/.csvs file). If the customer project file type is .csvs, user has to provide the customer project decryption key.
- AC 410, 450, MP, SG 400 Controllers:
  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.

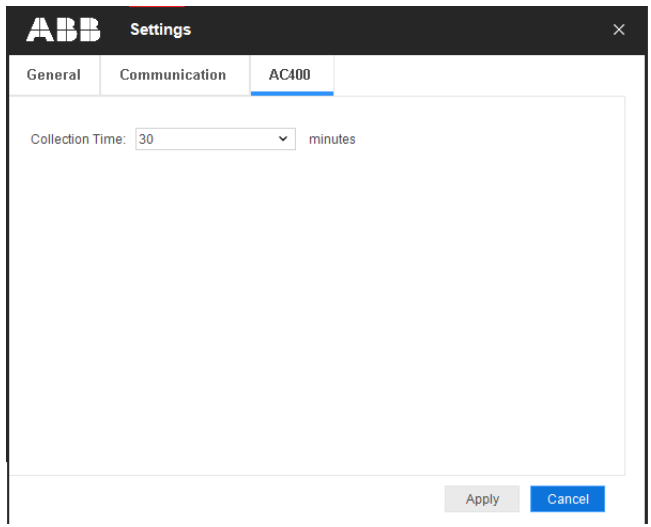

Figure 34. Collection time interval

- Melody Rack Controller:
  Melody Island Devices
  CSE_Conf File
  Asset Export Folder
  Composer Melody node IP Address
  User-name
  Password
- MOD300:
  Latest ATF file from AdvaBuild engineering node
- QCS controllers:
  Latest config.xml file from QCS connectivity server

9. 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.

10. 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.

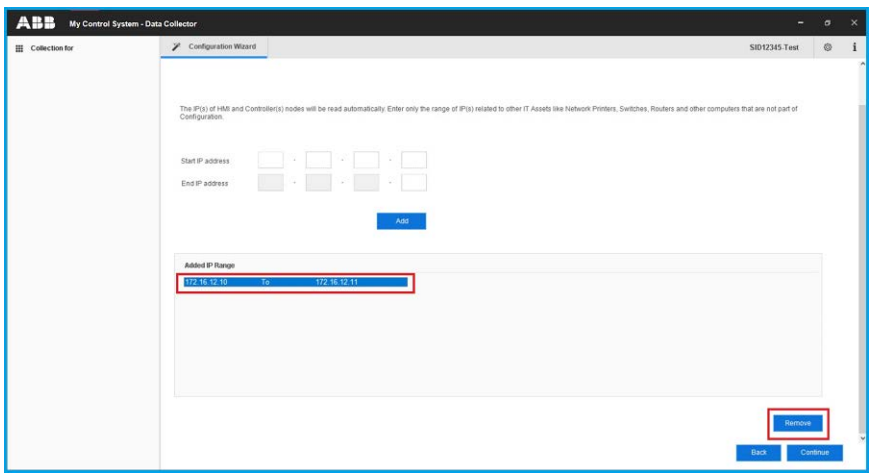

Figure 35. IP range Input

11. 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, life cycle and security data can be collected.

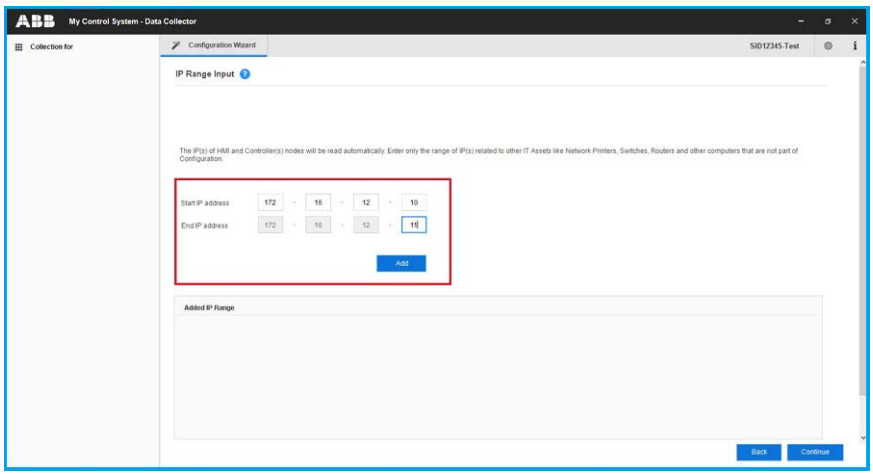

Figure 36. IP Details

12. 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, life cycle and security data can be collected.

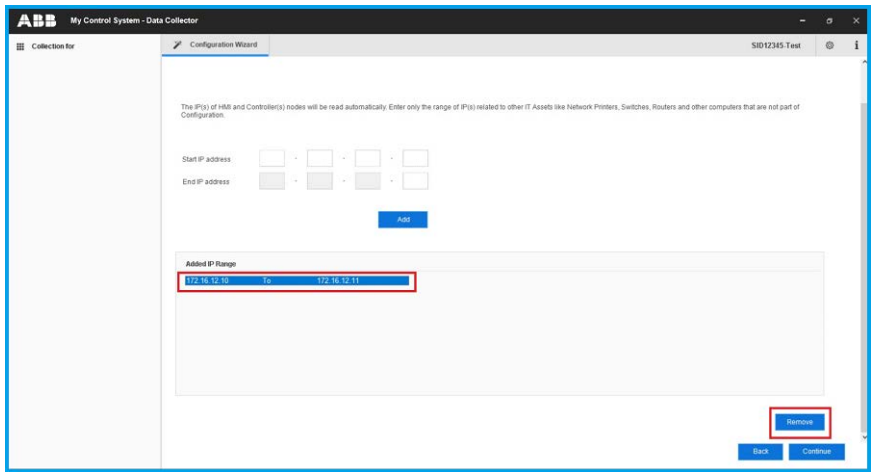

Figure 37. IP Range Input

13. Click on the **Continue** button to proceed. There is option to go back to the previous window in each step of the configuration.

14. 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 2.4, Prerequisites. Click the Add button.

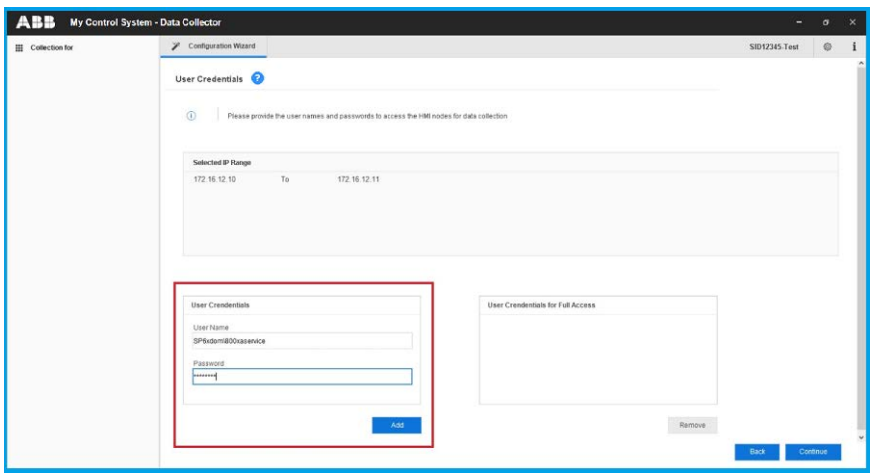

Figure 38. User Credentials

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

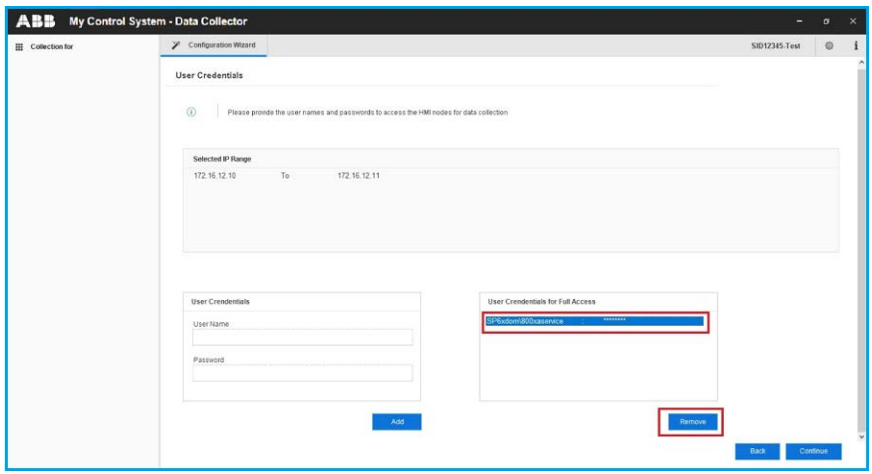

Figure 39. User Credentials

16. If the 800xA system 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 folder. 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.).

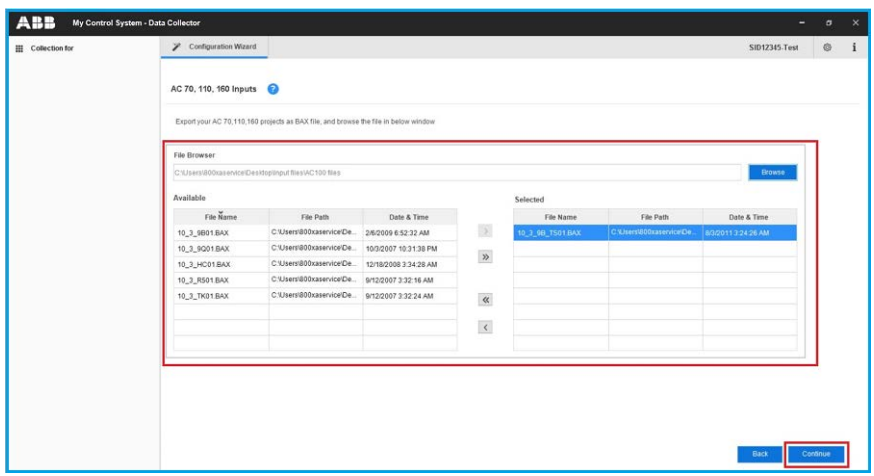

Figure 40. AC 70, 110, 160 Inputs

17. If the 800xA system 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).

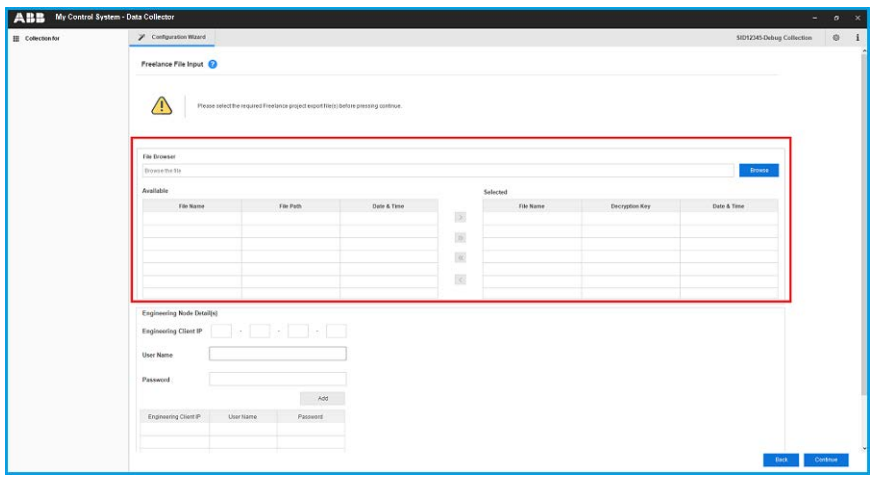

Figure 41. Freelance Input

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

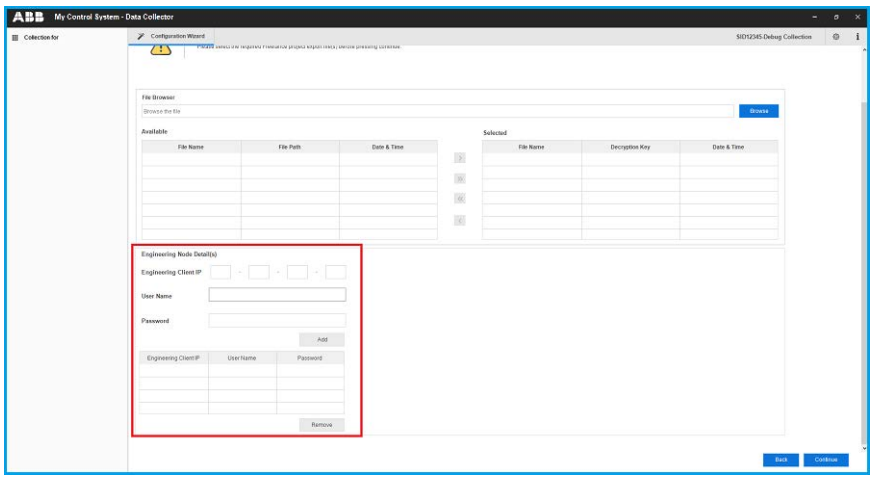

Figure 42. Engineering node IP

19. If the 800xA system 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 for exporting system configuration files).

    a. Melody Island Devices
    Click the **Browse** button to select the Melody Island Devices Export file

    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 user name

    f. Password
    Provide the Composer Melody node password

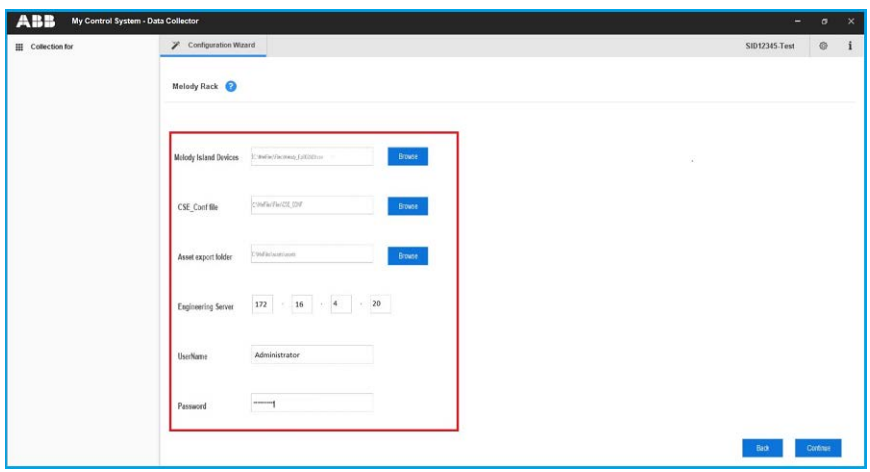

Figure 43. Melody Rack

20. If the 800xA system 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 for exporting system configuration files).

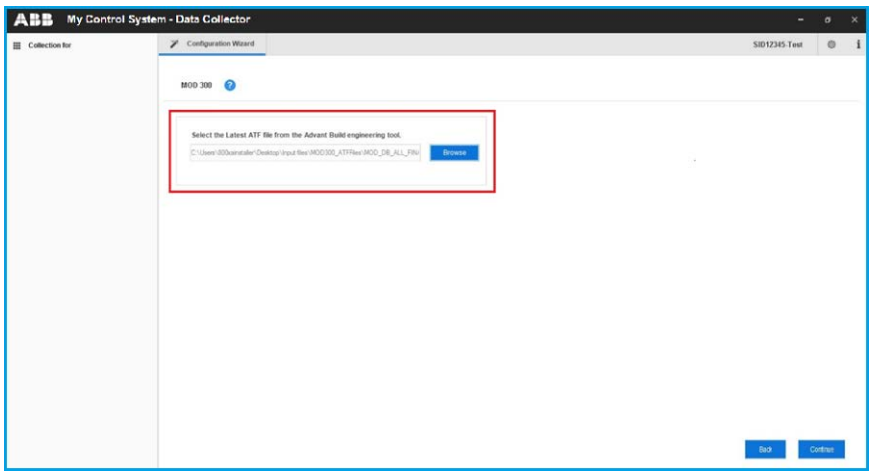

Figure 44. MOD 300

21. If the 800xA system 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.

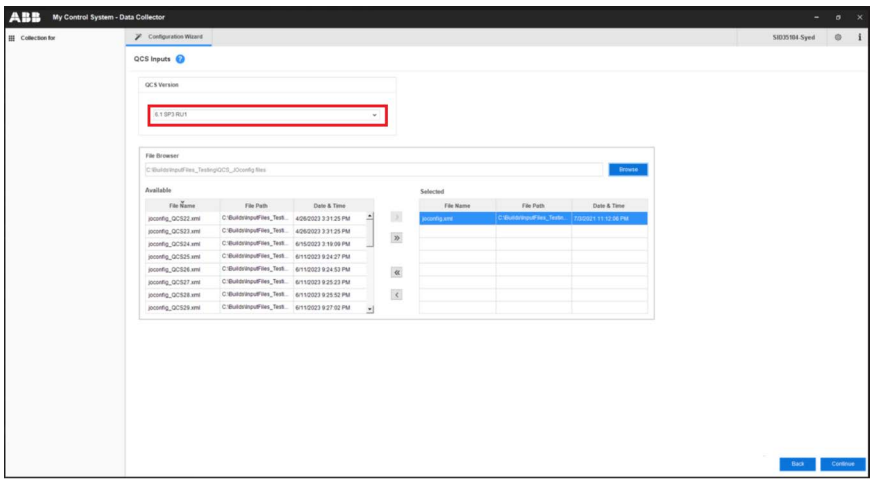

Figure 45. Configuration Wizard

22. 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 projects 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 sub-directories 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.

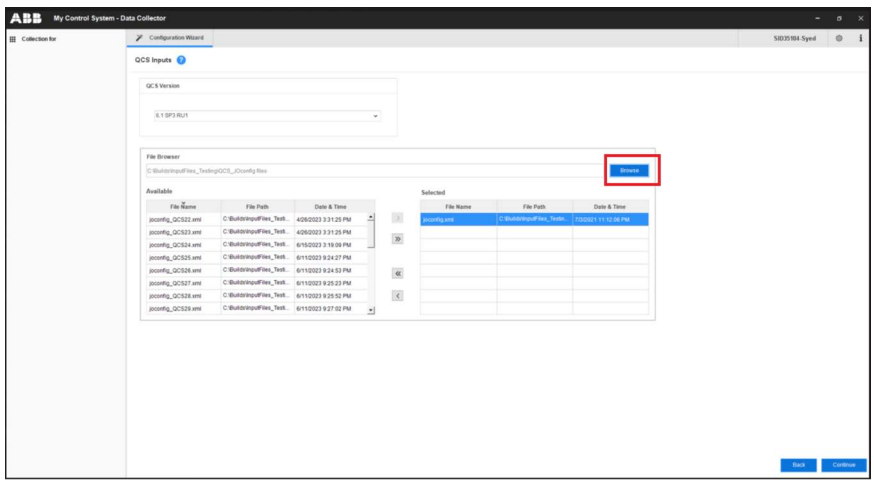

Figure 46. Browse option to browse joconfig.xml

23. 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 prerequisites by checking the check box 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 Section 2, Prerequisites.

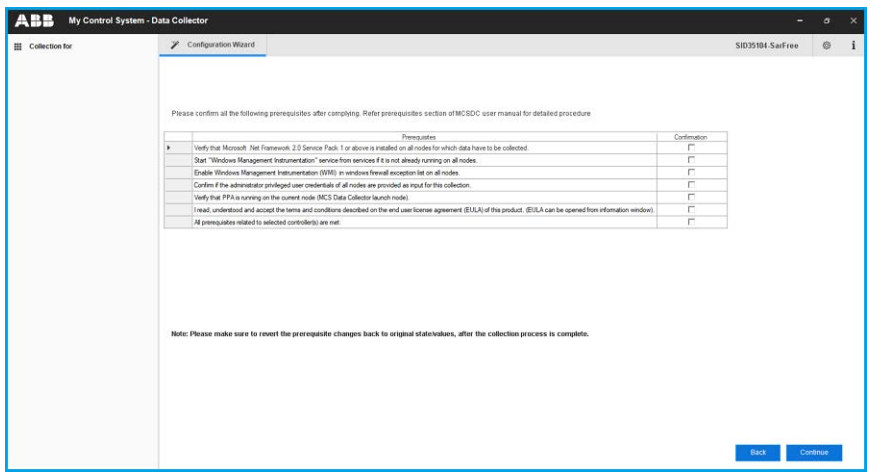

Figure 47. Configuration Wizard

24. Progress bar is shown to indicate the scanning progress.

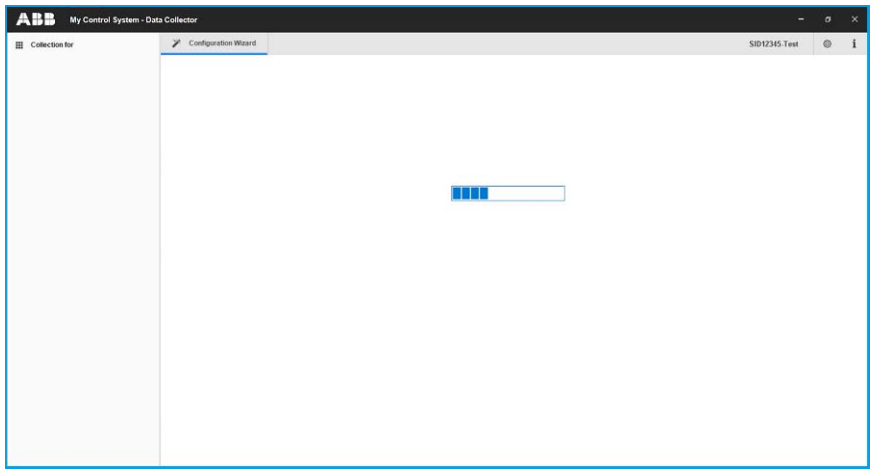

Figure 48. Progress

25. 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.

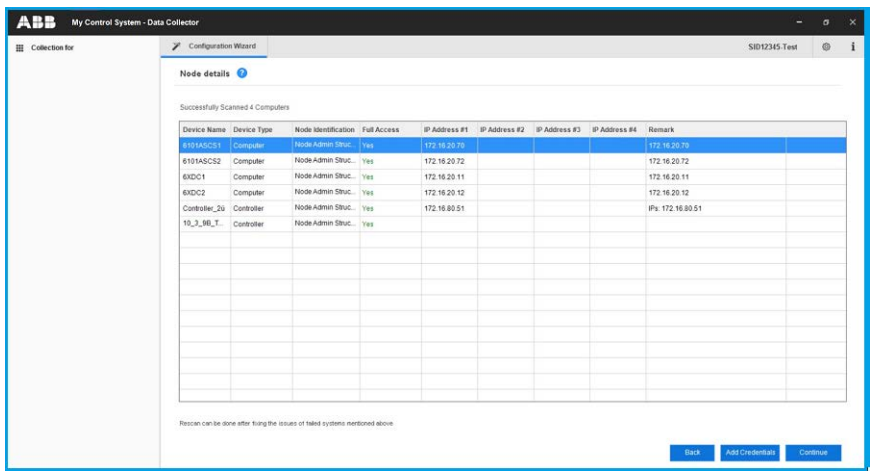

Figure 49. Node Details

26. 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.

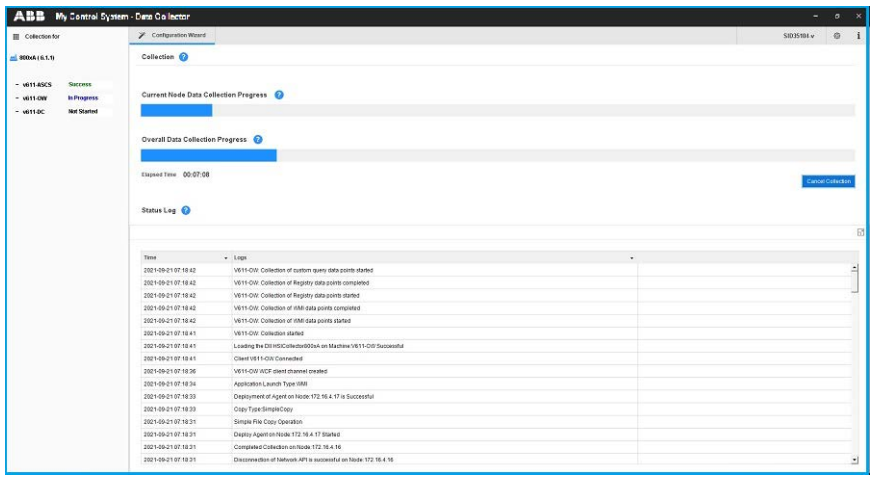

Figure 50. Data Collection

27. 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 that is successfully collected in the node.

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

28. 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.

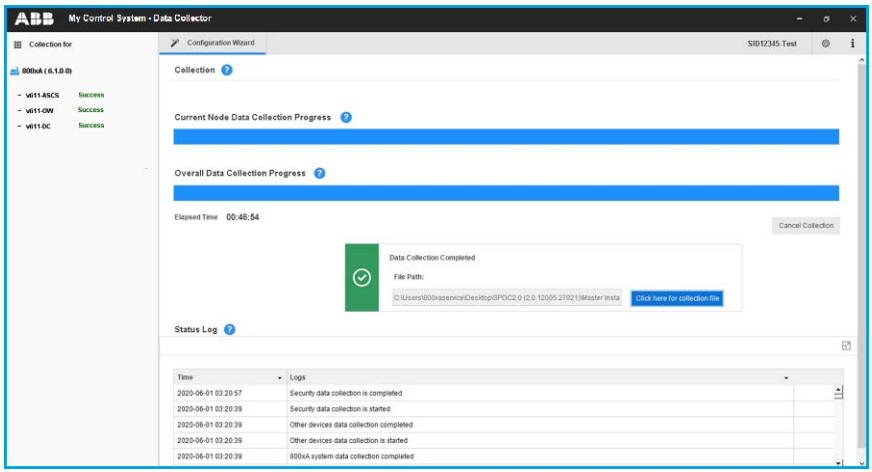

Figure 51. View Collection

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

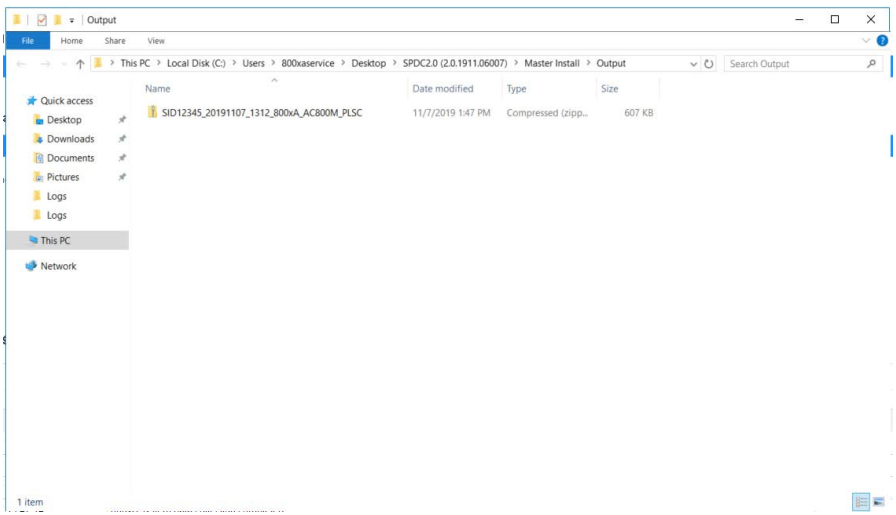

Figure 52. Collection Folder

3.3.2 Basic mode data collection for Freelance

1. Deploy MCS-DC in the hard drive (Operating System partition) of the node from which data collection must be executed. MCS-DC can be launched from any Freelance node.
2. Double-click the **MCS-DC_Launcher.exe**, to launch the tool. It is present inside the unzipped MCS-DC folder. The initial screen appears as shown in Figure 53. MCS-DC tool runs the below checks on the launch node. If the checks are passed, a Green tick mark is shown, click the **Launch** button to proceed with data collection. If the checks fails, a Red cross mark is shown, user has to fix the issue and launch the MCS-DC tool again.

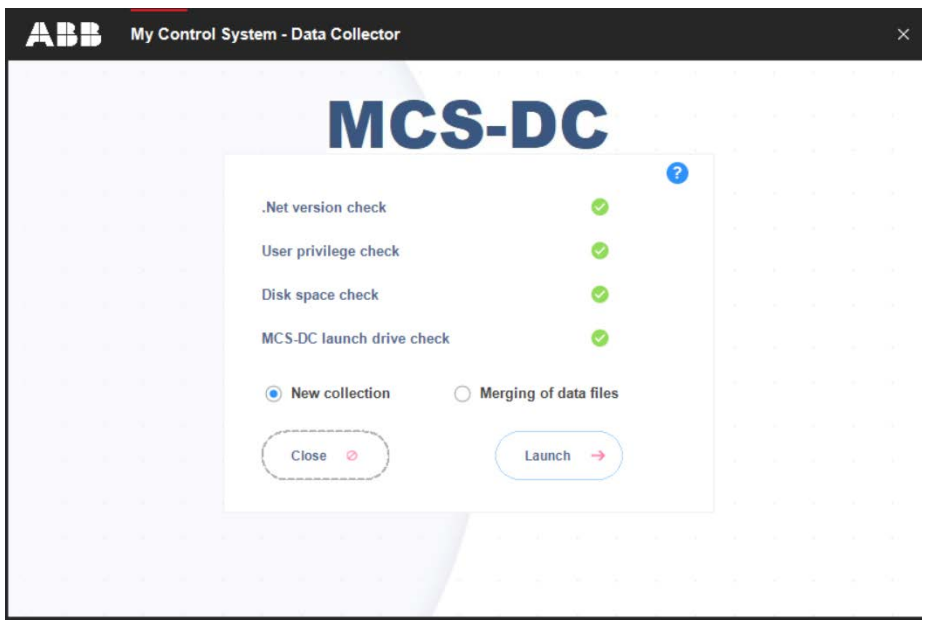

Figure 53. Launch Node Checks

- .NET Framework version check.

  If the .NET Framework version is 1.1 or above, then this check is passed and MCS-DC 2.X version can be launched for data collection.

  If the .NET Framework version is lower than 1.1, then this check is failed and MCS-DC 2.X version cannot be launched for data collection, instead MCS-DC 1.9.x version 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.

  a) User Privileges Check, checks if the MCS-DC Tool is launched in the user account with administrator privileges.

  b) System drive launch check, MCS-DC tool should be launched only from the local disk drive of the launch node.

  c) Required Disk Space Check, Free disk space of 500MB should be available on the disk drive from which the MCS-DC is launched.

3. Provide the System ID of the Freelance system and your full name and provide password for encryption. This 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.

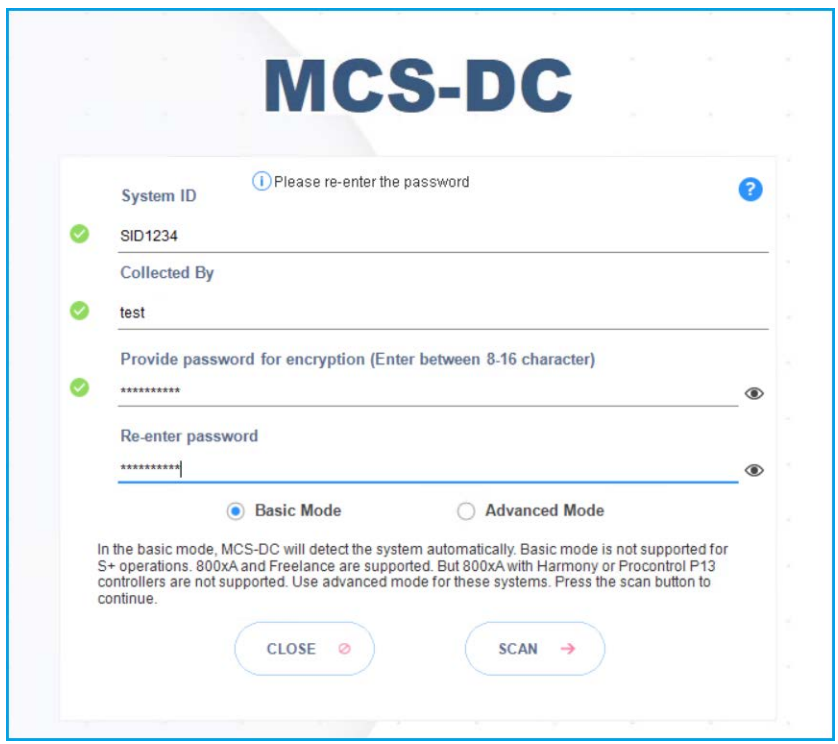

Figure 54. Login

4. Clicking on the **Scan** button initiates system scan by MCS-DC which results in identification of HMI, Controllers and System Version of that Freelance system. Progress bar is shown to indicate the status of the scanning.

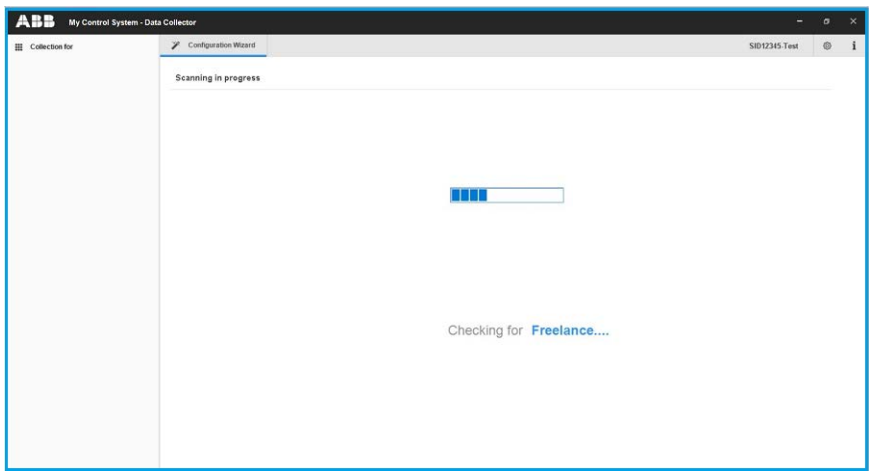

Figure 55. Scan Progress

5. After the scan is successfully completed, details of HMI, Controllers and System Version are displayed.

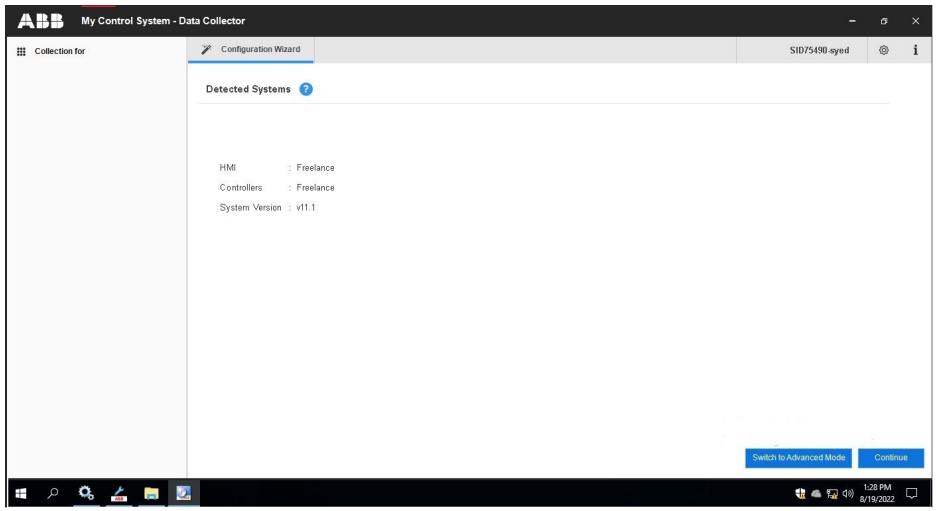

Figure 56. Detected System

6. Below are the supported controllers related to Freelance HMI:

   – Freelance

7. Below are the supported data category options for Freelance HMI:

   – Performance

   – Lifecycle

8. Below are the supported data category options for Freelance Controller:

   – Performance

   – Lifecycle

9. Refer below, the required inputs for each system.

   For procedure on exporting system configuration files, Refer Appendix D, System configuration export.

   Freelance HMI:

   – IP range (to scan and detect non-Freelance nodes)

   – Admin user credentials to access all computer nodes. If the customer project file type is .csvs, user has to provide the customer project decryption key

   – File location of customer project (.csv/.csvs file)

   Freelance controller:

   – File location of customer project (.csv/.csvs file). If the customer project file type is .csvs, user has to provide the customer project decryption key

10. 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.

11. 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).

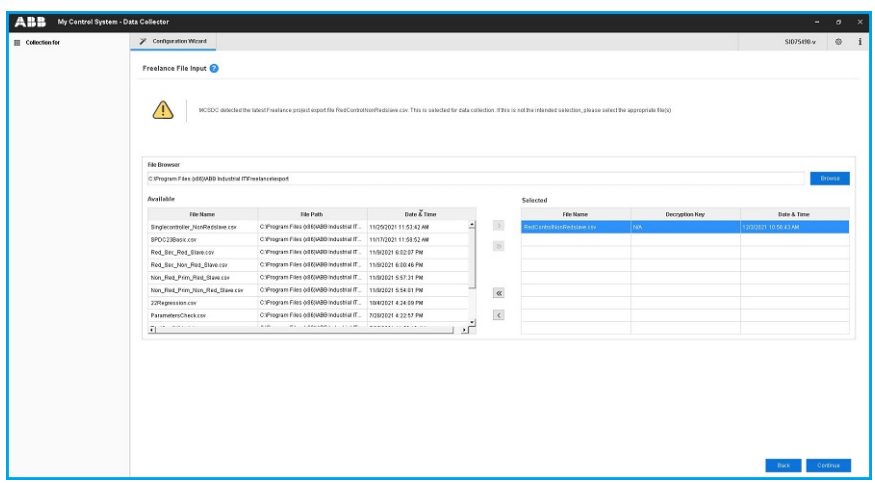

Figure 57. IP Range Input

12. 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.

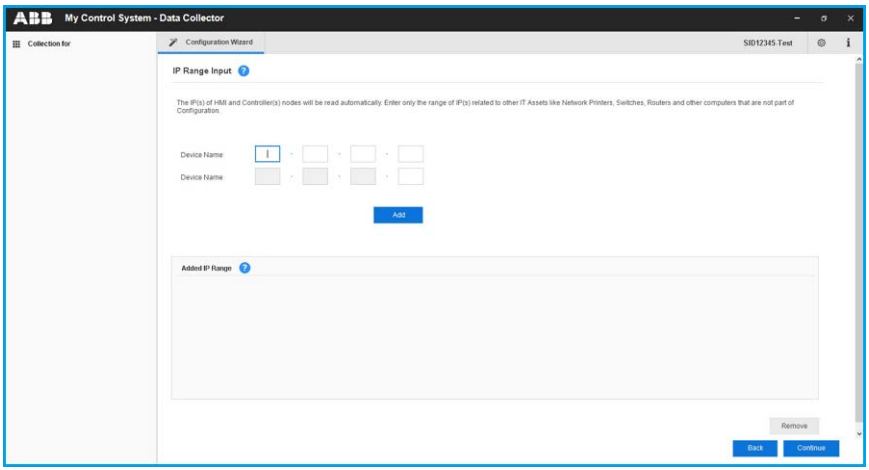

Figure 58. IP Range Input

13. 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.

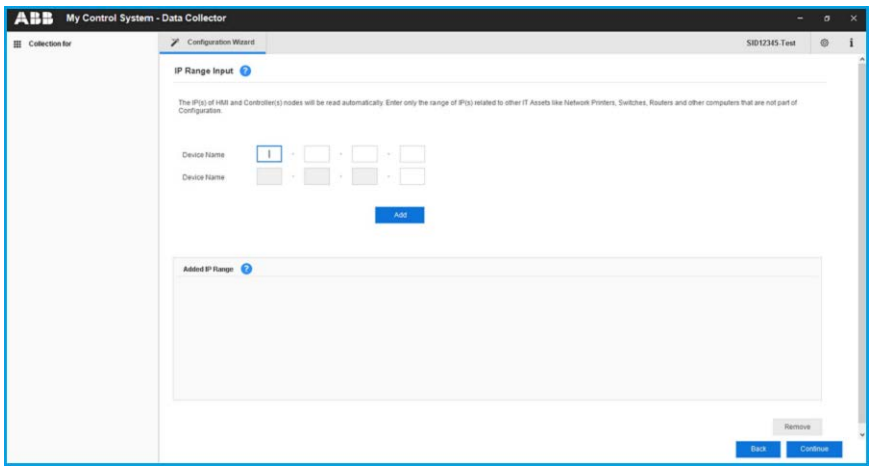

Figure 59. IP Range

14. 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.

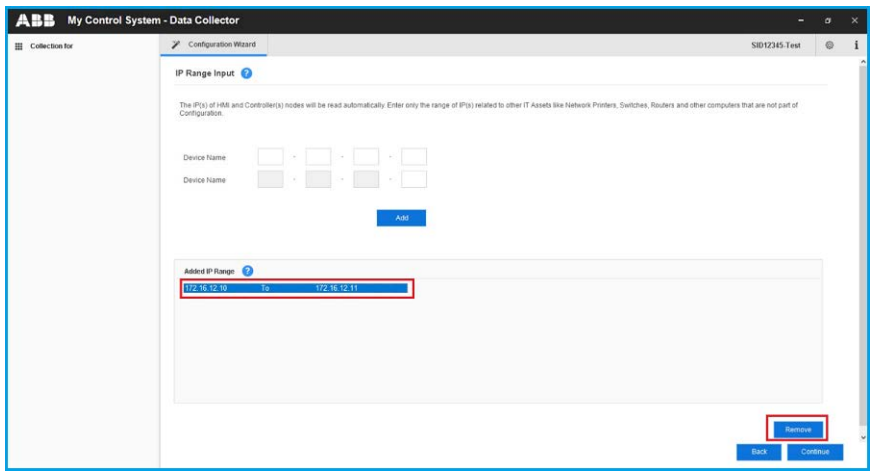

Figure 60. Remove IP Option

15. Click on the **Continue** button to proceed. There is an option to go back to the previous window in each step of the configuration.

16. Next input is user credential. Provide user name 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 2.5, Prerequisites. Click the Add button.

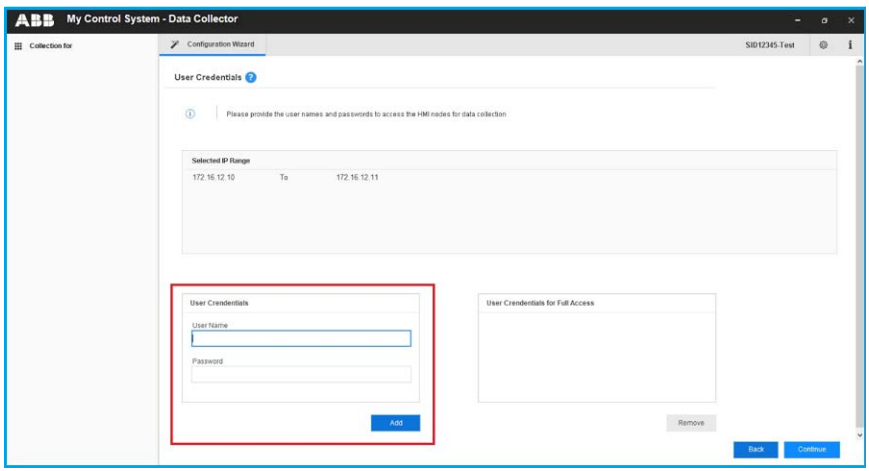

Figure 61. Freelance Folder

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

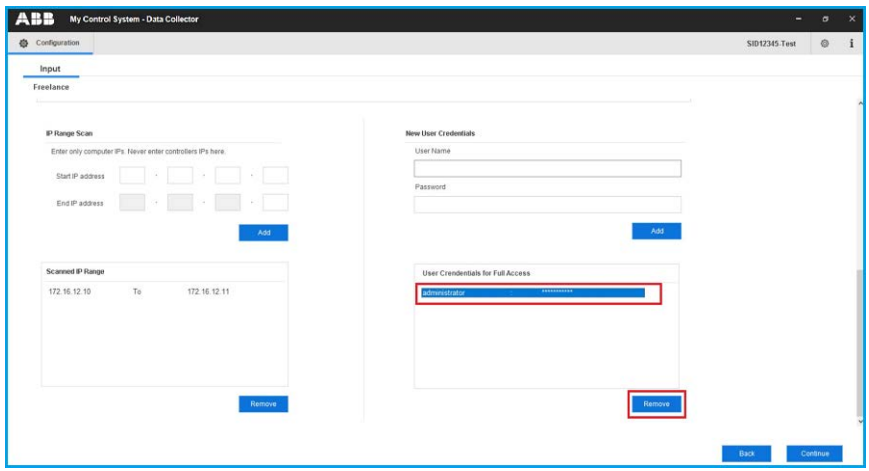

Figure 62. Remove Credentials

18. 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 prerequisites by checking the check box 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 Section 2, Prerequisites.

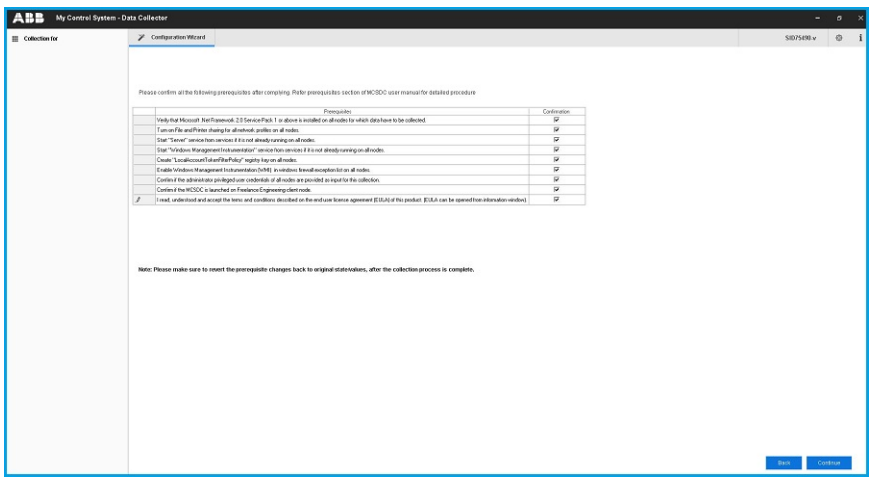

Figure 63. Configuration wizard

19. Click on the **Continue** button to proceed with the node scan.

20. Progress bar shows the scanning progress.

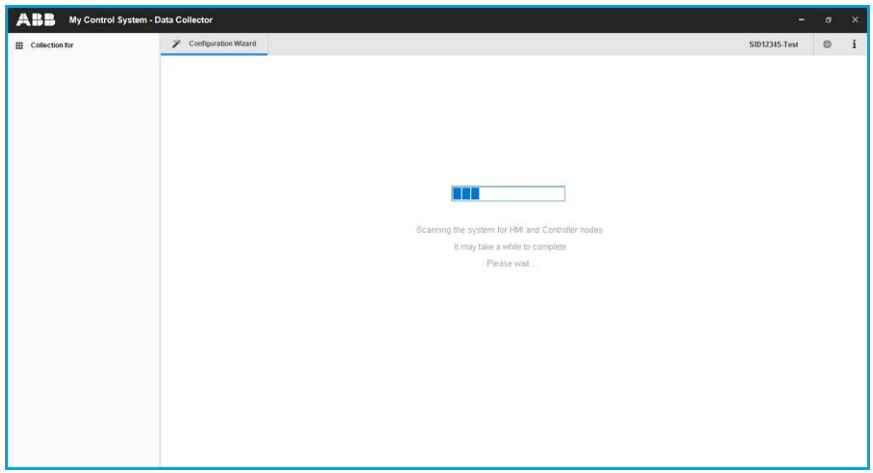

Figure 64. Scanning Progress

21. Once the scan is complete, all the available HMI and Controller nodes get listed. If the HMI nodes are fully accessible, it is indicated as **Yes** in the Full Access field. If the nodes are not fully accessible, it is indicated as **No** in the Full Access field. Possible reasons for non-accessible nodes could be invalid user credentials, IP not reachable, network issues, etc. The remark field shows the reasons for non-accessible nodes. User can fix the issue and perform a rescan. To perform re-scan, click on the **Back** button and repeat the scan. User can add new credentials by clicking on the **Add Credentials** button. It allows user to re-scan the failed nodes with a new credential. To proceed with the data collection, click on the **Continue** button.
22. In the next step collection screen will appear and data collection gets 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.

23. 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.

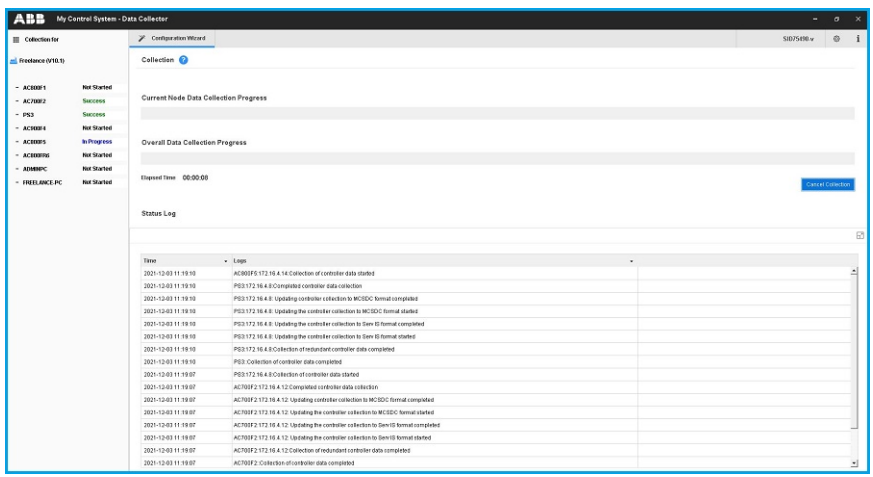

Figure 65. Scan Progress

24. Once the data collection gets 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.

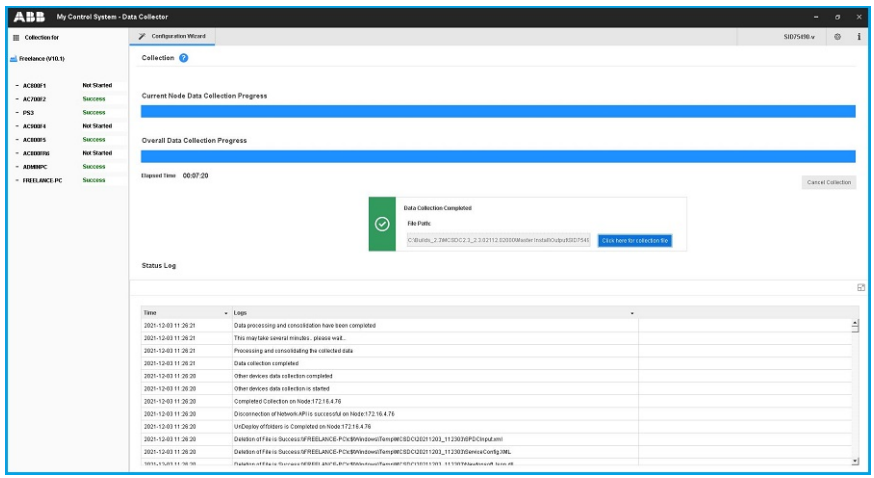

Figure 66. Collection File

25. After clicking on the **Click here for collection file** button, the collection file folder will open.

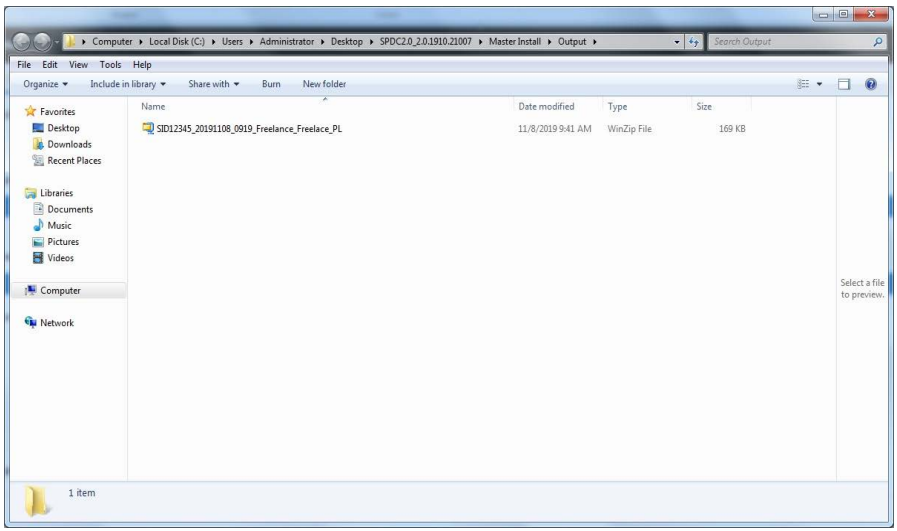

Figure 67. Collection Folder

3.4 Advanced Mode Data Collection

3.4.1 Advanced Mode Data Collection Process for 800xA HMI

1. Deploy MCS-DC in the hard drive (Operating System partition) of the node from which data collection must be executed. 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. Based on the controllers that must be collected, the suggested launch node may vary:
   - 800xA HMI with AC 800M controllers:

     a) LCS: Any 800xA node

     b) Performance: Any 800xA node
   - 800xA HMI with AC 70, 110, 160 controllers:

     a) LCS: Any 800xA node
   - 800xA HMI with Freelance controllers:

     a) LCS: Any 800xA node

     b) Performance: Any 800xA node
   - 800xA HMI with AC 410, 450, MP, SG 400 controllers:

     a) LCS: Any 800xA node

     b) Performance: Any 800xA node
   - 800xA HMI with Melody Rack controllers:

     a) LCS: Any 800xA node which is part of Onet network. Additionally CSE_Config has to be synchronized in all the 800xA nodes

     b) Performance: Any 800xA node which is part of Onet network. Additionally CSE_Config has to be synchronized in all the 800xA nodes
   - 800xA HMI with Harmony controllers: If 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 4.1, Post Collection Procedure for more details.

     a) LCS (For Harmony Rack modules): Node in which Composer Harmony is installed (Harmony Composer project .ebp is present)

b) LCS (For Symphony DIN): Any node which has HAPI installed and reachable through control network (recommended Composer Harmony node)

c) Performance (Controller): Any node which has HAPI installed and reachable through control network (recommended Composer Harmony node)

d) Performance\LCS (800xA) : Any 800xA node

- 800xA HMI with MOD 300 Controllers:

  a) LCS: Any 800xA node

- 800xA HMI with Procontrol P13 controllers:

  a) LCS: Any 800xA node

- 800xA HMI with QCS controllers:

  a) LCS: Any 800xA node

2. Double-click on the **MCS-DC_Launcher.exe**, to launch the tool. It is present inside the unzipped MCS-DC folder. The initial screen appears as shown in Figure 68. MCS-DC tool runs the below checks on the launch node. The Green tick marks refer to successful checks, click on the **Launch** button to proceed with data collection. If the check fails, a Red cross mark will indicate the same. User must fix the issue and re-launch the MCS-DC tool.

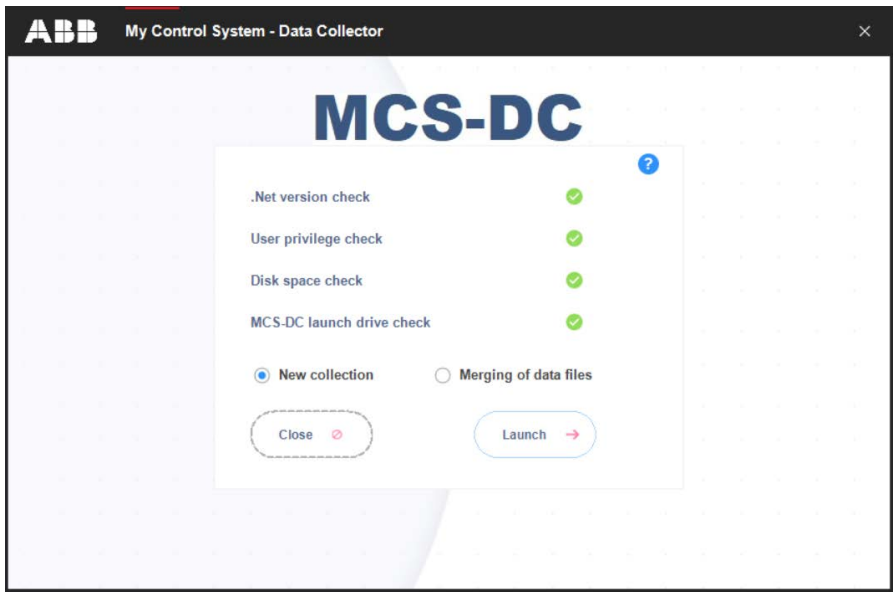

Figure 68. MCS-DC Launcher

- .NET Framework version check

  .NET Framework version 1.1 or above is required to pass this check and Launch MCS-DC 2.X version for data collection.

  If the .NET Framework version is lower than 1.1, this check will fail and user will be unable to launch MCS-DC 2.X version for data collection, instead MCS-DC 1.9.x version will be launched for data collection. Please refer to MCS-DC 1.9.x user manual for data collection procedure.

- Prerequisites check

  Below prerequisites needs to be validated. User can proceed with data collection only if these checks are passed.

  a) User privileges check, checks if the MCS-DC Tool is launched in the user account with administrator privileges.

  b) System drive launch check, MCS-DC tool should be launched only from the local disk drive of the launch node.

  c) Required Disk Space Check, Free disk space of 500MB should be available on the disk drive from which the MCS-DC is launched.

3. Provide System ID of the 800xA system first, your full name in the collected by filed next and set password in the provide password for encryption field. This 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 for respective fields. Correct the errors and click on the **OK** button to proceed further.

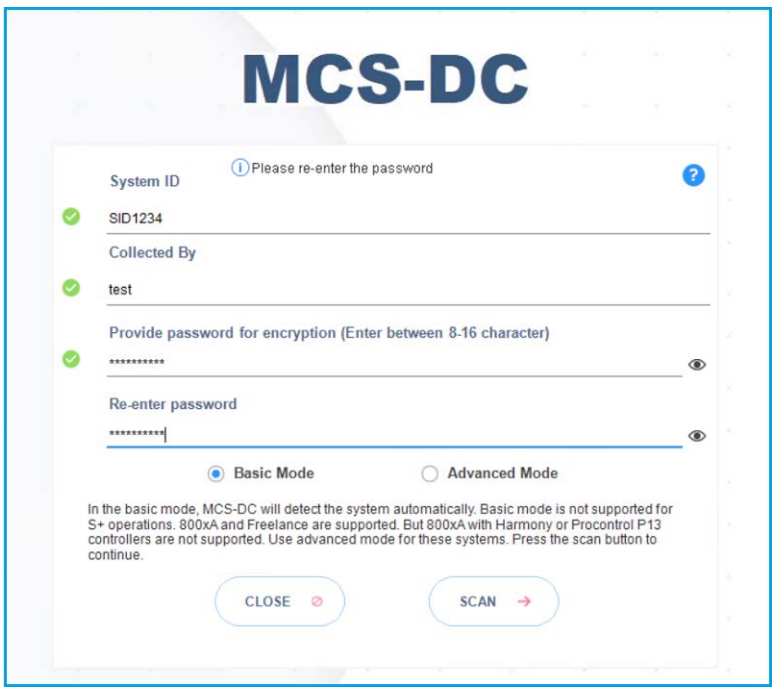

Figure 69. User Credentials

4. In the next step configuration screen will appear. User needs to select applicable HMI/controllers and data category (like Performance, Life cycle, etc.) on this screen. Supported HMIs are listed on the left half of the screen. When a 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.
5. Below are the supported controllers related to 800xA HMI on this release:
   - AC 800M
   - AC 800PEC
   - AC 70, 110, 160
   - Freelance
   - AC 410, 450, MP, SG 400
   - Melody Rack
   - Harmony
   - MOD 300
   - Procontrol P13
   - QCS
6. Below are the supported data category options for 800xA HMI:
   - Performance
   - Life cycle
   - Software
   - Security (Cyber security)

7. Below are the supported data category options for the controllers:
   - AC 800M:
     a) Performance
     b) Life cycle
   - AC 800PEC:
     a) Life cycle
   - AC 70, 110, 160:
     a) Life cycle
   - Freelance:
     a) Performance
     b) Life cycle
   - AC 410, 450, MP, SG 400:
     a) Performance
     b) Life cycle
   - Melody Rack:
     a) Performance
     b) Life cycle

- Harmony:
  a) Performance
  b) Life cycle
- MOD300:
  a) Life cycle
- Procontrol P13:
  a) Life cycle
- QCS:
  a) Life cycle

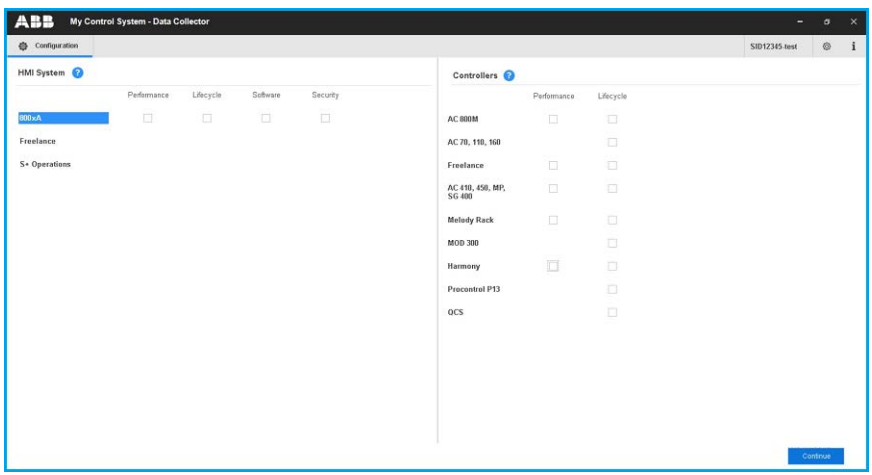

Figure 70. Data Collection

8. Select the required data category for HMI and controller and then click on the **Continue** button to proceed. Select Cyber Security option only when it is needed as it will take significantly longer time for data collection. A typical selection is shown in Figure 71. Please note, data collection for AC800M controllers should only be done along with an HMI.

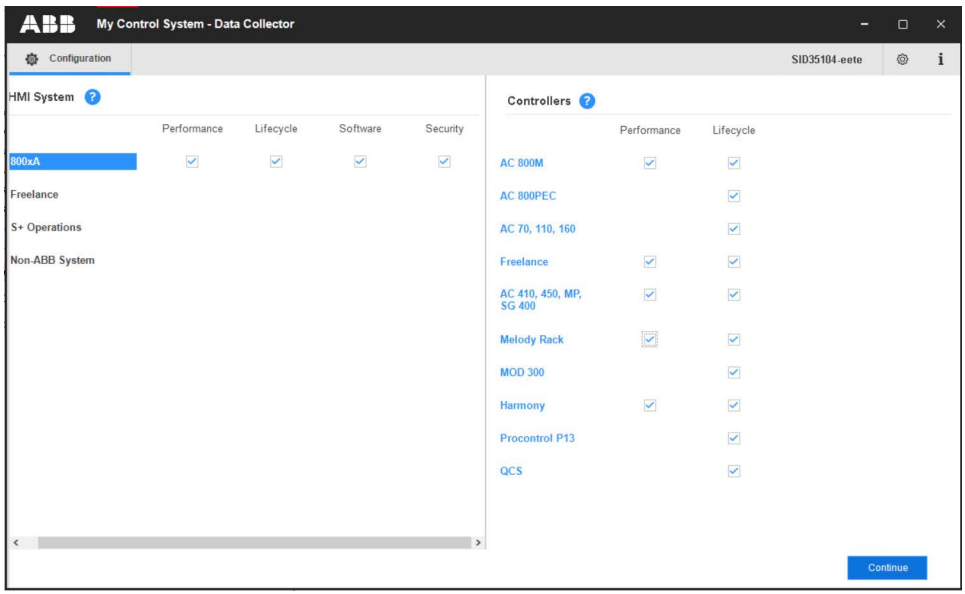

Figure 71. Controllers

9. Input configuration screen appears. The type of required inputs may vary based the HMI, controller and data categories, selected in the previous step. If user selects AC 800M and Advant Master (AC 410, 450, MP, SG 400) but do not select 800xA HMI, then no input is required and user can skip this screen. After the data category selection, collection screen appears.

10. Refer below for the required inputs of each system:

For the procedure on how to export system configuration files refer to Appendix D, System configuration export.

- 800xA HMI:
  IP range (to scan and detect non-800xA nodes) Admin user credentials to access all computer nodes.
- AC 800M controllers:
  No input settings are needed for collecting performance and life cycle data from AC800M controllers. However, controller crash files (logs) will be collected from primary as well as redundant AC800M connectivity server, for which, users can set the maximum size of the collection file. Click on settings (the gear icon on the top right corner) and select the tab AC800M. 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 15MB. Crash file collection can be disabled by unchecking the provided check box.

  By default, AC800M 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.

  The collection of AC 800M lifecycle data from a system with a large number of control structure objects (for e.g a large number of redundant IO modules) may time out in certain rare cases. Users are advised to uncheck the option 'Collect redundant devices' in such cases and proceed with the collection process.

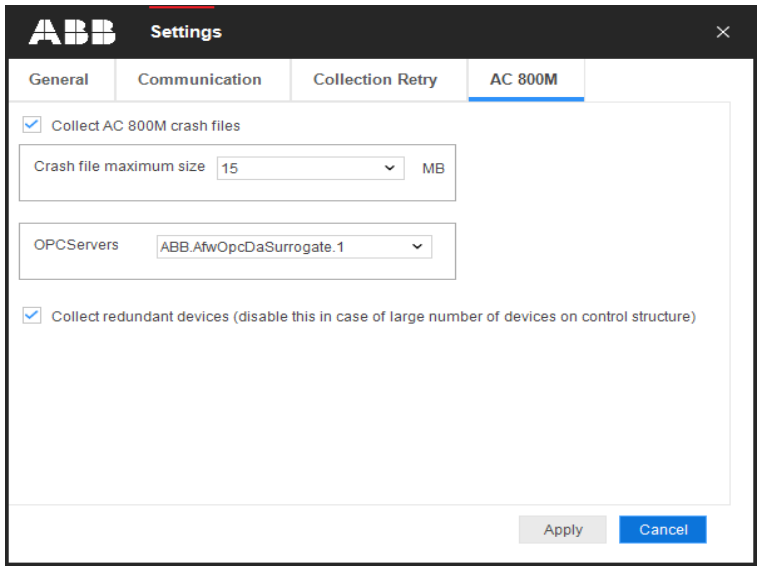

Figure 72. AC 800M data collection settings

- AC 70, 110, 160 Controllers:
  File location of customer project (.BAX file)
- Freelance Controllers:
  File location of customer project (.csv/.csvs file). If the customer project file type is .csvs, user has to provide the customer project decryption key.
- AC 410, 450, MP, SG 400 Controllers:
  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.

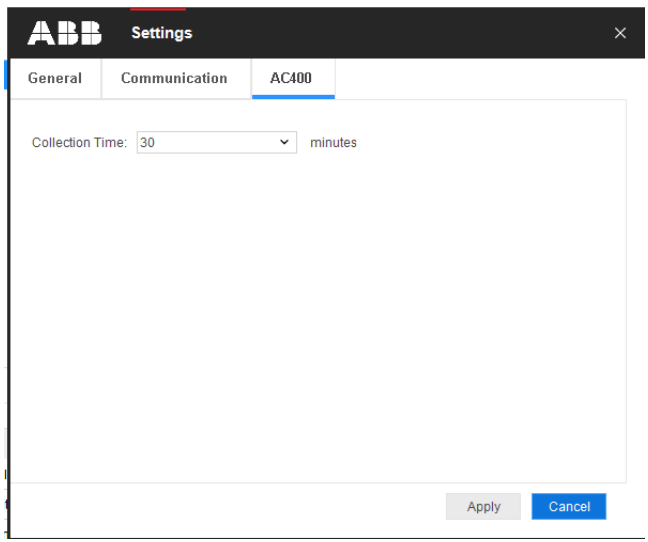

Figure 73. Collection Time Interval

- Melody Rack Controllers:
  Melody Island Devices
  CSE_Conf File
  Asset Export Folder
  Composer Melody node IP Address
  UserName
  Password

- Harmony Controllers: Refer to step 20 in this section for more details.

- MOD300 controllers:
  Latest ATF file from AdvaBuild engineering node
- Procontrol P13 controllers:
  File location of the latest P13 source file (.CSV). Please note, in the exported P13 Source file (.CSV), the text separator should be double quotes (“) and the field separator should be comma (,). For more details refer Appendix C

- QCS controllers:

  Latest config.xml files from QCS connectivity server

11. Under 800xA HMI tab, IP range scan input: 800xA nodes that are already part of Node Admin Structure of 800xA system will be detected by MCS-DC. If there are any non-800xA computers that are connected to 800xA system (for example Melody engineering node), user shall enter the IP range of these computers. This is an optional input. If no IP range is entered, then MCS-DC will collect only 800xA HMI nodes.

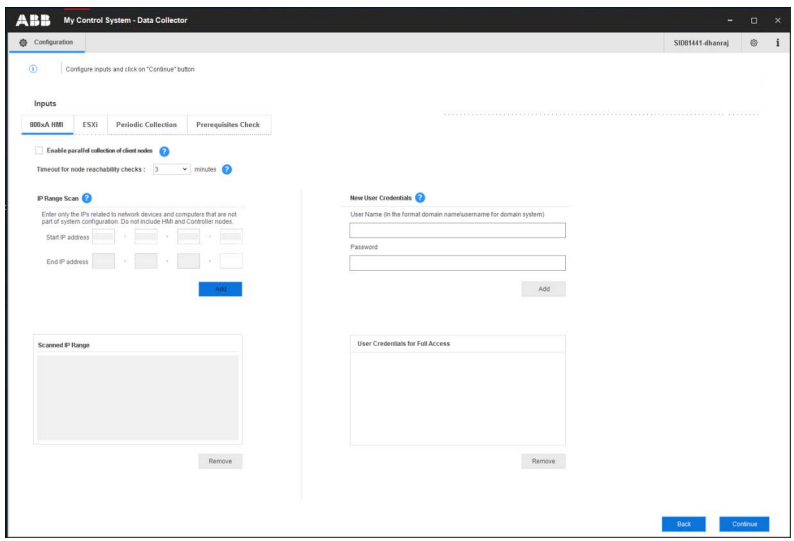

Figure 74. Inputs

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 check box "Enable parallel collection of client nodes". Note that this is an optional setting.

Parallel data collection is not applicable to server nodes. When the check box 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.

12. 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.

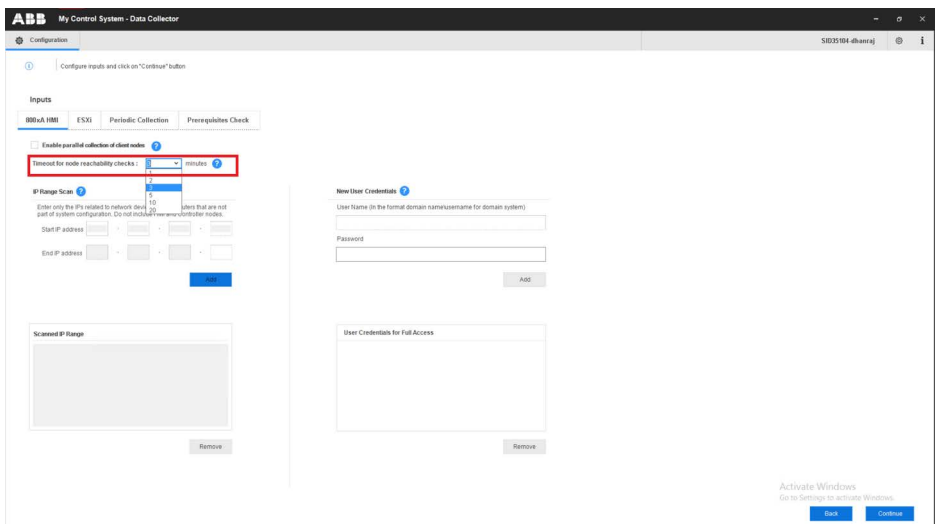

Figure 75. Timeout for node reachability check

13. Provide the IP range and click on **Add** button. User can provide multiple ranges. If the IP range is large, MCS-DC will complete the node scanning in significantly more time. Hence, it is better to provide specific range related to required computers.
14. In case an incorrect IP range is added, there is an option to remove it: select the incorrect IP range by clicking on it and then select the **Remove** button.
15. Next input is User Credentials. Provide the Username and Password of an Administrator 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”.
16. There is an option to remove the added credentials. To remove, select the added credential and click on the **Remove** button.

17. Click on **Continue** button to provide input for AC 70, 110, 160 controllers data collection, this tab will appear only if AC 70, 110, 160 is selected for data collection in the previous steps. Click on 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 Available section and vice versa. Move the required export files to Selected section (refer to Appendix D, System configuration export for exporting system configuration files).

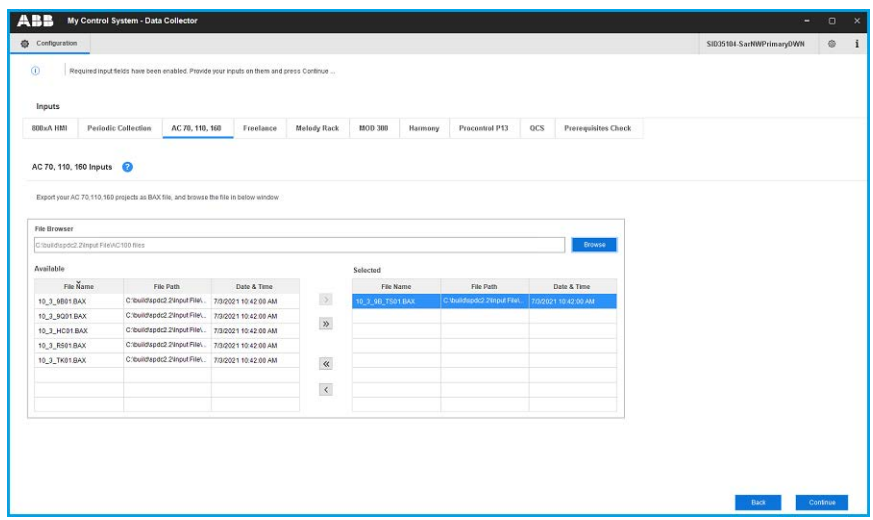

Figure 76. Browse Project Export Folder

18. If Freelance Controller category is selected in Step 8, 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. 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).

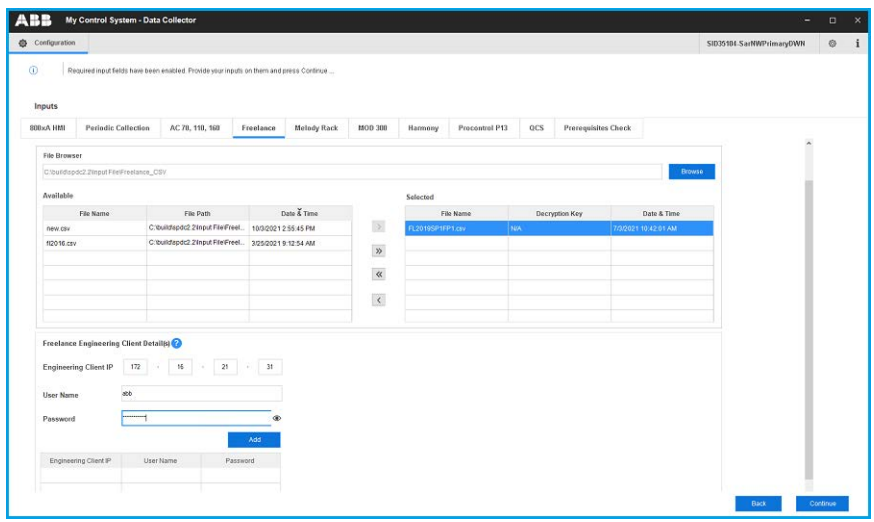

Figure 77. Select the Freelance project export folder

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

20. Harmony controllers Performance Input: If Harmony Controller category is selected in Step 8, click on Harmony tab to provide input for Harmony controllers data collection, Provide the below inputs to proceed with Harmony data collection. There are two panes in Harmony input page.

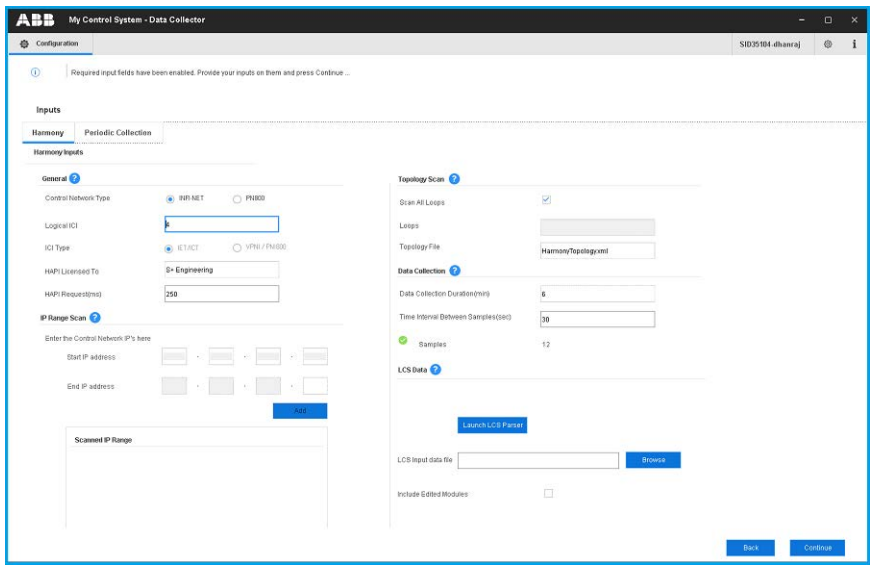

Figure 78. Harmony Rack

- 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): This interval, is the rate at which MCS-DC raise requests to the connected DCS System, in milliseconds and it is the minimum time interval between two consecutive requests to HAPI.

  Default value is 250 milliseconds. Higher value will decrease the load on control network. Keep the default input.

- f) Traverse across IEB: If IEB bridge is present in the network, MCS-DC can traverse through it and collect data from PN800 network. In this case, user needs to enable the check box and provide the IPT bridge module IP address.

In order to traverse the IEB bridge, a minimum CAPI version of 5.1.0.12 must be used.

- 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

  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 Samples = Data Collection Duration*60 / Time Interval Between Samples. Please note that the minimum Samples 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.

21. 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.
22. 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.

23. 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.

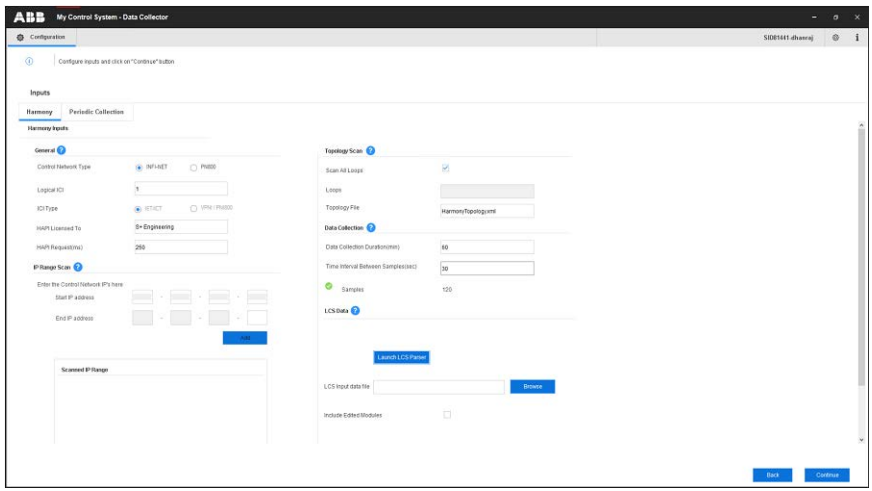

Figure 79. Harmony Rack

24. 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.

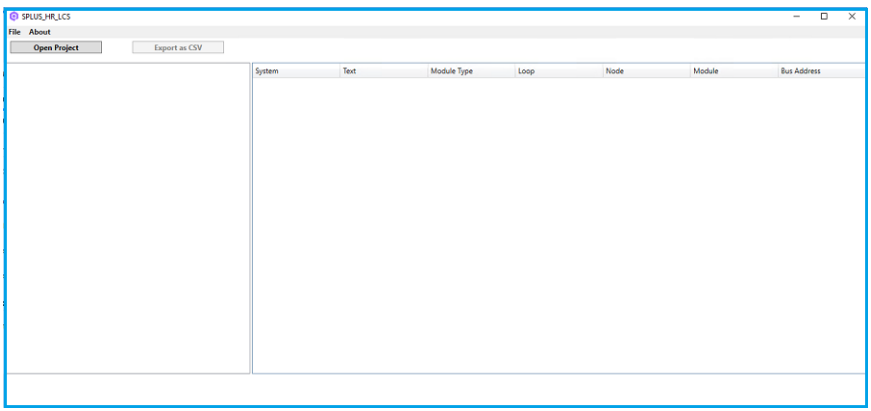

Figure 80. Open Project

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

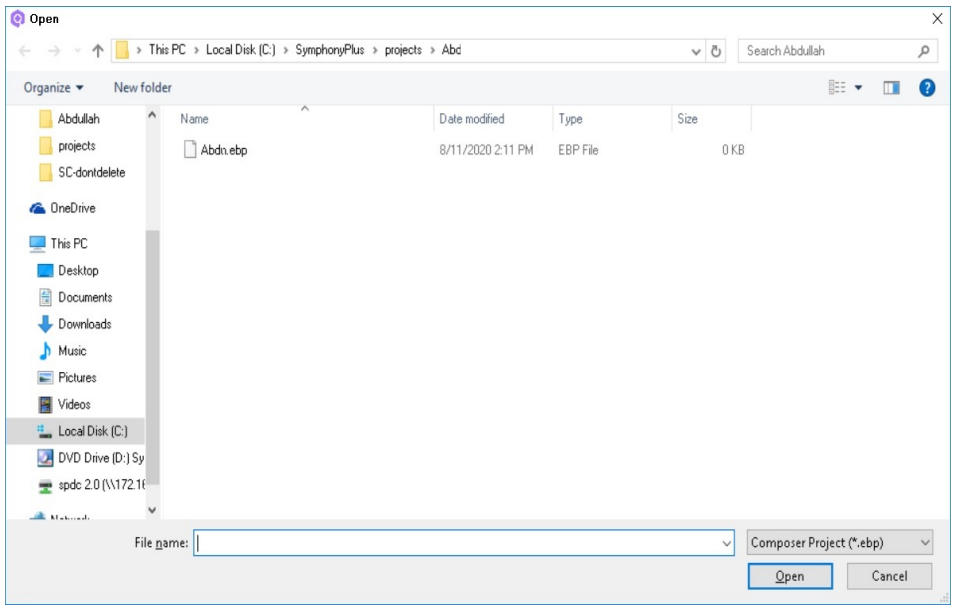

Figure 81. Open option

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.

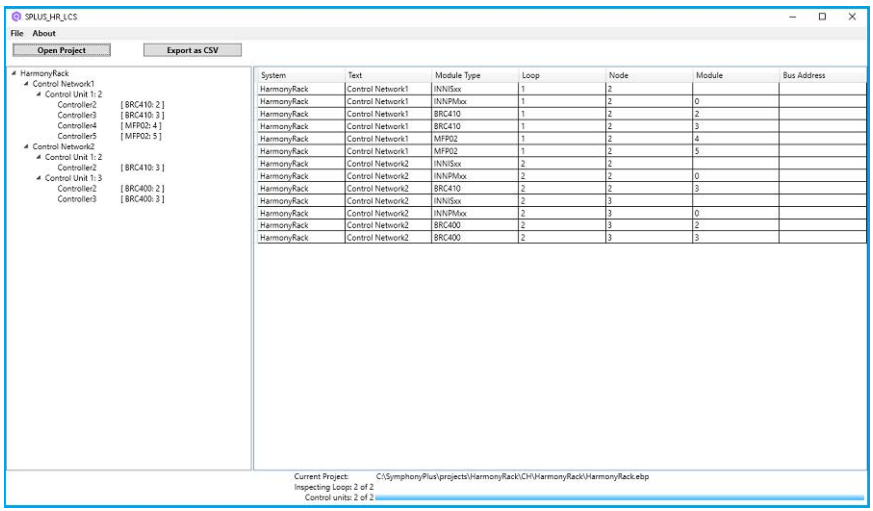

Figure 82. Export as CSV

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.

25. Click on **Continue** button to provide input for Melody Rack Controllers data collection; this tab appears only if Melody Rack data collection has been selected. Provide the below inputs to proceed with Melody Rack data collection (refer to Appendix D, System configuration export for exporting system configuration files).

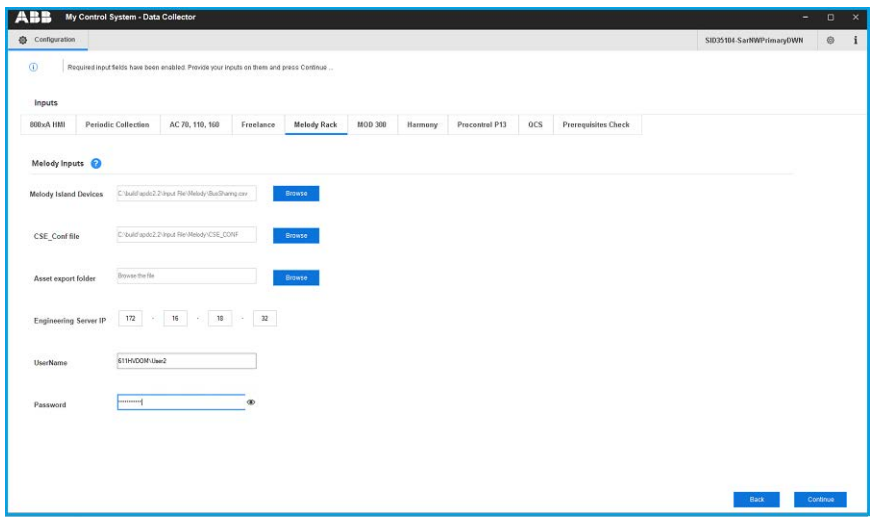

Figure 83. Melody Rack Tab

a. Melody Island Devices
Click the **Browse** button to select the Melody Island DevicesExport file.

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 user name.

f. Password
Provide the Composer Melody node server password

26. If MOD 300 Controller category is selected in Step 8, 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).

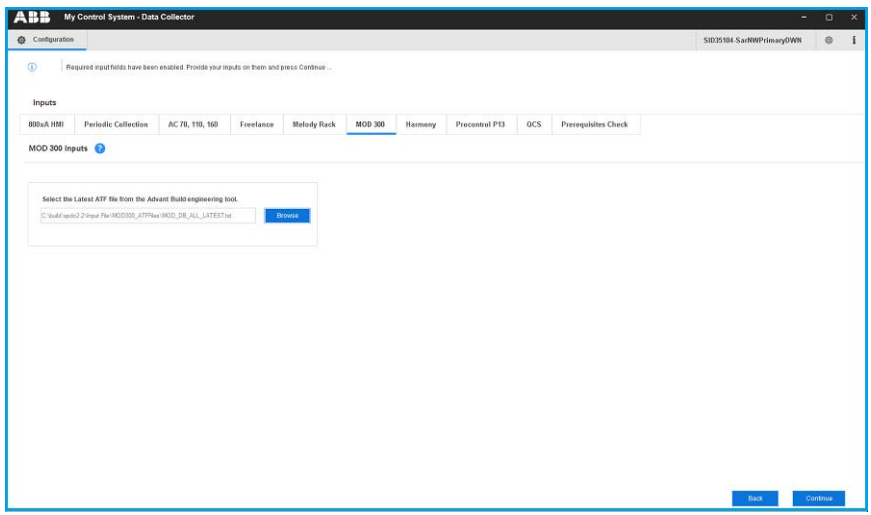

Figure 84. MOD300

27. If Procontrol P13 Controller category is selected in Step 8, click on **Procontrol P13** tab to provide input for Procontrol P13 controllers data collection. Click on **Browse** button to select the latest P13 source file (.CSV), taken from P13 engineering node.

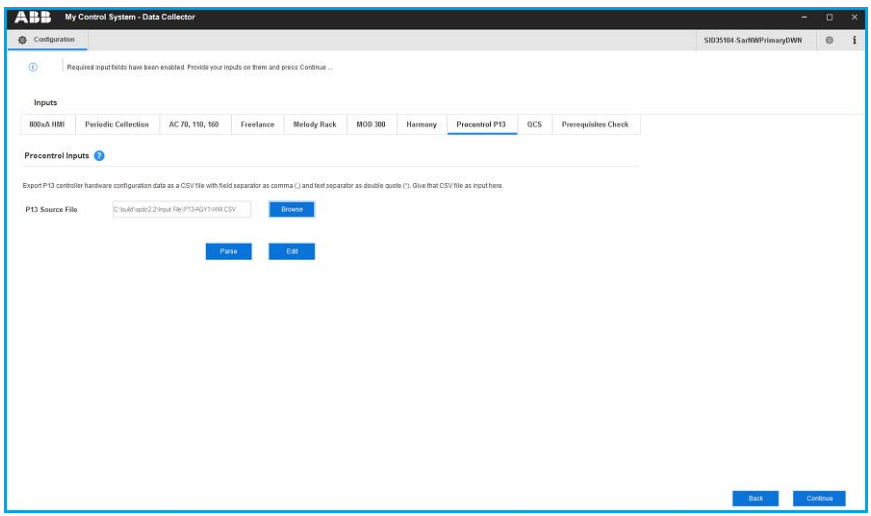

Figure 85. P13 Source File

28. Click **Parse** button. Contents of the P13 source file (.CSV) is displayed.

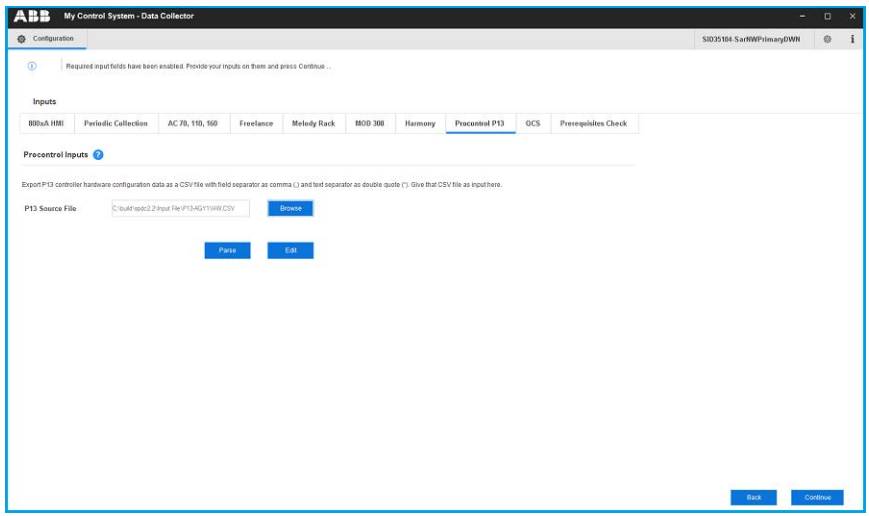

Figure 86. Parse Button

a. 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.

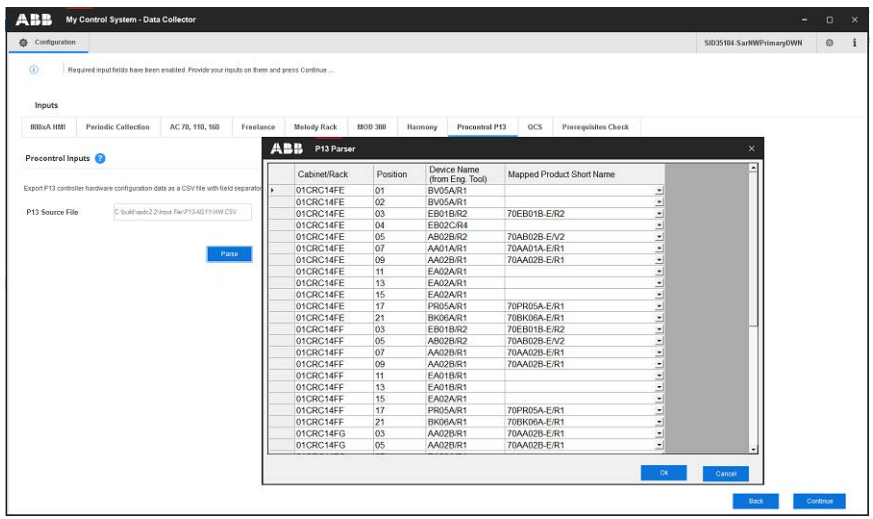

Figure 87. Mapped Product Short Name

b. If any modification is required, click **Edit**, to modify the parsed file. Click **Continue** to proceed.

29. If QCS Controller category is selected in Step 8, 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 projects 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 sub-directories 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..

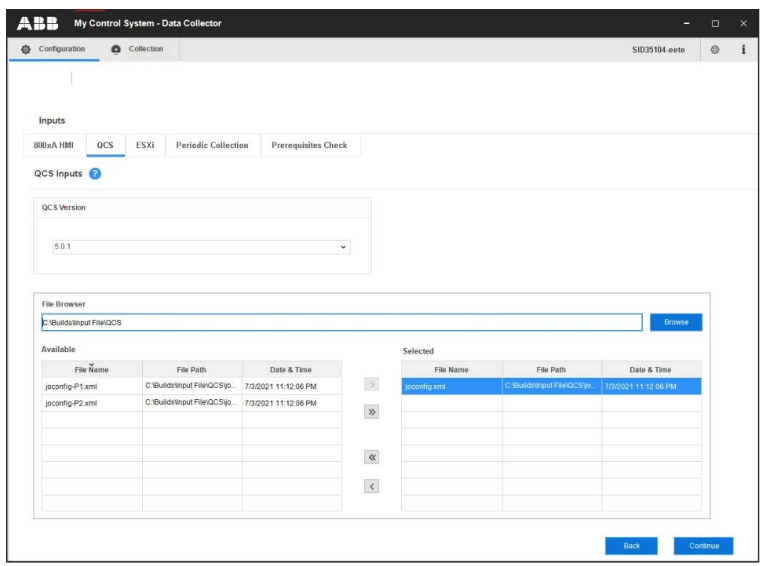

Figure 88. Select QCS version

30. 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 projects 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 the sub directories 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.

31. 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 prerequisites by checking the check box against them. Please note that this is only an acknowledgment that user has verified all the prerequisites for proceeding with data collection. For more details, refer Section 2, Prerequisites.

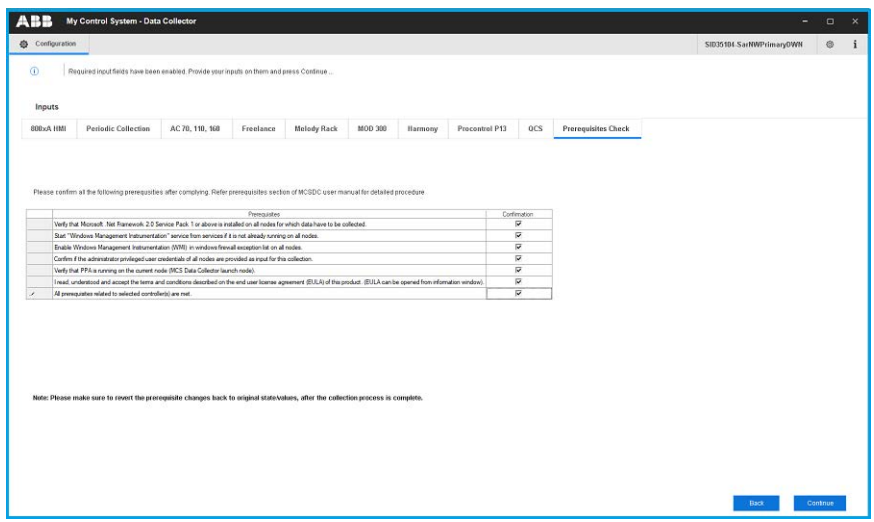

Figure 89. Prerequisites Check

32. Click on the **Continue** button to proceed to collection screen.
33. Collection screen appears. 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.

34. 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.

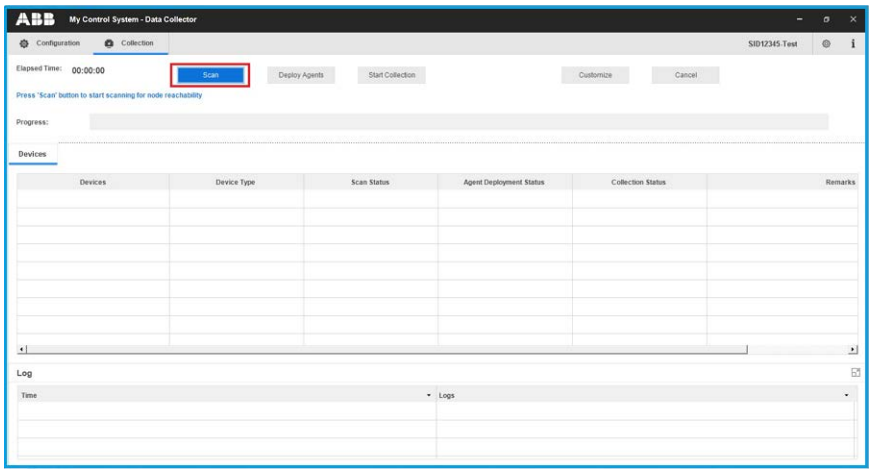

Figure 90. Scan the Nodes

35. Progress bar shows the progress of scanning.

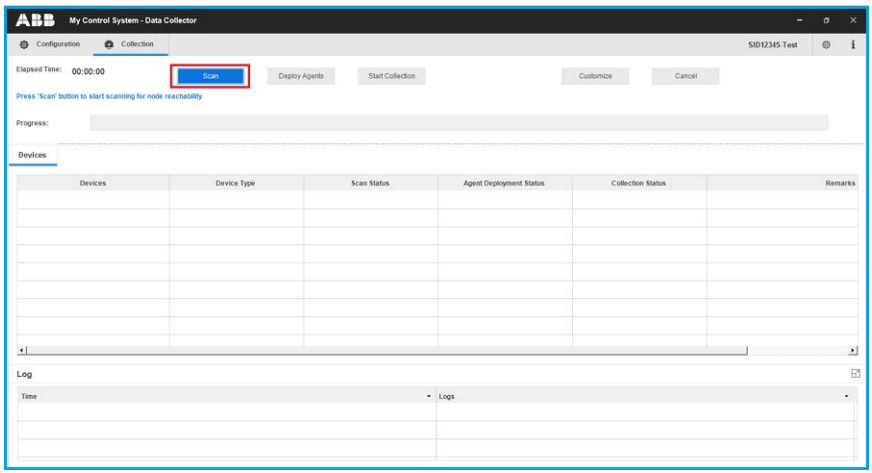

Figure 91. Scan Progress

36. Computers and controllers that are accessible from the MCS-DC launch node, are listed on the first column of the table shown in 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 (for example AC 800M controller), then the status is “Not applicable” in Grey.

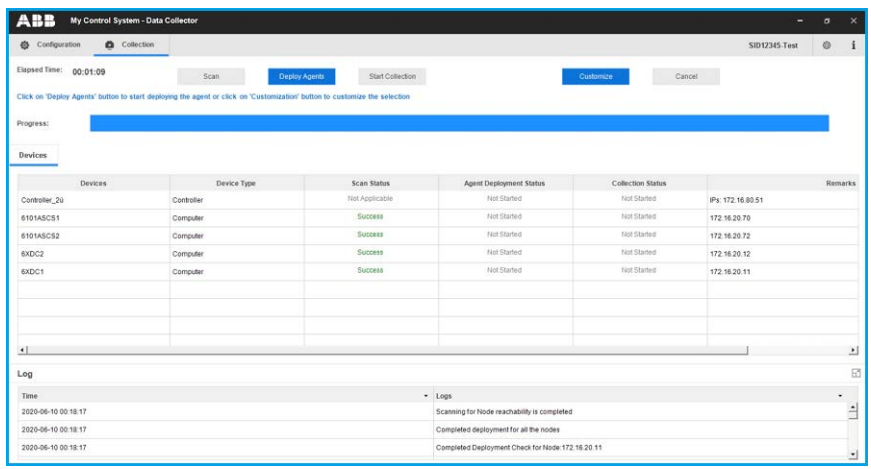

Figure 92. Data Collection Progress

37. 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 rescan (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.

38. Once node scan is completed, Deploy Agents and Customize buttons will be enabled. User can customize the collection by choosing only few HMI/controller nodes from the list of accessible nodes, using customize option. Clicking on the **Customize** button opens customization window.

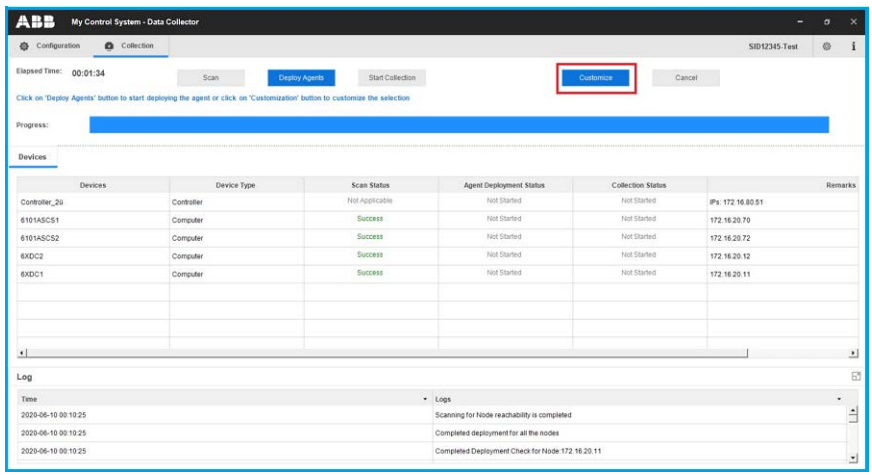

Figure 93. Select Required Nodes

39. User has an option to customize the Data collection nodes for Performance, Lifecycle, Security and Software data collection. To customize click on the **Customize** button. All accessible HMI and controller nodes are shown in the list. By default, all accessible HMI and controller nodes will be selected. User can de-select the nodes that are not desired to be collected by un-checking the respective check boxes against the node names. Click on **OK** button to save the customization configuration and close the customize window. Click on **Reset** button will reset the customization configuration. Please note, that controller customization is not available for this release.

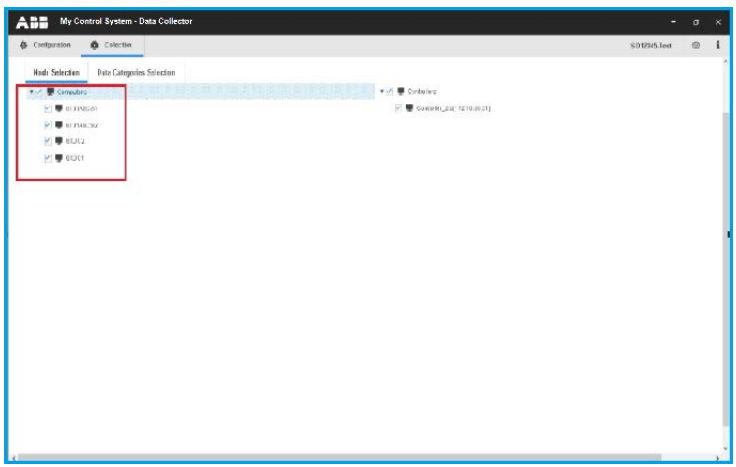

Figure 94. Deploy Agents

40. 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 de-select the data categories that are not desired to be collected by un-checking the respective check boxes against the data category names. Click on **OK** button to save the customization configuration and close the customize window. Click on **Reset** button to reset the customization configuration. Data categories customization is applicable only for HMI nodes, it is not applicable for controllers.

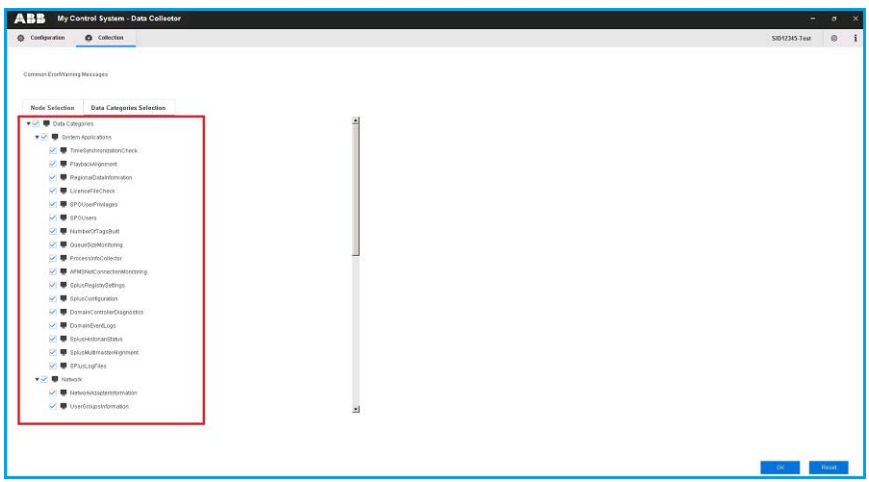

Figure 95. Data Categories Selection

41. 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.

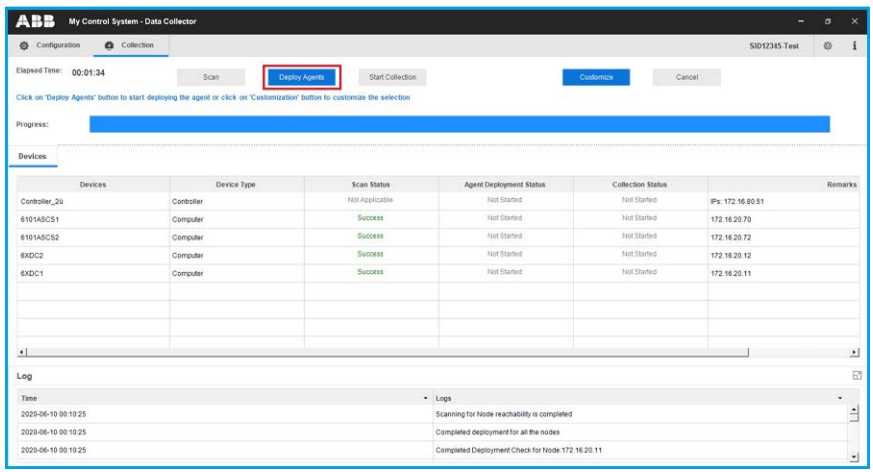

Figure 96. Deployment Status

42. 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 get enabled. Click on the **Start Collection** button to start the data collection.

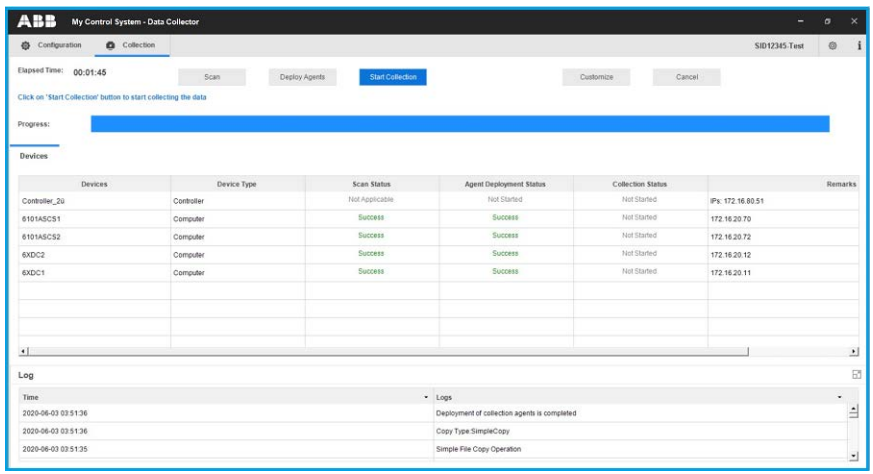

Figure 97. Collection Progress

43. Data collection progress can be seen on the progress bar and on the Collection Status column.

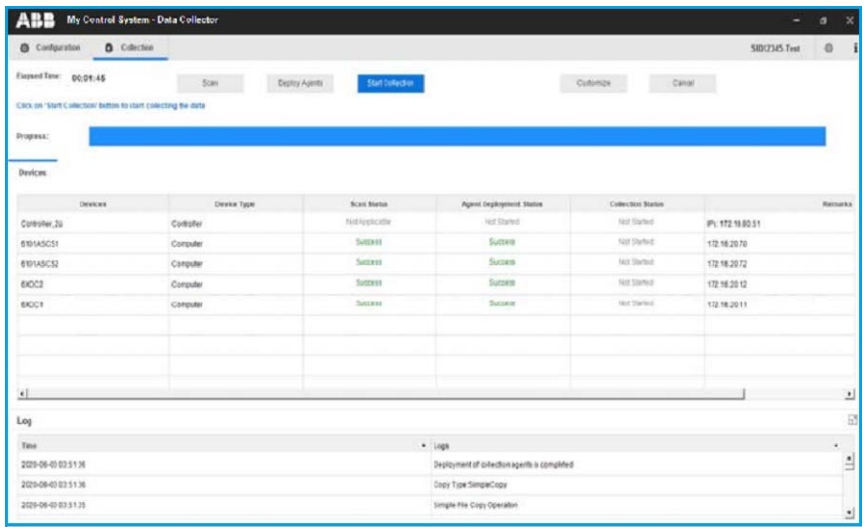

Figure 98. Collection File

44. 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 contains the hardware tree information and the bottom part contains the collection statistics.

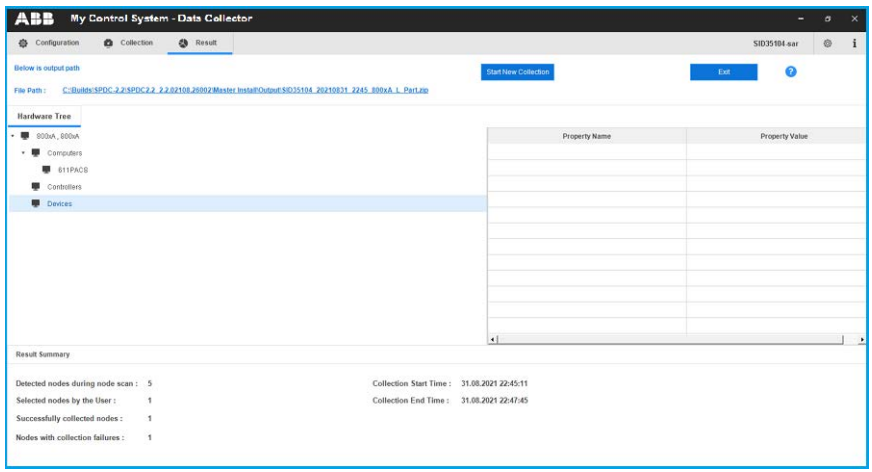

Figure 99. Collection File Path

45. 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.
46. Click on the **New collection** button to get back the Configuration screen and start a new collection. Clicking on the **Exit** button to close the MCS-DC application.

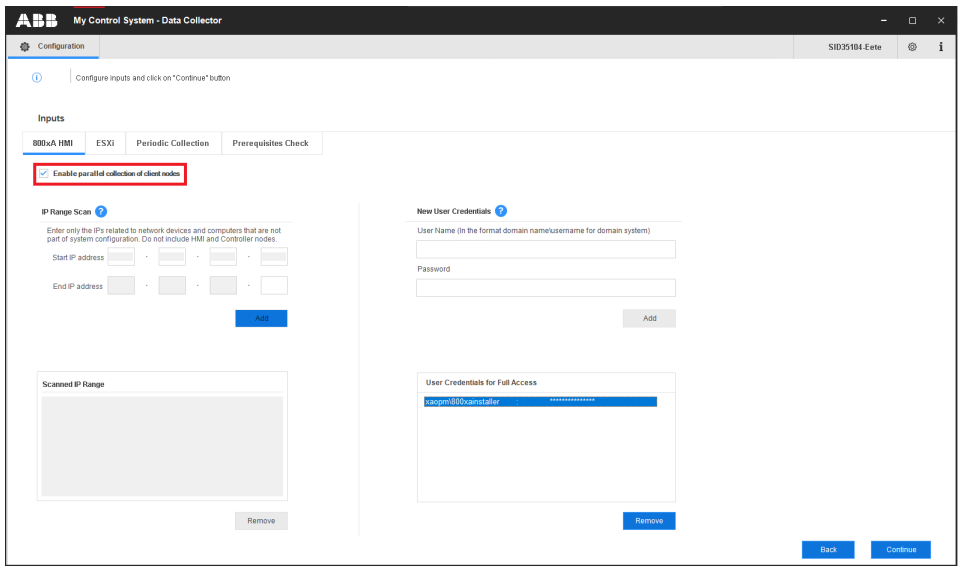

Figure 100. Parallel data collection from client nodes

3.4.2 Advanced Mode Data Collection Process for Freelance HMI

1. Deploy MCS-DC in the hard drive (Operating System partition) of the node from which data collection must be executed. MCS-DC can be launched from any Freelance node.
2. Double-click on the **MCS-DC_Launcher.exe**, to launch the tool. It is present inside the unzipped MCS-DC folder. The initial screen appears as shown in Figure 101. MCS-DC tool runs the below checks on the launch node. If the check is passed, a Green tick mark is shown, click the **Launch** button to proceed for data collection. If the check fails, a Red cross mark is shown, user has to fix the issue and launch the MCS-DC tool again.

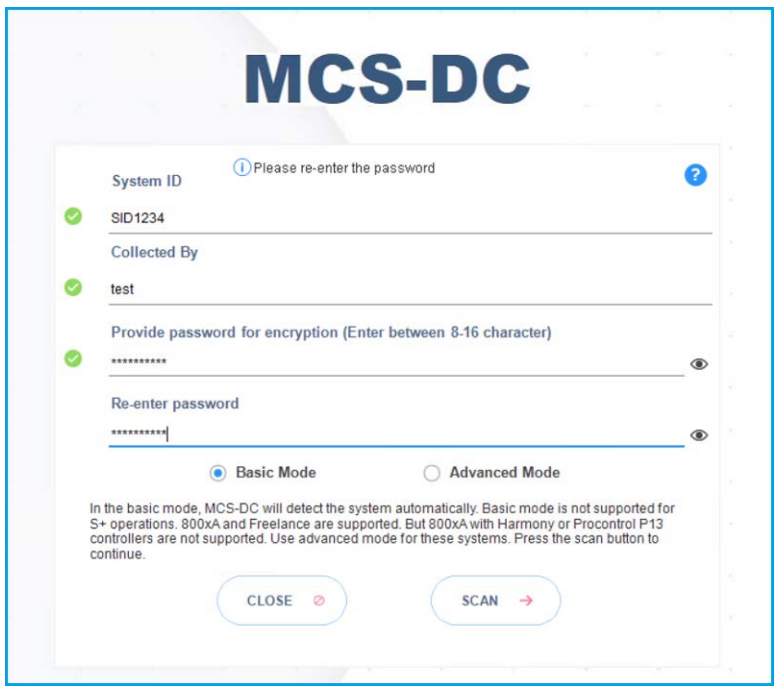

Figure 101. MCS-DC Launcher

- .NET Framework version check

  If the .NET Framework version is 1.1 or above, then this check is passed and MCS-DC 2.X version can be launched for data collection.

  If the .NET Framework version is lower than 1.1, then this check is failed and MCS-DC 2.X version cannot be launched for data collection, instead MCS-DC 1.9.x version 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.

  a) User Privileges Check, checks if the MCS-DC Tool is launched in the user account with administrator privileges.

  b) System drive launch check, MCS-DC tool should be launched only from the local disk drive of the launch node.

  c) Required Disk Space Check, Free disk space of 500MB should be available on the disk drive from which the MCS-DC is launched.

3. Provide the System ID of the Freelance system and your full name and provide password for encryption. This 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.

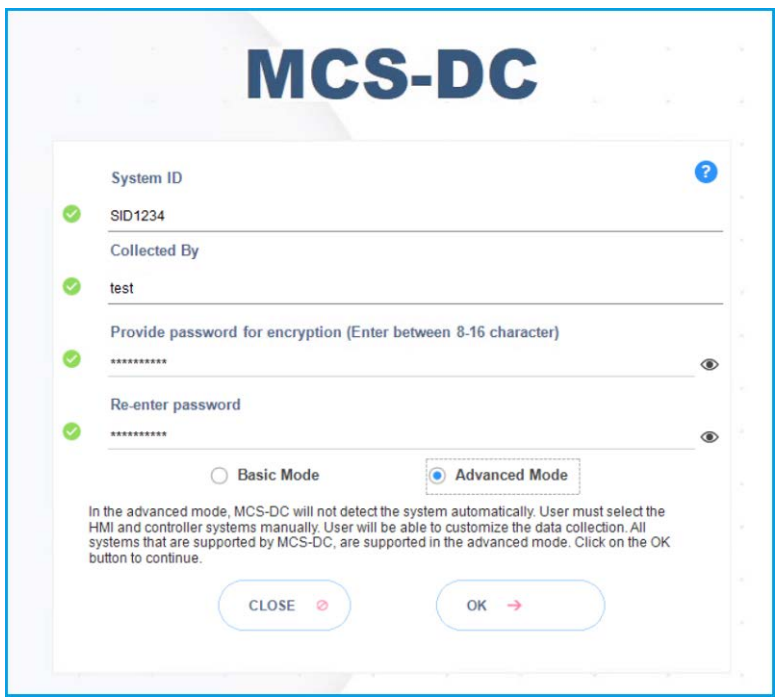

Figure 102. Login

4. Configuration screen appears. User needs to select applicable HMI/controllers and data category (like Performance, Life cycle, etc.) on this screen. Supported HMIs are listed on the left half of the screen. When a 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.
5. Supported controllers for Freelance HMI:
   - Freelance
6. Supported data categories for Freelance HMI:
   - Performance
   - Life cycle
   - Security
7. Supported data categories for Freelance Controller:
   - Performance
   - Life cycle
8. Select the required data categories and then press **Continue** to proceed. A typical selection is shown below:

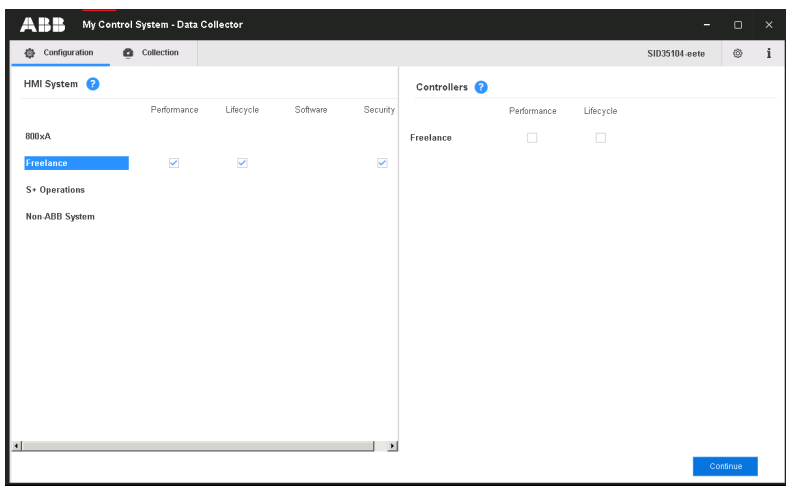

Figure 103. HMI

9. Input configuration screen appears. The type of required inputs may vary based on the HMI, controller and data categories, selected on the previous step.
10. Refer below the required inputs for each system.

For the procedure on how to export system configuration files refer to Appendix D, System configuration export.

Freelance HMI:

- IP range (to scan and detect non-Freelance nodes, optional)
- Admin user credentials to access all computer nodes. If the customer project file type is .csvs, user has to provide the customer project decryption key
- File location of customer project (.csv/.csvs file)

Freelance controller:

- File location of customer project (.csv/.csvs file). If the customer project file type is .csvs, user has to provide the customer project decryption key

11. 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. 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).

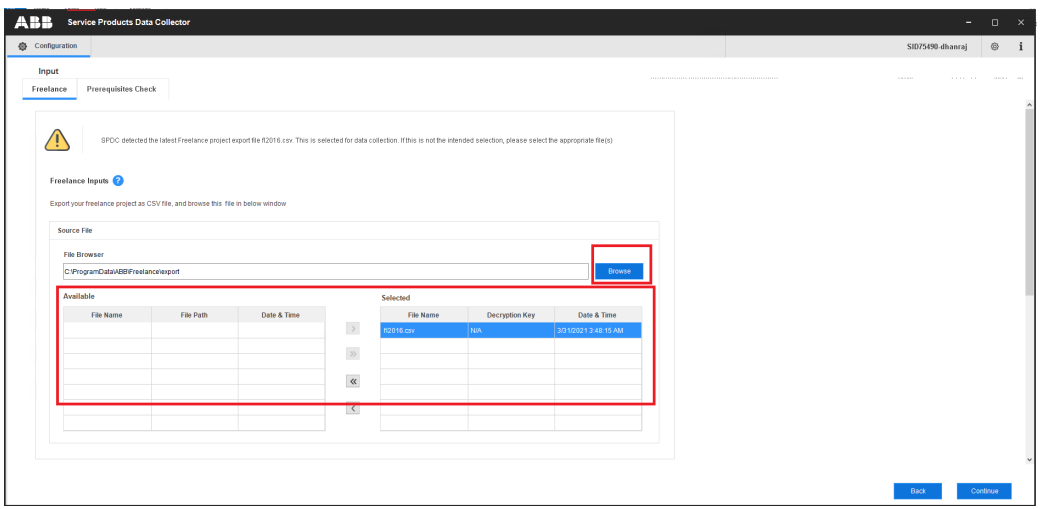

Figure 104. Project Folder

12. 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.

13. 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.

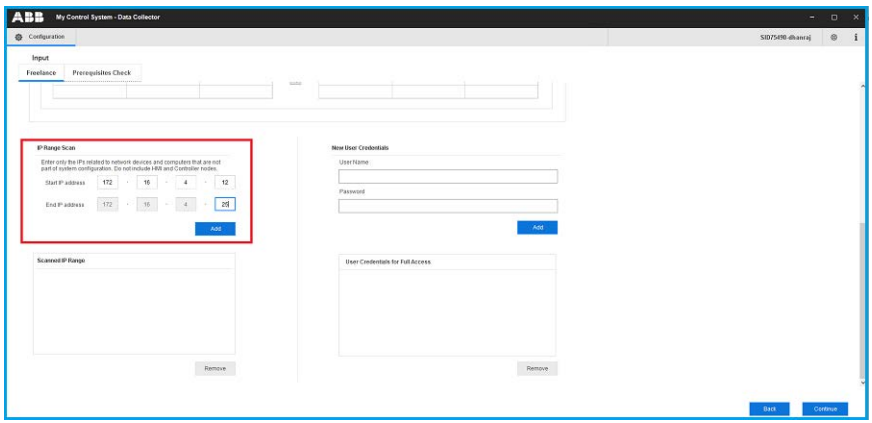

Figure 105. HMI Nodes

14. If an incorrect range is added, it can be removed: just select it and then select the **Remove** button.
15. Next input is user Credentials. Provide user name 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.
16. If incorrect credentials are added, they can be removed: just select these and then select the **Remove** button.
17. The last step it to acknowledge that all the prerequisites for data collection have been verified and are as expected. 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. If the up to the user to have implemented these in all the computers part of data collection. For this, click the tab Prerequisites and confirm each prerequisites by checking the check box 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 Section 2, Prerequisites.

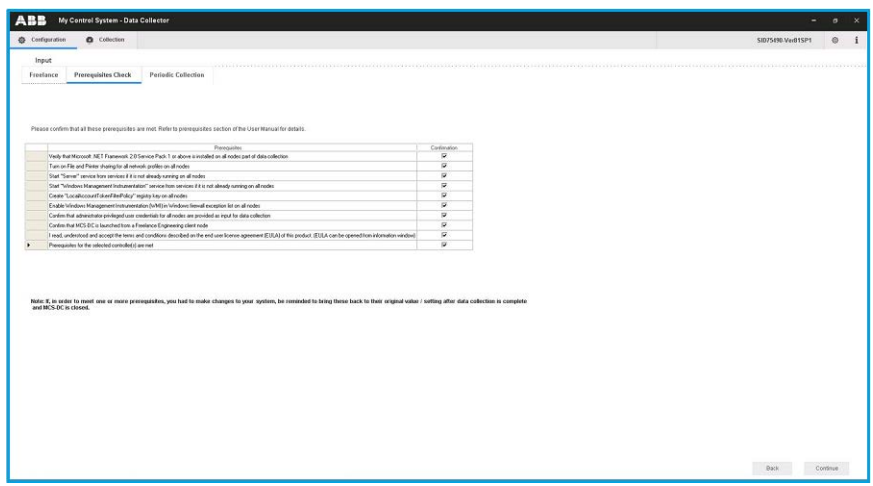

Figure 106. Prerequisites

18. Click on the **Continue** button to proceed to collection screen.
19. Collection screen appears. 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.
20. 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.

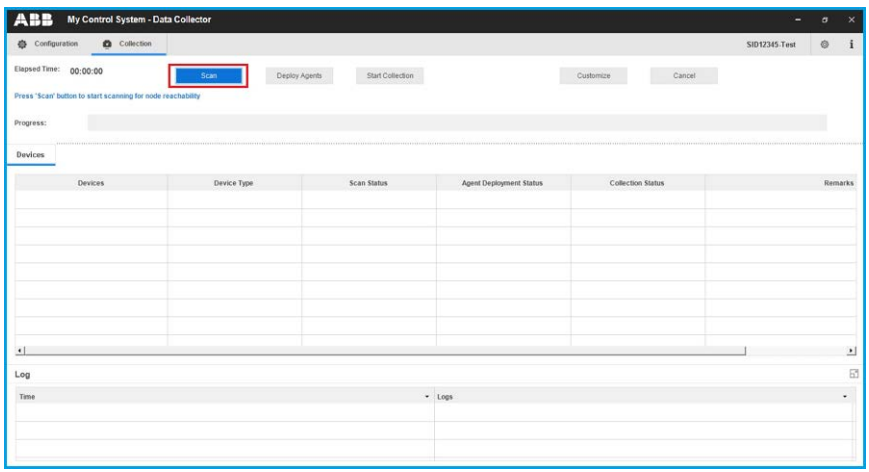

Figure 107. Scanning the Nodes

21. Progress bar shows the progress of scanning.
22. 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.

23. 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 rescan (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.

24. 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 rescan (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.

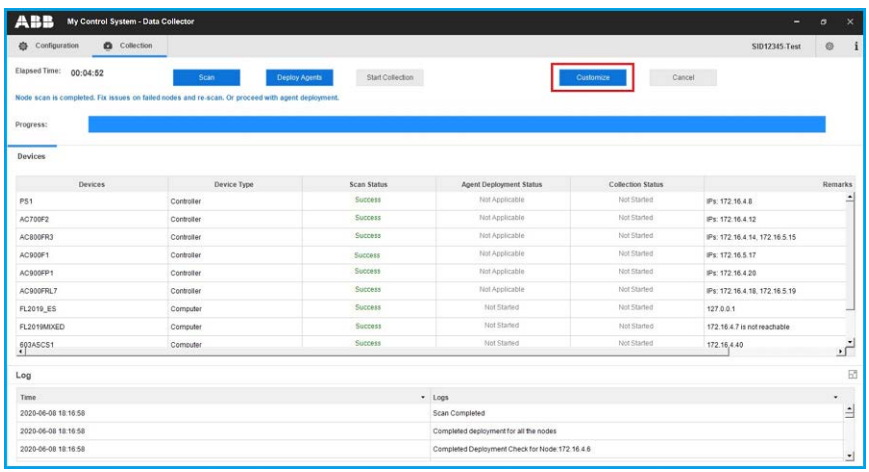

Figure 108. List of Nodes

25. 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 de-select the nodes that are not desired to be collected, by un-checking the respective check boxes 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.

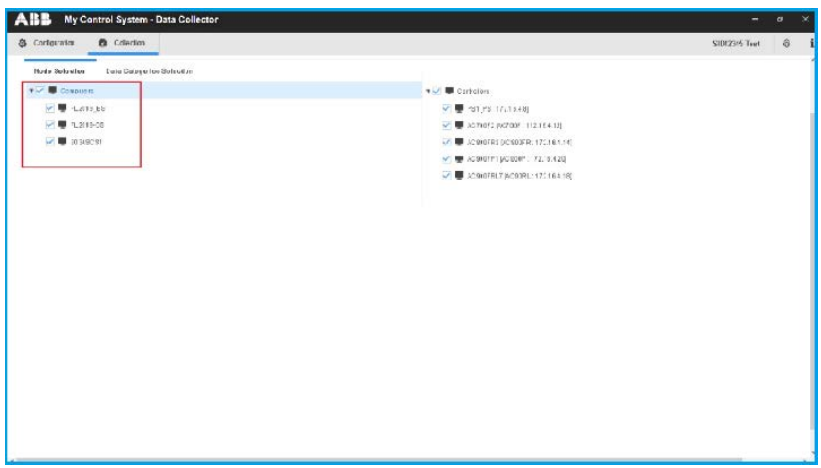

Figure 109. Customize Option

26. 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 de-select the data categories that are not desired to be collected by un-checking the respective check boxes against the data category names. Clicking on the **OK** button will save the customization configuration and close the customize 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.

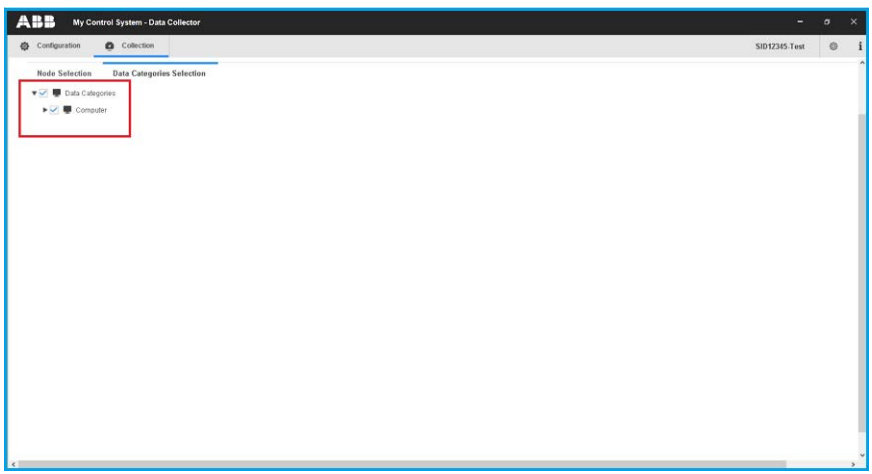

Figure 110. Select the Nodes

27. 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.

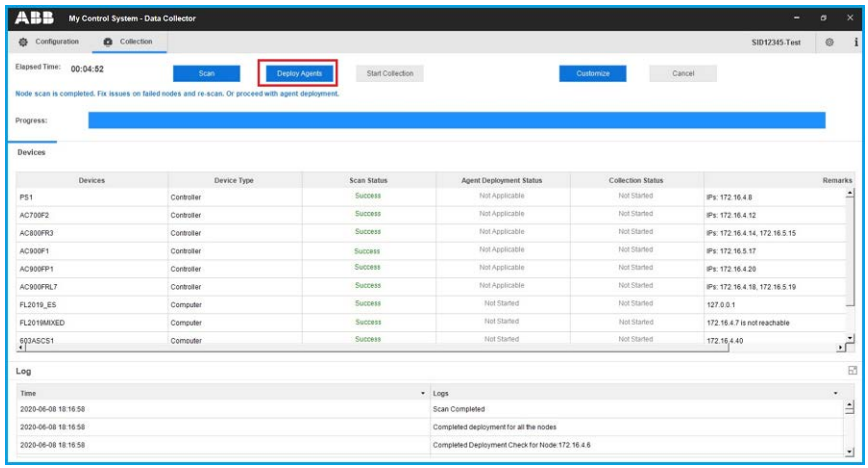

Figure 111. Deploy Agents

28. 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 on the **Start Collection** button to start the data collection.

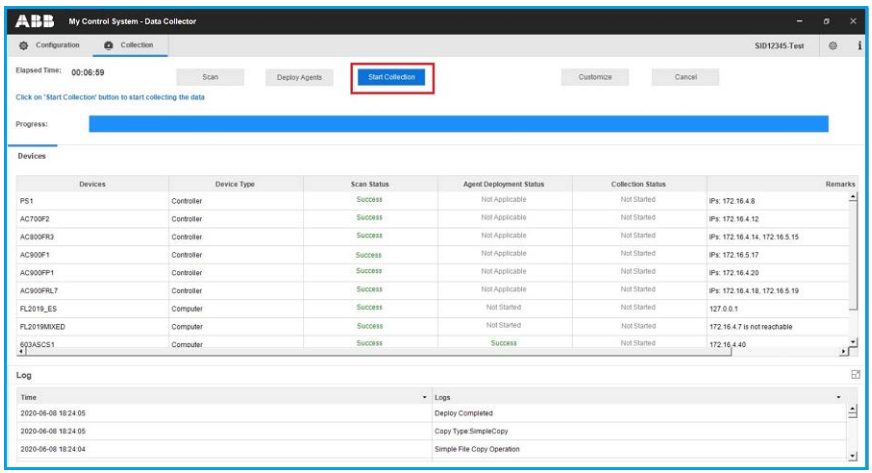

Figure 112. Agent Deployment Status

29. Data collection progress can be seen on the progress bar and on the Collection Status column.

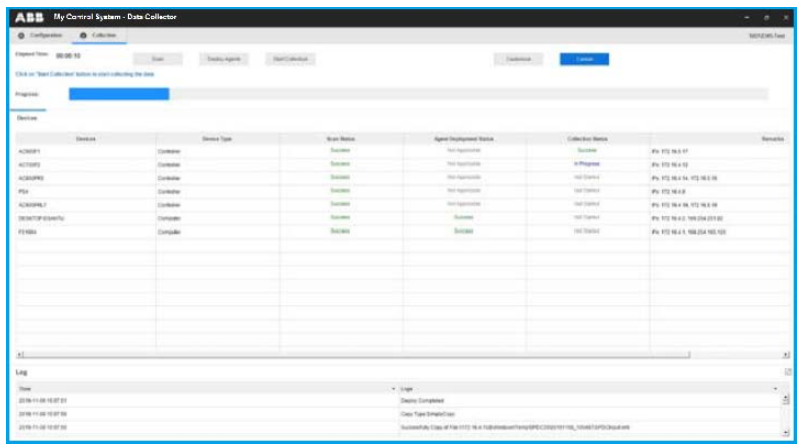

Figure 113. Data Collection Progress

30. 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.

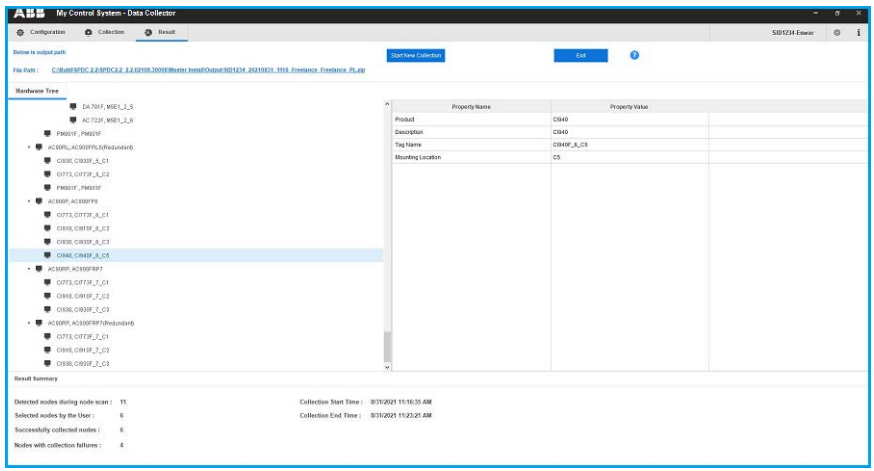

Figure 114. Collection File Path

31. 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.
32. Click on the **Start New collection** button to get back the Configuration screen and start with a new collection. Click on the **Exit** button to close the MCS-DC application.

3.4.3 Advanced mode data collection for S+ Operations with Harmony Controllers

1. Deploy MCS-DC in the hard drive (Operating System partition) of the node from which data collection must be executed.

   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.

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

     a) Performance and Lifecycle data: S+ Control Engineering node (Composer Harmony is present)

     b) Performance data only: Recommended on S+ Control Engineering node or any node from where control network is reachable.

2. Double-click on the **MCS-DC_Launcher.exe**, to launch the tool. The initial screen appears as shown below. MCS-DC tool runs some preliminary checks on the launch node. If the checks are passed, a Green tick mark is shown, click the Launch button to proceed for data collection. If the checks fails, a Red Cross mark is shown. What is missing, or exists but in an incorrect version, must be installed before launching the tool again. If there is not enough disk space, remove some old or temporary files in order to make space.

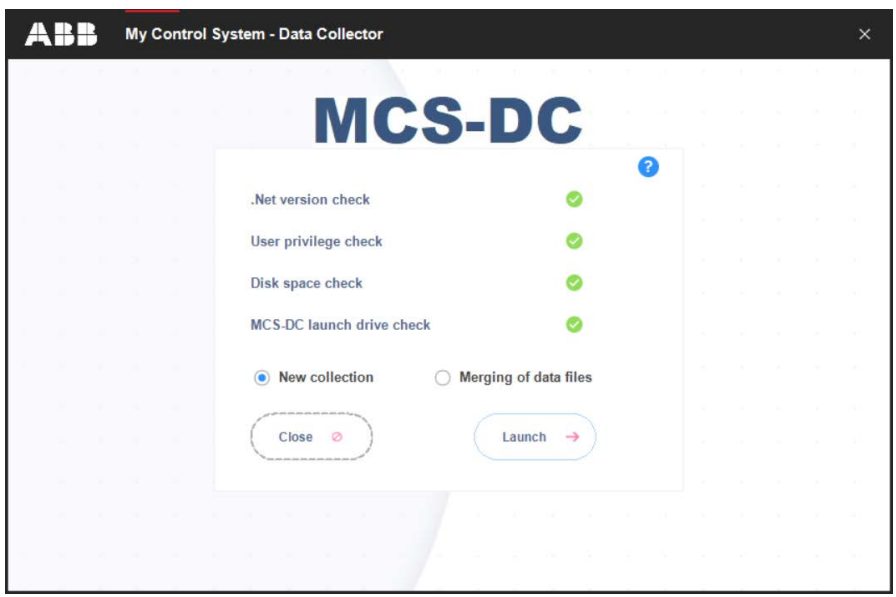

Figure 115. MCS-DC Launcher

- .NET Framework version check.

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

  If the .NET Framework version is lower than 1.1 the check fails, as MCS-DC can't be launched.

- Prerequisites check.

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

  a) User Privileges Check, checks if the MCS-DC Tool is launched in the user account with administrator privileges.

  b) System drive launch check, MCS-DC tool must be launched from the local disk drive of the launch node.

  c) Required Disk Space Check, Free disk space of 500MB must be available on the disk drive from which the MCS-DC is launched.

3. Provide the System ID of the S+ Operations HMI and your full name and provide password for encryption. This 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 is 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.

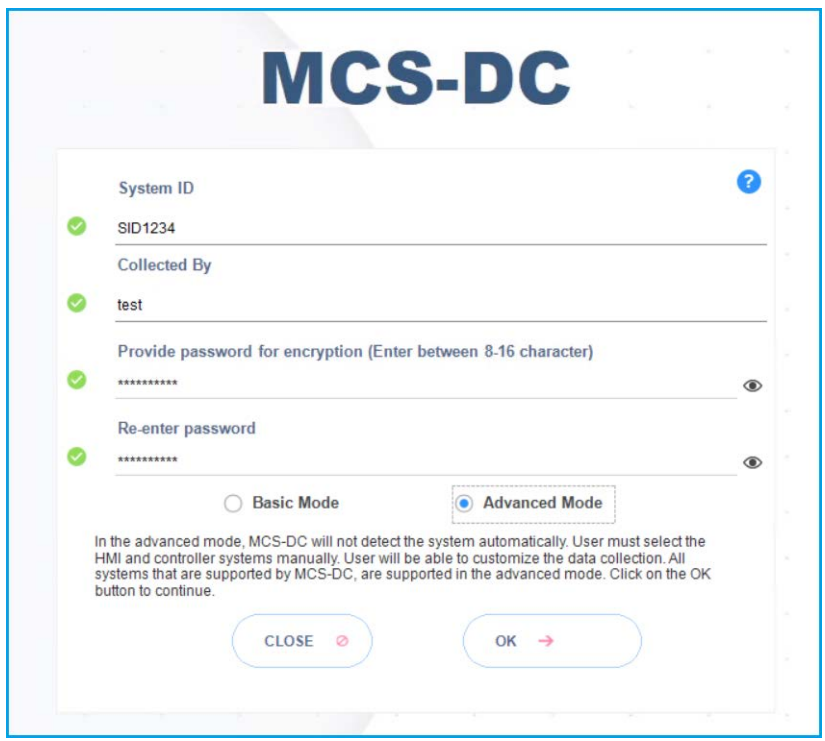

Figure 116. System credentials For Advanced Mode

4. Configuration screen appears. Click S+ Operations On the left pane and select the check box for the required data category (Performance, Life Cycle, Security). If Security is selected, data collection for each node will take some extra time. Security data can be collected only for S+ Operations version 2.1 or higher. Similarly, Select Harmony on the right pane and select the check box for the required data category (Performance, Life Cycle). Click Continue. Figure 117

Default selection of HMI is 800xA. To change the selection, click on the name of the HMI. Selected HMI is highlighted in Blue.

If S+ Operations HMI is selected, along with it only one Controller category can be selected at a time for data collection.

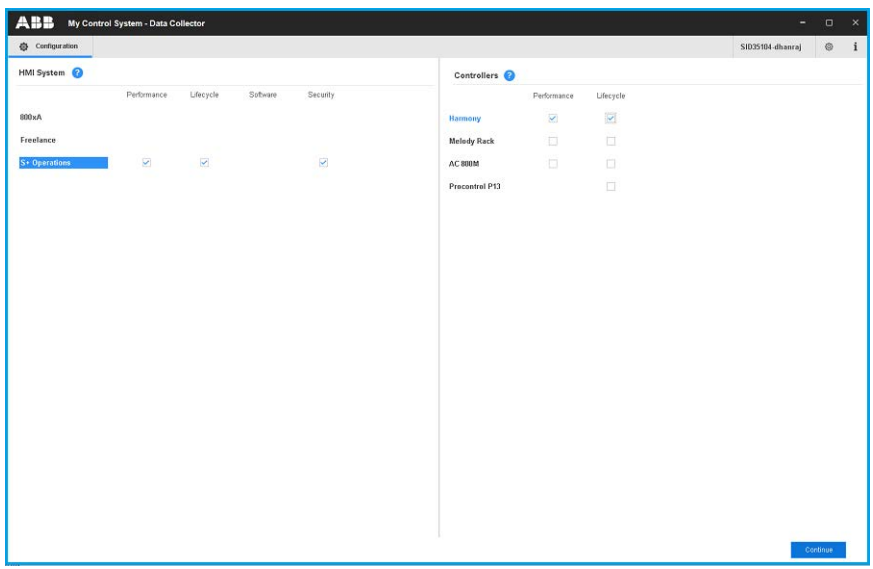

Figure 117. S+ Operations with Harmony

5. Input configuration screen appears.

6. 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.

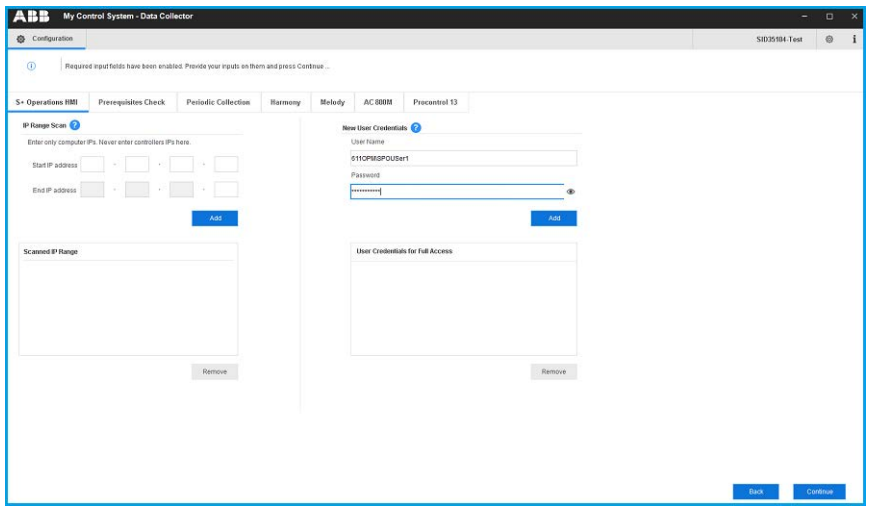

Figure 118. IP Range Scan

7. Provide the IP range and click on **Add** button. User can provide multiple ranges.

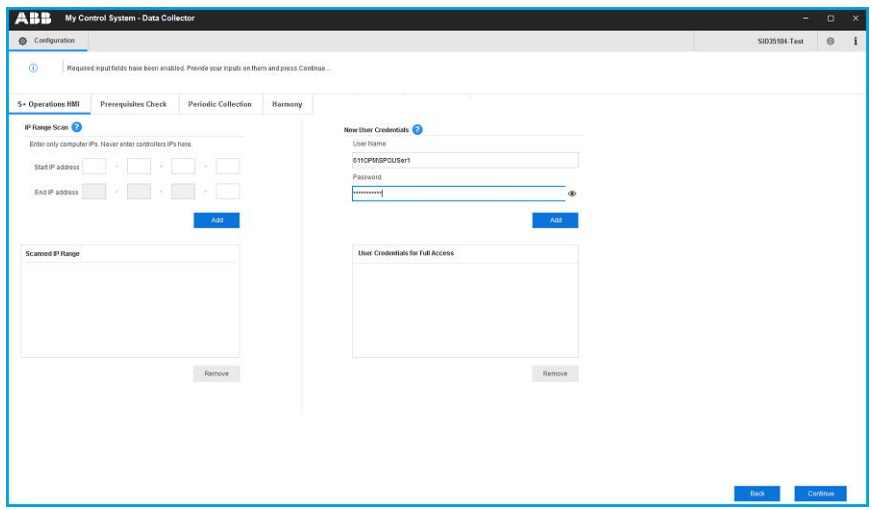

Figure 119. ADD IP Range

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

9. Harmony INFI-NET Controllers Performance Input: Click on **Harmony** tab to provide input for Harmony controllers data collection. User has option to select INFI-NET or PN800 control network. Provide the below inputs to proceed with INFI-NET controller data collection.

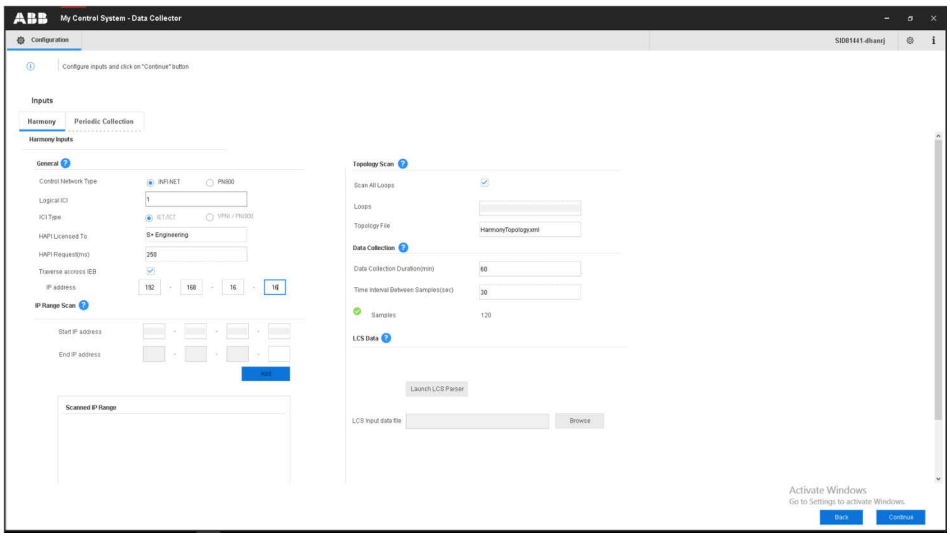

Figure 120. Harmony Rack Tab

- General

  a) Controller Type: Select INFI-NET as control network type.

  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): This interval, is the rate at which MCS-DC raise requests to the connected DCS System, in milliseconds and it is the minimum time interval between two consecutive requests to HAPI.

Default value is 250 milliseconds. Higher value will decrease the load on control network. Keep the default input.

f) Traverse across IEB: If IEB bridge is present in the network, MCS-DC can traverse through it and collect data from PN800 network. In this case, user needs to enable the check box and provide the IPT bridge module IP address.

In order to traverse the IEB bridge, a minimum CAPI version of 5.1.0.12 must be used.

- IP Scan Range- This input is applicable only if VPNI/PNI800 ICI Type is selected. Provide the required Controller IP range, Data collection will be done only for the Controllers for which the IP address is entered here.
- 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). It is must to mention the loop number connected to ICI.

  c) Topology File: Provide Name of Harmony Rack topology scan file
- Data Collection

  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 Samples = Data Collection Duration*60 / Time Interval Between Samples. Please note that the minimum Samples 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 entered, a Red cross mark will appear.

10. LCS data collection input: If the user already has a valid LCS input data file (.csv), skip this step and proceed to Step 11. For generating a new LCS Input data file, make sure that MCS-DC tool is launched in the Harmony Rack engineering node. In the harmony Rack inputs page, click on Launch LCS Parser button and follow the below procedure.

    a. Click on **Open Project** button.

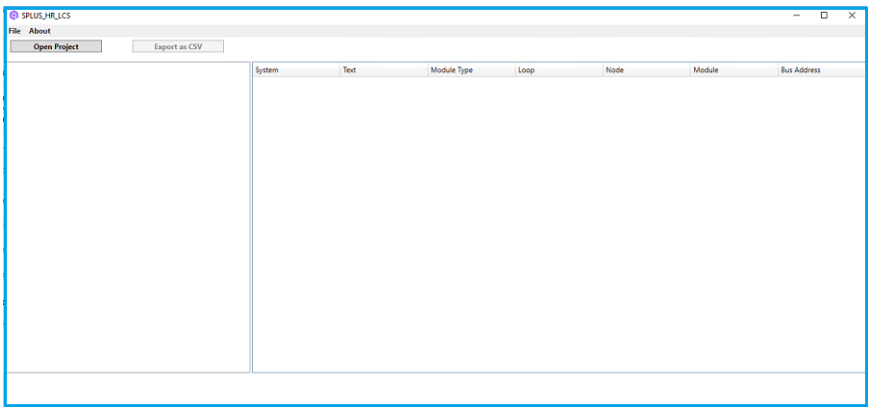

Figure 121. Open project

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

c. The following window appears with a progress bar as highlighted in Figure 122, 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.

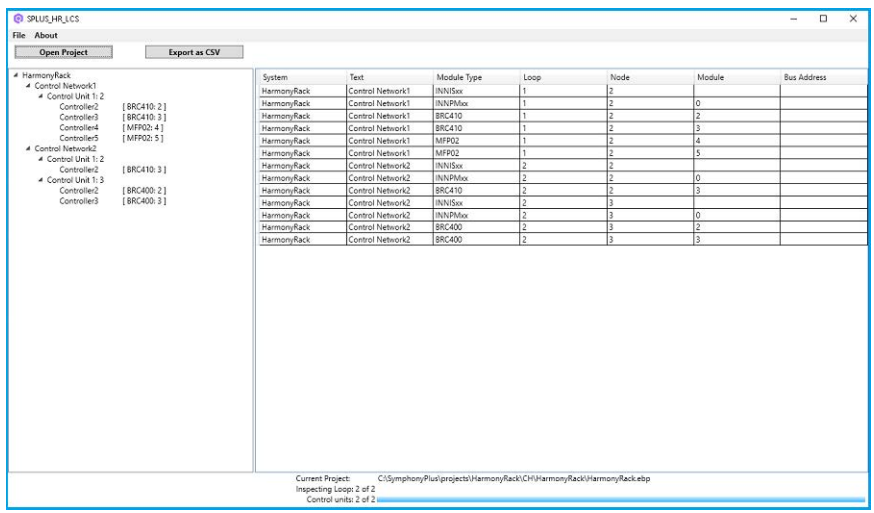

Figure 122. Export .CSV File

d. A popup appears as a confirmation that the .csv file is exported successfully. Click **OK**.

11. Click Browse button to select the .csv file generated in the previous step.

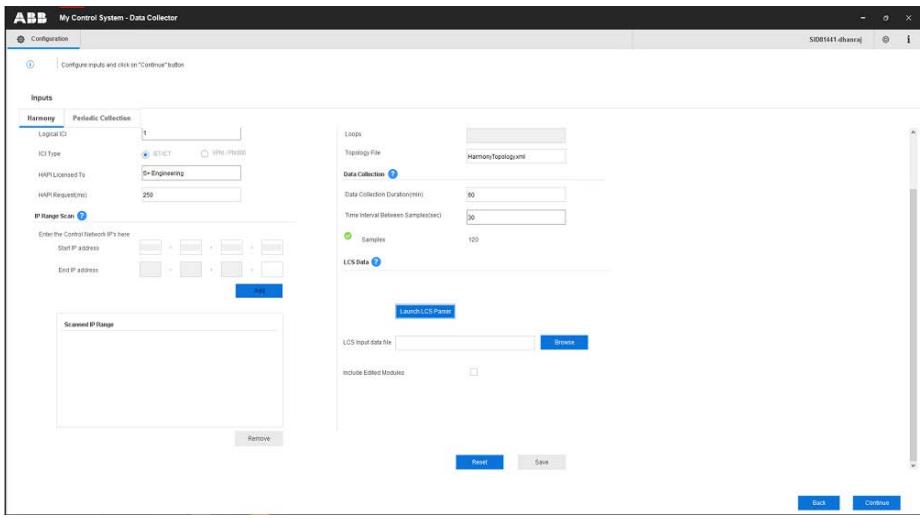

Figure 123. Harmony Rack Input Data File

12. Include Edited Module: If modules in the CSV file is to be manually edited to match with physical setup, this check box shall be checked. Also, it is possible to include certain hardware modules in the report for which data cannot be electronically read, if this check box is checked.

    This check box applicable for Harmony Rack module and when both performance and LCS data is collected.

13. PN800 Network Controller Performance Collection Input: Click on **Harmony** tab to provide input for Harmony controller data collection. User has option to select INFI-NET or PN800 control network. Provide the below inputs to proceed with PN800 network data collection.

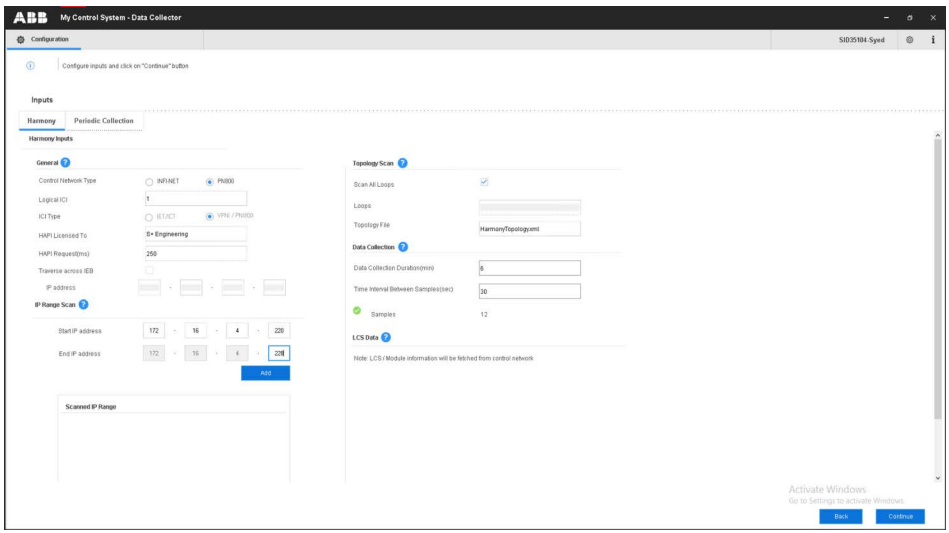

Figure 124. Harmony Rack

Input a to c is applicable for PN800 network modules performance data collection. Input a to d is applicable for PN800 network modules LCS data collection.

a. General:

1) Controller Type: PN800 control network type.

2) Logical ICI: Provide the ICI number configured by Harmony System Configuration Utility (hSysCfgU.exe) for connecting into control network.

3) HAPI Licensed To: Keep the default input S+ Engineering, unless it is different.

4) HAPI Request (ms): This interval, is the rate at which MCS-DC raise requests to the connected DCS System, in milliseconds and it is the minimum time interval between two consecutive requests to HAPI.

Default value is 250 milliseconds. Higher value will decrease the load on control network. Keep the default input.

5) ICI Type: This selection will be done automatically based on Control Network Type selection. For PN800, VPNI/PNI800 will be selected.

b. IP Scan Range - Provide the required Controller IP range, Data collection will be done only for the Controllers for which the IP address is entered here. Note that PNI800 module IP address must be included in the IP Scan Range, in order to make it part of the collection.

c. Topology Scan:

1) Scan All loops: Check this Check Box to scan all loops.

2) Loops: To Scan the specific loops, provide the loop numbers separated with comma (Example: 1, 5, 6). It is must to mention the loop number connected to ICI.

3) Topology File: Provide Name of Harmony Rack topology scan file.

d. Data Collection:

1) 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.

2) 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.

3) Samples: Samples are auto calculated based on the formula Samples = Data Collection Duration*60 / Time Interval Between Samples.

Please note that the minimum Samples 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.

14. Symphony Din and ENM controller Input, IP Scan Range: Provide the required Controller IP range and click on **Add**. User can provide multiple IP ranges. Data collection will be done only for the Controllers within the IP Address range that has been entered.
15. If a wrong IP range is added, there is an option to remove that. To remove a wrong IP range, select the IP range by clicking on it and then click on the **Remove** button. Click **Continue** to proceed.

16. Once all HMI and connect inputs are provided, it is required to acknowledge that all the prerequisites for data collection, collection are met. For this, select the Prerequisites tab and confirm each of these by checking the check box 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 Section 2, Prerequisites.

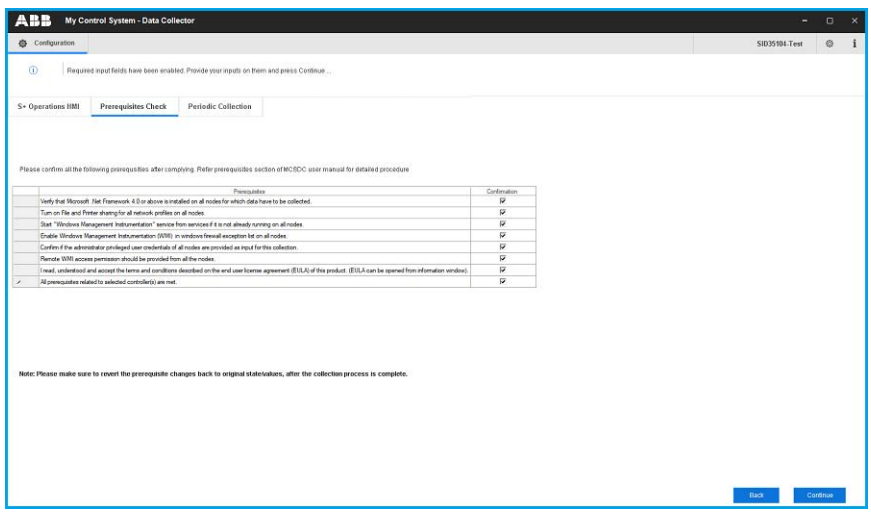

Figure 125. Prerequisite Check

17. Click on the **Continue** button to proceed to collection screen.

18. Collection screen appears. 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 to list 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.

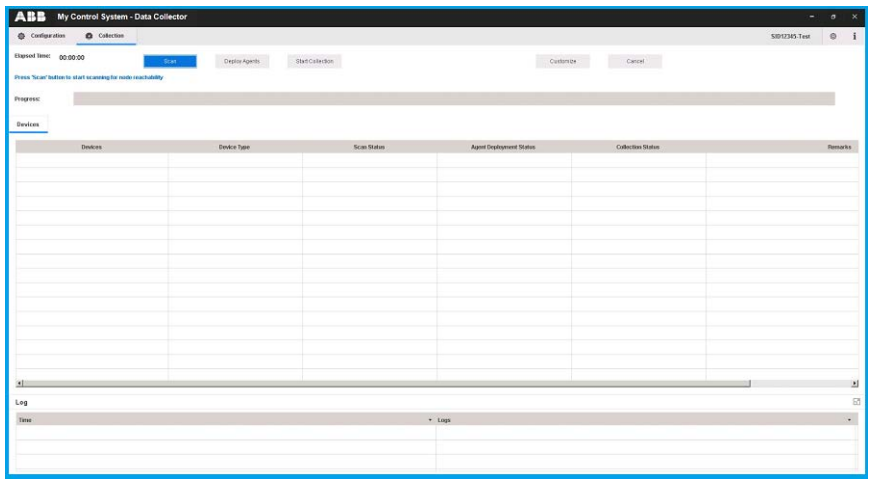

Figure 126. Data Collection Screen

19. 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.

20. Progress bar shows the progress of scanning.

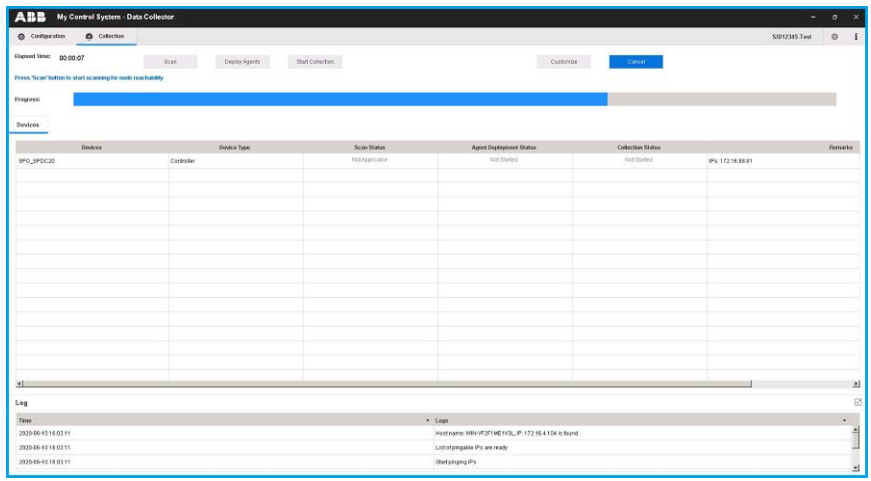

Figure 127. Scan Progress

21. 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 (for example AC 800M controller), then the status is “Not applicable” in Grey.
22. 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 rescan (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.

23. Once node scan is completed, Deploy Agents and Customize buttons will be enabled. User can customize the collection by selecting required HMI/controller nodes from the list of accessible nodes, using customize option. Clicking on the **Customize** button opens customization window.

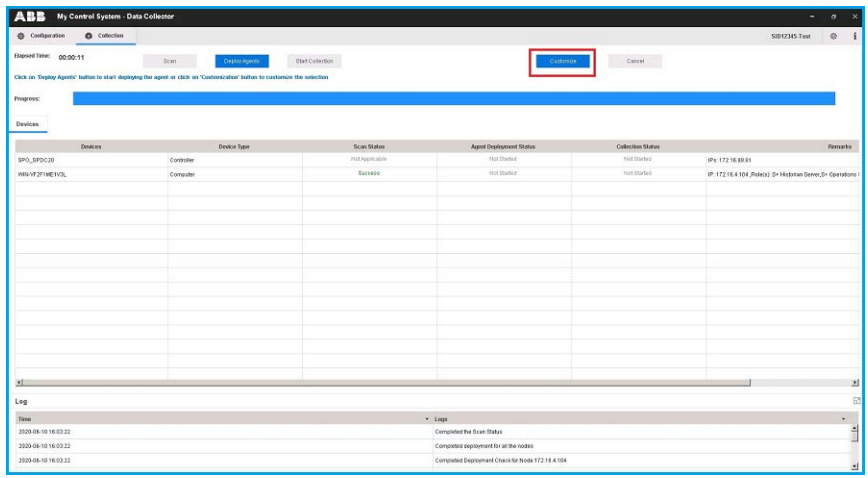

Figure 128. Scan Status

24. User has an option to customize the Data collection nodes for Performance and Lifecycle data collection, to Customize click on the **Customize** button. All accessible HMI and controller nodes are listed. All accessible HMI and controller nodes will be selected by default. User can de-select the nodes that are not desired to be collected, by un-checking the respective check boxes, 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.

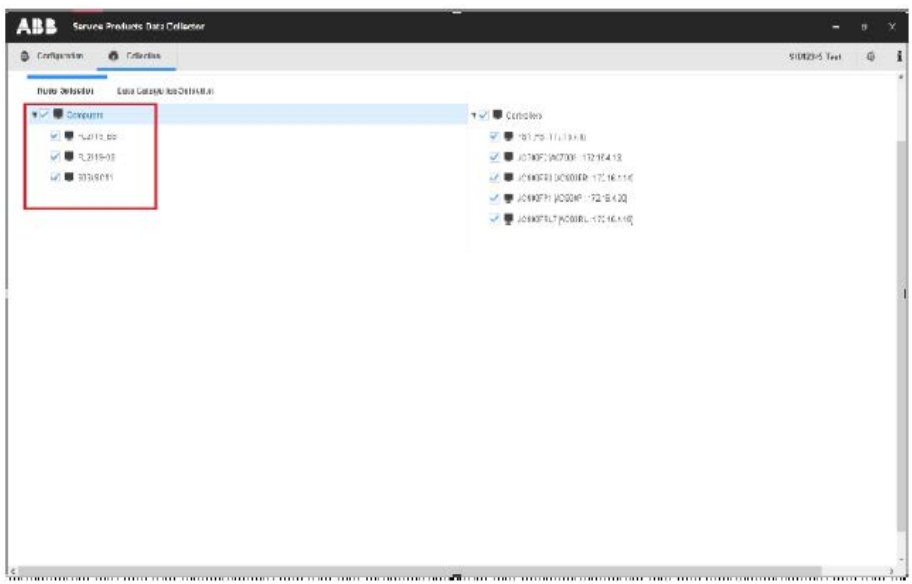

Figure 129. Node Selection

25. 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 de-select the data categories, that are not desired to be collected by un-checking the respective check boxes against the data category names. Click on **OK** button to save the customization configuration and close the customize window. Click on **Reset** button if you wish to reset the customization configuration. Data categories customization is applicable only for HMI nodes, it is not applicable for controllers.

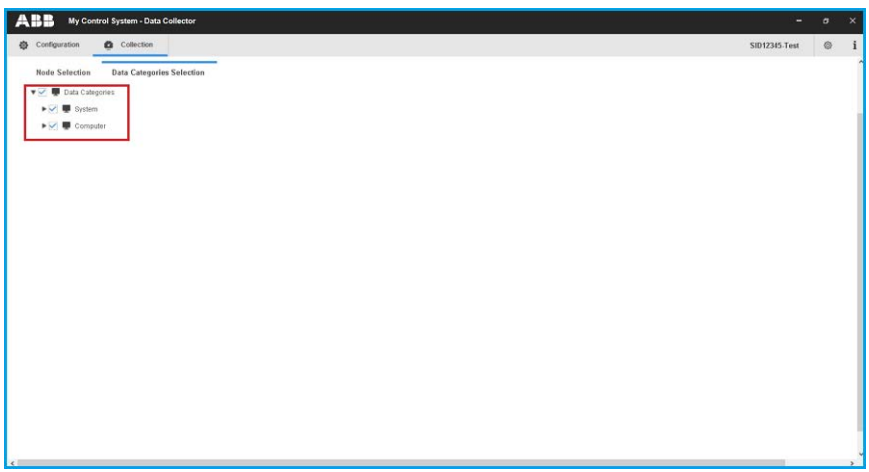

Figure 130. Data Category Selection

26. 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.

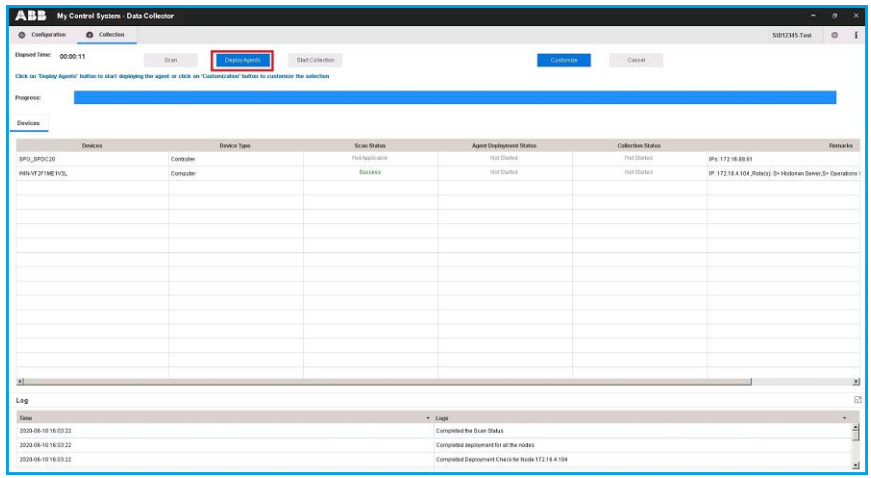

Figure 131. Start Collection

27. 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 is enabled. Click on the **Start Collection** button to start the data collection.
28. Data collection progress can be seen on the progress bar and on the Collection Status column.
29. 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 contains information about the hardware tree and the bottom part contains the collection statistics.

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

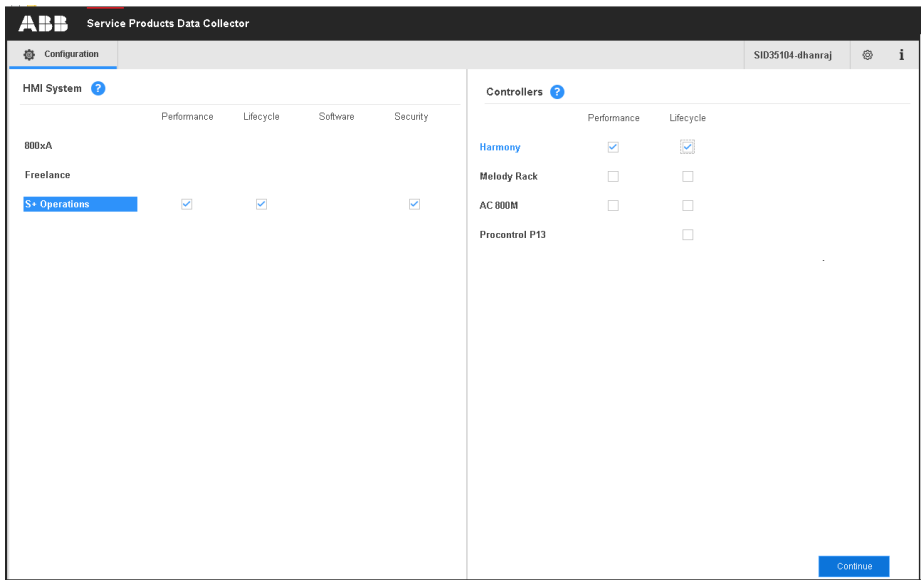

Figure 132. Collection File Path

31. Click on the **New collection** button to get back the Configuration screen and start with a new collection. Select the **Exit** button to close MCS-DC.

3.4.4 Advanced mode data collection for S+ Operations with Melody Controllers

1. Copy the downloaded files of MCS-DC into the local disk (hard disk drive partition for Operating System) of a desired System S+ Operations node. Unzip the downloaded MCS-DC package. Depending on the HMI/Controller, MCS-DC launch nodes may vary. For S+ Operations with Melody Controllers, Melody Rack engineering node or any S+ Operations node which is part of Onet network and S+ Operations network, shall be used. Additionally CSE_Config file has to be synchronized in the node.
2. Double-click on the **MCS-DC_Launcher.exe**, to launch the tool. It is present inside the unzipped MCS-DC folder. The initial screen appears as shown in Figure. MCS-DC tool runs the below checks on the launch node. If the check is passed, a Green tick mark is shown, click the Launch button to proceed for data collection. If the check fails, a Red Cross mark is shown, user has to fix the issue and launch the MCS-DC tool again.

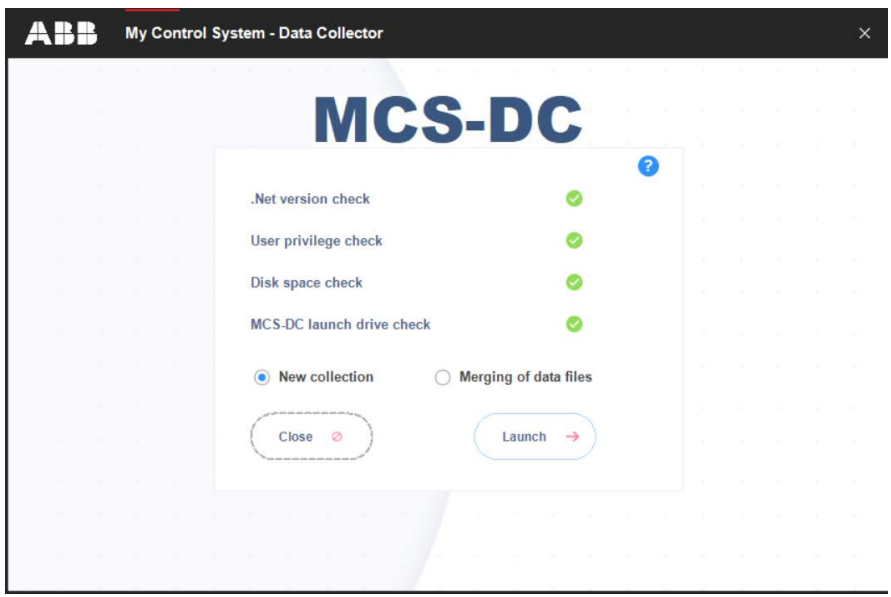

Figure 133. MCS-DC Launcher

- .NET Framework version check.

If the .NET Framework version is 1.1 or above, then this check is passed and MCS-DC 2.X version can be launched for data collection.

If the .NET Framework version is lower than 1.1, then this check is failed and MCS-DC 2.X version cannot be launched for data collection, instead MCS-DC 1.9.x version 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.

  a) User Privileges Check, checks if the MCS-DC Tool is launched in the user account with administrator privileges.

  b) System drive launch check, MCS-DC tool must be launched only from the local disk drive of the launch node.

  c) Required Disk Space Check, Free disk space of at least 500MB must be available on the disk drive from which the MCS-DC is launched.

3. Provide the System ID of the S+ Operations HMI and your full name and provide password for encryption. This 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.

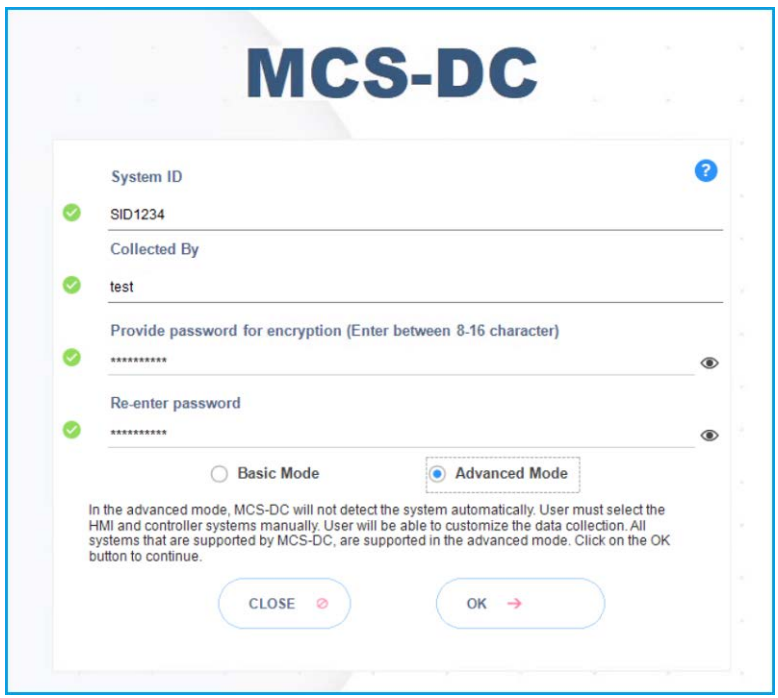

Figure 134. System credentials for Advanced Mode

4. Configuration screen appears. Click S+ Operations On the left pane and select the check box for the required data category (Performance, Life Cycle). Similarly, Select Harmony on the right pane and select the check box for the required data category (Performance, Life Cycle) and/or Security. Security option shall select only when it is needed as it will take significantly longer time for data collection. Click Continue. Figure 135

Default selection of HMI is 800xA. To change the selection, click on the name of the HMI. Selected HMI is highlighted in Blue.

If S+ Operations HMI is selected, along with it only one Controller category can be selected at a time for data collection.

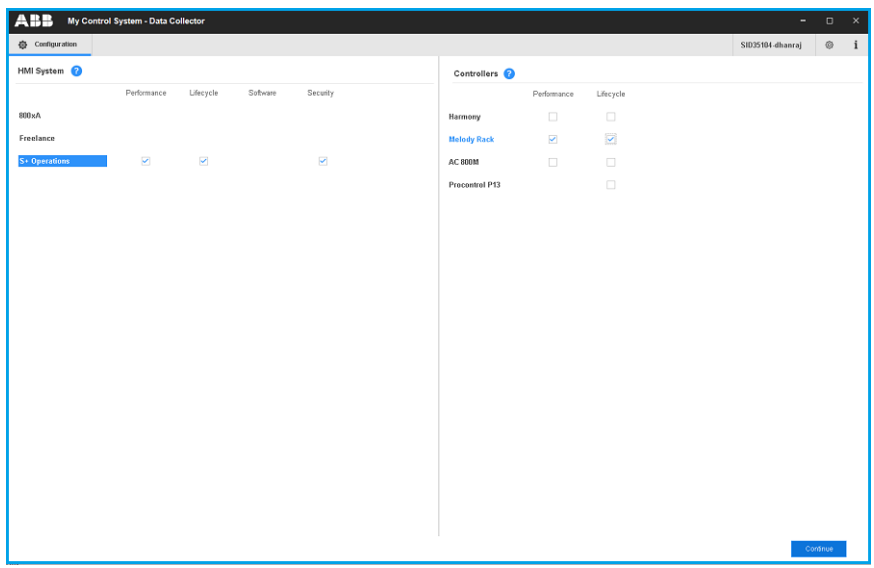

Figure 135. S+ Operations with Melody

5. Input configuration screen appears.

6. 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.

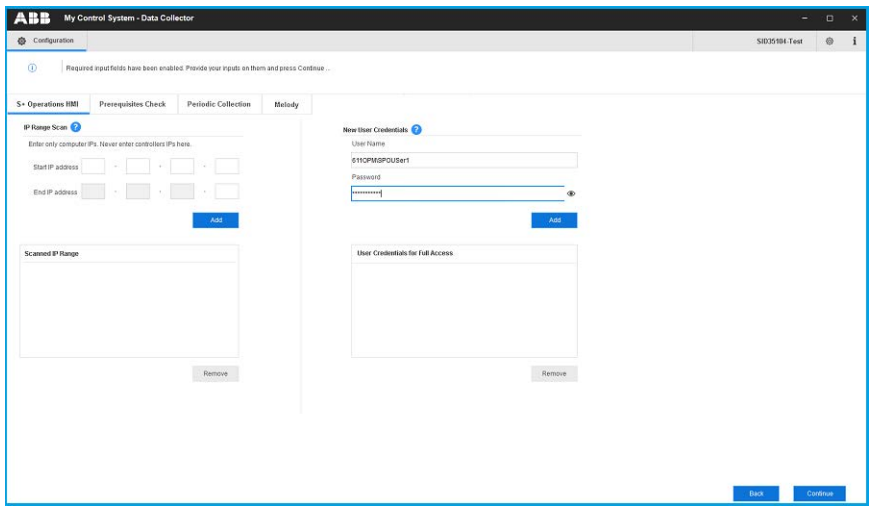

Figure 136. IP Range Scan

7. Provide the IP range and click on **Add** button. User can provide multiple ranges too.
8. 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.

9. Next input is user credential. Provide the **User Name** 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 on the **Add** button. Please note, for nodes in domain network, username should be provided in the format domain name\username.
10. There is an option to remove the added credentials. To remove, select the added credential and click on the **Remove** button.
11. Click on **Melody Rack** tab to provide input for Melody Rack controllers data collection (refer to Appendix D, System configuration export for exporting system configuration files).

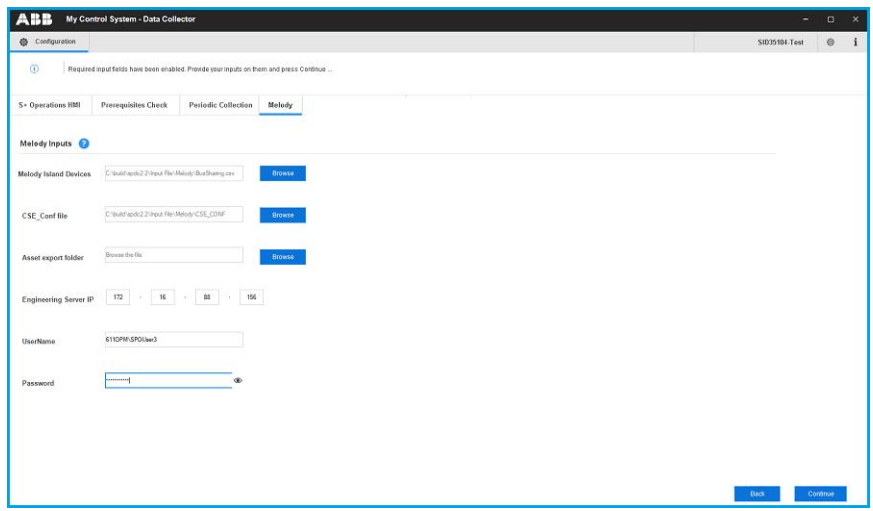

Figure 137. Melody Rack Data Collection Input

Provide the below inputs to proceed with Melody Rack controllers data collection and click Continue.

a. Melody Island Devices

   Click the **Browse** button to select the Melody Island Devices Export file.

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 user name.

f. Password

   Provide the Composer Melody node password.

12. 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 prerequisites by checking the check box 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 Section 2, Prerequisites.

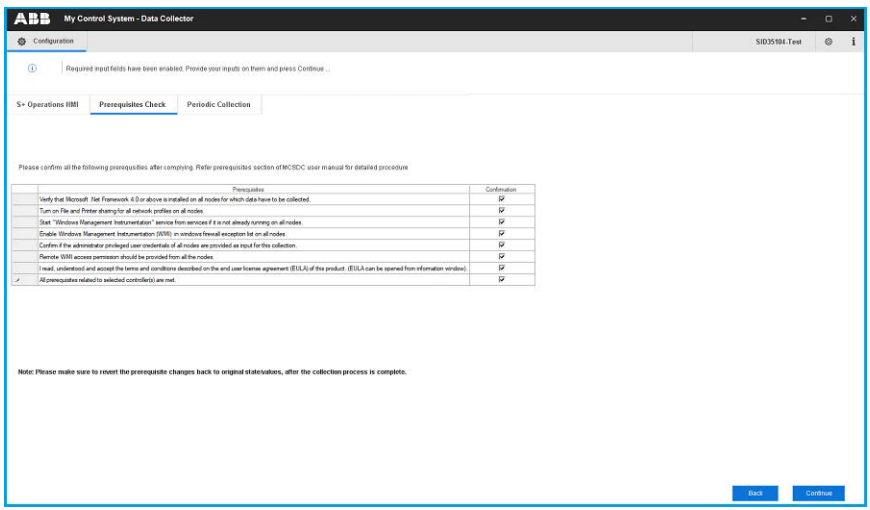

Figure 138. Prerequisite Check

13. Click on the **Continue** button to proceed to collection screen.

14. Collection screen appears. 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 to list 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.

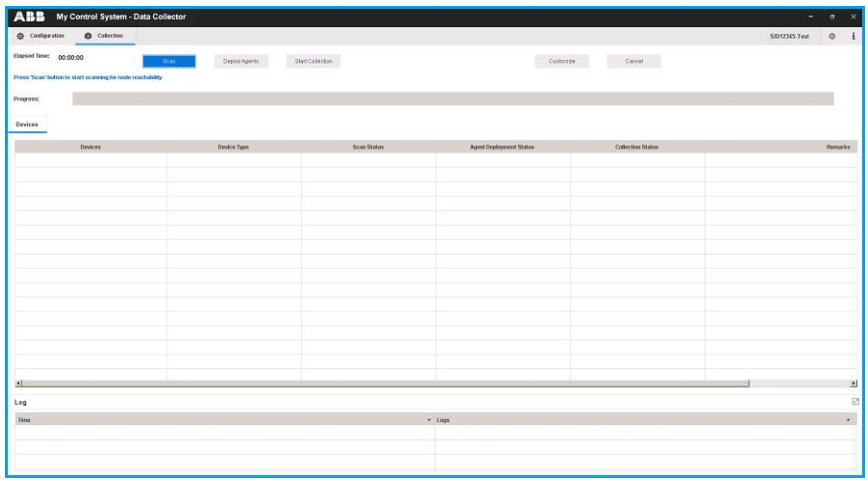

Figure 139. Data Collection Screen

15. 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.

16. Progress bar shows the progress of scanning.

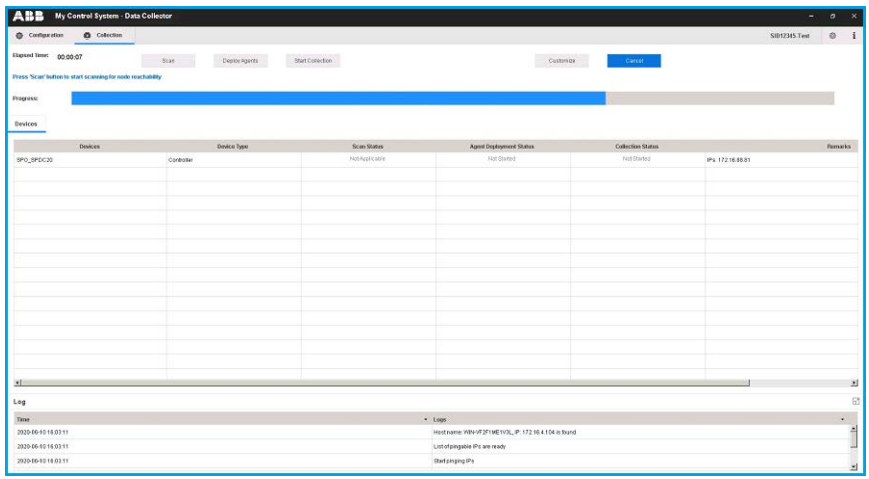

Figure 140. Scan Progress

17. 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 (for example AC 800M controller), then the status is “Not applicable” in Grey.
18. 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 rescan (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.

19. Once node scan is completed, Deploy Agents and Customize buttons will be enabled. User can customize the collection by choosing only few HMI/controller nodes from the list of accessible nodes, using customize option. Clicking on the **Customize** button opens customization window.

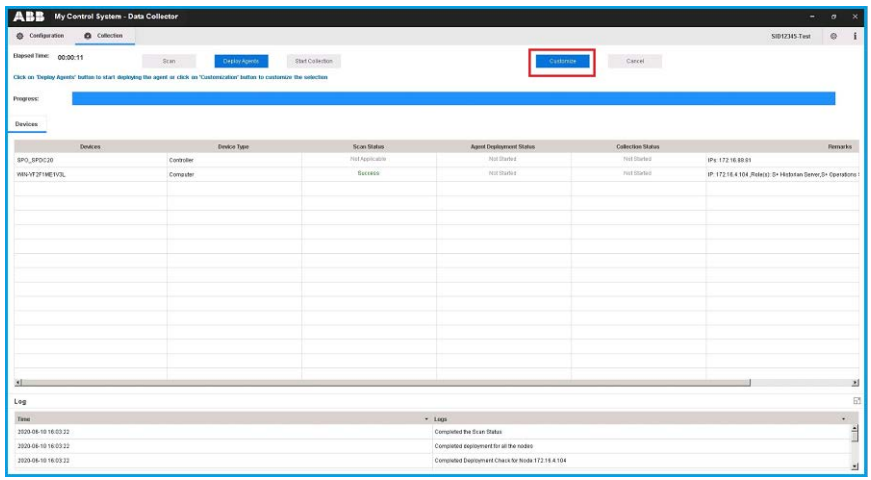

Figure 141. Scan Status

20. User has an option to customize the Data collection nodes for Performance and Lifecycle data collection, to Customize click on the **Customize** button. All accessible HMI and controller nodes are listed. All accessible HMI and controller nodes will be selected by default. User shall de-select the nodes that are not desired to be collected, by un-checking the respective check boxes, 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.

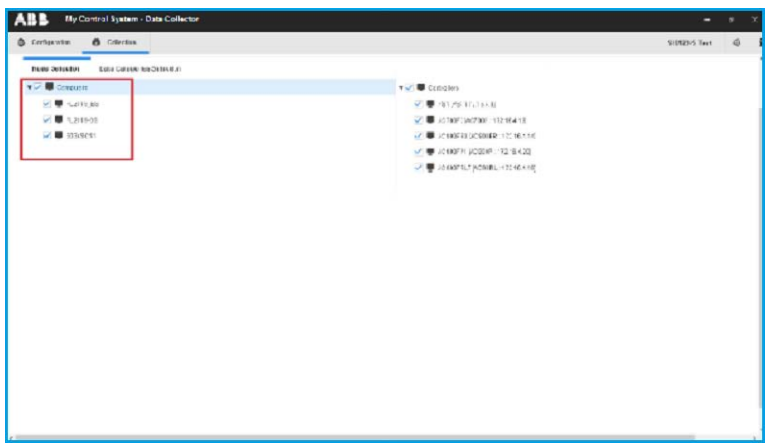

Figure 142. Node Selection

21. 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 de-select the data categories, that are not desired to be collected by un-checking the respective check boxes against the data category names. Click on **OK** button to save the customization configuration and close the customize window. Click on **Reset** button if you wish to reset the customization configuration. Data categories customization is applicable only for HMI nodes, it is not applicable for controllers.
22. 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.

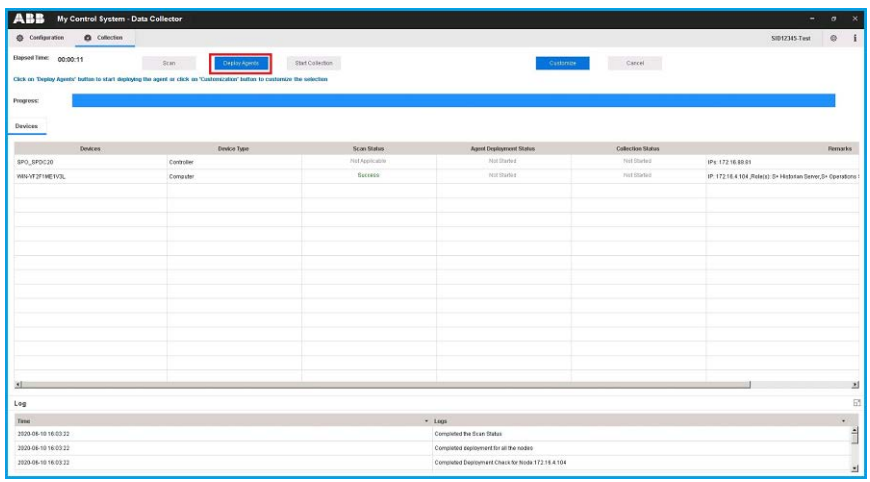

Figure 143. Start Collection

23. 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 get enabled. Click on the **Start Collection** button to start the data collection.
24. Data collection progress can be seen on the progress bar and on the Collection Status column.

25. 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 contains information about the hardware tree and the bottom part contains the collection statistics.
26. Collection file will be created automatically once the collection is completed. The collection file is created, and its file path appears on the screen. The collection file can be viewed by clicking on the file path.

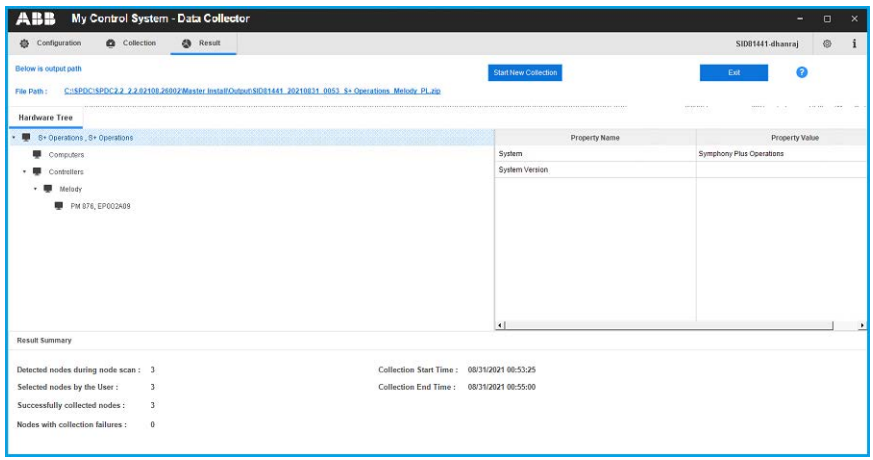

Figure 144. Collection File Path

27. Click on the **New collection** button to get back the Configuration screen and start with a new collection. Select the **Exit** button to close MCS-DC.

3.4.5 Advanced mode data collection for S+ Operations with AC800M Controllers

1. Copy the downloaded files of MCS-DC into the local disk (hard disk drive partition for Operating System) of a desired System S+ Operations node. Unzip the downloaded MCS-DC package. Depending on the HMI/Controller, MCS-DC launch nodes may vary. For S+ Operations with AC 800M Controllers, any S+ Operations node or AC 800M engineering node shall be used as launch node.
2. Double-click on the **MCS-DC_Launcher.exe**, to launch the tool. It is present inside the unzipped MCS-DC folder. The initial screen appears as shown in Figure. MCS-DC tool runs the below checks on the launch node. If the check is passed, a Green tick mark is shown, click the Launch button to proceed for data collection. If the check fails, a Red Cross mark is shown, user has to fix the issue and launch the MCS-DC tool again.

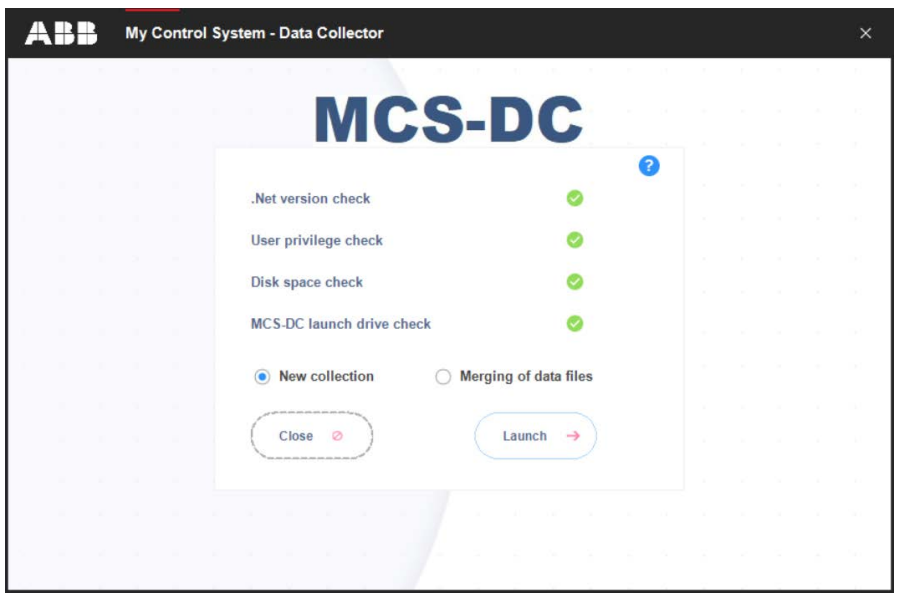

Figure 145. MCS-DC Launcher

- .NET Framework version check.

  If the .NET Framework version is 1.1 or above, then this check is passed and MCS-DC 2.X version can be launched for data collection.

  If the .NET Framework version is lower than 1.1, then this check is failed and MCS-DC 2.X version cannot be launched for data collection, instead MCS-DC 1.9.x version 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.

  a) User Privileges Check, checks if the MCS-DC is launched in the user account with administrator privileges.

  b) System drive launch check, MCS-DC must be launched only from the local disk drive of the launch node.

  c) Required Disk Space Check, Free disk space of at least 500MB must be available on the disk drive from which the MCS-DC is launched.

3. Provide the System ID of the S+ Operations HMI and your full name and provide password for encryption. This 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.

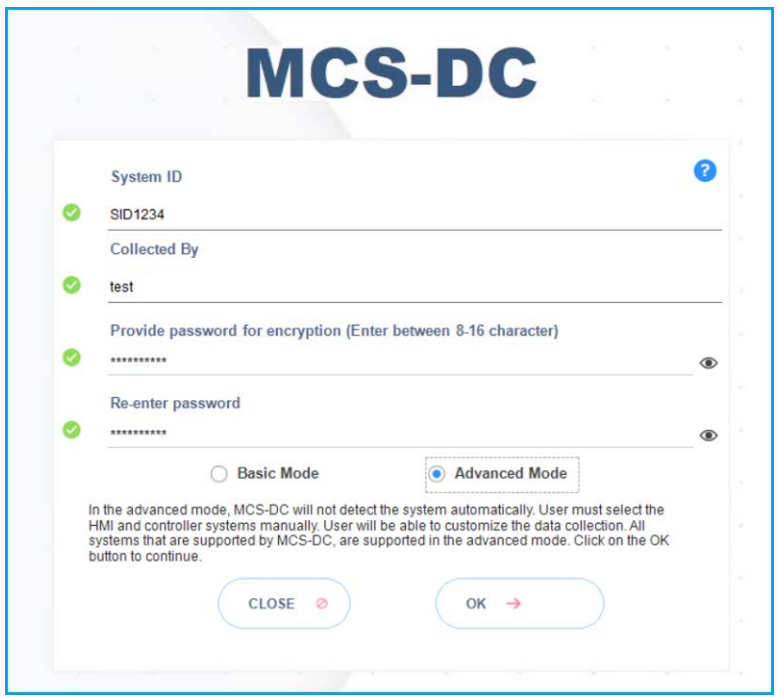

Figure 146. System credential For Advance Mode

4. Configuration screen appears. Click S+ Operations On the left pane and select the check box for the required data category (Performance, Life Cycle). Similarly, Select Harmony on the right pane and select the check box for the required data category (Performance, Life Cycle) and/or Security. Security option shall select only when it is needed as it will take significantly longer time for data collection. Click Continue. Figure 117

Default selection of HMI is 800xA. To change the selection, click on the name of the HMI. Selected HMI is highlighted in Blue.

If S+ Operations HMI is selected, along with it only one Controller category can be selected at a time for data collection.

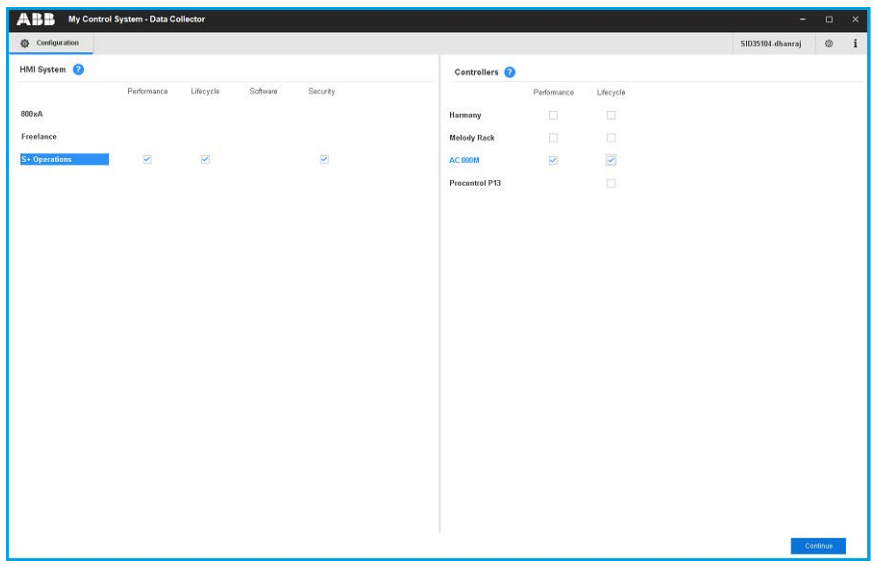

Figure 147. SPO with AC800M

5. Input configuration screen appears.
6. Under S+ Operations HMI tab, IP range scan input: 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.

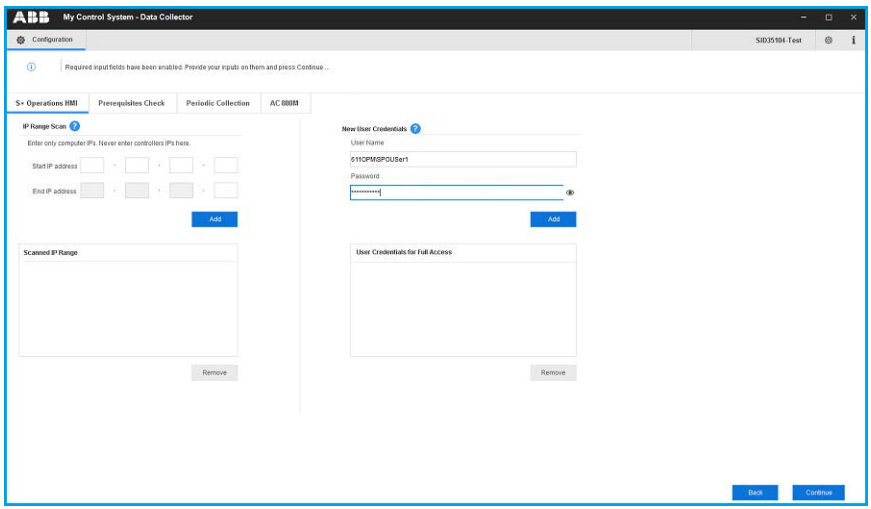

Figure 148. IP Range Scan

7. Provide the IP range and click on **Add** button. User can provide multiple ranges too.
8. 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.

9. Next input is user credential. Provide the **User Name** 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.
10. There is an option to remove the added credentials. To remove, select the added credential and click on the **Remove** button.
11. Click on **AC 800M** tab to provide input for AC 800M controllers data collection.

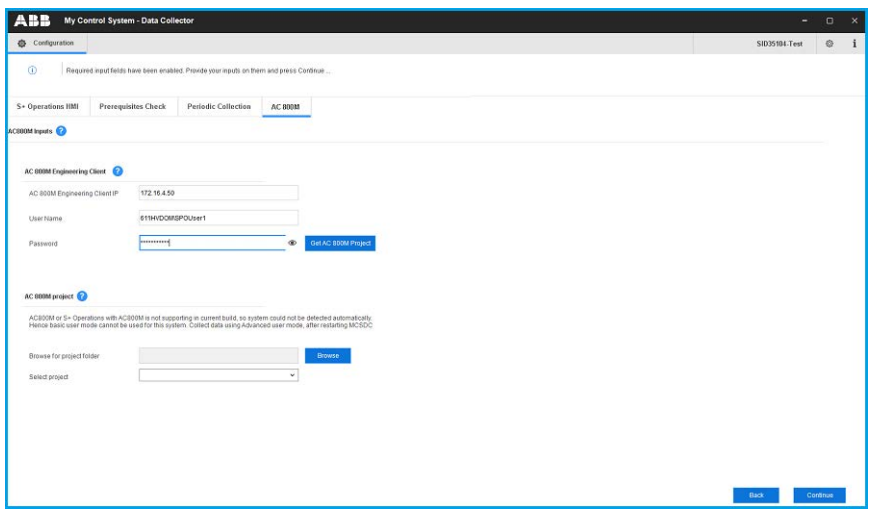

Figure 149. AC 800M Data Collection Input

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 user name of an user account of the engineering client with administrative right

c. Provide password of the user account

- AC 800M Project:

a. Browse For AC800M Project Folder by clicking Browse button.

b. Select the required AC800M project from the drop down list.

12. 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 auto populated. 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

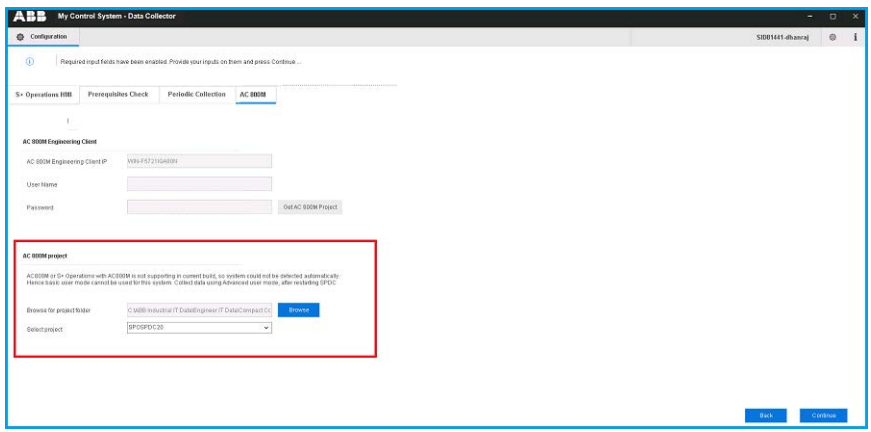

Figure 150. Browse and Select AC 800M Project

13. 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 prerequisites by checking the check box 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 Section 2, Prerequisites.

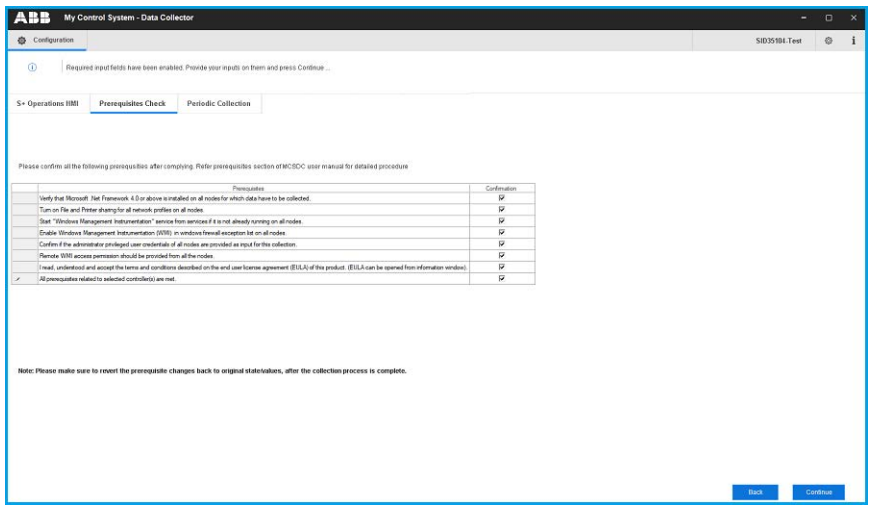

Figure 151. Prerequisite Check

14. Click on the **Continue** button to proceed to collection screen.

15. Collection screen appears. 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 to list 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.

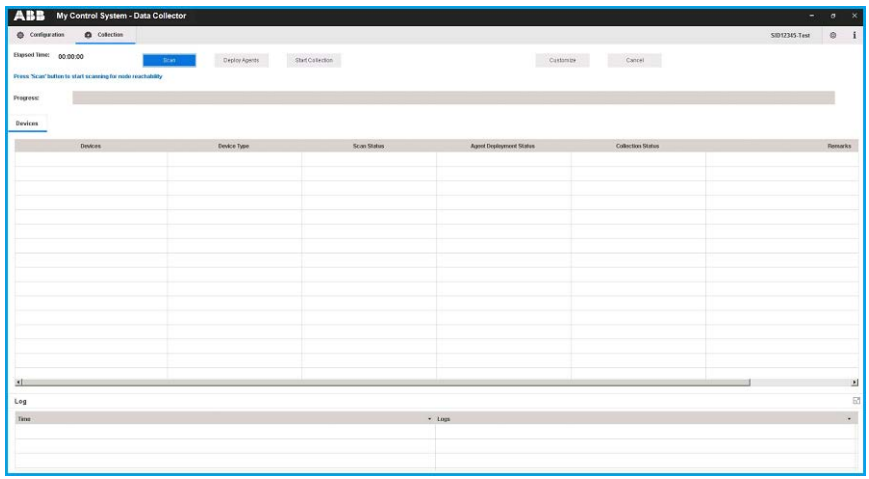

Figure 152. Data Collection Screen

16. 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.

17. Progress bar shows the progress of scanning.

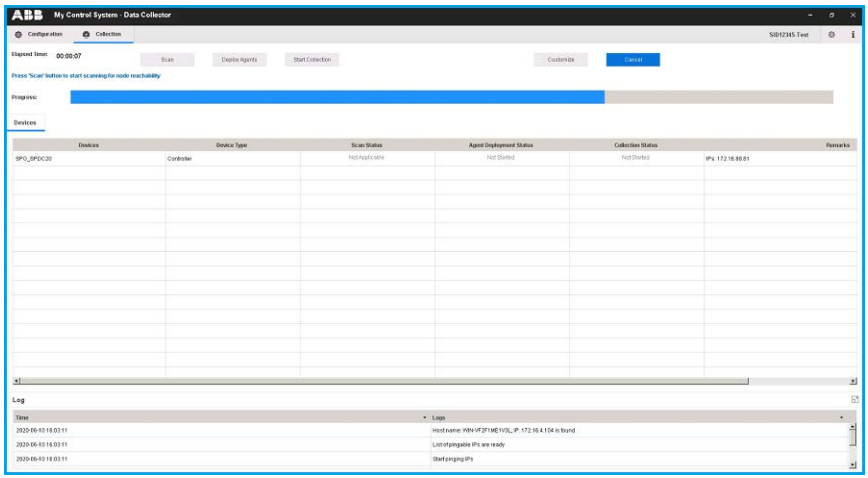

Figure 153. Scan Progress

18. 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 (for example AC 800M controller), then the status is “Not applicable” in Grey.
19. 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 rescan (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.

20. Once node scan is completed, Deploy Agents and Customize buttons will be enabled. User can customize the collection by choosing only few HMI/controller nodes from the list of accessible nodes, using customize option. Clicking on the **Customize** button opens customization window.

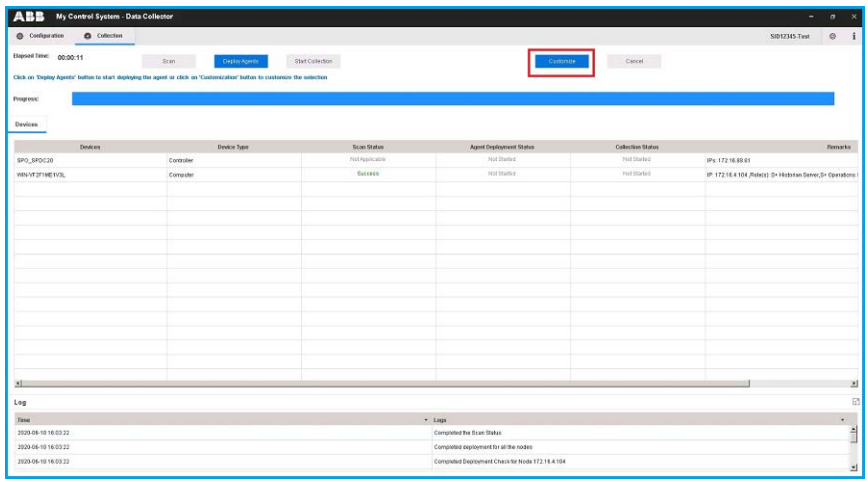

Figure 154. Scan Status

21. User has an option to customize the Data collection nodes for Performance and Lifecycle data collection, to Customize click on the **Customize** button. All accessible HMI and controller nodes are listed. All accessible HMI and controller nodes will be selected by default. User shall de-select the nodes that are not desired to be collected, by un-checking the respective check boxes, 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.

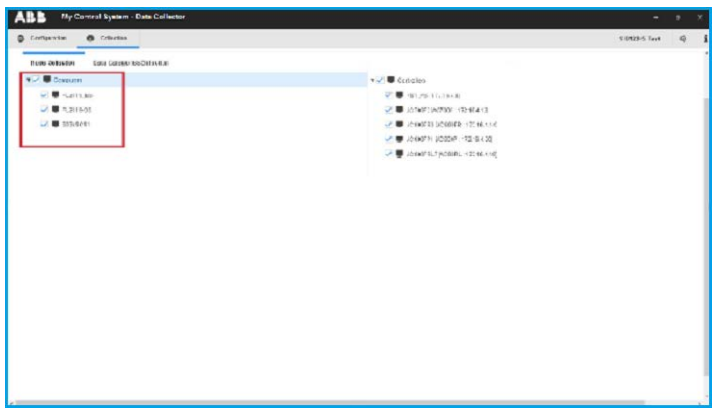

Figure 155. Node Selection

22. 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 de-select the data categories, that are not desired to be collected by un-checking the respective check boxes against the data category names. Click on **OK** button to save the customization configuration and close the customize window. Click on **Reset** button if you wish to reset the customization configuration. Data categories customization is applicable only for HMI nodes, it is not applicable for controllers.
23. 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.

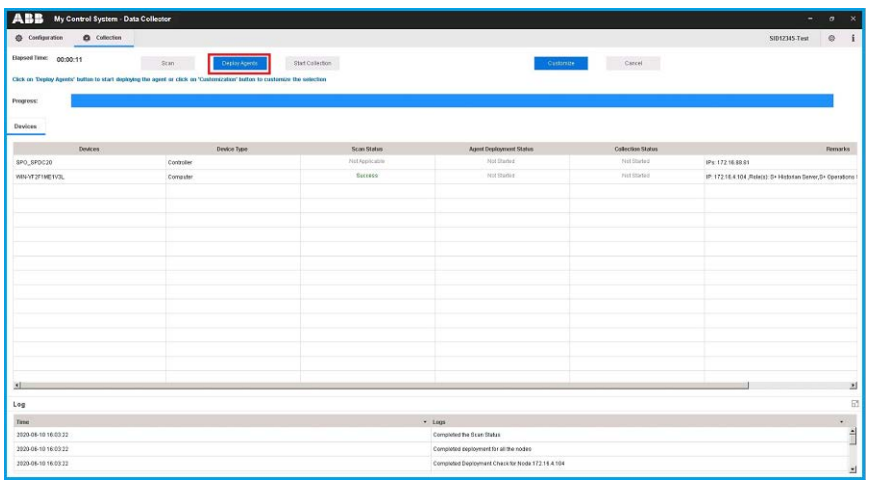

Figure 156. Start Collection

24. 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 get enabled. Click on the **Start Collection** button to start the data collection.

25. Data collection progress can be seen on the progress bar and on the Collection Status column.
26. 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 contains information about the hardware tree and the bottom part contains the collection statistics.
27. Collection file will be created automatically once the collection is completed. The collection file is created, and its file path appears on the screen. The collection file can be viewed by clicking on the file path.

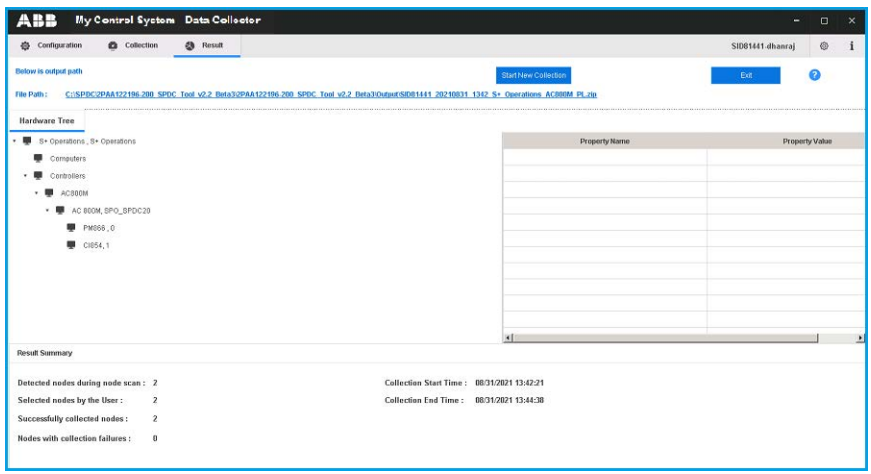

Figure 157. Collection File Path

28. Click on the **New collection** button to get back the Configuration screen and start with a new collection. Clicking on the **Exit** button to close the MCS-DC application.

3.4.6 Advanced mode data collection for S+ Operations with Procontrol P13

1. Copy the downloaded files of MCS-DC into the local disk (hard disk drive partition for Operating System) of a desired System S+ Operations node. Unzip the downloaded MCS-DC package. Depending on the HMI/Controller, MCS-DC launch nodes may vary. For S+ Operations with P13 Controllers, any S+ Operations node shall be used as launch node.
2. Double-click on the **MCS-DC_Launcher.exe**, to launch the tool. It is present inside the unzipped MCS-DC folder. The initial screen appears as shown in Figure. MCS-DC executes the below checks, on the launch node. If the checks are passed, a Green tick mark is shown, click the Launch button to proceed for data collection. If any check fails, a Red Cross mark is shown: “The issue must be resolved before launching MCS-DC again”.

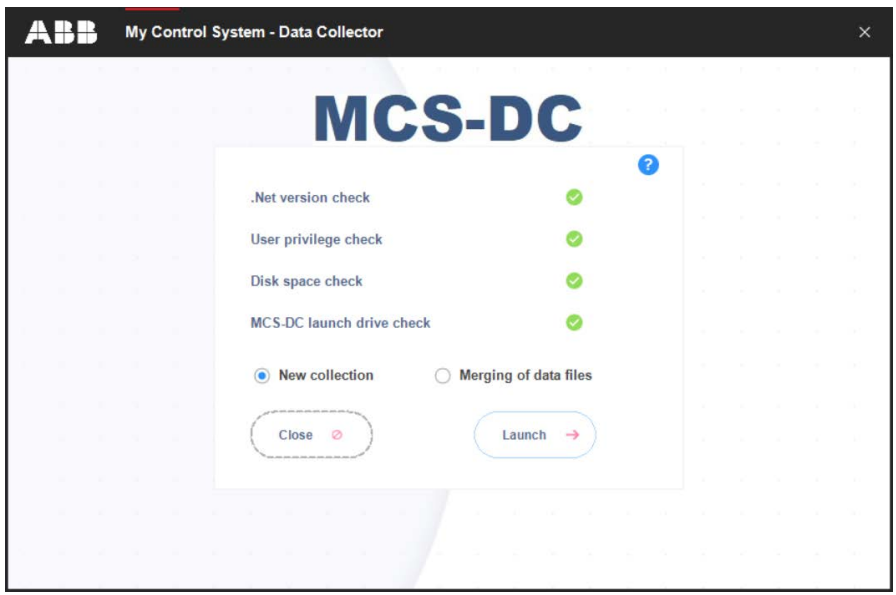

Figure 158. MCS-DC Launcher

- .NET Framework version check.

  If the .NET Framework version is 1.1 or above, then this check is passed and MCS-DC 2.X version can be launched for data collection.

  If the .NET Framework version is lower than 1.1, then this check is failed and MCS-DC 2.X version cannot be launched for data collection, instead MCS-DC 1.9.x version 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.

  a) User Privileges Check, checks if the MCS-DC is launched in the user account with administrator privileges.

  b) System drive launch check, MCS-DC must be launched only from the local disk drive of the launch node.

  c) Required Disk Space Check, Free disk space of at least 500MB must be available on the disk drive from which the MCS-DC is launched.

3. Provide the System ID of the S+ Operations HMI and your full name and provide password for encryption. This 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.

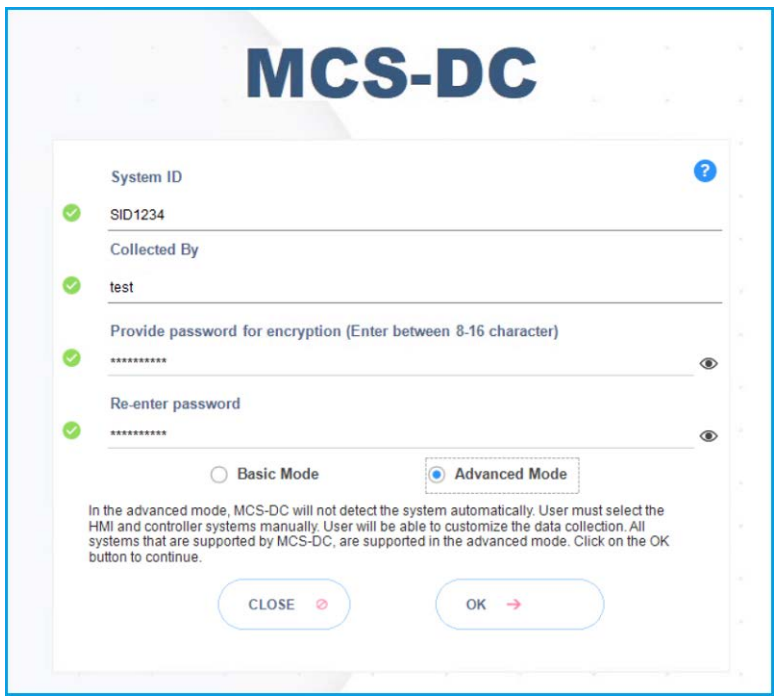

Figure 159. System credential For Advance Mode

4. Configuration screen appears. Click S+ Operations On the left pane and select the check box for the required data category (Performance, Life Cycle). Similarly, Select Harmony on the right pane and select the check box for the required data category (Performance, Life Cycle) and/or Security. Security option shall select only when it is needed as it will take significantly longer time for data collection. Click Continue. Figure 117

Default selection of HMI is 800xA. To change the selection, click on the name of the HMI. Selected HMI is highlighted in Blue.

If S+ Operations HMI is selected, along with it only one Controller category can be selected at a time for data collection.

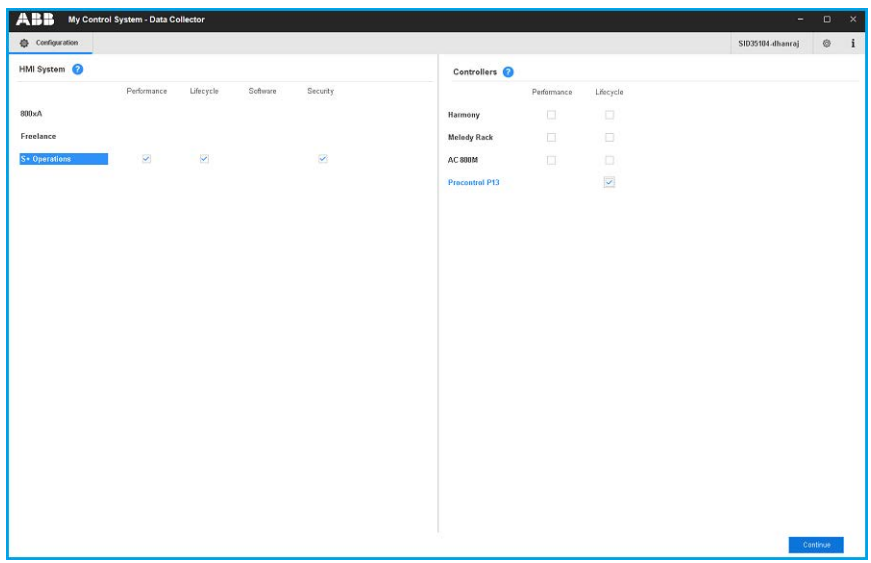

Figure 160. S+ Operations with P13

5. Input configuration screen appears.

6. Under S+ Operations HMI tab, IP range scan input: 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.

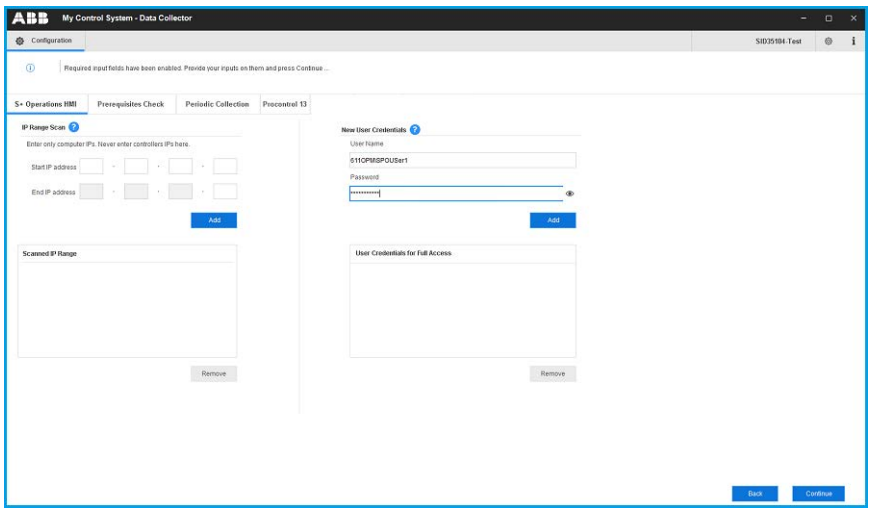

Figure 161. IP Range Scan

7. Provide the IP range and click on **Add** button. User can provide multiple ranges too.
8. 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.

9. Next input is user credential. Provide the **User Name** 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.
10. There is an option to remove the added credentials. To remove, select the added credential and click on the **Remove** button.
11. Click on **Procontrol P13** tab to provide input for Procontrol P13 controllers data collection. Click on **Browse** button to select the latest P13 source file (.CSV), taken from P13 engineering node.

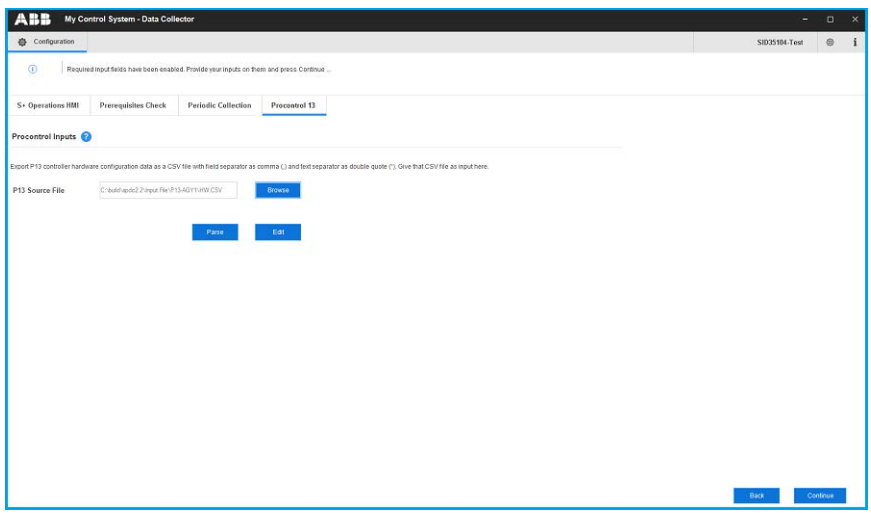

Figure 162. Procontrol P13 tab

12. 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 prerequisites by checking the check box 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 Section 2, Prerequisites.

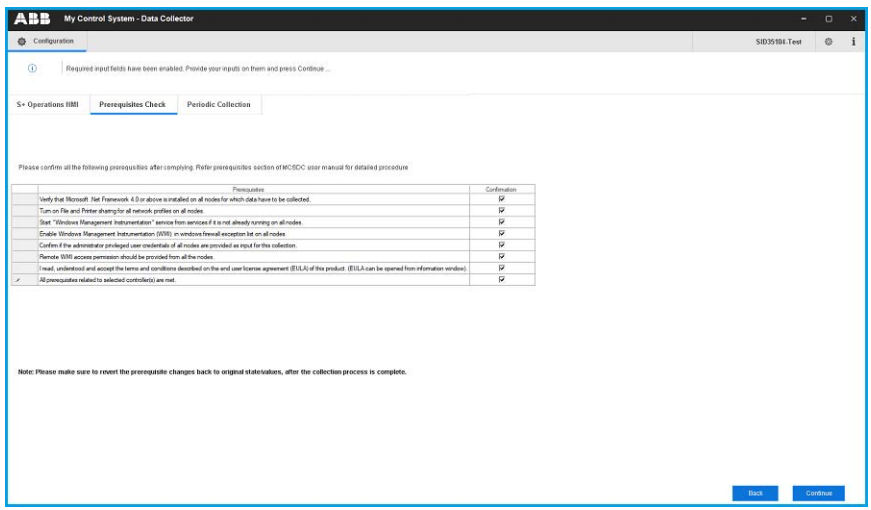

Figure 163. Prerequisite Check

13. Click on the **Continue** button to proceed to collection screen.

14. Collection screen appears. 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 to list 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.

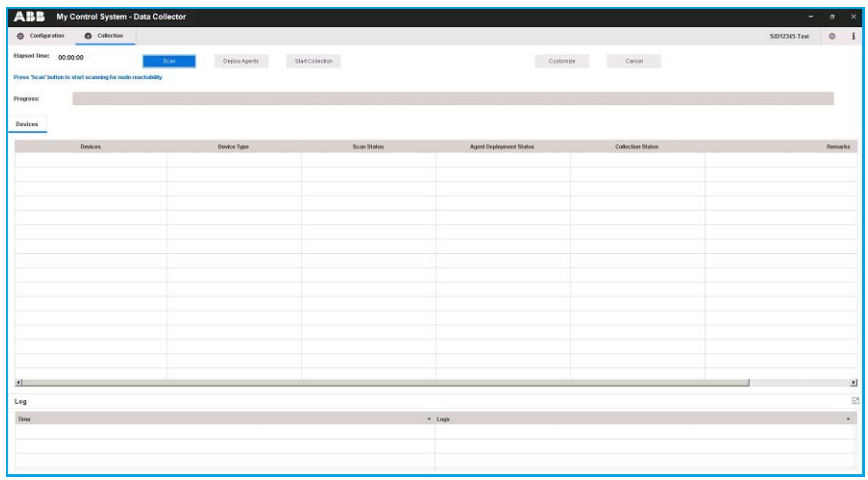

Figure 164. Data Collection Screen

15. 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.

16. Progress bar shows the progress of scanning.

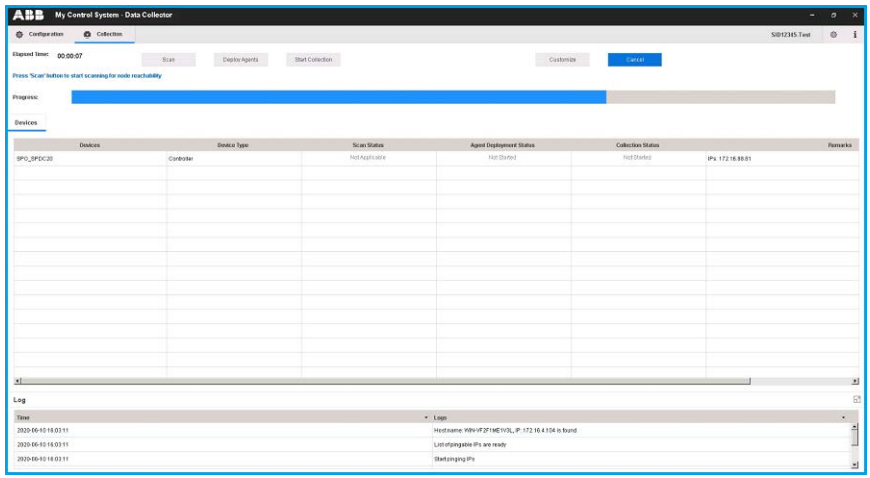

Figure 165. Scan Progress

17. 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 (for example AC 800M controller), then the status is “Not applicable” in Grey.
18. 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 rescan (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.

19. Once node scan is completed, Deploy Agents and Customize buttons will be enabled. User can customize the collection by choosing only few HMI/controller nodes from the list of accessible nodes, using customize option. Clicking on the **Customize** button opens customization window.

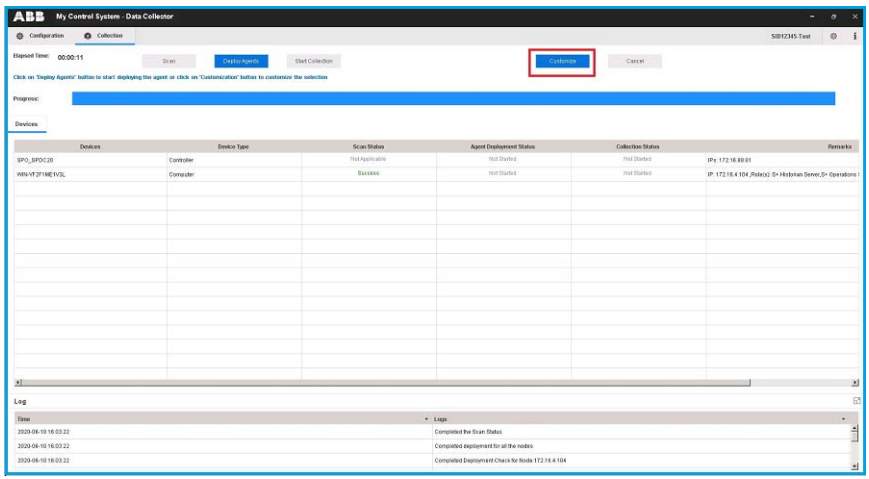

Figure 166. Scan Status

20. User has an option to customize the Data collection nodes for Performance and Lifecycle data collection, to Customize click on the **Customize** button. All accessible HMI and controller nodes are listed. All accessible HMI and controller nodes will be selected by default. User shall de-select the nodes that are not desired to be collected, by un-checking the respective check boxes, 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.

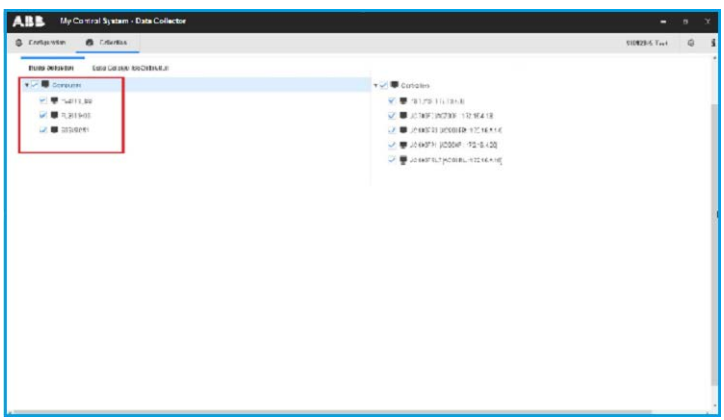

Figure 167. Node Selection

21. 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 de-select the data categories, that are not desired to be collected by un-checking the respective check boxes against the data category names. Click on **OK** button to save the customization configuration and close the customize window. Click on **Reset** button if you wish to reset the customization configuration. Data categories customization is applicable only for HMI nodes, it is not applicable for controllers.

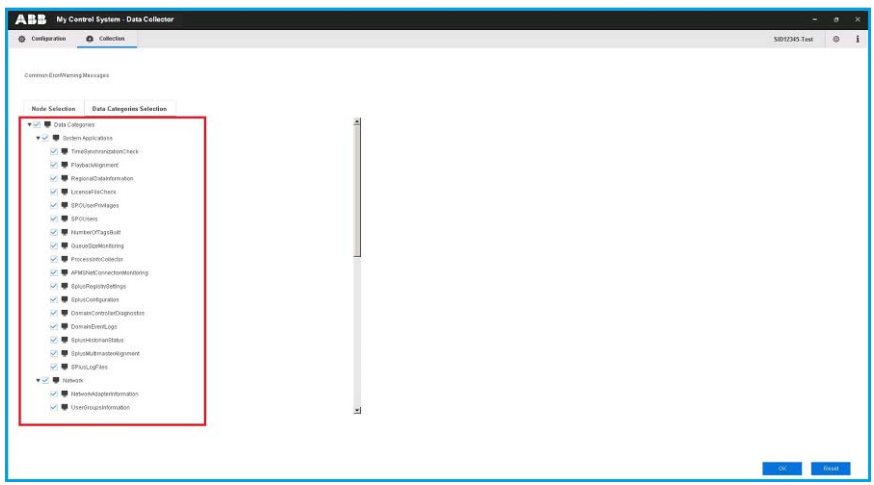

Figure 168. Data Category Selection

22. 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.

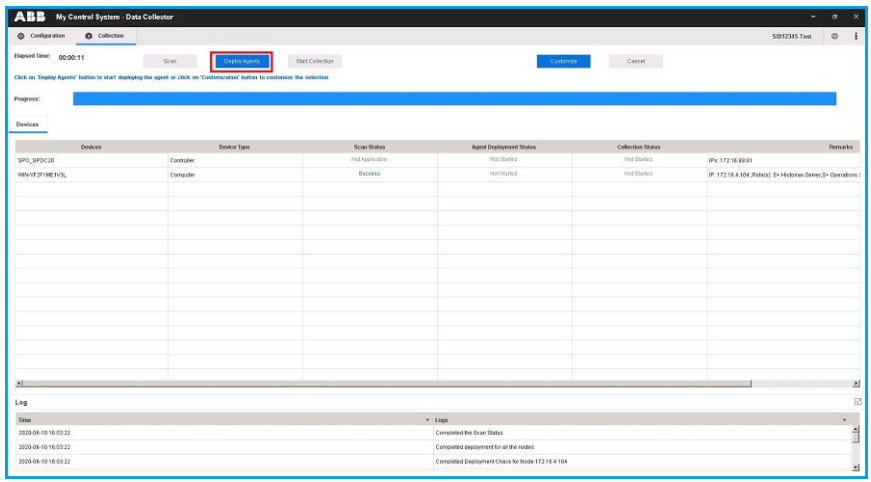

Figure 169. Start Collection

23. 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 get enabled. Click on the **Start Collection** button to start the data collection.
24. Data collection progress can be seen on the progress bar and on the Collection Status column.
25. 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 contains information about the hardware tree and the bottom part contains the collection statistics.

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

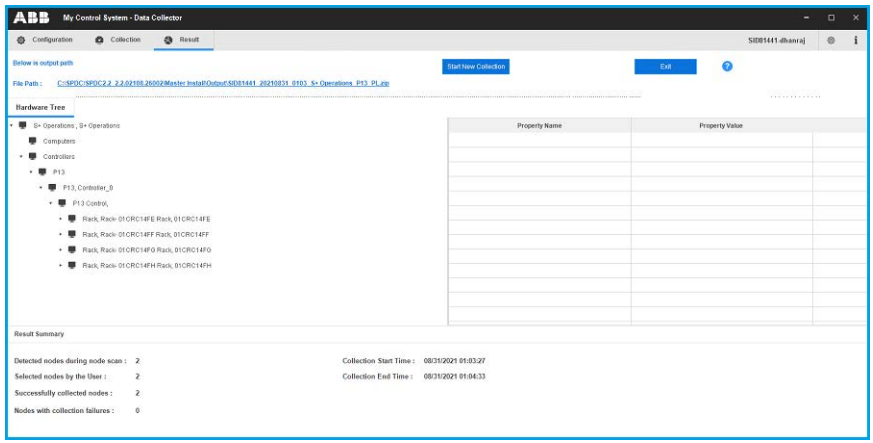

Figure 170. Collection File Path

27. Click on the **New collection** button to get back the Configuration screen and start with a new collection. Clicking on the **Exit** button to close the MCS-DC application.
28. Click on **Hardware tree** tab to view the hardware tree structure.

3.4.7 Security Data Collection from 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. Copy the downloaded files of MCS-DC into the local disk (hard disk drive partition for Operating System) of a desired System node in the control system. Unzip the downloaded MCS-DC package.
2. Double-click on the **MCS-DC_Launcher.exe,** to launch the tool. It is present inside the unzipped MCS-DC folder. The initial screen appears as shown in Figure. MCS-DC executes the below checks, on the launch node. If the checks are passed, a Green tick mark is shown, click the Launch button to

proceed for data collection. If any check fails, a Red Cross mark is shown: “The issue must be resolved before launching MCS-DC again”.

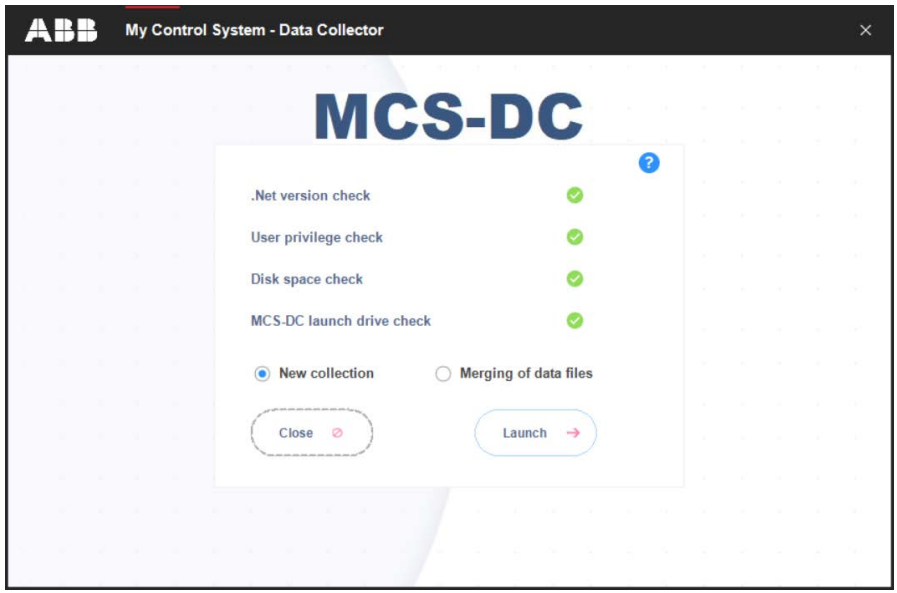

Figure 171. MCS-DC Launcher

- .NET Framework version check.

  If the .NET Framework version is 1.1 or above, then this check is passed. However, for Non-ABB system security data collection, minimum .Net framework version required is 3.5 SP1. Ensure that this prerequisite is met, before proceeding with data collection.

  If the .NET Framework version is lower than 1.1, then this check is failed and MCS-DC 2.X version cannot be launched for data collection, instead MCS-DC 1.9.x version will be launched. However, MCS-DC1.9 does not support Non-ABB system data collection.

- Other Prerequisites check.

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

a. User Privileges Check, checks if the MCS-DC is launched in the user account with administrator privileges.

b. System drive launch check, MCS-DC must be launched only from the local disk drive of the launch node.

c. Required Disk Space Check, Free disk space of at least 500MB must be available on the disk drive from which the MCS-DC is launched.

3. Provide System ID, user's full name and password for encryption. System ID should be in the format SID<number> (e.g. SID123). 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.

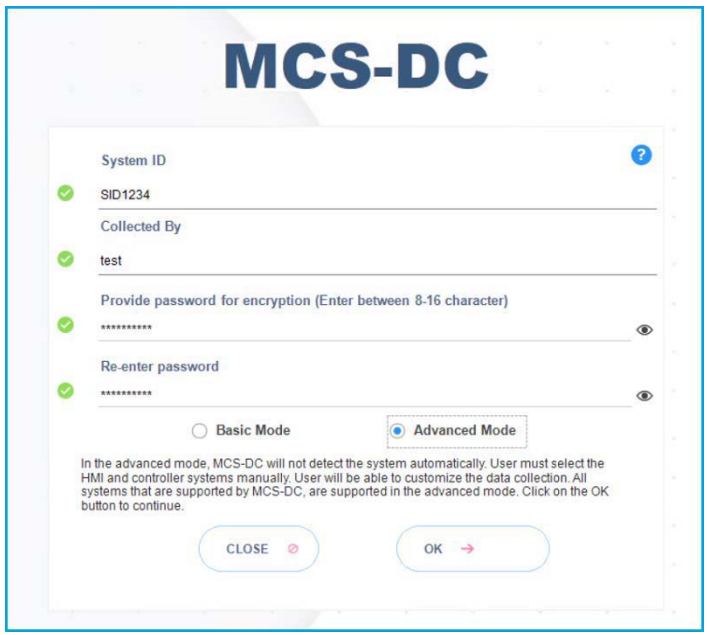

Figure 172. System credential For Advance Mode

4. Configuration screen appears. Click Non-ABB System on the left pane and select the check box Security. Click Continue.

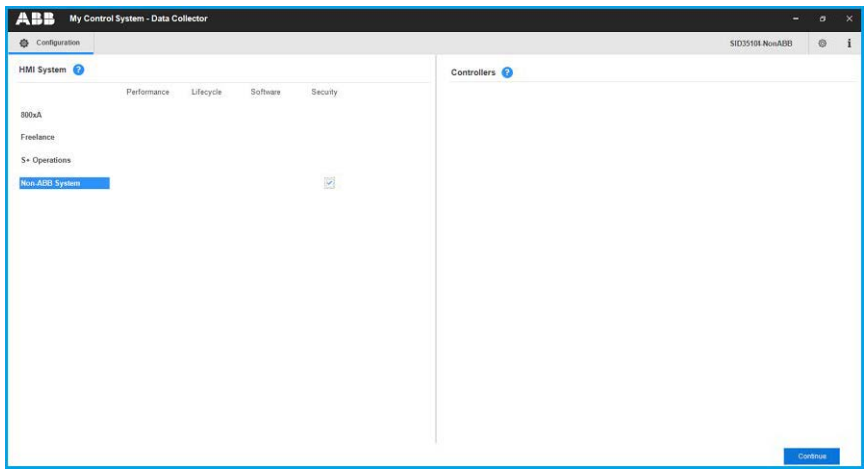

Figure 173. Non-ABB System

5. Input configuration screen appears.
6. 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.
7. 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.
8. Next input is user credential. Provide the **User Name** 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\user name.

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

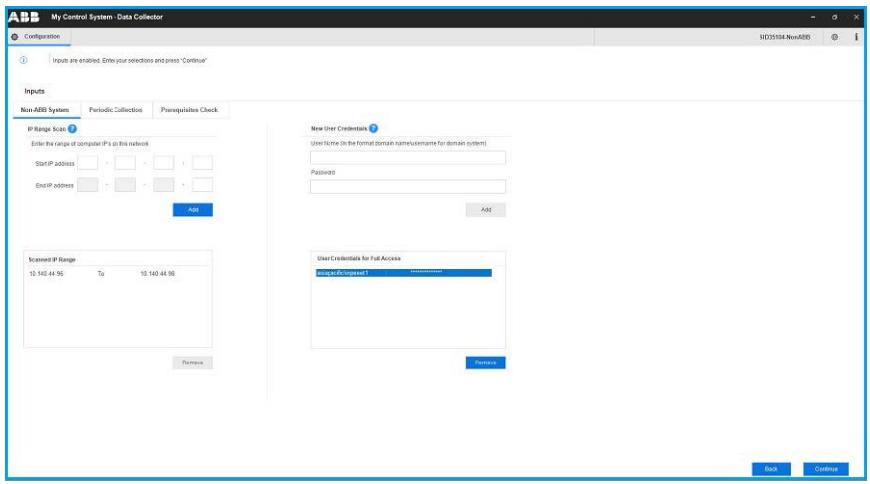

Figure 174. IP range and user credentials

10. Once all 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 prerequisites by checking the check box 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 Section 2, Prerequisites.

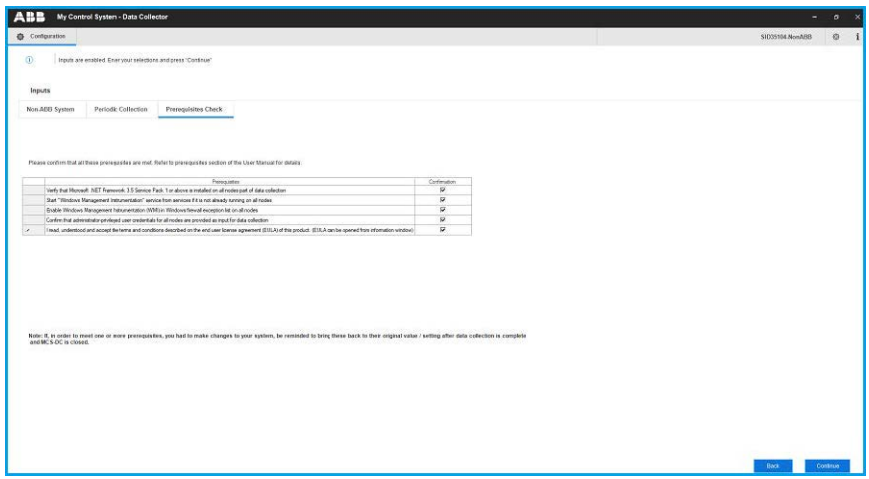

Figure 175. Prerequisites check

11. Click on the **Continue** button to proceed to collection screen.
12. Collection screen appears. 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 to list 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.

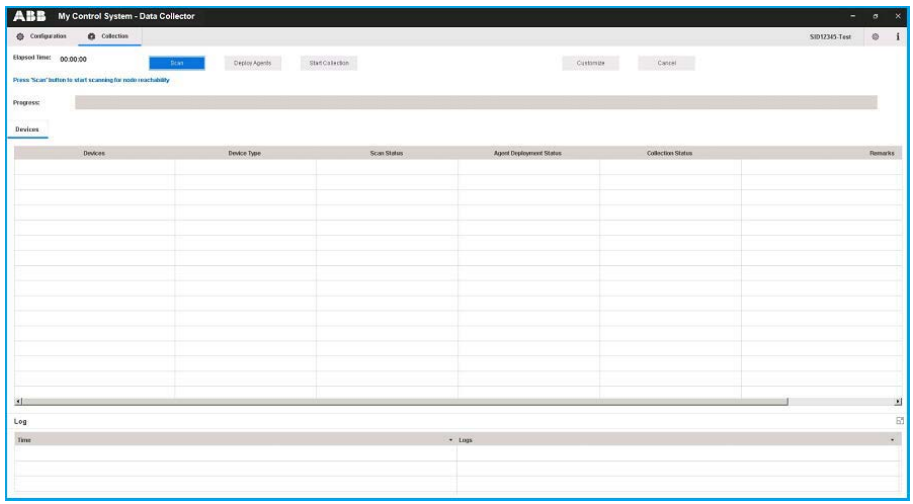

Figure 176. Data Collection Screen

13. 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.

14. Progress bar shows the progress of scanning.

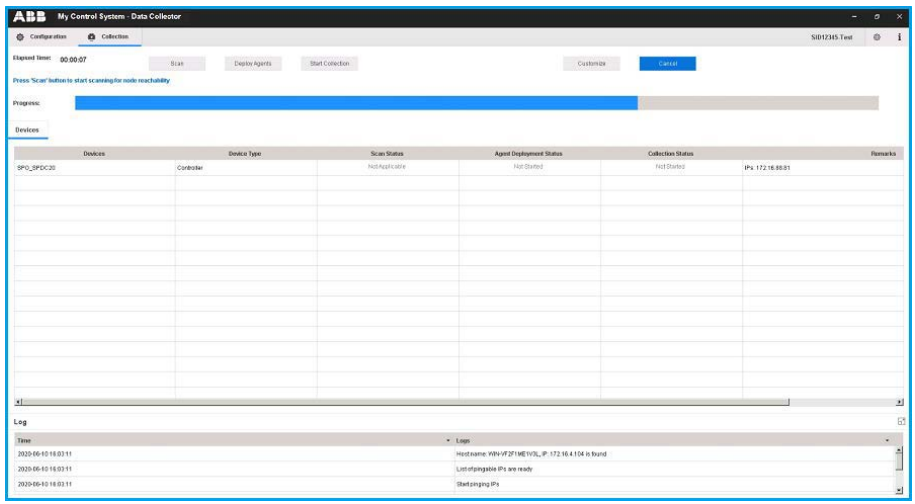

Figure 177. Scan Progress

15. 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 (for example AC 800M controller), then the status is “Not applicable” in Grey.
16. 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 rescan (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.
17. Once node scan is completed, Deploy Agents and Customize buttons will be enabled. User can customize the collection by choosing only few

HMI/controller nodes from the list of accessible nodes, using customize option. Clicking on the **Customize** button opens customization window.

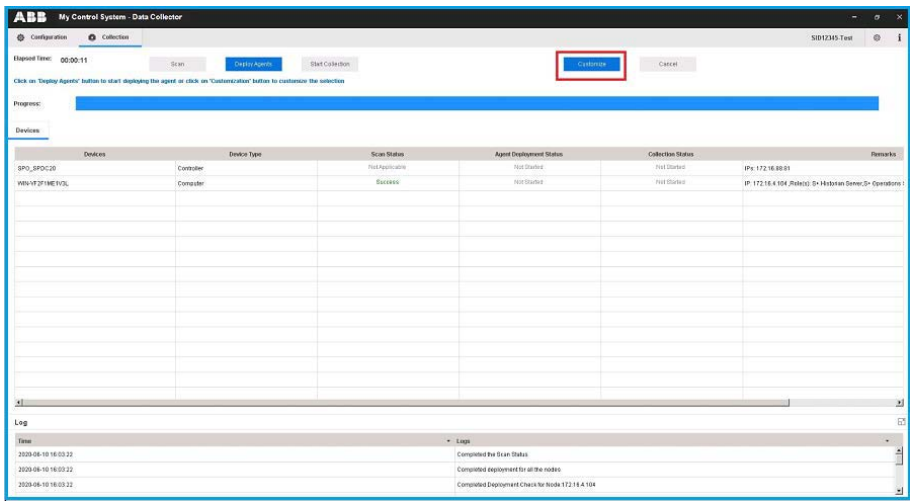

Figure 178. Scan Status

18. User has an option to customize the Data collection nodes for Performance and Lifecycle data collection, to Customize click on the **Customize** button. All accessible HMI and controller nodes are listed. All accessible HMI and controller nodes will be selected by default. User shall de-select the nodes that are not desired to be collected, by un-checking the respective check boxes, 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.

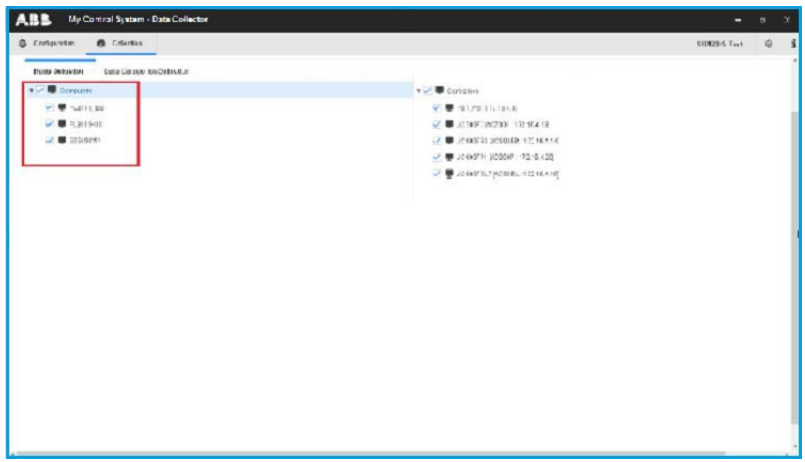

Figure 179. Node Selection

19. 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.

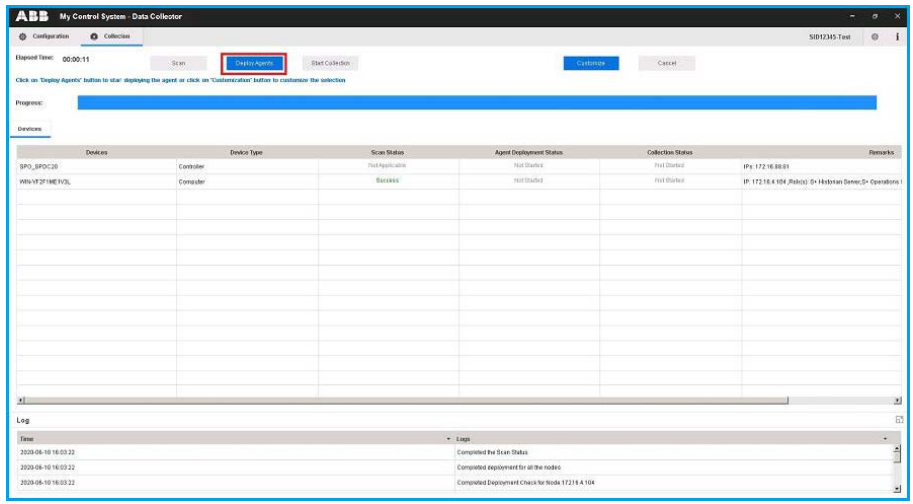

Figure 180. Start Collection

20. 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 get enabled. Click on the **Start Collection** button to start the data collection.
21. Data collection progress can be seen on the progress bar and on the Collection Status column.
22. 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 contains information about the hardware tree and the bottom part contains the collection statistics.

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

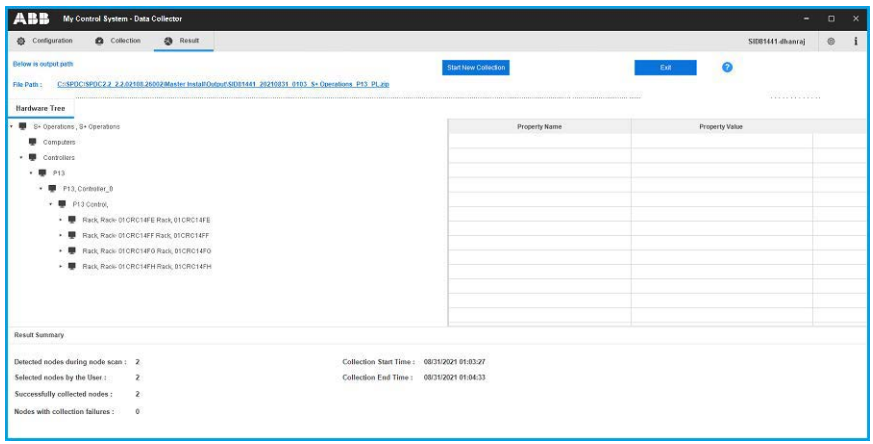

Figure 181. Collection File Path

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

3.4.8 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 4.1, Post Collection 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 3.4.1, Data Collection Process. If it is non-ABB Windows based control system, follow the Section 3.4.7, Data Collection Process).
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 3.4.3, Data Collection Process. Note that no controllers must be selected during this collection.

3. Follow the procedure mentioned in Section 4.1, Post Collection Procedure to merge the data files generated in step 1 and step 2.

3.5 Periodic Data Collection

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

After data collection inputs have been entered, click on Periodic Collection tab, as shown in the picture below:

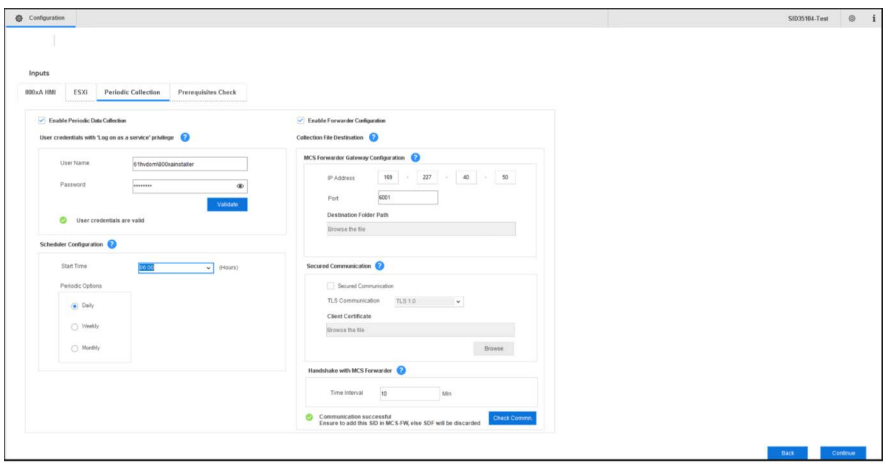

Figure 182. Scheduler Configuration

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:

a. The user account should have local administrator and log on as a service rights on this computer (MCS-DC launch computer). '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.

b. If the user is a domain user, enter the user name in the format **domain name\username**. If the system in work group, provide the credentials as **.\username**.

c. If the system is 800xA, make sure that the user is part of Industrial IT user group. Besides, in the Aspect server also, the user shall be added as log on as service and the user should have local admin rights in the aspect server.

Click on Validate button, to validate the credentials.

- **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.

- **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).

MCS Forwarder version must be 1.3 or newer. 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 frameworks 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 screen shot.

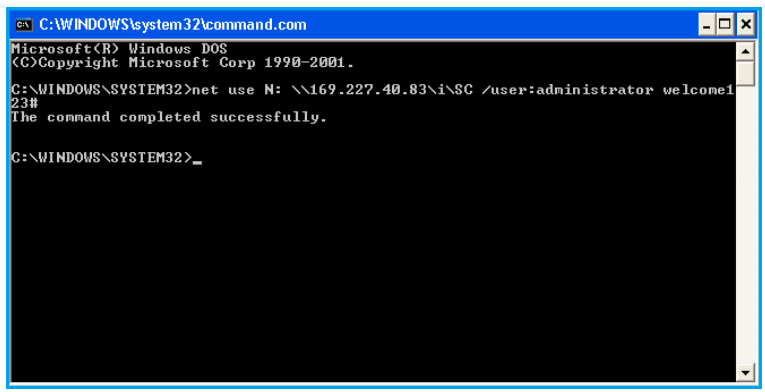

Figure 183. Map Network drive

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.

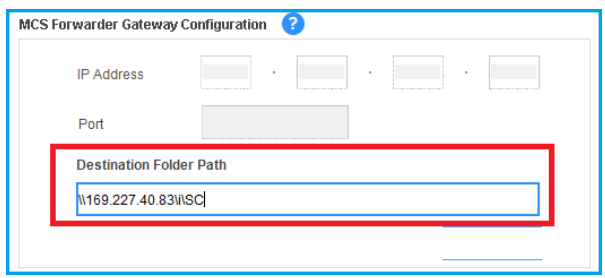

Figure 184. Complete UNC path of the remote folder

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.

- **Secured Communication:** Enable secured communication if applicable. Refer appendix B for more details on secured communication configuration.
- **Handshake with MCS Forwarder:** 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.
- **Check Communication Button:** This is to verify the communication status between MCS-DC and MCS-FW.

After configuring the scheduler parameters, Click next to go to scan page. See fig below.

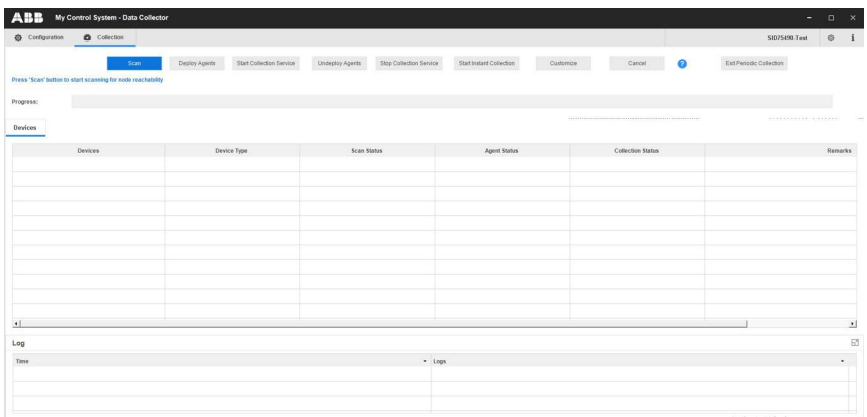

Figure 185. Node Scan

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

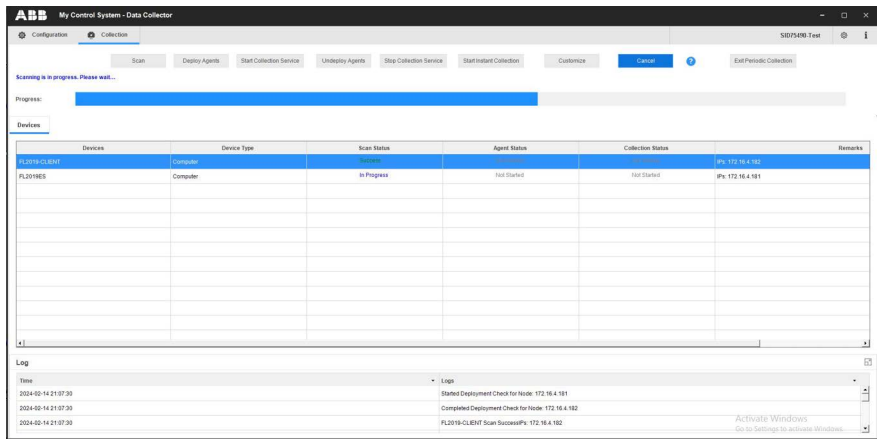

Figure 186. Node scan in progress

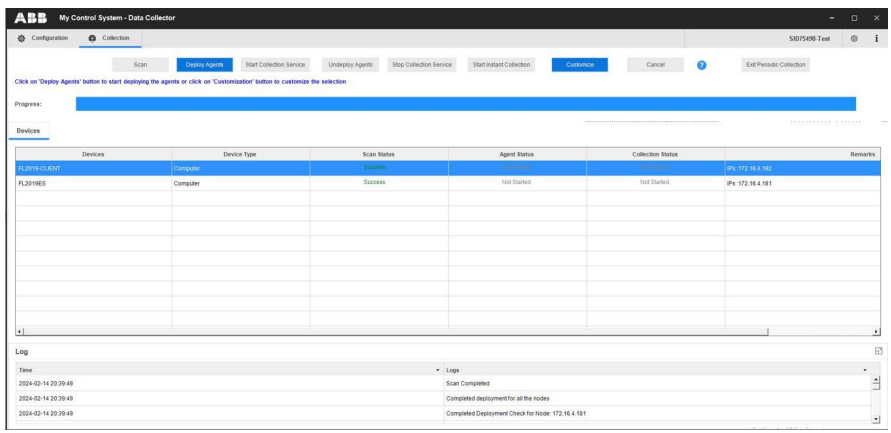

Figure 187. Deploy Agents

5. Click Deploy Agent button to deploy data collection agents to all the nodes. Refer Section 5, Troubleshooting if agent deployment fails.

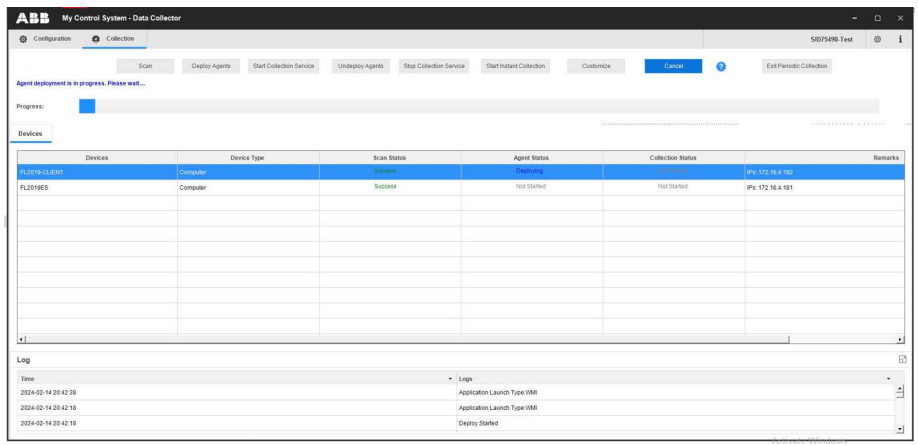

Figure 188. Agent deployment status

Start Collection Service: After deploying the data collection agents, Start Collection Service button enables. See Figure 189.

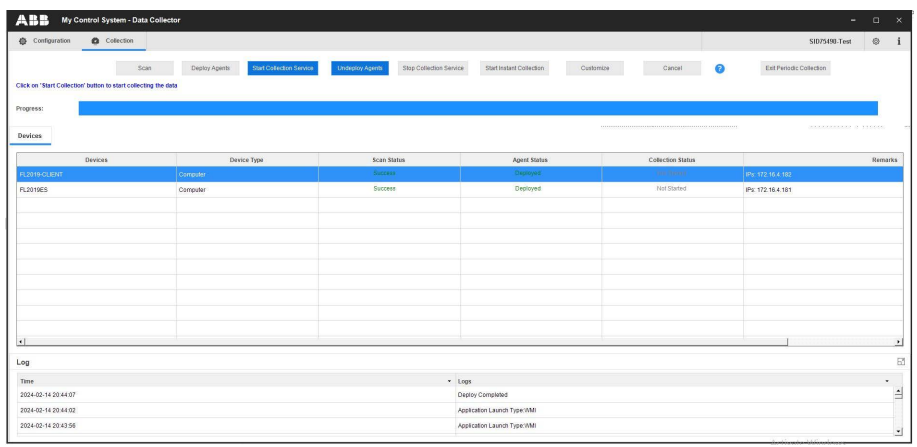

Figure 189. Start collection service

a. Provide the periodic data collector user credentials and click OK.

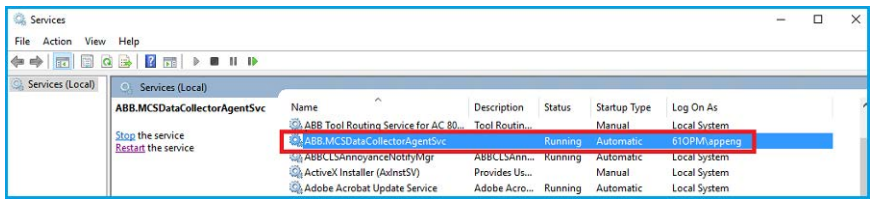

Figure 190. Log on as service

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

Click start collection service button to start the collection service.

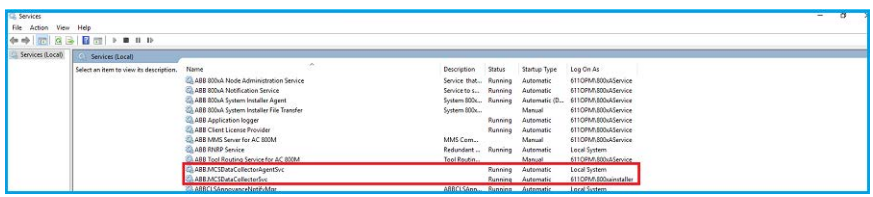

Figure 191. Agent Service

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: This 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.MCSDataCollectorsvc) will be stopped and therefor the collection.

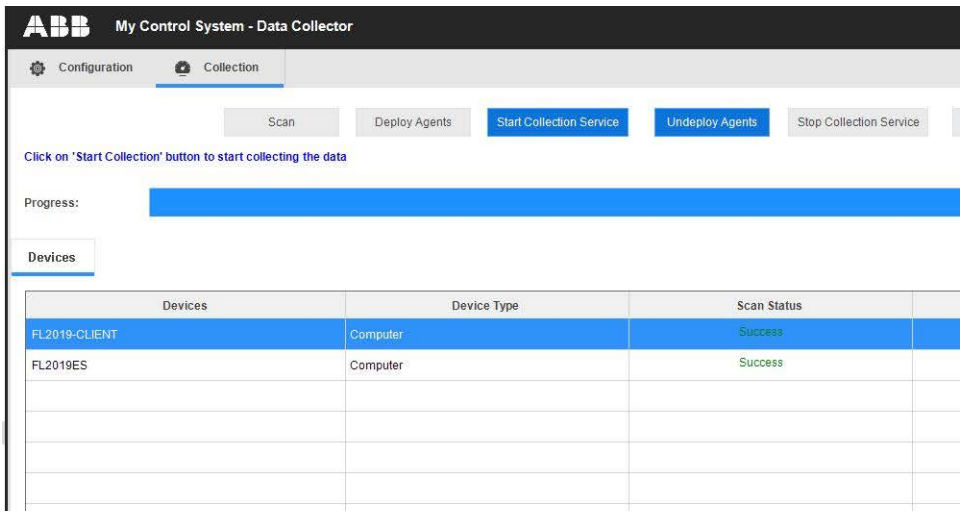

Figure 192. Stop collection service

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

Undeploy Agents: If any configuration changes need to be made in periodic collection, agents are to be **Undeployed** from all the nodes. The undeploy 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.Before exiting the tool, agents are to be undeployed.

After the agents are removed, user can reconfigure the periodic collection without closing the data collector.

Exit Periodic Collection: To exit from periodic collection, click on **Exit Periodic Collection** button. This button will be enabled after undeploying 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.

Start/Stop Instant Collection: Using this 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.

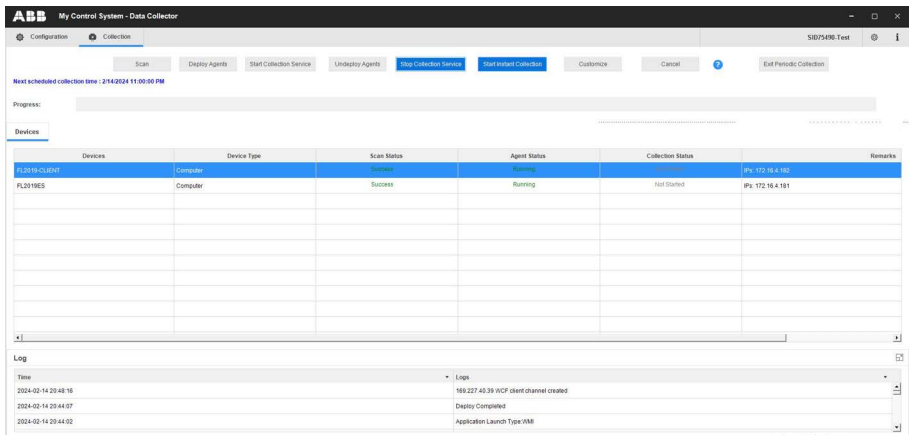

Figure 193. Start Instant Collection

3.6 ESXi Data Collection

In this chapter there is a detailed explanation about how to collect ESXi host server health data with MCS-DC. ESXi 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 life cycle must be selected to enable ESXi data collection.

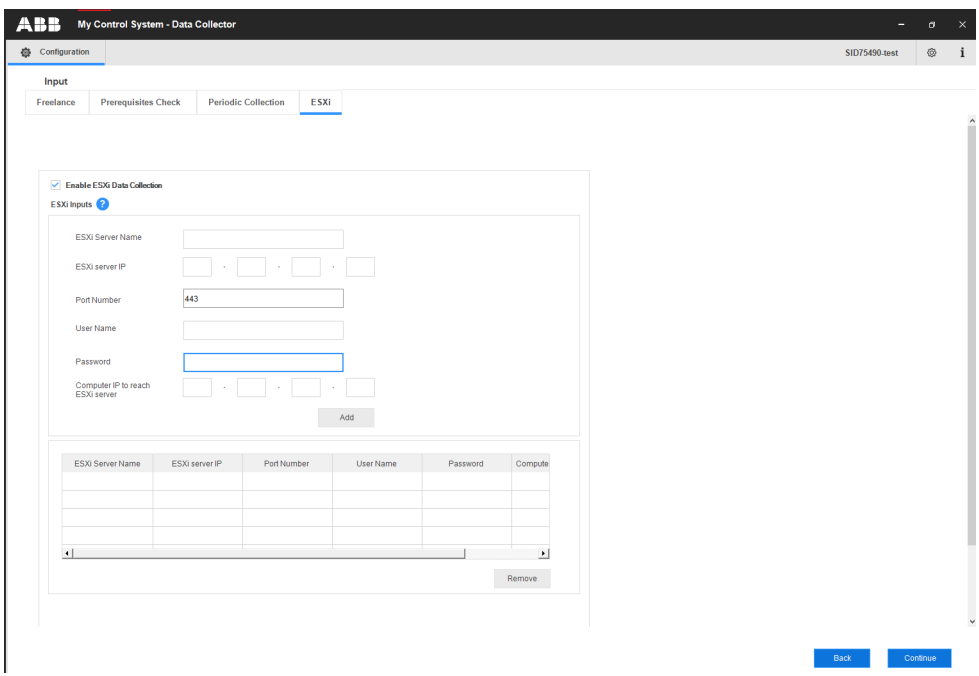

Figure 194. ESXi Data Collection - Input Configuration

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.

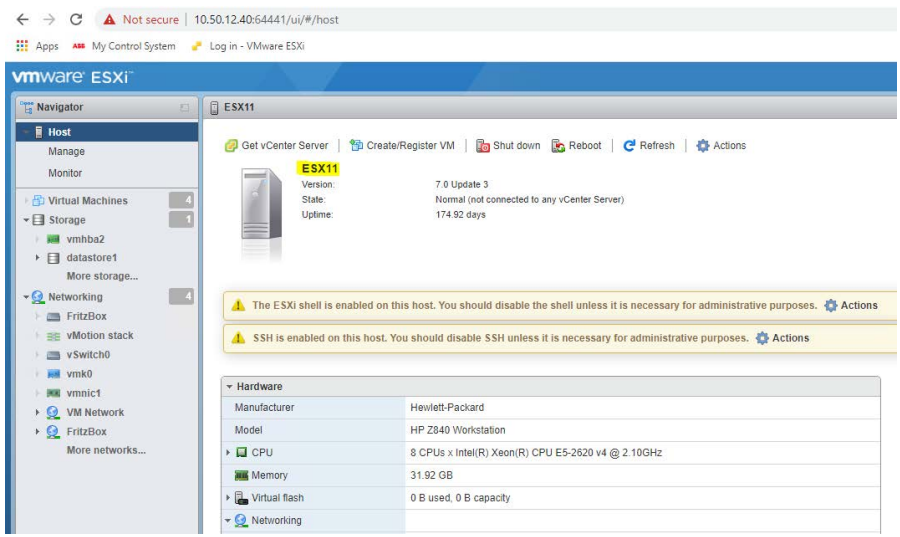

Figure 195. ESXi Server Name

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.

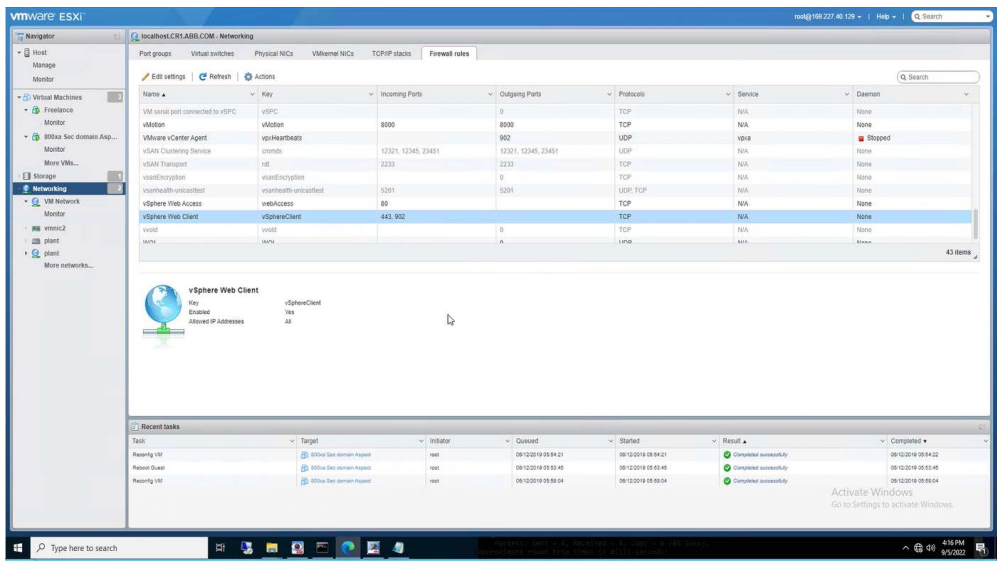

Figure 196. ESXi Access - Incoming Port

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 Post Collection Procedure

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 191
- ControllerSystemNames: Refer Figure 191
- DataCat:
  - L- Life cycle
  - 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.

4.1 Collection file merging

For certain system families, it is not possible to collect data in single step. For example, 800xA with Harmony controller system (Refer to Section 3.4.1, Data Collection Process). 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 3.4.8, Data Collection Process 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.

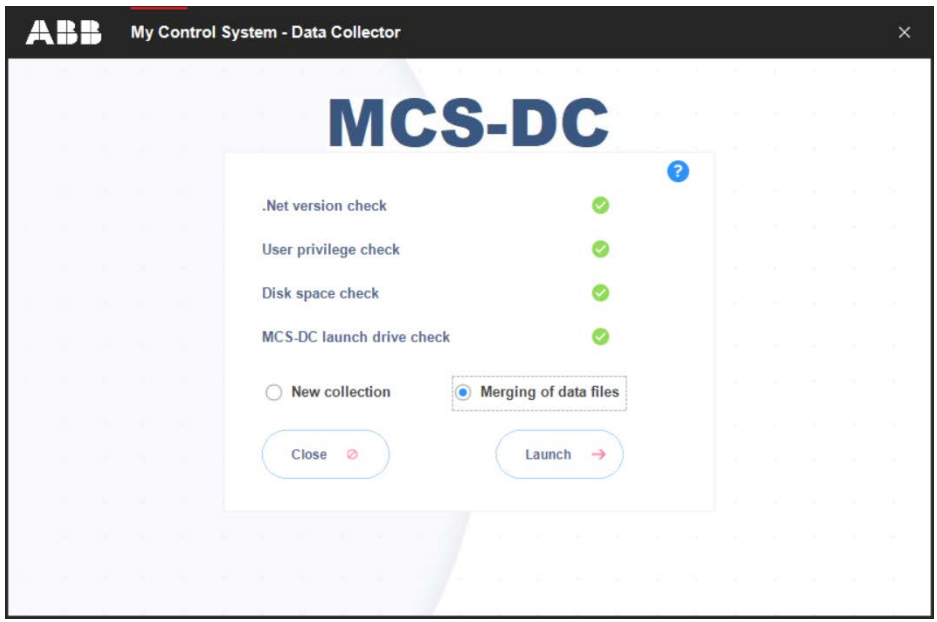

Figure 197. Merging of Data Files

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.

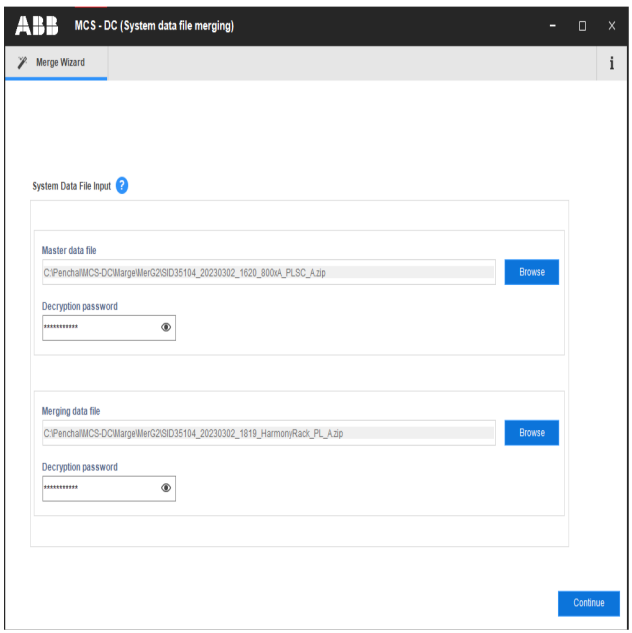

Figure 198. System Data File input

3. Select the systems\nodes to be merged from both the System data files. Ensure the following:
   a. Minimum version of .Net framework installed in the PC where MCS-DC is executed must be 4.7.2.
   b. Both system data files must belong to the same System ID.
   c. Both system data files must have been collected with the same MCS-DC version.
   d. The time gap between these two data collections must not exceed 90 days.
   e. Minimum one system must be selected from each system data file for merging.
   f. Same data file cannot be used twice as input files for merging.

g. Do not select more than one HMI system (800xA, Freelance or S+ operations).

h. 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 an 800xA system 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 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 2.3 or earlier versions, shall not be used for merging.

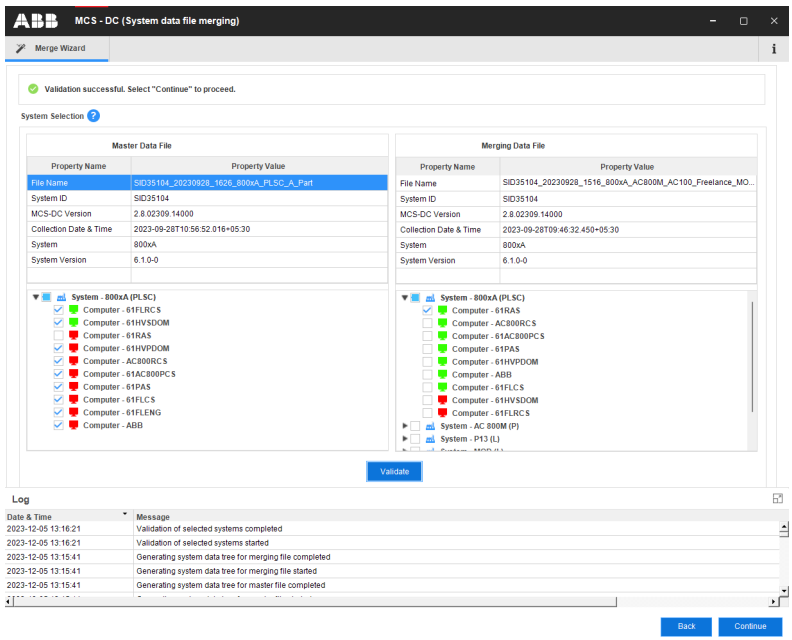

Figure 199. Validation

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.

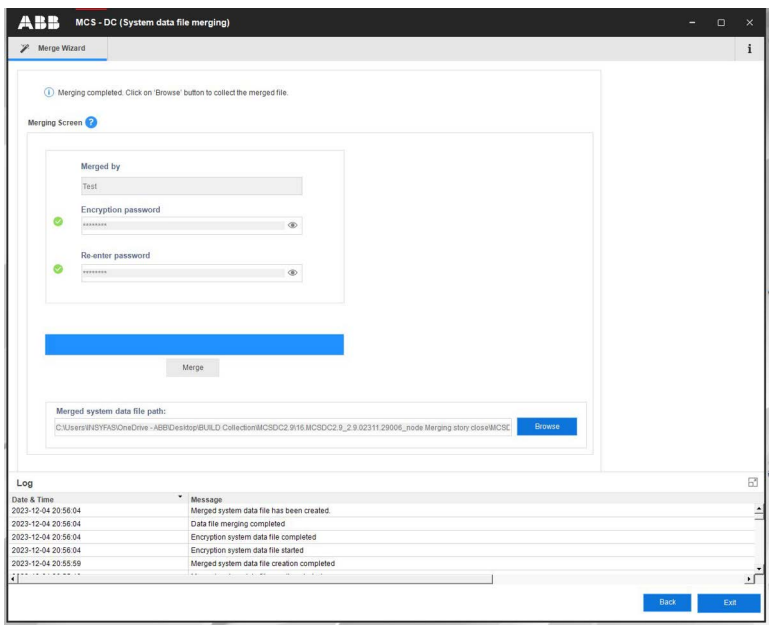

Figure 200. Merging Screen

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.

4.2 Limitations in data file merging.

Following are the restrictions in data file merging.

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

4.3 Report Generation from MyABB and uploading data file to ServIS.

Collection file must be uploaded to myABB / My Conrtol System to generate reports. To upload the collected data to ServIS, use SCX IBM version 1.20 or higher. Note that the upload of data to ServIS is restricted to specific ABB employees.

5 Troubleshooting

5.1 Issue 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.

5.2 Issue 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 privileges and run the command below -
sc delete ABB.MCSDataCollectorAgentSvc

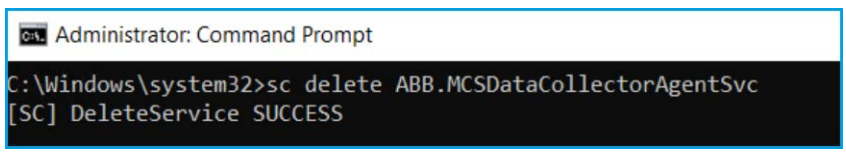

Figure 201. Delete service

5.3 Issue 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.

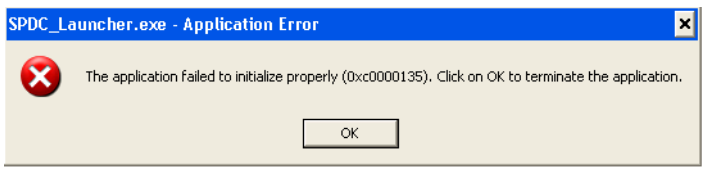

Figure 202. Error Message

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

5.4 Issue 4: Windows Firewall Settings for WMI

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 able to access the remote node and collect the data.

In case of WMI access denied error or failed to connect remote nodes error, check whether WMI traffic is blocked by the firewall. If the traffic is blocked, WMI needs to be enabled in the firewall. In this section there is an explanation of how to check, enable and disable WMI traffic in the Firewall.

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**.

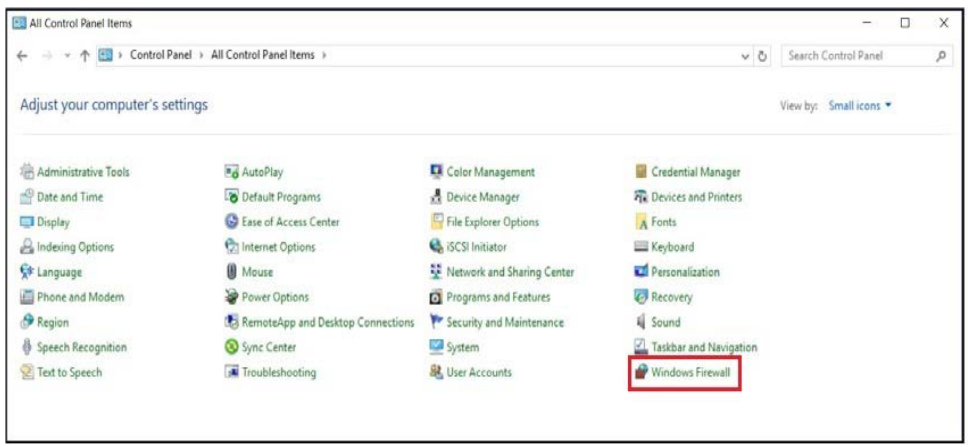

Figure 203. Control Panel

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

Figure 204. Advanced Settings

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.

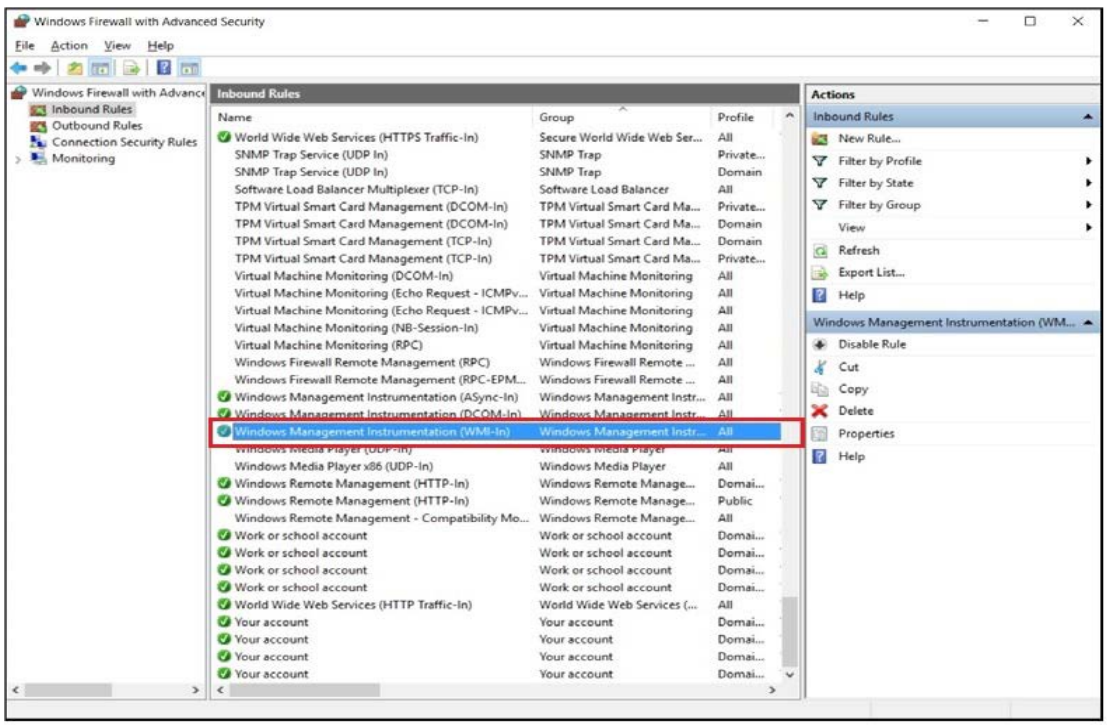

Figure 205. Windows Firewall with Advanced Security Screen

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**.

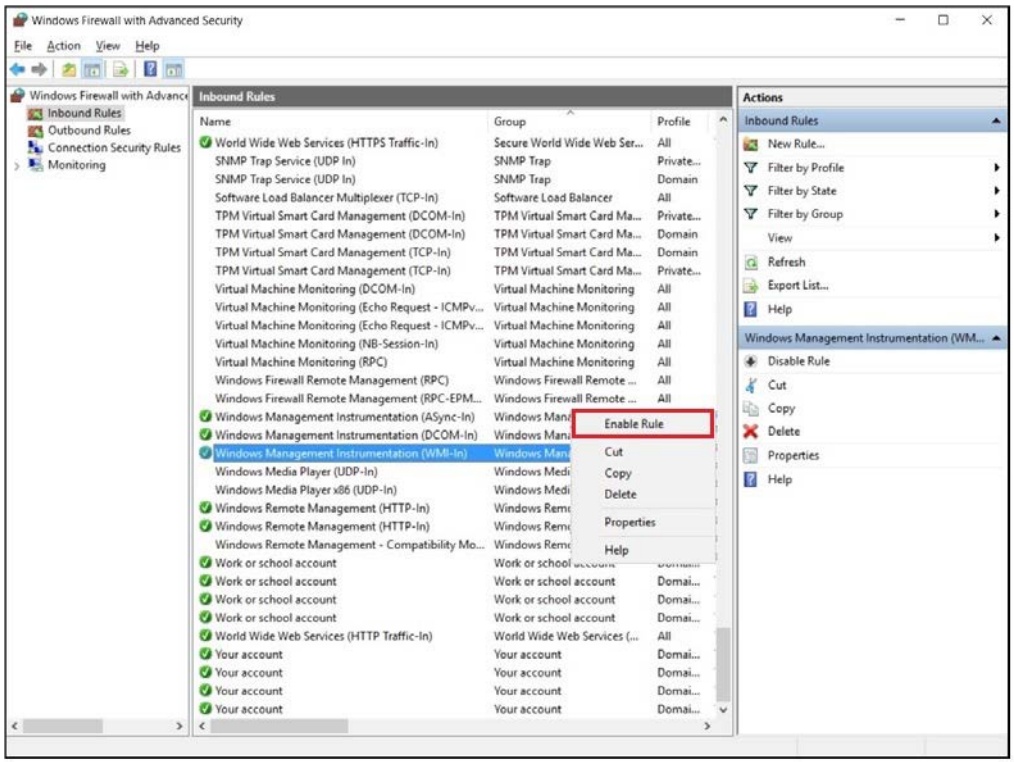

Figure 206. Enable Rule

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

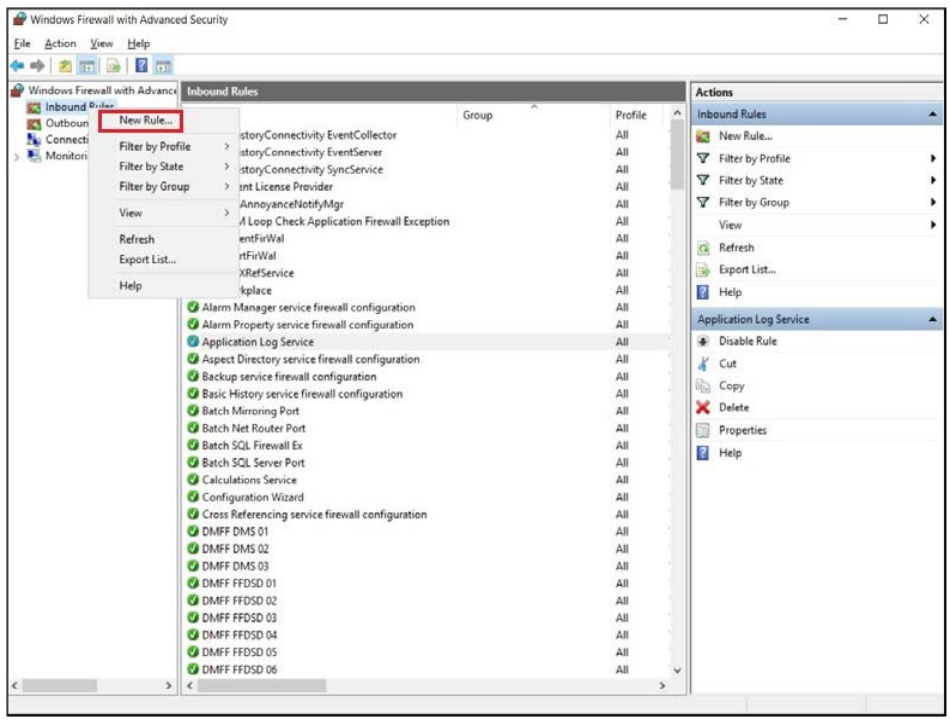

Figure 207. New Rule

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**.

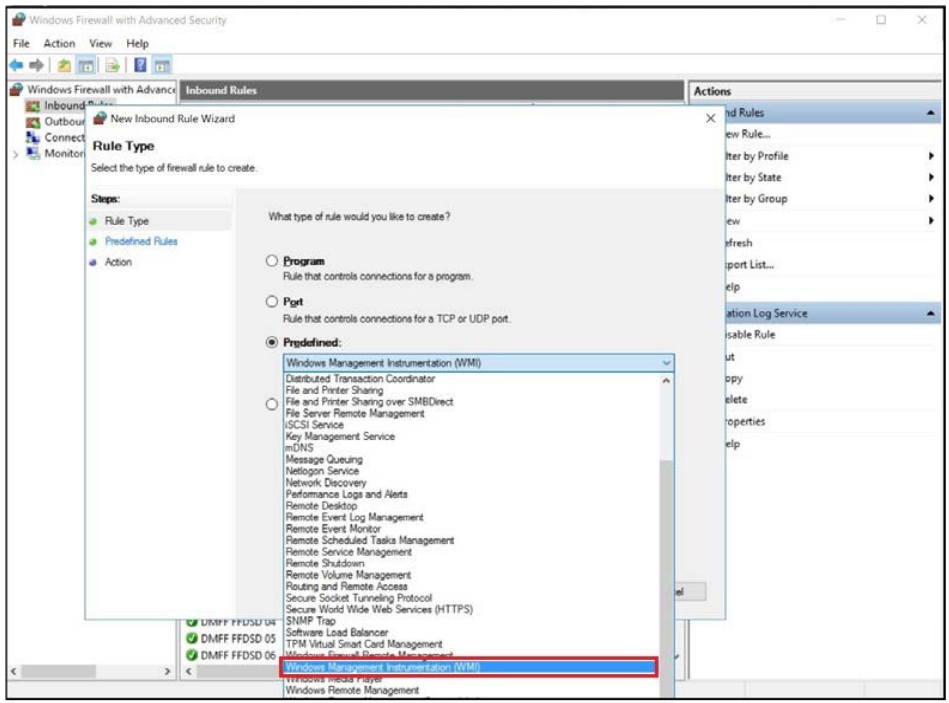

Figure 208. Predefined Option

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

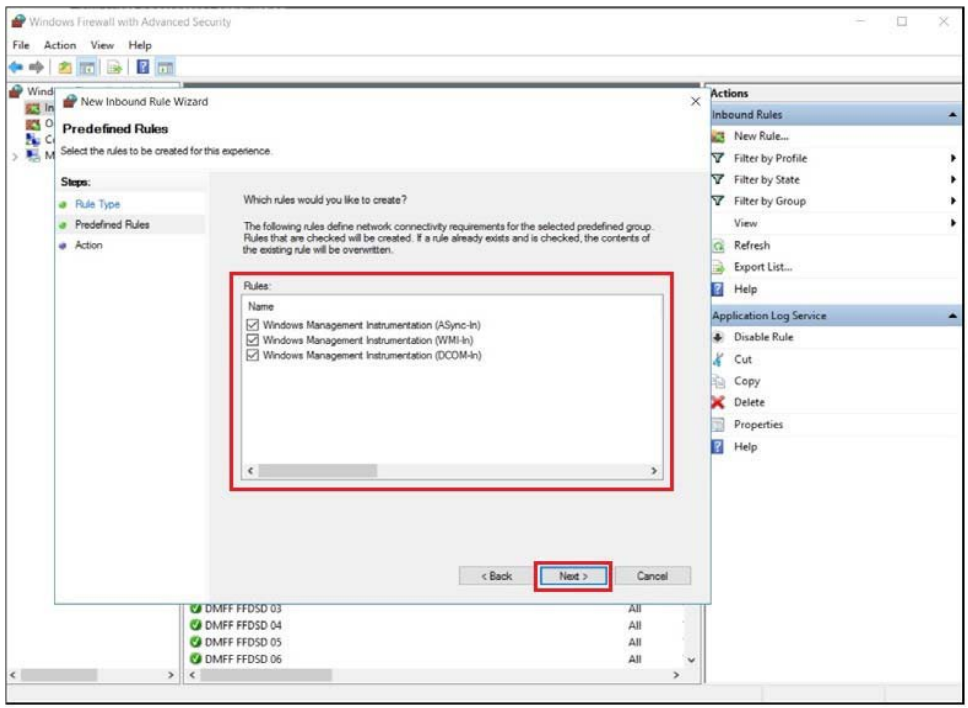

Figure 209. Select All Rules

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

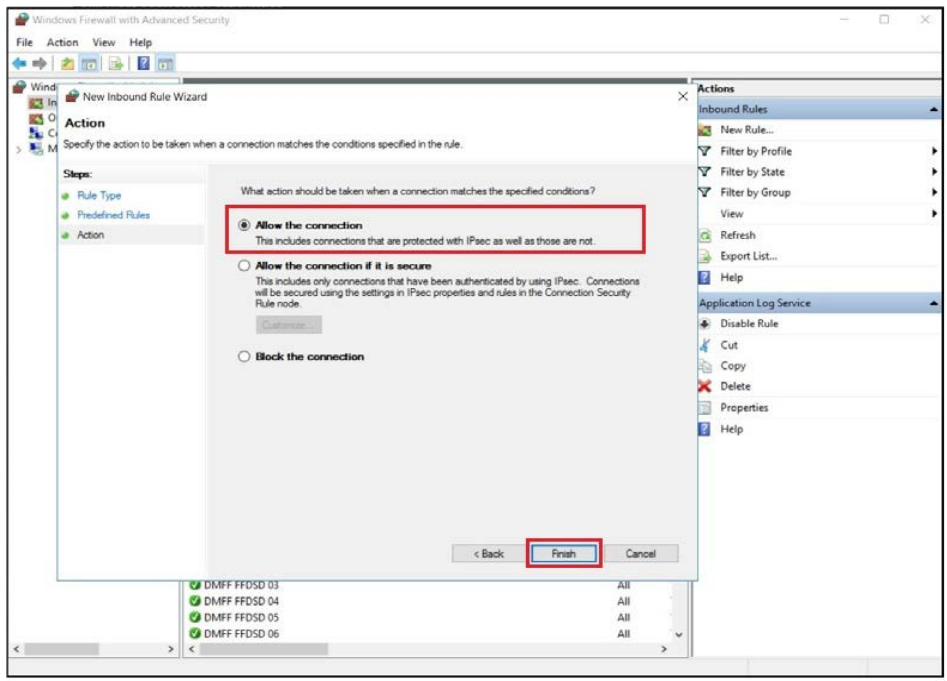

Figure 210. Allow the Connection

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

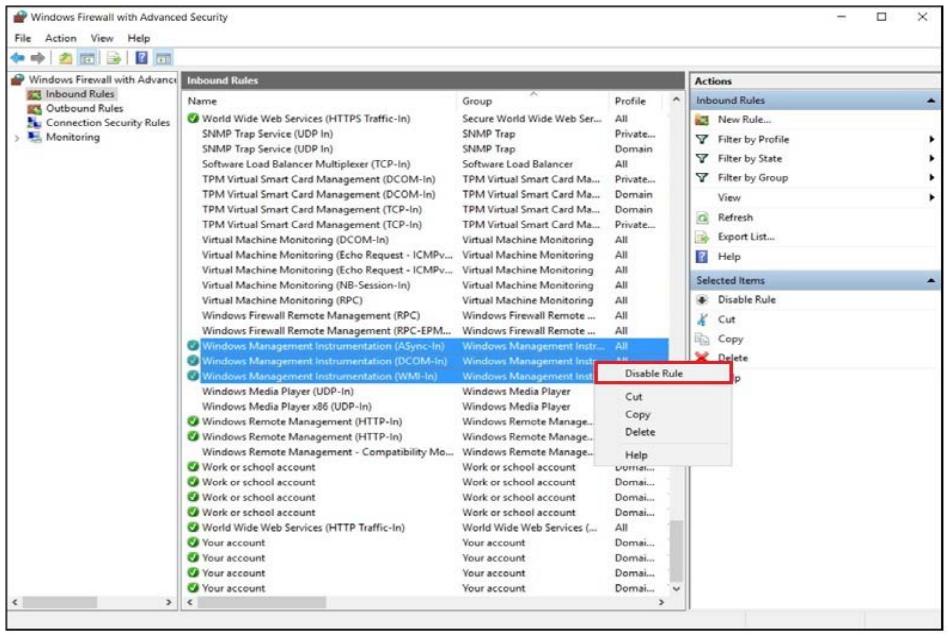

Figure 211. Disable the Rule

5.5 Issue 5: Enabling Windows Administrator Share Access for Freelance Data Collection.

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**

5.6 Issue 6: Disabling User Account Control

This applies only to Freelance 2016 SP1 or higher in Windows 10. In order to disable the UAC completely create a new registry key LocalAccountTokenFilterPolicy under the path

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilterPolicy and provide the value as 1.

Follow the Steps to create the register key.

1. Open the registry editor and go to the following path **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system**

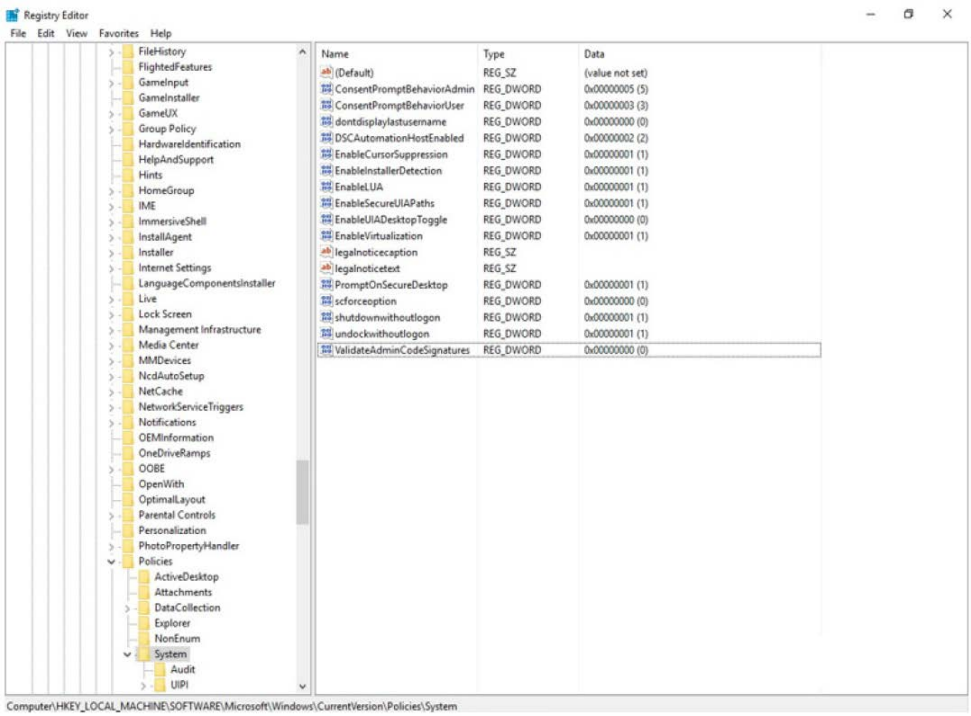

Figure 212. Registry editor

2. Right-click and create new registry key.

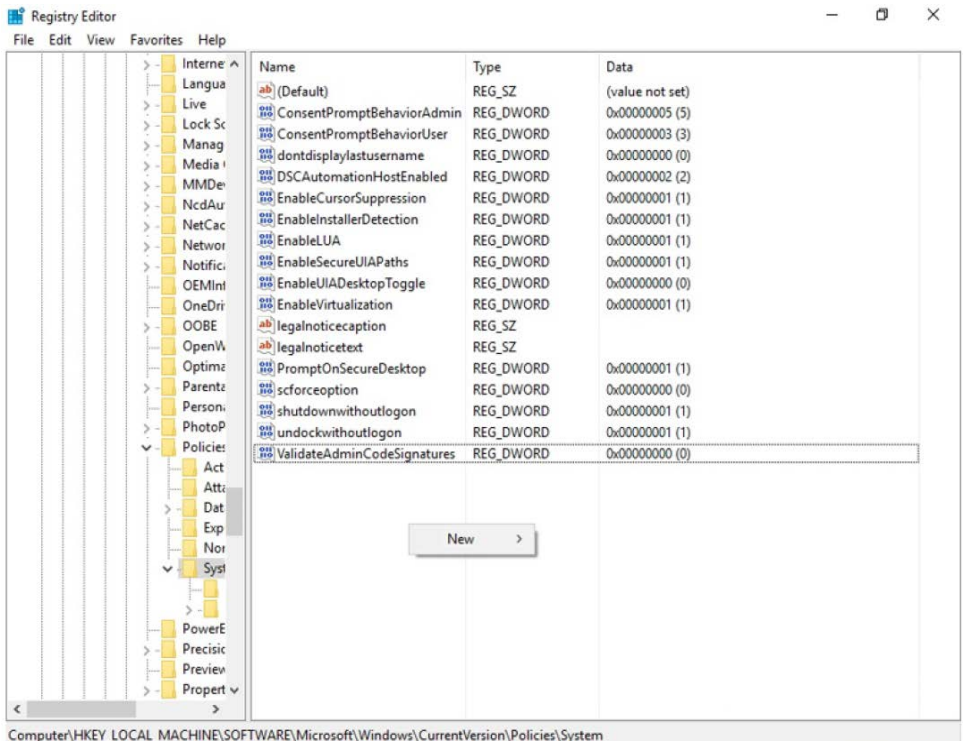

Figure 213. Create New registry Key

3. Select DWORD (32bit) Value.

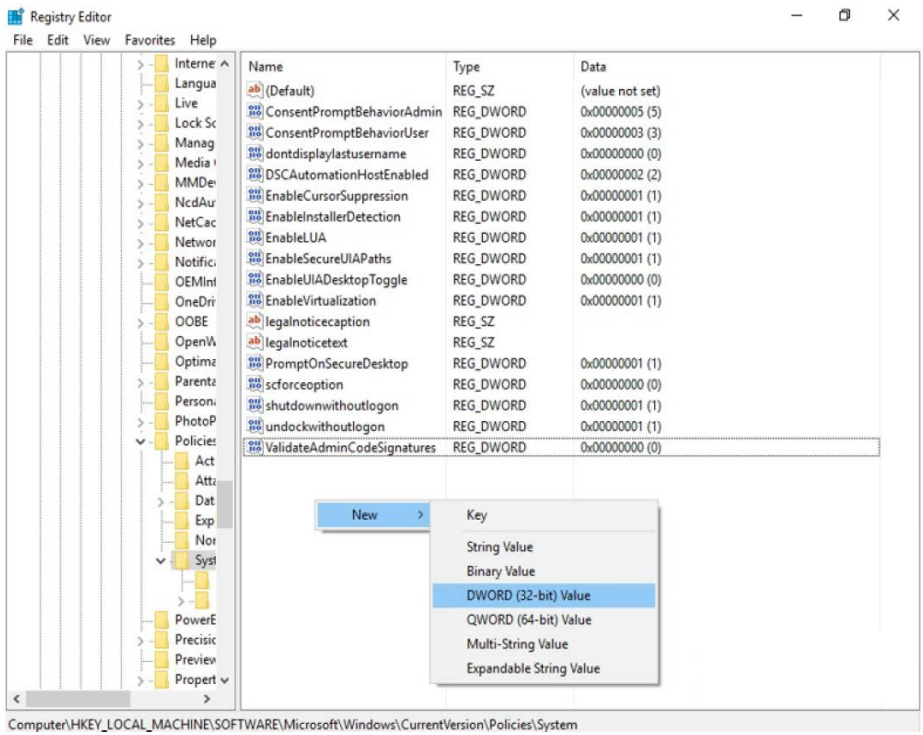

Figure 214. Select DWORD value

4. Rename the created registry key to LocalAccountTokenFilterPolicy.

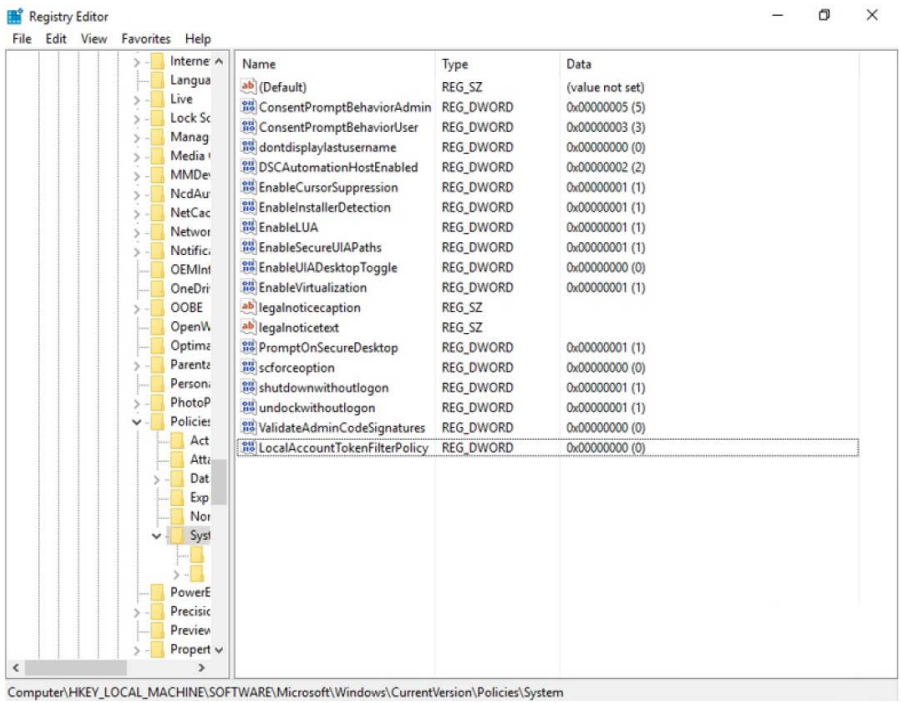

Figure 215. Rename the created registry key

5. Double-click the newly created registry key to edit and provide the value as "1". And Click OK.

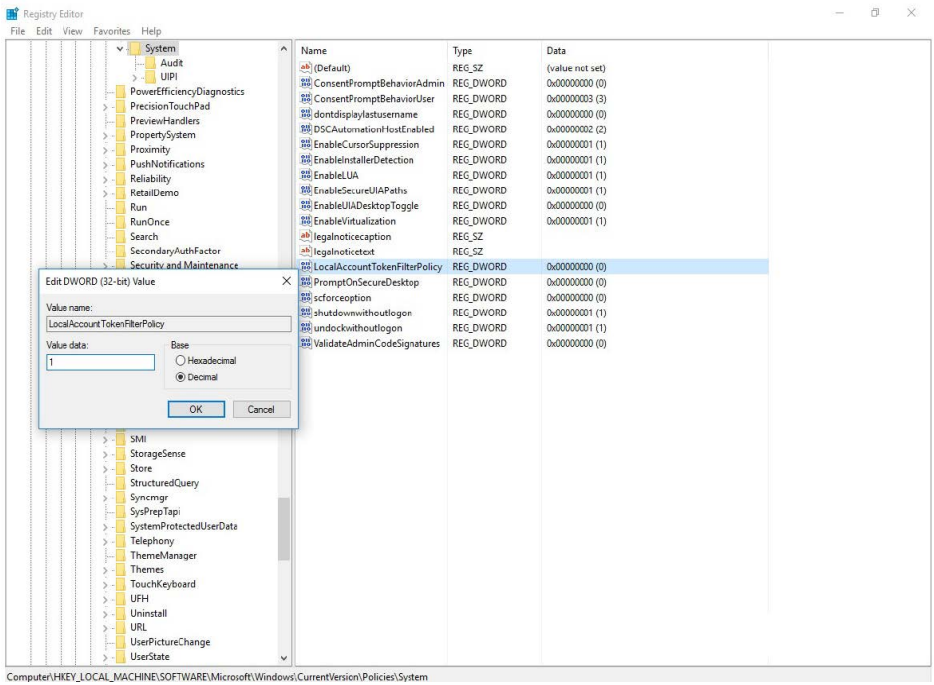

Figure 216. Edit registry key

The above mentioned account setting has to be done in all the nodes par of data collection, with the exception of the node where the MCS-DC is launched.

Disabling of UAC permanently is not recommended from Windows 10 onwards. Hence it is mandatory to delete the added registry keys after data collection is completed and MCS-DC is closed.

6 Additional Information

6.1 Listing of related documents

Table 2.

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

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.

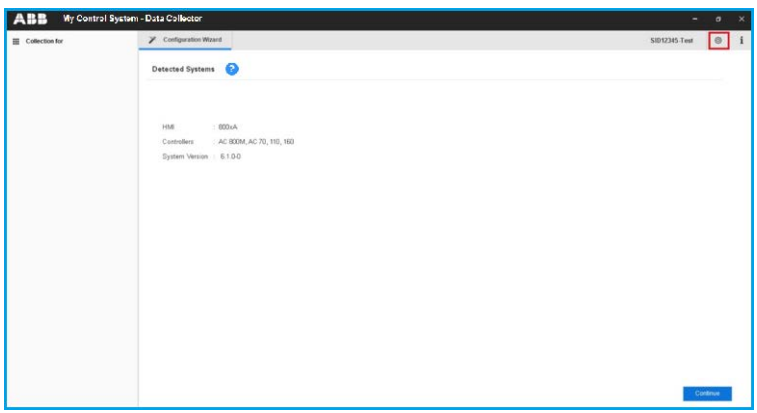

Figure 217. Click On Settings Icon

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

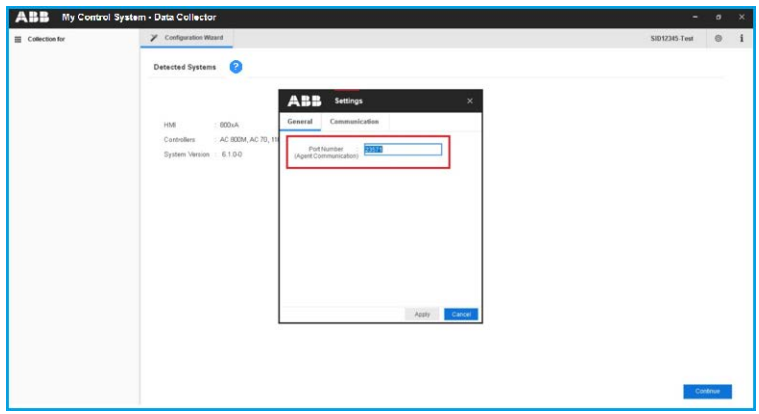

Figure 218. Provide New Port Number

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.

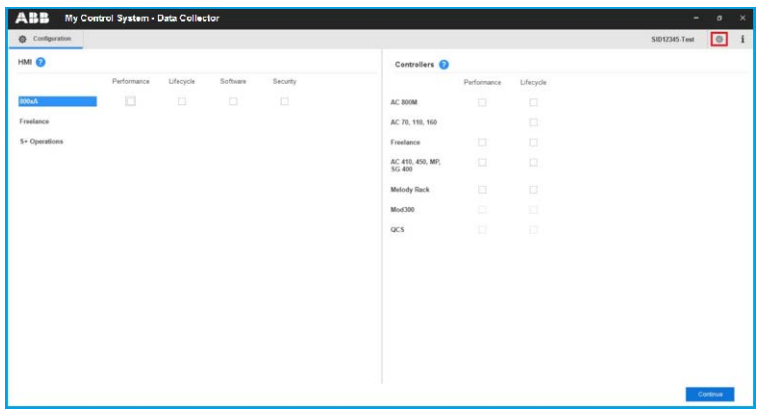

Figure 219. Click on Settings Icon

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

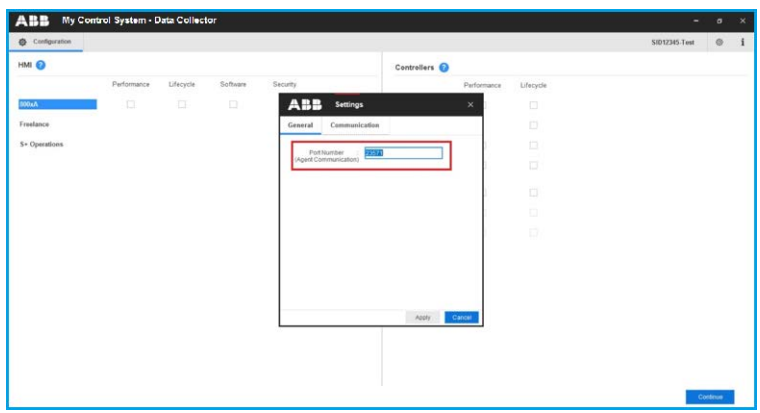

Figure 220. Provide Port Number

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. It is solely user's responsibility to get the Certificates.

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 **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.

For Self-Signed Certificate and Third-Party Certificates, it is solely user's responsibility to get the Certificates.

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.

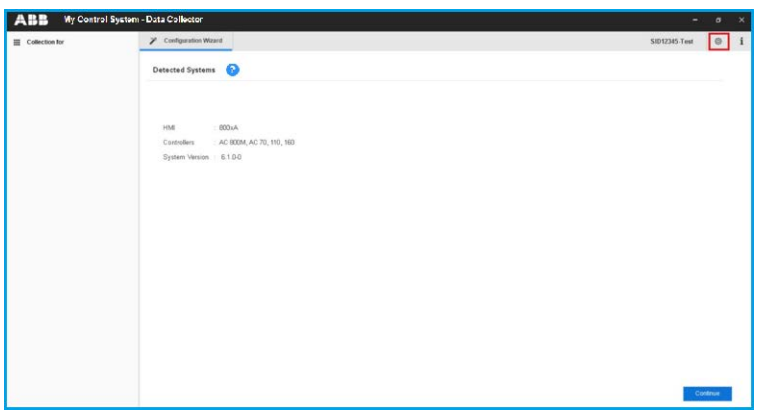

Figure 221. Basic Mode

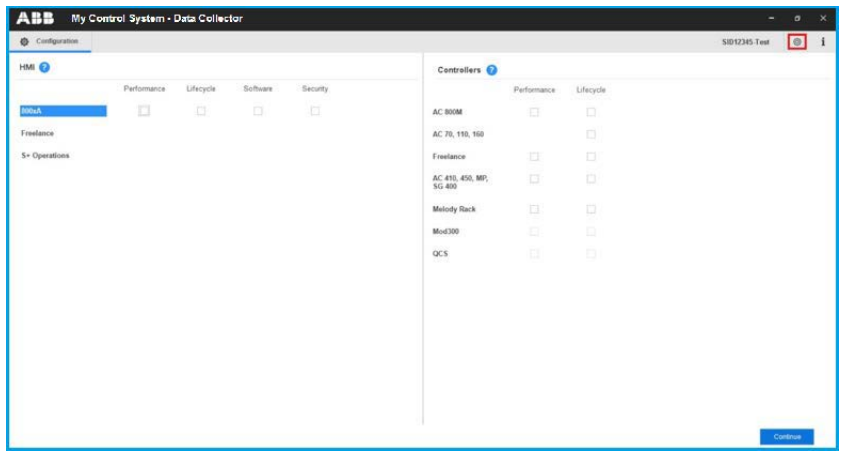

Figure 222. Advanced Mode

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

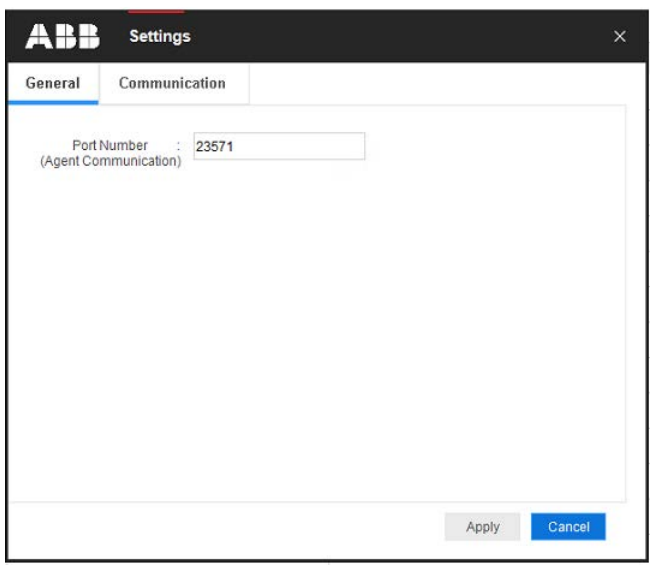

Figure 223. Communication Port

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

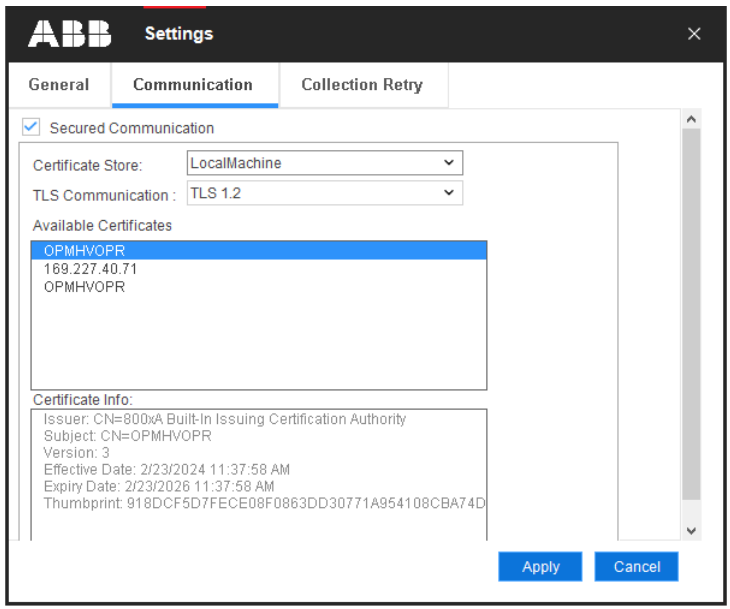

Figure 224. Communication Tab

4. 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.

In basic mode, the highest TLS version is automatically selected on remote computers. The communication will fail if it does not match the TLS version selected by the user on the host computer.

B.2 Selection of Client Certificate

If 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 running the utility

ABB.Services.UpdateClientCertificate (right click and run as administrator) from the folder path C:\Windows\Temp\MCSDC\<date_time> (for 800xA and Freelance) and C:\SPOHCLogger (for Symphony plus). 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.

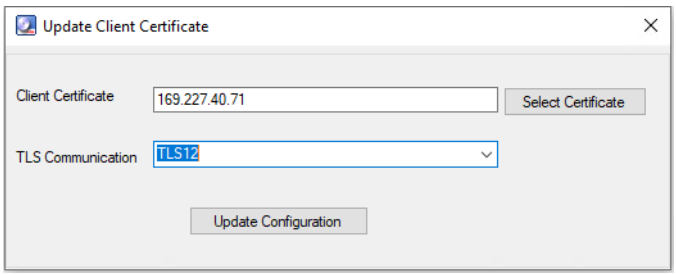

Figure 225. Update Client Certificate

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

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

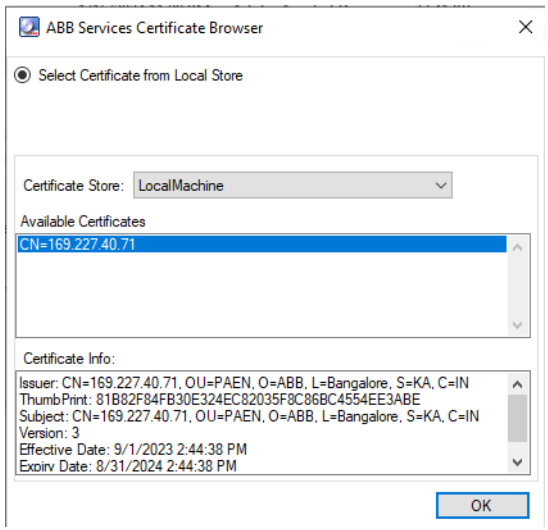

Figure 226. Client Certificate

B.3 Binding the server certificate to an IP address and port

It is required to bind the server certificate to the IP address and port used for secured communication. Follow the port binding procedure below.

https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/how-to-configure-a-port-with-an-ssl-certificate.

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 (,).

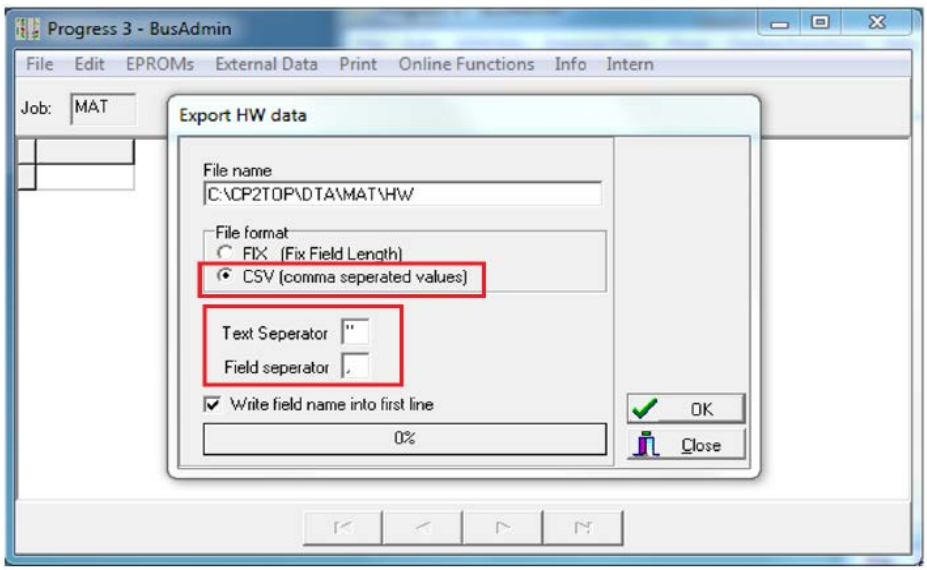

Figure 227. Export HW data

Appendix D System configuration export

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.

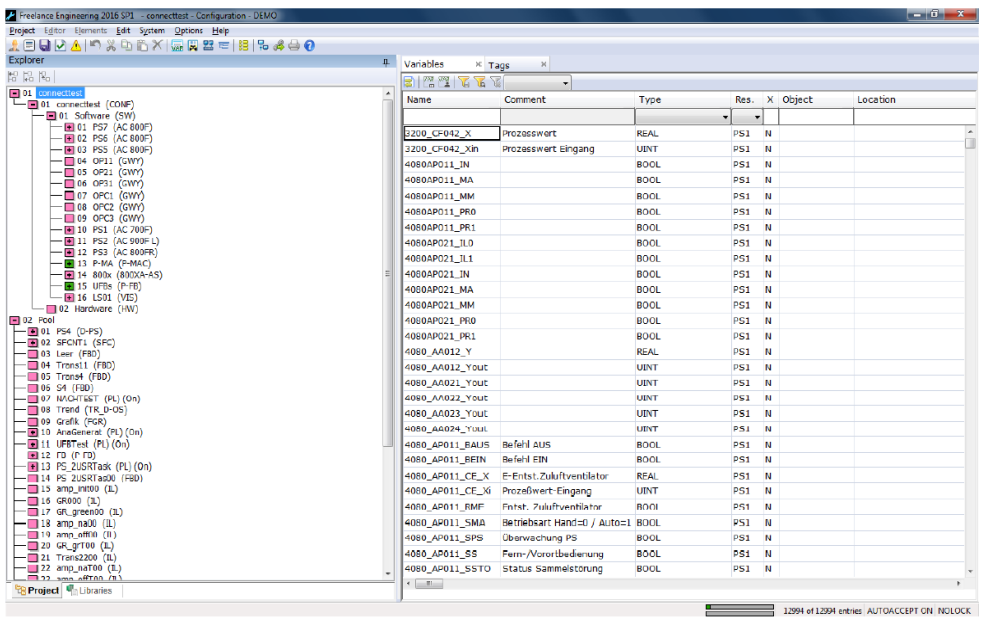

Figure 228. Freelance Engineering 2016 sp1

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

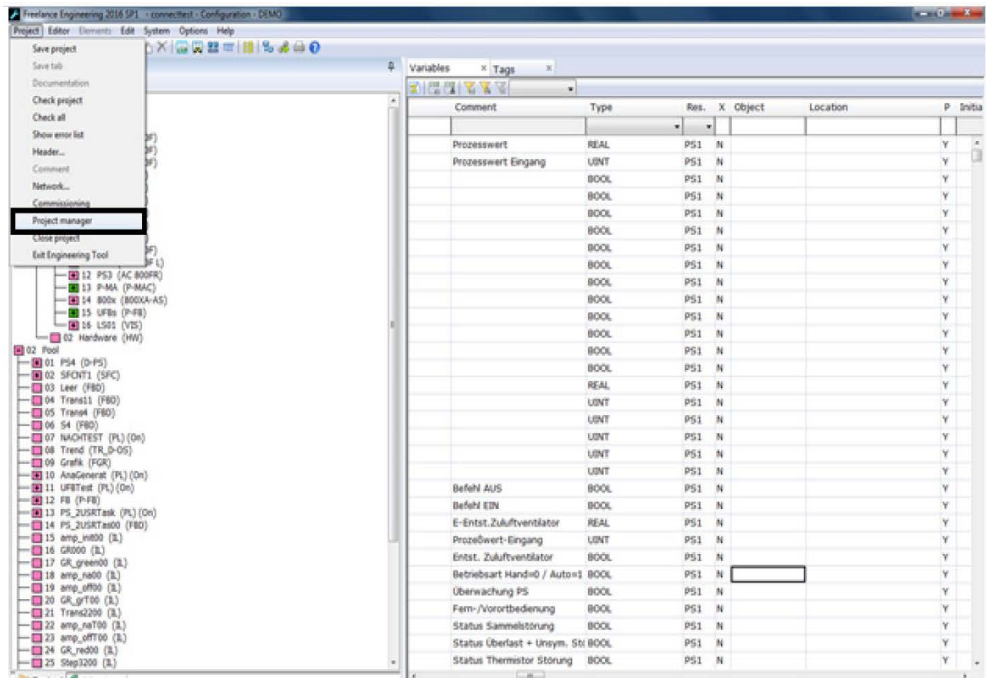

Figure 229. Project Menu

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

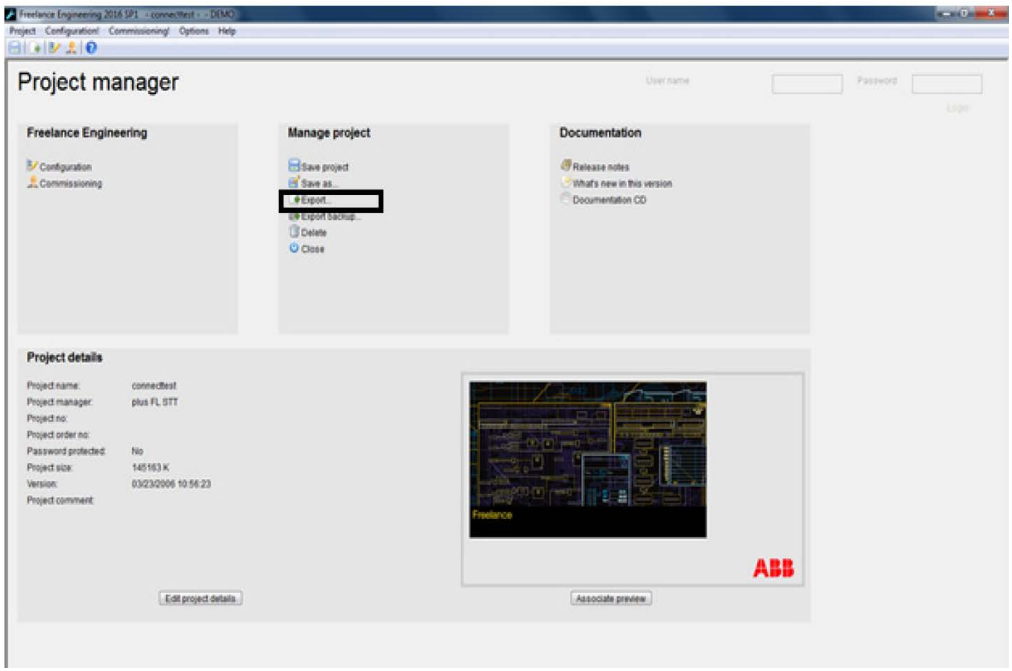

Figure 230. Export option

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

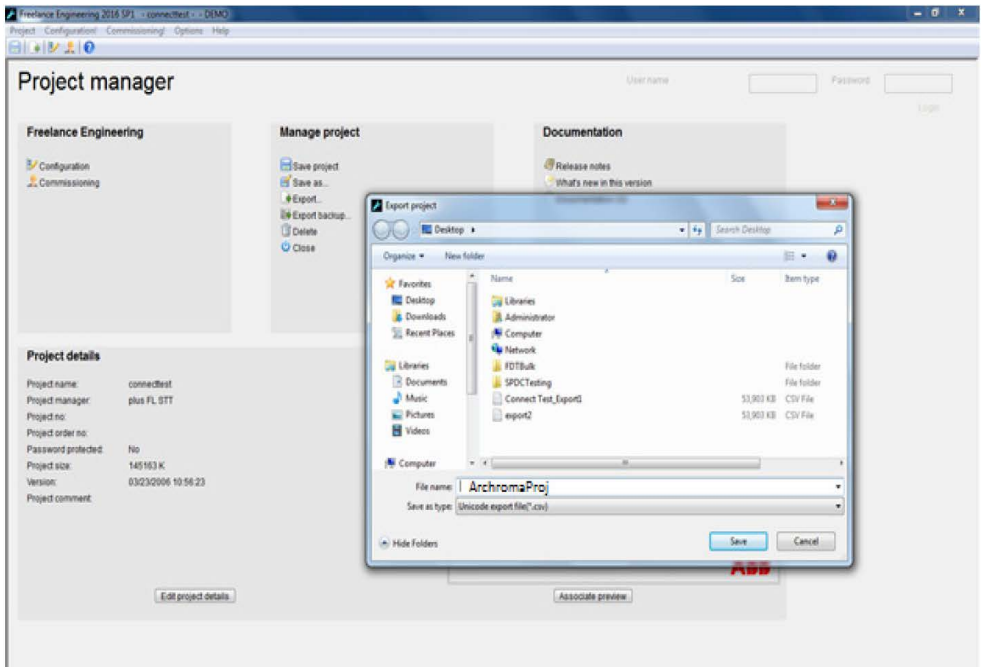

Figure 231. Project manager tab

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

D.2 Advant MOD 300

This sections 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, goto menu **Object > Special Commands** and select **Save_ATF**.

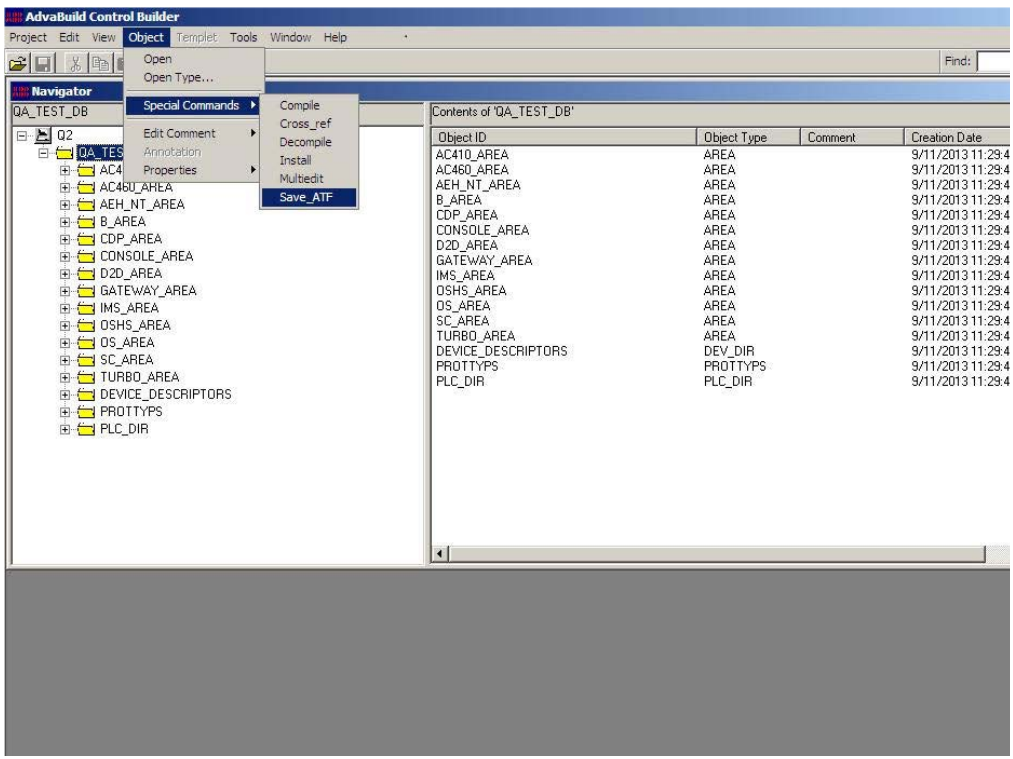

Figure 232. Object Tab

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.

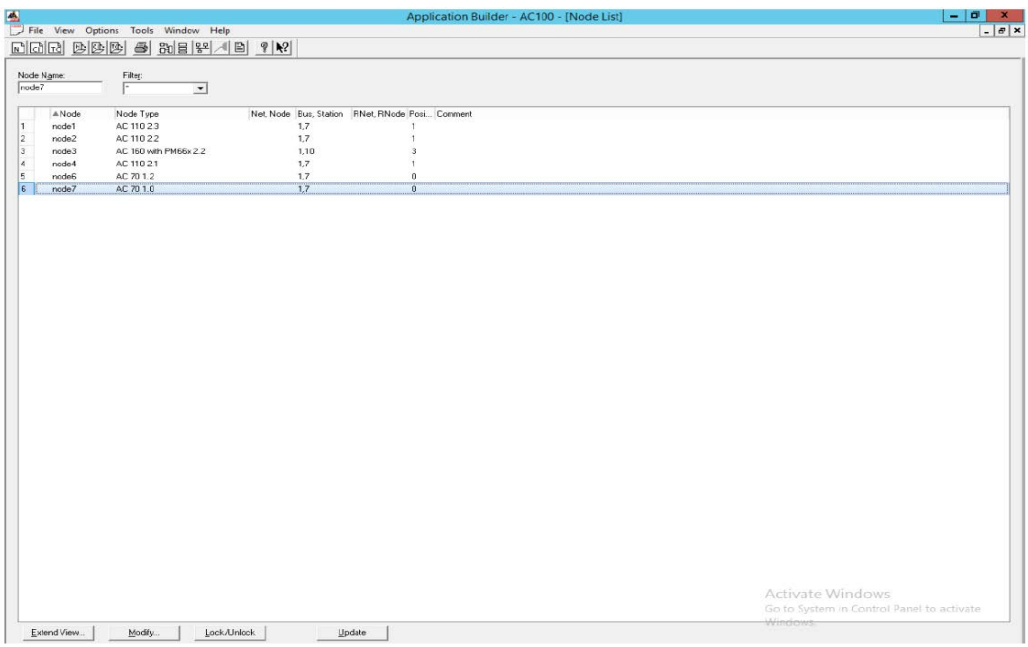

Figure 233. Application Builder AC100

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

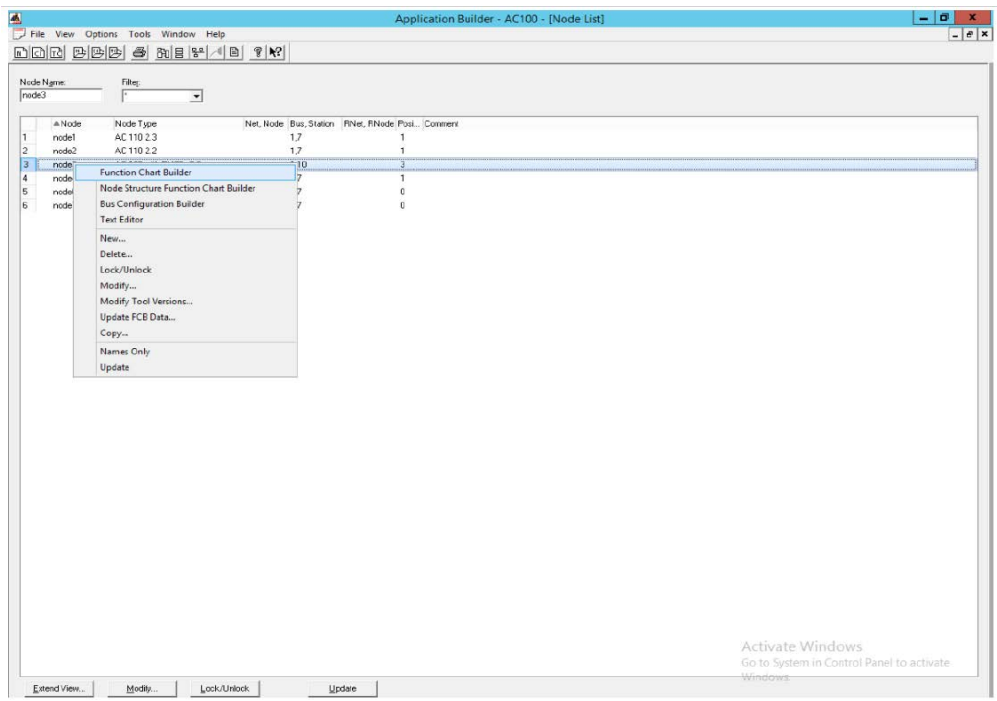

Figure 234. Function Chart Builder

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

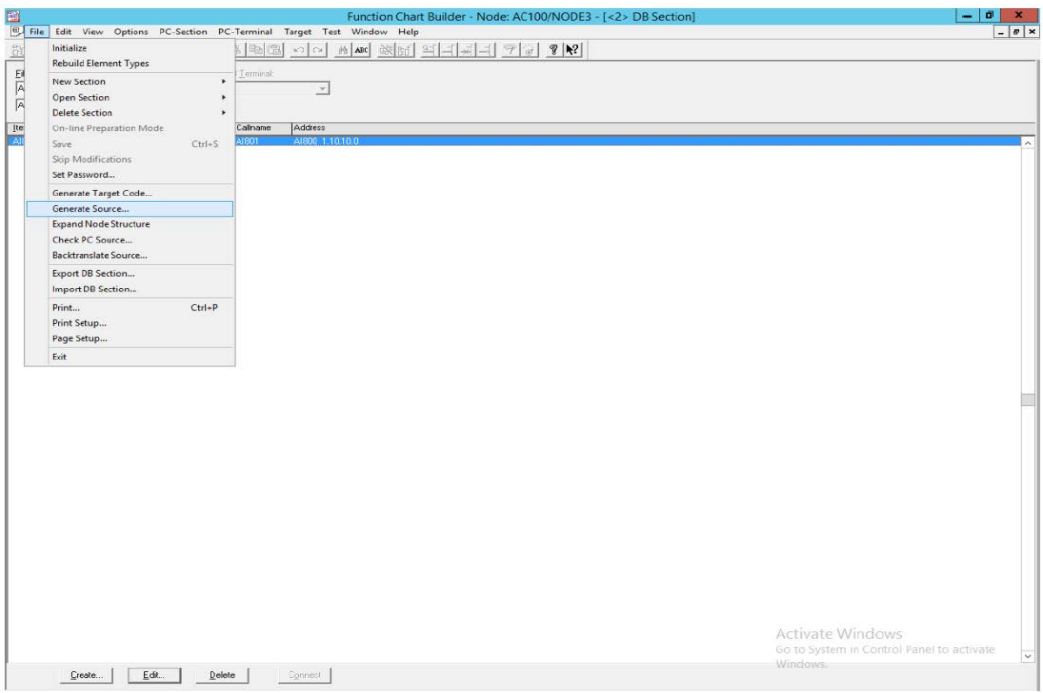

Figure 235. Generate Source

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

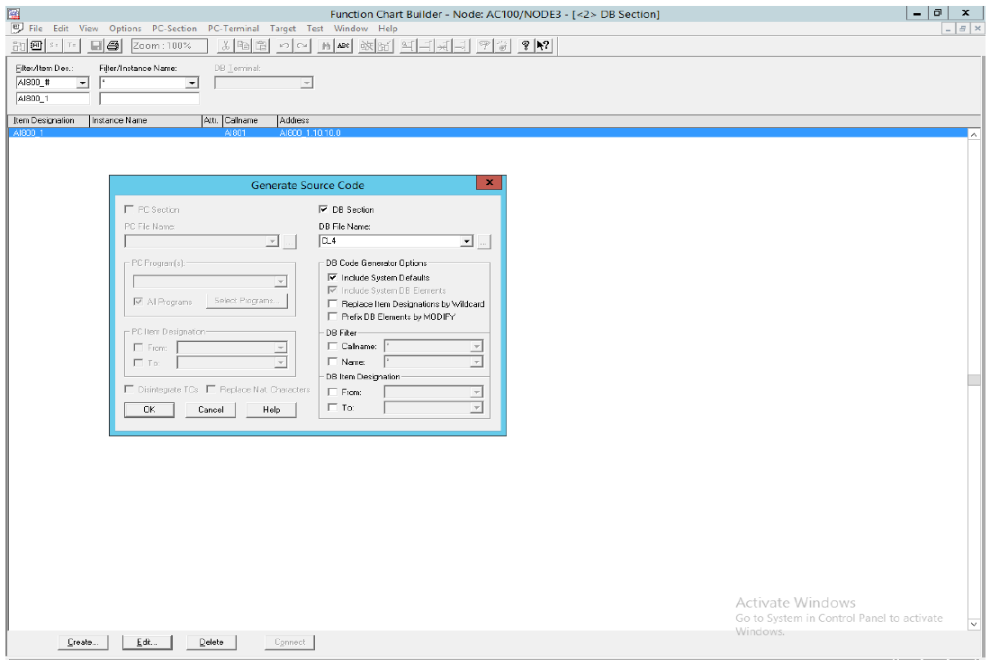

Figure 236. Generate Source Code

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.

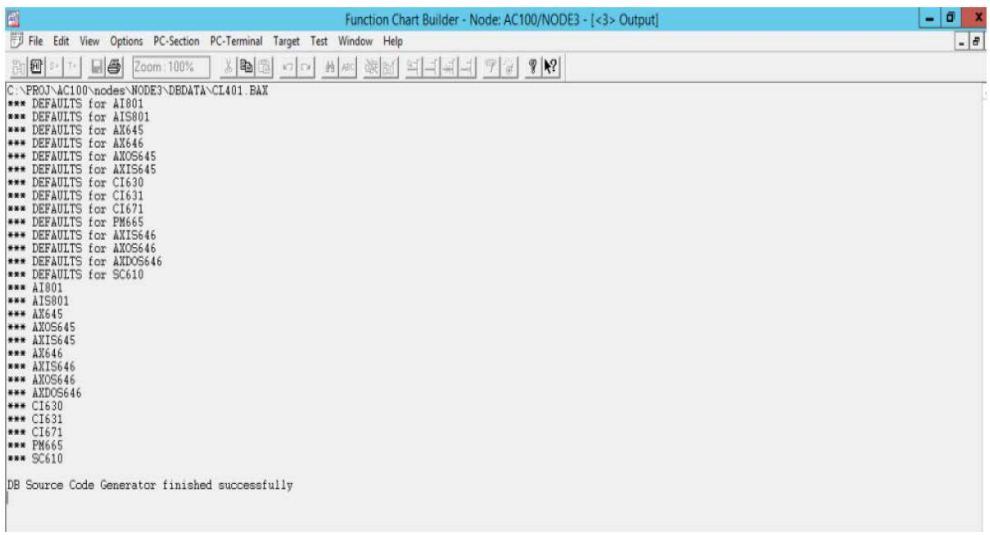

Figure 237. Function Chart Builder - Node AC 100/NODE3

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

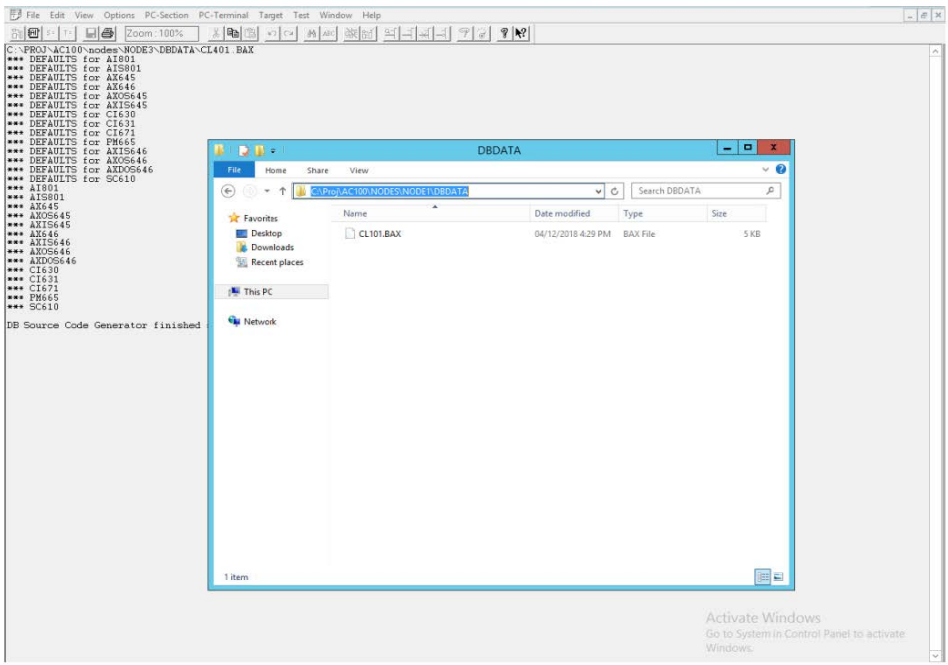

Figure 238. Saved file path location

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

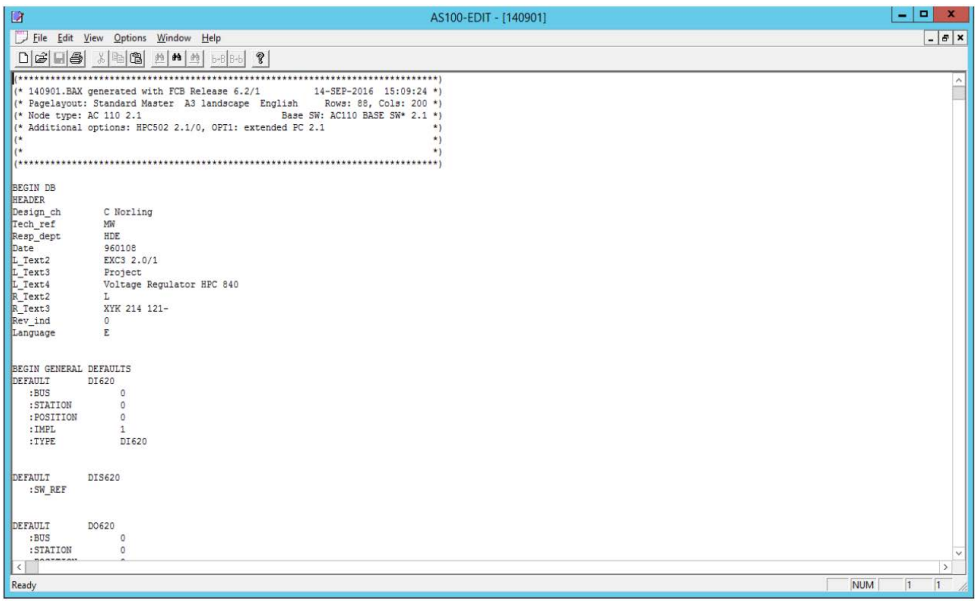

Figure 239. Sample of .bax file with AC100 configuration

D.4 Melody Rack

D.4.1 Composer Melody Rack version 6.0 or later

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

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

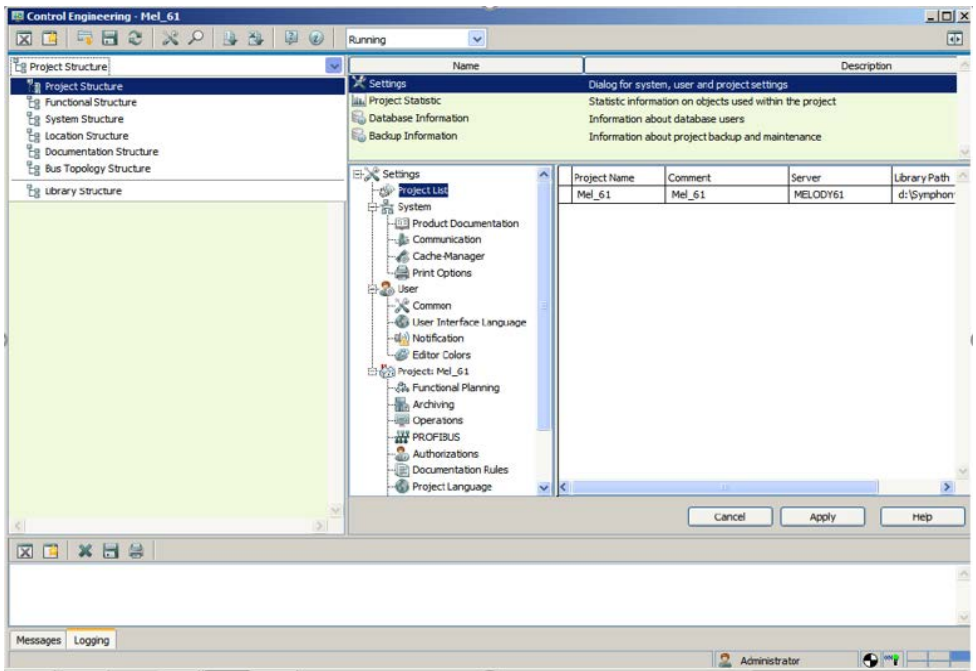

Figure 240. Open Composer and switch to Project Structure view.

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

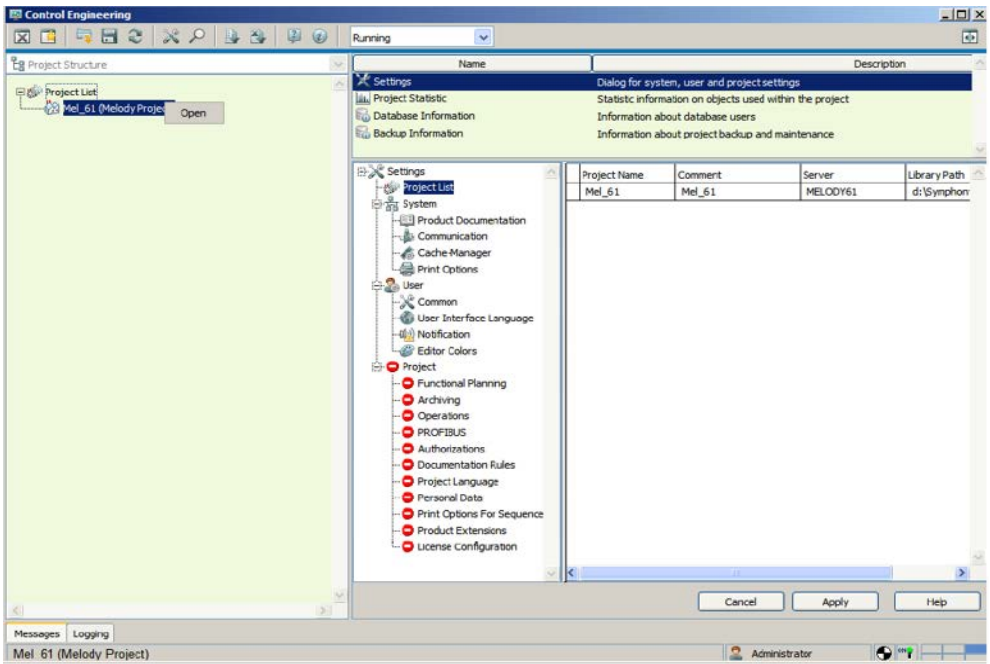

Figure 241. Open the project.

3. Select **Bus Topology Structure.**

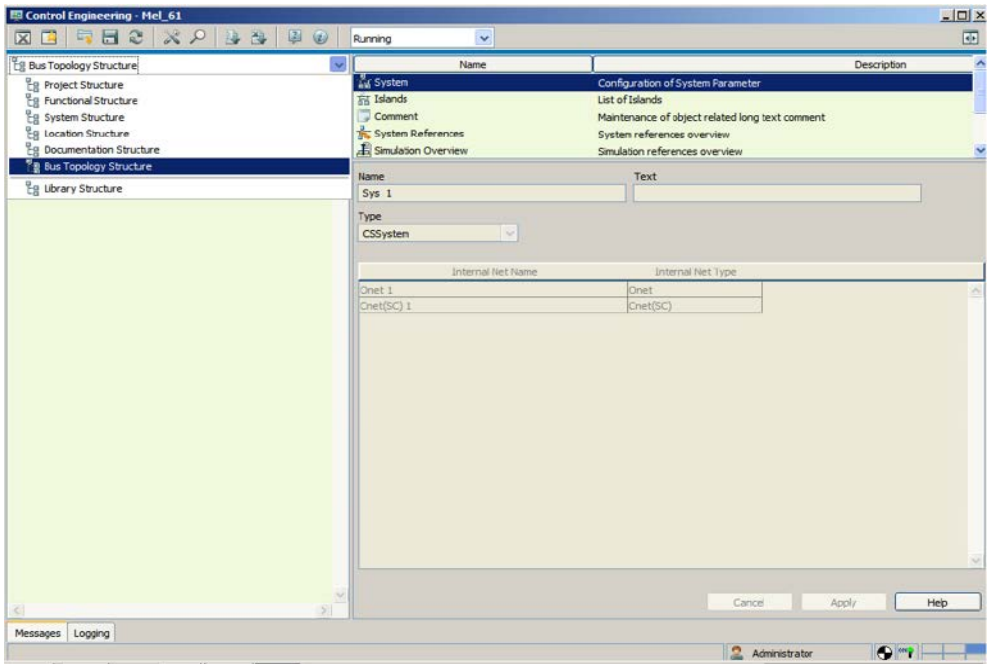

Figure 242. Select Bus Topology Structure view

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

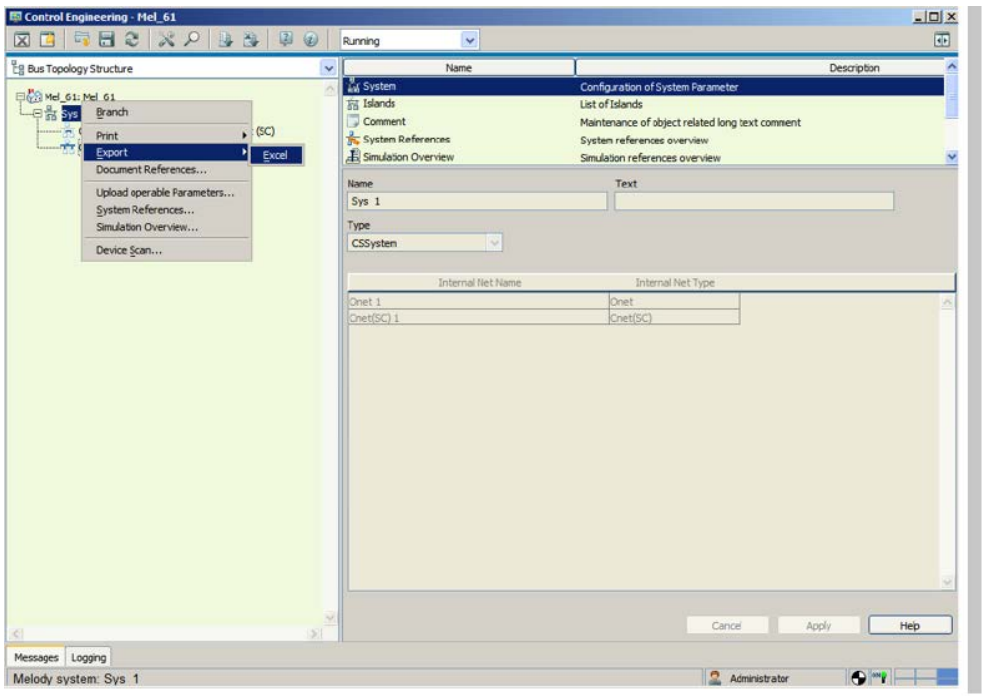

Figure 243. Select Export to export in Excel

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

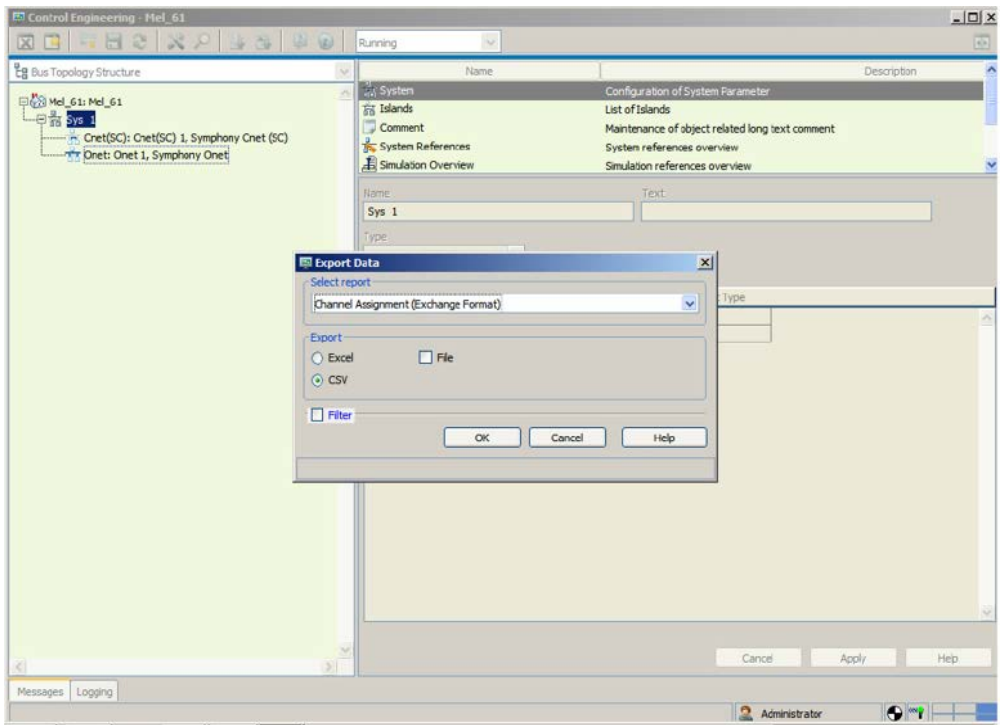

Figure 244. Select CSV Option

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

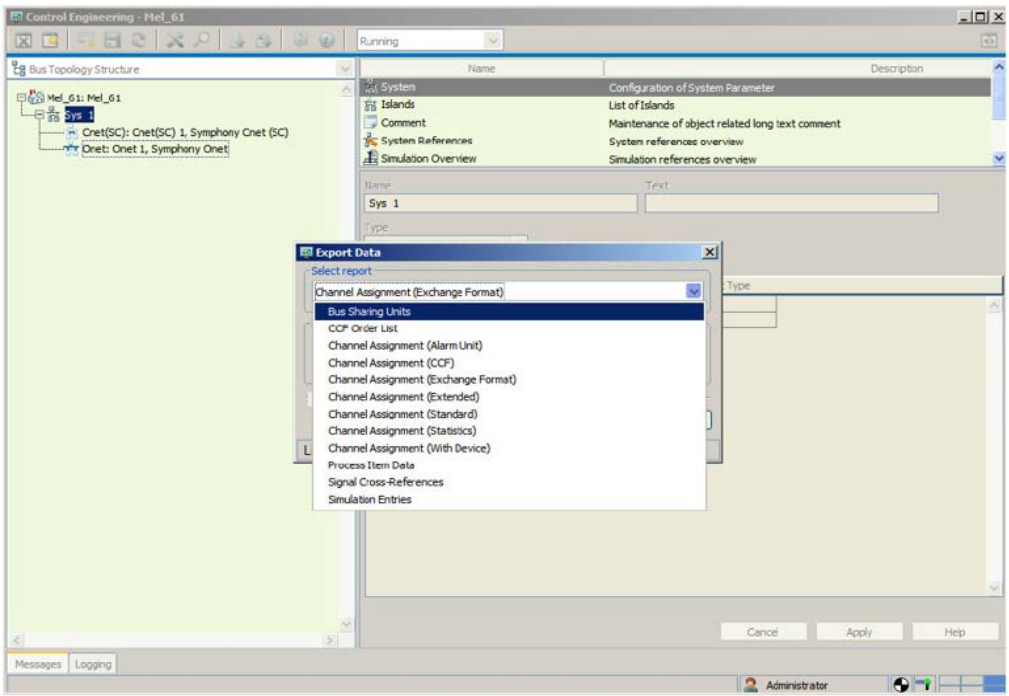

Figure 245. Export Data Bus Sharing Units

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

D.4.2 Asset structure export

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

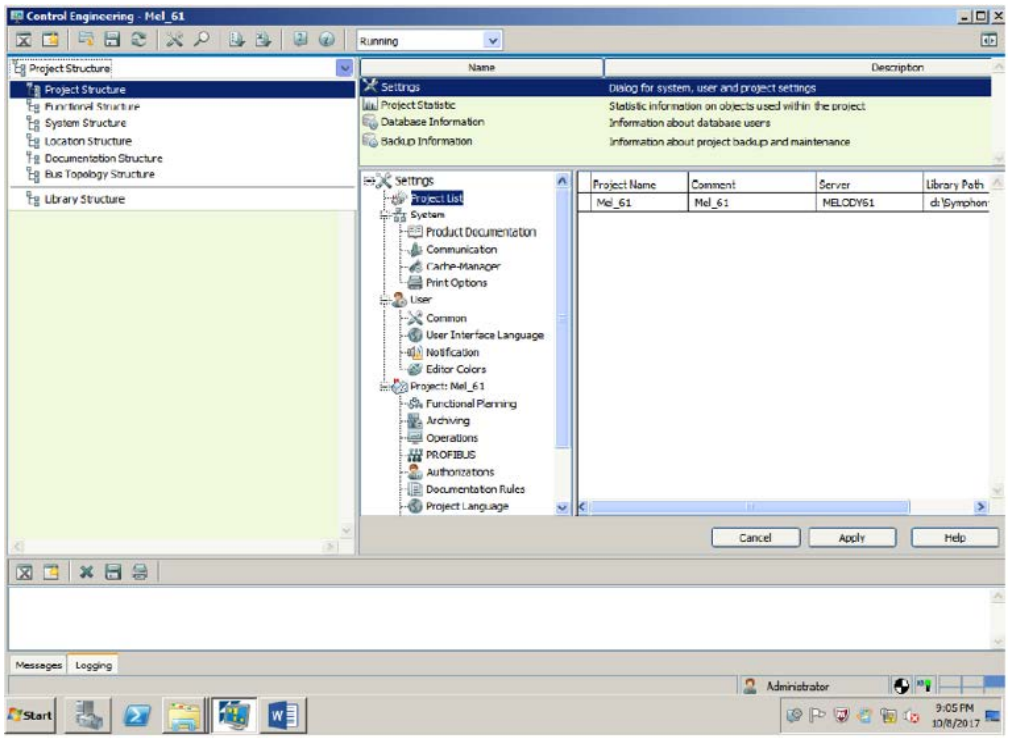

Figure 246. Project Structure View

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

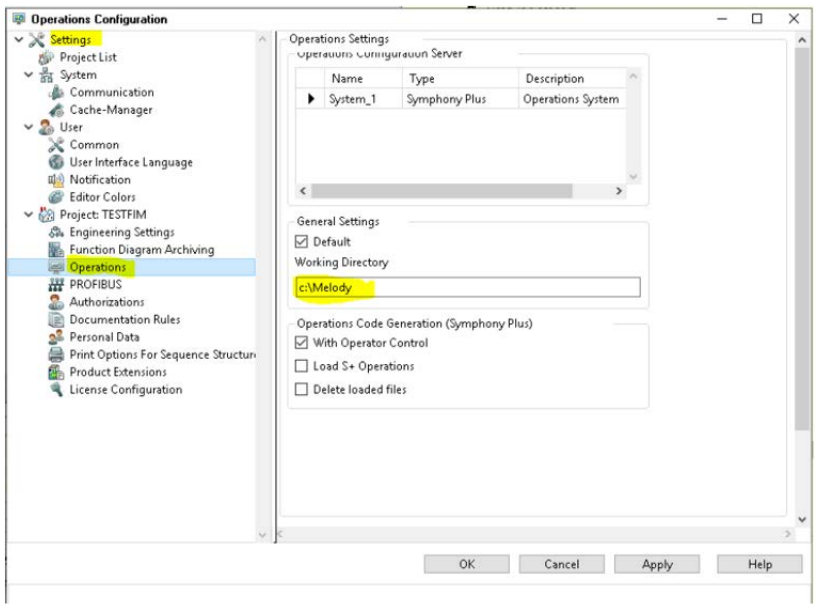

Figure 247. Operations Configuration Window

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

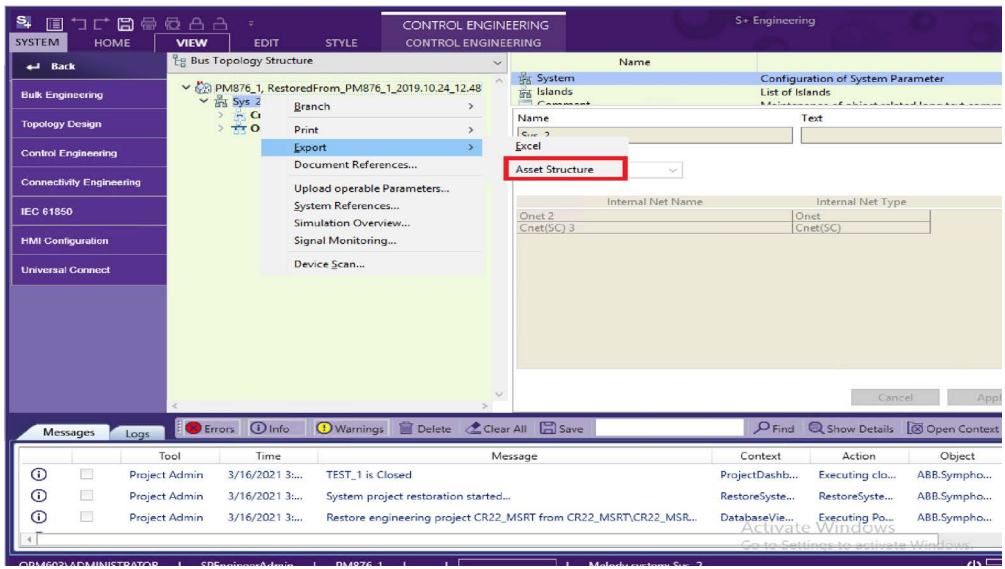

Figure 248. Export the asset from system structure

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

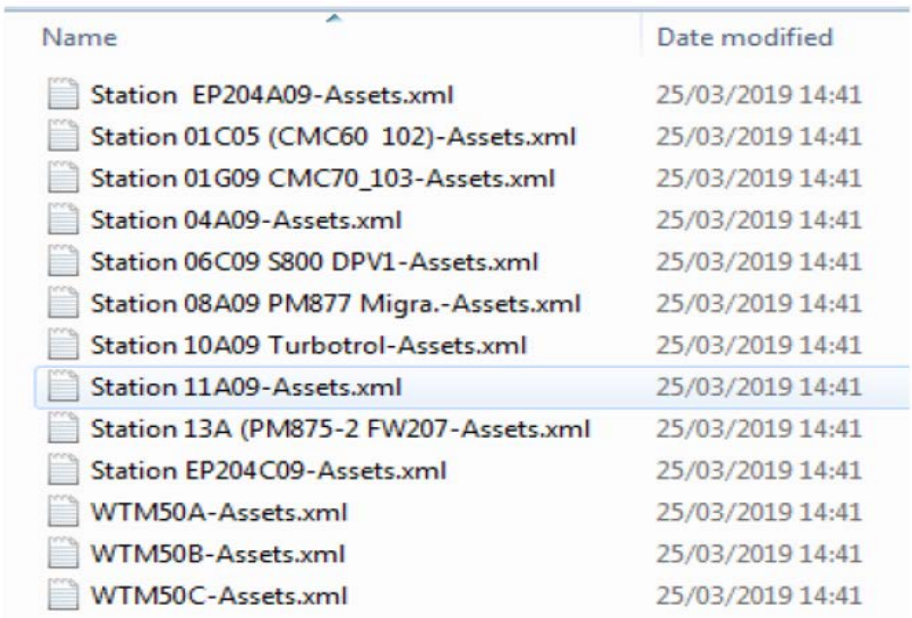

Figure 249. Exported Assets

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

D.4.3 Composer Melody Rack version 5.2 or earlier

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

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

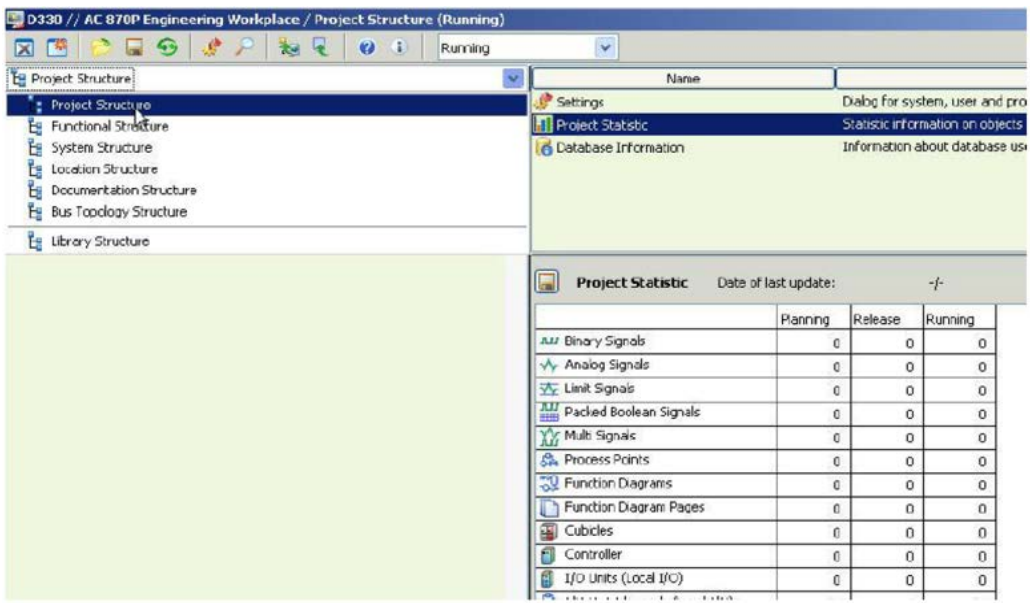

Figure 250. Open Composer and switch to Project Structure view.

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

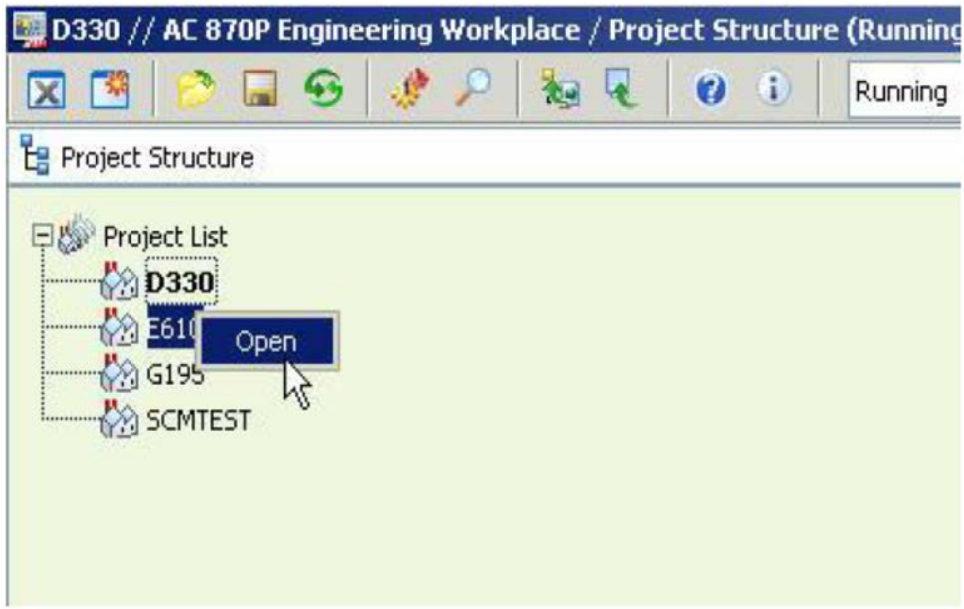

Figure 251. Select Open to Open customer's project

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

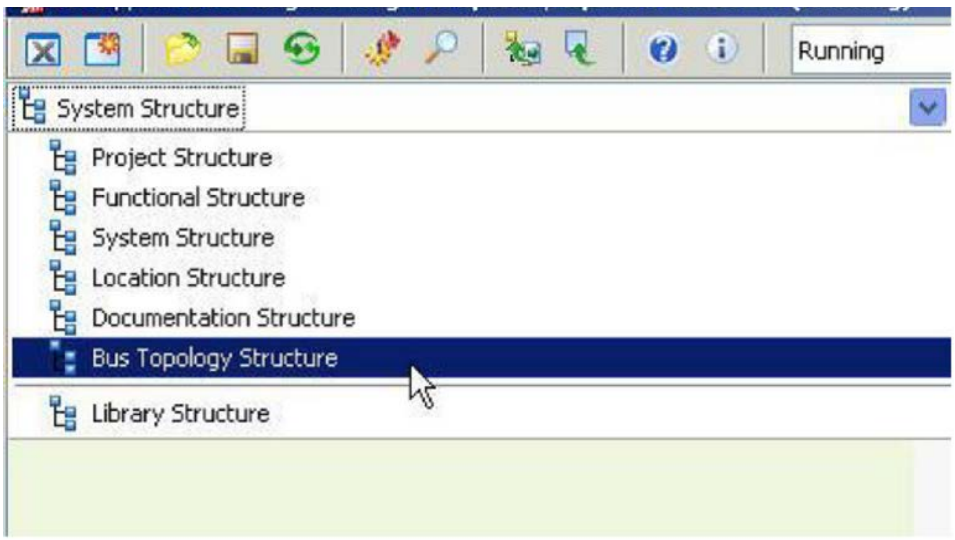

Figure 252. Bus Topology Structure view

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

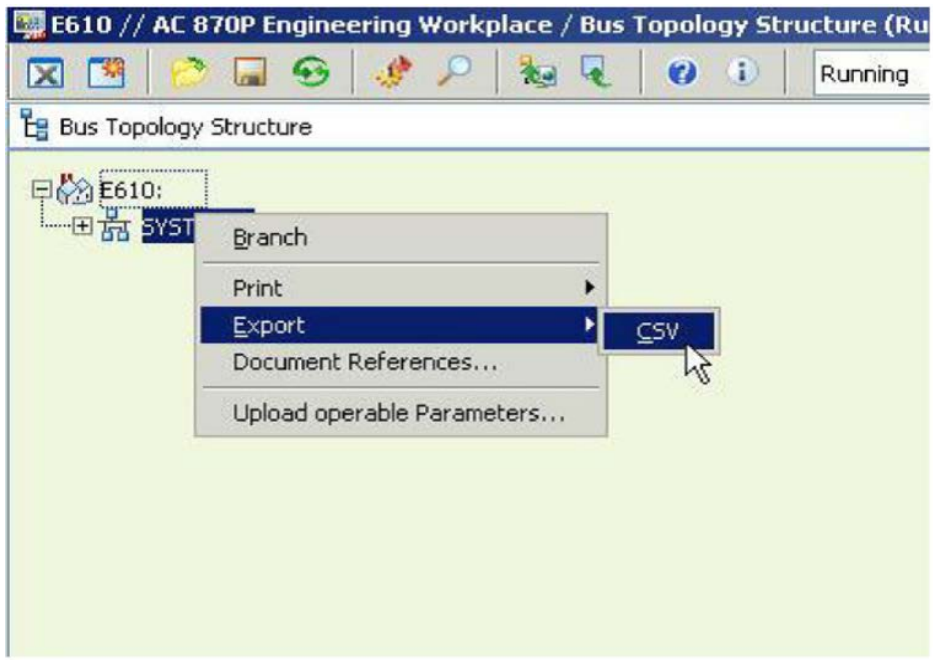

Figure 253. How to export CSV

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

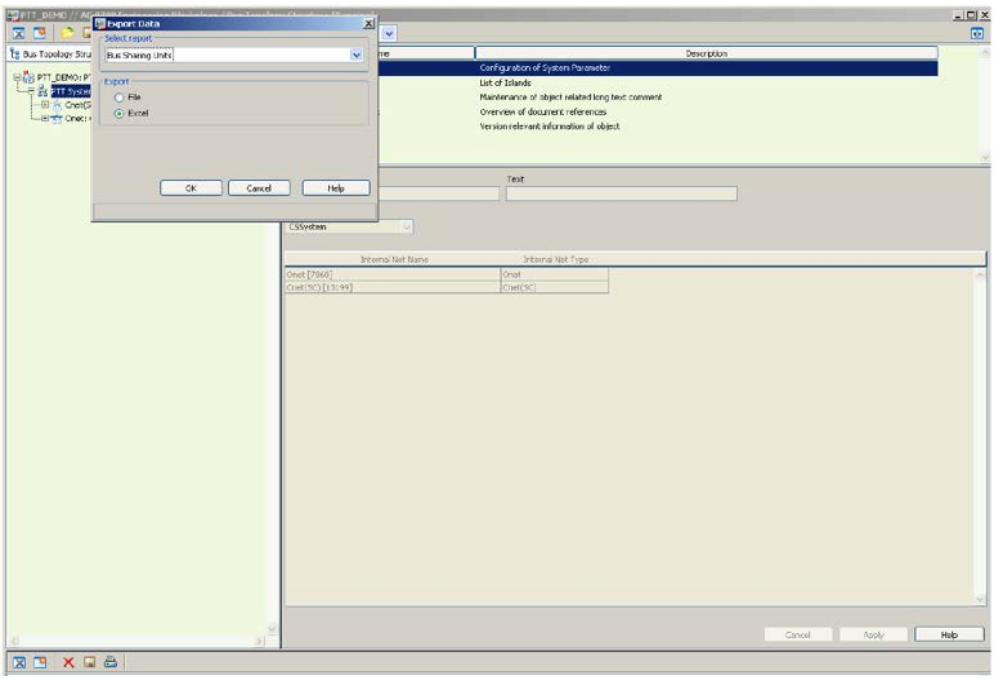

Figure 254. .CSV file export option

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

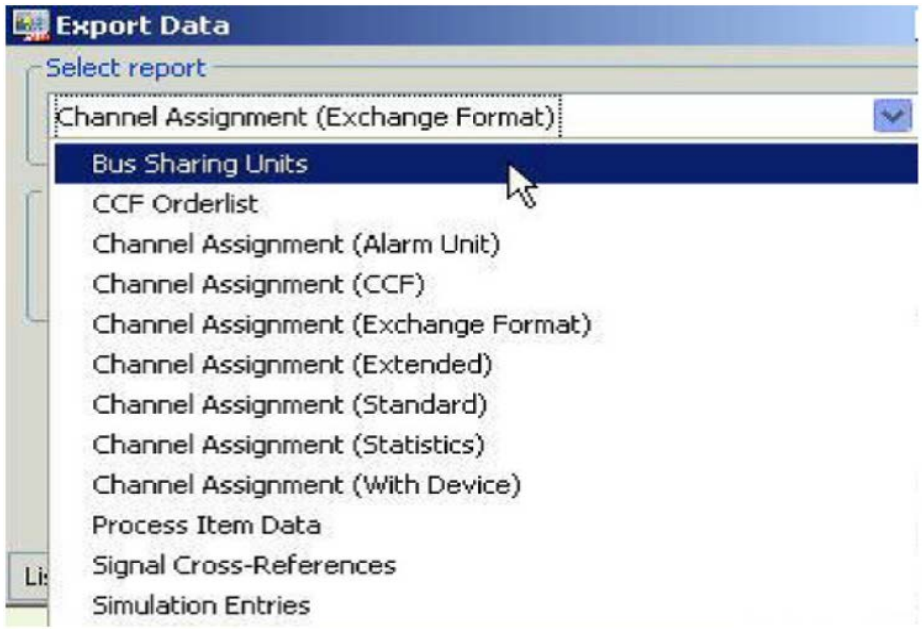

Figure 255. Choose Bus Sharing Units report

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.4.4 Melody CSE_Conf File

CSE_Conf file contains the EPC and IP addresses of all of 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.

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 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.

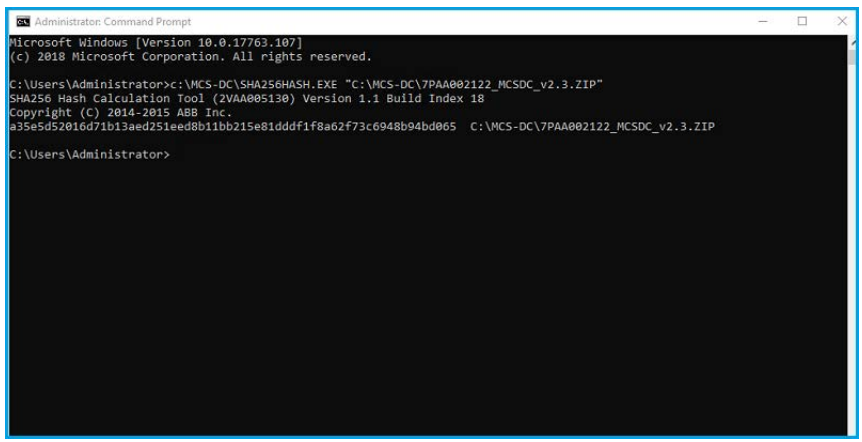

Figure 256. Hash Check

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 power shell: *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 257.

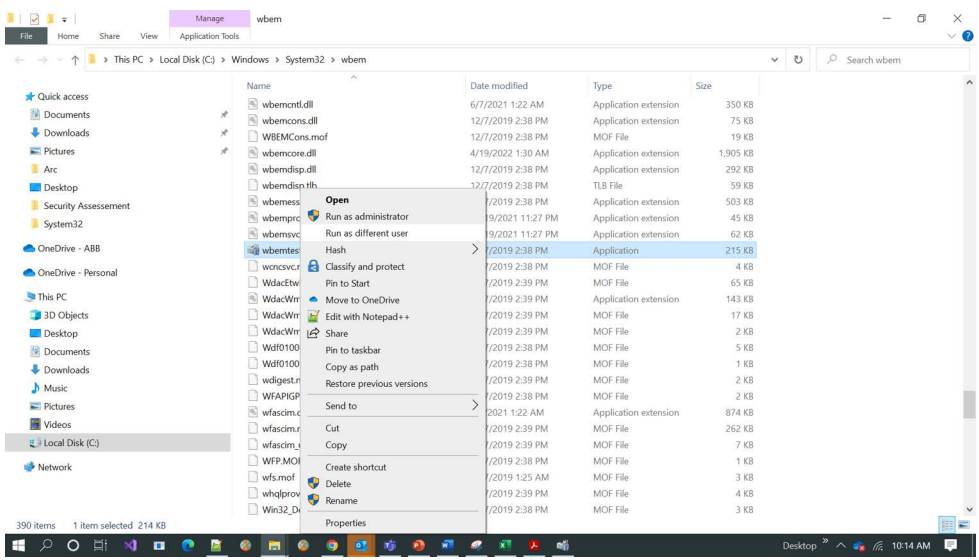

Figure 257. System32 Folder

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**.

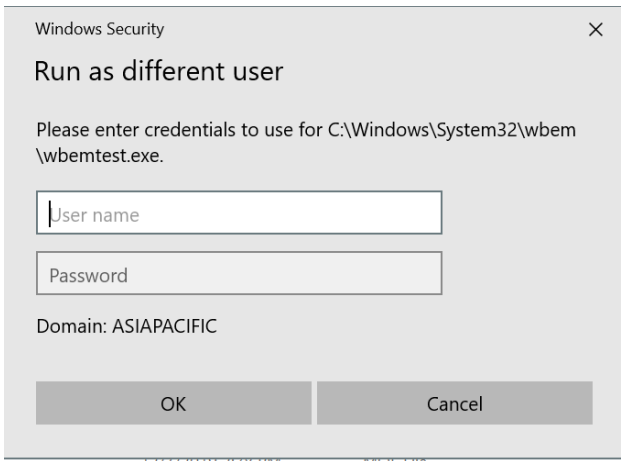

Figure 258. Enter Credentials

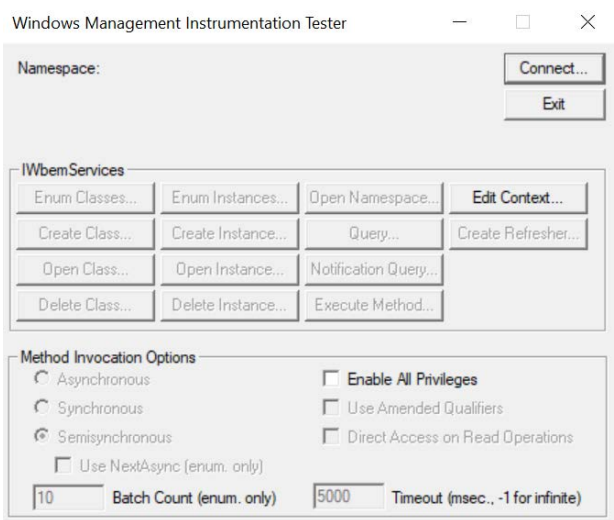

Figure 259. Windows Management Instrumentation Tester

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.

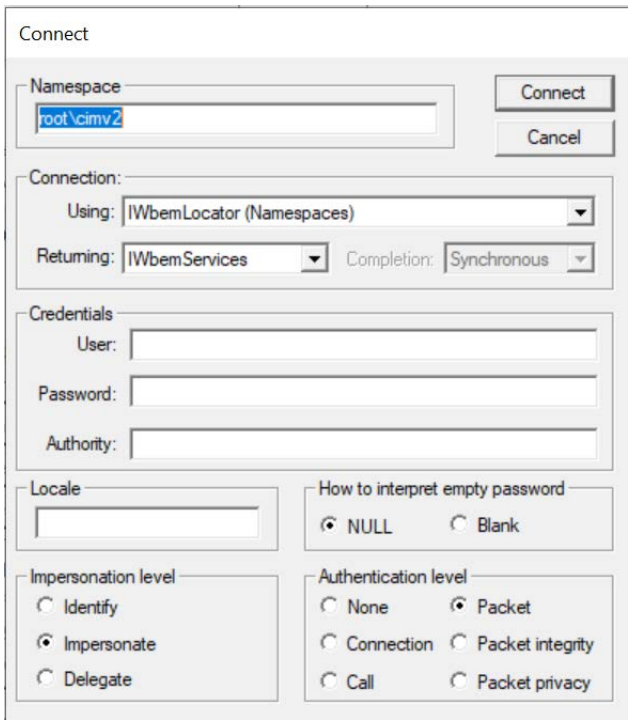

Figure 260. WMI query health check - Local computer

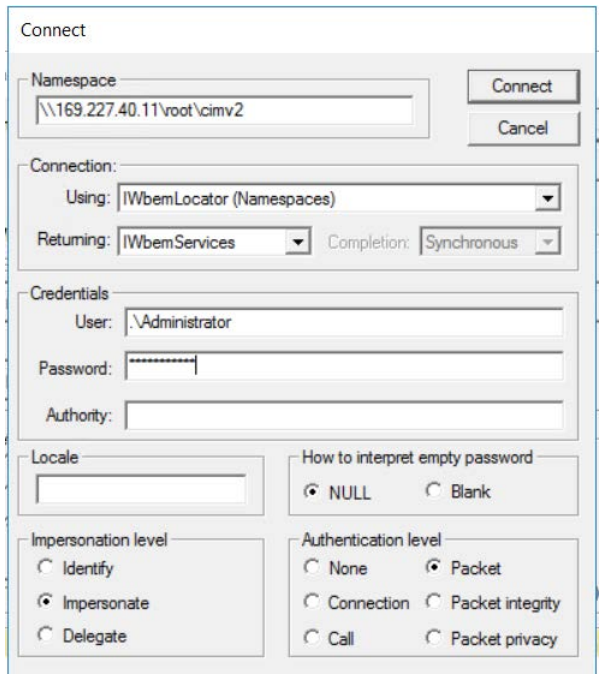

Figure 261. WMI query health check - Remote computer

4. Successful connect brings up the following Window.

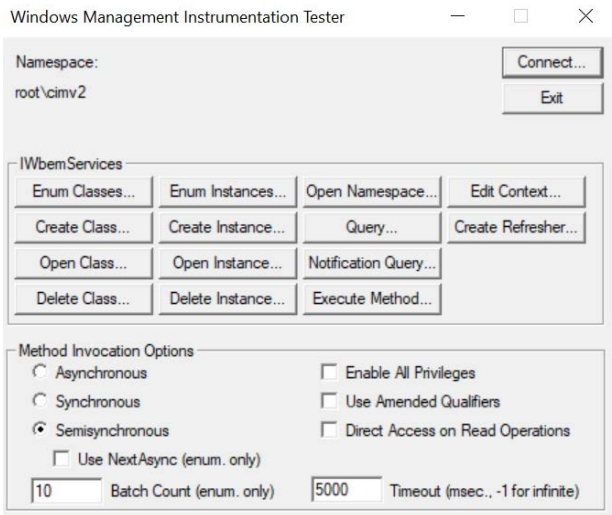

Figure 262. Connection successful - Local

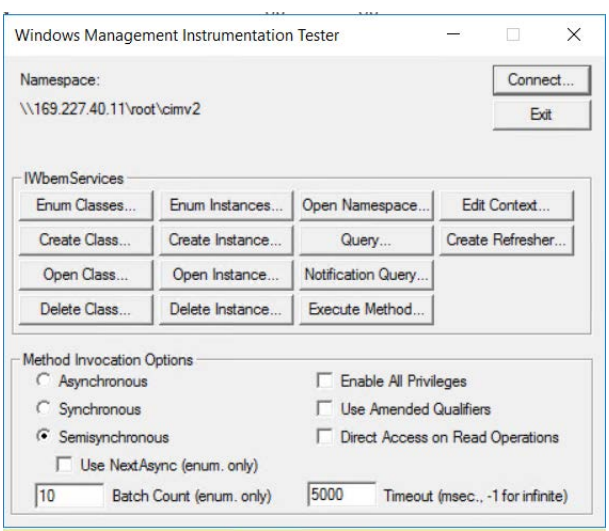

Figure 263. Connection successful - Remote

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

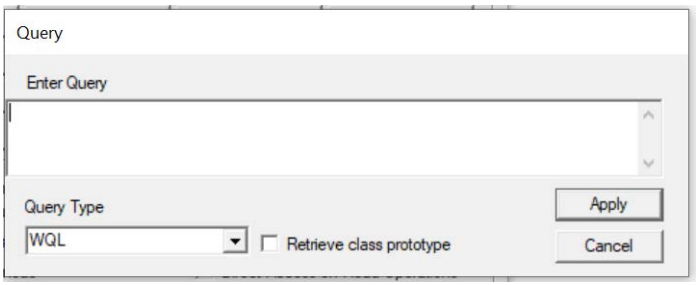

Figure 264. Enter Query

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.

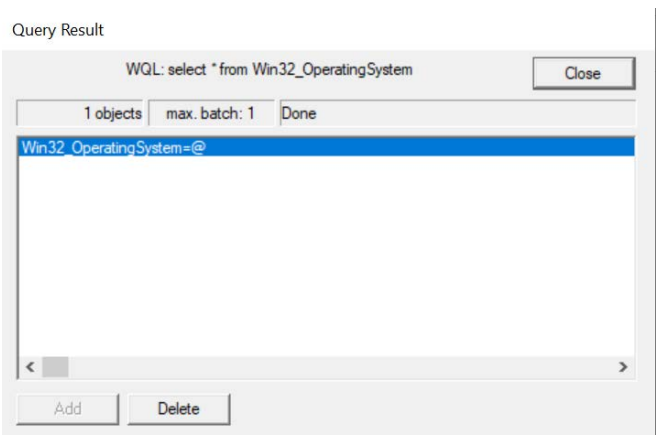

Figure 265. Query Result

8. Double click on the object **Win32_OperatingSystem=@**. Properties of this object will be listed as shown in Figure 266. For example, the property 'Caption' has a value 'Microsoft Windows 10 Enterprise'. The WMI query for this property is successful.

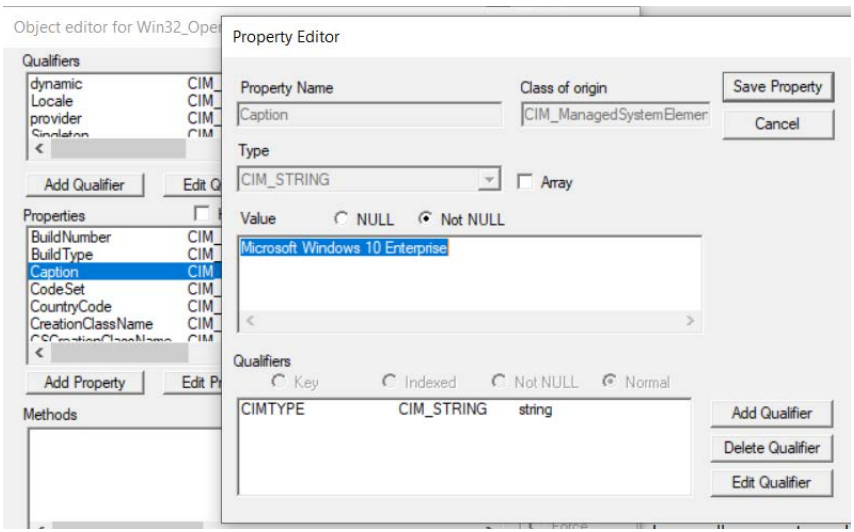

Figure 266. WMI query - OS caption

Appendix G Prerequisite tool

Copy the tools folder from the MCS-DC package to the C:\Temp folder of each computer node in the network. Double-click the file MCS-DC-Prerequisite_Tool.exe to run the tool.

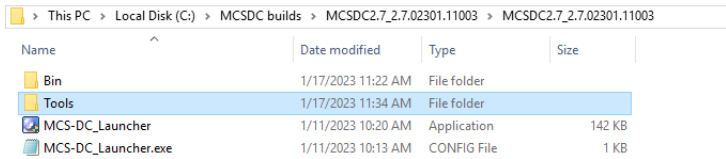

Figure 267. Tools folder

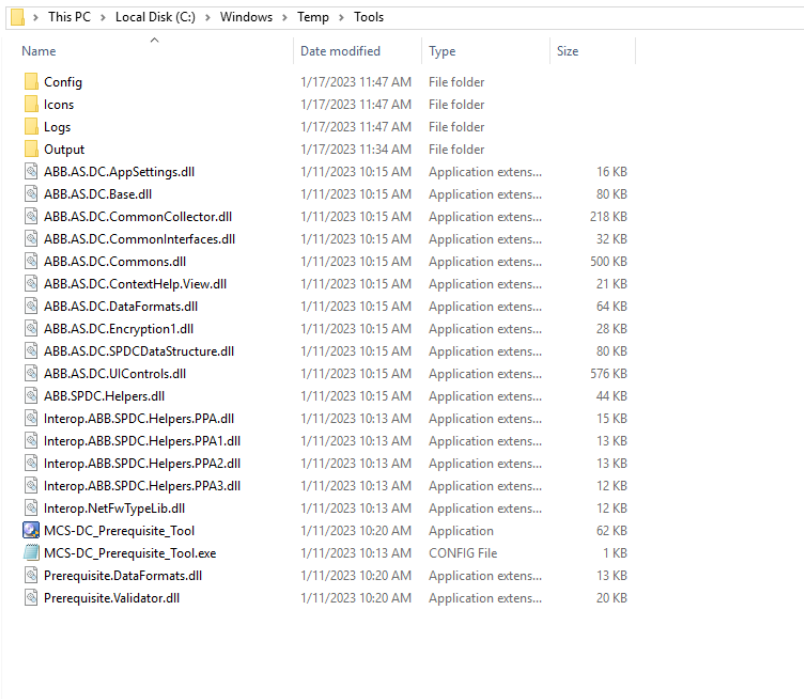

Figure 268. MCS-DC_Prerequisite_Tool

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

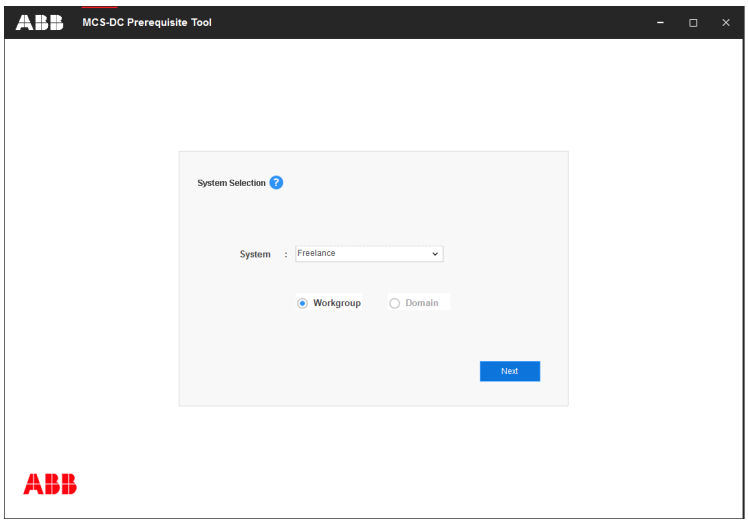

Figure 269. System Selection

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.

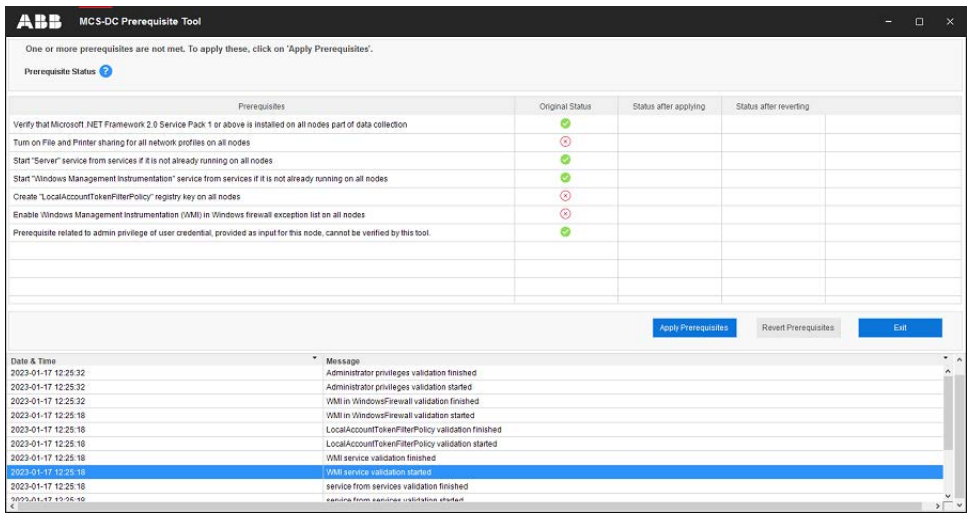

Figure 270. Original status

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 the Section 2.5, Prerequisites to set them manually. Ignore the status of these two prerequisites, shown by the tool. Rest of the prerequisites will work fine.

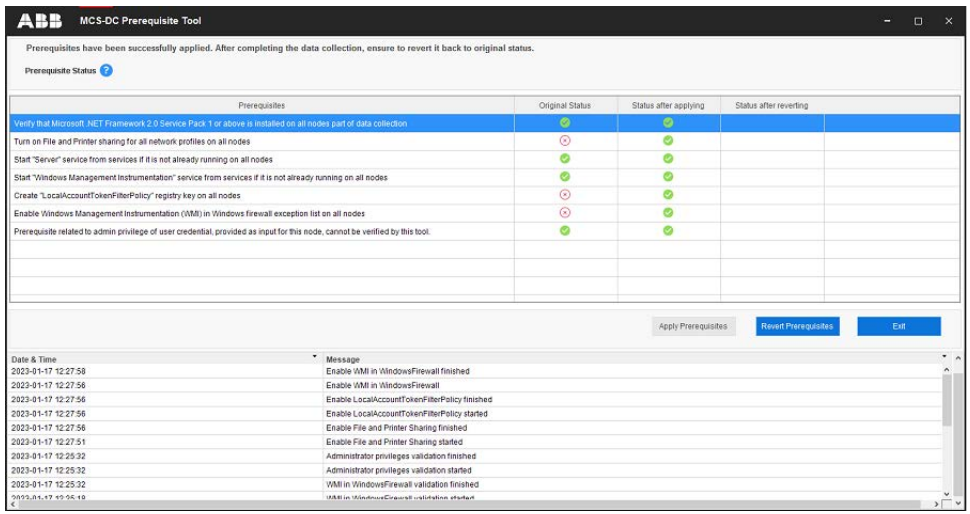

Figure 271. Status after applying prerequisites

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.

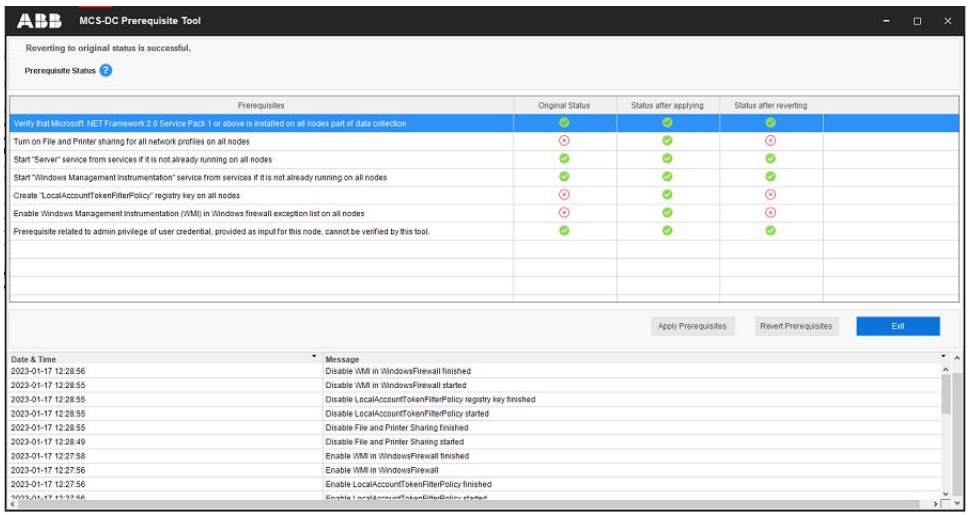

Figure 272. Status after reverting prerequisites

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

Revision History

Introduction

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 2021
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

Updated in Revision Index B

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

Table 3. Updated in Release version 2.0.1

Updated Section/Sub-section	Description of Update
Section 1.2	- 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	- Added Common Prerequisites - Updated Prerequisites for 800xA System - Added Prerequisites for S+ Operations HMI - Added Prerequisites for Harmony Rack - Added Prerequisites for Advant Master with 800xA System - Added Prerequisites for Melody Rack

Table 3. Updated in Release version 2.0.1

Updated Section/Sub-section	Description of Update
Section 3	- Updated Basic Mode data collection process for 800xA HMI - Updated Basic Mode data collection process for Freelance HMI - Added sub section for Basic Mode data collection process for S+ Operations HMI - Updated Advanced Mode data collection process for 800xA HMI - Updated Advanced Mode data collection process for Freelance HMI - Added Support information for Symphony DIN controllers with system 800xA HMI. - Added sub section for Advanced Mode data collection process for S+ Operations HMI. - Added support for Security data collection in S+ Operations system.
Section 4	- Updated Post collection procedure
Appendix	- 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.

Table 4. Updated in Release version 2.0.2

Updated Section/Sub-section	Description of Update
Section 2	- Added Prerequisites for Advant MOD 300 - Added Prerequisites for Procontrol P13 controllers
Section 3	- 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	- Added Appendix C

Updated in Revision Index D

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

Table 5. Updated in Release version 2.1

Updated Section/Sub-section	Description of Update
Section 2	- Added Prerequisites for QCS with 800xA HMI
Section 3	- 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	- Added Appendix D

Updated in Revision Index E

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

Table 6. Updated in Release version 2.2

Updated Section/Sub-section	Description of Update
Section 1	- Supported Systems and Versions
Section 3	- Data Collection process
Section 5	- “chkdsk” issue is removed
Section 2	- Modified .Net framework version - Freelance prerequisite settings for Windows XP client nodes in workgroup
Section 5	- 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.

Table 7. Updated in Release version 2.3

Updated Section/Sub-section	Description of Update
Section 3	- Periodic Data Collection - All Images - Product name change from SPDC to MSC Data collector
Section 5	- 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.

Table 8. Updated in Release version 2.4

Updated Section/Sub-section		Description of Update
Section 1.2	-	Supported Systems and Versions
Section 3.4.1	-	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.

Table 9. Updated in Release version 2.5

Updated Section/Sub-section		Description of Update
Section 2.13	-	Non-ABB System (Security Data collection).
Section 3.4.7	-	Security Data Collection from non-ABB Systems.
	-	Support for QCS with System 800xA HMI version 6.1 SP2.
Section 1.2	-	Supported Systems and Versions.
Section 4	-	Change in collection file name.

Updated in Revision Index I

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

Table 10. Updated in Release version 2.6

Updated Section/Sub-section		Description of Update
Section 3.1	-	Switch option from Basic to Advanced mode data collection.
Section 3.3.1, Section 3.4.1	-	AC800M crash file collection configuration.
Section 3.6	-	ESXi Data Collection
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.

Table 11. Updated in Release version 2.7

Updated Section/Sub-section		Description of Update
Section 1.2	-	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.

Table 12. Updated in Release version 2.8

Updated Section/Sub-section		Description of Update
Section 3.1	-	Parallel data collection of client
	-	AC800M controller collection configuration.

Updated in Revision Index L

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

Table 13. Updated in Release version 2.9

Updated Section/Sub-section	Description of Update
Section 1.2	- Supported Freelance versions. - Supported 800xA versions.
Section 3.1, 3.2	- AC800M controller 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.

Index

A

Advanced mode data collection for 800xA 127
Advanced mode data collection for 800xA HMI 101
Advanced mode data collection for 800xA HMI with Procontrol P13 controllers 128
Advanced mode data collection for 800xA HMI with QCS controllers 130
Advanced mode data collection for S+ Operations HMI with Procontrol P13 206
Advanced mode data collection for S+ Operations with AC800M Controllers 199
Advanced mode data collection for S+ Operations with Harmony controllers 162
Advanced mode data collection for S+ Operations with Melody controller 185
Advanced Mode Data Collection Process for Freelance HMI 145

B

Basic mode data collection for 800xA HMI with AC 70, 110, 160 controllers 70
Basic mode data collection for 800xA HMI with Freelance controllers 71
Basic mode data collection for 800xA HMI with Melody Rack contollers 73
Basic mode data collection for 800xA HMI with MOD 300 controllers 74
Basic mode data collection for 800xA HMI with QCS controllers 75

C

Caution 9
Changing the default Port number 283
Configuring Secured Communication 287, 293, 295, 327

D

Data Collection Process 55
Deleting Firewall Rules 288

I

Introduction 13

P

Post Collection Procedure 255
Prerequisites 19

T

Troubleshooting 263

W

Warning 9

www.abb.com

We reserve the right to make technical changes to the products or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. ABB does not assume any responsibility for any errors or incomplete information in this document.

We reserve all rights to this document and the items and images it contains. The reproduction, disclosure to third parties or the use of the content of this document – including parts thereof – are prohibited without ABB's prior written permission.

Copyright © 2024 ABB.
All rights reserved.

2PAA120980 - 200