



Knowledge Base Articles

DeltaV Data Collector Utility Quick Start Installation and Usage Guide

Article ID: **NK-1100-1172**
Publish Date: **17 Feb 2021**
Article Status: **Approved**
Article Type: **General Product Technical Information**
Required Action: **Information Only**

Recent Article Revision History:

Revision/Publish	Description of Revision
17 Feb 2021	Updated for DDC_5110 link.

(See end of article for a complete revision history listing.)

Affected Products:

Product Line	Category	Device	Version
DeltaV	Workstation Software	VE210x DeltaV Workstation	v9.3.x, v10.3.x, v11.3.x, v11.3.2, v12.3.x, v13.3.x, v14.x

1 Introduction

This Knowledge Base Article, **NK-1100-1172**, provides instructions on how to use the DeltaV Data Collector (DDC) utility. The DeltaV Data Collector utility automatically collects data from a DeltaV system that are typically gathered manually. The collected data can be uploaded to a corresponding CTS call to aid in troubleshooting an issue.

You can use the DDC utility on DeltaV v9.3 or later versions without any negative impact on the system.

2 Downloading the DeltaV Data Collector utility

Download the latest DDC version from this URL:

https://gsuds.emerson.com/pickup/PSG/DDC_5110.zip: (Size: 3449 KB)

Checksum: 0FD1C3A9D1F0BDCD9DC33054DCC3C626DA1140E1DD6C998D0557447914750F56

Always ensure and verify that the integrity of a downloaded file is good by following these guidelines:

1. Download the latest DDC utility only from the link in this KBA.
2. Check that the size of the downloaded file matches the file size noted in the download link.
3. Compare the SHA-256 checksum of the downloaded file with the checksum documented under the download link in this KBA.

Example: Open Windows Powershell and use the command below to compute the SHA-256 checksum of a downloaded **DDC_XXXX.zip** file that is saved in the *C:\Utilities* folder. Compare the Powershell computed checksum with the checksum value documented under the download link and make sure they match.

Get-FileHash "C:\Utilities\DDC_XXXX.zip" -Algorithm SHA256 | Format-List

Important: Customer's enterprise non-DeltaV PCs running McAfee Endpoint Security with the GTI feature enabled, may flag *DDC.exe* as malicious software (Trojan) during an on-demand scan. The McAfee GTI feature allows the scanner to submit and check the reputation of files to an online McAfee GTI server, which may cause certain files to be identified as malware (false positive detection), especially when the GTI sensitivity level is set to High/Very High. This is not an expected result when the DDC utility is scanned on a PC with Endpoint Security for DeltaV systems installed.

DeltaV stations with Endpoint Security for DeltaV Systems have the McAfee GTI feature disabled and do not have online internet connection to the McAfee GTI server. Endpoint Security for DeltaV McAfee antivirus protection is based on the up-to-dateness of the installed AMCore and Exploit Prevention content definition.

The DDC_5110 package updates the DDC to support DeltaV Virtual Studio v3.x.x and SQL query in Windows Server 2016.

For complete information on what the DDC collects from the DeltaV system, refer to the Readme file *DDC5110ReadMe.txt* in the *DDC_5110.zip* file.

3 Running the DDC utility

Important: McAfee Solidcore may block DDC utility when run on DeltaV stations installed with Application Whitelisting for DeltaV Systems.

DeltaV systems with Application Whitelisting for DeltaV version 2.3 or with Application Whitelisting for DeltaV version 1.3 that are already updated with the latest DeltaV Whitelisting Policies and Rule Groups will allow DDC version 5.11.0 to run while the Solidcore is in "Enabled" mode.

However, for DeltaV systems with Application Whitelisting for DeltaV version 1.3 that have not been updated yet, the Solidcore application's mode must be set from "Enabled" to "Update" mode to allow DDC to run on that system.

Refer to KBAs [NK-1600-0044: Application Whitelisting for DeltaV Systems v1.3.x Software Updates](#) and [NK-1800-0832: Application Whitelisting For DeltaV Systems v2.3 Software Updates](#) for the complete details on the respective latest software updates for each application version.

To run DDC and collect the data files, perform these steps:

1. You must be logged on to Windows and DeltaV locally as a user with Administrator privileges.
 2. Copy the DDC zip file into the node relevant to the issue:
 - **Controller-related issues:** ProfessionalPLUS station.
 - **Logic Solver (SLS)-related issues:** ProfessionalPLUS station.
 - **Batch-related issues:** Batch Executive.
 - **Operator Interface-related issues:** Operator Station.
 - **Network-related issues:** Workstation where the Smart Switch module is assigned.
 - **Software Application-related issues:** Application workstation or any node where the issue occurred.
 - **OPC-related issues:** DeltaV node with OPC server.
 - **Virtualization-related issues:** Node where DeltaV Virtual Studio is installed.
-

Note: When the DDC is run for virtualization issues, it will *only* collect virtualization-related information. To collect any DeltaV-related information, run the DDC on the relevant DeltaV node.

For more details, please refer to the Readme file included in the DDC bundle.

Important: Collection of virtualization-related information from a DVS machine with DVS version 3.3.x system is currently not supported by DDC utility. Collection of above mention information must be done manually in the DVS machine. However, DDC utility still supports collection of DeltaV-related information from a virtualized DeltaV machine within DVS v3.3.x system.

3. On the local DeltaV machine, the NIC binding order must be: 1) *DeltaV Secondary*, 2) *Plant LAN*, and 3) *DeltaV Primary*. If there are more than three NICs, refer to KBA [AP-1000-0015: Installation Instructions for Operating Systems Supported on DeltaV Releases](#) for more information about NIC binding settings.
-

Important: The DDC will connect to other nodes, such as controllers and Event Chronicle servers, to collect data.

Do not run multiple instances of the DDC simultaneously on the same system to avoid getting multiple simultaneous connections to these nodes.

4. Confirm that there is at least **8 GB** of free disk space on the root directory, typically drive D.
5. Paste the DDC zip file into the root directory and then check if it is blocked. The DDC zip file might be blocked due to a built-in Windows security feature.

a. To check if the zip file is blocked:

- i. Right-click the **zip file**, and then click **Properties**. On the **General** tab, the **Unblock** button is available if the zip file has been blocked by Windows after the DDC was downloaded. Otherwise, proceed to step 6.

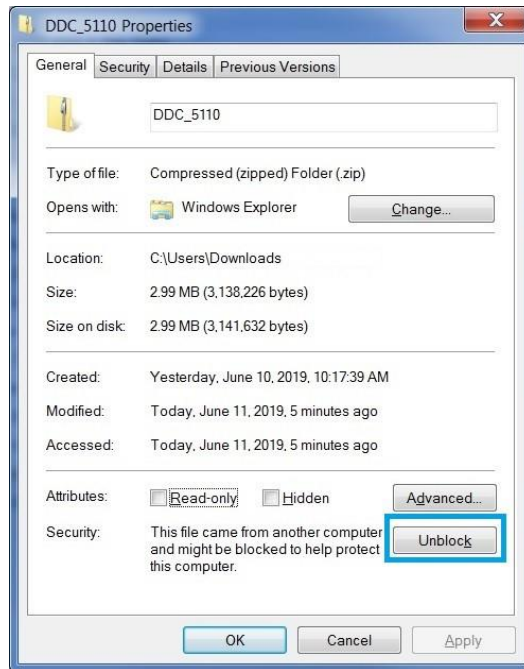


Figure 3-1: Blocked DDC zip file

- ii. To unblock the file, click **Unblock**, and then click **Apply**. The Security option becomes unavailable. Click **OK** to finish unblocking the zip file.

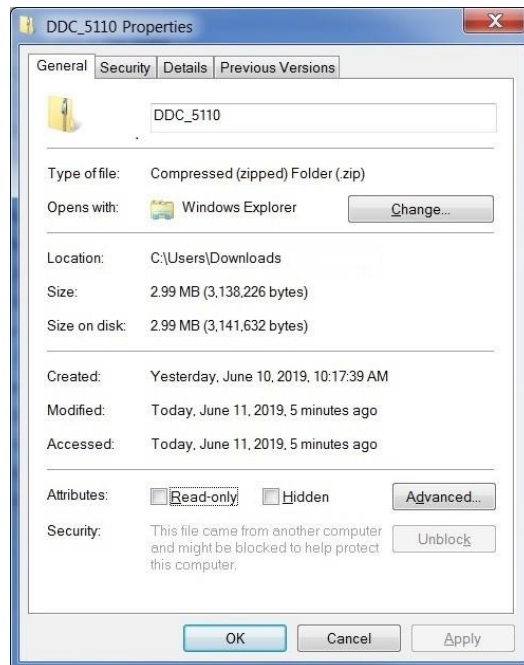


Figure 3-2: Unblocked DDC zip file

6. Extract the DDC zip file in the root directory.

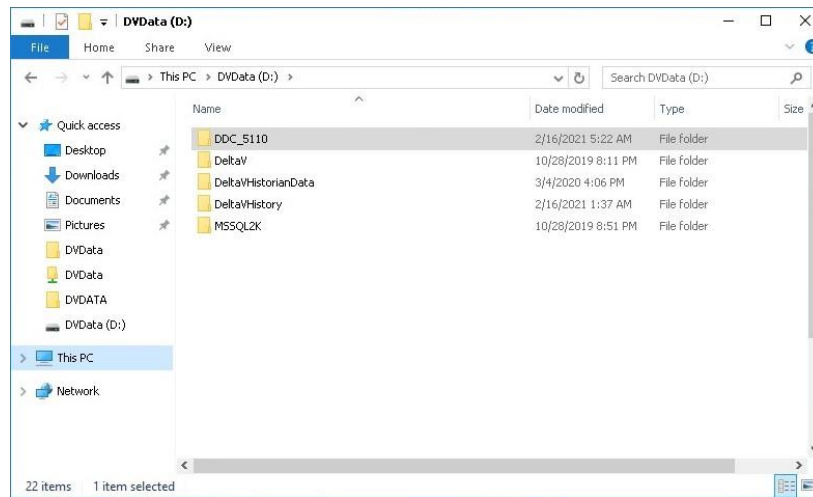


Figure 3-3: DDC folder location

7. Ensure that the System ID is connected to your ProfessionalPLUS machine (or any DeltaV node).

Important: When you run the DDC, the System ID connected to the ProfessionalPLUS machine must be the same System ID used in creating the call on the Guardian website or when contacting the Global Service Center (GSC).

8. Go to the extracted DDC folder, and then double-click **DDC.exe**.

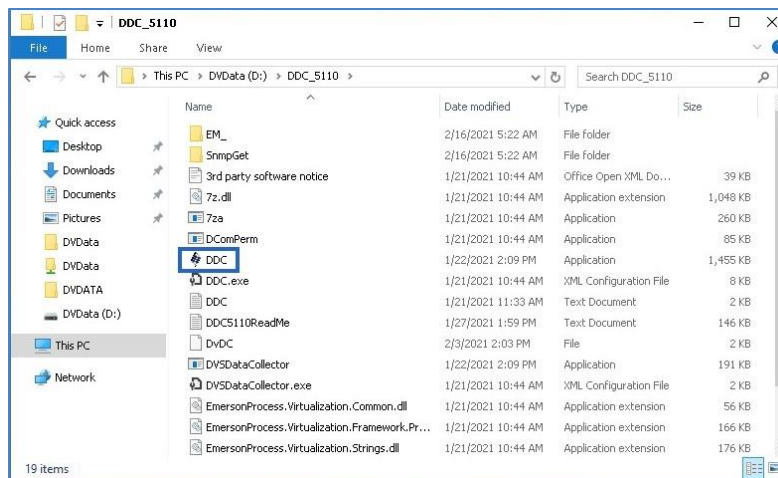


Figure 3-4: DDC.exe

Note: After running *DDC.exe*, the DDC setup wizard might not appear immediately. Verify from Windows Task Manager that *DDC.exe* is running and wait until the DDC setup wizard appears.

9. Security Warnings might appear. Clear the **Always ask before opening this file** check box, and then click **Run**.



Figure 3-5: Security Warning for DDC.exe



Figure 3-6: Security Warning for 7za.exe

- On the DDC Software License Agreement page, confirm the existence of a License Agreement with Emerson, and then click **Next**.

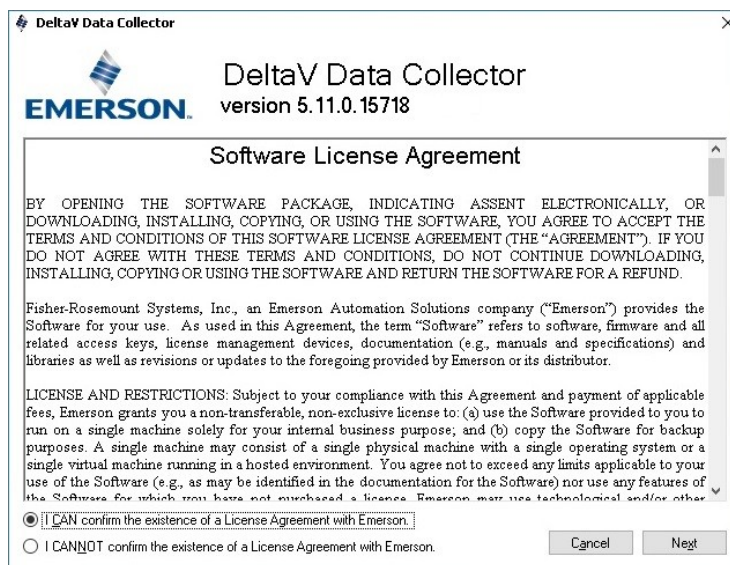


Figure 3-7: DDC Software License Agreement

In DDC version 5.7, *Preconditions and Collection Settings* forms are introduced. These forms initially run before the DDC starts collecting data. In these forms, the DDC checks for execution requirements and users can overwrite the DDC settings.

When running the DDC, the following forms appear:

1. Preconditions

- This form shows the prerequisites to run the DDC:
 - The logged-on user must be a Windows administrator.
 - A dongle or System ID must be installed.
 - The service DeltaV must be running.
- A green check indicates that the precondition is met, while a red cross indicates that it is not met.
- When a precondition is not met, a suggested action is displayed. You can stop the DDC and do the suggested action, and then run the DDC again or continue by clicking **Next**.

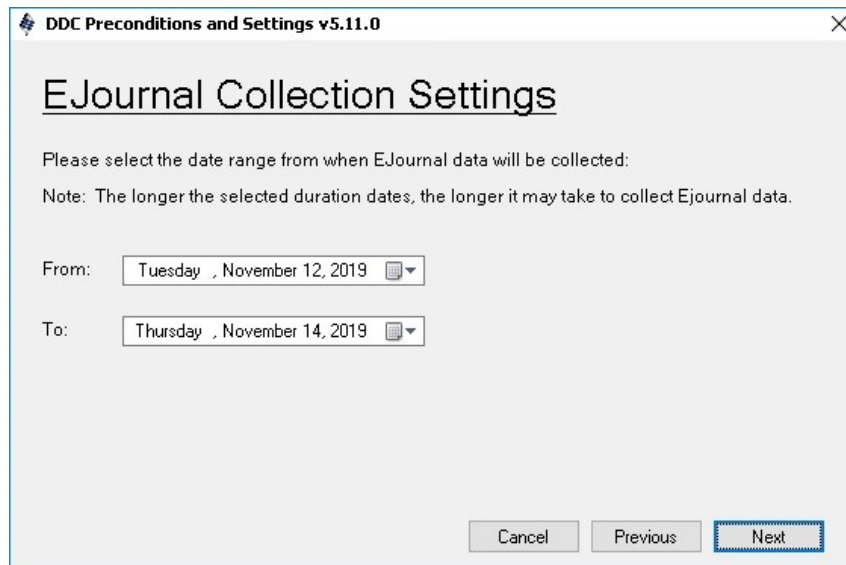
Note: Some files may not be collected if the user continues to run the DDC when a precondition is not met.



Figure 3-8: Preconditions

2. EJournal Collection Settings

- This form contains two date fields, with the default duration of three days from the current date.
- You can select the appropriate date range of the EJournal data to be collected.



DDC Preconditions and Settings v5.11.0

EJournal Collection Settings

Please select the date range from when EJournal data will be collected:
Note: The longer the selected duration dates, the longer it may take to collect Ejournal data.

From:

To:

Figure 3-9: EJournal Collection Settings

3. Batch Collection Settings

- This form contains two date fields, with the default duration of 45 days from the current date.
- You can select the appropriate date range of the Batch files to be collected.
- The DDC will collect Batch files with a Modified Date falling within the given range.



DDC Preconditions and Settings v5.11.0

Batch Collection Settings

Please select the date range from when Batch data will be collected:
Note: Please ignore entry or click Next if system is not Batch otherwise, the longer the selected duration dates, the longer it may take to collect Batch data.

From:

To:

Figure 3-10: Batch Collection Settings

4. Smart Switch Collection Setting

Important: The DDC Utility uses HTTP Access (enabled by default) on Smart Switches to collect switch data and logs. Switch data collection will fail if the HTTP Access is disabled.

A released DeltaV Security Notice (DSN18002-1) recommends disabling the HTTP access to DeltaV Smart Switches if sharing read-only information via the web interface (or using Hirschmann HiView) is a security concern. Emerson is currently exploring a more secure method other than HTTP access for the DDC to collect Smart Switch data.

- In this form, you can choose the credential the DDC will use to collect switch logs.
- If you used a custom account to configure the switch, click the radio button **Use Custom Credential**, and then type the custom account credentials.

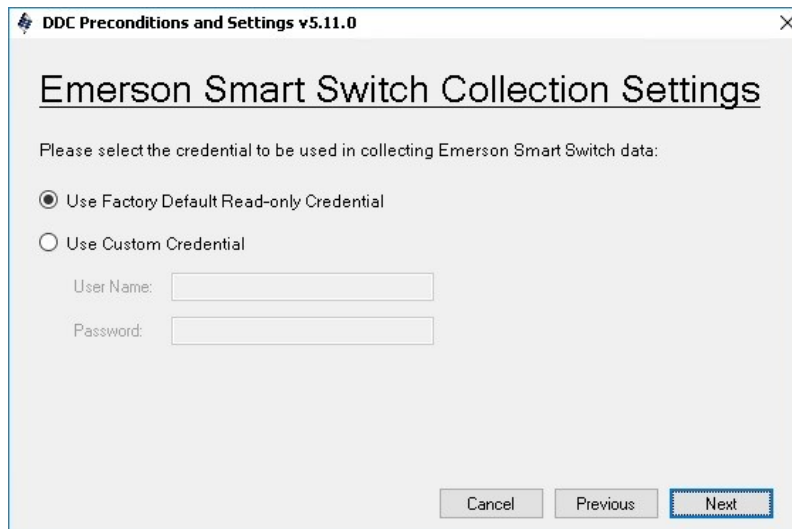


Figure 3-11: Smart Switch Collection Settings

5. Settings Summary

- This form lists the summary of all the preconditions and settings made from the previous forms to inform the user of the settings to be implemented before running the DDC.
- Click **Finish** to start the data collection.

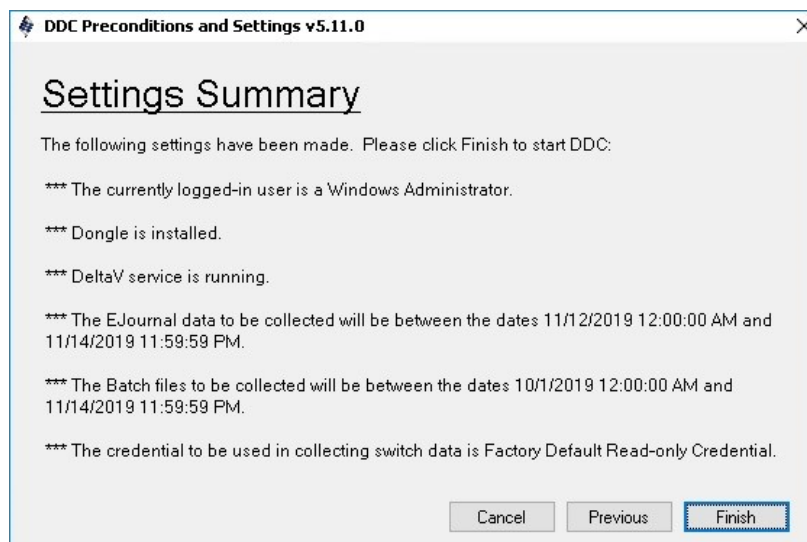


Figure 3-12: Settings Summary

The DDC will automatically check if there is sufficient disk space in the local directory where it is being run. If the partition where the DDC is run is less than 8 GB, the utility will save the output zipped file in the disk that has sufficient space. The drive where the Windows operating system is installed is set to be the least priority.

Once the data has been collected, the DDC will compress the output file automatically and name the zip file in this format: **DDC_Output\DDC_{DV system ID}_ddMMyyyy_HHmmsfff.zip**.

Important: Do not rename the file generated by the DDC.

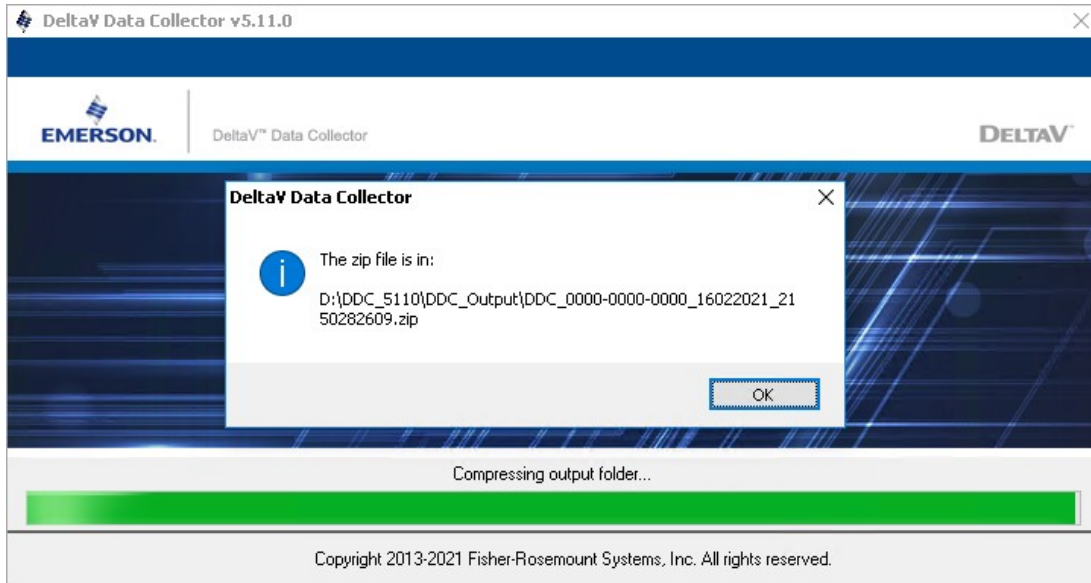


Figure 3-13: Completed data collection and zip file location

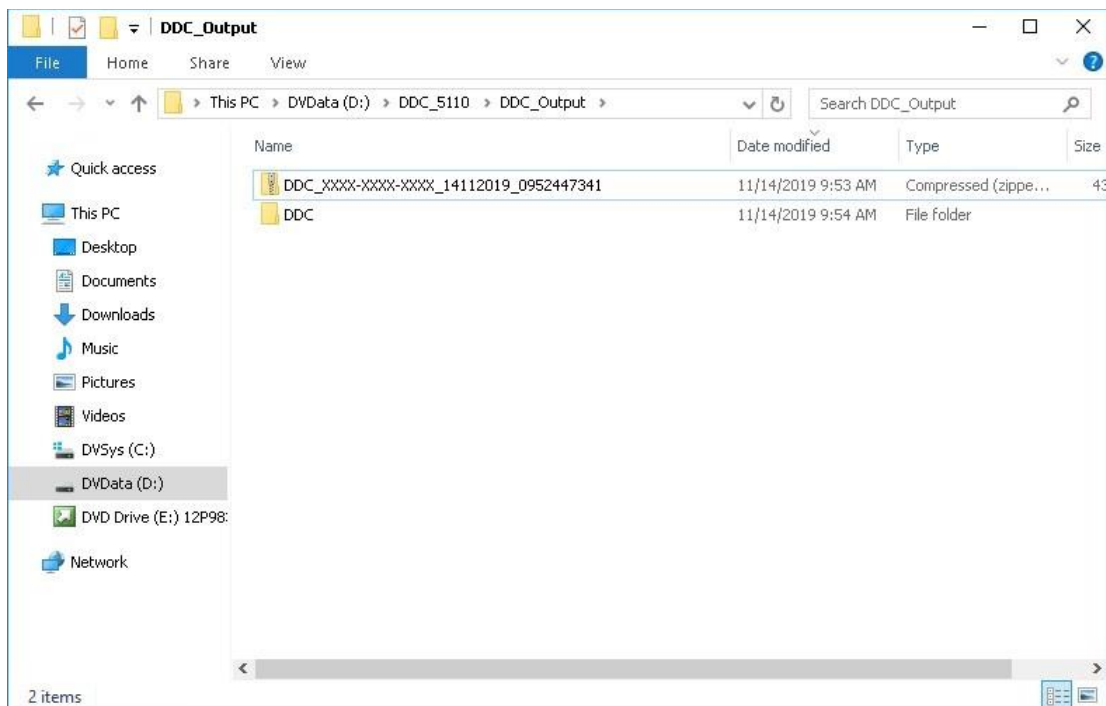


Figure 3-14: Sample DDC output file

4 Generating a Reference ID for the DDC output file

You can generate a Reference ID (formerly called download link) for the DDC output file using the **Emerson File Transfer** web portal. The steps are detailed as follows:

Important: Beginning October 1, 2020, Emerson Large File Transfer website (<https://Emerson.SendThisFile.com/>) has been retired and will no longer be utilized for generating download link for DDC output file

A valid Guardian user account is required to sign-in to the Emerson File Transfer website. If you do not have a valid Guardian user account yet, click the button **Request for new account** on the sign in page of the Emerson File Transfer website.

1. Go to <https://filetransfer.emerson.com>.
2. Sign in using your Guardian user account.

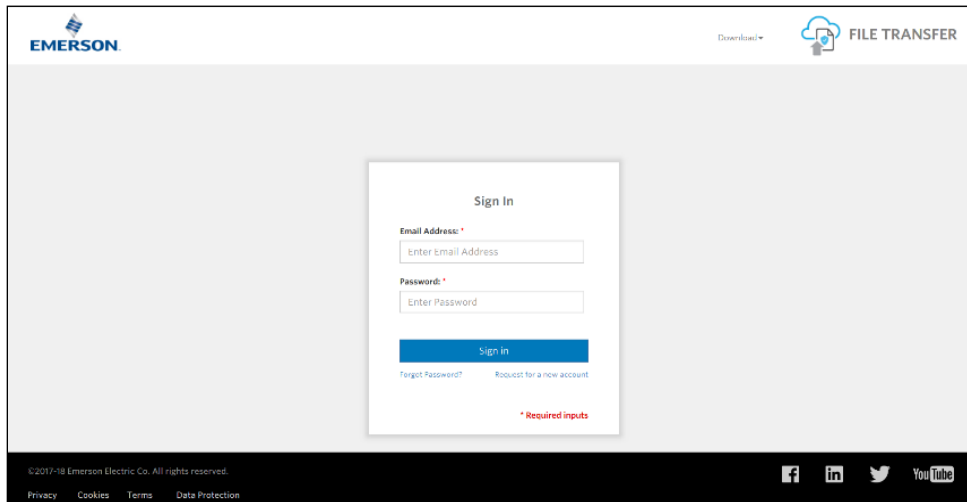


Figure 4-1: Emerson File Transfer sign in page

3. Select the DDC output file to be uploaded using any of the two options:
 - Click the **File Transfer** logo, browse for the DDC output file, and then click **Open**.

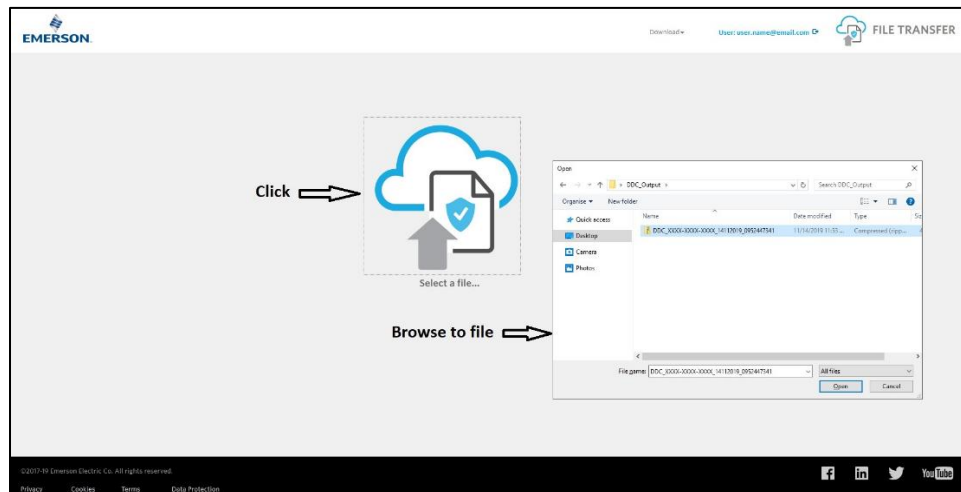


Figure 4-2: Browse to and select the DDC file

- Drag and drop the DDC output file from Windows Explorer to the Emerson File Transfer webpage.

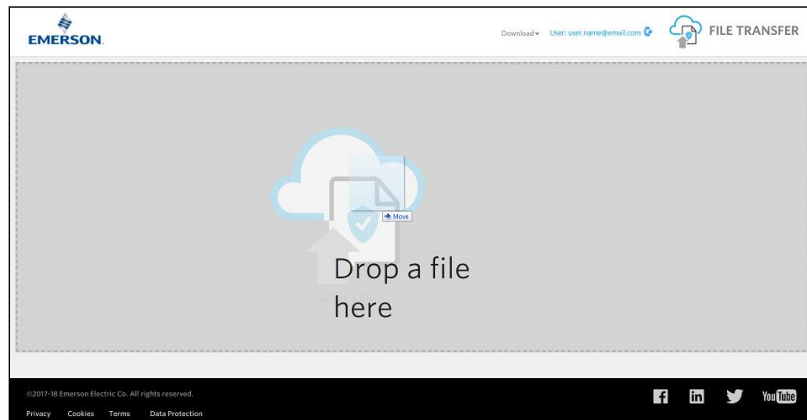


Figure 4-3: Drag and drop the DDC file

4. Click **Upload**.

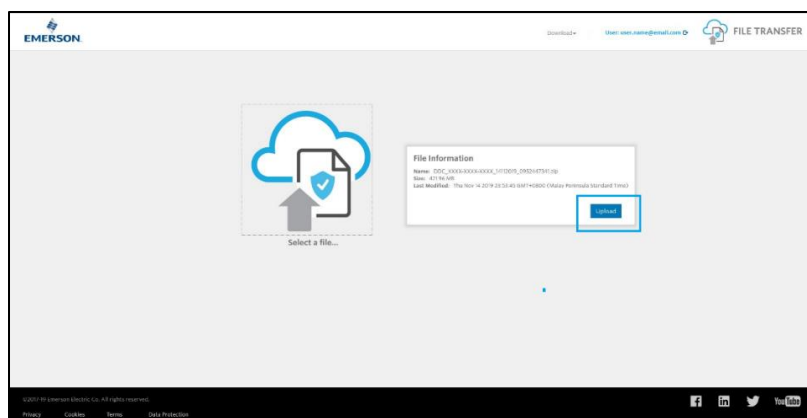


Figure 4-4: Upload the DDC file

Once the upload is completed, a *Reference ID* is generated and displayed in the *File Information* box of the page. Also, an email notification containing the file information including the Reference ID will be sent to the Guardian user's email address.

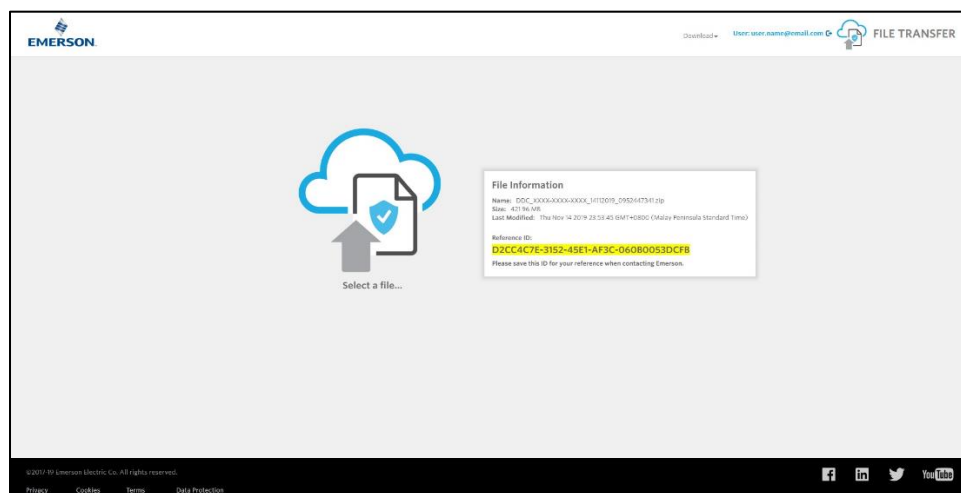


Figure 4-5: Emerson File Transfer Reference ID

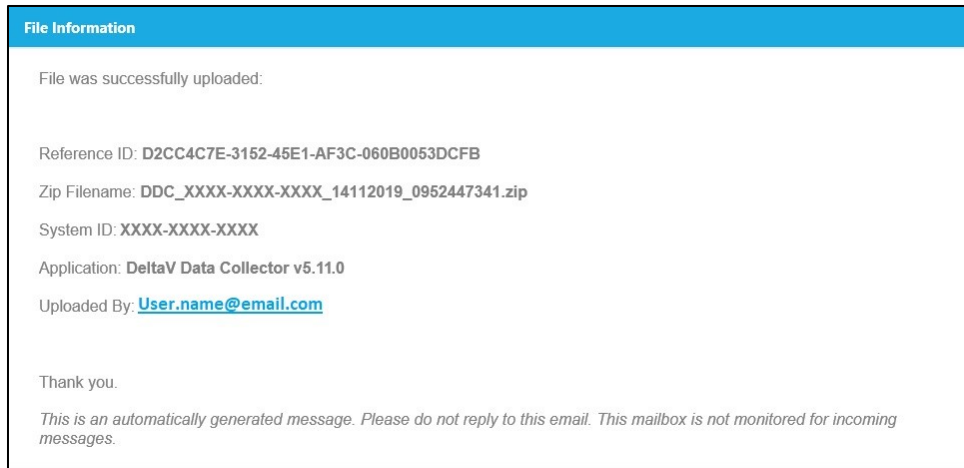


Figure 4-6: Emerson File Transfer email notification

Perform the instructions provided in the **Section 6 Uploading the DDC output file for customers with Guardian Web Access** or if you are already working with GSC engineers, send them the **Reference ID** so they can perform upload of the DDC output file on your behalf.

5 Sending DDC output file through OneDrive shared folder

There may be a scenario where customer may not be able to generate Reference ID and upload DDC file because of he/she has no Guardian account yet or there is an account access issue. Also, there may be an instance where the GSC engineer would need to request a copy of the DDC output file from the customer. In such cases, GSC will be utilizing the Microsoft OneDrive shared folder to request copy of DDC output file. The following are the steps for sending the DDC output file if needed.

1. GSC engineer will request DDC output file by sharing OneDrive folder. Then an email containing the shared folder link will be sent to customer's email address.
2. Once the email is received in the link click **Open**.

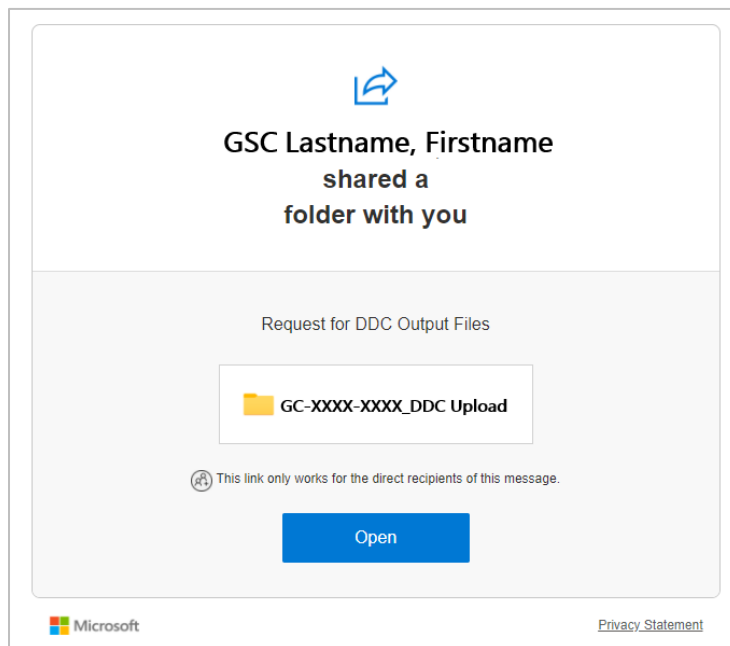


Figure 5-1: OneDrive shared folder link

3. Microsoft will request verification code. Click **Send Code**.

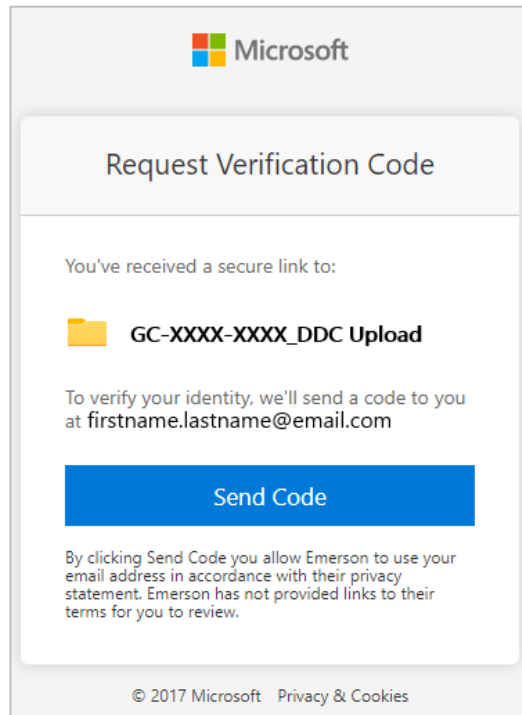


Figure 5-2: Request verification code

4. Microsoft will send the OneDrive verification code to the same email address.

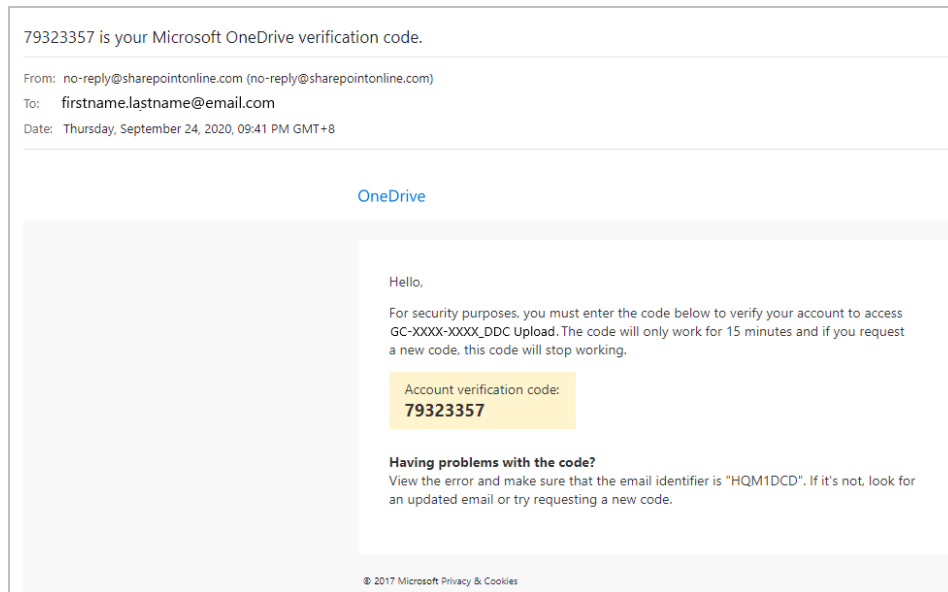


Figure 5-3: Verification code.

Note: The email with the verification code will be sent to the SPAM folder for the first time. Click on the **Not Spam**, if available in the email client application, so to categorize the email as non-spam in the future.

5. Go back to verification window, enter the verification code, and then click **Verify**.

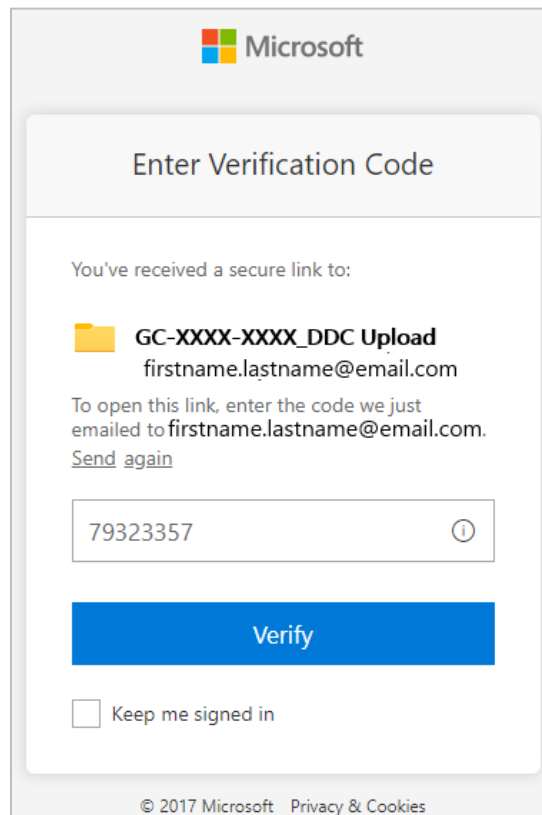


Figure 5-4: Entering verification code.

6. The OneDrive shared folder will open. Click **Upload** and select **Files** then browse to the DDC output file or alternatively drag and drop the DDC output file from windows explorer to the OneDrive Folder.

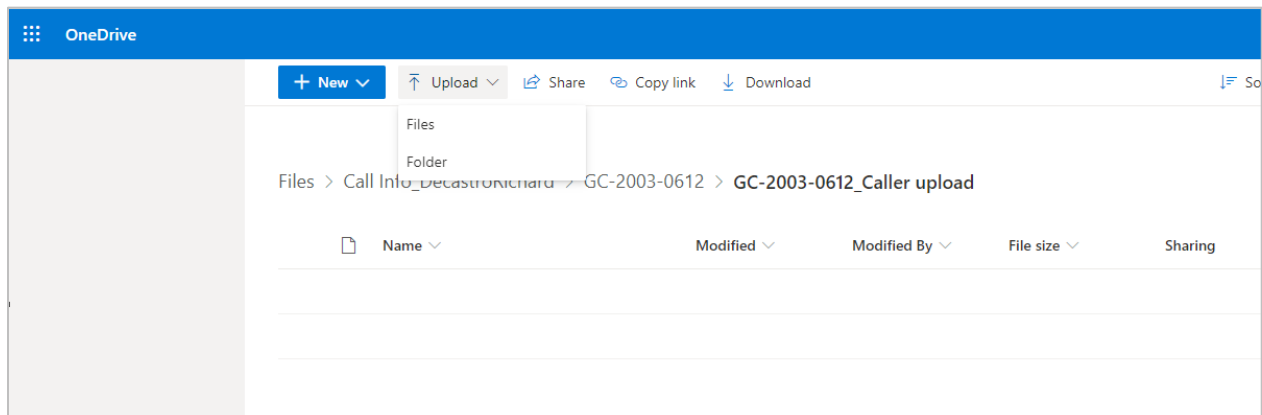


Figure 5-5: OneDrive shared folder

6 Uploading the DDC output file for customers with Guardian Web Access

For Customers with a Guardian Web Access subscription, follow these steps to upload the DDC output file:

1. Sign in to Guardian.
2. Click **Support**.
3. If there is an existing call number and the DDC output file is for that call number, perform steps 3.a–d below. Otherwise, proceed to steps 4–7.

- a. On the **Service Call Logs** tab, open the call number, and then click **Add Call Update**.
- b. On the **Add Call Update** form, type the necessary information.

Figure 6-1: Add Call Update form

- c. In the **Attachments** section, select the check box **Insert DeltaV Data Collector (DDC) download link(s)**, and then paste the *Reference ID* into the entry box.
- d. Click **Save** to save the **Add Call Update**, and then click **Close**.

Figure 6-2: Successful Add Call Update

4. On the **New Service Call** tab, on the **Service Call Form**, type the necessary information.
5. In the **Attachments** section, select the check box **Insert DeltaV Data Collector (DDC) download link(s)**, and then paste the Reference ID generated from the Emerson File Transfer web portal into the entry box (see **Figure 4-5** and **Figure 4-6**).

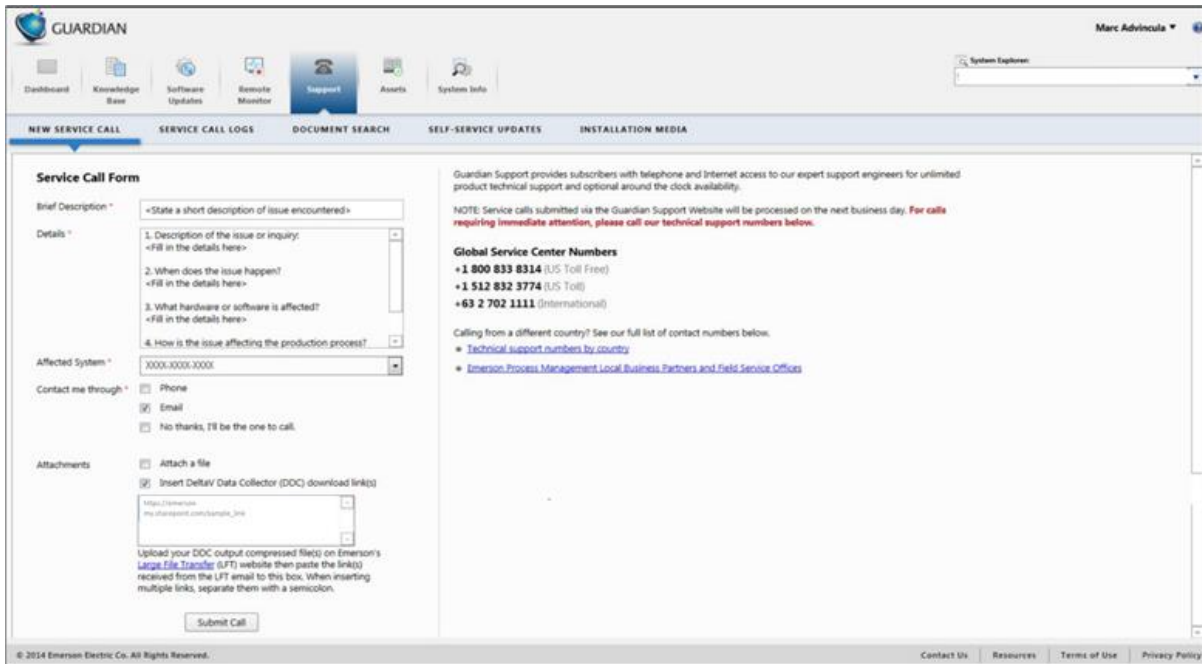


Figure 6-3: Guardian Service Call Form

6. Click **Submit Call**. The **Call Details** window will appear and show a summary of the logged call.

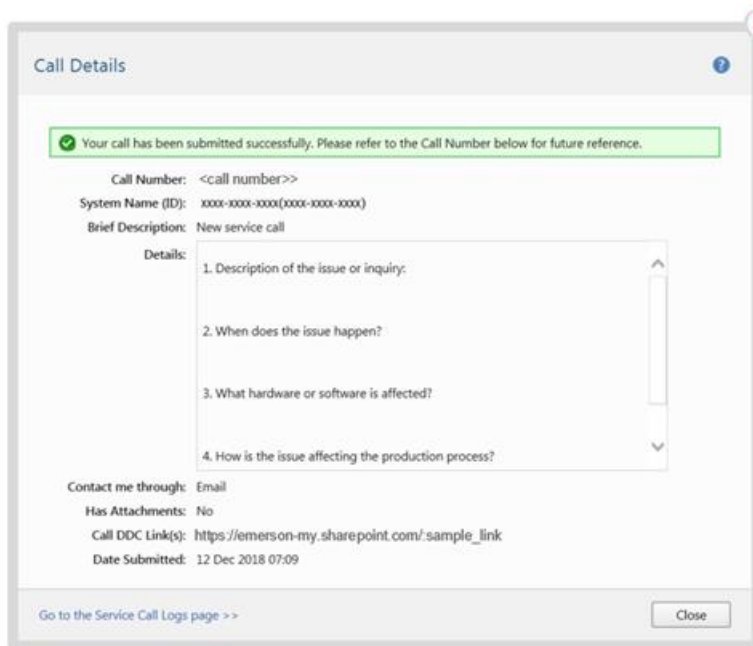


Figure 6-4: Call Details window

7. Take note of the Call Number for your reference. Click **Close**.

GSC Engineers will contact the sender regarding the initial data analysis and additional queries regarding the call.

Contact Information

Services are delivered through our global services network. To contact your Emerson local service provider, click [Contact Us](#). To contact the Global Service Center, click [Technical Support](#).

[Download the Sigcheck tool: Click This Link](#)

[To get information on how to use the Sigcheck tool: Click This Link](#)

Related products and services: [DeltaV DCS](#) | [Lifecycle Services](#)

Complete Article Revision History:

Revision/Publish	Description of Revision
17 Feb 2021	Updated for DDC_5110 link.
27 Oct 2020	Added an important note in Section 2. Included procedure on how to check file integrity of files downloaded from the KBA. Moved the Solidcore note to Section 3
02 Oct 2020	Updated Section 4, 5 and added Section 6 in reference to removal of retired Emerson SendThisFile system and added procedure using OneDrive Shared folder. Reviewed and applicable to DeltaV v14.FP1
07 May 2020	Added important note in section 3.1
13 Jan 2020	Updated important note in section 2 about McAfee Application Whitelisting (SolidCore)
18 Nov 2019	Updated for DDC 5101 link.
05 Aug 2019	Updated for DDC_5100. Reviewed and determined applicable for DeltaV v14.3.1
20 Dec 2018	Updated for DDC_590
02 Nov 2018	Updated for DDC_581
19 Jul 2018	Updated the link and information for DDC_580_2 package.
26 Jun 2018	Added Note in Step 10-d (Smart Switch Collection Settings).
04 Jun 2018	Updated with new version of DDC_580
24 Apr 2018	Reviewed and determined applicable for DeltaV v14.3
04 Jan 2018	Modified the steps to include information on how to send the DDC file to the Large File Transfer site
14 Nov 2017	Screenshots updated to reflect new version.
18 Jul 2017	Updated to DDC_572B; Resolved RegistryExport collection issue.
05 May 2017	Updated for DDC_572
20 Dec 2016	Reviewed and determined applicable to v13.3.1
28 Oct 2016	Updated for DDC_564
07 Jul 2016	Updated for DDC_563
29 Apr 2016	Updated for DDC_562
31 Mar 2016	Updated for DDC_561
02 Mar 2016	Added a note for DeltaV systems with McAfee on Page 1
27 Jan 2016	Minor formatting change.
05 Oct 2015	Updated for DDC_552 to collect additional items and parameters for DVOP, DeltaV Logbooks and DIR dumps
02 Sep 2015	Added a Note on procedure "For Customers with Guardian web access". Added checksum code.
10 Jul 2015	Updated for DDC_551
15 May 2015	Updated the link and information for DDC_541
20 Mar 2015	Updated the link and information for DDC v531.
26 Feb 2015	Modify DDC functionality statement
25 Feb 2015	Revised DDC functional details
25 Feb 2015	Updated DDC utility description and functionality.
20 Feb 2015	Updated for DDC_523
16 Jan 2015	Updated for DDC_522
11 Dec 2014	Updated for DDC v5.2.1
10 Oct 2014	Update for DDC v5.1.2 version, added collection parameters for Network Validation Tool and

25 Sep 2014	support for DeltaV systems with Wireless Gateway 1420
16 Sep 2014	Updated for DDC utility v5.1.1 version
21 Feb 2014	Updated for the latest version of DDC utility.
08 Dec 2011	Updated for the new version of the utility.
21 Nov 2011	Removed 7-Zip archive utility from DDC bundle.
	Original release of article

©Emerson Automation Solutions 2009-2021. All rights reserved. For Emerson Automation Solutions trademarks and service marks, [click this link to see trademarks](#). All other marks are properties of their respective owners. The contents of this publication are presented for informational purposes only, and while diligent effort has been made to ensure their accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available on request. We reserve the right to modify or improve the design or specification of such products at any time without notice.

[View Emerson Products and Services: Click This Link](#)