

Exceptional service in the national interest



Sandia
National
Laboratories

COMMON User Manual

Version 1.5

March 11, 2019



Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Acronyms

CAS	central alarm station
CPU	central processing unit
CSV	comma-separated values
DOE	Department of Energy
GB	gigabyte
IP	internet protocol
JSON	JavaScript Object Notation
MB	megabyte
NIC	network interface controller
NNSA	National Nuclear Security Administration
NSDD	Nuclear Smuggling Detection and Deterrence
PDF	portable document format
RAM	random access memory
RDS	radiation detection system
RPM	radiation portal monitor
SMART	self-monitoring, analysis and reporting technology
UPS	uninterruptable power supply

Table of Contents

Acronyms.....	i
Introduction—The Need for COMMON.....	5
1. Starting and Exiting COMMON.....	6
2. The COMMON User Interface.....	7
3. Home	8
3.1 Alerts	9
3.2 Status	11
4. Devices	12
4.1 CPU	13
4.2 Memory	14
4.3 Disk	15
4.4 Disk Performance.....	16
4.5 Network Interface.....	17
4.6 Running Services.....	18
4.7 Database	19
4.8 Processes	20
4.9 Installed Applications.....	21
4.10 UPS	22
4.11 Event Log Errors—System	23
4.12 Event Log Errors—Applications.....	24
5. Reports.....	25
5.1 Site Report.....	26
5.2 Server Report.....	27
5.3 Network Report	30
5.4 CAS Load Report.....	31
5.5 Issues Report	33
5.6 Site Configuration Report	34

6.	Site Name Tab.....	37
6.1	Help	38
6.2	About.....	39
6.3	Data Collection.....	40
6.4	Network History	41

Figures

Figure 1.	COMMON Tool Menu Bar.....	7
Figure 2.	COMMON Tool Home Page.....	8
Figure 3.	COMMON Tool Home Page, Alerts Window.....	9
Figure 4.	COMMON Tool Home Page, Status Window Displaying Summary Information.	11
Figure 5.	COMMON Tool Devices Page.....	12
Figure 6.	COMMON Tool Devices Page, CPU Usage Window.....	13
Figure 7.	COMMON Tool Devices Page, Memory Usage Window.....	14
Figure 8.	COMMON Tool Devices Page, Hard Disk Usage Window.....	15
Figure 9.	COMMON Tool Devices Page, Hard Disk Usage Window, SMART Information.	15
Figure 10.	COMMON Tool Devices Page, Disk Performance Window.	16
Figure 11.	COMMON Tool Devices Page, Network Interface Window.	17
Figure 12.	COMMON Tool Devices Page, Running Services Window.	18
Figure 13.	COMMON Tool Devices Page, Database Information Window.....	19
Figure 14.	COMMON Tool Devices Page, Database Information Window, Database Size Over Time.....	19
Figure 15.	COMMON Tool Devices Page, Processes Window.....	20
Figure 16.	COMMON Tool Devices Page, Processes CPU Usage Window.	20
Figure 17.	COMMON Tool Devices Page, Installed Applications Window.	21
Figure 18.	COMMON Tool Devices Page, Installed Applications History.....	21
Figure 19:	COMMON Tool Devices Page, UPS Window.	22
Figure 20.	COMMON Tool Devices Page, Event Log Errors—System Window.....	23

Figure 21. COMMON Tool Devices Page, Event Log Errors—Applications Window	24
Figure 22. COMMON Tool Reports Tab, Drop-Down Menu.	25
Figure 23. COMMON Tool Reports Page, Site Report Window.....	26
Figure 24. COMMON Tool Reports Page, Server Report Window.....	27
Figure 25. COMMON Tool Reports Page, Network Report Window.....	30
Figure 26. COMMON Tool Reports Page, CAS Load Report Window.....	31
Figure 27. COMMON Tool Reports Page, Site Configuration Report Window.	34
Figure 28. COMMON Site Name Tab, Drop-Down Menu.	37
Figure 29. COMMON Tool Site Name Page, Help Window.....	38
Figure 30. COMMON Tool Site Name Page, About Window.....	39
Figure 31. COMMON Tool Site Name Page, Data Collection Window.	40
Figure 32. COMMON Tool Site Name Page, Network History Window.....	41

Introduction—The Need for COMMON

The largest component in a radiation detection system (RDS) is the communications system which integrates all RDS sensors and systems and allows operators to adjudicate alarms. COMMON was developed to provide the operational status of RDS sensors and systems by collecting data on system performance and alerting users to potential issues that might hinder radiation portal monitor (RPM) data collection and the National Nuclear Security Administration's (NSDD's) ability to collect, store, and analyze the considerable amounts of data from RPMs deployed at partner countries' sites.

COMMON is an optional software tool that is *common* to all NSDD communications systems, regardless of system type, operating system, or solution vendor.

Local maintenance providers or system administrators who are responsible for the overall health and upkeep of an RDS can use COMMON to collect information needed to perform regular site visits or to resolve problems at the request of site officials. Site officials who work for the government agencies responsible for RDSs can use COMMON to obtain high-level information on system performance and status. Country team members and NSDD subject matter experts (the U.S.-based individuals who help countries operate RDSs) can use COMMON to identify historical trends in system operation. The tool comes with an installer to make it easily deployed by anyone with administrator access to the system and runs on the main RDS workstations and/or servers.

This manual is intended primarily for end users, local maintenance providers, and system administrators. This manual includes screen captures from a test system called "COMMON Test Lab" at Sandia National Laboratories that simulates a hypothetical RDS installation. No similarity to an actual system is implied.

1. Starting and Exiting COMMON

Once COMMON is installed and configured (refer to the separate COMMON Installation and Configuration Guide) the tool is started by opening an Internet browser and entering the IP address for the COMMON interface as deployed on the specific RDS.

TIPS: The COMMON installer will place a shortcut to COMMON on the desktop. COMMON supports Microsoft Internet Explorer 11 and higher and Google Chrome version 70.0.3538 and higher.

***COMMON supports Microsoft Internet Explorer 11 and higher
and Google Chrome version 70.0.3538 and higher.***

2. The COMMON User Interface

The COMMON user interface displays and reports the status of the user's RDS devices through pages sharing a single menu bar (see Figure 1). The menu bar allows users to easily access the following:

- **HOME** presents the most critical information COMMON collects on the communications system and is the main COMMON screen.
- **DEVICES** is an alternate means to access operating status information of individual RDS devices displayed on the HOME page.
- The COMMON tool also provides **REPORTS** to view and download information on system components for troubleshooting and repair systems issues.
- **LANGUAGE** will be visible if multiple languages have been enabled, allowing the COMMON user interface to be translated into an alternate language.
- Finally, **TESTBED** (usually a Site Name) accesses a drop-down menu to Data Collection and Network History. The tab also accesses the HELP page, which includes the email address for COMMON tool assistance and the COMMON User's Manual in portable document format (PDF), and an ABOUT page which provides background information on COMMON tool development and links.



Figure 1. COMMON Tool Menu Bar.

The menu bar collapses to a button with drop-down options if the browser window is too narrow to display the entire bar.

3. Home

COMMON opens on the HOME page and presents the most critical information COMMON collects on the communications system in two windows (Figure 2):

- ALERTS window provides an indicator of devices which require attention
- STATUS window provides details on operational device status

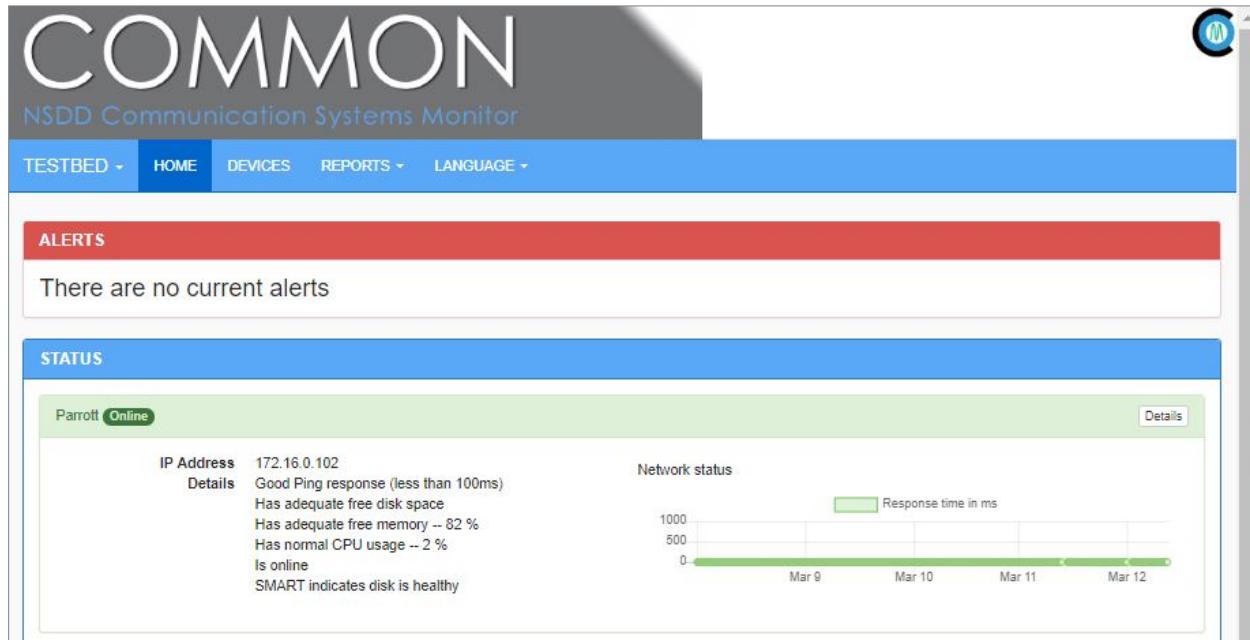


Figure 2. COMMON Tool Home Page.

- The **Details** button links to comprehensive information on a device's status by linking to the appropriate device page.

3.1 Alerts

The ALERTS window displays messages on the status of devices in a communications system which require immediate attention from the system administrator or local maintenance provider (Figure 3).



Figure 3. COMMON Tool Home Page, Alerts Window.

- Clicking on the device alert displays comprehensive information on a device's status by linking to the appropriate device page.

Alert status messages include:

Device Alert	Description	Allowed Values	Default Value
Excessive CPU usage	Percentage that CPU usage over time must exceed to generate an alert.	Between 0 and 100	75
Low on disk space	Percentage of hard disk space that must be used to generate an alert.	Between 0 and 100	80
Critically low on disk space	Percentage of hard disk space that must be used to generate a critical on disk space alert. This number should be higher than the value for "Low on disk space" alert.	Between 0 and 100	90
Low on free memory	Percentage of RAM space that must be used to generate an alert.	Between 0 and 100	80
Critically low on free memory	Percentage of RAM space that must be used to generate a critical on free memory alert. This number should be higher than the value for "Low on free memory" alert.	Between 0 and 100	90
Not recently rebooted	Number of days within which a system reboot will generate an alert that the system has not recently rebooted.	Number greater than 1	365

Device Alert	Description	Allowed Values	Default Value
Slow ping response times	The ping response time in milliseconds that a system ping must exceed to generate an alert.	Equal to, or more than, 500 milliseconds (ms)	
Is offline	Anytime a device configured on the COMMON tool is offline.	Not applicable	Not applicable
No current alerts	There are no devices with an alert.		

The device's alert thresholds are determined by the COMMON installer when COMMON is configured (refer to the separate COMMON Installation and Configuration Guide).

3.2 Status

This window gives a high-level overview of device status (Figure 4) and provides summary information on the following:

- IP Address (for all devices except the server COMMON is running on)
- Whether the device has adequate free disk space
- Whether the device has adequate free memory
- Has been recently rebooted
- Whether the device has normal central processing unit (CPU) usage
- And when appropriate, SMART¹ indication of disk health
- The device will display on a green background bar if the device is online and working within parameters configured by the COMMON installer, a red background bar if the device requires attention.
- Graph of Network status, ping response time in milliseconds (ms).

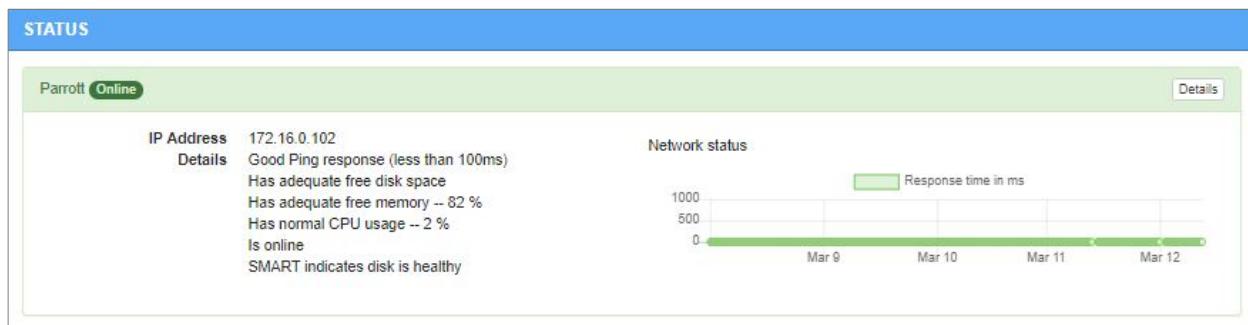


Figure 4. COMMON Tool Home Page, Status Window Displaying Summary Information.

- The **Details** button links to comprehensive information on a device's status by linking to the appropriate device page.

Settings for status thresholds are determined by the COMMON installer when COMMON is configured (refer to the separate COMMON Installation and Configuration Guide).

¹ Self-monitoring, analysis and reporting technology (SMART) monitoring system included in newer computer hard disk drives that detects possible drive failures.

4. Devices

The DEVICES tab on the menu bar provides a slide out list of devices, by individual device and by groups, as configured in COMMON. Each device (or group) page displays the device name, date and time of the device's last reboot, and current uptime in days, hours, minutes, and seconds (Figure 5).

- Beneath the device's window is a drop-down menu button labeled “Days to Retrieve” that allows users to select the number of days of device data to retrieve and display. Options include 15, 30, 60, 90, 120, 150, and 180 days.
- Each device page has an ALERTS window that displays information on issues that may indicate problems with the device and is the same ALERT message displayed on the HOME page.
- Beneath the ALERTS window are sub-sections that display comprehensive information on device status and performance, including CPU usage, memory usage, disk usage, disk performance, network interface usage, current database information, running processes, running services, installed applications, and event log errors for system and application. These windows are explained in detail below.

COMMON
NSDD Communication Systems Monitor

TESTBED ▾ HOME DEVICES REPORTS ▾ LANGUAGE ▾

Server

Last boot time: 2018-11-06 12:41:36
Uptime: 40 days, 20:48:49

ALERTS

IS LOW ON FREE MEMORY -- 20%
IS CRITICALLY LOW ON FREE DISK SPACE -- D: -- 96.5 %

CPU

Last Update: 2018-12-17 11:30:20
Current Usage: 2.0 %
Peak Usage: 89.0 % at 2018-11-28 13:25:47

CPU Usage Over Time

MEMORY

Last Update: 2018-12-17 11:30:20
Current Usage: 12.80 GB (80.4 %)
Current Free: 3.12 GB
Peak Usage: 14.34 GB (90.1 %) at 2018-11-28 13:25:46
Total Capacity: 15.92 GB

Days to Retrieve: 30 ▾

10
20
30
60
90
120
150
180

Figure 5. COMMON Tool Devices Page.

4.1 CPU

The CPU window displays the device's current processor usage as a percentage of total processor capacity not just CPU capacity used by COMMON and other RDS-related software (Figure 6).

- The CPU window displays date and time of last update, percentage of current CPU usage, percentage of peak usage as well as date and time of peak usage.
- The CPU window displays information on CPU usage over time in graph form. The vertical axis indicates total CPU capacity as a percentage. The horizontal axis indicates the month and day spanning the 15- to 180-day window of “Days to Retrieve” that was chosen at the top of the device’s page.
 - Hovering the cursor over a point on the graph provides date, time, and percentage of CPU usage at that reading.

By default, the graph displays the same number of days of data as indicated in the drop-down of “Days to Retrieve” at the top of the device’s page.

- To temporarily graph additional days of CPU usage, click on **Retrieve More Days**.

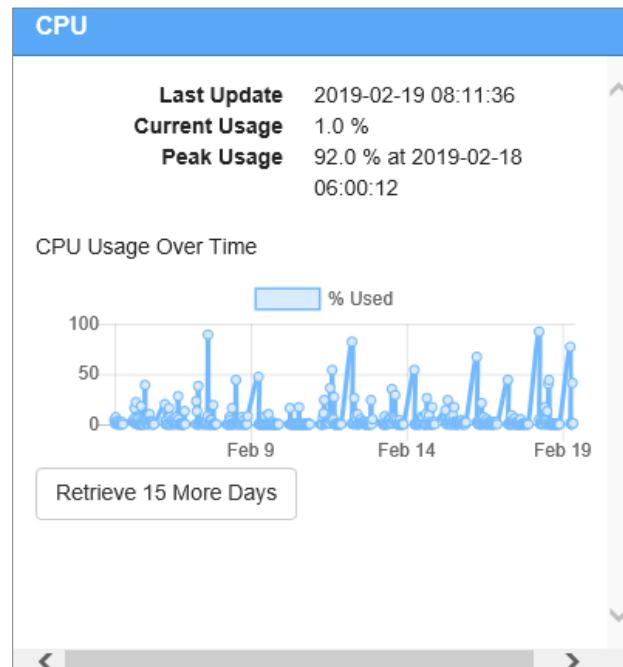


Figure 6. COMMON Tool Devices Page, CPU Usage Window.

4.2 Memory

The MEMORY window displays the selected device's current random-access memory (RAM) usage as a percentage of total installed RAM over time, not just RAM used by COMMON and other RDS-related software (Figure 7).

- The MEMORY window displays date and time of the last update on memory usage percentage, total memory used in gigabytes (GB) and percent, free memory in GB, peak usage of memory in GB (and percent) with time and date of that peak usage and provides the device's total memory capacity in GB.
- The MEMORY window provides a graphed display of memory use in GB over time. The vertical axis shows total system memory in GB. The horizontal axis indicates the month and day spanning the 15- to 180-day window of “Days to Retrieve” that was chosen at the top of the device’s page.
 - Hovering the cursor over a point on the graph provides date and time of the data point and the memory in GB used at that reading.

By default, the graph displays the same number of days of data as indicated in the drop-down of “Days to Retrieve” at the top of the device’s page.

- To temporarily graph additional days of memory usage, click on **Retrieve More Days**.

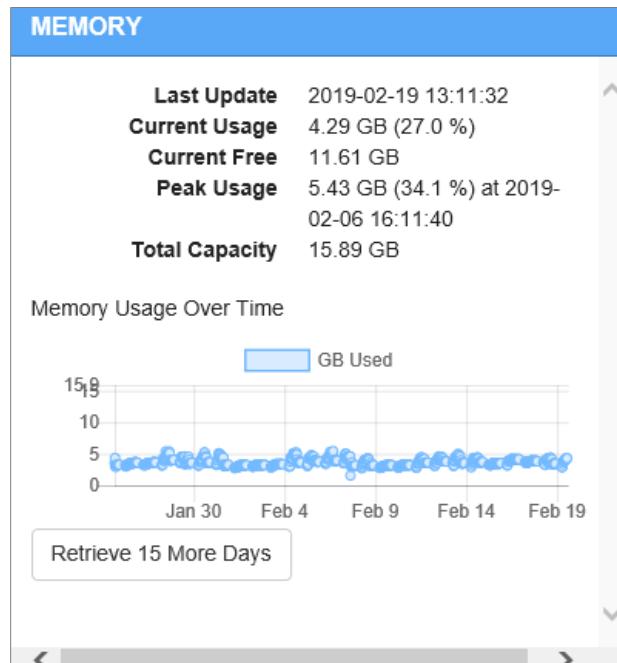


Figure 7. COMMON Tool Devices Page, Memory Usage Window.

4.3 Disk

The DISK window displays the device's current hard disk space usage as a percentage of total hard disk capacity not just hard disk space used by COMMON and other RDS-related software. The DISK window will have tabs for each device hard disk drive configured in COMMON (Figure 8).

- The DISK window displays date and time of the last update on the hard disk space usage percentage, total hard disk space used in gigabytes (GB) and percent, free hard disk space in GB, peak usage of hard disk space in GB (and percent) with time and date of that peak usage and provides the device's total hard disk space capacity in GB.
- The DISK window provides a graphed display of hard disk space use over time. The vertical axis shows total system hard disk space in GB. The horizontal axis indicates the month and day spanning the 15- to 180-day window of "Days to Retrieve" that was chosen at the top of the device's page.
 - Hovering the cursor over a point on the graph provides the date and time of the data point and the hard disk space in GB used at that reading.

By default, the graph displays the same number of days of data as indicated in the drop-down of "Days to Retrieve" at the top of the device's page.

- To temporarily graph additional days of disk space usage, click on **Retrieve More Days**.
- A SMART information window is available by clicking "Show SMART Data for C:" (Figure 9).



Figure 8. COMMON Tool Devices Page, Hard Disk Usage Window.

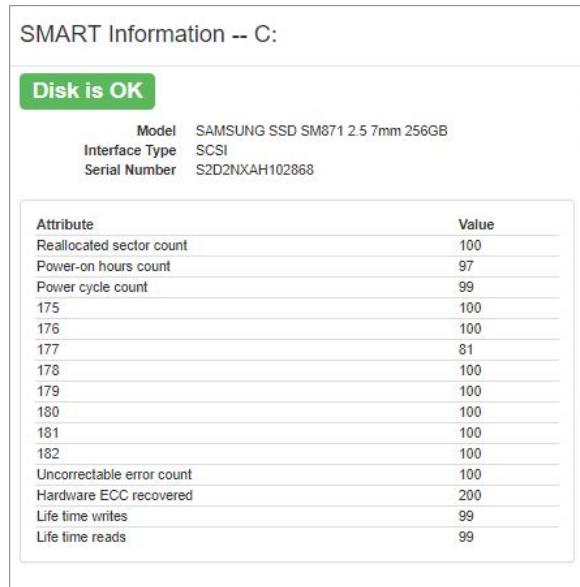


Figure 9. COMMON Tool Devices Page, Hard Disk Usage Window, SMART Information.

4.4 Disk Performance

The DISK PERFORMANCE window displays the percentage of time a hard disk spends reading and writing data, and the average disk queue length in average number of reading/writing requests that were queued for the selected disk during the sampling interval (Figure 10). The percent of time spent reading and writing data, indicates how heavily the system is using a hard disk. The average disk queue length, indicates how much data is waiting to be written to a hard disk; this figure will be very low unless disk failure is imminent. Both figures are based on the percentage of time the device spends across all hard disk space, not just hard disk space used by COMMON and other RDS-related software.

- The DISK PERFORMANCE window displays date and time of the last update on disk performance.
- The DISK PERFORMANCE window will have tabs for each device hard disk drive configured in COMMON.
- The DISK PERFORMANCE window provides a graphed display on the percentage of time a hard disk spends reading and writing data. The vertical axis indicates percentage of time spent reading and writing data. The horizontal axis indicates the month and day spanning the 15- to 180-day window of “Days to Retrieve” that was chosen at the top of the device’s page.
 - Hovering the cursor over a point on the graph provides date and time of the data point and the percentage of time a hard disk spent reading and writing at that polling.

By default, the graph displays the same number of days of data as indicated in the

drop-down of “Days to Retrieve” at the top of the device’s page.

- To temporarily graph additional days of disk performance, click on **Retrieve More Days**.

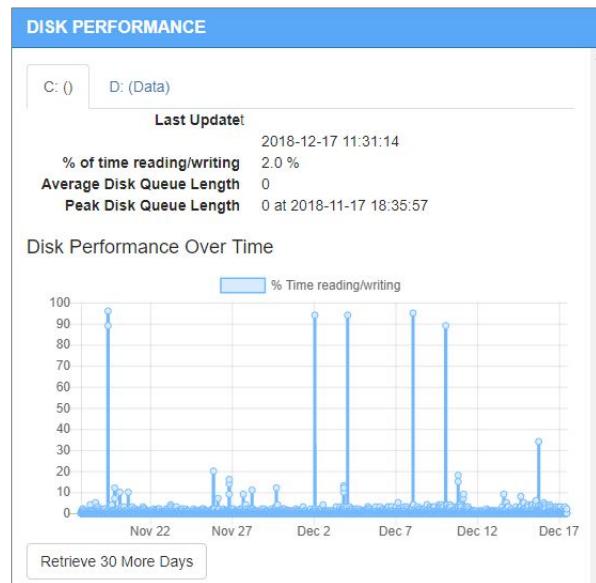


Figure 10. COMMON Tool Devices Page, Disk Performance Window.

4.5 Network Interface

The NETWORK INTERFACE window displays the device's current network interface card (NIC) capacity in bytes per second (and as a percentage) of total NIC throughput capability, not just traffic associated with COMMON and other RDS-related software (Figure 11).

- The NETWORK INTERFACE window displays date and time of the last update on NIC usage percentage, total NIC capacity used in bytes per second (and percent), peak usage of NIC in bytes per second (and percent) with time and date of that peak usage and provides the device's total NIC capacity in bytes per second.
- The NETWORK INTERFACE window provides a graphed display of NIC usage over time. The vertical axis indicates total NIC capacity as a percentage. The horizontal axis indicates the month and day spanning the 15- to 180-day window of “Days to Retrieve” that was chosen at the top of the device’s page.
- Hovering the cursor over a point on the graph provides the date and time of the data point and the percentage of NIC throughput used at that reading.

By default, the graph displays the same number of days of data as indicated in the drop-down of “Days to Retrieve” at the top of the device’s page.

- To temporarily graph additional days of NIC throughput, click on **Retrieve More Days**.

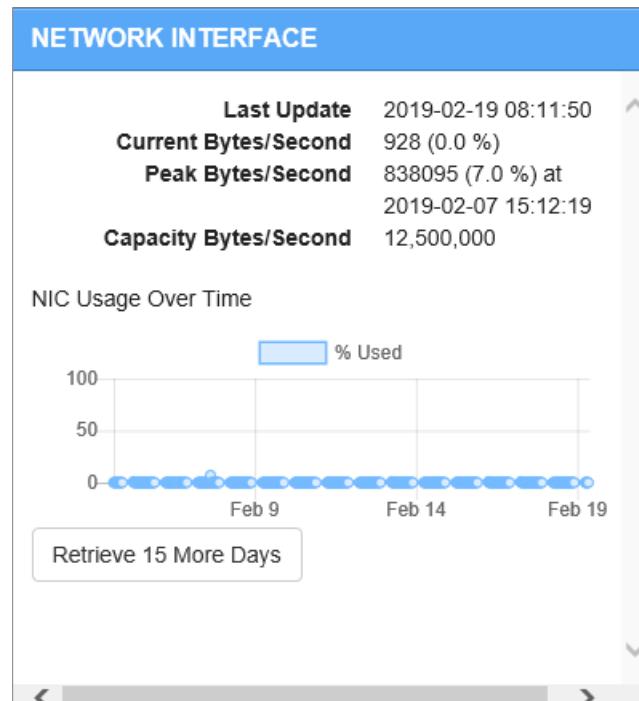


Figure 11. COMMON Tool Devices Page, Network Interface Window.

4.6 Running Services

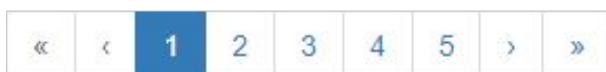
The RUNNING SERVICES window displays the number of Windows services currently running on the device (Figure 12). The list includes all services, not just services associated with RDS-related software. Services are applications that run in the background to serve core Windows operating system functions.

- Running services are listed in a table alphabetically and displays the date and time when the service list was last updated.

RUNNING SERVICES														
Last Update	2018-12-17 11:30:24													
Number of Services	82													
<hr/>														
Adobe Acrobat Update Service														
Application Host Helper Service														
Application Management														
Background Intelligent Transfer Service														
Background Tasks Infrastructure Service														
Base Filtering Engine														
CDPUserSvc_23212d														
Certificate Propagation														
CNG Key Isolation														
COM+ Event System														
<hr/>														
<table border="1"><tr><td>«</td><td><</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>></td><td>>></td></tr></table>		«	<	1	2	3	4	5	6	7	8	9	>	>>
«	<	1	2	3	4	5	6	7	8	9	>	>>		

Figure 12. COMMON Tool Devices Page, Running Services Window.

- A maximum of ten services is displayed at a time, users can page forward and backward using buttons at the bottom of the table:



- Clicking << moves to beginning of the list.
- Clicking < moves to the previous page.
- Clicking the number buttons (1, 2, 3, etc.) moves to a specific page.
- Clicking > moves to the next page.
- Clicking >> moves to the end of the list.

4.7 Database

The DATABASE window displays number, name, and size of the system's databases and the time of last update (Figure 13). The DATABASE window appears only for servers in a system.

The Database window appears only for servers in a system.

- The DATABASE window lists databases associated with the RDS, not any unrelated databases stored on a system.
- Databases are listed by database name and sorted by size in megabytes (MB) from largest to smallest.

- Clicking on a database's name opens a graph showing the change in the size of the database over time (Figure 14). The vertical axis indicates the size of the database in MB over time. The horizontal axis indicates the month and day the readings were taken.

DATABASE	
Current Database Information	
Last Update 2018-12-17 11:31:14	
Number of Databases	6
Name	Size in Megabytes
Hippo	10104
C:\COMMON\common.sqlite	1439
tempdb	72
model	16
msdb	15
master	6

Figure 13. COMMON Tool Devices Page, Database Information Window.



Figure 14. COMMON Tool Devices Page, Database Information Window, Database Size Over Time.

4.8 Processes

The PROCESSES window lists all processes currently running on the device not just processes associated with RDS-related software (Figure 15). Processes are the executable programs that run as part of an application.

- Processes are listed by name and sorted by percentage of CPU capacity used from highest to lowest, then alphabetically if multiple processes have the same CPU usage.
- The PROCESSES window displays the date and time when the process list was last updated.
- A maximum of ten processes are listed at a time, users can page forward and backward using the buttons at the bottom of the window.
- Clicking on a process name opens a graphed display of that processes' CPU usage over time (in green) and amount of memory used for that process in MB (in blue). The vertical, left axis indicates CPU usage as a percentage while the vertical, right axis indicates memory usage in MB. The horizontal axis indicates the month and day the readings were taken.
- Hovering the cursor over a point on the graph provides the date and time of the data point and the percentage CPU usage in the case of a CPU data point, or memory used in MB in the case of a Memory data point.

PROCESSES	
	Last Update 2018-12-17 11:30:23
	Number of Processes 43
Process	CPU Usage %
WmiPrvSE	1
ApplicationFrameHost	0
armsvc	0
ccSvchst	0
chrome	0
COMMON	0
conhost	0
csrss	0
dllhost	0
dwm	0

« < 1 2 3 4 5 > »

Figure 15. COMMON Tool Devices Page, Processes Window.

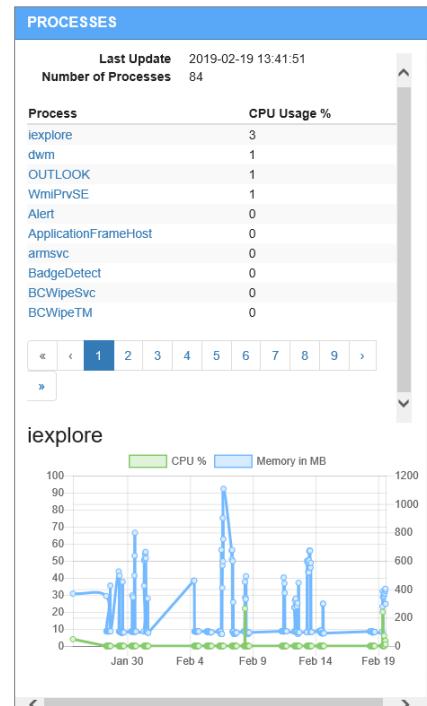


Figure 16. COMMON Tool Devices Page, Processes CPU Usage Window.

4.9 Installed Applications

The INSTALLED APPLICATIONS window displays the software applications installed for a device (Figure 17). This list includes all installed applications, not just RDS-related applications.

- The window displays the date and time when the device was last checked for installed applications.
- Installed applications are listed with each application's name and version.
- Users can page forward and backward using the buttons at the bottom of the window.
- Clicking on an application's name displays the application version currently installed and a timestamp showing when the application was updated or removed (Figure 18).

INSTALLED APPLICATIONS	
Last Update	2019-02-18 15:41:56
Number of Applications	43
Application	Version
Office 16 Click-to-Run Extensibility Component	16.0.9126.2356
Office 16 Click-to-Run Localization Component	16.0.9126.2356
Office 16 Click-to-Run Extensibility Component 64-bit	16.0.9126.2356
Registration	
Office 16 Click-to-Run Licensing Component	16.0.9126.2356
MFA Service	1.0.0
Microsoft Visual C++ 2017 x64 Minimum Runtime - 14.11.25325	14.11.25325
Entrust Entelligence Security Provider 10.0 for Windows COMMON	10.0.40.4468
Microsoft Visual C++ 2017 x64 Additional Runtime - 14.11.25325	14.11.25325
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.40660	12.0.40660
« < 1 2 3 4 5 > » ▼	

Figure 17. COMMON Tool Devices Page, Installed Applications Window.

INSTALLED APPLICATIONS	
Last Update	2017/08/08 09:50:17.512 -0600
Application	Version
Microsoft Application Error Reporting	12.0.6012.5000
Microsoft Application Error Reporting	12.0.6015.5000
Microsoft SQL Server System CLR Types	10.51.2500.0
Microsoft Help Viewer 1.1	1.1.40219
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4974	9.0.30729.4974
Sql Server Customer Experience Improvement Program	12.1.4100.1
Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219	10.0.40219
Microsoft System CLR Types for SQL Server 2014	12.1.4100.1
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219	10.0.40219
Microsoft SQL Server 2012 Native Client	11.0.2100.60
« < 1 2 3 4 5 > »	
Microsoft SQL Server 2012 Native Client	
Version	Timestamp
11.0.2100.60	2017/02/09 00:00:30.155 -0700

Figure 18. COMMON Tool Devices Page, Installed Applications History.

4.10 UPS

The UPS window displays the status of the uninterruptible power source (Figure 19) and estimates how long the UPS can continue to provide power.

- The UPS window also displays the date and time of the last update, percentage of current UPS charge, and the estimated run time.
- Hovering the cursor over a point on the graph provides date, time, and percentage of UPS usage at that reading.

By default, the graph displays the same number of days of data as indicated in the drop-down of “Days to Retrieve” at the top of the device’s page.

- To temporarily graph additional days of UPS usage, click on **Retrieve More Days**.

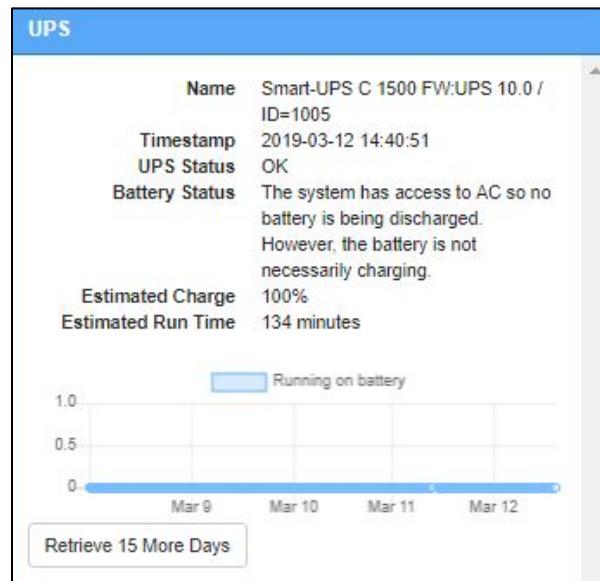


Figure 19: COMMON Tool Devices Page, UPS Window.

4.11 Event Log Errors—System

The EVENT LOG ERRORS—SYSTEM window displays non-application system errors. For each type of error, the log will display the number of times each error has occurred, and the date range between the oldest and most-recent error (Figure 20).

- The list includes all logged system errors, not just errors associated with RDS-related hardware or software. These errors include security-related events such as unsuccessful logons to a Windows computer, setup events associated with computers configured as domain controllers, and system events logged by Windows and Windows system services.
- The order of display will begin with the most recent event error logged.

EVENT LOG ERRORS – SYSTEM			
An TLS 1.1 connection request was received from a remote client application, but none of the cipher suites supported by the client application are supported by the server. The TLS	52	2019-02-06 19:21:22 – 2019-02-18 18:20:53	
connection request has failed.			
The server {37998346-3765-45B1-8C66-AA88CA6B20B8} did not register with DCOM within the required timeout.	68	2019-02-05 13:04:34 – 2019-02-17 16:09:01	
Smart Card Reader 'HID Global OMNIKEY 3x21 Smart Card Reader 0' rejected IOCTL TRANSMIT: No media in drive. If this error persists, your smart card or reader may not be functioning correctly. Command Header: 0c a6 00 00	4	2019-02-05 17:11:21 – 2019-02-18 09:52:24	
Request[0](CLS=0x80,INS=0xC2,P1=0x0,P2=0x0,Lc=18,Le=0,.NETServiceMethod=0x17D0BD7F)			2019-02-18 09:52:24
<input type="button" value="«"/> <input type="button" value="<"/> <input style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 2px 5px;" type="button" value="1"/> <input type="button" value="2"/> <input type="button" value="3"/> <input type="button" value="4"/> <input type="button" value=">"/> <input type="button" value="»"/>			
<input type="button" value="Retrieve 15 More Days"/>			

Figure 20. COMMON Tool Devices Page, Event Log Errors—System Window.

System event log errors are shown in a table that displays a maximum of ten errors at a time.

- Users can page forward and backward through the list of items using the buttons at the bottom of the window.

By default, the table displays the same number of days of data as indicated in the drop-down of “Days to Retrieve” at the top of the device’s page.

- To temporarily list additional days of event log errors, click on **Retrieve More Days**.

4.12 Event Log Errors—Applications

The EVENT LOG ERRORS—APPLICATION window displays application-related system errors. For each type of error, the log will display the number of times each error has occurred, and the date range between the oldest and most-recent error (Figure 21). The list includes all logged application errors, not just errors associated with RDS-related software.

- Application errors include significant problems such as a loss of data, warnings of issues that might indicate future problems, and informational errors that describes the successful operation of a program, driver, or service.
- The order of display will begin with the most recent event error logged.

EVENT LOG ERRORS -- APPLICATIONS		
Message	Count	Time
Faulting application name: WINWORD.EXE, version: 16.0.9126.2356, time stamp: 0x5c4990a2 Faulting module name: wplib.dll, version: 16.0.9126.2356, time stamp: 0x5c539fcb Exception code: 0xc0000005 Fault offset: 0x000d2e6a Faulting process id: 0xa6c Faulting application start time: 0x01d4c862e5779a3a Faulting application path: C:\Program Files (x86)\Microsoft\Office\Root\Office16\WINWORD.EXE Faulting module path: C:\Program Files (x86)\Microsoft\Office\Root\Office16\wplib.dll Report Id: 267b7786-e471-488f-bdc6-96c58c35aa7 Faulting package full name: Faulting package-relative application ID:	1	2019-02-19 10:10:28
An error occurred while retrieving some provider parameter: The operation requires a smart card, but no smart card is currently in the device.	7	2019-02-18 09:52:28 -- 2019-02-19 06:00:04
Faulting application name: backgroundTaskHost.exe, version: 10.0.17134.1, time stamp: 0xcb43d9c5 Faulting module name: ContentDeliveryManager.Background.dll, version: 0.0.0.0, time stamp: 0xb1a4570 Exception code: 0xc0000409 Fault offset: 0x000000000003ed0 Faulting process id: 0x22a4 Faulting application start time: 0x01d4c7dc6a8dfa3 Faulting application path: C:\WINDOWS\system32\backgroundTaskHost.exe Faulting module path: C:\Windows\SystemApps\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\ContentDeliveryManager.Background.dll Report Id: b89e3fec-13a0-46e7-90f8-5bb24aa4e5b8 Faulting package full name: Microsoft.Windows.ContentDeliveryManager_10.0.17134.1_neutral_neutral_cw5n1h2txyewy Faulting package-relative application ID: App An error occurred while decrypting a message: An internal error has been detected, but the source is unknown.	1	2019-02-18 15:56:01
Windows cannot load the extensible counter DLL. rdyboost. The first four bytes (DWORD) of the Data section contains the Windows error code.	5	2019-02-18 09:52:24 2019-02-07 15:12:17 -- 2019-02-19 06:00:04

Figure 21. COMMON Tool Devices Page, Event Log Errors—Applications Window.

Application event log errors are shown in a table that displays a maximum of ten errors at a time.

- Users can page forward and backward through the list of items using the buttons at the bottom of the window.

By default, the table displays the same number of days of data as indicated in the drop-down of “Days to Retrieve” at the top of the device’s page.

- To temporarily list additional days of Event Log Errors, click on **Retrieve More Days**.

5. Reports

The REPORTS page displays information on system components that can be printed or saved as a PDF file for delivery to local maintenance providers, NSDD experts, and others for help in troubleshooting and repairing system issues (Figure 22). COMMON can generate reports on the following:

- Site Report
- Server Report (per server)
- Network Report
- CAS Load Report
- Issues Report
- Site Configuration Report

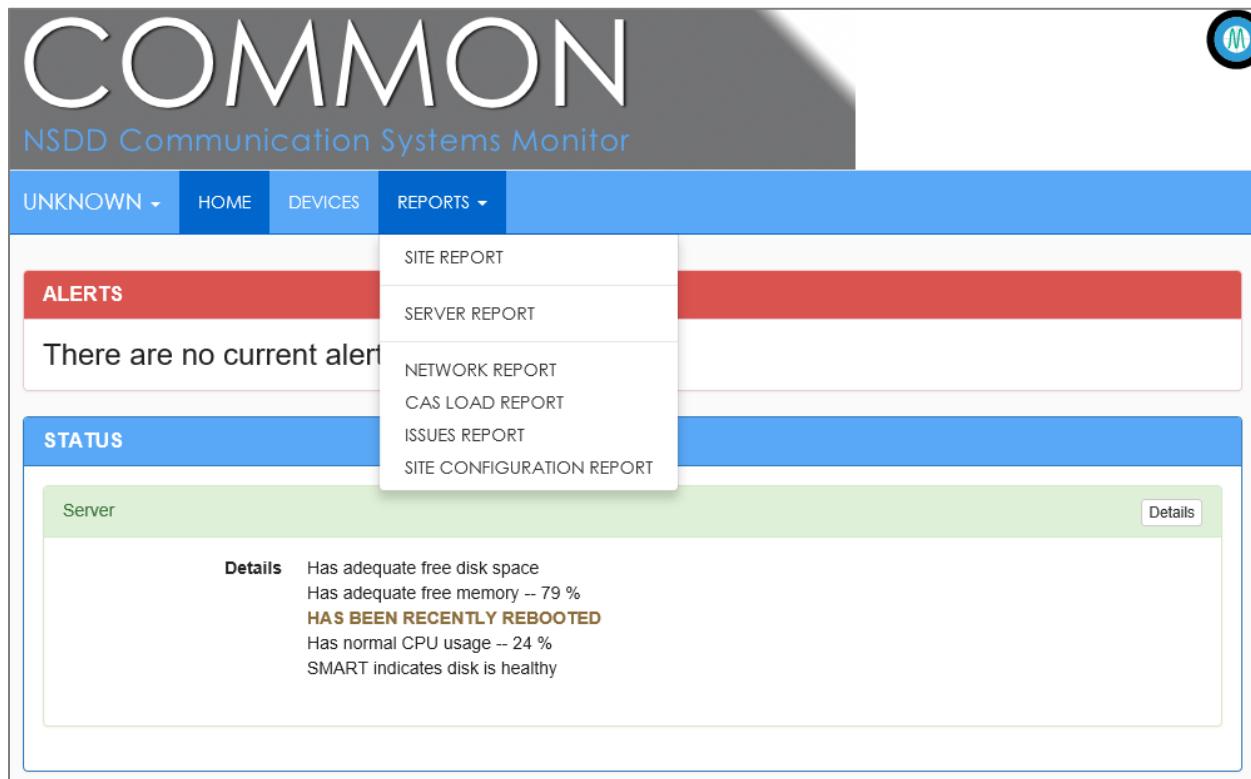


Figure 22. COMMON Tool Reports Tab, Drop-Down Menu.

- Any of the reports can be printed or saved as a PDF file for use by a local maintenance provider or NSDD technical support by clicking the “Print” button. It can then be saved to a user’s preferred location and opened in a reader such as Adobe Acrobat.

5.1 Site Report

The SITE REPORT contains the current state of the network, and the current state of Windows devices that are being monitored.

- To print the SITE REPORT, click the “Print” button.

The default date range reported will be the most recent complete month.

- Alternately, using the Start and End date options can generate a new report instantly for printing.

The SITE REPORT includes the following:

- Date and time the report was generated.
- Network Report, a list of devices in the system and provides status, IP address, the average response time (in milliseconds), uptime percentage, date and time of last successful ping, and a graph of offline network status history.
- A subsection is provided for each Window device named and includes the following information:
 - IP address and last boot time in hours, minutes and seconds.
 - Current percentage used and maximum (peak) use with date and time of that max for each parameter: Memory, Disks, CPU, and NIC.

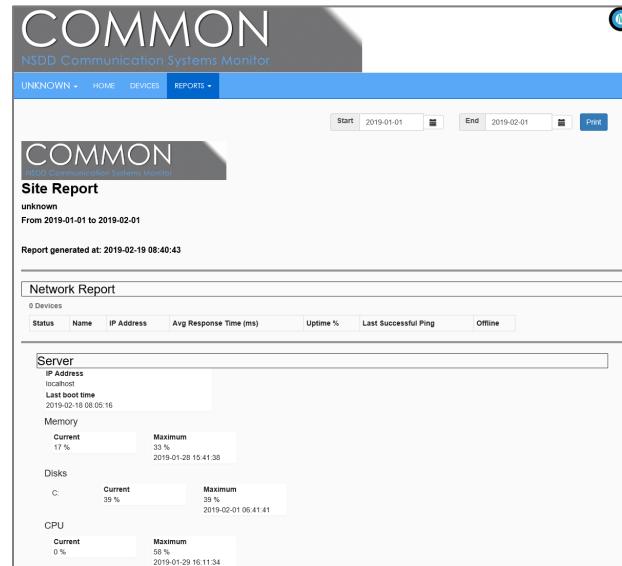


Figure 23. COMMON Tool Reports Page, Site Report Window.

5.2 Server Report

The SERVER REPORT includes device issues and trends identified by COMMON (Figure 24).

- To print the report, click the “Print” button.

By default, the report covers the same number of days as indicated in the drop-down of “Days to Retrieve” at the top of the device’s page.

- To report additional number of days, click on **Days to Retrieve**, options include 15, 30, 60, 90, 120, 150, and 180 days.

The screenshot displays the COMMON NSDD Communication Systems Monitor interface. At the top, there's a navigation bar with 'UNKNOWN' (dropdown), 'HOME', 'DEVICES', and 'REPORTS' (dropdown). A 'Days to Retrieve: 15' dropdown and a 'Print' button are located in the top right corner. The main content area is titled 'Server Report' and includes the following sections:

- System Status:** Shows 'unknown' status, 'Report Date: 2019-02-19 08:46:16', and '15 days' of history.
- System Metrics:** Includes 'Last boot time: 2019-02-18 08:05:16' and 'Uptime: 0 days, 07:36:28'.
- Alerts:** States 'There are no current alerts'.
- Memory:** Shows 'Current: 24 %', 'Maximum: 34 %', and timestamp '2019-02-06 16:11:40'.
- Disk:** Shows 'C: Current: 38 %', 'Maximum: 43 %', and timestamp '2019-02-10 06:00:13'.
- CPU:** Shows 'Current: 2 %', 'Maximum: 92 %', and timestamp '2019-02-18 06:00:12'.
- Network Interface:** Shows 'Current: 0 %', 'Maximum: 17 %', and timestamp '2019-01-25 16:11:45'.
- System Error Messages:** A table showing error messages with columns 'Message', 'Count', and 'Time'. One entry is visible: 'The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {9BA05972-F6A9-11CF-A442-00A0C90A8F39} and APPID {9BA05972-F6A8-11CF-A442-00A0C90A8F39} to the user SANDIA\amnmtc SID (S-1-5-21-2076390139-1363556362-943750798-1167878) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission can be modified using the Component Services administrative tool.' Count: 55, Time: 2018-12-17 07:28:50 -- 2019-02-18 12:55:36.
- System Error Messages:** Another table showing error messages with columns 'Message', 'Count', and 'Time'. One entry is visible: 'The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {8BC3F05E-D86B-11D0-A075-00C04FB68820} and APPID {8BC3F05E-D86B-11D0-A075-00C04FB68820} to the user SANDIA\amnmtc SID (S-1-5-21-2076390139-1363556362-943750798-1167878) from address LocalHost (Using LRPC) running in the application container Microsoft.Windows.ContentDeliveryManager_10.0_17134_1_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-350187224-1905355452-1037786396_3028148496-2624191407-3283318427-1255436723). This security permission can be modified using the Component Services administrative tool.' Count: 106, Time: 2018-12-18 06:00:40 -- 2019-02-18 06:00:20.

Figure 24. COMMON Tool Reports Page, Server Report Window.

The SERVER REPORT window includes the following:

- Name of the site
 - Report date, time, and number of days selected for reporting (e.g., 15 days, 30 days, etc.).
 - Last boot date and time.
 - Server uptime number of days, hours, minutes, and seconds.
 - Alert status at time of report.
 - Memory
 - Current memory usage displayed as a percentage of total system RAM used.
 - Max memory spike as a percentage of total system RAM used and the date and time of the spike.
 - Disks
 - Current disk usage as percentage of total system disk space.
 - Maximum disk space usage as percentage of total system disk space and the date and time of the spike
 - Separate entries for each physical hard disk drive in a system.
 - CPU
 - Current CPU usage as a percentage of total system CPU capacity.
 - Max CPU usage spike as percentage of total capacity with date and time of spike.
 - Network Interface
 - Current NIC usage as a percentage of total NIC throughput capacity.
 - Max NIC usage spike percentage and the date and time of the spike.
 - System Error Messages
 - Lists all system-related event log error messages. COMMON lists all error messages, not only those associated with the RDS.
 - These are the same errors listed in a device's EVENT LOG ERRORS--SYSTEM under the DEVICES page.
- Note: the report will be limited to listing the 20 most recent errors.
- Application Error Messages
 - Lists all application-related event log error messages. COMMON lists all error messages, not only those associated with the.

- These are the same errors listed in a device's EVENT LOG ERRORS--APPLICATION under the DEVICES page.

Note: the report will be limited to listing the 20 most recent errors.

- Processes Used

- Lists all Windows processes used by the device. COMMON lists all processes, not only those associated with the RDS.

- Running Services

- Lists all services running on the device. COMMON lists all services, not only RDS-related services.

- Application Changes

- Lists applications, their version and date and time when the application was added or updated: if removed, with date and time the device was deleted. COMMON lists all applications, not only those associated with the RDS.

- Database Data

- Lists the name and size of the RDS-related databases.

5.3 Network Report

The Network Report window displays the current network connectivity status of all devices in a system (Figure 25).

- The window displays the name of the site, date and time of the report, and the date and time of the last ping attempt for the complete network.
 - The Network Report window lists the status of each device, the device's name and IP address, average response time (in milliseconds), uptime percentage, and graphically displays an offline network status history (this is the same network status graph included in the SITE REPORT).
- To print the report, click the “Print” button.

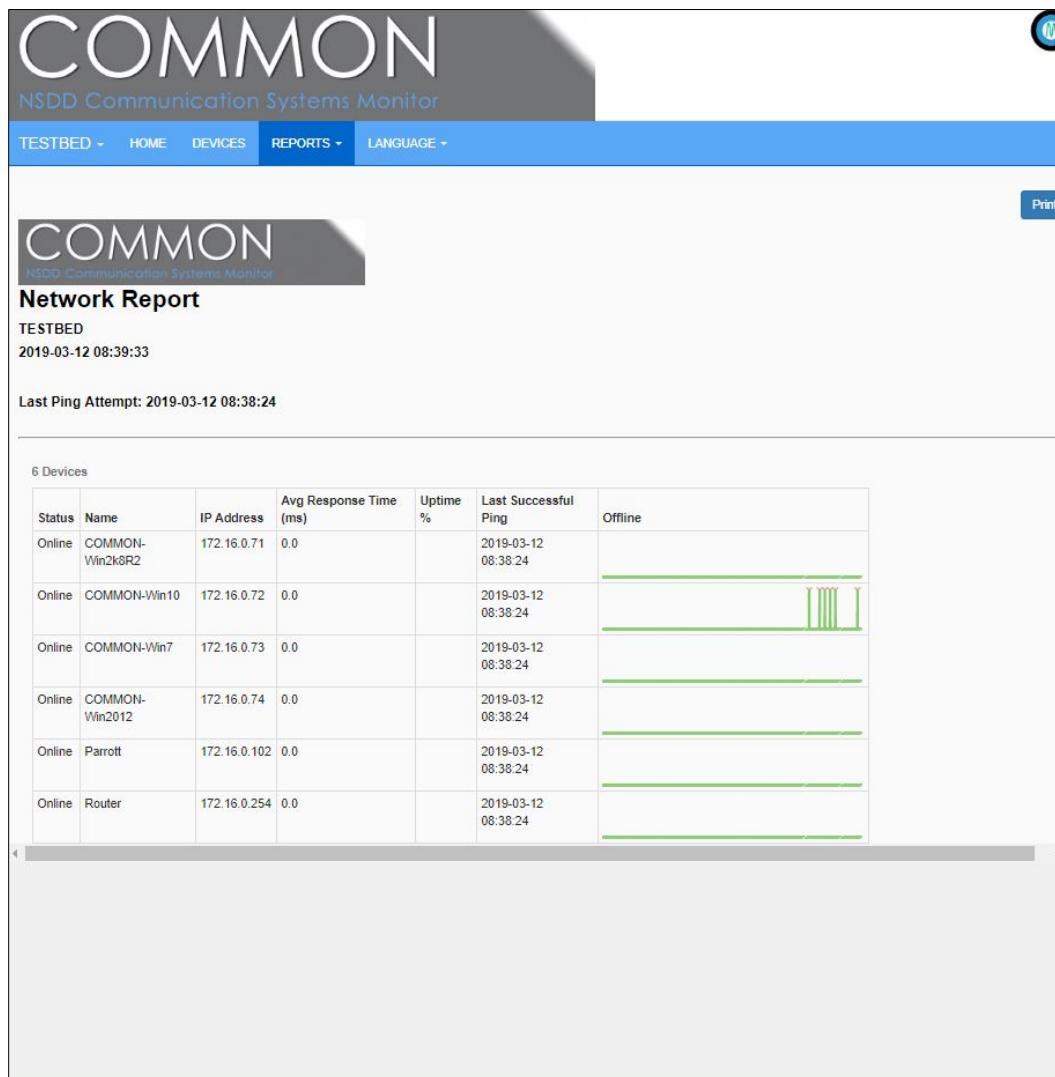


Figure 25. COMMON Tool Reports Page, Network Report Window.

5.4 CAS Load Report

The CAS Load Report provides a report on central alarm station (CAS) device loads and trends. The report contains separate sections for each device in the CAS (Figure 26).

By default, CAS Load Report covers the same number of days as configured when the COMMON tool was installed.

- To print the report, click the “Print” button.

The screenshot shows the COMMON NSDD Communication Systems Monitor interface. The top navigation bar includes links for TESTBED, HOME, DEVICES, REPORTS (selected), and LANGUAGE. A 'Print' button is located in the top right corner. The main content area displays the 'CAS Load Report' for two hosts:

- COMMON-Win10**
 - Last boot time: 2019-02-19 18:08:57
 - Uptime: 19 days, 19:20:14
 - Memory**: Current 16.3 %, Maximum 17.1 %, Last updated 2019-03-12 00:44:00
 - Disk**: C: 14.2 %, D: 1.7 %, Last updated 2019-03-12 00:44:00
 - CPU**: Current 3 %, Maximum 38 %, Last updated 2019-03-12 00:44:11
 - Network Interface**: Current 759 Bytes Per Second, Maximum 445669 Bytes Per Second, Last updated 2019-03-10 11:28:46
- COMMON-Win2012**
 - Last boot time: 2018-12-11 12:20:26
 - Uptime: 90 days, 00:35:51
 - Memory**: Current 30.6 %, Maximum 33.2 %, Last updated 2019-03-12 05:42:53
 - Disk**: C: 10.7 %, D: 0.4 %, Last updated 2019-03-12 05:42:53
 - CPU**: Current 0 %, Maximum 40 %, Last updated 2019-03-11 18:32:57
 - Network Interface**: Current 248 Bytes Per Second, Maximum 353175 Bytes Per Second, Last updated 2019-03-11 18:32:57

Figure 26. COMMON Tool Reports Page, CAS Load Report Window.

The CAS Load Report includes the following information:

- Name of the site
- Date and time of the report.
- Device name.
 - Last boot time date and time.
 - Uptime in days, hours, minutes, and seconds.
 - Memory:
 - Current memory usage as a percentage of total RAM.
 - Maximum memory usage as a percentage of total RAM with date and time of spike.
 - Disks:
 - Current disk usage as a percentage of total disk capacity.
 - Each hard disk is displayed in a separate line.
 - CPU:
 - Current CPU usage as a percentage of total system CPU capacity.
 - Maximum CPU capacity spike as percentage of total CPU capacity, with the date and time of the spike.
 - Network Interface:
 - Current NIC usage in bytes per second.
 - Max network interface usage spike in bytes per second and the date and time of the spike.

5.5 Issues Report

The Issues Report provides information on the issues that COMMON has recorded for the number of days configured when the COMMON tool was installed. The report is intended as a high-level overview of the system, in contrast to the detailed device network, and CAS load reports.

- To print the report, click the “Print” button.

If no issues have been identified, the Issues Report will read, “There are no current alerts.” Issues that will appear in this report include:

- Device is offline (no report entry if system is online).
- Device is low on free disk space (no report entry if the system has adequate disk space).
- Device is critically low on free disk space (no report entry if the system has adequate disk space).
- Device is low on free memory (no report entry if the system has adequate free memory).
- Device is critically low on free memory (no report entry if the system has adequate free memory).
- Device has recently been rebooted (no report entry if the system has not been rebooted recently).
- Device has excessive CPU usage (no report entry if CPU usage is normal).
- Device has slow ping response times of more than 500 milliseconds (no report entry if ping times are 500 milliseconds or less).
- Device is currently being powered by the UPS
- Device has a hard drive where SMART status is indicating potential failure

5.6 Site Configuration Report

The Site Configuration Report assembles information on how COMMON is configured to collect data on a device (Figure 27). The configuration is the current configuration at the time the report is generated.

- To print the report, click the “Print” button.

The screenshot shows the COMMON NSDD Communication Systems Monitor interface. At the top, there's a navigation bar with links for TESTBED, HOME, DEVICES, REPORTS (which is currently selected), and LANGUAGE. A blue header bar also contains these links. On the right side of the header is a 'Print' button. The main content area is titled 'Site Configuration Report' and displays two sections: 'Device Configuration' for 'COMMON-Win10' and 'COMMON-Win2012'. Each section lists various system collectors along with their enabled status and collection frequency in minutes. The data is presented in a table format with columns for 'Collectors', 'Is Enabled', and 'Frequency in Minutes'.

Collectors	Is Enabled	Frequency in Minutes
Memory	yes	5
Disk	yes	5
CPUUsage	yes	5
NICUsage	yes	5
Uptime	yes	1440
LastBootTime	yes	1440
Processes	yes	5
InstalledApplications	yes	1440
Services	yes	5
SystemErrors	yes	5
ApplicationErrors	yes	5
DatabaseSize	no	5
UPS	no	5
DiskSpeed	yes	5
SMART	yes	5

Collectors	Is Enabled	Frequency in Minutes
Memory	yes	5
Disk	yes	5
CPUUsage	yes	5
NICUsage	yes	5
Uptime	yes	1440
LastBootTime	yes	1440
Processes	yes	5
InstalledApplications	yes	1440
Services	yes	5
SystemErrors	yes	5
ApplicationErrors	yes	5
DatabaseSize	yes	5
UPS	no	5
DiskSpeed	yes	5
SMART	yes	5

Figure 27. COMMON Tool Reports Page, Site Configuration Report Window.

The Site Configuration Report includes the following information:

- Name of the site
- Date and time of the report.

- Device Configuration section contains information on the configuration of each device in the RDS separated by device name and includes the following information:
 - IP Address.
 - Collectors, data points which can be collected; whether collection has been enabled; and the configured frequency in minutes for collection of that data. These data points include:

■ Memory	■ LastBootTime	■ ApplicationErrors
■ Disk	■ Processes	■ DatabaseSize
■ CPUUsage	■ InstalledApplications	■ UPS
■ NICUsage	■ Services	■ DiskSpeed
■ Uptime	■ SystemErrors	■ SMART
- Configuration Parameters provides information on how COMMON report files are generated, stored, managed, and delivered. These items are configured by the COMMON installer (refer to separate COMMON Installation and Configuration Guide).

Configuration Parameter	Description
ServerName.database.type	Type of database on the system server.
ServerName.database.connection_string	Details of the text string needed to connect to the system database.
site.name	Name of the site where COMMON has been installed.
cpu.usage.alert	Percentage that CPU usage must exceed to generate an alert.
cpu.usage.alert.counts	Number of CPU usage percentage readings averaged together when COMMON tracks data for alerts
dailyfile.location	Location where the COMMON daily data files will be written. For example, c:\DailyFiles.
delete.days	Number of days of data COMMON stores.
disk.low.alert	Percentage of a hard disk that must be used for COMMON to generate a low free disk space alert.
disk.low.critical.alert	Percentage of a hard disk that must be used for COMMON to generate a critically low free disk space alert.

Configuration Parameter	Description
memory.low.alert	Percentage of RAM that must be used for COMMON to generate a low memory alert.
memory.low.critical.alert	Percentage of RAM that must be used for COMMON to generate a critically low memory alert.
reboot.recent.alert	Number of days within which a system reboot will generate the recently rebooted alert.
reboot.long.alert	Number of days within which a system reboot will generate an alert that the system has not been rebooted recently. This alert is designed primarily for those systems that perform better when periodically rebooted.
ping.num_pingers	Sets the number of simultaneous pings that will be sent. This setting is needed because some communications systems will not respond correctly if they receive too many simultaneous pings.
dailyfile.compress	Setting this value to 1 enables compression of the JSON daily files as they are saved to disk. Enabling this feature can save disk space and speed file transmission. A setting value of 0 indicates compression has been disabled.
dailyfile.compress.delete_after_compression	Setting this value to 1 enables automatic deletion of raw, uncompressed JSON files after the compressed version is created. Enabling this feature saves disk space. A setting value of 0 indicates automatic JSON file deletion has been disabled.
country.code	Two-letter code for the country in which the system is installed. For example, US for United States.
languages	Two-letter codes for the language(s) that have been enabled for COMMON. For example: EN for English

6. Site Name Tab

When COMMON is first configured for a site, the configuration tool allows the first tab in the menu bar to be named for the site; until then, the default label for this tab is “Unknown.” (Refer to the separate COMMON Installation and Configuration Guide.)



Figure 28. COMMON Site Name Tab, Drop-Down Menu.

6.1 Help

The HELP page provides the email address for the COMMON help desk and access to a PDF file version of this manual (Figure 29).

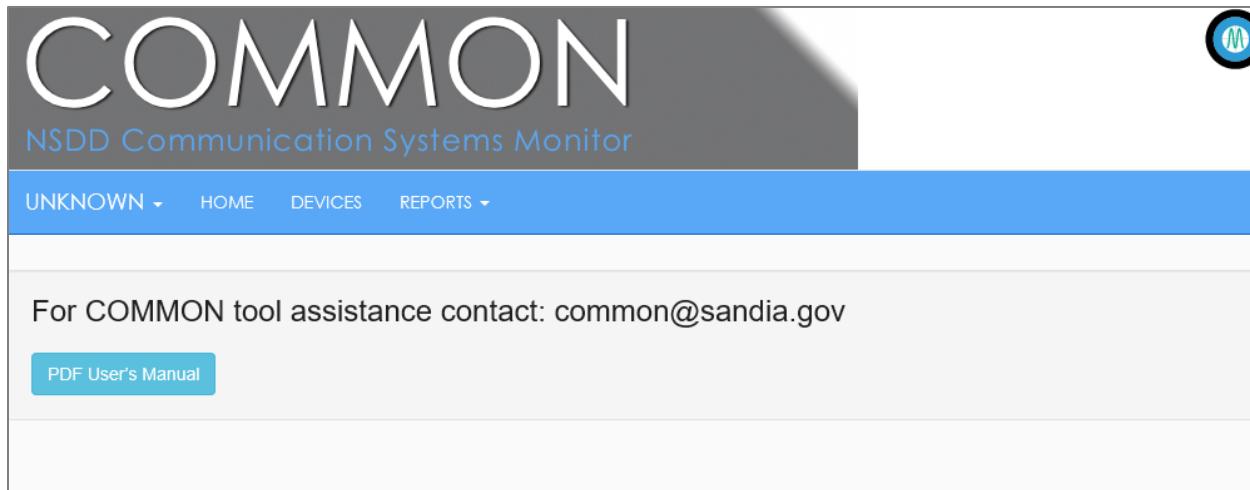


Figure 29. COMMON Tool Site Name Page, Help Window.

6.2 About

The ABOUT page provides links to the laboratories, NSDD, and U.S. government agencies responsible for COMMON (Figure 30). The page also provides a list of software products used to produce COMMON with links to product information pages and license agreements.

The screenshot shows the 'About' section of the COMMON tool. At the top, the COMMON logo is displayed with the subtitle 'NSDD Communication Systems Monitor'. Below the logo is a navigation bar with links for 'TESTBED', 'HOME', 'DEVICES', 'REPORTS', and 'LANGUAGE'. The main content area starts with the text 'COMMON -- version 1.5' and a copyright notice. It then features two boxes: one for 'Sandia National Laboratories' with their logo and name, and another for 'NSDD Partnership' with their logo and tagline 'Working Together to Prevent Nuclear Trafficking'. Below these boxes is a section titled 'Software Tools Used in COMMON Development' containing a table of tools and their licenses.

Product	License
angular-chart.js	BSD
angular-translate	MIT
AngularJS	MIT
AngularUI	MIT
Bootstrap	MIT

Figure 30. COMMON Tool Site Name Page, About Window.

6.3 Data Collection

DATA COLLECTION provides a “snapshot” of the status of data collection points. The UP NEXT window lists the next 10 data points for which data is scheduled to be collected with the next collection time, last collection attempt, last successful collection and frequency (in minutes) for that data point (Figure 31).

- The SYSTEM and SERVER windows provide an option to collect data now with a **Collect Now** button or to **Collect All Now** for all server data points.

The SYSTEM and SERVER windows lists the status of all data points COMMON is configured to collect. The data point name will indicate its status with one of the following symbols:

- ★ Is currently being collected
- ✓ Was successfully collected
- ✗ COLLECTION FAILED
- ⌚ Has not been collected

Name	Next Collection Time	Last Collection Attempt	Last Successful Collection	Frequency (minutes)
Server.Memory	2019-02-19 08:11:29	2019-02-19 07:41:32	2019-02-19 07:41:33	30
Server.Disk	2019-02-19 08:11:31	2019-02-19 07:41:33	2019-02-19 07:41:34	30
Server.CPUUsage	2019-02-19 08:11:31	2019-02-19 07:41:34	2019-02-19 07:41:38	30
Server.NICUsage	2019-02-19 08:11:35	2019-02-19 07:41:48	2019-02-19 07:41:49	30
Server.Processes	2019-02-19 08:11:37	2019-02-19 07:41:48	2019-02-19 07:41:49	30
Server.Services	2019-02-19 08:11:39	2019-02-19 07:41:49	2019-02-19 07:41:50	30
Server.SystemErrors	2019-02-19 08:11:40	2019-02-19 07:41:50	2019-02-19 07:41:50	30
Server.ApplicationErrors	2019-02-19 08:12:07	2019-02-19 07:42:11	2019-02-19 07:42:12	30
Server.UPS	2019-02-19 08:12:45	2019-02-19 07:42:52		30
Server.DiskSpeed	2019-02-19 08:12:46	2019-02-19 07:42:52	2019-02-19 07:42:53	30

Name	Next Collection Time	Last Collection Attempt	Last Successful Collection	Frequency (minutes)
Ping	2019-02-19 08:11:29	2019-02-19 07:41:32	2019-02-19 07:41:32	30

Name	Next Collection Time	Last Collection Attempt	Last Successful Collection	Frequency (minutes)
Memory	2019-02-19 08:11:29	2019-02-19 07:41:32	2019-02-19 07:41:33	30
Disk	2019-02-19 08:11:31	2019-02-19 07:41:33	2019-02-19 07:41:34	30
CPUUsage	2019-02-19 08:11:31	2019-02-19 07:41:34	2019-02-19 07:41:38	30
NICUsage	2019-02-19 08:11:35	2019-02-19 07:41:48	2019-02-19 07:41:49	30
Uptime	2019-02-19 15:41:35	2019-02-19 15:41:44	2019-02-18 15:41:45	1440
LastBootTime	2019-02-19 15:41:36	2019-02-19 15:41:45	2019-02-18 15:41:45	1440
Processes	2019-02-19 08:11:37	2019-02-19 07:41:48	2019-02-19 07:41:49	30
InstalledApplications	2019-02-19 15:41:38	2019-02-19 15:41:56	2019-02-18 15:41:56	1440
Services	2019-02-19 08:11:39	2019-02-19 07:41:49	2019-02-19 07:41:50	30
SystemErrors	2019-02-19 08:11:40	2019-02-19 07:41:50	2019-02-19 07:41:50	30
ApplicationErrors	2019-02-19 08:12:07	2019-02-19 07:42:11	2019-02-19 07:42:12	30
DatabaseSize	2019-02-19 09:42:30	2019-02-19 06:00:31		360
UPS	2019-02-19 08:12:45	2019-02-19 07:42:52		30
DiskSpeed	2019-02-19 08:12:46	2019-02-19 07:42:52	2019-02-19 07:42:53	30
SMART	2019-02-19 09:42:46	2019-02-19 06:00:45	2019-02-19 06:00:46	360

Figure 31. COMMON Tool Site Name Page, Data Collection Window.

6.4 Network History

The NETWORK HISTORY page displays network history graphs by group. The graphs display ping response time in milliseconds. Example shows Router; Servers, with two devices; and Workstations, with two devices (Figure 32).

By default, the graph displays the same number of days as configured when the COMMON tool was installed.

- To temporarily graph additional days of ping response, click on **Show more**.



Figure 32. COMMON Tool Site Name Page, Network History Window.

- Hovering the cursor over a point on the graph provides the date, time, ping response at time of reading.