# CA Spectrum® Infrastructure Manager

## SSLogger User Guide

r9.2

# CA Product References

This guide references CA Spectrum® Infrastructure Manager (CA Spectrum).

# Contact CA

**Contact Technical Support**

For your convenience, CA provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA products. At http://ca.com/support, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

**Provide Feedback**

If you have comments or questions about CA product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA product documentation, complete our short customer survey, which is also available on the CA Support website, found at http://ca.com/docs.

# Contents


## Chapter 1: Introduction 7

Benefits of SSLogger . . . . . 8
Disabling CA Spectrum Native Logging . . . . . 8
SSLogger Functionality When Contact Status is Lost . . . . . 8

## Chapter 2: Examples 9

Set Up SSLogger . . . . . 9
Example 1: Logging Device Statistics . . . . . 10
    Modify the Data File . . . . . 12
    Run SSLogger . . . . . 13
    Tail the SSLogger Output File . . . . . 14
Example 2: Logging List Attribute Statistics . . . . . 15
    Log List Attribute Statistics . . . . . 15
Example 3: Logging Port Statistics . . . . . 17
    Log Port Statistics . . . . . 18

## Chapter 3: SSLogger Input and Output 21

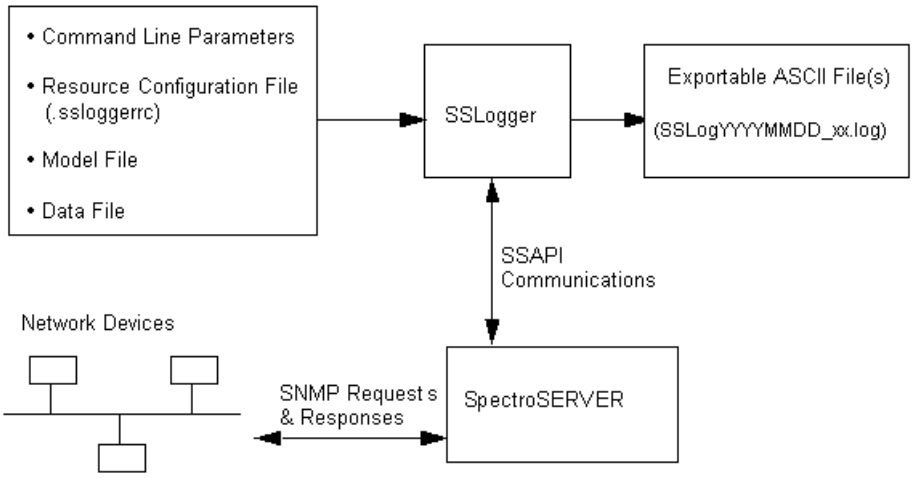
Command-Line Parameters . . . . . 21
.ssloggerrc Configuration File . . . . . 22
Model File . . . . . 23
Data File . . . . . 23
    group . . . . . 24
    SSlogger_relation . . . . . 25
    child_mtype_handles . . . . . 25
    mtype . . . . . 25
    Rotate_log_interval . . . . . 26
    on_rotate_execute . . . . . 26
SSLogger Output . . . . . 26

## Index 29

# Chapter 1: Introduction

This section describes the SSLogger application and its benefits when compared with native CA Spectrum logging.

SSLogger is a CA Spectrum command-line application that works with SpectroSERVER to poll network devices and log the data to a simple ASCII file suitable for import into databases and reporting systems. As shown in the following diagram, you control SSLogger activity using command-line options and three input files (a configuration file, a model file, and a data file) which specify the target SpectroSERVER, the target devices and ports, the target attributes, the logging frequency per attribute, and the output file rotation frequency. SSLogger uses the SSAPI to communicate with SpectroSERVER, which obtains data from the target devices using SNMP requests. SSLogger then logs the specified data to an ASCII file, closing the current output file and creating a new one depending on your needs.




This section contains the following topics:

Benefits of SSLogger (see page 8)
Disabling CA Spectrum Native Logging (see page 8)
SSLogger Functionality When Contact Status is Lost (see page 8)

# Benefits of SSLogger

SSLogger offers several advantages over CA Spectrum's native method of logging statistics:

- SSLogger lets you specify particular devices for which you want to log statistics. The CA Spectrum native method only allows you to specify the *types* of devices for which you want to log data, which means that you often are forced to poll and log more data than you want.
- SSLogger lets you set the polling and logging frequency for each attribute. The CA Spectrum native method only allows you to specify the frequency per model type.
- SSLogger writes data to a simple, readily exportable ASCII file. The CA Spectrum native method writes data to the Archive Manager's database, which requires additional steps to export the data.

# Disabling CA Spectrum Native Logging

If you decide to log CA Spectrum statistics using SSLogger, you can turn off CA Spectrum native logging by setting the stat_logging_disabled flag to TRUE in CA Spectrum's /SS/.vnmrc file and then restarting SpectroSERVER. Setting this value to TRUE also turns off the polling of these logged attributes. It prevents CA Spectrum from using SNMP get actions to check attribute values and prevents CA Spectrum from writing the values to the Archive Manager database. This results in reduced device traffic as well as a reduced load on the Archive Manager database.

# SSLogger Functionality When Contact Status is Lost

SSLogger functions differently when the contact status of a device (or group of devices) it is monitoring is lost. When SSLogger is scheduled to collect statistical data from a device and that device goes down, SSLogger will not write any data from the downed device to the .log file, effectively ignoring the device. SSLogger will not retry the downed device until the next scheduled poll cycle. SSLogger will continue to log data from devices that are up on the scheduled interval with no interruption. Once CA Spectrum regains contact with the downed device, SSLogger will log its data on the configured scheduled interval.

# Chapter 2: Examples

This section provides detailed examples of how to use SSLogger in three different scenarios of increasing complexity. These examples will help you understand how to use SSLogger to log different types of CA Spectrum statistics. The examples are designed to let you follow along on your own system, creating your own input files and substituting your own and model ID values for the ones used in the examples. Sample output files are also provided. Although it is likely that most users will want to use SSLogger to log statistics associated with individual ports (interfaces) on network devices, the examples start with a simpler scenario and work their way up to the logging of ports. It is strongly suggested that you work through each of these three examples in succession before setting up your own production SSLogger scenario.

This section contains the following topics:

Set Up SSLogger (see page 9)
Example 1: Logging Device Statistics (see page 10)
Example 2: Logging List Attribute Statistics (see page 15)
Example 3: Logging Port Statistics (see page 17)

## Set Up SSLogger

Before using the three examples, you should complete the setup procedure described here.

**To set up SSLogger**

1. Launch SpectroSERVER and OneClick.
2. Model a device (or choose one that you have already modeled) and write down the name of the device for future reference.
3. Create a text file called "modelfile" in the CA Spectrum SSLogger directory.

4. Type the following into the file and then save and close the file:

```
#**********************************************************************
# modelfile
#
# This file specifies devices to monitor.
#**********************************************************************
Create another text file called “datafile” in the SSLogger directory.
Type the following into the file and then save and close the file.
#**********************************************************************
# datafile
#
# This file specifies device information to monitor.
#**********************************************************************
```

   Open /SSLogger/.ssloggerrc with a text editor and modify it to reflect the name of your SpectroSERVER (vnm name) and the names of your model file and data file name. This file provides default parameters for running SSLogger. You can override the vnm, modelfile, and datafile settings by entering alternate values at the command line as needed.

```
listen_port=
vnm=<your SpectroSERVER name>
vnm_port=
modelfile=modelfile
datafile=datafile
max_threads=
thread_priority=
debug_interval=
max_oreq=
```

5. Start the Command Line Interface (CLI) from a terminal/Command Prompt window on your machine by navigating to the vnmsh directory and entering the following command:

```
./connect
```

   You are now ready to perform the steps involved in the following three examples.

**More information:**

Command-Line Parameters (see page 21)

# Example 1: Logging Device Statistics

To complete the first example, you must modify your model and data files, run SSLogger, and analyze the output file.

The model file specifies the device models that you want SSLogger to target, or log statistics from. In this example, you will specify only one device model. However, you can list hundreds or thousands of devices in this file if desired.

**To modify the model file**

1. From the CA Spectrum vnmsh directory, enter the following CLI command:

   ```
   ./show models mname=<name of your model>
   ```

   A list of all models whose name begins with the specified model name appears, identifying each model by model handle, model name, model type handle, and model type name. CA Spectrum often uses IP addresses to name models. The following sample output shows what the list might look like if the IP address 172.19.57.220 is used as the model name.

   The entry with the model handle value 0x40001a represents the device, while the other models represent applications or ports of that device.

   ```
   0x400059     172.19.57.220_IC   0x230012    ICMP_App
   0x400056     172.19.57.220_Do   0x230052    CtDownLoadApp
   0x400022     172.19.57.220_FD   0xd80004    FddiMAC
   0x40004b     172.19.57.220_St   0x590006    RMONApp
   0x40005b     172.19.57.220_IP   0x230016    IP2_App
   0x400057     172.19.57.220_RS   0x230046    RFC1317App
   0x40005d     172.19.57.220_DS   0xc40006    DS1App1406
   0x40001a       172.19.57.220 0x1c80018   2M46_04
   0x40001f     172.19.57.220_Tr   0xd0031     CT_Tp_Appl
   0x40004a     172.19.57.220_21   0xd000a     CSIIfPort
   ```

2. Find your device in the resulting list, then add all four of the device information values to the model file you set up. For the device in this example, the model file would appear as follows:

   ```
   #*****************************************************************
   # modelfile
   #
   # This file specifies devices to monitor.
   #*****************************************************************
   0x40001a    172.19.57.220     0x1c80018   2M46_04
   ```

3. Separate the four device information values with semicolons, as shown below.

   ```
   #*****************************************************************
   # modelfile
   #
   # This file specifies devices to monitor.
   #*****************************************************************

   0x40001a;   172.19.57.220;    0x1c80018;  2M46_04
   ```

## Modify the Data File

The data file specifies the attributes for which you want to log values. In this example you will use the following three attributes:

- ipInReceives
- ipOutRequests
- sysUpTime

**To build the data file**

1. From the vnmsh directory, enter the following CLI command using the model type handle for your device model from the third column in your model file:

   `./show attributes mth=<your model type handle> flags=E`

   All of the specified model type's attributes for which the external (E) flag is set are listed. For each attribute, the list shows the attribute ID, attribute name, attribute type, and attribute flag or flags.

   The following sample output shows what the list might look like if the 172.19.57.220 device's model type handle of 0x1c80018 is used.

```
0x10098     ipInReceives          Counter      E,R
0x10099     ipInHdrErrors         Counter      E,R
0x1009a     ipInAddrErrors        Counter      E,R
0x1009b     ipForwDatagrams       Counter      E,R
0x1009c     ipInUnknownProtos     Counter      E,R
0x1009d     ipInDiscards          Counter      E,R
0x1009f     pInDelivers           Counter      E,R
0x100a0     ipOutRequests         Counter      E,R
0x100a1     ipOutDiscards         Counter      E,R
0x100a2     ipOutNoRoutes         Counter      E,R
0x101c1     icmpOutAddrMaskReps   Integer      E,R
0x10245     sysUpTime             Time Ticks   E,R,M,P
0x10b5a     sysContact            Text String  E,R,W,M
0x10b5b     sysName               Text String  E,R,W
```

2. In the output that you generate, find the three attributes targeted in this example (ipInReceives, ipOutRequests, and sysUpTime), and then add their names and IDs to your data file along with the model type name of your model so that it looks like the following example:

```
#*****************************************************************
# datafile
#
# This file specifies device information to monitor.
#*****************************************************************
group: device_information
 sysUpTime            ; 10 ; 0x0 ; 0x10245 ; .0
 ipInReceives         ; 10 ; 0x0 ; 0x10098 ; .0
 ipOutRequests        ; 10 ; 0x0 ; 0x100a0 ; .0
mtype: <model type name of your model>
 device_information
```

   In this data file example, group is an SSLogger data file keyword referring to a group of attributes. You can name a group anything you want. In this case, the device_information group includes the three target attributes, and there are five columns of information about them. The first column specifies the attribute name. You can use any name, but it is suggested that you use the CA Spectrum names as they appear in the output from Step 1. The second column tells SSLogger how often (in seconds) to poll and log the attribute value associated with the attribute. A polling interval of once every ten seconds would normally be too frequent, but it is used in this example to give you a large amount of output data in a short time. It is recommended that you set the polling interval to the same value as the Rotate_log_interval. The third column specifies the model type where the attribute is found. 0x0 indicates the *device* model type. In a later example, you will set this field to a *port* model type handle for certain attributes. The fourth column specifies the CA Spectrum attribute ID. The fifth column indicates whether the attribute is a list attribute; in this case the .0 means the attribute is *not* a list attribute.

**More information:**

Rotate_log_interval (see page 26)

## Run SSLogger

To run SSLogger, enter the following command from the SSLOGGER directory:

```
./SSlogger
```

A message similar to the following appears:

```
sslogger version 3.0rev0 -- built on Jul 3 2001 at 09:33:13
SSlogger started at: Fri Jul 27 10:36:55 2001
```

## Tail the SSLogger Output File

While SSLogger is running, you can look at the output file by using the "tail" command and specifying the name of the file, which contains the current date in YYYYMMDD format followed by a two-digit sequence number and a .log extension. For example, the first log file created by SSLogger on September 12, 2001 would be named SSLog20010912_01.log.

**Note:** See Rotate_log_interval for more information on how log files are sequenced and closed.

Assuming this is the currently active log file, you could view statistics being added to the end of the file by entering the following command from the SSLOGGER directory:

```
tail -f SSLog20010912_01.log
```

Replace the filename in the tail command above with the name of your own SSLogger output file, execute the command, and you will see a display similar to the following example.

```
1 20010718; 10:51:43; 10:51:43; 0x40001a; -; 0x10245; 239765127
2 20010718; 10:51:43; 10:51:43; 0x40001a; -; 0x10098; 1152773
3 20010718; 10:51:43; 10:51:43; 0x40001a; -; 0x100a0; 1142885
4 20010718; 10:51:53; 10:51:53; 0x40001a; -; 0x10245; 239766128
5 20010718; 10:51:53; 10:51:53; 0x40001a; -; 0x10098; 1152774
6 20010718; 10:51:53; 10:51:53; 0x40001a; -; 0x100a0; 1142886
7 ...
```

The output file contains seven columns of information:

- The first column shows the date.
- The second column shows the time just before SSLogger reads the attribute value.
- The third column shows the time just after SSLogger reads the attribute value.
- The fourth column shows the device model handle.
- The fifth column shows "-" if the attribute is *not* a list attribute. Otherwise, as seen in a later example, it shows the table index.
- The sixth column shows the attribute ID.
- The seventh column shows the attribute value.

**Note:** For more information about the output file contents, see SSLogger Output.

**More information:**

SSLogger Output (see page 26)
Rotate_log_interval (see page 26)

# Example 2: Logging List Attribute Statistics

In Example 1, you logged single-value device attributes. Example 2 shows you how to log *list* attributes or tables of attribute data. As with the first example, this means modifying your data file, running SSLogger, and examining the resulting output file data.

## Log List Attribute Statistics

In this example you will use the following two attributes:

- ifInOctets
- ifOutOctets

**To log list attribute statistics**

1. From the CA Spectrum vnmsh directory, enter the following CLI command using the model type handle for your device model from the third column in your model file:

   ```
   ./show attributes mth=<your model type handle> flags=ET
   ```

   Because you use the "E" and "T" flags, this command will list all of the specified model type's attributes for which the external (E) and table (T) flags are set. For each attribute, the list will show the attribute ID, attribute name, attribute type, and attribute flag or flags. The following sample output shows what the list might look like if the 172.19.57.220 device's model type handle of 0x1c80018 is used.

   ```
   0x100cd     ifInOctets            Counter          E,R,[]
   0x100ce     ifInUcastPkts         Counter          E,R,[]
   0x100cf     ifInNUcastPkts        Counter          E,R,[]
   0x100d0     ifInDiscards          Counter          E,R,[]
   0x100d1     ifInErrors            Counter          E,R,[]
   0x100d2     ifInUnknownProtos     Counter          E,R,[]
   0x100d3     ifOutOctets           Counter          E,R,[]
   0x100d4     ifOutUcastPkts        Counter          E,R,[]
   ```

2. In the output that you generate, find the two attributes targeted for this example (ifInOctets and ifOutOctets) and add their names and IDs to your data file so that it looks like the following example:

```
#*****************************************************************
# datafile
#
# This file specifies device information to monitor.
#*****************************************************************
group: device_information
 sysUpTime            ; 10 ; 0x0 ; 0x10245 ; .0
 ipInReceives         ; 10 ; 0x0 ; 0x10098 ; .0
 ipOutRequests        ; 10 ; 0x0 ; 0x100a0 ; .0
 ifInOctets           ; 10 ; 0x0 ; 0x100cd ; .1
 ifOutOctets          ; 10 ; 0x0 ; 0x100d3 ; .1
mtype: <model type name of your model>
 device_information
```

**Note:** The new lines have ".1" at the end which indicates that these attributes represent tables of information. Any value except ".0" indicates that the attribute is a table attribute. So you may want to put a complete OID in place of ".1" for documentation purposes.

3. Run SSLogger.

4. Tail the SSLogger output file. Again, you can look at the output file by using the "tail" command and specifying the name of the file, which should be the same as the name you used in the first example (see SSLogger Output for information on how and when new output files are opened). To do this, enter the following command from the SSLOGGER directory:

```
tail -f SSLog<current date in YYYYMMDD format>_01.log
```

This time your output should appear as follows:

```
20010724; 10:17:26; 10:17:26; 0x40001a; 1; 0x100cd; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 1; 0x100d3; 0
20010724; 10:17:26; 10:17:26; 0x40001a; -; 0x10245; 291399900
20010724; 10:17:26; 10:17:26; 0x40001a; -; 0x10098; 1307231
20010724; 10:17:26; 10:17:26; 0x40001a; -; 0x100a0; 1297366
20010724; 10:17:26; 10:17:26; 0x40001a; 2; 0x100cd; 2041440626
20010724; 10:17:26; 10:17:26; 0x40001a; 2; 0x100d3; 2308773051
20010724; 10:17:26; 10:17:26; 0x40001a; 3; 0x100cd; 2794679535
20010724; 10:17:26; 10:17:26; 0x40001a; 3; 0x100d3; 2497597136
20010724; 10:17:26; 10:17:26; 0x40001a; 4; 0x100cd; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 4; 0x100d3; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 5; 0x100cd; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 5; 0x100d3; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 6; 0x100cd; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 6; 0x100d3; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 7; 0x100cd; 183630755
20010724; 10:17:26; 10:17:26; 0x40001a; 7; 0x100d3; 176510228
```

```
20010724; 10:17:26; 10:17:26; 0x40001a; 14; 0x100cd; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 14; 0x100d3; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 15; 0x100cd; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 15; 0x100d3; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 16; 0x100cd; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 16; 0x100d3; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 17; 0x100cd; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 17; 0x100d3; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 18; 0x100cd; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 18; 0x100d3; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 19; 0x100cd; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 19; 0x100d3; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 20; 0x100cd; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 20; 0x100d3; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 21; 0x100cd; 0
20010724; 10:17:26; 10:17:26; 0x40001a; 21; 0x100d3; 0
```

**Note:** The fifth column shows the table index on lines that represent table attribute data.

**More information:**

Run SSLogger (see page 13)
SSLogger Output (see page 26)

# Example 3: Logging Port Statistics

This example shows how to log statistical information associated with a port. Once again, you will modify your data file, run SSLogger, and look at the output file. Note that you do *not* have to modify the model file, nor do you have to specify the model handles of the port models at all. Instead of stipulating port model handles, you will specify port model *type* handles and CA Spectrum relations. In this example you will also use the ifInOctets and ifOutOctets attributes.

## Log Port Statistics

**To log port statistics**

1. From the vnmsh directory, enter the following CLI command using the model handle for your device model from the first column in your model file:

   ```
   ./show children rel=HASPART mh=<your model handle>
   ```

   This CLI command shows you the port models associated with your target device. You need to execute this command to determine the model type handles of the ports you want to target. In this case, all ports are the same model type. The sample output below shows what the list might look like using the 0x40001a model handle from the first example.

   ```
   MHandle     MName             MTypeHnd    MTypeName        Relation
   0x40003f    172.19.57.220_1   0xd000a     CSIIfPort        HASPART
   0x400040    172.19.57.220_2   0xd000a     CSIIfPort        HASPART
   0x400041    172.19.57.220_3   0xd000a     CSIIfPort        HASPART
   0x400042    172.19.57.220_5   0xd000a     CSIIfPort        HASPART
   ```

2. If your output shows several different kinds of ports, select one port model type and use its model type handle in the following command:

   ```
   ./show attributes mth=<your port model type handle> flags=E
   ```

   This returns a list of external attributes associated with the specified port model type as shown here:

   ```
   0x10e3f     ifAdminStatus            Integer       E,R,W,[]
   0x10e40     ifOperStatus             Integer       E,R
   0x10e41     ifInOctets               Counter       E,R
   0x10e42     ifOutOctets              Counter       E,R
   0x11315     ifInUcastPkts            Counter       E,R
   0x11317     ifInNUcastPkts           Counter       E,R
   0x11318     ifInDiscards             Counter       E,R
   0x11319     ifInErrors               Counter       E,R
   0x1131a     ifInUnknownProtos        Counter       E,R
   ```

   Your command output may or may not show the attributes ifInOctets and ifOutOctets. If not, you will have to choose a few of your own to use as you follow along with this example.

3. Add a new group called port_information to your data file, and then enter the attribute name, model type handle (not 0x0, which indicates device models), and attribute ID for each of your attributes. Finally, add the information for the SSlogger_relation and child_mtype_handles so that your data file looks like the example shown below.

```
#*****************************************************************
# datafile
#
# This is a sample data input file for sslogger.
#*****************************************************************
group: device_information
 sysUpTime            ; 10 ; 0x0 ; 0x10245 ; .0
 ipInReceives         ; 10 ; 0x0 ; 0x10098 ; .0
 ipOutRequests        ; 10 ; 0x0 ; 0x100a0 ; .0
 ifInOctets           ; 10 ; 0x0 ; 0x100cd ; .1
 ifOutOctets          ; 10 ; 0x0 ; 0x100d3 ; .1
group: port_information
 ifInOctets           ; 10 ; 0xd000a ; 0x10e41 ; .0
 ifOutOctets          ; 10 ; 0xd000a ; 0x10e42 ; .0
SSlogger_relation: HASPART
child_mtype_handles:
 0xd000a
mtype: <model type name of your model>
 device_information
 port_information
```

   The SSlogger_relation keyword specifies which relations SSLogger should follow between any devices specified in your model file and any models of model types specified in the attribute lines of your data file. In this example, the value for this keyword is HASPART because that is the relation a CA Spectrum device model has to its port models.

   **Note:** You can see a list of all CA Spectrum relations using the CLI "show relations" command.

   The child_mtype_handles keyword affects ONLY the display of the fourth column of the SSLogger output file (see example in following section). By default, only a device model handle appears in this column. By specifying the port model type handle under the child_mtype_handles keyword, you instruct SSLogger to display *both* the device model handle and the port model handle in the fourth column of the output file.

4. Run SSLogger.

5. Once again, look at the output file by using the "tail" command and specifying the name of the SSLog file, which should be the same as the name you used in the previous examples (see SSLogger Output for information on how and when new output files are opened). To do this, enter the following command from the SSLOGGER directory:

   `tail -f SSLog<current date in YYYYMMDD format>_01.log`

Your output should appear similar to the following sample:

```
20010718; 14:40:56; 14:40:56; 0x40001a; -; 0x10245; 241140428
20010718; 14:40:56; 14:40:56; 0x40001a; -; 0x10098; 1159008
20010718; 14:40:56; 14:40:56; 0x40001a; -; 0x100a0; 1149142
20010718; 14:40:56; 14:40:56; 0x40001a:0x400040; -; 0x10e41; 1582426060
20010718; 14:40:56; 14:40:56; 0x40001a:0x400040; -; 0x10e42; 1808004560
20010718; 14:40:56; 14:40:56; 0x40001a:0x400041; -; 0x10e41; 2251080181
20010718; 14:40:56; 14:40:56; 0x40001a:0x400041; -; 0x10e42; 1999870610
20010718; 14:40:56; 14:40:56; 0x40001a:0x400042; -; 0x10e41; 0
20010718; 14:40:56; 14:40:56; 0x40001a:0x400042; -; 0x10e42; 0
20010718; 14:40:56; 14:40:56; 0x40001a:0x40003f; -; 0x10e41; 0
20010718; 14:40:56; 14:40:56; 0x40001a:0x40003f; -; 0x10e42; 0
```

**Note:** Both the device and port model handles appear in the fourth column as described previously.

**More information:**

Run SSLogger (see page 13)
SSLogger Output (see page 26)

# Chapter 3: SSLogger Input and Output

This section describes SSLogger input and output. It includes information about its command-line parameters as well as the content and syntax of the associated input files.

The SSLogger application uses the following four sources for input:

- Command-line parameters
- .ssloggerrc configuration file
- Model file
- Data file

Each of these input sources is described individually in this section.

This section contains the following topics:

Command-Line Parameters (see page 21)
.ssloggerrc Configuration File (see page 22)
Model File (see page 23)
Data File (see page 23)
SSLogger Output (see page 26)

## Command-Line Parameters

You can use one or more of the following parameter flags with the SSLogger command. If you use these flags to specify a vnm, modelfile, or datafile that is different from the ones specified in your .ssloggerrc file, the values entered at the command line take precedence.

**-help**

Causes SSLogger to show a help message.

**-vnm <*machine name*>**

Specifies the target SpectroSERVER.

**-modelfile <*model file name*>**

Specifies the model file that SSLogger should use.

**-datafile <*data file name*>**

Specifies the data file that SSLogger should use.

**-debug**

Causes SSLogger to output debug information during operation.

**-ctrace**

Causes SSLogger to output SSLogger/SpectroSERVER communication information.

**-strace**

Causes SSLogger to output security information.

# .ssloggerrc Configuration File

The SSLogger resource configuration file is named .ssloggerrc and contains the following keywords:

**listen_port=**

Specifies the port on which SSLogger communicates with the SpectroSERVER.

**Default:** 0xd00f

**vnm=**

Specifies the target SpectroSERVER.

**vnm_port=**

Specifies the target SpectroSERVER communication port.

**Default:** 0xbeef

**modelfile=**

Specifies the name of the model file that SSLogger should use.

**datafile=**

Specifies the name of the data file that SSLogger should use.

**max_threads=**

Specifies the maximum number of worker threads that SSLogger should allocate for the work of logging attributes.

**Default:** 30

**thread_priority**

Specifies the thread priority of each worker thread.

**Default:** 80

**debug_interval**

Specifies how often (in seconds) SSLogger should output debug information if the -debug command line flag is used.

**Default:** 600 seconds

**max_oreq=**

Specifies the maximum number of polling requests that SSLogger can have outstanding at one time. A zero (0) indicates that SSLogger can have an infinite number of outstanding requests. You can use this keyword to limit SSLogger's effect on SpectroSERVER performance.

**Default:** 0

# Model File

The model file specifies a list of devices that SSLogger will target. It can include devices of many different model types. Information is divided into four columns, as shown below.

```
#****************************************************************
# modelfile
#
# This file specifies devices to monitor.
#****************************************************************

0x40001a;   172.19.57.220;    0x1c80018;  2M46_04
0x40013c;   172.19.57.221;    0x1c80018;  2M46_04
0x40032c;   172.19.57.222;    0x1c80018;  2M46_04
0x4004ad;   172.19.57.223;    0x1c80018;  2M46_04
0x400063;   10.253.2.26;      0x2c60021;  RstoneSwRtr
0x400063;   10.253.2.27;      0x2c60021;  RstoneSwRtr
0x400063;   10.253.2.28;      0x2c60021;  RstoneSwRtr
0x400063;   10.253.2.29;      0x2c60021;  RstoneSwRtr
```

The entry for each device contains the model handle, model name, model type handle, and model type name. Semicolons are required. You can log statistics from a new device simply by adding a new line to the model file without changing the data file at all.

# Data File

The data file tells SSLogger which attribute values to read. The file can include the keywords listed in this section.

## group

The group keyword specifies a group of attributes. The name of the group is up to you. Information that defines each attribute in the group falls into the following five columns:

- The first column specifies the attribute name. You can use any name you want in this column, but it is recommended that you use the CA Spectrum attribute name as displayed in the CLI output in SSLogger Output.
- The second column specifies how often (in seconds) SSLogger should poll and log the attribute.
- The third column specifies the model type where the attribute is found. A value of 0x0 indicates the device model type.

  **Note:** Under the example's port information group, there is a value of 0xd000a, which is the model type handle for port models.
- The fourth column is the CA Spectrum attribute ID.
- The fifth column specifies whether the attribute is a list/table attribute. The value.0 means the attribute is *not* a list/table attribute. Any other number or text means the attribute *is* a list/table attribute. You may want to put the OID in this field. The example below uses .1 to indicate a list/table attribute.

### Example:

```
group: device_information
 sysUpTime            ; 10 ; 0x0 ; 0x10245 ; .0
 ipInReceives         ; 10 ; 0x0 ; 0x10098 ; .0
 ipOutRequests        ; 10 ; 0x0 ; 0x100a0 ; .0
 ifInOctets           ; 10 ; 0x0 ; 0x100cd ; .1
 ifOutOctets          ; 10 ; 0x0 ; 0x100d3 ; .1

group: port_information
 ifInOctets           ; 10 ; 0xd000a ; 0x10e41 ; .0
 ifOutOctets          ; 10 ; 0xd000a ; 0x10e42 ; .0
```

**More information:**

SSLogger Output (see page 26)

## SSlogger_relation

When you want SSLogger to log attributes associated with a port that is associated to a device specified in your model file, you do not actually specify a port model handle. Instead, you specify the port's model type handle in the third column of an attribute line under a group keyword in the data file. You also specify how the port model is associated to the device model. This is done by using the SSlogger_relation keyword, one relation per keyword. If you do not specify any SSlogger_relation keywords, SSLogger will, by default, follow the two shown below. Otherwise, it will only follow the ones you specify.

```
SSlogger_relation: HASPART
SSlogger_relation: PossPrimApp
```

## child_mtype_handles

The child_mtype_handles data file keyword affects *only* the display of the fourth column of the SSLogger output file. By default, only a device model handle appears in this column. By specifying the port model type handle under the child_mtype_handles keyword in the example data file below, you instruct SSLogger to display both the device model handle and the port model handle in the fourth column of the output file.

```
child_model_handles:
    0xd000a
```

## mtype

The mtype keyword specifies a model type name and not a model name. This is how SSLogger interprets this keyword. For every device in the model file of this model type, poll and log the groups of attributes listed.

```
mtype: 2M46_04
    device_information
    port_information
```

### Rotate_log_interval

The Rotate_log_interval keyword specifies how often (in hours or a fraction of an hour) SSLogger should close the current output file and open another one. If you do not specify this keyword, SSLogger will close the current output file and open a new one at midnight every 24 hours. A value of 1 tells SSLogger to close the current output file at the top of the next hour and open a new output file. If the Rotate_log_interval value specified is .15, SSLogger will close the current output file and open a new output file every 15 minutes. If a value of 1.xx is entered, the value will be rounded to the nearest whole number. If you specify 2 and the current time is 2:25 p.m., SSLogger will close the current output file at 4:00 p.m., open a new file, close that file at 6:00 p.m., and so on.

### on_rotate_execute

The on_rotate_execute keyword specifies a path to an executable to be run when the SSLogger log file is rotated. The path must be the full path to the executable. You must have read and executed privileges to run the executable.

```
on_rotate_execute: <full path to executable>
```

## SSLogger Output

This section describes the content of the log file that is generated when you run SSLogger. SSLogger writes information to an ASCII file. The name of this output file is similar to the following: SSLog20010727_01.log.

**Note:** The filename contains the date. If you set the Rotate_log_interval keyword in the data file so that more than one SSLog file will be created in a single day, SSLogger increments the last two numbers in the output file name accordingly.

The output file is organized into the following seven columns, as shown below:

```
20010724; 10:17:26; 10:17:26; 0x40001a; -; 0x10245; 291399900
20010724; 10:17:26; 10:17:26; 0x40001a; 2; 0x100cd; 2041440626
20010724; 14:40:56; 14:40:56; 0x40001a:0x400040; -; 0x10e41; 1582426060
DATE ; START TIME ; END TIME ; MODEL HANDLE ; INTERFACE ; ATTRID ; VALUE
```

Each line in the file represents one reading of the attribute value:

- The first column indicates the date in YYYYMMDD format.
- The second column specifies the time just before SSLogger reads the attribute.
- The third column specifies the time just after SSLogger reads the attribute.

- The fourth column specifies the model handle of the model for which the attribute value is read. If you enter the port model type handle (0xd000a) under the child_mtype_handles keyword in the data file, this column will display both the device model handle and the port model handle.
- The fifth column displays a dash (-) if the attribute is *not* a list/table attribute. Otherwise, it displays the index number of a list/table attribute.
- The sixth column displays the attribute ID.
- The seventh column shows the attribute value itself.

# Index


## C

contacting technical support • iii
customer support, contacting • iii

## D

datafile • 22
debug_interval • 22

## G

group • 24

## L

listen_port • 22

## M

max_oreq • 22
max_threads • 22
modelfile • 22
mtype • 25

## O

on_rotate_execute • 26

## P

parameters • 21

## R

Rotate_log_interval • 26

## S

SSlogger_relation • 25
support, contacting • iii

## T

technical support, contacting • iii
thread_priority • 22

## V

vnm • 22
vnm_port • 22