# Kofax Communication Server

## Service User Manual

Version: 10.3.0

Date: 2019-12-13

KOFAX

# Legal Notice

# Table of Contents

Chapter 1

# Preface

At the moment, KCS Service (TCSRV) is the only Windows service installed by the Kofax Communication Server (KCS).

The purpose of TCSRV is to start up parts of KCS and to ensure these parts (processes) keep running. Such parts are for example TCOSS, TCPOP3, TCLANPRT… If any of the started processes fails, TCSRV attempts to restart it.

Currently, TCSRV can handle only programs designed especially for being controlled by TCSRV. In future KCS releases, TCSRV will be able to monitor other Windows services such as the IIS.

In a normal environment, TCSRV starts automatically at the system startup.

Chapter 2

# Starting a Process

TCSRV tries to start every process specified in the configuration parameter *Startup* in the registry. Every single name in this list of processes specifies a subkey within the Registry where the actual command line for the process is taken from.

**Important** The *Startup* parameter is case sensitive! It must exactly match the value of the subkey.

Additionally, TCSRV can take the UserID/Password/Domain from this registry key in order to create a specific access token for the process being started. Every process in the system has an access token associated to it. It is used by the system to verify the user rights and privileges when a process accesses resources and to pass the user's logon credentials when connecting to a network resource.

If you use UserID/Password/Domain from the registry, the specified user must be part of the local administrator's group. Otherwise the process will not be started.

**Important** The access token is not the user profile!

The user profile (e.g. user specific settings for installed applications) will always be taken from the user currently logged in interactively or from the default profile if no user is logged in.

If no UserID/Password/Domain is specified for a process, it will inherit the access token from TCSRV, which is usually the local system account.

**Note** It is not possible to access network resources using the system account.

TCSRV will fail to start the process if it cannot create the access token by logging in the specified user. In this case it does not try to create the process with the default access token.

After starting a process, TCSRV continuously polls the status of the process using a TCRPC channel. The poll cycle is about 10 seconds.

If a process fails by either terminating, returning a fatal error code, or if the connection to it is interrupted, TCSRV will restart it.

TCSRV will attempt to start a process only 3 times (default; configurable in the registry) if a process continues to fail within the first 10 minutes after being started.

If all three attempts failed, the process is considered to be improperly configured or a permanent network problem occurred. In this situation, TCSRV tries only once (default; configurable in registry) to start the process every hour (configurable).

Once the process has run properly for more than 10 minutes, all retry counters are reset.

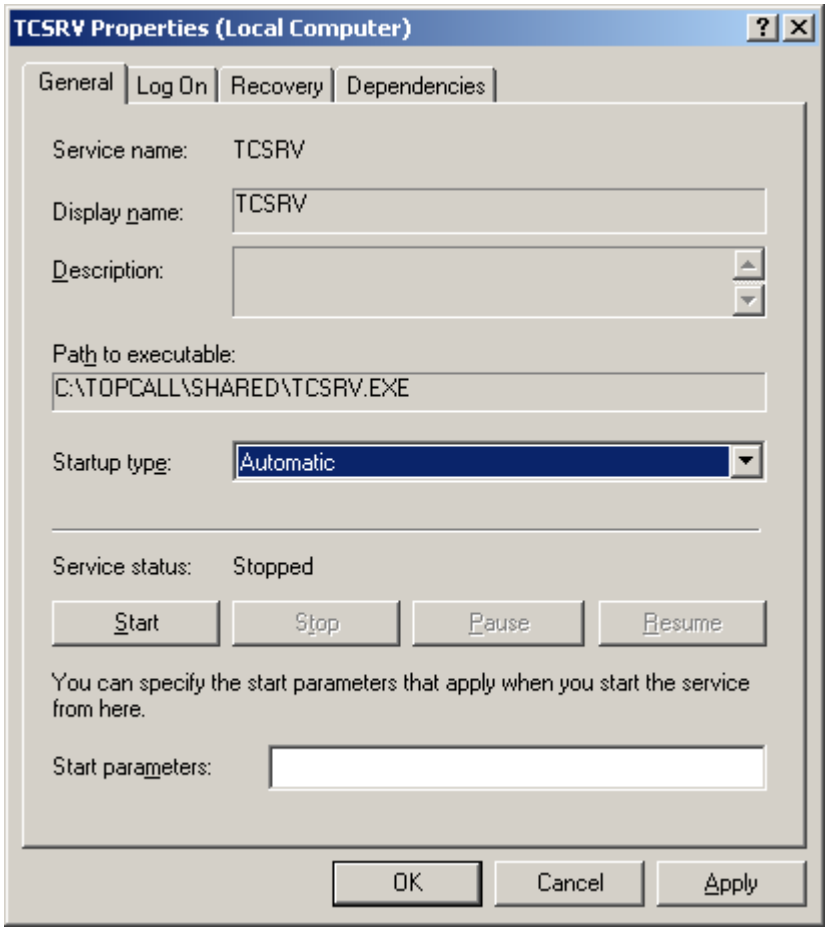
TCSRV internally stores a list of processes and current status of every process. This list can be queried by an external program such as KCS Monitor.

Chapter 3

# System Configuration

The setup program of Kofax Communication Server performs all necessary steps to install the service. It should only be necessary to adjust the type of startup from manual to automatic startup.

In Control Panel | Administrative Tools | Services, double-click “TCSRV” to display its properties.




TCSRV should always log on using the System Account! This is necessary to have sufficient rights and privileges.

When testing a system it is useful to allow the service to interact with the desktop. In this case the service and every process started by the service displays a console window with the trace output (if any). In a productive environment interaction with the desktop should be switched off because there is almost always some output to the screen that may confuse the customer.

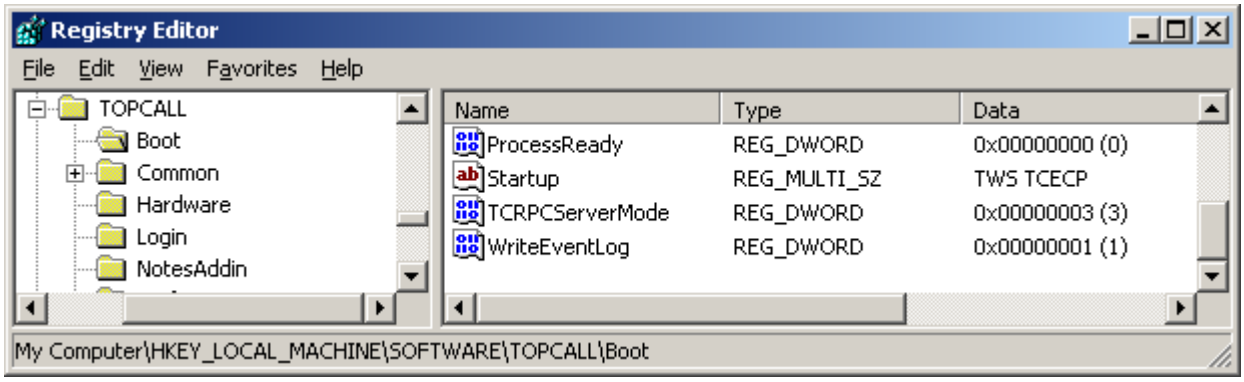
Chapter 4

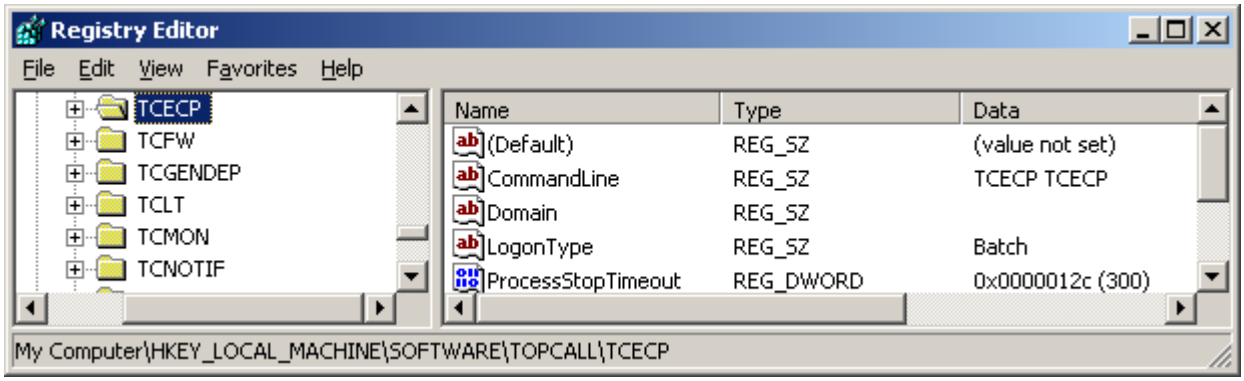
# General Registry Settings

KCS registry keys are stored in the following path:

- For 32-bit systems: HKEY_LOCAL_MACHINE\Software\TOPCALL
- For 64-bit systems: HKEY_LOCAL_MACHINE\Software\Wow6432Node\Topcall

In this document, this registry path is referred as <*KcsRegistryPath*>




The registry subkey for TCSRV has the name *Boot*.

TCSRV requires a list of processes to be started. This list is stored in:

<*KcsRegistryPath*>\Boot\Startup

This list actually contains names of the registry subkeys of the processes being started. For TCSRV these are the actual process names regardless of the executable file name. It is NOT possible to specify the

same name repeatedly in the startup list in order to start multiple instances of a process. Every instance must have a unique name. TCSRV can start up to 200 processes.

TCSRV takes a process name and reads the actual command line from the registry subkey owned by this process:

<*KcsRegistryPath*>\<Name>\CommandLine

Optionally, UserID, Password and Domain of a user account can be specified to get the process rights and privileges of the specified user. The password can be specified in clear text or encrypted (standard encryption used by KCS setup).

It is recommended to use encrypted passwords. Otherwise, an encrypted version of the passwords will be written to the registry after a successful logon.

<*KcsRegistryPath*>\<Name>\UserId

<*KcsRegistryPath*>\<Name>\Password

<*KcsRegistryPath*>\<Name>\Domain

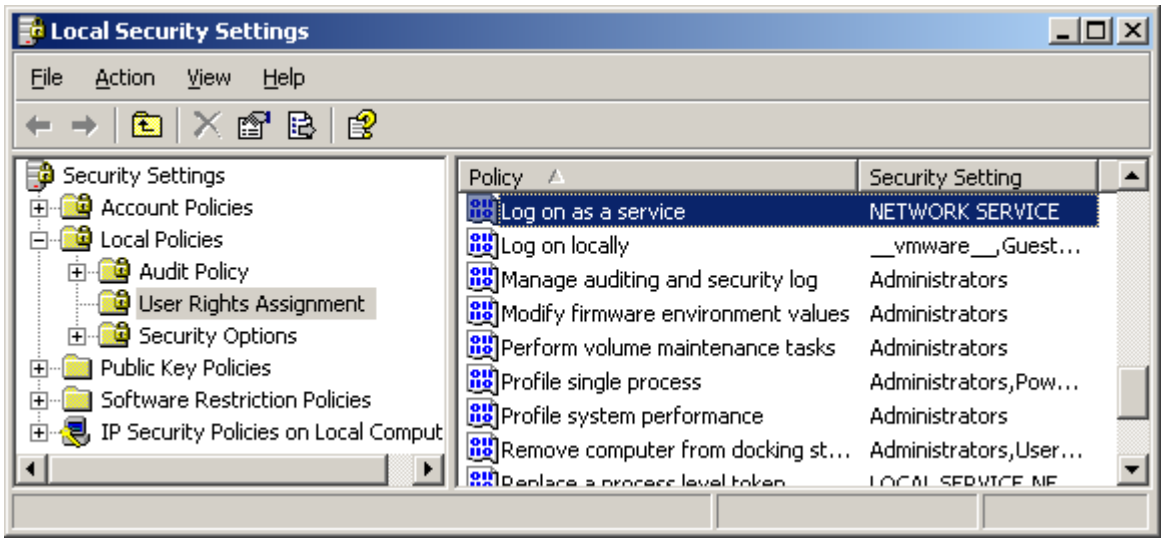
By default, the specified user is logged in as a service. This type of logon can be changed by the optional parameter:

<*KcsRegistryPath*>\<Name>\LogonType

For a description of all possible values and their effects refer to *Logon Types and Interaction with the Desktop*.

It is recommended not to change this value.

For the specified user account to be logged in with type *Service*, you have to grant the "*Log on as service*" right to that account. Since Windows 2000 this configuration has to be done in Administrative Tools | Local Security Settings | Local Policies | User Rights Assignment.




The number of tries TCSRV performs to start a process can be configured within the registry.

<*KcsRegistryPath*>\<Name>\StartupRetries1

Integer value (default is 3) specifying the initial number of tries to start a process. This value will be used if this is the first attempt or if the process has run properly for at least 10 minutes.

<*KcsRegistryPath*>\<Name>\StartupRetries2

Integer value (default is 1) specifying the tries to start a process after previous attempts failed and TCSRV waited one hour (configurable) to restart the process.

<*KcsRegistryPath*>\<Name>\StartupCycle

Integer value (default is 60 = 1 hour) which allows one to configure the timeout after one set of retries failed until the next set of startup retries. This value can be set with a granularity of 1 minute.

<*KcsRegistryPath*>\<Name>\Autostart

Integer value (default is 1 = enable). If you set this registry value to 0, the process is no more automatically started after startup of TCSRV. Instead it shows “Autostart disabled” and waits until it is manually started with KCS Monitor.

<*KcsRegistryPath*>\<Name>\ RPCInterfaceVersion

Integer value (default is 1 = old interface) which specifies if the process supports the new interface (2 = new interface). The new interface supports two additional commands:

- Reload configuration
- Kill process

<*KcsRegistryPath*>\<Name>\ProcessStopTimeout

Integer value (default is 60) which specifies a duration in seconds. When a process is stopped it is given this duration for terminating itself. If the process has not stopped after this period, TCSRV will kill the process.

Chapter 5

# Logon Types and Interaction with the Desktop

This section describes the logon types and interaction with the desktop.

## Logon Types

The following values are possible as logon types (only the first character is significant):

**Note** For running TCSRV with a domain user, the user (for TCSRV or Links) must have the following rights:

- Local administrator rights
- Log on as a service
- Replace a process level token

**S(ervice)**

Logon as a service user. The user account requires the privilege “Logon as a Service”. This logon type will be the default if no such registry value or an invalid value is specified. This type caches the user credentials.

Requires Windows 2000 or above.

**B(atch)**

Logon as a batch user. The user account requires the privilege “Logon as a Batch process” (using the Policy Editor – see above). This type does NOT cache the user credentials.

Requires Windows 2000 or above.

**I(nteractive)**

Logon as an interactive user. The user account requires the privilege “Logon on locally” (using the Policy Editor – see above). This type caches the user credentials.

Requires Windows 2000 or above.

**Note** This is NOT related to “Interact with Desktop” and does not make the process visible on the desktop.

**N(etwork)**

This logon type distinguishes between access to local resources and access to remote resources via the network.

Basically, the process being started runs in the security context of the local system account, and for all accesses to local resources the access permissions for this account apply.

When accessing any network resources (such as shares), the access permissions are checked against those of the user as specified in the registry for the process being started.

Additionally, the user specified in the registry is verified locally to ensure proper values are given for domain/user/password.

This verification is performed by logging the user on as *Batch* user (see above) before the process gets started. If the user does not have the necessary privileges to logon as *Batch* user, the user will be probed with logon type *Interactive*. If the user cannot be logged on locally using one of the two methods, the process will not be started and an error message will be displayed.

**Note** The *LogonType* may be set to *Network* if the process or one of its child processes has a graphical user interface (like the TC/DC) and the processes are allowed to interact with the desktop (i.e. TCSRV is configured with the enabled option *Allow Service to Interact with Desktop*).

**Restriction**: The support of Network on Windows 2003 or above is limited. Please use Network only for TCDCLink and/or TC/Link-LN, if needed.

## Interaction with Desktop

By default, all processes inherit the desktop of TCSRV. If, for example, the service TCSRV was configured to be visible at the interactive desktop (“Interact with Desktop” in the service properties panel of Windows), also the child processes started by TCSRV interact with the visible desktop.

This default behavior can be overridden by a 1-character prefix to the *LogonType* string:

Prefix “+” forces the usage of the interactive (and therefore visible) desktop for the specific process.

Prefix “-” prevents the usage of the interactive desktop and gives the process a hidden desktop of its own.

**Example**:

| | |
|---|---|
| “+N” | for e.g. TC/DC to let the conversion applications like Word be visible. |
| “-” or “-B” | for e.g. TC/Link-FI to hide the console window |

The prefixes must be the first character of the string allowing the actual logon type to start at the second character. The prefix character to control desktop interaction is independent of the actual logon type and of whether a logon type is required at all. Even if a process does not need any user logon and the security context is inherited from TCSRV, it will be possible to specify the prefix characters “+” or “-” to determine how the process will interact with the visible desktop.

**Note** For details about supported operating systems, refer to *Environment Guide - Platform System Manual*.

Chapter 6

# Tracing

TCSRV supports all common trace parameters such as *TraceLevel, MaxTraceFiles, MaxTraceFileSize*, …

<*KcsRegistryPath*>\Boot\TraceLevel

<*KcsRegistryPath*>\Boot\MaxTraceFiles

<*KcsRegistryPath*>\Boot\MaxTraceFileSize

The trace level is the sum of different bit values. Each bit turned-on enables certain events to be traced. Possible bit values are:

| | |
|---|---|
| 0x01 | errors, warnings |
| 0x02 | general TCSRV information |
| 0x04 | NLB port control trace |
| 0x08 | Detailed NLB port control trace |
| 0x10 | Logon info trace (logon errors are written with flag 0x01) |
| 0x10000000 | general TCRPC information |
| 0x20000000 | TCRPC calls |

Since TRSRV has the process name *Boot,* the trace files generated by default are *Boot0.trc* and *Boot1.trc*.

```
******************************************************
** Windows NT 4.00 Build 1381 ()
** Boot ***** Tuesday, 9-Sep-1997
** C:\TCOSS\SYSTEM\TCSRV.EXE (b4)
** created: 19:47:28.533 Tuesday, 9-Sep-1997
** kernel mode:        0:00:00.040
**   user mode:        0:00:00.020
19:47:28.593 (b4/b5) main thread created handle=84, id=b9
19:47:28.593 (b4/b5) Supervisor service active
19:47:38.698 (b4/b8) workerthread started: handle=90, id=b8, name=TCOSS
19:47:44.707 (b4/b8) createprocess: started C:\TCOSS\System\TCOSS /M:JERRY /
TCP:193.81.166.122, hProcess=94, ProcessID=ba, hThread=a4, ThreadID=bb
19:47:53.770 (b4/b7) RPC-TCSRV0:receive error '109 - The pipe has been
 ended.'/1,cnt=0,ok=0
19:59:08.310 (b4/b8) TCOSS stopped, status=268437565 ?-Shutdown requested (0. retry)
 (EventLog)
19:59:15.280 (b4/b7) RPC-TCSRV0:receive error '109 - The pipe has been
 ended.'/1,cnt=0,ok=0
19:59:25.785 (b4/b8) createprocess: started C:\TCOSS\System\TCOSS /M:JERRY /
TCP:193.81.166.122, hProcess=ac, ProcessID=136, hThread=b4, ThreadID=135
19:59:33.305 (b4/b7) RPC-TCSRV0:receive error '109 - The pipe has been
 ended.'/1,cnt=0,ok=0
20:01:20.760 (b4/b5) Shutting down supervisor service
20:01:21.641 (b4/b8) TCOSS stopped by external request
20:01:29.713 (b4/b8) workerthread stopped: handle=90, id=b8, name=TCOSS
```

```
20:01:33.278 (b4/b3) ** Library Closed
** C:\TCOSS\SYSTEM\TCSRV.EXE (b4)
** created: 19:47:28.533 Tuesday, 9-Sep-1997
** kernel mode:        0:00:00.200
**   user mode:        0:00:00.110
************************************************************
```

Even if trace level 3 is used for TCSRV, there will not be much trace output. The trace only shows when a process was stopped or started and some additional information such as command line, process and thread IDs.

Chapter 7

# Events

Event log entries are created with the following messages.

| Code | Description |
|---|---|
| 21500 | A process failed to start |
| 21501 | A process restarts |
| 21502 | Startup of a process |
| 21503 | A fatal error occurred during the startup of a process |
| 21504 | TCSRV was not shut down last time |
| 21505 | A critical event occurs in the hardware |
| 21506 | A process was started successfully |
| 21507 | A fatal error occurred during the startup of a process |
| 21508 | Restart information |
| 21509 | TCSRV started |
| 21510 | TCSRV stopped |
| 21511 | Failed to register a function to handle TCSRV's service control requests |
| 21512 | Create DoneEvent failed. |
| 21513 | Cannot open TCRPC channel |
| 21514 | Cannot create the main thread |
| 21515 | A thread exception occurred |
| 21516 | Unable to switch thread priority |
| 21517 | Unable to create CmdEvent |
| 21518 | EnableLoader is not supported |
| 21519 | Process creation failed |
| 21520 | TCSRV runloader is killing TOS server |
| 21521 | Out of memory |
| 21522 | Unable to create an event |
| 21523 | Unable to start a worker thread |
| 21524 | Stopping a process timed out |
| 21525 | Termination of a worker thread and a process |
| 21526 | Termination of a thread |

| Code | Description |
|---|---|
| 21527 | A process stopped (with status information) |
| 21528 | Unable to logon user |
| 21529 | Security identification number deleted |
| 21530 | Security identification number set |
| 21531 | Unable to reset TC9X watchdog |
| 21532 | Watchdog timeout too short |
| 21533 | Installer process terminated (with status) |
| 21534 | Shutdown of the service control manager |
| 21535 | Process <name> is still running. |

Setting the following registry key to “1” will generate an event log entry if a process is up and running (TCSRV_PROCESS_READY). This is only done when a process starts for the first time.

<*KcsRegistryPath*>/Boot/ProcessReady [DWORD] default 0.

No restart of TCSRV is necessary if you change this registry key.

The name of a process is shown in the event log for events which refer to a certain process.

# Heartbeat Events

This event log entry is written by TCSRV periodically if a process is alive.

| Code | Description |
|---|---|
| 21535 | Process <name> is still running. |

This feature can be enabled for each process which is started by TCSRV, by writing the interval in minutes into the registry value **HeartBeat** below the application's registry key. In the following example heartbeat events are created with a frequency of 30 minutes for TCSNMP as long as this process is running:

<*KcsRegistryPath*>\TCSNMP\HeartBeat 30

If the interval is set to 0, which is the default value, the heartbeat feature will be disabled. The heartbeat interval can be changed without restarting the observed processes. The changes are activated after 1 minute at the latest.

Chapter 8

# Performance Counters

TCSRV is able to create a performance counter that monitors the availability of a process. The counters are created for the object “Boot”, and the counter name is the name of the process. These are the valid values for those counters.

| | |
|---|---|
| 0 | The process is running |
| 901 | The process is starting |
| 902 | The process is stopping |
| 903 | The process is waiting |
| 1900 | The process is being restarted |
| 1999 | Unknown process |
| 2900 | The process stopped or failed |
| 3000 | The process failed and will be restarted immediately |

For this to work, you must set the following registry key to 1.

HKLM\Software\Topcall\Boot\EnablePerformanceCounters [REG_DWORD]

This registry key will automatically be created with the default value 0 at the first start of TCSRV

Chapter 9

# Protocol Type

TCSRV supports Named Pipes and TCP/IP as protocol types at the server channels. KCS Monitor or TCOSS connect to the server channels in order to query the process status.

There are only two channels. One is used by KCS Monitor and the other by TCOSS in a tandem environment.

The protocol type can by changed by means of registry values.

For KCS Monitor (TCMON):

<*KcsRegistryPath*>\Boot\TCRPCServerMode

For TCOSS:

<*KcsRegistryPath*>\Boot\TCRPCServerMode1

| | |
|---|---|
| Values: | 1: TCP/IP |
| | 3: Named Pipes (default) |

The values are set automatically by the setup program.

Chapter 10

# Enhanced Command Set

For security reasons, configuration reloading during run time and a set of commands for future enhancements were implemented in the interface between KCS Monitor and TCSRV.

All commands are available in a secure and a non-secure form. Secure commands can be used if security check is enabled and as long as the security identifier is correct.

If the security check is disabled, secure and non-secure commands can be used equally.

With the new commands it is possible to

- Set or delete security identifier
- Write to TCSRV's trace file
- Read, Write or Delete registry values at the server
- Read TCSRV's version string
- Reload the configuration of TCSRV (Startup list, Tracelevel) – allows to add or remove processes during run-time

Chapter 11

# Hardware Monitoring

On the new KCS Mainboards TC10 the Winbond W83781D Monitoring Chip is included. Three thermal inputs (one for the CPU, two for hard disks), five voltage inputs (VcoreA, VcoreB, +3.3V, +5V, +12V), two negative voltage inputs (-12V, -5V) and three fan speed controls can be viewed by the Windows Performance Monitor. The voltages are shown in millivolts, the negative voltages are shown as positive values.

An event log entry will be made if a value is not in the range between the critical values defined in

<*KcsRegistryPath*>\BOOT:

Program default

| | | |
|---|---|---|
| Temperature1CriticalMax | 55 | °C |
| Temperature1CriticalMin | 10 | °C |
| Temperature2CriticalMax | 55 | °C |
| Temperature2CriticalMin | 10 | °C |
| Temperature3CriticalMax | 55 | °C |
| Temperature3CriticalMin | 10 | °C |
| Voltage3.3CriticalMax | 3500 | mV |
| Voltage3.3CriticalMin | 3100 | mV |
| Voltage5CriticalMax | 5400 | mV |
| Voltage5CriticalMin | 4600 | mV |
| Voltage12CriticalMax | 13000 | mV |
| Voltage12CriticalMin | 11000 | mV |
| NegVoltage12CriticalMax | 13000 | mV |
| NegVoltage12CriticalMin | 11000 | mV |
| NegVoltage5CriticalMax | 5400 | mV |
| NegVoltage5CriticalMin | 4600 | mV |
| Fan1Critical | 3000 | rpm |
| Fan2Critical | 3000 | rpm |
| Fan3Critical | 3000 | rpm |

All Registry keys are of type DWORD. SNMP alert is possible for each warning.

Writing events in the event log can be enabled or disabled with the registry key

HKLM\Software\TOPCALL\BOOT\WriteEventLog [DWORD]

The default of this key is “1”. This means that if during hardware monitoring a critical event occurs, it will be reported in the event log. Setting this key to “0” prevents TCSRV from writing into the event log (only for hardware monitoring).

**Note** The hardware monitoring not supported since version 7.84.00 on Vista and Windows Server 2008.

# S.M.A.R.T. Monitoring

By using S.M.A.R.T. technology for reading the hard drive temperature, hard drives can be monitored. S.M.A.R.T. monitoring can be enabled or disabled with the registry key

HKLM\Software\TOPCALL\BOOT\EnableSmart [DWORD]

Default value is 0 on non-AS1 hardware and 1 on AS1 hardware.

The value for the critical HD temperature can be defined in

HKLM\Software\TOPCALL\BOOT\TemperatureHDCriticalMax [DWORD]

The default value is 85°C. If the temperature exceeds the configured maximum value, an event log entry will be created.

# Third Party Hardware Server Support

Third party hardware with PCI printer port cards is supported. Since these cards may use non-standard printer port addresses, the following additional registry values have been defined.

The program “finddriver” (released with KCS) adds the following registry keys:

```
HKLM\Software\Topcall\TCPCI\VendorNum [DWORD]
```

Defines the number of PCI card vendors. Default is 0, which means that only standard addresses for LPT1 and LPT2 are tried.

```
HKLM\Software\Topcall\TCPCI\Vendor{n} [DWORD]
```

Returns the ID of Vendor “n” (n is decimal, first card has n=1)

```
HKLM\Software\Topcall\TCPCI\{VendorId}BaseNum [DWORD]
```

Number of base addresses for Vendor with ID “VendorId”

```
HKLM\Software\Topcall\TCPCI\{VendorId}Base{x} [DWORD]
```

Base address of port {x} from Vendor with ID “VendorId”

**Note** These values can be used with TC10 main boards.

```
HKLM/Softw/Topcall/TCPCI/VendorNum (DWORD) = 1
HKLM/Softw/Topcall/TCPCI/Vendor1 (DWORD)   = 0x1415 (HEXADECIMAL !!!!)
HKLM/Softw/Topcall/TCPCI/1415Base1 (DWORD) = 0x378 (BaseAddress of card)
```

Finddriver is using a program for reading the base-addresses of the PCI cards. It will install all necessary dlls when started for the first time.

**Note** If you change a card or place it in another PCI slot, the base-address will change. In this case you must run “finddriver” again. If you do not change anything, it is only necessary to run this program once (AFTER installing the PCI card).

**Note** This feature is implemented since TP80.dll 7.09.09, but it is working since 7.11.01.

# Power Supply

An event log entry will be created every day if only one power supply is installed in AS1. A registry key will be automatically created, which will turn off or on the checking of the status of the power supply.

```
HKEY_LOCAL_MACHINE/SOFTWARE/TOPCALL/BOOT/PowerSupplyEvent
```

The default value is “0”, which means that no checks are done. If TCSRV finds a second power supply, this key will be set to 1 and monitoring will start. If a power supply fails, an event log entry will be generated every 24 hours.

Chapter 12

# Windows NLB Port Control for TC/LINK-SM

The TCSRV “NLB port control” supervising adds to the TC/LINK-SM NLB cluster installations complete failover and high availability. This is the feature that enables fault-tolerant TC/LINK-SM NLB cluster installations at all. (Please refer to *TCLINK-SM / TC/LINK-OC Technical Manual* to get more details on the TC/LINK-SM NLB cluster installation.) TC/LINK-SM NLB cluster installations must be operated always with enabled “NLB port control” because the NLB alone does not provide full fault tolerance. This applies also for all other TC/LINK-SM-derived link types like TC/LINK-MFP or TC/LINK-SC7.

Note that TCSRV “NLB port control” feature affects the Mail (e.g. SAP7) -> TC/LINK-SM (-> Kofax Communication Server) message transfer direction. This is the direction where the TC/LINK-SM acts as SMTP server and this is just the TCP-based service to which NLB+TCSRV can add load balancing and fault tolerance.

The Windows NLB concept itself provides failover only for the case when an NLB node (=machine) in the cluster is completely shut down: NLB directs all TCP-based traffic automatically only to the working NLB nodes. However, NLB does not provide a failover solution for the case when the machine itself is running but the TCP-based service on the node (in our case the TC/LINK-SM SMTP-listener) is stopped or hangs. The NLB infrastructure itself does not detect this and NLB continues to route SMTP connection requests to this machine. This portion of the SMTP connection requests will fail.

Now, the TCSRV “NLB port control” feature closes this gap: It checks continuously the “health state” of the TC/LINK-SM process(es); and SMTP connection requests to the TC/LINK-SM SMTP port will only be allowed when the belonging TC/LINK-SM process is operational.

The TCSRV “NLB port control” feature makes use of the following NLB feature: it is possible to “NLB-enable” / “NLB-disable” a certain port/port-range on a certain NLB-node. NLB directs the traffic only to those machines where the destination port is “NLB-enabled”. So, by permanently synchronizing the “NLB-enable” / “NLB-disable” status of the TC/LINK-SM receiver ports (registry setting <link>/TCLSM/Port2TC) with the health state of the according TC/LINK-SM processes, TCSRV can drive the SMTP traffic to those nodes where TC/LINK-SM is healthy (=just running) and divert SMTP traffic from nodes where the TC/LINK-SM service is down.

TCSRV “NLB port control” feature supports multiple TC/LINK-SM instances running in parallel on the same machine. Each TC/LINK-SM instance (=SMTP listener) must use a unique port number. All these ports are individually controlled by TCSRV. When a particular TC/LINK-SM instance on this machine is down, then TCSRV stops the SMTP traffic to the belonging port, but other ports belonging to other TC/LINK-SM instances on this machine can be still operational. TCSRV never disables the whole NLB node. It disables only a certain port or ports on this node.

The TCSRV NLB port control runs in parallel with the normal TCSRV supervising operation. When the normal supervising starts, then the NLB port control supervising starts as well; and when the normal supervising stops, so does NLB supervising. The prerequisite for the high availability is the permanent NLB port control which requires that all involved TC/LINK-SM instances stay under permanent TCSRV control.

# Configuration

This section describes the configuration.

## Configuration in TC/LINK-SM

Set registry setting <link>/TCLSM/NLBPortControl (DWORD) = 1 to enable the NLB port control feature for a particular TC/LINK-SM instance.

Note, however, that the “NLB port control” is performed by TCSRV, and accordingly, this registry setting will be evaluated/used by TCSRV (and not by TC/LINK-SM) and it will only have effect when

a) the TCSRV service is running on the TC/LINK-SM machine and

b) the TC/LINK-SM instance stays under TCSRV control.

Changing this setting takes effect only after TCSRV restart!

## Configuration in TCSRV

No extra configuration is needed in the registry.

TCSRV service must be installed and permanently run on all NLB nodes. All involved TC/LINK-SM instances must be under TCSRV control (=listed in the registry setting .../Topcall/Boot/Startup).

(TCSRV checks on start whether there is (1 or more) TC/LINK-SM process among the processes listed in the registry setting …\Topcall\Boot\Startup. A process will be considered as TC/LINK-SM process when it has the registry key <link>/TCLSM/Port2TC. If yes, then it checks whether the registry setting <link>/TCLSM/NLBPortControl=1 is set for this (these) link instance(s). If yes, then it activates the “NLB port control” feature for the according port(s) configured in <link>/TCLSM/Port2TC.)

## Configuration Windows NLB

The only prerequisite for the TCSRV “NLB port control” feature:

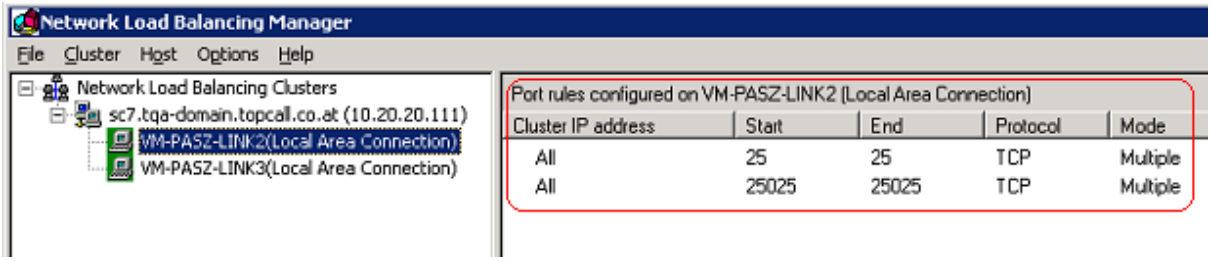
Each involved TC/LINK-SM must have its own port rule defined on NLB, where the port range must consist of one single port number:

Port range from = Port range to = value of the <link>/TCLSM/Port2TC registry setting.

By default, the <link>/TCLSM/Port2TC is 0, which means the default SMTP port (normally 25).

In this case, the actual default SMTP port number (that is 25) must be configured in the port rule and not 0, of course.

**Example**: One with “Port range from = Port range to = 25” and another with “Port range from = Port range to = 25025”.




# Operation

- The TCSRV service must permanently run on all NLB nodes.
- Never connect with the KCS Monitor to the common NLB IP address! Use the individual IP address of each NLB node to connect to it with the KCS Monitor.
- The NLB should not be controlled manually in normal production operation. (=Start/stop/suspend NLB node operation or enable/disable/drain NLB ports.) Nevertheless, TCSRV recognizes the NLB status changes (with a delay of max. 30 sec) and it will reset it to the original state that matches to the health state of the supervised TC/LINK-SM instances. E.g., if an NLB node is “suspended” manually, but at least one of the TC/LINK-SM instances is healthy on this node, than the TCSRV will reactivate this node within 30 seconds.
- After changing the registry setting <link>/TCLSM/NLBPortControl the TCSRV service must be restarted on the link machine. Note, however, that it is not recommended to operate a TC/LINK-SM (and derived links) on NLB with disabled TCSRV NLB port control because the NLB alone provides only limited fault tolerance. So, once the NLB and the according link are set up the NLBPortControl setting must be always 1.

# High Availability Restrictions

The NLB port control still leaves some short unavailability time windows (normally in the 1..8 sec range) where the failover is not provided and the SMTP connection to the common NLB IP address will fail. This occurs (always) in the following situations:

1. Unavailability time window when link server machine stops abruptly:

   In this case, it is the NLB (and not the TCSRV) that handles this situation.

   NLB requires ~5 seconds to detect a failed host.

   NLB requires 2 to 3 seconds to remove the failed host and redistribute its load to the live hosts.

2. Unavailability time window at link server boot.

   Some seconds elapse when the NLB service starts to run (always with enabled ports) until the ports are disabled by TCSRV. (They must be disabled because all links are down at machine startup.)

3. Unavailability time window at TC/LINK-SM crash

   Some (1…3) seconds elapse until TCSRV detects the crash and the according port is NLB-disabled.

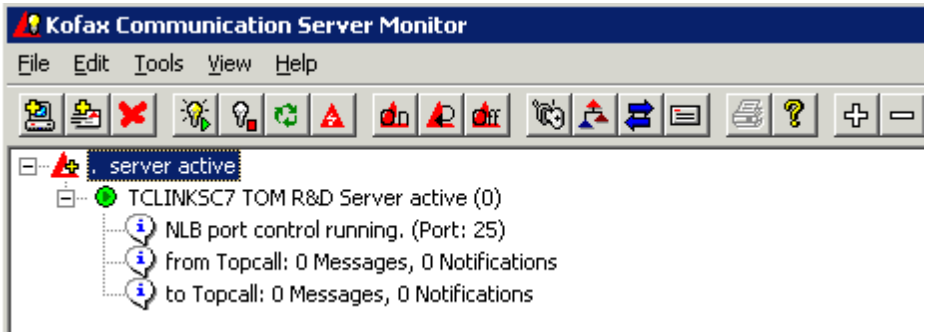
Nevertheless, when the sender SMTP client has the feature that it performs send retries (like e.g. the SAPconnect SMTP node) then the second attempt will presumably be outside of this time window and the connection request will be directed to a working node.

# Troubleshooting TCSRV NLB Port Control System

The following methods can be used to determine whether the TCSRV NLB port control system is operating properly:

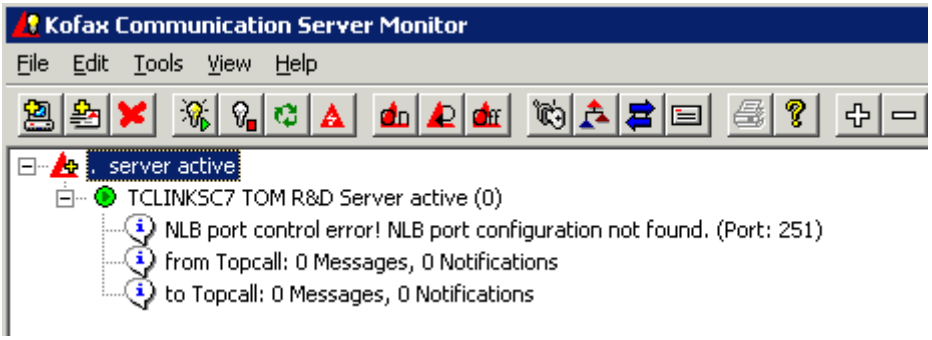
**KCS Monitor display**

Check the status line on the KCS monitor display:




“NLB port control running.” indicates proper operation.

Otherwise, the text “NLB port control error!” and an explanation is displayed:



**Note**

- This status line will only be shown, when the according link process is just running. Nevertheless, the NLB port control operates even when the process is stopped / restarting / … etc. – actually, as long as the TCSRV service runs. (This restriction in the “NLB port control” status line display is somewhat misleading. It will be corrected in the next releases.)
- Often, in error case, the message “NLB port configuration not found.” is displayed, even if this is not the most plausible explanation for the error. E.g., the machine is not part of an NLB cluster at all or the network connection to the machine is broken. The first things to check in this case: Is the machine (=node) part of an NLB at all; is this NLB node operational (“converged”); are the port rules defined at all.

**Event log**

When an error occurs during the operation, than an event log entry is written to the “Application” event log folder.

**Trace file**

In the registry setting .../Topcall/Boot/TraceLevel, the bit 0x40 activates the NLB port control trace. The bit 0x80 provides an even more detailed trace. Trace file location / name: c:\TCOSS\trace \Boot0.trc, Boot1.trc, and so on. When NLB trace is activated, it is suggested to configure increased .../ Topcall/Boot/MaxTraceFiles and .../Topcall/Boot/MaxTraceFileSize values. E.g.: MaxTraceFiles = 10, MaxTraceFileSize=5000. The operation is continuously traced, so it is possible any time to check the current port NLB states and the process health state and whether the operation is just active at all.

Chapter 13

# Troubleshooting

## TCSRV Does Not Start For a Domain User

If you start TCSRV with a domain user, any KCS application may not start with the same or other user. For TC/LINK-SM, following error is logged in Windows Event Viewer:

```
A fatal error occurred during the startup of a process C:\TCOSS\TCLP
\TCLINK.EXE "TCLINKSM" domain: kichyd UserID: <username> LogonType: S (1314 -
A required privilege is not held by the client.) Check settings, registry and
user rights.
```

**Resolution**

For running TCSRV with a domain user, the user (for TCSRV or Links) must have the following rights:

- Local administrator rights
- Log on as a service
- Replace a process level token