

Monitoring Internet Services

[Using the Internet Services Monitor](#)

[Monitoring system protocols](#)

[Viewing system abuse information](#)

[Controlling basic functions](#)

[Internet Services file logging](#)

[Debugging](#)

[Logging levels](#)

[The task list](#)

[SMTP transaction logging](#)

One of the most important day-to-day activities you will perform as an administrator is monitoring your FirstClass system. Understanding the Internet Services Monitor and how logging and debugging works helps you control possible system abuse and maintain your Internet Services to avoid any down time.

[Top](#)

Using the Internet Services Monitor

Using the [Internet Services Monitor](#), located in the Internet Services folder on the administrator's Desktop, you can perform a variety of administrative tasks either at your Internet Services machine or remotely:

- monitor the active protocols on your system
- view information on suspected abuse of your Internet Services system
- control the basic functions of Internet Services, such as logging, caching, reloading configuration files, forcing Internet connections, and shutting down Internet Services
- set logging levels for debug categories on your system per session instead of configuring the inetsvcs.cf file.

Monitoring system protocols

You can monitor the activity of your Internet protocols on the Protocols tab. Protocols are divided into two groups: outbound and inbound. The outbound group consists of outgoing SMTP mail. You set the total number of outbound mail and news sessions at "Max outgoing mail" on the Basic Internet Setup form's Mail - Main tab.

The inbound group consists of inbound mail and news plus Directory and web client connections. You set the total number of inbound Internet sessions in "Internet sessions" on the Service tab. If peak usage occurs, either increase the number of available sessions or disable low priority protocols within the group.

If you find the Task load consistently shows amber or red colors, you should try these options:

- shut down unnecessary outside applications on the Internet Services machine
For example, if your platform is Windows, turn off unnecessary NT services.
- reduce the number of Internet Sessions on the Basic Internet Setup form
This will reduce the number of Internet Sessions tasks.
- check that your Internet Services machine has enough memory and processor speed.
If necessary, upgrade your machine.

Viewing system abuse information

You can monitor security breaches, attacks on your system, and statistics for your RBL configuration, on the Security tab. For example, IP addresses attempting to launch Denial Of Service attacks, the number of connection attempts to your webserver, and messages suspected of being spam. IP addresses can also be added to the temporary IP blocklist or cleared.

Controlling basic functions

You can update template and web page changes, log tasking, clear your DNS, and perform other basic functions that you previously had to perform from the Internet Services console, on the Control tab. Some common tasks performed using this tab are:

- reloading the configuration forms after changing the web templates

Note

FirstClass will reload the configuration forms automatically every couple of minutes. However, if you don't want to wait, you can click Refresh.

- flushing the HTTP cache after changing the web pages
- logging and clearing the list of blacklisted and blackholed sites.

Other intermittent tasks are:

- checking the speed at which Internet Services completes its tasks
- viewing what users import on their Mail Import form
- clearing the DNS cache.

If you find that the task load is running slow, you can create a file by clicking the Log IS Task List button. This allows you to see which tasks are using the most resources.

[Top](#)

Internet Services file logging

You can configure Internet Services to write logging information to disk, so that it can be reviewed at a later date. The Internet Services log file is called InetSvcs.log (Windows) or fcisd.log (UNIX daemon). This file is stored in the same folder as the Internet Services executable.

To write logging information to disk, use this keyword in the [Config] section of the inetsvcs.cf file that is also located in the same folder as the Internet Services executable:

```
Logging = 1
```

To disable logging (the default), use:

```
Logging = 0
```

If you specify no logging, you can force logging on while Internet Services is running by clicking the Write Log to Disk button on the Logging tab of the Internet Services Monitor. The next time you restart Internet Services, the logging value set in inetsvcs.cf will once more be used.

With logging on, Internet Services creates a new log file on startup. By default, the existing log file is renamed inetsvcs.OLD (or fcisd.OLD), and any previous .OLD log file is lost. If you want to keep older log files, use this keyword in the [Config] section of the inetsvcs.cf file:

```
LogRollover = 1
```

The previous .OLD log file will then be renamed xxxYYYYMMDD_HHMM.log before the existing log file is renamed to .OLD.

Debugging

You can control Internet Services debugging from three different locations:

- from the [Debug] section of the inetsvcs.cf file at startup

This section is used to set the initial levels for Internet Services debugging. The debug keywords used in this file are prefixed by "DBG_". For example, to set the initial level of HTTP server debug logging to 3 when Internet Services starts up, you would use this keyword:

```
DBG_ICHTTP = 3
```

- from the Logging tab on the Internet Services Monitor form while Internet Services is running
- from the Headermatch file, on a per-request basis, using a "set debuglevel=<int>" statement.

Debug categories

Setting debug levels causes Internet Services to log information about its protocol activities. The higher the level set the more verbose the logging information Internet Services will generate. We recommend that

you activate debug logging only on the advice of OpenText Customer Support, because using debug logging may negatively affect the performance of Internet Services.

In this table, Type is the keyword used in the .log file to indicate the type of debugging. Level is the keyword used in the inetsvcs.cf file to set the initial debug level.

Category	Logs	Type	Level
Configuration	the loading and parsing of configuration data	InetCfg	DBG_InetCfg
DNS Resolver	the actions of the DNS resolver	Resolver	DBG_Resolver
FCP Proxy	the connections and data transfer of proxy sessions	FCPProxy	DBG_FCPProxy
Gateway Monitor	the FCP communication between Internet Services incoming message protocols and the FirstClass server	GWSrvr	DBG_GWSrvr
FTP Server	the actions of the FTP server	ICFTP	DBG_ICFTP
HTTP Scripting	HTTP script operations	ICHTTPScr	DBG_ICHTTPScr
HTTP Server	the actions of the HTTP server	ICHTTP	DBG_ICHTTP
IMAP Importer	the scheduling of inbound messages from an IMAP server	IMAP4CIn	DBG_IMAP4CIn
IMAP Import Message	the receiving of inbound IMAP messages	IMAP4Msg	DBG_IMAP4Msg
IMAP4 Server	the actions of the IMAP4 server	ICIMAP4	DBG_ICIMAP4
Internet Services	the handling of incoming connections	InetSvc	DBG_InetSvc
LDAP Messages	the constructing of responses for the LDAP protocol LDAP logging is separated into two parts: the first manages the LDAP connection and the second interprets and formulates responses to the LDAP client's request.	LDAPMsg	DBG_LDAPMsg
LDAP Server	the actions of the LDAP server	ICLDAP	DBG_ICLDAP
Mail Decoding	the decoding of Internet messages	IMRFCd	DBG_IMRFCd
Mail Encoding	the encoding of Internet messages	IMRFCe	DBG_IMRFCe
MIME Decoding	the decoding of MIME messages	IMMIMEIn	DBG_IMMIMEIn
Name Translation	the parsing and translating of email addresses	FCNmTrn	DBG_FCNmTrn
Notifications	the sending of Apple and BlackBerry push notifications	Notify	DBG_Notify
POP3 Client	the scheduling of inbound POP3 messages (POP3 import)	POP3CIn	DBG_POP3CIn
POP3 Client Messages	receiving of inbound POP3 messages (POP3 import)	POP3Msg	DBG_POP3Msg
POP3 Server	the actions of the POP3 server	ICPOP3	DBG_ICPOP3
RSS Importer	the scheduling of connections to RSS feeds	RSSCIn	DBG_RSSCIn
RSS Import Message	the receiving of inbound RSS feeds	RSSMsg	DBG_RSSMsg
Server to FC Connections	FCP communication between Internet Services and the FirstClass server for client and Directory protocols (POP3, FTP, HTTP, LDAP)	InetCli	DBG_InetCli
SMTP Connection	queuing of outbound SMTP messages	SMTPCIn	DBG_SMTPCIn

SMTP Messages	delivery of outbound SMTP messages	SMTPMsg	DBG_SMTPLMsg
SMTP Server	delivery of inbound SMTP messages	SMTPCon	DBG_SMTPLCon
SSL	information relating to the SSL encryption layer on secure connections	SSL	DBG_SSL
Task List	the reports about changes in Internet Services task states	TaskList	DBG_TaskList

Logging levels

Each debug category is set to a logging level between 0 and >5. In general, these levels are

- 0 - none
- 1 - connection messages about connecting and disconnecting
- 2 - session messages about the progress of the request
- 3 - protocol messages showing communication at the protocol level
- 4 -"Verbose" debugging information
- 5 -"Very verbose" debugging information
- >5 - will severely impact performance and generate huge log files.



Tip

We recommend you set logging levels at or below 2, unless you require more information to identify a problem. If this is the case, only change the specific debugging categories relating to the problem or the logging may affect the performance of Internet Services.

The task list

The main function of the task list is to show which tasks Internet Services is doing at any particular time. Examples of tasks include adding Internet sessions or enabling and disabling a protocol, setting connection times, and opening ports.

You can access the task list option from the Control tab on the Internet Services Monitor form, when Internet Services is running as a Windows service or Unix daemon.

The task list can be very helpful in correlating log information; think of it as a snapshot of what you can see when you have the debug keyword DBG_TaskList set to 5. Task list information is most useful in debugging situations where Internet Services stops processing a particular protocol or connection.

The task list itself starts with a number in brackets [], which is the task ID of the item. This number can have a character before it indicating the task's kernel state, the most common being S which means waiting for a semaphore. Following the task ID is the task's name, which correlates with the DBG_xxxx keywords without the DBG_ prefix. The state of the task is then displayed as numbers (with separating commas) followed by a text description of the state. For example:

```
[s 3] main- 0. 0. 0. 0: 0, 0, 0, 0, Idling
[s 4] DNSr- 0. 0. 0. 0: 0, 0, 0, 0, Lurking
[S 5] ISvc- 0. 0. 0. 0: 0, 1, 0, 0, Waiting for queued connection
[S 6] ISvc- 0. 0. 0. 0: 0, 1, 0, 0, Waiting for queued connection
[S 7] ISvc- 0. 0. 0. 0: 0, 1, 0, 0, Waiting for queued connection
So it is now [1 2] 3- 4.4.4.4: 5, 6, 7, 8, 9.
```

Task numbers

- 1 == semaphore flag
- 2 == task id
- 3 == task type
- 4 == connection IP address
- 5 == connection port
- 6 == connection time
- 7 == task data 1

- 8 == task data 2
- 9 == task state

[Top](#)

SMTP transaction logging

The SMTP transaction log is intended to be a forensic tool that tracks all SMTP commands sent and received by Internet Services, as well as the Subject and Message-ID, which allows you to verify what email has (or hasn't) been sent or received. This is a separate log file from the diagnostic log file and can be enabled with minimal impact on performance.

All inbound and outbound SMTP transfers are logged in a file named smtp-YYYYMMDD.log. Log entries are in the form:

[<date and time>] <Client or Server>-<TID>: <what>: <data>

where

[<date and time>]	is in the same format as the log file
<Client or Server>	is Client when IS is sending a message to another SMTP server or Server when IS is receiving a message
<TID>	is the task id as in the log file
<what>	is one of Snd, Rcv, ID or Sub Snd and Rcv are used the same as in the log file (the SMTP commands). ID indicates the Message-ID of the message. Sub is the Subject.
<data>	is what was sent, received, the Message-ID or the Subject.

To configure and activate the SMTP transaction log, fill in the SMTP Log tab on the Advanced Mail form.

[Top](#)