2

Taskmaster Web Configuration

Chapter 2 provides information that complements the instructions for installing, configuring, and running Taskmaster Web found in the *Taskmaster 7.5 Installation and Configuration Guide*, including:

2.1 Introduction

The *Taskmaster 7.5 Installation and Configuration Guide* describes the steps you take to install, configure and run all of the *Taskmaster* components, including the set up of the major *Taskmaster Web* components:

- **Taskmaster Web Server.** This Microsoft IIS instance is home to the Taskmaster Web Site and manages the information that flows between pages of the Web Site and *Taskmaster*.
- **Taskmaster Web Site.** The IIS Web Site consists of *Taskmaster Web's* **Home** page and pages assigned to individual applications. These pages are in the folders of the **Datacap** directory's **tmweb.NET** folder.
- **Taskmaster Web Clients**. A Taskmaster Web Client is a computer and user with access to the Taskmaster Web Site.

2.2 Apps.ini File Settings

Providing Taskmaster Web Clients with access to an application requires a set of entries in *Taskmaster Web's* **apps.ini** file. This file is found on the Server **\datacap\tmweb.NET** directory.

When you open the file with a text editor such as *Notepad*, specifications for each pre-configured application appear sequentially.

For a complete explanation of the format of the connection strings that connect the application to its Admin, Engine, and Report Viewer databases, see the *Taskmaster Administrator's Guide* Appendix A Connection Strings.

Here are the current specifications for the *1040EZ* training application:

```
[1040EZ]
TMServer=127.0.0.1
Port=2402
AdmDSN=PROVIDER=MSACCESS;DSN=C:\Datacap\1040EZ\process\1040Adm.mdb;CATALOG=;DBNTA=;
EngDSN=PROVIDER=MSACCESS;DSN=C:\Datacap\1040EZ\process\1040Eng.mdb;CATALOG=;DBNTA=;
RptDSN=PROVIDER=MSACCESS;DSN=C:\Datacap\1040EZ\process\Rptview.mdb;CATALOG=;DBNTA=;
DateTimeSeparator=#
Delay=10
Retries=3
BatchSelectionCustomFields=
Debug=0
Oracle=0
```

The table below describes each setting in a section of the **apps.ini** file. If your **Datacap** configuration includes multiple applications, you must configure each application in the

apps.ini file separately. The table below uses the settings from the *1040EZ* application for its examples.

Specification	Description
[1040ez]	The Application ID. Users must enter this value when they access the application.
`TMServer = 127.0.0.1`	The name ***or*** address of the ***computer*** on which Taskmaster Server resides: this server is the link between the Taskmaster Web Site and the individual application.
`Port=2402`	The TCP/IP port for communications to Taskmaster Server. The default value is *2402*. The value can be change when you set up Taskmaster Server. For details, see the *Taskmaster Administrator's Guide.*
`AdmDSN=Provider= MSACESS……`	The Connection String associated with the application's Admin database. Appendix A of the *Taskmaster Administrator's Guide* explains and provides samples of Connection Strings
`EngDSN=Provider= MSACESS……`	The Connection String of the application's Engine database. Appendix A of the *Taskmaster Administrator's Guide* explains and provides samples of Connection Strings
`RptDSN=DSN=1040Rpt`	The Connection String for the application's Report Viewer database. Appendix A of the *Taskmaster Administrator's Guide* explains and provides samples of Connection Strings
`DateTimeSeparator=#`	The delimiter used to separate elements of a Date or Time. If the application's Engine database is an Access database, `DateTimeSeparator=#.` For a SQL Server or Oracle database, `DateTimeSeparator='` (apostrophe)_
`Delay=10`	The number of seconds all Taskmaster Web Clients are to wait before running the next task – or before looking for the next batch to be processed by the current task. If this setting is set to 2 or less, the OK and Continue buttons shown when the task is finished are grayed out, and disabled. This is useful if you only want users to be able to put batches on *Hold*, or to be able to *Stop* batch processing.
`Retries=3`	The number of times *Taskmaster Web* is to attempt to re-connect with Taskmaster Server Service if the initial attempt fails.

Specification	Description
`BatchSelectionCustom Fields=`	**Optional:** The names) of any "custom" field(s) you have added to the Batch Information Table of the **Job Monitor** page and **Batch Selection** page. (For more about custom fields, see Chapter 3 of this guide, and Chapter 5 of the *Taskmaster Windows & Dialogs Reference.)*
`Debug = 0`	Indicates if *Taskmaster Web* is to update the **Debug** table of the application's Engine database (`Debug=1`0.) This table accumulates information about the steps of each batch in the current workflow.
`Oracle=0`	Stipulates that the application's databases are not Oracle databases. `Oracle=1` specifies Oracle databases.

2.3 Application Security

Taskmaster Application Security intentionally imposes further restrictions on the ability of a *Taskmaster Web* user – an operator, Administrator or Supervisor – to access an application's information and operations.

These restrictions take three forms:

Security IDs. To sign on to *Taskmaster Web*, a user ***must*** supply three codes: User ID, Password, and Station ID. The User ID and Password are elements of a formal User Definition; the Station ID is an element of a Station Definition.

Administrative Privileges. Settings in the User Definition strictly limit an individual's access to administrative data ***and*** to administrative procedures. As a result, a "typical" operator cannot review or modify a workflow's structural components or its processing detail.

Job-Task Permissions. To launch a particular task assigned to a particular job, the definitions of both user ***and*** station must include permission to carry out this Job/Task combination.

For more information about Application Security, see Chapter 3 of this guide, Chapter 5 of the *Taskmaster Administrator's Guide,* and the Help topics covering *Taskmaster Web's* Security pages.

2.4 Clustering and Network Load Balancing

Microsoft supports clustering and network load balancing (NLB) options on Windows 2000 Advanced, or Datacenter Server and Windows 2003 Server. NLB allows multiple IIS servers to share loads in a single application such as *Taskmaster Web*. You'll find a good guide to initial setup at

http://support.microsoft.com/default.aspx?scid=kb;en-us;323437.

Taskmaster Web requires some particular settings, and only certain configurations have been tested successfully.

Dual NIC NLB Clustering Setup Procedures

To set up NIC NLB Clustering, take these steps:

1. Set up a second network card on each computer in the cluster. These will be used for NLB "administrative" communications only.

2. Assign the *admin* NIC's fixed IP addresses in a separate subnet that is completely different from the subnet used on your primary NIC. The second subnet can use a "made up" address range. Microsoft recommends using addresses such as 10.0.0.1 and 10.0.0.2: the subnet mask can be 255.0.0.0.

3. Connect the second NIC cards together to a dedicated hub or switch that is not connected to your primary LAN.

   Dual NIC clustering works with unicast operation mode. The cluster name is case-sensitive and it has to be same fully-qualified domain name on each host; otherwise, the NLB cluster will not converge.

   Cluster parameters and port rules are set identically on all cluster hosts. Both the dedicated IP address and the cluster IP address must be static IP addresses. They cannot be DHCP addresses.

4. Ensure that all hosts in a cluster belong to the same subnet and that the cluster's clients are able to access this subnet.

5. To install and configure NLB in Windows 2003, right-click on **My Network Places**, then select **Properties**. The resulting ***Network Connections*** dialog box lets you configure the multiple network interfaces for a particular cluster host

NLB Port Rules:

Affinity Single

Create a port rule for HTTPS:
Affinity Single

Port rule for TMServer:
  Port range 2402 to 2402
Protocols Both
Affinity Single

From Microsoft Technet
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/operate/nlbbp.asp:

The following tools can be used to troubleshoot NLB clusters:

1) Event Viewer.

2) NLB.exe Display & Query Commands.

3) Ping.exe.

4) Network Monitor parser for NLB - part of the Windows 2000 Server resource kit. (Refer to KB article Q280503 for more information.)

5) Performance Monitor : CPU Load, Network Interface: packets/sec, Web Service: connection attempts/sec.