3

Installation and Setup

- Installation and Setup Overview

- Installing Control Station

- Establishing Web Server Security

This chapter describes how to install the Control Station server. It also offers guidance on how to set up web server security.

Installation and Setup Overview

This chapter describes how to install and set up Control Station. The Control Station is a browser-based tool that has a server-side component that communicates with a Java applet. The Control Station server-side component installs and operates on an NT machine. The Java applet client operates from within any of the supported browsers.

Before you can use Control Station, you must:

- Install the Control Station server-side components
- Establish web server security

Installation Requirements

This section describes the server and client requirements needed to support Control Station. The Control Station server runs on a Windows NT server. Each client machine that accesses Control Station requires Internet Explorer 5.5 or Netscape 4.72 installed.

NT Server Requirements

The following table lists the minimum NT server hardware requirements needed to effectively support Control Station:

Table 3.1 Hardware Requirements for Control Station

Resource	Requirement
Machine Type	Pentium II workstation or all-purpose laptop
# of CPUs/Speed	1/400MHz
RAM	128MB
Hard Drive Space	15MB

The following table lists the minimum NT server software requirements needed to effectively support Control Station:

Table 3.2 Server Software Requirements for Control Station

Resource	Requirement
Operating System	Microsoft Windows NT 4.0 Service Pack 6a; Option Pack
Web Server	• Microsoft Internet Information Server (IIS) 4.0 • Microsoft Management Console (MMC) 1.1a Service Pack (for Daystrom Scheduler)
Drive Formatting	Format your hard disk to be NTFS compliant.

The Microsoft Internet Information Server (IIS) 4.0 operates as your web server. If the Daystrom Scheduler is going to be used, then the Microsoft Management Console (MMC) 1.1a must be installed on the Control Station server machine. The scheduler operates as an MMC snap-in utility that provides the administrator with a tool to schedule scripts that reside on the scheduler server.

In addition to the above requirements, you must map a network drive on your Control Station server to the `daystrom.ini` file on the Content Server.

Client Requirements

This table lists the client software requirements needed to access Control Station:

Table 3.3 Client Software Requirements for Control Station

Resource	Requirement
Web Browser	Internet Explorer 5.5 or Netscape 4.72

Installing Control Station

If you are installing Control Station as part of a distributed (or single server) configuration, perform "Installing the Control Station Server" on page 18.

For more information about installation, configuration and the Content Server, refer to the Daystrom *Installation and Setup for NT* or the *Daystrom Installaton and Setup for Solaris Ultra Sparc* manual.

Installing the Control Station Server

> ℹ Make sure you have installed Microsoft IIS with MMC 1.1a and Internet Explorer 5.5 or Netscape 4.72 prior to installing the Control Station server. Map a network drive on your Control Station server to the `daystrom.ini` file on the Content Server.

1 On the NT machine you have designated as the Control Station server in your configuration diagram, run the `Setup.exe` file from the `Install` directory of the Control Station installation CD. The Welcome dialog box appears.

2 Click Next. The License Agreement dialog box appears.

3 Read the agreement and click Yes. The Setup Types dialog box appears.

4 Choose Control Station from the list and click Next. The Choose Destination Location dialog box appears.

5 Click Browse to navigate to the installation destination where all files will be written. The default is `c:\daystrom`.

6 Click Next. The Configuration File dialog box appears.

7 Type the path or click Browse to navigate to the mapped network drive where the `daystrom.ini` file on your Content Server is located.

8 Click Next and the System Information dialog box appears.

9 The IP address of the current machine displays in the text box. If this is the IP address that should be used, click Next, otherwise type the desired IP address.

10 Type the port for Control Station to listen for requests (the default is 82). Click Next. The Information dialog box appears listing the web tool setup information you entered.

11 Click Next if the information is correct or click Back to change any setup information.

12 A message appears stating that you must run the csreg.bat script after installation. Click OK.

13 The Restarting Windows dialog box appears, suggesting that you restart your system. You cannot run Control Station until you restart Windows. Click Yes to restart Windows.

14 At the Command Prompt, change to the `[daystrom]\bin` directory, where `[daystrom]` is the eCommerce Solutions installation location.

15 Type the following to run the script that registers DLLs for Control Station:

```
csreg
```

How Does Control Station Establish Connections?

The following connections are established by default and can be changed during installation:

Table 3.4 Default Control Station Connections

By default, Control Station establishes connections with each:	Using:
Web Broker machine	port 8900 for the Admin port. The port number will automatically be incremented by 1 for each additional Web Broker instance installed in a site. For example 8901, 8902, etc.
Public PAS	port values ranging from 8502 to 8599 (depending upon the number of installed PASs in a site). The port number will automatically be incremented by 1 for each additional PAS instance. For example 8503, 8504, etc.
Business Station PAS	port 8501.

You should assign the appropriate port connections for your own system. Consult your configuration map for the ports assigned to each Daystrom server component in the configuration.

For more information about port assignments and your configuration map, refer to the Daystrom *Installation and Setup for NT* or the Daystrom *Installaton and Setup for Solaris Ultra Sparc* manual.

Establishing Web Server Security

Before you can use Control Station, you must establish web server security. This section describes the requirements to set up user account security on your web server. Procedures in this section describe how to:

- Set up a dedicated user account for accessing Control Station on your web server

- Configure Control Station to allow access to the configuration file

- Set up the web server for HTTPS

Overview of Security Requirements

Security is controlled by the Microsoft Internet Information Server (IIS). You will configure the Control Station web site to use anonymous authentication with a dedicated domain account (for example, CS_USER) for a distributed setup or a single server setup. In a single server setup, you can set the anonymous user to the oasisusr account. In either case, it is critical that you change the Control Station administrative password for security purposes.

For more information on the Control Station administrative password, see "Administrative Accounts Management" on page 103.

The user must also install a Secure Sockets Layer (SSL) secure certificate on the web server to utilize HTTPS (a secure protocol). A secured server uses SSL technology to provide a safe, secure way to transmit sensitive information. It consists of software installed in browsers and on servers and can be easily obtained by obtaining a Seller's Certificate from a certificate authority and installing it on your existing secured server.

For more information on SSL, see "Setting Up the Control Station Web Server for HTTPS" on page 28.

How Do You Set Up User Accounts for Control Station Web Servers?

To set up a dedicated account for accessing Control Station, you must perform the following steps:

- Obtain a domain user name (for example, CS_USER) from your NT domain administrator.

- Grant the CS_USER domain user CHANGE access to the Control Station home directory.

  For more information, see "Granting CHANGE Access to the Control Station Home Directory" on page 23.

- Grant the CS_USER domain user CHANGE permission to the directory containing the `daystrom.ini` file.

  For more information, see "Granting CHANGE Permission to the Directory Containing the Daystrom.ini File" on page 24.

- Change the anonymous user of the Control Station web site to the appropriate account based on the type of Commerce Exchange configuration.

- **For more information, see "Reconfiguring Anonymous Users" on page 27.**

  > ⓘ The users created by these procedures are NT users. These are not the same as Control Station administrative users.

Granting CHANGE Access to the Control Station Home Directory

ⓘ Do not run any eCommerce Solutions services when permissions are being set.

1 Open a Windows NT Explorer window.

2 In Windows NT Explorer, find the installation directory for Control Station. For example: `C:\daystrom`

3 Right-click the home directory of the Control Station installation to open a drop-down menu.

4 In the drop-down menu, click Properties. The Properties dialog opens.

5 Click the Security tab and click the Permissions button. The Permissions dialog opens.

You can either view or set permission information on the selected items. By default, this is set to "Everyone."

6 Remove the name "Everyone" and add the CS_USER domain user to use the Control Station client.

7 Assign the CS_USER domain user CHANGE access and save your work. Click OK.

8 Check "Replace Permissions on Subdirectories."

9 Check "Replace Permissions on Existing Files."

10 A message box appears asking you if you want to replace the security information on all existing subdirectories. Click Yes.

11 Continue with "Granting CHANGE Permission to the Directory Containing the daystrom.ini File" on page 24.

Granting CHANGE Permission to the Directory Containing the Daystrom.ini File

> ⓘ Do not run any eCommerce Solutions services when permissions are being set.

1 Click Start > Settings > Control Panel.

2 In the Control Panel window, click System.

3 In the System Properties window, click the Environment tab.

4 In the System Variables pane, scroll up or down to find the IW_REGISTRY variable.

5 In the Value field, read the complete path to the `daystrom.ini` file and make a notation of that path name.

6 Click Cancel to close the System Properties window.

7 Open an Explorer window and find the directory referenced in the path to the `daystrom.ini` file from Step 5.

8 Highlight the directory name containing the `daystrom.ini` file and right-click to open a drop-down menu.

9 In the drop-down menu, click Properties.

10 In the <dir name> Properties dialog, click the Security tab.

11 Click the Permissions button to open the Directory Permissions window.

- Do not check "Replace Permissions on Subdirectories." Remove the check beside this option, if it is checked.
- Check "Replace Permissions on Existing Files."

You can either view or set permission information on the selected items. By default, this is set to "Everyone."

12 Remove the name "Everyone," and replace it with the new group name that was created for the Control Station users. Click OK.

13 Assign the CS_USER domain account CHANGE access.

14 Click OK in the Directory Permissions window to close it and accept the changes.

15 Click the Sharing tab and then the Permissions button. The Access Through Shared Permissions window appears.

16 Remove the EVERYONE group and add the CS_USER domain account and the local administrators group where the oasisusr account is located. Assign CHANGE permission to the CS_USER domain account and FULL CONTROL permission to the local administrators group. Click OK.

17 Click OK in the <dir name> Properties window to close it.

How Do You Allow User Access to the Configuration File?

If the `daystrom.ini` file is not local to the Control Station Web Server, then the anonymous account information must match the access account for the machine on which the configuration file resides.

The following sections identify possible relationships for the setting of the web server's Allow Anonymous Access parameter to both the location and accessability of the configuration file. In each case, they summarize how the anonymous user has access to the Control Station server.

Single Server Configuration

In a single server configuration, the `daystrom.ini` file is on the same machine as the Control Station. By default, every incoming user will be associated with the security context of the local IIS user (for example, IUSR_COMPUTERNAME). No further configuration is necessary for NT.

Distributed Configuration with Anonymous Access

In this configuration, the web server authentication method, Allow Anonymous Access, is enabled. The configuration file is not on the local Control Station server. To allow an anonymous user to access Control Station, you must configure the anonymous user with a valid domain user that exists on the server containing the configuration file.

For more information on configuring anonymous users, see "Reconfiguring Anonymous Users" on page 27.

Reconfiguring Anonymous Users

> ⓘ Perform this procedure if the Control Station server is on a different machine than the Content Server.

1 Open Programs > Windows NT 4.0 Option Pack > Microsoft Internet Information Server > Internet Service Manager

2 Right-click CSWebSite and select Properties. The CSWebSite Properties dialog box appears.

3 On the Directory Security tab, click the Edit tab. Enable the Allow Anonymous Access option only.

4 Click the top Edit button beside Allow Anonymous Access. The Anonymous User Account dialog box appears.

5 Click the Browse button. The Select Windows NT User Account dialog box appears.

6 Choose the domain where your Control Station domain account resides. Select a valid user account from the list of NT User Accounts. That user account must have at least CHANGE access to the `daystrom.ini` file.

7 On the Anonymous User Account window, uncheck Enable Automatic Password Synchronization and enter the password for the user selected.

8 Click OK and retype the password to confirm it. Click OK.

9 Continue clicking OK until the CSWebSite Properties dialog box closes.

> ⓘ If Control Station and eCommerce Solutions are installed on the same machine, the anonymous user can be the local oasisusr account. If eCommerce Solutions and Control Station are on different machines, then the anonymous user is the CS_USER domain account.

Setting Up the Control Station Web Server for HTTPS

User authentication is provided by establishing a Control Station administrative user account on the machine running the HTTP server and configuring the HTTP server to require user authentication at login. The Control Station client supports both the HTTP and HTTPS protocols.

The out-of-the-box installation defaults to HTTP support. A single administrative user account is created on the Control Station server machine with a default username and password. The defaults are ControlStation/ControlStation.

For more information on administrative user accounts, "Administrative Accounts Management" on page 103.

In order to use SSL (HTTPS) from the browser to the Control Station server-side component, a digital certificate must be installed and set up. This provides the security on the web server used to host the Control Station server-side component. The use of SSL will be transparent to the Control Station server-side component and will be supported by the Control Station client. Administrators will be able to choose the level of security they require based on their own personal security policy.

> ⓘ The use of the SSL (HTTPS) protocol on the IIS to encrypt the transmission of sensitive data, including user names and passwords is strongly recommended.