Enclosed is a new edition of *User Interface Installation and Administration* for Release 17/18
UI Desktop 2.2/UI Web 2.3 Envision 4.8.1. This edition replaces your existing manual.

**The Primary Changes Made**

- The manual has been updated for UI Web 2.3.
- AnswerNet issues 35443.52 and 37819.56 have been resolved.
- References to UniData Distributed, a configuration that is no longer supported, have been removed from the manual.

**Updating Your Manual**

Replace *all copies* of your existing manual with this new edition as it will be the basis for all future updates.
User Interface Installation and Administration

Release 17/18
UI Desktop 2.2/UI Web 2.3
Envision 4.8.1
April 7, 2008

For last-minute updates and additional information about this manual, see AnswerNet page 670.
Implementing Security ................................................................. 5-6
  Implementation Options ......................................................... 5-6
Implementing Security for the Application Server .................. 5-8
  Obtaining Certificates for the Application Server ................ 5-8
  Procedure for Obtaining a Certificate for the Application Server 5-8
  Installing a Certificate on UniData ........................................ 5-11
  Applying a Certificate to the Application Server ................. 5-13
  Procedure for Applying a Certificate to the Application Server 5-14
Implementing Security for the UI Web Server ....................... 5-16
  Obtaining Certificates for the UI Web Server ..................... 5-16
  Importing Certificates to Generate the Vault File ............... 5-18
  Generating the Vault File .................................................. 5-20
  Installing the Vault File ................................................... 5-22
  Procedure for Installing the Vault File ............................... 5-22
  Applying a Certificate to the UI Web Server ..................... 5-29
Viewing Certificates ............................................................... 5-32
  Procedure for Viewing Certificates ................................. 5-33

Query Builder Security
In This Chapter ................................................................................... 6-1
Understanding Query Builder Security ............................................ 6-2
  Keywords Allowed in Query Builder ....................................... 6-2
  Forms Used .............................................................................. 6-3
Securing Query Builder ................................................................. 6-4
  The UI Administration Parameters (UIPR) Form .................... 6-4
    Noteworthy Fields on the UIPR Form .................................. 6-4
  The Sec Class QueryBuilder Access (SCQA) Form ............... 6-5
    Noteworthy Fields on the SCQA Form ................................. 6-6
  The Query Builder Computed Column (QBCC) Form ............ 6-7
    Noteworthy Fields on the QBCC Form ............................... 6-8
  Procedure for Securing Query Builder .................................. 6-9

Defining the Startup Sequence
In This Chapter ................................................................................... 7-1
Before You Begin ............................................................................. 7-1
Startup Sequence for a Colleague Session ............................... 7-2
  Understanding the Startup Sequence for a Colleague Session 7-2
    Operating System Startup Sequence (UNIX Only) .............. 7-4
    Database Startup Sequence ............................................. 7-4
    Considerations for Strings and Prompts .......................... 7-6
  Procedure for Defining the Startup Sequence for a Colleague Session 7-7
    Updating Local Installations With Changes to the Startup Sequence 7-9
    Method A ......................................................................... 7-9
    Method B ......................................................................... 7-10
  Setting the Startup Directory (Windows Only) ..................... 7-10
  Setting the Max Logon Attempts Allowed ............................ 7-13
  Procedure for Setting the Max Login Retries Allowed ........... 7-13
# Client Deployment

In This Chapter ................................................................. 8-1
Before You Begin ................................................................. 8-1
  Startup Sequence ............................................................... 8-2
  Secure Transmissions ......................................................... 8-2
Procedure for Installing UI Desktop a on User’s PC .................. 8-3
Deploying the wIntegrate Applet Client for UI Web .................. 8-8

# Client Setup

In This Chapter ................................................................. 9-1
Before You Begin ................................................................. 9-1
Setting Up the UI Web Exit URL ........................................... 9-2
  Procedure for setting up the UI Web Exit URL ...................... 9-2
Adding and Removing UI Web Users ...................................... 9-3
  Procedure for Adding Users to a Database ......................... 9-3
  Procedure for Removing User Access ................................. 9-4
Adding Databases ............................................................... 9-6
  Procedure for Adding a Database in UI Desktop .................. 9-6
  Procedure for Adding a Database in UI Web ....................... 9-7
Viewing a User’s Databases ................................................ 9-8
Customizing User Fields ..................................................... 9-10
  Customizing Tab Sequencing .............................................. 9-11
    Procedure For Customizing Tab Sequencing ....................... 9-11
  Customizing Required Fields ............................................ 9-13
    Procedure for Customizing Required Fields ....................... 9-13
  Customizing Field Access ................................................ 9-14
    Procedure for Customizing Field Access ......................... 9-14
Using the Browser-Based Help System .................................... 9-16
  A Tip about Web Browsers ................................................ 9-17
    Microsoft Internet Explorer ........................................... 9-17
    Mozilla Firefox ........................................................ 9-18
    Apple’s Safari ......................................................... 9-19

# Uninstalling UI

In This Chapter ................................................................. 10-1
Uninstalling UI Desktop 2.x ............................................... 10-2
  Procedure to Uninstall UI Desktop 2.x ............................... 10-2
Uninstalling UI Desktop 1.5 ................................................ 10-3
  Creating the Unregister Batch File ..................................... 10-3
Uninstalling UI Desktop from a User’s PC .............................. 10-4
  Uninstalling a Full Local Installation ................................. 10-4
  Uninstalling a Shared Installation ..................................... 10-4
  Uninstalling the UI Desktop Master Client Software ............. 10-5
Uninstalling UI Web ............................................................ 10-6

# Appendixes

A. Integrating Your Existing Practices

In This Appendix ................................................................. A-1
B. Example Procedures for the Operating System Startup

In This Appendix ........................................................................................ B-1
Examples ................................................................................................. B-1
   Example A: Mapping the UIRM Form to Access the Appropriate Database
      from a Login Menu ........................................................................ B-2
   Example B: Mapping UIRM to React to Password Expiration ............. B-3
   Example C: Mapping the UIRM Form to Bypass a Login Menu .......... B-5
Introduction

About This Manual

What This Manual Covers

This manual provides procedures for installing User Interface (UI) Desktop and UI Web, two types of graphical user interface for Colleague and Benefactor. UI enables any user to easily and intuitively navigate the Colleague/Benefactor system. With UI, users have a fast, secure and transparent tool to interact with Colleague/Benefactor, so they can work more efficiently.

How This Manual is Organized

Chapter 1, “Introduction,” which you are reading now, provides information about this manual and an overview of the installation process.

Chapter 2, “Before You Begin,” describes hardware and software requirements and steps that you need to take before installation.

Chapter 3, “Installation,” provides procedures for installing UI Desktop and UI Web components.

Chapter 4, “Setup,” provides procedures for defining the parameters for UI Desktop and UI Web for an entire application environment. The parameters allow you to set up options that take effect for all users in a specified environment or security class.

Chapter 5, “Security,” explains setting up security in your client environment and testing your secure connection.

Chapter 6, “Query Builder Security,” explains the security options available for Query Builder.
Chapter 7, “Defining the Startup Sequence,” tells you how to set up the startup sequences in each database to present appropriate prompts to the user, whether the user accesses Colleague or Benefactor through UI Desktop or UI Web.

Chapter 8, “Client Deployment,” provides procedures for installing UI Desktop components to each user’s PC.

Chapter 9, “Client Setup,” provides information for using UI Desktop and UI Web to set up components on each user’s PC.

Chapter 10, “Uninstalling UI,” provides procedures for removing UI Desktop and UI Web.

Appendix A, “Integrating Your Existing Practices,” provides recommendations for integrating your existing practices and your custom software into UI Desktop and UI Web.

Appendix B, “Example Procedures for the Operating System Startup Sequence,” provides examples for defining how UI Desktop and UI Web respond to operating system startup prompts.

Where to Find More Information

For last-minute updates and additional information about these installation procedures, see AnswerNet page 670.

Datatel’s Guide to User Interfaces contains a description of UI, as well as step-by-step instructions for accomplishing basic tasks, such as accessing a form, finding a record, and using online help.

UI Desktop or UI Web?

Depending on the specific needs of users, UI can be deployed in either a Desktop or Web version. While both versions deliver rich functionality and navigation controls, each offers different options for setting up navigation. This allows you to address the needs of heavy data entry users versus more casual navigation users.
UI Desktop

The Desktop version of UI enables power users to easily navigate Colleague/Benefactor with minimal mouse movement during heavy data entry workflows, while also offering:

- More intuitive usability with Microsoft Windows “XP” navigation icons.
- Fast data entry with user-defined tab sequencing.
- Easy setup of user-defined field access.
- Personalized color indicators for required data entry fields.

UI Web

The Web version of UI allows users to access Colleague/Benefactor within a Web browser, taking advantage of standard browser navigation features. In addition to the functionality provided in the desktop version, UI Web also delivers:

- Anywhere, anytime access.
- Full support of standard Web browsers, such as Microsoft Internet Explorer and Firefox.
- Access to Colleague and Benefactor via Macintosh and Linux operating systems.
Installation Overview

The installation of UI Web and UI Desktop is similar in many ways. This section describes why there is a choice of two client interfaces. Each version has its own advantage. You can deploy one or both of these, depending on your needs.

The main differences are:

- When installing UI Web, you must install the UI Web server and Web component.
- When implementing security for UI Web, you can additionally install the wIntegrate server certificate.
- Because UI Web is accessed from a Web browser, you do not need to deploy UI Web to each user’s PC.

Whether you choose to use UI Desktop, UI Web, or both, should be determined by the amount of effort that is required to administrate them. UI Web requires a separate Windows Server. UI Web is usually more appropriate when you want to minimize administration, usually in a distributed (multi-campus) environment. For a large number of users, server-based administration is more efficient.

UI Web requires no installation to users’ workstations, but an HTML page containing the Java applet must be set up on a Web server.

UI Desktop Installation

There are some instances where UI Desktop may be a more appropriate solution than UI Web.

Advantages of UI Desktop:

- Slightly faster than UI Web, because it communicates directly with the host.
- Inter-application compatibility (for example, opening PDF files from SEVIS forms, and running documents that were merged in MS Word).
- UI Desktop is required for functions that call Powerview 3.0 components (such as ExpressLoad).

As a typical Windows application, UI Desktop is built from ActiveX components. The window-and-keyboard interface uses an ActiveX component that does most of the work.
Installation Overview

Installation of UI Desktop consists of the following main steps.

<table>
<thead>
<tr>
<th>Step</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify the databases (Colleague or Benefactor) that you want to make accessible through UI Desktop.</td>
<td></td>
</tr>
<tr>
<td>Load software updates, if required.</td>
<td>Only certain types of databases require a software update. For more information, see “Before You Begin” on page 3-1.</td>
</tr>
<tr>
<td>Install the administrative installation using the InstallShield available from the Datatel Web site.</td>
<td>Later, you will use this administrative installation to install the client software to each user’s PC.</td>
</tr>
<tr>
<td>Set up UI Desktop as follows:</td>
<td></td>
</tr>
<tr>
<td>• Enable the UI Desktop menu options for administering databases.</td>
<td></td>
</tr>
<tr>
<td>• Add databases available through UI Desktop.</td>
<td></td>
</tr>
<tr>
<td>• Limit user access to certain UI Desktop features.</td>
<td></td>
</tr>
<tr>
<td>• Set UI Desktop parameters.</td>
<td></td>
</tr>
<tr>
<td>• If desired, set up security to enable secure communications between the UI client and Colleague/Benefactor databases.</td>
<td></td>
</tr>
<tr>
<td>• Define the startup sequences in each database.</td>
<td></td>
</tr>
<tr>
<td>Install the client software on each user’s PC.</td>
<td></td>
</tr>
</tbody>
</table>

**Table 1-1**: Steps in the UI Desktop Installation Process

**Components Installed With UI Desktop**

When you install UI Desktop, the following components are installed.

- UI Desktop folders and files are installed to the hard drive of the installation workstation.
- Datatel icons are installed on the Start menu and the desktop of the installation workstation, permitting you to maintain the UI Desktop software as well as run UI Desktop from the installation workstation.

**Administrative Installation vs. Standard Installation**

The UI Desktop InstallShield offers two installation choices: Administrative and Standard. The Administrative option prompts you for your customer information, which is used to retrieve a new license key from the Datatel licensing server. The Standard option only prompts for the location of the license.wil file that was generated by a previous Administrative installation.
Datatel recommends installing the *license.wil* file to a network drive. When installing UI Desktop, first create the Administrative installation and then install UI Desktop on user’s PCs using the Standard installation.

## UI Web Installation

Implementing UI Web gives you the advantage of running UI inside a Web browser as a Java applet. Files are stored on the UI Web server. Users can connect from any supported Web-based device and use the same settings.

The UI Web Java client can be deployed for in-house users, or on the Web. If you choose to deploy the Java client on the Web, Datatel recommends that you run it through the firewall using a port forwarding utility (redirector) on the Web server as a bridge between the client and the UI Web server.

Advantages of UI Web:
- UI Web does not need to be installed on each client workstation.
- Reduced administration.
- User settings are centrally stored on the server.

## UI Web Overview

UI Web consists of a client component, a Web server component, and the wIntegrate server component.

The UI Web client component is a Java applet, which runs in select Web browsers on a variety of client workstation platforms. The applet is responsible for creating the GUI interface between the Web browser and Colleague/Benefactor. The applet relies on the wIntegrate server component for information regarding how to create the GUI, and to determine what data must be retrieved or displayed in the GUI.

The Web server is needed to distribute the Java applet client component. Java applets are embedded in HTML documents through the use of special HTML tags. In the sample *index.html* file that is delivered with UI Web, the cross-platform APPLET tag is used to attach the applet to the *index.html* page. There are many different HTML tags that can be used to embed an applet within an HTML page, and each generally has its own unique advantage. You
should determine which tag best suits your institution. When a browser opens an HTML page that contains an embedded applet, the applet is downloaded to the user's browser with the HTML page and the applet is executed.

**Note:** The browser must be running a JRE of 1.5.x to run the applet (Java 6 on Windows Vista).

Once the Web server has delivered the HTML document, applet, and any other items embedded in the HTML page, the Web server's role in UI Web is complete.

**Note:** The applet uses sockets for communicating, so there is no security advantage to putting the HTML page and applet on an secure server, as you are only securing the transmission of the Web page and applet to the user's Web browser. There is no disadvantage either, but if your intention is to secure communications between the applet and wIntegrate Server, you need to configure security on the wIntegrate server. See “Implementing Security” beginning on page 5-6 for more information.

The UI Web wIntegrate server component is responsible for interpreting the Datatel scripts, which define how the Java applet client creates the GUI and how the GUI behaves. The wIntegrate server is derived from the same wIntegrate engine, which User Interface Desktop is built on. As such, UI Web and UI Desktop share many of the same scripts. The wIntegrate server relays the GUI specs interpreted from Datatel scripts to the Java applet running in the user's browser. The wIntegrate server also manages communications between the applet and the application server where Colleague/Benefactor is running.

The wIntegrate server is the central component in UI Web, since it must be able to communicate with both the application server and the applet client. The applet makes a TCP/IP socket connection with the wIntegrate server, and the wIntegrate server in turn opens a (secure) telnet connection with the application server.

UI Web server refers to the physical server where the wIntegrate server software component, the Datatel scripts, and Datatel graphics are installed. The UI Web Server must be a Windows platform server and must have a fully qualified domain name by which the applet client can use to open a line of
communication with the wIntegrate server software running on the UI Web Server. The UI Web Server in turn must be able to communicate with the application server.

**Technical Tip:** Some of the keyboard shortcuts available in UI Desktop are not available in UI Web. Specifically, any keyboard shortcut that uses the “Alt” key is not available in UI Web. “Alt” is used to access the menu of the front-most application. Because UI Web runs as an applet inside a Web browser, the Web browser is the front-most application; therefore, the “Alt” key will access the menu for the Web browser.

**UI Web Configuration**

Datatel recommends that the UI Web server and the Web server exist on different servers (external configuration). In this type of configuration, the Web server and UI Web server can be installed on opposite sides of your firewall. This makes UI Web available to users who are outside the firewall. An example of the external configuration of UI Web is shown in Figure 1-1 on page 1-9.

**UI Web Using Port Forwarding/Redirection Software**

If the applet does not have direct access to the UI Web Server (for example, if you are allowing access to UI Web from outside of the firewall), the applet must still be able to open a line of communication back to the wIntegrate server software running on the UI Web server inside the firewall.

To allow the applet access through the firewall, Datatel recommends using a port forwarding utility for a proxy server between the applet and the UI Web Server. The primary goal of the port forwarding software is to capture TCP/IP packets from the source application and forward the packets through the firewall, unchanged, to the intended target application. There are freeware port forwarding utilities available on the internet for your choosing. As recommended from IBM/wIntegrate engineering, Datatel has used an open source Java application called TCPReflector for testing.
The port forwarding utility must listen on port 55638 on your Web server, or another server in your DMZ, and in return, it must open a socket to the UI Web Server using the same port.

**Note:** If you are using a port forwarding utility when embedding the applet in your own HTML page, you must use the name of the server in the server applet parameter tag where the utility is running, not the UI Web Server. This ensures that the applet will contact the proxy server. Then, be sure to have your port forwarding utility forward the packets to the UI Web Server.

![Diagram of UI Web External Configuration](image)

**Figure 1-1: UI Web External Configuration**

**UI Web Internal Configuration**

A second configuration option for UI Web is to install both the Web and UI Web servers on one server (internal configuration). This configuration eliminates the need for a port forwarding utility (proxy server), but does not allow access to users who are outside the firewall. An example of the internal configuration for UI Web is shown in Figure 1-2.
Figure 1-2: UI Web Internal Configuration
Administration Overview

After installing UI Desktop, UI Web, or both, you will configure some optional and required parameters before you and your users can start using UI.

Setup

The parameters allow you to set up options that take effect for all users in a specified account or security class. You must perform this initial setup before users can start using UI. The setup is identical for UI Desktop and UI Web. After you set up these parameters, you can then implement them in either version of UI.

See “Setup” beginning on page 4-1 for more information about setting up the parameters.

Security

You may optionally choose to implement security for your institution. If you do not implement security, you and users at your institution can still use UI, however you may risk unauthorized access to confidential information stored in your databases. Separate procedures are provided for UI Desktop and UI Web.

See “Security” beginning on page 5-1 for more information about setting up security for UI Desktop and UI Web.

Startup Sequence

Before users at your institution can access UI, you will need to define the startup sequence for each database. The startup sequence determines the order in which start-up prompts are presented to a user. It also determines whether the user accesses the database through User Interface (UI) or the Terminal (Character) interface.
See “Defining the Startup Sequence” beginning on page 7-1 for more information about defining the startup sequence.

**Client Deployment**

This chapter provides procedures for installing components to each UI Desktop user’s PC.

You do not need to install software for UI Web. UI Web is accessed from an Internet address, and does not need to be installed on client PCs. It is deployed via a Web page where the applet resides.

See “Client Deployment” beginning on page 8-1 for more information about the client deployment.

**Client Setup**

This chapter provides procedures for using UI to set up components on each user’s PC.

UI Desktop and UI Web allows administrators and users to administer databases and customize user fields in similar ways.

Because of the nature of the UI Web applet configuration, adding and removing users is handled differently. Because UI Web is not installed on users’ PCs, user access must be maintained from the Web User Add/Remove Databases dialog. This ensures the integrity of the applet from unauthorized Web users.

See “Client Setup” beginning on page 9-1 for more information about setting up UI on users’ PCs.
Before You Begin

Hardware and Software Requirements

This section lists the hardware and software requirements for the workstations involved in the installation of UI.

Please ensure that you have met all of the hardware and software requirements before attempting to install or configure UI. Installation and setup worksheets are provided at the end of this chapter to help you gather information that you need during the installation of UI.
UI Desktop Requirements

Note: At the time of publication, this certification list was accurate. To see the most up-to-date list of certifications for User Interface, see the Product Certifications page, [www.datatel.com/productcertifications](http://www.datatel.com/productcertifications), on the Datatel web site.

Table 2-1 lists the minimum hardware and software requirements necessary to install UI Desktop.

<table>
<thead>
<tr>
<th>Component</th>
<th>Comments</th>
<th>Required Hardware and Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application host computer</td>
<td>The computer on which Colleague or Benefactor resides.</td>
<td>Colleague 17.0 at Envision 4.7.1 or later.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Colleague 18.0 at Envision 4.8 or later.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Benefactor 5.1 at Envision 4.7.1 or later.</td>
</tr>
<tr>
<td>Installation workstation</td>
<td>The computer from which you install components to the network drive.</td>
<td>Operating system: Windows XP or Windows Vista.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection to the Internet.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection to the network drive where you want to install shared UI files.</td>
</tr>
<tr>
<td>Network drive</td>
<td>Must be accessible from the installation workstation and from users’ PCs.</td>
<td>Free disk space: About 1 MB.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Free disk space for installed files and cached scripts: About 35 MB.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection to the network drive where you installed shared UI files.</td>
</tr>
</tbody>
</table>

Table 2-1: Requirements for Installing UI Desktop
UI Web Requirements

Note: At the time of publication, this certification list was accurate. To see the most up-to-date list of certifications for User Interface, see the Product Certifications page, www.datatel.com/productcertifications, on the Datatel web site.

Table 2-2 lists the minimum hardware and software requirements necessary to install UI Web.

<table>
<thead>
<tr>
<th>Computer</th>
<th>Comments</th>
<th>Required Hardware and Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browsers</td>
<td>Depending on your operating system, these Web browsers are compatible with UI Web.</td>
<td>Windows: Internet Explorer 6+.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Linux or Windows: Mozilla 1.7+, Firefox 2.0+.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Macintosh: Safari 2.x.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sun Java Runtime Environment (JRE) 5 (Java 6 for Windows Vista only).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTE: The applet will not run on an MS Java virtual machine.</td>
</tr>
<tr>
<td>Application Host Computer</td>
<td>The computer on which Colleague or Benefactor resides</td>
<td>Colleague 17.0 at Envision 4.7.1 or later.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Colleague 18.0 at Envision 4.8 or later.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Benefactor 5.1 at Envision 4.7.1 or later.</td>
</tr>
<tr>
<td>UI Web Server</td>
<td>The physical server where the UI Web software is installed.</td>
<td>Operating system: Windows 2000 or Windows 2003 Server</td>
</tr>
<tr>
<td></td>
<td>This server will accommodate up to 200 concurrent users under normal usage.</td>
<td>CPU Power Minimum: Intel 2.0+ GHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number of CPUs: 2+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minimum RAM: 2GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Usable Storage: RAID 1 OS (36 GB)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network: 100 Base-T Minimum</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection to the Internet</td>
</tr>
<tr>
<td>User Workstation</td>
<td></td>
<td>Sun Java Runtime Environment (JRE) 5, except JRE 6 for Windows Vista only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supported Workstations:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Macintosh OSX Tiger (10.4).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Windows XP or Windows Vista.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Linux Red Hat 7.2.</td>
</tr>
<tr>
<td>Web Server</td>
<td>Is needed to distribute the Java applet client component.</td>
<td>Connection to the Internet</td>
</tr>
</tbody>
</table>

Table 2-2: Requirements for Installing UI Web
Worksheets

While you are installing the software, the InstallShield prompts you for the information about the databases you will be accessing. Table 2-3 on page 2-5 lists the information needed to install UI Desktop. Table 2-5 on page 2-7 lists the information needed to install UI Web. Before running either InstallShield, record the information in the “Entry” column in the appropriate worksheet.

If you are upgrading an existing UI Desktop installation, the InstallShield will copy the defined list of databases from the older UI Desktop installation to the new installation.

If you are not upgrading a UI Desktop installation, you must specify a database during installation. You can add only one database (Colleague or Benefactor) during the initial installation. If you want to make additional databases accessible through User Interface, you must add them later during the advanced administrative setup. Record the information about those databases in the “Entry” column in the worksheet in Table 2-4 on page 2-6.
### Table 2-3: UI Desktop Installation Worksheet

<table>
<thead>
<tr>
<th>Information</th>
<th>Example</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organization information, provided by Datatel</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization name</td>
<td>MyInstitution</td>
<td></td>
</tr>
<tr>
<td>Organization code</td>
<td>M99</td>
<td></td>
</tr>
<tr>
<td>Organization password</td>
<td>123456</td>
<td></td>
</tr>
<tr>
<td><strong>Information about the application host computer and network drive</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination folder</td>
<td>F:\DATATEL\UI</td>
<td>This is the path to the location on the network drive where you want to install UI Desktop.</td>
</tr>
<tr>
<td>License folder</td>
<td>F:\DATATEL/LICENSE</td>
<td>This is the path to the location on the network drive where you direct the InstallShield to copy the license file.</td>
</tr>
<tr>
<td>Host name</td>
<td>hpd370</td>
<td>You can use either the name or the IP address of the host computer.</td>
</tr>
<tr>
<td>Host operating system</td>
<td>UNIX</td>
<td>Choices are UNIX or Windows.</td>
</tr>
<tr>
<td>Database name</td>
<td>collive</td>
<td>Enter the name that you want your users to see when they are selecting the Colleague or Benefactor database that they want to access.</td>
</tr>
</tbody>
</table>
| Database path                                    | UNIX: /datatel/live/collive  
Windows: D:/datatel/live/collive | The database name cannot contain spaces or any of the following characters: . , ; : / < > " ? " |
### Table 2-4: UI Desktop Add Databases Worksheet

<table>
<thead>
<tr>
<th>Information</th>
<th>Entry</th>
<th>Example</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>First additional database</td>
<td></td>
<td>hpd370</td>
<td>You can use either the name or the IP address of the host computer. If you plan to implement UI Security, the Host Name must be the server’s fully qualified domain name (such as server.domain.edu). You cannot use the server’s IP address.</td>
</tr>
<tr>
<td>Host name</td>
<td></td>
<td></td>
<td>Enter the name that you want your users to see when they are selecting the Colleague or Benefactor database that they want to access through User Interface. The database name cannot contain spaces or any of the following characters: .,:;/&lt; &gt;&quot;?</td>
</tr>
</tbody>
</table>
### Table 2-5: UI Web Installation Worksheet

<table>
<thead>
<tr>
<th>Information</th>
<th>Entry</th>
<th>Example</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organization information, provided by Datatel</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization name</td>
<td></td>
<td>MyInstitution</td>
<td></td>
</tr>
<tr>
<td>Organization code</td>
<td></td>
<td>M99</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td>123456</td>
<td></td>
</tr>
<tr>
<td><strong>Information about the application host computer and network drive</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination folder</td>
<td></td>
<td>D:\Program Files\Datatel\UI Web\</td>
<td>This is the path to the location on the server where you want to install UI Web.</td>
</tr>
<tr>
<td>User ID</td>
<td></td>
<td>jsmith</td>
<td>This ID is used to identify the person who installed the software for this database. It does not need to be a login ID for the host computer.</td>
</tr>
<tr>
<td>Server name</td>
<td></td>
<td>hpd370</td>
<td>You can use either the name or the IP address of the server where Colleague/Benefactor is installed.</td>
</tr>
<tr>
<td>If you plan to implement security, the Host Name must be the server’s fully qualified domain name (such as server.domain.edu). You cannot use the server’s IP address.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server operating system</td>
<td></td>
<td>UNIX</td>
<td>Choices are UNIX or Windows</td>
</tr>
<tr>
<td>Information</td>
<td>Entry</td>
<td>Example</td>
<td>Comments</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>----------------</td>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Database name</td>
<td>collive</td>
<td></td>
<td>Enter the name that you want your users to see when they are selecting the Colleague or Benefactor database that they want to access through User Interface.</td>
</tr>
<tr>
<td>Database path</td>
<td></td>
<td>UNIX: /datatel/live/collive</td>
<td>The database name cannot contain spaces or any of the following characters: . , ; / &lt; &gt; * ?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows: D:\datatel\live\collive</td>
<td></td>
</tr>
<tr>
<td>UI Web Server fully qualified domain name</td>
<td></td>
<td>myserver.myschool.edu.</td>
<td>Enter the fully qualified domain name of the server where you are installing UI Web.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NOTE: If you are using port forwarding software (as detailed in the external configuration setup), use the name of the server where the utility is running (likely the Web server).</td>
</tr>
</tbody>
</table>

Table 2-5: UI Web Installation Worksheet (cont’d)
In This Chapter

This chapter provides procedures for installing UI Desktop and UI Web components.

Before You Begin

Before you perform these installation procedures, ensure that you do the following:

- Review “Before You Begin” beginning on page 2-1 and complete the relevant worksheets in that chapter.
- Load any UI software updates.

The UI Desktop and UI Web InstallShields connect to IP address 205.231.22.30 in order to verify your client information. You will need to make sure your firewall is not blocking access to this address during installation.
Installing the Administrative Client

If you are upgrading from an earlier version of UI Desktop, refer to the appropriate upgrade topic below for the version of UI Desktop from which you are upgrading. If you are not upgrading, skip to “Procedure for Installing the UI Desktop Administrative Client” beginning on page 3-3.

Upgrading from UI Desktop 2.1

You must first uninstall UI Desktop 2.1 from the installation PC. Use the standard Windows “Add or Remove Programs” function to uninstall UI Desktop 2.1. The settings for UI Desktop will not be deleted because they were created after UI Desktop was installed. Therefore, the uninstaller has no knowledge of those files. UI Desktop 2.2 will use those same settings, saving you some setup work.

Upgrading from UI Desktop 1.5 or Earlier

Do not uninstall UI Desktop before installing UI Desktop 2.2. The InstallShield will copy your settings from the older UI Desktop installation forward to the new installation. You can uninstall the older version of UI Desktop after installing UI Desktop 2.2, if desired.

Because there is no longer a concept of a shared installation with UI Desktop 2.2, you do not need a separate server for UI Desktop. Be sure to revisit your settings on the UI Administration Parameters (UIPR) form for the location of the license files if the location changes. See “Setting Up the Administrative Parameters” beginning on page 4-6 for more information.
Procedure for Installing the UI Desktop Administrative Client

**Technical Tip:** If your institution uses Communication Management, refer to AnswerNet document 28201.15 for information about creating the C:\DATATEL directory to resolve an error message.

Perform this procedure from the installation workstation. See “Hardware and Software Requirements” on page 2-1 for hardware and software requirements for the installation workstation.

**Step 1.** From your Web browser, access the UI Desktop Web page on the Datatel Web site. Current software downloads can be found at www.datatel.com/support/softwaredownloads.cfm.

**Step 2.** Download the executable file to your PC.

**Step 3.** Double-click the UIDesktop220Setup.exe file to start the InstallShield. The Welcome window displays, as shown in Figure 3-1.

---

**Figure 3-1:** Welcome Window
Step 4. On the Welcome window, click **Next** to continue. The Installation Type window is displayed, as shown in Figure 3-2.

![Figure 3-2: Select Installation Type Window](image)

Step 5. Select **Administrative**. Click **Next** to continue. The License Agreement window is displayed, as shown in Figure 3-3.

![Figure 3-3: License Agreement Window](image)
Step 6. Select I accept the terms of the license agreement. Click Next to continue. The Customer Information window is displayed, as shown in Figure 3-4.

![Image of Customer Information Window]

Figure 3-4: Customer Information Window

Step 7. Enter your organization information. Enter only alphanumeric characters (no commas, periods, etc.). Click Next to continue. The Destination Folder window is displayed, as shown in Figure 3-5.
Step 8. If you want to change the installation location, click **Change...** and navigate to the directory where you want UI Desktop installed. Datatel recommends that you install UI Desktop in the default location. Click **Next** to continue. The License Folder window is displayed, as shown in Figure 3-6.
Step 9. Click **Change...** and navigate to the network path where you want to install the *license.wil* file and the *ui_ins.ini* file. The license file is used when you perform installations on client PCs. If you do not install the license file on a network drive, you will need to perform an administrative installation on every client PC. This directory is where you “point” on the UIPR form during setup. See “Setting Up the Administrative Parameters” on page 4-6 for more information.

Step 10. Click **Next** to continue. The Database Information window is displayed, as shown in Figure 3-7.

![Database Information Window](image-url)

**Figure 3-7: Database Information Window**

Step 11. Are you upgrading an existing UI Desktop installation?

Yes. Leave all fields on this window blank. The InstallShield will copy the databases defined in the existing *datatel.ini* file in the existing UI Desktop 1.5 installation. The settings for a UI Desktop 2.1 installation remain in their location and are used for UI Desktop 2.2
No. Enter the information about the host computer and database. See Table 2-3 for information about these fields. In particular, note the following:

- If you plan to implement UI Security, the Host Name must be the server’s fully qualified domain name (such as server.domain.edu). You cannot use the server’s IP address.
- You can identify only one database during the initial install. Later, you can add additional databases during advanced administrative setup.

Step 12. Click Next to continue. The Ready to Install window is displayed, as shown in Figure 3-8.

![Figure 3-8: Ready to Install Window](image)

Step 13. Click Install to install UI Desktop.

After a few minutes, the Successful Installation window is displayed, as shown in Figure 3-9.
Step 14. Click Finish to exit the InstallShield.

Step 15. Continue with “Setup” beginning on page 4-1.

Technical Tip: Save a copy of the InstallShield to a network drive that can be accessed from a user’s PC. You can then instruct users to run the InstallShield themselves to upgrade their UI Desktop installation. No client code or password is needed when using the Standard UI Desktop installation option.
Installing UI Web

Note: Install only one instance of UI Web per server. For a discussion, see “UI Web Installation” on page 1-6.

Procedure for Installing UI Web

Perform this procedure from the server where the UI Web is to be installed. See “Hardware and Software Requirements” on page 2-1 for hardware and software requirements for the installation workstation.

To allow the applet access through the firewall, Datatel recommends using a port forwarding utility for a proxy server between the applet and the UI Web Server. See “UI Web Using Port Forwarding/Redirection Software” on page 1-8 for more information about port forwarding.

Step 1. Do you have UI Web installed on the server where you will install UI Web 2.3?

Yes. You must uninstall UI Web before installing UI Web 2.3. Continue with Step 2 below.

No. Skip to Step 7.

Step 2. Create a backup copy the ui_ins.ini and web_dbs.ini files from your UI Web installation directory (the default is \Program Files\Datatel\UI Web). You will restore the backup copies in a later step.

ALERT! It is very important that you make backup copies of the ui_ins.ini and web_dbs.ini files. When the older version of UI Web is uninstalled, these files become corrupt.

Step 3. From the Start menu, select Programs, then Datatel, then UI Web, and finally Service Control Program. The wIntegrate Server Service Control Program starts, as shown in Figure 3-10.
Step 4. Click Stop to stop the wIntegrate server.

Step 5. Click Close to exit the wIntegrate Server Service Control Program.

Step 6. From the Start menu, select Programs, then Datatel, then UI Web, and finally Uninstall to uninstall the wIntegrate server.

Step 7. From your Web browser, access the UI Web page on the Datatel web site. Current software downloads can be found at www.datatel.com/support/softwaredownloads.cfm.

Step 8. Download the executable file to the server where UI Web is to be installed.

Step 9. Open the UIWeb230.exe file to run the UI Web InstallShield.
Installation

3-12

User Interface Installation and Administration, April 7, 2008
© 2008 Datatel, Inc.

Figure 3-11: UI Web InstallShield Welcome Window

Step 10. On the Welcome window, click Next to continue.

Figure 3-12: License Agreement Window

Step 11. On the License Agreement window, select I accept the terms of the licensing agreement, and then click Next.
Step 12. On the Organization Information window, enter your organization name, organization code, and password, and then click Next.
Step 13. On the Choose Destination Location window, browse to the location where you want to install the UI Web files and then click **Next**.

![UI Web 2.3.0](image)

**Figure 3-15: Enter Database Information Window**

Step 14. On the Enter Database Information window, enter the information about the host computer and database path that you recorded in the worksheet in Table 2-5 on page 2-7. Then click **Next**.

**Note:** The User Login ID should be the user’s login for the application server.
Step 15. On the Domain Name window, enter the fully qualified domain name of the UI Web server, and then click Next.

Note: If you are using port forwarding, the domain name must be that of the server running the port forwarding/redirector software.
Step 16. On the Start Copying Files window, review the installation details you have selected. Click **Next** to start the installation of the files.

Step 17. Click **Finish** on the InstallShield Wizard Complete window to finish the initial installation.

Step 18. If you are upgrading from an earlier version of UI Web, restore your backup `ui_ins.ini` and `web_dbs.ini` files to the location where you installed UI Web 2.3 (the default is `\Program Files\Datatel\UI Web`), overwriting the existing corrupt files.
**Step 19.** Copy the *wIntJava* directory from the directory in which you installed the UI Web files to the document directory on your Web server. The *wIntJava* directory contains the following files:

- **index.html.** A sample HTML page (wrapper). You can use this as an example of how to call the applet from your HTML page.
- **template.css.** A sample style sheet that controls UI Web font and color settings.
- **wint1.jpg.** A sample header graphic.
- **wIntJavaApplet.jar.** The wIntegrate Java applet client for the HTML page.
- **datatel.ico.** Datatel icon.

If you are upgrading an existing installation of UI Web, you only need to copy the *wIntJavaApplet.jar* file to the Web server, replacing the old version.

**Technical Tip:** If you do not copy the *wIntJavaApplet.jar* file to the Web server, you will see an error message when attempting to use the old applet with the new wIntegrate server.

**Step 20.** Continue with “Setup” beginning on page 4-1.

---

**Test Your Connection to UI Web**

After you install UI Web, you can use the following procedure to test your connection.

**Step 1.** Access the *index.html* page on your Web server to display the Datatel UI Web login dialog.
Step 2. Enter the user ID that you entered on the Enter Database Information window during the installation of UI Web.

Step 3. Log in to the UI Web application.

UI Web Utilities

After running the UI Web InstallShield, you can optionally run one or both of the utilities that are installed with UI Web. They are:

- **UI Web User Administration.** Allows you to assign additional databases to UI Web users.

- **UI Web License Update.** Allows you to update the number of UI users for UI Web at your institution.
Procedure for UI Web User Administration

Before you can access UI Web to install databases for yourself or users, you must first add any initial users from the database administrator.

**Step 1.** From your Start menu, navigate to **All Programs**, then **Datatel**, then **UI Web**, and finally **UI Web User Access** to launch the database administration tool.

**Figure 3-19:** UI Web User Database Administration

**Step 2.** From the User Login ID drop-down, select the ID of the user you want to assign databases for.

**Note:** If the ID of the user you want to add databases for is not in the list of IDs, you can add it by clicking the New button, typing the ID, and clicking Add User.

**Step 3.** From the Available Databases list, select the Database you want the selected user to access.

**Step 4.** Click the left arrow to move the selected database to the list of available databases.

**Step 5.** Click **Exit** when you are finished.
Procedure for Running the UI License Update

You can use the UI license update to increase or decrease the number of users who can access UI Desktop and UI Web at your institution.

**Step 1.** From your Start menu, navigate to **All Programs**, then **Datatel**, then **UI Web**, and finally **UI License Update** to launch the License Update utility.

![UI License Update - InstallShield Wizard](image)

**Figure 3-20: Welcome Window**

**Step 2.** On the Welcome window, Click **Next** to continue.
Step 3. On the UI Licence Update License Agreement, select I accept the terms of the license agreement, and then click Next.
Step 4. On the Organization Information window, enter your organization name, organization code, and password, and then click **Next**.

![InstallShield Wizard Complete Information](image)

**Figure 3-23**: InstallShield Wizard Complete Information

Step 5. On the InstallShield Wizard Complete window, click **Finish** to complete the license update.
Setup

In This Chapter

This chapter provides procedures for defining the parameters for User Interface (UI). The parameters allow you to set up options that take effect for all users in a specified account or security class. Table 4-1 lists the topics in this chapter.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of Parameters</td>
<td>4-2</td>
</tr>
<tr>
<td>Setting Up Miscellaneous Parameters</td>
<td>4-4</td>
</tr>
<tr>
<td>Setting Up the Administrative Parameters</td>
<td>4-6</td>
</tr>
<tr>
<td>Setting Up the Multi-line Text Editor</td>
<td>4-15</td>
</tr>
<tr>
<td>Setting Up the UI Exit Button</td>
<td>4-18</td>
</tr>
<tr>
<td>Setting Up FTP Transfers</td>
<td>4-20</td>
</tr>
<tr>
<td>Setting Up Security</td>
<td>4-24</td>
</tr>
<tr>
<td>Setting Up Field Customization</td>
<td>4-27</td>
</tr>
<tr>
<td>Setting Up the Terminal-Style Bar Graph</td>
<td>4-33</td>
</tr>
<tr>
<td>Setting Up the Browser-Based Help System</td>
<td>4-35</td>
</tr>
<tr>
<td>Setting Up the Record Delete Icon</td>
<td>4-39</td>
</tr>
<tr>
<td>Limiting User Access to Features</td>
<td>4-41</td>
</tr>
</tbody>
</table>

Table 4-1: Topics in This Chapter

For UI Web, you must have an administrative installation of UI Desktop in order to set up the UI parameters.
Overview of Parameters

Most UI parameters are defined from the UI Administration Parameters (UIPR) form, the UI Usage Parameters (UIPM) form, and the Security Class Definition (SCD) form. The parameters defined on the UIPR and UIPM forms are applicable to all users in an application environment. The parameters defined on the SCD form are applicable to all users assigned to a security class and override the same settings on the UIPR and UIPM forms. Figure 4-1 shows the location in this manual of the procedures for defining the parameters on the UIPR form. Figure 4-2 shows the location of the procedures for the UIPM form. Figure 4-3 shows the location of the procedures for the SCD form.

**Note:** The examples in this chapter display forms captured in the UI Desktop interface. UI Web allows you to perform the same functions, but the forms may look slightly different.
Overview of Parameters

Figure 4-2: UI Usage Parameters (UIPM) Form

- See “Procedure for Defining Miscellaneous Parameters” on page 4-4
- See “Procedure for Enabling the UI Exit Button” on page 4-19
- See “Setting Up Field Customization” on page 4-27
- See “Setting Up the Terminal-Style Bar Graph” on page 4-33
- See “Setting Up the Browser-Based Help System” on page 4-35

Figure 4-3: Security Class Definition (SCD) Form

- See “Setting Up the Administrative Parameters” on page 4-6
- See “Setting Up Field Customization” on page 4-27
- See “Limiting User Access to Features” on page 4-41

See “Setting Up the Multi-line Text Editor” on page 4-15
Setting Up Miscellaneous Parameters

The miscellaneous parameters defined on the UI Usage Parameters (UIPM) form are shown in Figure 4-4. The miscellaneous parameters consist of the Imaging Enabled, Issue Final Prompts, and Disable Function Keys parameters.

![Figure 4-4: Miscellaneous Parameters on the UIPM Form](image)

**Procedure for Defining Miscellaneous Parameters**

Use this procedure to set up the miscellaneous UI parameters.

**Step 1.** In the UT application, access the UIPM form.

**Step 2.** In the Imaging Enabled field, enter **Yes** if you want to enable the interface to third party imaging software.
Step 3. In the Issue Final Prompts field, enter Yes if you want users to see the final confirmation prompt when they are about to save changes on a form.

Datatel recommends leaving this set to Yes. If set to No, users won’t have an opportunity to return to the form to undo changes if they see warning messages after saving.

Step 4. In the Disable Function Keys field, enter Yes if you want to disable the function keys (F1, F2, and so on) in UI.

Step 5. Save your changes on the UIPM form.
Setting Up the Administrative Parameters

The options described here provide a convenient method for both system administrators and users to maintain their UI configuration from within a UI session.

The UI Administration Parameters (UIPR) and Security Class Definition (SCD) forms, shown in Figure 4-5, are used to define which users have access to these menu options.
Figure 4-5: Administrative Menu Options: UIPR and SCD Forms

The Options menu in UI can include two administrative options, shown in Figure 4-6.

- **Add/Remove Databases.** Permits users to maintain the list of databases they see in the drop-down list when they access UI. For more information,
see “Adding Databases” on page 9-6. The system administrator defines which databases are available to the user, as discussed below.

- **Administer Databases.** Permits the system administrator to maintain the list of databases available through UI. For details, see “Procedure for Administering Databases” beginning on page 4-13.

In a typical installation, where users have access to the network drive where the license file is installed, you might want all users to have the Add/Remove Databases option, but only system administrators to have the Administer Databases option. Also, you might want to grant the Add/Remove Databases menu option to users for only a brief window of time, after you first set them up with UI, to allow them to add the necessary databases.

![Figure 4-6: Options Menu in UI](image)

The fields highlighted on Figure 4-5 work as follows:

- All of the fields highlighted on Figure 4-5 are delivered empty, so that no one has access to either of the administrative menu options.
- The entries on the UIPR form globally grant or deny access to all users.
- The entries on the SCD form override, for that security class, the corresponding entries on the UIPR form. For example, the Allow UI Admin Features field on the SCD form overrides the Enable UI Admin Features field on the UIPR form. Only if the field on the SCD form is left blank will the corresponding field on the UIPR form apply to users in that security class.
For example, assume that you wanted all users to have access to the Add/Remove Databases menu option, but only wanted system administrators (in the ADMIN security class) to have access to the Administer Databases menu option. The setup shown in Table 4-2 would be one way to achieve that result.

<table>
<thead>
<tr>
<th>Users</th>
<th>Form</th>
<th>Field</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>UIPR</td>
<td>Enable Add Database</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enable UI Admin Features</td>
<td>No</td>
</tr>
<tr>
<td>System administrators (ADMIN security class)</td>
<td>SCD</td>
<td>Allow Add Database</td>
<td>(empty)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Allow UI Admin Features</td>
<td>Yes</td>
</tr>
<tr>
<td>Users</td>
<td>SCD</td>
<td>Allow Add Database</td>
<td>(empty)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Allow UI Admin Features</td>
<td>(empty)</td>
</tr>
</tbody>
</table>

Table 4-2: Example of Administrative Menu Options With Users Permitted to Add Databases

In this example, system administrators have access to the Administer Databases menu option because the “Yes” entry in the Allow Administer Databases field on the SCD form overrides the “No” entry in the Enable UI Admin Features field on the UIPR form. For users, on the other hand, the defaults defined on the UIPR form are appropriate, so both fields can be left empty on the SCD form.

**Note:** If a user is a member of two or more security classes, and access to one of these menu options is denied for any of those security classes, then the user will not have access to that menu option.

For example, if the user is a member of two security classes, and the entry in the Allow Add Databases field on the SCD form is “No” for one security class and “Yes” for the other security class, then the user will not have access to the Add/Remove Databases option.

If your users don’t have access to the network drive where the license file is installed, then they cannot add databases because they cannot access the list of available databases defined by the system administrator. Table 4-3 shows an appropriate setup for that configuration.

<table>
<thead>
<tr>
<th>Users</th>
<th>Form</th>
<th>Field</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>UIPR</td>
<td>Enable Add Database</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enable UI Admin Features</td>
<td>No</td>
</tr>
</tbody>
</table>

Table 4-3: Example of Administrative Menu Options With Users Not Permitted to Add Databases
Procedure for Enabling the Administrative Menu Options

This is a two-part procedure:

■ The first part is to globally grant or deny access to the menu options (UIPR form).
■ The second part is to override the UIPR form defaults for a particular security class (SCD form).

Before performing this procedure, read “Setting Up the Administrative Parameters” beginning on page 4-6 and define your strategy for setting these parameters.

Procedure for Administering Global Access (UIPR Form)

Perform the following procedure to globally grant or deny the administrative options to all users. You can later override these entries for users in a particular security class.

**Step 1.** In the UT application, access the UIPR form.

**Step 2.** In the Enable Add Database field, enter **Yes** to globally grant access to the Add/Remove Databases menu option, or **No** to globally deny access.

You can later override your entry for users in a particular security class.
**Step 3.** In the Enable UI Admin Features field, enter **Yes** to globally grant access to the Administer Databases menu option, or **No** to globally deny access.

You can later override your entry for users in a particular security class.

**Step 4.** In the Drive Name for Master Client and Full Path for Master Client fields, enter the path to your UI license folder.

The path is the one you chose during installation (Step 9 on page 3-7).

If your users have the drive mapped from their PCs, your entries should look similar to the example. In the following example, the path is \N:\datatel\ui.

<table>
<thead>
<tr>
<th>Field</th>
<th>Example entry</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive Name for Master Client</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Full Path for Master Client</td>
<td>datatel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ui</td>
<td></td>
</tr>
</tbody>
</table>

**Table 4-4:** Example Entries for a Mapped Network Drive

If your users do not have the drive mapped from their PCs, your entries should look like the following example. In this example, the path, using the Universal Naming Convention (UNC), is \server\share\datatel\ui.

<table>
<thead>
<tr>
<th>Field</th>
<th>Example entry</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive Name for Master Client</td>
<td>server</td>
<td>Name of the computer</td>
</tr>
<tr>
<td></td>
<td>share</td>
<td>Name of the shared folder corresponding to the drive</td>
</tr>
<tr>
<td></td>
<td>datatel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ui</td>
<td></td>
</tr>
</tbody>
</table>

**Table 4-5:** Example Entries for No Mapped Network Drive

Do not include delimiters (‘:\’ and ‘/’) in your entries.

**Step 5.** Save your changes on the UIPR form.
Procedure for Administrating Options for Users in a Security Class (SCD Form)

Perform the following procedure to override, for a particular security class, the Enable Add Database and Enable UI Admin Features entries on the UIPR form.

**Note:** You must enter a value in the Drive Name for Master Client field on the UIPR form in order for this procedure to succeed.

**Note:** If both entries on the UIPR form apply for the users in a security class, then you don’t need to perform this procedure for that security class. Instead, leave both fields blank on the SCD form for that security class.

**Step 1.** In the UT application, access the Security Class Definition (SCD) form.

**Step 2.** At the Security Class ID LookUp prompt, enter the security class.

**Step 3.** In the Allow Add Database field, do one of the following to define access to the Add/Remove Databases menu option:
- Leave blank to allow the default, defined on the UIPR form, to apply to users assigned to this security class.
- Enter Yes to grant access to this menu option to all users assigned to this security class.
- Enter No to deny access to this menu option to all users assigned to this security class.

**Step 4.** In the Allow UI Admin Features field, do one of the following to define access to the Administer Databases menu option:
- Leave blank to allow the default, defined on the UIPR form, to apply to users assigned to this security class.
- Enter Yes to grant access to this menu option to all users assigned to this security class.
- Enter No to deny access to this menu option to all users assigned to this security class.

**Step 5.** Save your changes on the SCD form.
Step 6. Repeat Steps 2 through 5 for all security classes for which you want to override the defaults defined on the UIPR form.

Note: When you have completed this procedure, exit and then reenter your UI session. This will ensure that you have the Administer Databases menu option for the next procedure.

Procedure for Administering Databases

Step 1. From the Options menu in UI, select Administer Databases. The Administer Databases dialog box is displayed, as shown in Figure 4-7.

![Administer Databases Dialog Box](image)

Figure 4-7: Administer Databases Dialog Box

Step 2. Do you want to add a database that your users can access through UI?

No. Skip to Step 8.

Yes. Click Add. The Add Database dialog box is displayed, as shown in Figure 4-8.

1. If the “Administer Databases” option does not appear on your Options menu, it may have not been enabled for your login. See “UI Administration Parameters (UIPR) Form” beginning on page 4-2.
Step 3. Select UNIX or Windows for the type of operating system on the host computer.

Step 4. In the Host Name, Database Name, and Database Path fields, enter the information about the database that you recorded in the worksheet in Table 2-4 on page 2-6.

Note: You can use either the name or the IP address of the host computer.

Note: If you plan to implement UI Security, the Host Name must be the server’s fully qualified domain name (such as server.domain.edu). You cannot use the server’s IP address.

Step 5. In the Installer field, enter your user ID.

Step 6. Click OK.

Step 7. Repeat Steps 2 through 6 for each database that you want to add.

Step 8. If you want to edit an existing database definition, click Edit. If you want to delete an existing database definition, click Delete.

Step 9. In the Administer Databases dialog box, click OK to finish the installation.
Setting Up the Multi-line Text Editor

Many Envision forms allow your users to access a standard form to maintain text. In UI, you can set this form to use either a single-line editor or a multi-line editor, as shown in Figure 4-9 on page 4-15. The multi-line editor provides significant advantages in ease of editing, including word wrap, select all, cut, copy, and paste. For more information about the features of the multi-line text editor, see Guide to User Interfaces.

If you enable the multi-line editor, it will be available when your users detail on most fields that have UTEDIT capability, such as a Comments field or Description field. Some older forms and fields with UTEDIT capability are not coded to use the multi-line editor.

A consideration to using the multi-line editor is the time required for the text to appear. The multi-line editor loads the entire text message at once (the single-line editor only loads one form, or fifteen lines, at a time). This download time is a concern only in cases where the text message is large, and only if you have not enabled FTP transfers. As a result, if you choose to enable multi-line text editing and your users typically enter very lengthy comments, you will probably want to also enable FTP transfers as described in “Setting Up FTP Transfers” beginning on page 4-20.

Figure 4-9: Multi-Line Control Parameter on the UIPM Form
The example in Figure 4-4 was created by detailing from the Description field on the Courses (CRSE) form.

Figure 4-10: Single- and Multi-Line Editors
Procedure for Setting Up the Multi-line Text Editor

**Step 1.** In the UT application, access the UIPM form, shown in Figure 4-4 on page 4-4.

**Step 2.** In the Enable Multi-Line Controls field, enter Yes if you want to use the multi-line editor.

Enter No if you want to use the single-line editor. The default is No.

**Step 3.** Save your changes on the UIPM form.
Setting Up the UI Exit Button

Previous versions of UI included an Exit button by default, which could be used to close the UI session (as shown in Figure 4-11). This feature is available only for UI Desktop.

Other, more standard, methods of closing UI are available, such as the following:

- Click the close window box (“X”) in the upper right corner.
- Double-click the Datatel icon in the upper left corner.
- Select Exit from the File menu.

Consequently, the Exit button is no longer displayed in UI as a default. However, if you want to restore the Exit button for your users, you can enable it using the following procedure.

Figure 4-11: Exit Button
Procedure for Enabling the UI Exit Button

**Step 1.** In the UT application, access the UIPM form.

**Step 2.** In the Enable UI Exit Button field, enter **Yes** to enable the exit button for this application environment.

Enter **No** if you do not want to enable the exit button for this application environment. “No” is the default value for this field.

**Step 3.** Save your changes on the UIPM form.
Setting Up FTP Transfers

Transfer of data from the host computer to the users’ PCs can occur by either telnet or FTP. FTP facilitates transfers such as the multi-line text editor and the Print Local and Import (Save As) features in the UI report browser.

Note: This feature is available only for UI Desktop.

Users must have FTP access and their FTP login and password must match their telnet login and password before you can enable FTP transfers.

Use the following fields to enable FTP transfers:

- **Use FTP for data transfers.** If this field is set to “Yes,” FTP is used for transfers that are of a type that can use FTP (such as the multi-line text editor and the report browser) and are above the size threshold specified in the FTP Cutoff field. If this field is set to “No,” telnet is used for all data transfers.

- **FTP Cutoff.** Threshold for FTP transfer, in number of characters. Below this threshold, transfer is by telnet; above this threshold, transfer is by FTP.

- **Leave Open.** If this field is set to “Yes,” then once the FTP connection is opened in a UI session, it is left open for the duration of the session. If this field is set to “No,” the connection is closed after each transfer and re-opened for the next transfer. Opening the connection can take several seconds, so leaving the connection open can improve performance. A consideration is that an extra connection into your system will be left open, possibly using up resources that are needed elsewhere.

- **FTP Root Path Adjustment.** This field enables a process running winteg FTP to adjust the absolute path of the Unidata files to match the “view” of FTP. In some cases, FTP can be set to any necessary level by the system administrator. This view may or may not be the same as the absolute path of a file in a given account. This field allows the system administrator to specify the prefix to remove from the absolute path in order to arrive at the proper directory level for FTP to recognize.

  For example, at Datatel we have a development account in directory path \D:\Datatel\Apps\sdnt4db\... However, FTP can only “see” as high as \Apps\sdnt4db\... Therefore, this field must contain “D:\Datatel” in order for the FTP processing to know to remove that string from the beginning of the absolute path of a data file before building the winteg FTP script. This ensures that FTP and the script are looking at the same directory level.

- **FTP Domain Name.** Use this field to authenticate valid domain users.
Considerations for Setting FTP Parameters

FTP transfer significantly shortens the time needed for large text messages to be downloaded when using the multi-line text editor. Therefore, if you have enabled the multi-line text editor, as discussed in “Setting Up the Multi-line Text Editor” beginning on page 4-15, then you will probably want to also enable FTP.

You can set up UI for secure transmission using telnet (see “Security” beginning on page 5-1). FTP transfers are not secure. The decision on whether to use FTP is a trade-off between the improved performance with FTP and the risk of unsecure transmission. You may decide that the types of information that would be transmitted with FTP (based on the specified minimum size) do not need to be secure.

Your entries in the FTP Cutoff field and the Leave Open field are interrelated:

■ If you choose to leave the FTP connection open (by entering Yes in the Leave Open field), then FTP will always be faster than telnet. For this situation, you should set the FTP Cutoff to a low value (100 characters or less) so that FTP is used for most transfers.

■ On the other hand, if you choose to close the FTP connection after each transfer (by entering No in the Leave Open field), then each FTP transfer will include the time to open the connection plus the transfer time. In this situation, telnet will be faster for small transfers. You would want to set the FTP Cutoff to a higher value. Datatel suggests initially setting the cutoff to 5000 characters and using trial-and-error to determine an appropriate value.
Procedure for Setting Up FTP Transfers

Step 1. In the UT application, access the UIPR form.

Step 2. In the Use FTP for data transfers field, enter Yes if you want to use FTP for some data transfers.

If you enter Yes, then FTP is used for transfers that are of a type that can use FTP (such as text for the multi-line text editor) and are above the size threshold specified in the FTP Cutoff field.

Enter No if you want to use telnet for all transfers. The default is No.

Step 3. In the FTP Cutoff field, enter the threshold for FTP transfer, in number of characters.

If less than this threshold, transfer is by telnet. If greater than this threshold, transfer is by FTP.
Step 4. In the Leave Open field, enter **Yes** to have the FTP connection stay open after it is first opened in a UI session.

Enter **No** to have the FTP connection close after each transfer and re-open for each new transfer.

Step 5. In the FTP Root Path Adjustment field, enter the file path prefix necessary for FTP processing. Depending on your setup, you may not need to enter a value in this field.

Step 6. In the FTP Domain Name field, enter the domain name used for FTP transfers.

Step 7. Save your changes on the UIPR form.
Setting Up Security

Use the UI Administration Parameters (UIPR) form to enable SSL secure connections. You must modify the UIPR parameters in each application environment in which you want to establish secure communications.

If you change any of these fields, users are prompted to refresh their UI scripts the next time they attempt to log in to this application environment. The script refresh is necessary to propagate the client SSL parameters to the UI client.

Note: The Connection Secure field in the header area indicates whether the current session is secure.

After enabling your secure connection, refer to “Security” beginning on page 5-1 for information about how to request certificates, install certificates, apply certificates to an account, and view the certificates in the key store path.

Figure 4-14 shows the security parameters for the UIPR form.

![UIPR - UI Administration Parameters](image)

**Figure 4-14: Security Parameters on the UIPR Form**
Procedure for Enabling a Secure Connection

Step 1. Access the UIPR form from the UT application.

Step 2. Change the Enable SSL field to Yes. This field allows you to indicate whether you want to enable secure telnet communication to the current application environment.

Step 3. In the Suppress SSL Failure Message field, indicate whether you want to suppress the SSL connect failure error message (Figure 4-15) for users. Set this to Yes only when you are testing the secure location. Ensure that you return this field to No upon implementation.

![Figure 4-15: SSL Connect Failure Error Message](image)

Step 4. In the Disable Unsecured Connections field, enter Yes to disable the option to use a non-secure connection to re-connect to the host.

**ALERT!** Datatel strongly recommends that you set this field to Yes only if you are sure that SSL is functioning properly and you are prepared to disable your non-secure telnet port.

Step 5. In the Allow User Connection Choice field, indicate whether users can choose if they connect to this application environment with a secure or non-secure telnet.

If you enter Yes, then the Use Secure Connection check box appears in the Datatel Login form (Figure 4-16) when users select this application environment in the Database field on that form.
Step 6. Save and finish from the UIPR form.

Step 7. Close and restart UI.

Step 8. Refresh the scripts.

Step 9. Restart UI.

The connection is now secure, as indicated by the padlock icon in the upper left corner of the UI application. The Connection Secure field in the header area on the UIPR form also displays “Yes.”

Figure 4-17 shows the UIPR form when the connection is secure.
Setting Up Field Customization

Both system administrators and users can optionally specify settings for tab sequencing, make fields required, and restrict field access. Administrators can specify these settings in either of the following ways:

- The User Field Customizations (UIFC) form (see “Customizing User Fields” on page 9-10).
- The Customize Field Properties option from the Tools menu of the form you want to customize (refer to Guide to User Interfaces).

As the system administrator, you define which settings users can customize. You can set up field customization preferences in the security class of each user from the Security Class Definition (SCD) form, or for all users from the UI Usage Parameters (UIPM) form.

Before the settings are activated, you must additionally enable the user overrides from the UIPM form.

Table 4-6 describes the functionality of each field customization parameter on the SCD and UIPM forms.

<table>
<thead>
<tr>
<th>Field</th>
<th>SCD</th>
<th>UIPM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow User Ovr Tab Seq</td>
<td>Allows users in this security class to set up UIFC tab sequencing fields (Next Field Ovr, Last, and First Field) for themselves. Overrides UIPM setting for a selected security class.</td>
<td>Allows all users to set up UIFC tab sequencing fields (Next Field Ovr, Last, and First Field) for themselves.</td>
</tr>
<tr>
<td>Allow User Ovr Field Access</td>
<td>Allows users in this security class to set up UIFC Required and Field Access fields for themselves. Overrides UIPM setting for a selected security class.</td>
<td>Allows all users to set up UIFC Required and Field Access fields for themselves.</td>
</tr>
<tr>
<td>Allow Global Ovr Tab Seq</td>
<td>Allows users in this security class to set up UIFC tab sequencing fields (Next Field Ovr, Last, and First Field) for themselves, another user, or all users.</td>
<td>None</td>
</tr>
</tbody>
</table>

Table 4-6: Field Customization Settings
Keep in mind the following:

- All of the fields highlighted on Figure 4-18 have no default, so users initially do not have access to any of the field customization options.
- The entries on the UIPM form globally grant or deny access to all users.
- The entries on the SCD form override, for a selected security class, the corresponding entries on the UIPM form.

<table>
<thead>
<tr>
<th>Field</th>
<th>SCD</th>
<th>UIPM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Global Ovr Field Access</td>
<td>Allows users in this security class to set up UIFC Required and Field Access fields for themselves, another user, or all users.</td>
<td>None</td>
</tr>
<tr>
<td>Enable User Overrides</td>
<td>None</td>
<td>Activate any field customization settings set up on the SCD and UIPM forms.</td>
</tr>
</tbody>
</table>

**Table 4-6:** Field Customization Settings (cont’d)
Field Customization Parameters

Figure 4-18: Field Customization Parameters
Procedure for Enabling Field Customizations For All Users

Perform the following procedure to grant or deny the field customization options to all users. You can later override these entries for users in a particular security class.

Step 1. In the UT application, access the UIPM form.

Step 2. In the Allow User Ovr Tab Sequence field, enter Yes to allow users to customize tab sequencing for themselves on a form.

Enter No, or leave blank, if you do not want to enable all overrides for tab sequencing and field access.

Step 3. In the Allow User Ovr Field Access field, enter Yes to allow users to customize field access for themselves on a form.

Enter No, or leave blank if you do not want to allow users to customize tab sequencing.

Step 4. Save your changes on the UIPM form.

Procedure for Enabling Field Customization for Users in a Security Class

Perform the following procedure to allow access to or prevent access from the field customization options to users in a specified security class. These settings override, for a particular security class, the Allow User Ovr Tab Sequence and Allow User Ovr Field Access specifications on the UIPM form.

Note: If a user is a member of two or more security classes, and access to field customization is denied for any of those security classes, then the user will not have access to field customizations.

Step 1. In the UT application, access the Security Class Definition (SCD) form.
Step 2. At the Security Class ID LookUp prompt, enter the security class.

Step 3. In the Allow Global Ovr Tab Sequence field, do one of the following to define whether users can globally customize tab sequencing:
- Enter Yes to allow users in this security class to set up tab sequencing for themselves, another user, or all users.
- Enter No, or leave blank, to prevent users in this security class from globally customizing tab sequencing for themselves, another user, or all users.

Step 4. In the Allow User Ovr Tab Sequence field, do one of the following to define whether users can customize tab sequencing for themselves:
- Leave blank to allow the default, defined on the UIPM form, to apply to users in this security class.
- Enter Yes to allow users in this security class to customize tab sequencing for themselves.
- Enter No to prevent users in this security class from customizing tab sequencing for themselves.

Step 5. In the Allow Global Ovr Field Access field, do one of the following to define whether users can globally customize field access:
- Enter Yes to allow users in this security class to customize field access for themselves, another user, or for all users.
- Enter No, or leave blank, to prevent users in this security class from customizing field access for themselves, another user, or for all users.

Step 6. In the Allow User Ovr Field Access field, do one of the following to define whether users can customize field access for themselves:
- Leave blank to allow the default, defined on the UIPM form, to apply to users in this security class.
- Enter Yes to allow users in this security class to customize field access for themselves.
- Enter No to prevent users in this security class from customizing field access for themselves.

Step 7. Save your changes on the SCD form.

Repeat Steps 2 through 6 for all security classes for which you want to override the defaults defined on the UIPM form.
Procedure for Enabling Field Customization Settings

Setting up field customization parameters in either the UIPM or SCD form defines the parameters, but does not implement them. To enable the field customization settings, you must enable them from the UIPM form.

Step 1. In the UT application, access the UIPM form.

Step 2. In the Enable User Overrides field, enter Yes to enable all overrides for tab sequencing and field access.

Enter No if you do not want to enable overrides for tab sequencing and field access.

Step 3. Save your changes on the UIPM form.
Setting Up the Terminal-Style Bar Graph

Some processes may use techniques that are not currently supported by the GUI bar graph. If the GUI bar graph causes widespread disruption to batch processing in your application environment, you can revert to using the terminal-style bar graph.

![Terminal-Style Graph Parameter](image)

**Figure 4-19: Terminal-Style Graph Parameter**

**Procedure for Enabling the Terminal-Style Graph**

**Step 1.** In the UT application, access the UI Usage Parameters (UIPM) form.

**Step 2.** In the Enable Terminal-Style Graph field, enter **Yes** to enable the terminal-style bar graph for this application environment.

Enter **No** if you do not want to enable the terminal-style bar graph for this application environment. “No” is the default value for this field.
Step 3. Save your changes on the UIPM form.

**Note:** If you experience issues with only a few processes, you can use the terminal-style bar graph for only those select processes by using the Ignore UI Bar Graph (UIIG) form. Enter the process mnemonic for the process that does not work with the new GUI bar graph.
Setting Up the Browser-Based Help System

**Note:** This section provides information about setting up the Colleague Release 18 browser-based help system. This browser-based help system is not available for Colleague Release 17.

You can use the help servlet, included with WebAdvisor 3.x, to display help for UI users. Your users will benefit from being able to view help using the help servlet because it is displayed in a browser window and supports typical browser functions (searching, printing, changing the font size, etc.). See “Using the Browser-Based Help System” beginning on page 9-16 for additional information.

For more information about WebAdvisor and the help servlet, see *WebAdvisor Installation and Administration*.

There are two methods for defining which users will use the help system. You can set up an application environment so that every user of that environment will use the help system, or you can specify individual users to use the help system. Use the UI Usage Parameters (UIPM) form, shown in Figure 4-20, to set up an application environment to use the help system. Use the Operator Definition (SOD) form, shown in Figure 4-21, to give help system access to a specific user.
Figure 4-20: The UI Usage Parameters (UIPM) Form

Figure 4-21: The Operator Definition (SOD) Form
Procedure for Setting Up Browser-Based Help for All Users

Use this procedure to allow all users of an application environment to view help in the browser-based help system.

Step 1. Access the UI Usage Parameters (UIPM) form.

Step 2. In the Use Help Servlet field, enter Yes.

Step 3. In the Help Servlet field, enter the SERVLETS.ID for the help servlet, as defined in your WebAdvisor 3.x instance.

Step 4. In the Security Token Expires field, enter the amount of time, in seconds, after which the security token for the UI user will expire.

Step 5. Save from the UIPM form.

Technical Tip: Any users who are currently logged into the application environment for which you enable the browser-based help system will need to log out and then log back in to see the changes.

Procedure for Setting Up the Help System for a Specific User

Use this procedure to allow a specific user to view help in the browser-based help system.

Step 1. Complete “Procedure for Setting Up Browser-Based Help for All Users” on page 4-37 but leave the Use Help Servlet field set to “No.”

Step 2. Access the Operator Definition (SOD) form.
Step 3. At the Operator ID LookUp prompt, enter the operator ID for which you want to grant help system access.

Step 4. In the Use Help Servlet Override field, enter Yes.

Step 5. Save from the SOD form.

Step 6. Repeat this procedure for other users who want to use the help system.
Setting Up the Record Delete Icon

In UI, some users have the record delete icon on the toolbar and others do not. UI checks the user’s devices record for a keyboard definition. The keyboard definition record is then examined for an entry in the record delete field. If the record delete field contains an entry, it means that the user had permission to delete a record in character mode, so they should be able to do so in UI. Conversely, if the user did not have permission in character mode, the user should not have permission in UI. If the user does not have a devices record, they will automatically get the record delete icon.

Figure 4-22: Record Delete Icon in UI

Procedure for Adding the Record Delete Icon

If you have users that had permission to delete records in character mode but do not have the record delete icon in UI, use the following procedure to add the record delete icon.

**Step 1.** Use a line editor to open the desired keyboard definition record (K*...) in the KEYDEFS file.

**Step 2.** Go to the second field (KBD.FUNCTION.MAP) of the record and type EV. The EV command expands the contents of a multi-valued field so the values can be edited as though they were fields of a record. EV essentially starts up an editor within the editor.

**Step 3.** Navigate to value 47 of the KBD.FUNCTION.MAP multi-valued field. Place a character at value 47. If there were other values present in the KBD.FUNCTION.MAP field, avoid entering duplicate data.
Step 4. FILE twice: Once to save the changes made to the values of the KBD.FUNCTION.MAP field and then FILE again to save the changes to the record.

Note: There is, however, a caveat when using this method. The KBD.FUNCTION.MAP field is compiled from data gathered by the Define Terminal Keyboard (SKB) form, Define Function Keys (SKB1) form, and Define Cursor Keys (SKB2) form in UT. Therefore, if you manually edit the keyboard definition record from an editor, you will lose those changes if you pull the record up in any one of those three forms and finish from the form.
Limiting User Access to Features

Some features that are available in UI should not be available to all of your users. In particular, consider limiting access to the features listed in Table 4-7.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query Builder</td>
<td>This is a selection on the Options menu. It provides a graphical interface for users to query directly against the database.</td>
<td>“Query Builder Security” on page 6-1</td>
</tr>
<tr>
<td>Import File and Export File</td>
<td>These are selections on the Options menu. They allow a user to transfer files between the application host computer and their PC.</td>
<td>Online help in UI.</td>
</tr>
<tr>
<td>Administer Databases</td>
<td>This is a selection on the Options menu. It permits the system administrator to maintain the list of databases available through User Interface, and to define whether users have access to a terminal interface and the Datatel User Setup program.</td>
<td>“Setting Up the Administrative Parameters” on page 4-6.</td>
</tr>
<tr>
<td>SHEL</td>
<td>This mnemonic gives users access to most of the commands available from the UniData colon prompt.</td>
<td>“Colon Prompt Access” on page A-1.</td>
</tr>
<tr>
<td>UI Administration Parameters (UIPR) form, UI Usage Parameters (UIPM) form</td>
<td>System administrators use the UIPR and UIPM forms to specify User Interface parameters, including defaults for administrative menu options.</td>
<td>“Setup” on page 4-1.</td>
</tr>
<tr>
<td>User Interface Response Map (UIRM) form</td>
<td>System administrators use the UIRM form to set up different startup sequences for the terminal interface and UI.</td>
<td>“Defining the Startup Sequence” on page 7-1.</td>
</tr>
<tr>
<td>User Interface Databases (UIDB) form</td>
<td>System administrators may use the UIDB form to view and maintain the databases available from a user’s PC.</td>
<td>“Viewing a User’s Databases” on page 9-8.</td>
</tr>
</tbody>
</table>

Table 4-7: Recommended Limited-Access Features
Limiting access to these features basically involves two steps:

1. Create or update security classes on the Security Class Definition (SCD) form.
2. Assign the security classes to users on the Operator Definition (SOD) form.

Because the setup and assignment of security classes is unique to each institution, no step-by-step procedure is provided here. Figure 4-23 shows an example of the SCD form, which restricts access to all of the features listed above. Note the different methods used to secure these features:

- To secure the Query Builder option, enter No in the Allow Query Builder Access field. Similarly, to secure the Import/Export Files options, enter No in the Allow Import field and the Allow Export field.
- To secure the Administer Databases option, follow the procedure in “Setting Up the Administrative Parameters” beginning on page 4-6. That section describes how the Allow Administer Databases field on the SCD form interacts with setup on the UI Administration Parameters (UIPR) form.

![Figure 4-23: Limiting User Access From the SCD Form](image)
In This Chapter

This chapter explains how to set up User Interface (UI) to establish a secure telnet connection between UI and the Colleague or Benefactor server. It explains how to request certificates, install certificates, apply certificates to servers, and view the certificates in the key store path. This chapter also describes how to customize the server’s secure sockets layer (SSL) configuration and how to renew certificates.

Table 5-1 lists the topics in this chapter.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding Security</td>
<td>5-2</td>
</tr>
<tr>
<td>Implementing Security</td>
<td>5-6</td>
</tr>
<tr>
<td>Viewing Certificates</td>
<td>5-32</td>
</tr>
</tbody>
</table>

Table 5-1: Topics in This Chapter

If you do not want to establish secure transmissions, you can skip this chapter. UI will still work, but transmissions will be non-secure.
Understanding Security

UI uses SSL technology to secure communications between UI and Colleague/Benefactor.

If you choose to deploy security, you must have one certificate for each server that you intend to secure. All Colleague and Benefactor environments that run on a server with a certificate are capable of using SSL-secured communications. Though SSL is enabled at the environments level, certificates are managed for all environments on the server.

Note: For Release 17, you must use an installation account for certificate management.

The security forms simplify SSL configuration for clients who are unfamiliar with certificate technology. However, these forms do not allow you to generate keys with a great deal of flexibility. Experienced SSL clients may find the security forms too restrictive. For those users, the UniAdmin system administration tool offers a more robust alternative. Please refer to IBM’s UniAdmin documentation for more information about UniAdmin.

If you do not want to establish a secure telnet connection, you may continue using non-secure telnet.

After implementing the secure telnet service, you may disable your standard telnet service. However, other components of the Datatel system require that you temporarily re-enable standard telnet for tasks, such as software installations. For example, certain InstallShields interact with the host telnet port, and require that you open the port.

Public and Private Keys

A server employing SSL encryption requires two keys:

- **Private key.** Kept protected and is known only to the owner.
- **Public key.** Distributed openly to all devices that request a connection to the server through an SSL-secure port.

As part of the public key’s certification process, the key is packaged up, with the key owner’s information, into a certificate-signing request. The public key, with information identifying the key pair owner, becomes the certificate. After a trusted independent authority (known as a Certificate Authority)
validates the information regarding the key owner. When the key pair owner’s identity is verified, the CA approves the public key with a digital signature. The signed public key is known as the certificate.

Security Overview

UI Desktop Security Overview

To enable Secure Sockets Layer (SSL) in a Colleague or Benefactor account, you must first purchase a certificate from a Certificate Authority (such as VeriSign), and install the certificate on your server using the security forms. Datatel recommends purchasing at minimum a 128-bit certificate.

You must install the certificate on an install account. You can then enable security in all main accounts on the server, regardless of which install account the main accounts are associated with. Datatel recommends using your live install account because it is likely to be the most stable account.

To purchase a digital certificate, you first need to create a certificate request. When creating your certificate request on the UI Certificate Request (UICR) form, you must enter your server’s fully qualified domain name. This must be the same as the Host Name you used during Database Administration Setup to set up UI accounts for the server (see “Procedure for Administering Databases” on page 4-13).

When a user logs on to Colleague by using SSL authentication, UI compares the host name that it used to connect to the server with the server certificate’s common name. If the names are different, the SSL Server Validation dialog (Figure 5-1) warns the user about the discrepancy in names and asks whether the user trusts the server. If the user selects No, they could potentially connect to the server over an non-secure port.

Figure 5-1: The SSL Server Validation Dialog Box
Most Certificate Authorities (CAs) do not sign a certificate unless the common name is the server’s fully qualified domain name. If you used the IP address for Host Name during the Database Administration Setup, and your CA does not allow that, you must change it to the server’s fully qualified domain name by doing the following:

1. Change the UI database definition’s host name to use the server’s fully qualified domain name (see “Procedure for Administering Databases” on page 4-13).

2. Ensure that all users remove, and then re-add the database definition in their local datatel.ini (see “Adding Databases” on page 9-6).

**Note:** UI uses the Root Certificates stored in Internet Explorer’s Trusted Root Certificate Authority store. If you do not have Internet Explorer 5.5 or later on the PC that is running UI, you may need to use the Windows Certificate Import Wizard to install the Certificate Authority’s root certificate.

The parameter settings, consisting of the client configuration settings necessary for you to connect UI to the database server via SSL, are delivered on the UI Security software update.

**Note:** You must have administrator permissions to set up SSL. You must also be logged on as a root user (or, you can change the file permissions to $UDTHOME/unishared/unisecurity). This file contains sensitive data, and must be kept secure.

In addition to this setup, UNIX clients must also configure the secure telnet server. Refer to your UniData documentation for the procedure. For example, this information is in Appendix C, “Configuring SSL for Telnet,” in IBM’s Administering UniData on UNIX manual, Version 6.0, available from the IBM Web site.

**Note:** After SSL is configured for UI Desktop, the line of communication between the UI Web server and Colleague will also be secure.

**UI Web Security Overview**

To enable SSL on the UI Web server, you must purchase a certificate from a certificate authority (CA) and install the certificate on your UI Web server, using the Microsoft Management Console (MMC). Datatel recommends purchasing, at minimum, at 128-bit certificate.
The UI Web server certificate must first be combined with its corresponding private key into a .pkcs12-vault file. When the vault file has been generated, the certificate can be imported into the UI Web server’s OS key store for the “local machine.” When importing the vault file, it is important that you:

- Use the local PC’s personal store.
- Mark the vault file private key as “exportable.”

Failure to do these will result in SSL not working for the UI Web server.
Implementing Security

You can implement security for UI Desktop, UI Web, or both. This section describes the security options, and provides detailed procedures for implementing them.

Implementation Options

If you plan to deploy SSL with UI Desktop, you should install the certificate on the application server where the Colleague/Benefactor accounts are stored, as shown in Figure 5-2. “Implementing Security for the Application Server” beginning on page 5-8 describes how to implement SSL for UI Desktop.

If you do not install certificates on the appropriate servers, you can still use UI Desktop and UI Web, but the connection will not be secure.

SSL with UI Desktop

Figure 5-2: SSL with UI Desktop

If you plan to deploy SSL with UI Web, you should install the certificate on both the application server and the UI Web server, as shown in Figure 5-3.

Use the following procedures to implement SSL in this configuration:
■ “Implementing Security for the Application Server” on page 5-8.
■ “Implementing Security for the UI Web Server” on page 5-16.
If you plan to deploy SSL with both UI Desktop and UI Web, you should also install the certificate on both the application server and the UI Web server, as shown in Figure 5-4.

Use the following procedures to implement SSL in this configuration:

- “Implementing Security for the Application Server” on page 5-8.
- “Implementing Security for the UI Web Server” on page 5-16.
Implementing Security for the Application Server

To enable security on the application server, you must do the following on the server where the Colleague/Benefactor application resides:

- Obtain the Certificate.
- Install the Certificate.
- Apply the Certificate to the Server.

Obtaining Certificates for the Application Server

Use the UI Certificate Request (UICR) form, shown in Figure 5-5, to create key pairs and certificate requests on the application server. You do not need to create key pairs and certificate requests at the same time.

If you are creating a certificate request, you must complete the organization information fields on the lower half of the form. Specify a directory to place the keys and requests. If an item already exists, you must confirm that you want to overwrite the existing files.

Envision displays the certificate request in the Certificate Signing Request dialog, shown in Figure 5-6. Copy the request from this dialog and submit it to your CA for verification.

Procedure for Obtaining a Certificate for the Application Server

Use this procedure to obtain a certificate for the application server. Perform this procedure from an install account. Datatel recommends using your live install account because it is likely to be the most stable account.

Step 1. Create the key store directory at the OS level and make sure that it is accessible only to administrators.

If you are renewing a certificate and remember the keystore password, you can skip this step and proceed directly to Step 2. If you are renewing a certificate but have forgotten the keystore password, you should create a new key store directory. (This is easier than overwriting the contents of the existing key store.)
Step 2. From the Envision Run-Time (UT) application, access the UI Certificate Request (UICR) form.

Step 3. In the Key Store Path field, enter the path to the directory created in Step 1.

If you are renewing a certificate, enter the path to the directory containing the key pair you want to use.

Step 4. In the Generate New Key Pair field, enter Yes. If you are renewing a certificate, enter No.

Step 5. In the Key Password field, enter a password for the private key. Remember this password. You will need it to access the key on the UI Security Context Record (USCR) form later.

Step 6. In the Generate New Request field, enter Yes.

Step 7. In the lower portion of the form, enter information about your organization.
Step 8. Save from the UICR form.

A dialog appears displaying the generated certificate signing request, SERVERsign.csr.

![Certificate Signing Request Dialog Box](image)

**Figure 5-6: The Certificate Signing Request Dialog Box**

Step 9. Highlight and copy the certificate signing request contents (including the Begin Certificate Request and End Certificate Request lines) from the dialog.

The UICR process generates the following OS files:

- **SERVERpriv.pem.** The private key (encrypted).
- **SERVERpub.pem.** The public key.
- **SERVERsign.csr.** The certificate signing request (the public key in addition to your information).

Step 10. Send the signing request to the trusted Certificate Authority, according to the CA's procedure for doing so.

The CA then sends you a server certificate (usually accompanied with an intermediate root certificate).
Installing a Certificate on UniData

Use the appropriate procedure to install the certificate, depending on whether the CA issues the certificate to you in an e-mail or as an OS file.

Perform this procedure from an install account. Datatel recommends using your live install account because it is likely to be the most stable account.

**Procedure for Installing a Certificate Issued to You by E-Mail**

If your certificate is issued to you in an e-mail, use the UI Certificate Management (UICM) form (Figure 5-7) to import your CA-issued certificate to the server. You must store the certificate in the same directory as its private key counterpart. Therefore, the Key Store Path must be the same path used on the UI Certificate Request (UICR) form. If you access the UICM form directly after using the UICR form, the key store path is already set.

**Step 1.** From the Envision Run-time application, access the UI Certificate Management (UICM form).

![UI Certificate Management (UICM) Form](image)

*Figure 5-7: UI Certificate Management (UICM) Form*
Step 2. Enter the same path to the directory where the key pair and signing request were generated on the UICR form (Step 3 on page 5-15).

Step 3. Detail on the Upload Certificate field.

Step 4. Copy the certificate text from the e-mail, including the labels.

----BEGIN CERTIFICATE-----/-----END CERTIFICATE-----

Step 5. Paste the certificate text into the dialog and click OK.

Note: If your Certificate Authority issued an Intermediate Root Certificate with your Server Certificate, you must “chain” the certificates together by pasting the Intermediate Certificate below the Server Certificate. The Intermediate Certificate contains the public key that is used to verify the signature on your Server Certificate.

Step 6. Save out of the UICM form.

Step 7. The UICM process generates the following OS file:

SERVERcert.cer. Your signed server certificate containing the public key generated on the UICR form.

Step 8. If you are renewing a certificate, select Yes to overwrite the existing file.

Procedure for Installing a Certificate Issued to You in an OS File

If your certificate is issued to you in an OS file, use the following steps to import the CA signed certificate to your server.

Step 1. Upload the certificate to the server.

Step 2. Place the certificate in the key store path where the private key and signing request were generated on the UICR form.

Step 3. Name the file SERVERcert.cer.
Applying a Certificate to the Application Server

If you apply a certificate for use with UI Desktop or UI Web, you can use the UI Security Context record (USCR) form (Figure 5-8) in Envision to apply a certificate to the application server.

The UI Security Context Record stores a private key and matching certificate for use with secure connections to the server. The security context record is stored encrypted. To decrypt a security context record, you must supply the correct password. There can be multiple security context records, but only one is used by the secure telnet server. Because the security context is global, all Colleague and Benefactor accounts on a server use the same secure connection information. These accounts have enabled the account parameter for SSL communications, and are running on the same secure telnet server.

When UI requests an SSL-secure connection to the server:
1. The server retrieves the certificate stored in the active security context record, and gives the certificate to UI. UI is responsible for verifying that the certificate’s signature is valid. It does this by using the signing authority’s root certificate, which is installed on the PC that is running UI.
2. UI acknowledges that the certificate’s signature has been verified and is trusted, and then sends a message to the server.
3. The server retrieves the private key stored in the security context record, encrypts UI’s message using the private key, and sends the encrypted message back to UI.
4. UI decrypts the message using the server’s public key located in the certificate the server had issued earlier.
5. If UI can read the message, then authentication (or SSL handshake) is complete, and the communications between UI and the server are secure.

When you create a security context record on the USCR form, you first assign it a name. You are then prompted to assign a password for the record. For enhanced security, this password must be at least eight characters long. The security context record is stored encrypted. You will need this password to decrypt and access the security context record. Do not confuse the security context password with your private key password (you assigned the private key password while generating the private/public key pair on the UICR form).

Note: You must create the security context record in an install account.
The certificate (signed public key) and the private key are the key pair that was initiated from the UICR form. When you create a security context, the key pair must match (otherwise encryption will not work). The USCR process ensures that the key pair match before it creates the security context record.

**Procedure for Applying a Certificate to the Application Server**

Perform this procedure from the same install account where you created and installed the certificate.

**Step 1.** From the Envision Run-Time (UT) application, access the UI Security Context Record (USCR) form.

![USCR-UI Security Context Record](image)

**Figure 5-8:** The UI Security Context Record (USCR) Form

**Step 2.** At the UI Security Context ID LookUp prompt, enter a name for the security context record.
Step 3. At the Security Context Password prompt, enter a password for the security context record.

Note: The security context record is stored encrypted. Remember this password. You cannot access the context record without its password.

Step 4. In the Key Store Path field, enter the path to the key store, which contains the server certificate and private key that you want the server to use for secure connections.

If the SERVERcert.cer and SERVERpriv.pem files do not exist in the directory supplied, an error occurs. If they do exist, they appear in the Private Key File and Certificate File fields.

Step 5. In the Private Key Password field, enter the password for the SERVER private key so it can be unlocked and stored in the security context record.

This is the password that you created in the Key Password field on the UICR form (Step 5 on page 5-15).

The Private Key File and Certificate File are inquiry fields that display the assumed file paths to the private key and certificate that are added to the security context.

Step 6. Set the Current Context Record field to Yes, which configures the secure telnet server to use the current security context record for securing communications.

Step 7. Save and finish from the USCR form.

USCR generates a security context record in the _SECUCTX_ file.
Implementing Security for the UI Web Server

To enable security with UI Web, you must (in addition to securing the application server) establish SSL on the UI Web server by doing the following:
1. Obtain the Certificate.
2. Import the Certificate.
3. Generate the Vault File.
4. Install the Vault File.
5. Apply the Certificate to the Server.

Obtaining Certificates for the UI Web Server

Use the UI Certificate Request (UICR) form, shown in Figure 5-5, to create key pairs and certificate requests on the wIntegrate server (for UI Web). You do not need to create key pairs and certificate requests at the same time.

If you are creating a certificate request, you must complete the organization information fields on the lower half of the form. Specify a directory to place the keys and requests. If an item already exists, you must confirm that you want to overwrite the existing files.

Envision displays the certificate request in the Certificate Signing Request dialog, shown in Figure 5-6. Copy the request from this dialog and submit it to your CA for verification.

Procedure for Obtaining Certificates for the UI Web Server

Step 1. Create the key store directory at the OS level and make sure that it is accessible only to administrators.

If you are renewing a certificate and remember the keystore password, you can skip this step and proceed directly to Step 2. If you are renewing a certificate but have forgotten the keystore password, you should create a new key store directory. (This is easier than overwriting the contents of the existing key store.)
Step 2. From the Envision Run-Time (UT) application, access the UI Certificate Request (UICR) form.

Step 3. Populate the fields on the UICR form as follows:

- In the Key Store Path field, enter the path to the directory created in Step 1. If you are renewing a certificate, enter the path to the directory containing the key pair you want to use.
- In the Generate New Key Pair field, enter Yes. If you are renewing a certificate, enter No.
- In the Key Password field, enter a password for the private key. Remember this password. You will need it to access the key on the UI Security Context Record (USCR) form later.
- In the Generate New Request field, enter Yes.

In the lower portion of the form, enter information about your organization.

Note: When installing a certificate for UI Web, the Common Name is the DNS name of the UI Web server.

Step 4. Save from the UICR form.

A dialog appears displaying the generated certificate signing request, SERVERsign.csr.

Step 5. Highlight and copy the certificate signing request contents from the dialog.

The UICR process generates the following OS files:

- SERVERpriv.pem. The private key (encrypted).
- SERVERpub.pem. The public key.
- SERVERsign.csr. The certificate signing request (the public key in addition to your information).

Step 6. Send the signing request to the trusted Certificate Authority, according to the CA's procedure for doing so.

The CA then sends you a server certificate (usually accompanied with an intermediate root certificate).
Importing Certificates to Generate the Vault File

Use the appropriate procedure below to install the certificate, depending on whether the CA issues the certificate to you in an **e-mail** or as an **OS file**.

Perform this procedure from an install account. Datatel recommends using your live install account because it is likely to be the most stable account.

**Procedure for Importing Certificates Issued to You by E-Mail**

If your certificate is issued to you in an **e-mail**, use the UI Certificate Management (UICM) form (Figure 5-7) to import your CA-issued certificate to the server. You must store the certificate in the same directory as its private key counterpart. Therefore, the Key Store Path must be the same path used on the UI Certificate Request (UICR) form. If you access the UICM form directly after using the UICR form, the key store path is already set.

**Step 1.** Access the UICM form.

![UICM UI Certificate Management (UICM) Form](image)

**Figure 5-9:** UI Certificate Management (UICM) Form

**Step 2.** Enter the same path to the directory where the key pair and signing request were generated on the UICR form (Step 3 on page 5-15).
Step 3. Detail on the Upload Certificate field.

Step 4. Copy the certificate text from the e-mail, including the labels.

```
-----BEGIN CERTIFICATE-----/-----END CERTIFICATE-----
```

Step 5. Paste the certificate text into the dialog and click OK.

**Note:** If your Certificate Authority issued an Intermediate Root Certificate with your Server Certificate, you must “chain” the certificates together by pasting the Intermediate Certificate below the Server Certificate. The Intermediate Certificate contains the public key that is used to verify the signature on your Server Certificate.

Step 6. Save out of the UICM form.

The UICM process generates the following OS file:
- `SERVERcert.cer`. Your signed server certificate containing the public key generated on UICR.

Step 7. If you are renewing a certificate, select **Yes** to overwrite the existing file.

**Procedure for Importing Certificates Issued to You in an OS File**

If your certificate is issued to you in an OS file, use the following steps to import the CA signed certificate to your server.

Step 1. Upload the certificate to the server.

Step 2. Place the certificate in the key store path where the private key and signing request were generated on the UICR form.

Step 3. Name the file `SERVERcert.cer`. 
Generating the Vault File

Use the UI Web Server Certificate (UIWC) form to generate a pkcs12-vault file (certificate and private key) for use by the UI Web Server.

A pkcs12-formatted file is often referred to as a Vault File or Keystore. It contains both a signed certificate (public key) and its corresponding private key. The pkcs12-vault file safely stores a key pair (certificate and private key), so that the vault file is stored encrypted, preserving the secrecy of the private key contained within. The UIWC process sets the pkcs12-vault file’s password using the private key’s password. The same password is used for both files.

When you create a pkcs12-vault file on the UIWC form, you first enter the OS directory where the certificate and private key reside. The certificate (SERVERcert.cer) and private key (SERVERpriv.pem) are displayed in their respective fields (if they exist in the directory that you supplied). The key pair must match. Otherwise encryption will not work. The UIWC process ensures that the key pair matches before creating the pkcs12-vault file.

Because the private key is stored encrypted, you must provide the password that you used when you created the private key on the UI Certificate Request (UICR) form. If you do not know this password you cannot access the private key, and therefore cannot generate the pkcs12-vault file.

The UI Web server uses the Windows Operating System’s certificate store to store its certificate. After the pkcs12-vault file is generated on the UIWC form, you must copy it from the database server to the Windows Server running the UI Web server software. When the pkcs12-vault file is there, you must then import the certificate into the Windows server certificate store.

Procedure for Generating the Vault File

Step 1. From the Envision Run-Time (UT) application, access the UI Web Server Certificate (UIWC) form.
Step 2. Populate the fields on the UIWC form as follows:

- Enter the same path to the directory where the key pair and signing request were generated on the UICR form (Step 3 on page 5-15). If you are renewing a certificate, enter the path to the directory containing the key pair you want to use.
- In the Private Key Password field, enter a password for the private key. Remember this password. You will need it later to install the certificate on the UI Web server.
- In the Generate UI Web Cert field, enter Yes to generate a pkcs12-vault file.

When you enter Yes for UI Web Cert, a message is displayed, informing you that the UI Web certificate has been generated.

Step 3. Click OK.

The UI Web Cert File field now shows the OS path to the newly-created pkcs12-vault file (UI Web Certificate).

Step 4. After the UI Web Certificate file is generated, detail on the UI Web Cert File field to display the Save UI Web Certificate dialog.
Step 5. From the Save UI Web Certificate dialog, select the Windows server where the UI Web server is installed.

**Note:** If the Windows server is not available from the dialog, you must manually copy the file to the appropriate directory.

**Installing the Vault File**

Use Microsoft Management Console to install the vault file into the server’s Personal certificate store as outlined in the following steps. This allows the wIntegrate server to access the vault file.

**Procedure for Installing the Vault File**

**Step 1.** From the Windows Start menu, select Run and enter **MMC** to start the Microsoft Management Console.
Figure 5-12: Microsoft Management Console

**Step 2.** From the File menu of the console, select **Add/Remove Snap-in...** to display the Add/Remove Snap-in dialog.

Figure 5-13: MMC Standalone Tab
Step 3. On the **Standalone** tab, click **Add** to display the list of Standalone Snap-ins.

![Add Standalone Snap-In Dialog](image)

**Figure 5-14: Add Standalone Snap-In Dialog**

Step 4. Select Certificates, then click **Add**.

![Certificates Snap-In Dialog](image)

**Figure 5-15: Certificates Snap-In Dialog**
Step 5. Select the Computer Account certificate snap-in to manage certificates for the wIntegrate server service, then click Next to display the Select Computer dialog.

Figure 5-16: Select Computer Dialog

Step 6. Select the computer you are going to manage, then click Finish.

Note: If you are at the server console, select the Local computer.

Step 7. Close the Add Standalone Snap-in dialog to return to the Add/Remove Snap-in dialog. The Certificates snap-in is displayed in the list of snap-ins.

Step 8. Click OK to return to the console screen.
Step 9. Right-click on the Personal node, select All Tasks, then Import to launch the Certificate Import Wizard.

Step 10. Click Next to display the File to Import page.
Step 11. In the File Name field, enter the path to the UIWEBcert.p12 certificate file, then click Next to display the Password page.

Step 12. In the Password field, enter the private key’s password, check the Mark this key as exportable...box, and click Next.
Step 13. Confirm that the certificate is placed in the wIntegrate server certificate store, and click Next.

Figure 5-21: Certificate Store Window

Figure 5-22: Completing the Certificate Import Wizard Window
Step 14. Click **Finish**.

Step 15. If the certificate was imported successfully, a confirmation dialog appears. You can also confirm that the certificate was successfully imported by selecting Certificates from the Personal mode, and viewing the list of certificates in the right pane.

![Example of Successful Certificate Import](image)

**Figure 5-23:** Example of Successful Certificate Import

### Applying a Certificate to the UI Web Server

If you are applying a certificate for use with UI Web, you must use the wIntegrate Administrator tool to apply the certificate.

**Procedure for Applying a Certificate to the UI Web Server**

**Step 1.** From the Windows start menu, select **All Programs**, then **Datatel**, then **UI Web**, and then **Administration** to display the wIntegrate Administrator dialog.
Figure 5-24: wIntegrate Administrator Dialog

**Step 2.** Connect to the wIntegrate server:

- a. Click **Connect**.
- b. Enter **UIWeb** in the Username field (leave Password field blank).
- c. Click **OK**.

**Step 3.** Click **Options** to display the Options dialog.

**Step 4.** In the Options dialog box, select the Server tab, and populate the fields as follows:

- a. Select the SSL box.
- b. In the SSL Certificate field, enter the name of the server that you are securing.

**Note:** This should be the same as the certificate common name that you entered in Step 3 of “Procedure for Obtaining Certificates for the UI Web Server” beginning on page 5-16.

- c. Click **OK**.
Step 5. On the Administrator dialog, click the Close button.

Step 6. Restart the wIntegrate server service as follows:

   a. From the Windows Start menu, navigate to the Control Panel, then Administrative Tools, then Services, and then wIntegrate Server.
   
   b. Click the Restart Service button.
      
      The connection between the applet and the wIntegrate server are now secure.
Viewing Certificates

Use the UI Certificate Inquiry (UICI) form, shown in Figure 5-27, to view the certificates and certificate signing requests in the given key store path.

![UI Certificate Inquiry](image)

**Figure 5-27:** The UI Certificate Inquiry (UICI) Form

After entering a key store path, you can detail on a certificate type to display the certificate in a dialog box. The corresponding certificate or request must already exist in the specified directory.

Figure 5-28 is an example of a certificate dialog box.
Procedure for Viewing Certificates

Step 1. From the Envision Run-Time (UT) application, access the UI Certificate Inquiry (UICI) form.

Step 2. Enter the Key Store Path.

Step 3. Detail on the item you want to view.
Query Builder Security

In This Chapter

This chapter explains how to set up Query Builder security.

Table 6-1 lists the topics in this chapter.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Understanding Query Builder Security&quot;</td>
<td>6-2</td>
</tr>
<tr>
<td>&quot;Securing Query Builder&quot;</td>
<td>6-4</td>
</tr>
</tbody>
</table>

**Table 6-1**: Topics in this Chapter
Understanding Query Builder Security

Query Builder is a utility available in UI that users can use to perform queries. The advantage of giving users access to Query Builder is that those users will no longer need access to the colon prompt.

With Release 18, the colon prompt is no longer available. Users who may have performed queries at the colon prompt in previous releases must now use Query Builder to perform queries.

Any user who has access to Query Builder should also have security restrictions (for example, which files the user is allowed to query). Query Builder security is similar to Envision security in that security classes are used to determine the level of access available to a user.

You most likely currently have security classes defined for different classes of users at your institution. You may use these existing security classes to define Query Builder security or you can define new security classes and add those classes to a user’s OPERS record. You will need to determine which method is best for your institution’s needs.

**ALERT!** As delivered, Query Builder has no security. If you allow your users access to Query Builder, be sure to complete the security setup detailed in this chapter for all users.

Keywords Allowed in Query Builder

Due to the potentially malicious nature in which some previously-available keywords could be used, only certain keywords are allowed with Query Builder. The full list of allowed keywords is in the QB.VALID.KEYWORDS record in the UT.PARMS file. Two keywords that previously could be used but are now no longer available include ALL and DELETING. Both keywords could be used to circumvent established security policies at your institution.
Forms Used

Table 6-2 lists the forms used in this chapter.

<table>
<thead>
<tr>
<th>Form</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query Builder Computed Column (QBCC)</td>
<td>Used to define which computed columns are available for queries.</td>
</tr>
<tr>
<td>Sec Class QueryBuilder Access (SCQA)</td>
<td>Used to define security parameters for a security class.</td>
</tr>
<tr>
<td>UI Administration Parameters (UIPR)</td>
<td>Used to globally control access to Query Builder.</td>
</tr>
</tbody>
</table>

Table 6-2: Forms Used to Secure Query Builder
Securing Query Builder

Three forms are used to secure Query Builder: The UI Administration Parameters (UIPR) form, the Sec Class QueryBuilder Access (SCQA) form, and the Query Builder Computed Column (QBCC) form.

The UI Administration Parameters (UIPR) Form

Use the UIPR form, shown in Figure 6-1, to globally control access to Query Builder for an application environment.

![UI Administration Parameters (UIPR) Form](image)

**Figure 6-1:** UI Administration Parameters (UIPR) Form

Noteworthy Fields on the UIPR Form

Below are the noteworthy fields on the UIPR form for defining Query Builder security. Refer to online help and “Setup” on page 4-1 for information on other fields on this form.
Securing Query Builder

**The Allow Query Builder Access Field**

Enter **Yes** if you want to allow users access to Query Builder for this environment. Enter **No** if you do not want to allow users access to Query Builder.

You can override the value of this field for an individual security class using the SCQA form.

**The Restrict Query Builder Apps Field**

Enter **Yes** to restrict users to querying files from a predefined list of allowed applications, as defined on the SCQA form. Allowed applications from all security classes assigned to a user are combined into a single combined list. The user’s queries in Query Builder are limited to files from the applications in this combined list.

Enter **No** to allow users to query files from any application.

**The Allow Computed Columns in QB Field**

Enter **Yes** if you want computed columns to be available for queries from Query Builder. Enter **No** if you do not want to allow computed columns to be used in queries from Query Builder.

This parameter is the default for this application environment. You can override this value for a specific security class on the SCQA form. You can also restrict computed columns in a specific file from being used in queries from Query Builder on the QBCC form.

**The Sec Class QueryBuilder Access (SCQA) Form**

Use the SCQA form, shown in Figure 6-2, to define the Query Builder security parameters for a specific security class.
The SCQA form allows you to define Query Builder security for a security class, not for a specific user. If you have multiple security classes assigned to a user, you will need to carefully evaluate the Query Builder security parameters for that user.

For example, if you have the PERSON file listed as an allowed file for querying for security class ADMIN and you have the PERSON file listed as a restricted file for querying for security class HR_OFFICE and a user is assigned to both those security classes, that user will not be able to query against the PERSON file.

**Noteworthy Fields on the SCQA Form**

Below are the noteworthy fields on the SCQA form. Refer to online help for information on other fields on this form.

**The Allow Query Builder Access Field**

Enter **Yes** to allow users assigned to this security class access to Query Builder. Enter **No** to restrict users assigned to this security class access to Query Builder. The value in this field overrides the value on the UIPR form.
If you have multiple security classes assigned to a particular user, a “No” entry in this field for any of the security classes will prevent that user from accessing Query Builder, regardless of the entry in this field for the rest of the assigned security classes.

**The Valid Applications for Query Builder Field**

If you are restricting which applications a user assigned to this security class may query, list the applications in this field that you want the user to be able to query.

If you have multiple security classes assigned to a particular user and application restriction activated for any of the security classes, a list of valid applications is created from the entries in this field for each security class.

**Technical Tip:** If you want to allow users to query a custom file that is not associated with an application but you also want to restrict application queries, list NULL as an entry in the Valid Applications for Query Builder field.

**The Query Builder Computed Column (QBCC) Form**

Use the QBCC form, shown in Figure 6-3, to define whether specific computed columns can be used in queries.
Noteworthy Fields on the QBCC Form

Below are the noteworthy fields on the QBCC form. Refer to online help for information on other fields on this form.

The Allow Computed Columns in Query Builder Field

Indicate if computed columns in this file can be used in queries.

Enter **Yes** if you want computed columns in the current file to be available for queries through Query Builder. Enter **No** if you do not want to allow computed columns in the current file to be used in queries from Query Builder. A blank value in this field is treated as a “Yes” value.

The entry in this field is the most restrictive value for allowing computed columns to be used in queries from Query Builder. If you enter “No” in this field, computed columns in this file will not be available for queries, regardless if a user is allowed to use computed columns in queries (as specified in the security classes assigned to that user).
Procedure for Securing Query Builder

Use this procedure to define Query Builder security.

**Step 1.** Access the UI Administration Parameters (UIPR) form.

**Step 2.** Do you want to allow access to Query Builder for all users?

- **Yes.** Enter Yes in the Allow Query Builder Access field. Continue with the rest of this procedure.
- **No.** Enter No in the Allow Query Builder Access field. Skip to Step 6 to define Query Builder security for a specific security class. If you do not want to define security for any security classes, you are finished with this procedure.

**Step 3.** Do you want to restrict queries to allowed applications only?

- **Yes.** Enter Yes in the Restrict Query Builder Appls field.
- **No.** Enter No in the Restrict Query Builder Appls field.

**Step 4.** Do you want to allow computed columns to be used in queries?

- **Yes.** Enter Yes in the Allow Computed Columns in QB field.
- **No.** Enter No in the Allow Computed Columns in QB field.

**Technical Tip:** You can use the Query Builder Computed Column (QBCC) form to define which computed columns are available for queries.

**Step 5.** Finish from the UIPR form.

**Step 6.** Access the Sec Class QueryBuilder Access (SCQA) form. At the LookUp prompt, enter the security class for which you want to define security for Query Builder.

**Step 7.** Do you want to allow access to Query Builder for users with this security class? Your entry in this field overrides the value entered in Step 2.
Yes. Enter Yes in the Allow Query Builder Access field.

No. Enter No in the Allow Query Builder Access field.

Step 8. Do you want to restrict queries to allowed applications only for users with this security class? Your entry in this field overrides the value entered in Step 3

Yes. Enter Yes in the Restrict Query Builder Applications field.

No. Enter No in the Restrict Query Builder Applications field.

Step 9. Do you want to allow users assigned to this security class to be able to use computed columns in queries?

Yes. Enter Yes in the Allow Computed Columns in QB Queries field.

No. Enter No in the Allow Computed Columns in QB Queries field.

Step 10. In the Valid Applications for Query Builder field, enter the list of applications against which users assigned to this security class may query. You only need to complete this step if you entered “Yes” in Step 8.

Step 11. In the Valid Verbs for Query Builder field, enter the list of verbs (such as SORT) users assigned to this security class may use.

Step 12. In the Files to Include (Do Only These) field, enter any files to which you want to restrict queries. If you do not enter any files, users assigned to this security class will be able to query all files across all applications or all files within the allowed list of applications, depending on whether the user is restricted to certain applications.

Step 13. In the Files to Exclude (Never Do These) field, enter any files against which you do not want users assigned to this security class to be able to query.

Step 14. Do you want to allow Before and After commands for users with this security class?

Yes. Enter Yes in the Allow Before/After Commands field. Continue with Step 15.
No. Enter No in the Allow Before/After Commands field. Skip to Step 16

Step 15. In the Valid Commands for Before/After Processing, enter any commands users assigned to this security class can use before or after a query statement.

If you do not list any commands and Before/After commands are allowed, any valid command can be executed. Valid commands include UniData Verbs, Paragraphs, and Compiled programs.

Step 16. Finish from the SCQA form.

If you want to set up Query Builder security for additional security classes, repeat this procedure starting from Step 6.
Defining the Startup Sequence

In This Chapter

This chapter tells you how to set up the startup sequences in each database. Table 7-1 lists the topics in this chapter.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Before You Begin”</td>
<td>7-1</td>
</tr>
<tr>
<td>“Startup Sequence for a Colleague Session”</td>
<td>7-2</td>
</tr>
<tr>
<td>“Setting the Max Logon Attempts Allowed”</td>
<td>7-13</td>
</tr>
</tbody>
</table>

Table 7-1: Topics in This Chapter

Before You Begin

Before you define the startup sequence, you must install and set up UI. Refer to the following sections for information about installation and setup.

- “Installation” beginning on page 3-1.
- “Setup” beginning on page 4-1.

**ALERT!** The User Interface Response Map (UIRM) and Database Server Response Map (UIDR) forms described in this chapter allow you to view and modify startup sequences for UI. Accordingly, Datatel recommends that you strictly limit access to these forms. For the procedure, see “Limiting User Access to Features” on page 4-41.
Startup Sequence for a Colleague Session

When a Colleague user logs in to a Colleague environment through User Interface, a wIntegrate session is started on the user’s PC to communicate with the application server computer. This section addresses the startup sequence during that login. Table 7-2 lists the topics in this section.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Understanding the Startup Sequence for a Colleague Session”</td>
<td>7-2</td>
</tr>
<tr>
<td>“Procedure for Defining the Startup Sequence for a Colleague Session”</td>
<td>7-7</td>
</tr>
<tr>
<td>“Updating Local Installations With Changes to the Startup Sequence”</td>
<td>7-9</td>
</tr>
<tr>
<td>“Setting the Startup Directory (Windows Only)”</td>
<td>7-10</td>
</tr>
</tbody>
</table>

Table 7-2: Topics in This Section

Understanding the Startup Sequence for a Colleague Session

Depending on your institution’s setup, users may be able to choose which interface (Terminal or UI) to use when accessing a Colleague or Benefactor database. The desired sequence during operating system and database startup is typically different for these interfaces.

With the Terminal interface, user interaction is usually required. For example, the user might be prompted to select a database during the operating system portion of the startup, or to specify a printer during the database portion of the startup.

UI, on the other hand, is designed to start up with no further user interaction after the user enters a login, password, and database.

Using the User Interface Response Map (UIRM) form, shown in Figure 7-1 on page 7-4, you can set up the startup sequence for UI. In particular, you can define the following:

■ (UNIX operating system only) In the String/Response Map field, you can define appropriate responses to each command in the .profile file when the
user accesses the database with UI. For more information, see “Operating System Startup Sequence (UNIX Only)” beginning on page 7-4.

- In the User Interface Startup Paragraph field, you can create a startup paragraph that will run during database startup when the user accesses the database with UI. For more information, see “Database Startup Sequence” beginning on page 7-4.

Other fields on the UIRM form can be considered in two categories, as shown in Figure 7-1:

- Operating system prompts. During startup, UI receives messages and prompts from the operating system. Your entries in these fields enable UI to recognize these prompts.

- Script reload. These fields enable you to refresh the script to reflect your changes on the UIRM form, and to ensure that users will load the new script at their next login.

More information about these fields is provided in “Procedure for Defining the Startup Sequence for a Colleague Session” beginning on page 7-7.

The information you enter on the UIRM form is compiled into the record RESPMAP.WIS in the THINDEFS file. It is then loaded to each user’s workstation at the next login. The mapping information is encrypted to secure the trigger strings and responses.
Operating System Startup Sequence (UNIX Only)

Note: If you are using the Windows operating system, you can skip this section. The setup described here is not required for Windows.

The `.profile` file defines a user’s UNIX login parameters by specifying environment variables, aliases, and menus that offer user options for various applications. You can maintain an interactive `.profile` that presents users with a numerical-choice menu or other interactive event when they use the terminal interface. For instance, you may want a terminal window to be displayed upon login for those users whose passwords are about to expire. Doing so will introduce a complication for UI, however. You must map out in advance UI’s responses to any menus or change-of-password routines. This mapping is done in the String/Response Map field on the UIRM form.

The clearest way to demonstrate mapping responses is through examples. “Example Procedures for the Operating System Startup Sequence” beginning on page B-1 presents mapping responses for the situations that are most likely to arise.

Database Startup Sequence

During the database portion of the startup, the database LOGIN paragraph is executed. One of the commands in the LOGIN paragraph is ENVINIT (R17) or SQLENVINIT (R18). Any lines in the LOGIN paragraph that come after ENVINIT or SQLENVINIT are executed only for the terminal interface; they are not executed for UI. This allows you to include commands in the LOGIN paragraph that are executed for the terminal interface only (such as a prompt for a printer).

There may, however, be lines from your LOGIN paragraph you do not want to bypass. If so, you can restore interactive functionality to the UI login by defining a startup paragraph in the User Interface Startup Paragraph field on the UIRM form. This paragraph, if it exists, is run as part of the initialization logic that occurs when a user accesses the database using UI.
For example, suppose you wanted to execute a custom initialization program named XULINIT when users log in with UI. You would enter a paragraph name, such as UI_START, in the User Interface Startup Paragraph field on the UIRM form. Then you would detail to define the paragraph, as shown in Figure 7-2 on page 7-6.
Considerations for Strings and Prompts

On the UIRM form (Figure 7-1), the String/Response Map field and the "Operating system prompts" fields require that you enter a string that the operating system might send to UI during startup. The following are considerations for these fields:

■ Do not use strings that appear in more than one place during login, including custom dialogs and messages, because UI will react to the first occurrence of any string you map.1

■ Strings you map as triggers do not have to be the very last characters that UNIX displays before waiting for a response. For example, if your UNIX prompt were “Hello There>”, you could trigger on any unique subset of that string, such as “>” or “There” or “Hello.” However, if you do map a string that occurs before the prompt’s end, you need to be sure that the prompt will not be disrupted by a premature response from UI.

■ In the String/Response Map field, you will mostly enter strings as UI’s response; however, the following are special responses worth noting:
  • Response strings do not automatically end with a return. In order to have UI send a response followed by a return, you need to add \r to the end of the string.
  • In some cases, you may want UI to reply with Esc; in that case, enter \e in the Response field.
  • To change the environment to terminal emulation mode, enter TRM
  • To change the environment back to GUI mode, enter GUI
  • To issue commands, enter
    \=command

  where command is the literal command syntax. (You’ll need to know scripting language in order to use this option.) For example, you could enter something like

    \=MessageBox "Error",SB_OK

  which displays a dialog box with the message “Error” and waits for the user to click OK.

1. The exception to this rule is the Default UNIX Prompt map, because the various characters or strings mapped there may appear in several triggers, depending upon your situation.
Procedure for Defining the Startup Sequence for a Colleague Session

**Note:** Because anyone who has access to the UIRM form will be able to see UI's mapped response to hidden prompts, Datatel strongly recommends that you define the security for this form very narrowly. It would be best to make it part of a privileged security class used at your site.

Perform the following procedure in each database that your users will access using UI.

**Step 1.** Access the User Interface Response Map (UIRM) form.

**Step 2.** (UNIX only) In the String/Response Map field, enter the following for each string that you want to map:

a. On the first line, enter all or part of the string that UNIX will send to the operating system.

b. On the second line, enter the desired response for UI.

For instance, if in terminal mode UNIX displays a menu giving users numerical choices, you can map the menu’s prompt string (or part of it) and have UI respond with the numerical option that corresponds to the appropriate database. Thus, on the first of the UIRM form’s “String/Response” lines, you would enter the prompt from the menu, and on the second you would enter whatever number corresponds to the database that you are configuring.

For more discussion of this field, see “Considerations for Strings and Prompts” on page 7-6. For some examples, see “Example Procedures for the Operating System Startup Sequence” beginning on page B-1.

**Step 3.** In the Login Prompts field, enter a string that will signal a login prompt from the operating system.

You can enter several possible strings here, each on its own line, to cover multiple contingencies. The defaults are “Login” and “login.” When the operating system sends the string, UI will respond with the login that the user entered in the initial login box for UI.
Step 4. In the Password Prompts field, enter a string that will signal a password prompt from the operating system.

You can enter several possible strings here to cover multiple contingencies. The defaults are “Password” and “password.” When the operating system sends the password prompt, UI will respond with the password that the user entered in the initial login box for UI.

Step 5. In the Invalid Login Strings field, enter a string that will signal a login error message from the operating system.

Several defaults are provided; however, given the variability of operating system prompts, you may need to add a string for your platform.

Step 6. In the Change Password Strings field, enter a string that will signal a password expiration notice from the operating system.

When UI receives such a string, it will drop to a text window and allow the change-of-password procedure to execute. After the user has changed the password, UI resumes loading, and the text window closes.

Step 7. (UNIX Only) In the Default UNIX Prompts field, enter the characters that signal a UNIX prompt.

The defaults provided cover the most common prompt characters, such as $, >, %, and #. But if users have customized their prompts, you will need to collect and map them so that UI can react appropriately. An alternative would be to have each user with a custom string modify his DATATEL.INI record (located in the WINDOWS directory) by adding a unix_prompt entry in the “thinclient” section of DATATEL.INI.

Use caution when using custom prompts. For example, if your UNIX prompt is $Hello>, UI will become confused because there are actually two UNIX prompt characters present (the “$” and the “>”). Make sure that there is only one character present (changing the prompt to $Hello:).

Step 8. Do you want to specify a database login paragraph specifically for UI login?

   Yes. Continue with Step 9.

   No. Skip to Step 11.
Step 9. In the User Interface Startup Paragraph field, enter a name for the paragraph.

Step 10. Detail to write or edit the paragraph.

For more information, see “Database Startup Sequence” on page 7-4.

Step 11. In the Flag For Global Reload field, enter Yes if you want to update each user’s script the next time they log in.

You should select Yes only when you are certain the triggers and responses you have mapped are correct and work properly. Until you have thoroughly tested your UI response mapping, leave No (which is the default) in this field.

Step 12. In the Reload Current Session Immediately field, enter Yes if you want to update the script for the copy of UI you are currently using or pointing to.

Step 13. Save your changes on the UIRM form.

Step 14. Exit UI and restart it to test your changes.

Updating Local Installations With Changes to the Startup Sequence

If you make changes to the startup sequence as described above, you can use either of the following methods to apply those changes to a UI Desktop installation on a user’s PC.

Method A

Step 1. Delete the database folder on the user’s PC.

For example, a database with the name of collive would have a folder C:\Documents and Settings\<username>\Local Settings\Application Data\Datatel\Scripts\collive where <username> is the Windows login for the user.
Step 2. Delete and then re-add the database definition.

For the procedure, see “Adding Databases” beginning on page 9-6.

Method B

Step 1. Copy the resmap.wis file from the database folder in the administrative installation to the database folder on the user’s PC.

For example, copy to C:\Documents and Settings\<username>\Local Settings\Application Data\Datatel\Scripts\collive\ where <username> is the Windows login for the user.

Setting the Startup Directory (Windows Only)

Note: Perform this procedure only if your Envision, Colleague, or Benefactor databases are installed on a computer that uses the Windows operating system. If not, you can skip this section.

UniData Telnet allows you to specify a startup directory for all users. When users access the server via an emulation session, they go directly to the designated startup directory. If the startup directory is not the UniData demo account, users who attempt to access a Datatel account via UI will be forced to the startup directory even if they select a different database. For example, if the UniData telnet startup directory is C:\datatel\live\collive and the UI user selects a database that is “pointed” to C:\datatel\work\coltest, they will end up in the collive database (C:\datatel\live\collive).

To prevent this problem, use the following procedure:

Step 1. Start the UniData Admin program. (See Figure 7-3 on page 7-12.)
Step 2. In the left pane:

a. Double-click on the server name to expand it (agg in Figure 7-3).

b. If prompted, enter your login ID and password.

c. Double-click on the Configuration folder to expand it.

d. Double-click the UDTeInetServer icon.
   The Telnet Server window appears in the right pane.

Step 3. In the Telnet Server window, click the Users tab.

Step 4. Click on the DEFAULT user to select it.

Step 5. Click Edit to display the User Configuration window (Figure 7-3).

Step 6. Do either of the following:
   - In the Startup Directory box, enter the path to the UniData demo account.
   - Check the “Prompt Directory” box.

   If you check the “Prompt Directory” box, UI users will go to the database they selected when they logged in. Users who access via the terminal (character) interface are prompted to enter a valid UniData account directory.

Step 7. Click OK to return to the Telnet Server window.

Step 8. In the Telnet Server window, click Apply to save the changes.

Step 9. If there are other users besides DEFAULT, repeat Steps 4 through 8 for all listed users.
Figure 7-3: Setting the Startup Directory in the UniData Admin Program
Setting the Max Logon Attempts Allowed

If your clients are having difficulty logging into a UI session, make sure the connection is not being closed before password verification. The logon script contains several “Enter” commands, which are used to ensure that the logon prompt is available. These “Enter” commands might be interpreted as a failed logon by some operating systems. If the max logon attempts is reached prior to your user actually sending their password, the host will close the connection and the user will never be able to log on. Use the procedure below to increase the max logon attempts allowed.

Procedure for Setting the Max Login Retries Allowed

Use this procedure to set the maximum logon attempts allowed on the UniData Telnet server.

Step 1. Start the UniData Admin program. (See Figure 7-4 on page 7-14.)

Step 2. In the left pane:

a. Double-click on the server name to expand it (pjs in Figure 7-4).

b. If prompted, enter your login ID and password.

c. Double-click on the Configuration folder to expand it.

d. Double-click the UDTeleServer icon.
   The Telnet Server window appears in the right pane.

Step 3. Set the Max. Logon Attempts field to 5. You can set it higher if you want, but 5 is the minimum recommended.
Figure 7-4: Setting the Max Logon Attempts in the UniData Admin Program

Step 4. Click Apply to save the changes. Click OK to close the window.
In This Chapter

This chapter provides procedures for installing UI Desktop components to each user’s PC.

**Note:** Install only one instance of UI Desktop on each PC.

You do not need to install software for UI Web. UI Web is accessed from a Web server and does not need to be installed on client PCs. UI Web is accessed via a link to a Web page where the applet resides.

Before You Begin

Table 8-1 lists the tasks that must be complete before you can continue with the procedures in this chapter.

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the license file.</td>
<td>See “Installation” beginning on page 3-1.</td>
</tr>
<tr>
<td>Set up the UI administrative parameters.</td>
<td>See “Setup” beginning on page 4-1.</td>
</tr>
<tr>
<td>If desired, set up secure transmissions.</td>
<td>See “Security” beginning on page 5-1.</td>
</tr>
<tr>
<td>Define the startup sequence.</td>
<td>See “Defining the Startup Sequence” beginning on page 7-1.</td>
</tr>
</tbody>
</table>

**Table 8-1:** Tasks to Complete Before You Begin the Client Installation
Startup Sequence

If you have previously defined the startup sequence, you can have the UI Desktop InstallShield propagate those changes to the local copy during installation. The startup sequence is defined in the `respmap.wis` file. Copy this file from your administrative installation (for example, `C:\Documents and Settings\jsmith\Local Settings\Application Data\Datatel\Scripts`) to the location where you installed the license file.

If the startup sequence is the same for all environments, do not change the name of the file. If the startup sequence is different for each environment, rename the `respmap.wis` file to `<environmentname>.wis`. For example, for collive, rename the file to `collive.wis`.

If you make changes to the startup sequence after performing a local installation, you can still apply those changes to the user’s installation as described in “Updating Local Installations With Changes to the Startup Sequence” on page 7-9.

Secure Transmissions

The UI Desktop software installed on each user’s PC, using the procedures in this chapter, will initially use either secure or non-secure transmissions, depending on whether you have already set up security on the Colleague/Benefactor databases using the procedures in “Security” beginning on page 5-1.

- If you have set up security on the Colleague or Benefactor database before installing the user client software, then the initial communication from each user’s PC to that database will be secure.
- If you have not set up security on the Colleague/Benefactor database before installing the user client software, then the initial communication from each user’s PC will be non-secure. If desired, you can later set up security on the Colleague/Benefactor database. The next time a user attempts to access that database, they will be prompted to refresh their scripts. Subsequent communications between that user and that database will be secure.

You may, for security reasons, have configured your system so that your users have access only to secure telnet. If so, make sure that you set up security on the Colleague/Benefactor databases before installing the UI client software on users’ PCs. Otherwise, the first time the user attempts to access a database, UI will try (and be unable to) communicate with the database using non-secure telnet.
Use this procedure to install a local copy of UI Desktop on a user’s PC.

**Technical Tip:** If you did not install the `license.wil` file to a network drive, refer to AnswerNet document 5159 for instructions on copying the `license.wil` file to a CD for local installations.

**Step 1.** From the user’s PC, run the UI Desktop InstallShield. You can either download this from the Datatel Web site or run it from a saved location on a network drive. If you download it from the Datatel Web site, you will need a client login and password.

After launching the InstallShield, the Welcome window is displayed, as shown in Figure 8-1.

**Figure 8-1: Welcome Window**

**Step 2.** On the Welcome window, click **Next** to continue. The Installation Type window is displayed, as shown in Figure 8-2.
Step 3. Select **Standard**. Click **Next** to continue. The Destination Folder window is displayed, as shown in Figure 8-3.

Figure 8-3: Destination Folder Window
Step 4. If you want to change the installation location, click **Change...** and navigate to the directory where you want UI Desktop installed. Datatel recommends that you install UI Desktop in the default location. Click **Next** to continue. The License Folder window is displayed, as shown in Figure 8-4.

![License Folder Window](image)

**Figure 8-4: License Folder Window**

Step 5. Click **Change...** and navigate to the network path where the license file resides. This file was installed during the administrative installation (Step 9 on page 3-7). Click **Next** to continue. The Database Information window is displayed, as shown in Figure 8-5.
Step 6. Are you upgrading an existing UI Desktop installation?

Yes. Leave all fields on this window blank. The InstallShield will copy the databases defined in the existing datatel.ini file in the existing UI Desktop 1.5 installation. Settings for UI Desktop 2.1 remain in their location and are used by UI Desktop 2.2.

No. Enter the information about the host computer and database.

Step 7. Click Next to continue. The Ready to Install window is displayed, as shown in Figure 8-6.
Procedure for Installing UI Desktop a on User’s PC

Figure 8-6: Ready to Install Window

Step 8. Click Install to install UI Desktop. After a few minutes, the Successful Installation window is displayed, as shown in Figure 8-7.

Figure 8-7: Successful Installation Window

Step 9. Click Finish to exit the InstallShield.
Deploying the wIntegrate Applet Client for UI Web

Deploying UI Web entails providing users with a link to an HTML page that links to the applet. When a Web browser opens a Web page that contains an applet, the browser automatically downloads and starts the applet.

The wIntegrate applet that is deployed by UI Web is digitally signed to allow the applet access to the local file system of the workstation from where it is running. This allows UI Web users to import files and print to local printers. When users first open the UI Web page, they are prompted with a security dialog asking them if they want to trust IBM’s signed applet (see Figure 8-8).

Users can select one of the following:

- **Always.** Instruct users to select Always, so they will not see the security dialog again.
- **No.** Discourage users from selecting No, as this is sometimes difficult to reverse, and may prevent them from being able to run the applet from their browser.
- **Yes.** Selecting Yes causes the security warning dialog to be issued each time they open the page (until they select Always or No).
A sample index.html file is included on the UI Web InstallShield, which can be found in the wIntJava directory of your wIntegrate Server installation (for example: C:\Program Files\Datatel\UI Web\wIntJava\index.html). Index.html illustrates how a Java applet is embedded into a Web page using HTML tags.

The index.html example uses the <APPLET> tag, because it is used by most industry Web browsers across all major operating systems. However, there are many HTML tags that can also be used to embed the wIntegrate applet in your own Web page.

The following <APPLET> HTML tags are used in index.html:

```html
<APPLET CODE = "wintapplet/wIntApplet.class" WIDTH = "955" HEIGHT = "615">
  <PARAM NAME = CODE VALUE = "wintapplet/wIntApplet.class">
  <PARAM NAME = "archive" VALUE = "wIntJavaApplet.jar">
  <PARAM NAME = "type" VALUE = "application/x-java-applet;version=1.5.0">
  <PARAM NAME = "scriptable" VALUE = "false">
  <PARAM NAME = "server" VALUE = "UIWebServer.datatel.com">
  <PARAM NAME = "user" VALUE = "UIWeb">
  <PARAM NAME = "password" VALUE = ">
  <PARAM NAME = "autologin" VALUE = "yes">
  <PARAM NAME = "stylesheet" VALUE = "template.css">
</APPLET>
```

Include the following applet parameter tags to correctly embed the applet in your Web page:

**Server.** The server parameter is relative to your configuration.

- Use the address of the server running the port forwarding utility if you are using an external configuration (see Figure 1-1 on page 1-9).
- Use the UI Web Server address if you are deploying an internal configuration (see Figure 1-2 on page 1-10).

**User.** “UIWeb” is the template user ID used for automated login.
Password. "" (null) is the template password for the automated login.

Autologin. “Yes” avoids the wIntegrate server login dialog, which would prompt for User/Password/wIntegrate Server in addition to the UI login.

Stylesheet. template.css is the path to the style sheet containing the UI Web fonts and colors properties.

**ALERT!** Do not change User, Password, or Autologin. They are boilerplate parameters needed to bypass the wIntegrate Server’s login page. In bypassing the wIntegrate server login page the, users are prompted only with the Datatel UI Web login page.
In This Chapter

This chapter provides procedures for using User Interface (UI) to set up components on each user’s PC.

UI Desktop and UI Web allow administrators and users to administer databases and customize user fields in similar ways.

Because of the nature of the UI Web applet configuration, adding and removing users is handled differently. Because UI Web is not installed on users’ PCs, user access must be maintained from the UI Web User Access dialog. This ensures the integrity of the applet from unauthorized Web users.

To complete these procedures for UI Web, you must have a administrative installation of UI Desktop. See “Installing the Administrative Client” beginning on page 3-2 for more information.

Before You Begin

Before you set up individual users, do the following:

<table>
<thead>
<tr>
<th>UI Desktop</th>
<th>UI Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the administrative installation. See “Installing the Administrative Client” beginning on page 3-2.</td>
<td>Install the server software. See “Installing UI Web” beginning on page 3-10.</td>
</tr>
<tr>
<td>Set up the software. See “Setup” beginning on page 4-1.</td>
<td>Set up the software. See “Setup” beginning on page 4-1.</td>
</tr>
<tr>
<td>If desired, set up secure transmissions. See “Security” beginning on page 5-1.</td>
<td>If desired, set up secure transmissions. See “Security” beginning on page 5-1.</td>
</tr>
<tr>
<td>Define the startup sequence. See “Defining the Startup Sequence” beginning on page 7-1.</td>
<td>Define the startup sequence. See “Defining the Startup Sequence” beginning on page 7-1.</td>
</tr>
<tr>
<td>Install the client software. See “Client Deployment” beginning on page 8-1.</td>
<td></td>
</tr>
</tbody>
</table>

**Table 9-1:** Before You Set Up Clients
Setting Up the UI Web Exit URL

Database administrators can choose to direct users to a specific URL when they close their UI Web session. If a URL is not specified, the Web page that wraps the applet stays open though there is nothing else for the user to do on that page.

Procedure for setting up the UI Web Exit URL

You can define the UI Web Exit URL from either UI Desktop or UI Web. Before you can complete this procedure, you must meet the following conditions.

■ Correctly defined the location of the license folder installation on the UI Administration Parameters (UIPR) form. See “Setting Up the Administrative Parameters” beginning on page 4-6 for more information.
■ You must have a security class that allows you to administer UI options. See “Setting Up the Administrative Parameters” beginning on page 4-6 for more information.

Step 1. From the Options menu, select UI Web Exit URL.
   ■ If you are defining this parameter from UI Desktop, continue with step 2.
   ■ If you are defining this parameter from UI Web, skip to step 3.

Step 2. If necessary, define the location of your wIntegrate server.

Step 3. From the Configure Exit URL dialog box, enter the URL of the Web page you want to display when users close their UI Web session, then click OK.

Figure 9-1: Configure Exit URL Dialog
Adding and Removing UI Web Users

You can use the Add/Remove options in UI Web to allow or restrict user access to an account.

**Technical Tip:** When you add a new user to an account, the user’s information is placed in the *UIins.ini* and *Web_dbs.ini* files, which are located in the wIntegrate server application directory on the UI Web server (for example, `\UIWebServer\Public\Program Files\Datatel\UIWeb`). When a user attempts to log into UI Web, access is granted only if the ID is a valid one in the INI files.

The following procedures describe how to add and remove users.

**Procedure for Adding Users to a Database**

In UI Web, use the following procedure to add users to a database.

**Step 1.** Access the Windows server where the UI Web software is installed. Click on **Start**, then **Programs**, then **Datatel**, then **UI Web**, and finally **UI Web User Access**.

The UI Web User Access window is displayed, as shown in Figure 9-2.
Step 2. Click **Add** to display the Add User dialog box, as shown in Figure 9-3.

Step 3. Enter a login ID to assign to the new user, and click **OK**. The new user ID displays in the list of User Login IDs.

When you are finished entering users, click **Exit** to save your changes.

**Procedure for Removing User Access**

In UI Web, use the following procedure to remove users from a database.
Step 1. Access the Windows server where the UI Web software is installed. Click on Start, then Programs, then Datatel, then UI Web, and finally UI Web User Access. The UI Web User Access window is displayed, as shown in Figure 9-4.

![UI Web User Access Window](image)

Figure 9-4: UI Web Access Window

Step 2. In the list of user login IDs, select the ID of the user you want to remove.

Step 3. Click Remove and then click OK. The deleted user is no longer displayed in the list of user login IDs.

When you are finished removing users, click Exit to save your changes.
Adding Databases

You can add a database in any of the following ways:

■ The Options menu in UI Desktop.
■ The Options menu in UI Web.

While the functions performed are the same, the configuration of the dialog boxes is different, so separate procedures are provided in the following sections.

Procedure for Adding a Database in UI Desktop

Use this procedure if you are adding a database from the Options menu in UI Desktop.

Step 1. From the Options menu in UI Desktop, select Add/Remove Databases. The Add/Remove Databases window is displayed, as shown in Figure 9-5.

![Figure 9-5: Add/Remove Databases Window](image)

Click this button to add a database.

Step 2. Identify the databases (listed in the Available Databases field) that you want this user to be able to access through UI Desktop. Move each of those databases to the Installed Databases window by selecting the database and then clicking the single left arrow (<) button.

Step 3. Click OK to save your changes.
Procedure for Adding a Database in UI Web

You can use the UI Web User Access utility to grant or deny access to specific user IDs, or to all users who access the page. When a user links to an HTML page (which contains the UI Web applet), the UI Web login page is displayed. When the user enters a user ID, they see only the databases that you assigned to that ID. If you have not assigned databases to that user’s ID, then that user cannot see any databases.

You also have the option to maintain a default list of databases that are available for others (users who are not defined in the UI Web User Access list). You may, by default, grant access to certain databases to any user who links to the page. In this case you would add the desired databases to the Others user ID in the UI Web User Access utility.

You can additionally exclude access to all users who are not defined in the UI Web User Access list. In this case you would not have any databases associated with the Others ID.

Use the following procedure to add a database from the Options menu in UI Web.

**Note:** Within the list of available users is a user called “<others>,” which encompasses all other logins that are not defined. If databases are not removed from the “<others>” login, an invalid login could see a list of all installed databases (though they may not be able to successfully log in). To prevent this, make sure the “<others>” user does not have any assigned databases.

**Step 1.** From the Options menu in UI Web, select **UI Web User Access**. The UI Web User Access window is displayed, as shown in Figure 9-6.
Step 2. In the list of user login IDs, select a user login ID.

Step 3. Identify the databases (listed in the Available Databases field) that you want this user to be able to access through UI Web. Move each of those databases to the Installed Databases window by selecting the database and then clicking the single left arrow (<) button.

Step 4. Click Exit to save your changes.

Viewing a User’s Databases

To view information about the databases available from a user’s PC, access the User Interface Databases (UIDB) form in UI, as shown in the example in Figure 9-7.

This feature is available only from UI Desktop.
Figure 9-7: Example of the User Interface Databases (UIDB) Form

The UIDB form shows the database information stored in the user’s datatel.ini configuration file. You can create, edit, or delete database definitions from this form.

**Note:** This form is intended to be used for diagnostic purposes. If you want to change the databases available to a user, Datatel recommends that you use the Administer Databases menu option to edit the database information, and assign (or delete) the databases available to the user as described in “Adding Databases” beginning on page 9-6.

**ALERT!** Because the UIDB form allows the user to view and modify database information, we recommend that you apply very restrictive security to this form. For the procedure, see “Limiting User Access to Features” on page 4-41.
Customizing User Fields

Use the User Field Customization (UIFC) form to override the default behavior for fields on a UI form. You can override the controls for tab sequencing, required fields, and field access.

- **Tab Sequencing.** Use the First Field, Next Field Override, and Last fields to specify tab sequencing.

- **First Field.** Identify which field the cursor appears in when a user first accesses the form, and the path followed through the form each time a user presses the Tab key.

- **Required Fields.** Indicate which fields on the form are required. If a field is already specified as required by the Envision Tool Kit, it is always required. However, fields that are not specified as required fields in the Toolkit can additionally be designated as required here.

- **Field Access.** Indicate if a field is Inquiry Only (the user can see the field, but cannot enter information) or No Access (the field is not visible to the user). Leaving this field blank allows the user to enter information.

**Note:** Before you can customize fields for a form, you must first set up your preferences for field customization using the UI Usage Parameters (UIPM) and Security Definition (SCD) forms. See “Procedure for Enabling Field Customizations For All Users” on page 4-30 for more information.

Keep in mind that the behavior for each field on each form is initially defined in the Envision Tool Kit. Using the UIFC form, you cannot take away behavior that is defined in the Tool Kit. For example, if a field is set in the Toolkit as Required, it is always required. The same reasoning applies to the Field Access feature. If a field is set in the Tool Kit as Required, you cannot set that same field in UIFC to Inquiry Only or No Access on the UIFC form.

You can also specify field behavior for a form from within the form itself. Selecting Customize Field Properties from the Tools menu of the form you want to customize provides similar capabilities as those offered here.

**Note:** If you are customizing a form that has not yet been generated with the version of the generators that was released in June 2003 or later, you must regenerate that form before you can restrict field access or designate a required field.
Customizing Tab Sequencing

Customizing your tab sequence can optimize the speed with which you move through a form. You can specify which fields you need to enter data into, and in which order. Each time you press the Tab key, you move to the next field in the specified tab sequence. When you leave the last field in your customized tab sequence, the form updates the record.

Note: You may not have access to all of the options provided in this procedure, depending on the level of access granted to you from the UIPM and SCD forms. This procedure describes the process as if you have access to all of the customization options.

Procedure For Customizing Tab Sequencing

Step 1. In the UT application, access the User Field Customization (UIFC) form.
**Step 2.** At the Enter Process Mnemonic to Customize prompt, enter the mnemonic of the form you want to customize, and click **OK**.

**Step 3.** At the Operator ID LookUp, enter the login ID of the user you want to specify customizations for.

To specify customizations for all users, do not enter a specific login ID at the prompt.

**Step 4.** In the First Field field, enter the name of the first field in the tab sequence.

If you leave this field blank, the first field on the form remains the first field in the tab sequence.

**Step 5.** In the list of Process Fields, find the name of the field that you designated to be the first field.

In the Next Field Override for that field, enter the name of the next field in the tab sequence.

**Step 6.** In the list of Process Fields, find the name of the field that you designated to be the next field in the tab sequence.

In the Next Field Override for that field, enter the name of the next field in the tab sequence.

**Step 7.** Repeat Step 6 for each field in the tab sequence.

**Step 8.** In the list of Process Fields, find the name of the desired last field in the tab sequence. In the Last field for that field, enter **Yes**.

**Step 9.** Finish out of the UIFC form.
Customizing Required Fields

You can specify whether you want a field on a form to be required. The user cannot finish from the form without entering data into the required fields. If a field is already specified as required by the Envision ToolKit, it is always required. However, fields that are not specified as required fields in the ToolKit can be overridden here. By the same logic, if a field is defined as inquiry-only or no access, you cannot set that field to Required (if users cannot access a field, you cannot require them to populate it).

Note: You may not have access to all of the options provided in this procedure, depending on the level of access granted to you from the UIPM and SCD forms. This procedure describes the process as if you have access to all of the customization options.

Procedure for Customizing Required Fields

Step 1. In the UT application, access the User Field Customization (UIFC) form.

Step 2. At the Enter Process Mnemonic to Customize prompt, enter the mnemonic of the form you want to customize.

Step 3. At the Operator ID LookUp, enter the login ID of the user you wish to specify customizations for. Or, press the Enter key to specify customizations for all users.

Step 4. In the list of Process Fields, find the name of the field that you want to be required. In the Req field for that field, enter Yes.

Step 5. Repeat step 4 for each field that you want to designate as required.

Step 6. Finish out of the UIFC form.
Customizing Field Access

Use the Field Access field to select a security control override for the corresponding field. If this field is left empty, the default UI form behavior occurs.

You can select one of the following options:

- **Inquiry Only.** Users may only view the data; they cannot update or delete data.
- **No access.** User cannot view, add, change, or delete data. If a field is already specified as Denied Access through security classes as defined on the Field Security Definition (SCD) form, it is always Denied Access (Denied Access performs the same functionality as No Access).

If a field is already specified as Inquiry Only through security classes, it is always at least Inquiry Only. However, you can designate the field No Access because it is more restrictive. Overrides can be used to provide more restrictive access, but they cannot be used to provide less restrictive access.

By the same logic, if a field is defined as required, you cannot set that field to inquiry-only or no access (if users are required to populate a field, you cannot deny them access to it).

*Note:* You may not have access to all of the options provided in this procedure, depending on the level of access granted to you from the UIPM and SCD forms. This procedure describes the process as if you have access to all of the customization options.

**Procedure for Customizing Field Access**

**Step 1.** In the UT application, access the User Field Customization (UIFC) form.

**Step 2.** At the Enter Process Mnemonic to Customize prompt, enter the mnemonic of the form you want to customize.

**Step 3.** At the Operator ID LookUp, enter the login ID of the user you want to specify customizations for. Or, press the Enter key to specify customizations for all users.
Step 4. In the list of Process Fields, find the name of the field for which you want to customize field access. In the corresponding Field Access field, select Inquiry Only or No Access.

Step 5. Repeat Step 4 for each Field Access customization.

Step 6. Finish from the UIFC form.
Using the Browser-Based Help System

**Note:** This section provides information about setting up the Colleague Release 18.0 browser-based help system. This browser-based help system is not available for Colleague Release 17.0.

You can use the help servlet, included with WebAdvisor 3.x, to display help for UI users. You will benefit from being able to view help using the help servlet because it is displayed in a browser window and supports typical browser functions (searching, printing, changing the font size, etc.). Figure 9-9 shows an example of the process help for the Operator Definition (SOD) form displayed in both online help and the help system.

![Figure 9-9: Help Displayed by the Help System vs. UI](image)

**Help for the UTOPRS (SOD) Form**

- **Overview**
  - Use the Operator Definition (SOD) screen to define operator records for all individuals who are allowed access to Envision-based applications.
  - You may define operator records from within any application in the hierarchy; however, we strongly recommend that you define all operator records at the UT level makes it easier for you to keep track of your operator definitions and reduces the likelihood of users having problems accessing certain applications.

- **Field Descriptions**
  - Application
  - User ID
  - How do I...

---

**Figure 9-9:** Help Displayed by the Help System vs. UI
A Tip about Web Browsers

When the browser-based help system is enabled and a user requests help, UI sends a browser event to the default browser defined on your user’s system. The resulting window is automatically resized, a behavior that your users may not be expecting.

Web browsers’ default configuration is usually set to reuse existing browser windows for events sent from other applications. To prevent this, instruct your users to set their browsers to create a new window for incoming events.

Use the following instructions as a guide on how to set up the three supported Web browsers. Consult your Web browser documentation for the latest documentation.

Microsoft Internet Explorer

For Microsoft Internet Explorer, choose the Tools menu, then Internet Options, and then the Advanced tab. Clear the Reuse windows for launching shortcuts checkbox.

![Internet Explorer Options](image)

**Figure 9-10:** Internet Explorer Options
Mozilla Firefox

For Mozilla Firefox, choose the Tools menu, then Options, and then click on the Tabs tab. In the “Open links from other applications” group, choose a new window.

![Firefox Options](image)

**Figure 9-11:** Firefox Options
Apple’s Safari

For Apple’s Safari, choose the Safari menu, then Preferences, and then click on the General tab, if not already selected. For the “Open links from applications” group, select in a new window.

![Figure 9-12: Safari Preferences](image-url)
Uninstalling UI

In This Chapter

This chapter contains information on how to uninstall UI Desktop. Table 10-1 lists the topics in this chapter.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Uninstalling UI Desktop 2.x”</td>
<td>10-2</td>
</tr>
<tr>
<td>“Uninstalling UI Desktop 1.5”</td>
<td>10-3</td>
</tr>
<tr>
<td>“Uninstalling UI Web”</td>
<td>10-6</td>
</tr>
</tbody>
</table>

Table 10-1: Topics in this Chapter
Uninstalling UI Desktop 2.x

Uninstalling UI Desktop 2.x from a user’s PC is much simpler than UI Desktop 1.5.

Procedure to Uninstall UI Desktop 2.x

Use this procedure to uninstall UI Desktop 2.x.

**Step 1.** From the user’s PC, use the Add or Remove Programs function to remove UI Desktop 2.x.

**Step 2.** Delete the cached scripts folder for any user that logged onto the PC. The cached scripts folder is located in the *Local Settings* folder. For example, 

`C:Documents and Settings\jsmith\Local Settings\Application Data\Datatel`

is the location of the cached scripts folder for a user named jsmith.

**Technical Tip:** The Windows Add or Remove Program functionality does not remove this folder because it is created after UI Desktop is installed. In other words, the installer has no knowledge of this directory.
Uninstalling UI Desktop 1.5

This section contains information on how to uninstall UI Desktop 1.5. Do not remove UI Desktop 1.5 before installing UI Desktop 2.2 unless you do not want the UI Desktop 2.2 InstallShield to copy forward the defined list of databases.

Creating the Unregister Batch File

Use the following procedure to create the unregister batch file. You will use this file later to unregister components in the Windows registry.

**Step 1.** In a text editor, enter the text shown in Figure 10-1. Note that the text beginning with “WCHECK” and ending with “WINTCOMP.OCX” should be typed as a single line.

If you are viewing this manual online, you can copy the text using the Text Select Tool in Adobe Acrobat, and then paste it into the text editor.

```
ECHO OFF
CLS
WCHECK -UNREGSERVER "DATATEL.EXE" "WSESSION.OCX" "WINTEGSM.EXE" "WSTATBAR.OCX" "WSERIAL.OCX" "WWINSOCK.OCX" "WGRID.OCX" "WINTCONV.DLL" "WINTLAY.DLL" "WDIVIDER.DLL" "WINTCALC.OCX" "WINTCOMP.OCX"
```

**Figure 10-1:** Text for the Unregister Batch File

**Step 2.** Save the file as a batch file (with a “bat” extension), in the folder where you installed the UI master client software.

For example, save the file as unregister.bat.

The folder is the one specified during the installation of UI Desktop or UI Web. This is the folder where the wCheck.exe file is installed.
Uninstalling UI Desktop from a User’s PC

To uninstall UI Desktop from a user’s PC, you must first unregister the registered components, and then delete folders and files. Use the appropriate procedure below for the type of install (full local or shared) on the user’s PC.

**ALERT!** The UI InstallShield installs an executable program called *wCheck.exe*, which is invoked by the unregister batch program in the following procedure. Do *not* run *wCheck.exe* directly. Doing so can damage the Windows registry.

### Uninstalling a Full Local Installation

**Step 1.** Copy the unregister batch file to the folder on the user’s PC where you installed UI Desktop.

The unregister batch file is the file you created using the procedure on page 10-3. This is the folder where the *wCheck.exe* file is installed.

**Step 2.** From the user’s PC, run the unregister batch file program.

**Step 3.** Delete the folders and files under the folder where UI Desktop is installed.

**Step 4.** Delete the Cache folder, and all folders and files in that folder, under `C:\Datatel\Thingui`.

Forms that the user accessed through UI Desktop are cached under the Cache folder. If you later decide to reinstall UI on this PC, the Cache folder will be automatically recreated when the user first uses the interface.

**Step 5.** Delete the Datatel icons from the desktop and Start menu.

### Uninstalling a Shared Installation

**Step 1.** From the user’s PC, run the unregister batch file program.
Uninstalling UI Desktop 1.5

The program is on the network drive, in the location that you specified in Step 2 on page 10-3.

**Step 2.** Delete the Cache folder, and all folders and files in that folder, under C:\Datatel\Thingui.

Forms that the user accessed through UI are cached under the Cache folder. If you later decide to reinstall UI Desktop on this PC, the Cache folder will be automatically recreated when the user first uses the interface.

**Step 3.** Delete the Datatel icons from the desktop and Start menu.

### Uninstalling the UI Desktop Master Client Software

**ALERT!** The UI InstallShield installs an executable program called wCheck.exe, which is invoked by the unregister batch program in the following procedure. Do not run wCheck.exe directly. Doing so can damage the Windows registry.

**Note:** If any of your users have shared installs, you must uninstall from those users’ PCs before uninstalling the master client software from the network drive. Otherwise, you will not have access to the unregister batch file and wCheck.exe when you uninstall from those users’ PCs.

Perform the following procedure from the installation workstation.

**Step 1.** Run the unregister batch file program.

The program is in the location you specified in Step 2 on page 10-3. This could be on a network drive or the hard drive of the installation workstation, depending on where you installed UI.

**Step 2.** Delete the folders and files under the folder where UI Desktop is installed.

The folder is the one you specified during the installation of UI Desktop. Again, this could be on either a network drive or the hard drive of the installation workstation.
Uninstalling UI Web

Use this procedure to uninstall UI Web.

**Step 1.** From the Start menu, select Programs, then Datatel, then UI Web, and finally Service Control Program. The wIntegrate Server Service Control Program starts, as shown in Figure 10-2.

![Figure 10-2: wIntegrate Server Service Control Program](image-url)

**Step 2.** Click Stop to stop the wIntegrate server.

**Step 3.** Click Close to exit the wIntegrate Server Service Control Program.

**Step 4.** From the Start menu, select Programs, then Datatel, then UI Web, and finally Uninstall to uninstall the wIntegrate server.

**Step 5.** Remove the UI Web files from the Web Server.
User Interface Installation and Administration

Appendixes
Integrating Your Existing Practices

In This Appendix

This appendix provides guidelines for integrating your existing practices and your custom software into UI.

Colon Prompt Access

User Interface supports access to a colon prompt similar to UniData’s colon prompt via the SHEL mnemonic. SHEL supports most UniData dot commands, but not all of them. Enter .? at the SHEL prompt to see a list of supported dot commands. Note that SHEL does not remember your previous commands after you exit SHEL and return to the graphical interface.

**Technical Tip:** If you want to prevent some or all users from accessing the colon prompt, restrict the access to the SHEL mnemonic. For the procedure, see “Limiting User Access to Features” on page 4-41.

As an alternative, system administrators can enable the creation of a Datatel Terminal icon. For the procedure, see “Setting Up the Administrative Parameters” beginning on page 4-6. If you enable this option, then when you do a user installation the user will get a “Datatel Terminal” icon on their Start menu that allows them to start a terminal session, which they can use to access the colon prompt.

As an alternative to the colon prompt, consider migrating your queries to Envision, by building Envision forms for them and putting them on the menu. This would allow you to take advantage of the report browser, and positions you to automatically take advantage of new Envision features that get added down the road—your own custom software is able to evolve as Envision evolves. Your goal moving forward should be to eliminate any and all need for colon prompt access.

**Note:** Colon prompt access is not available for Release 18.0.
Custom Forms

If you have developed forms using standard Envision procedures, these will readily convert to the UI. However, because UI has to alter the geometry of the forms when they are painted in a graphical format, the appearance of the form may not meet your expectations. On some of your custom forms you may want to move the text for some of the fields, adjust the field labels and then re-generate the forms in UI.

Custom Report Browser

If you have created a custom report browser, you may find that it does not work in UI. In this situation, consider using one of the following alternatives:

■ Whenever possible, rework your custom program to use standard Envision techniques, so that it can use Envision’s standard peripheral defaults form at run-time. Envision then correctly directs output to the report browser.
■ If this is not an option, after directing your output to the HOLD file, invoke the report browser by calling S.EXECUTE as follows:

```
CALL S.EXECUTE("UTBROWSE <record name> _HOLD_")
```

This solution, while not encouraged, will cause the report browser to come up and allow the user to browse the report and print it if desired.

Using the Report Browser With Query Paragraphs

If you have custom query paragraphs, you can rework them to use the graphical report browser if desired. To do this, modify your custom paragraph as follows:

**Step 1.** Use a SETPTR command to redirect output to the HOLD file. Make sure the query statement uses the LPTR command to send output to the printer.

**Step 2.** After the query statement, add a statement for UTBROWSE, such as:

```
UTBROWSE <record name> _HOLD_
```

This will open the report browser displaying the results of the query.
Example Procedures for the Operating System Startup Sequence

In This Appendix

This appendix provides example procedures for defining how UI responds to operating system startup prompts.

Examples

The following example procedures for mapping UI’s response to an interactive .profile cover the situations most likely to arise.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>How to map UI’s response to access a database upon login.</td>
<td>“Example A: Mapping the UIRM Form to Access the Appropriate Database from a Login Menu” beginning on page B-2</td>
</tr>
<tr>
<td>How to map UI’s response to password expiration.</td>
<td>“Example B: Mapping UIRM to React to Password Expiration” beginning on page B-3</td>
</tr>
<tr>
<td>How to map UI’s response to bypass a login menu.</td>
<td>“Example C: Mapping the UIRM Form to Bypass a Login Menu” beginning on page B-5</td>
</tr>
</tbody>
</table>

Table B-1: Examples in this Appendix

Other situations may arise, but these examples should provide enough information to extrapolate a workable solution to any of them.

Note: These example procedures are written for the case where each user has an individual .profile in UNIX. If you use global .profiles that are used by more than one person, these procedures can still be used. However, be aware that your changes will affect all people who are using that .profile.
Example A: Mapping the UIRM Form to Access the Appropriate Database from a Login Menu

Note: This procedure applies only if you are using the UNIX operating system.

The object of this procedure is to enable UI to respond to a menu invoked by users’ .profile files and access the appropriate database. The following instructions assume the most likely scenario for using this feature, that is, that the .profile file is already set up and you need to adapt UI to its requirements. This example assumes that you are using UNIX scripts to give users the following menu:

1. Colleague live
2. Colleague test
3. Colleague development
4. Logout

Enter Selection --->>>

Note: Perform this procedure in the main remote account.

Step 1. If you use a UNIX menu script for your own login, comment out the menu in your .profile so that your login goes directly to the UNIX prompt.

Step 2. Using User Interface, access the database for which you want to define the startup sequence.

Step 3. In the UT application, access the User Interface Response Map (UIRM) form.

Step 4. In the String/Response Map field, enter Enter Selection --->>> in the first field, and the number corresponding to the appropriate account in the second field.

For example, when setting up the live account in the above example, you would enter 1\r in the second field, indicating that User Interface should transmit a “1” followed by a carriage return in response to the “Enter Selection --->>>” menu prompt.
Step 5. Enter **Yes** in the Reload Current Session Immediately field to load the new response mapping to your PC.

Step 6. Re-enable your UNIX menu script.

Step 7. Verify that you can access UI for the appropriate database with the UNIX menu script activated for your login.

Step 8. Copy the *resmap.wis* file to any other UI Desktop installation. Copy the file to the same directory path as your current installation, with the difference being the username. For example, `C:\Documents and Settings\jsmith\Local Settings\Application Data\Datatel\Scripts` for the same startup sequence for all environments or `C:\Documents and Settings\jsmith\Local Settings\Application Data\Datatel\Scripts\collive` for a specific environment (in this instance, collive).

**Example B: Mapping UIRM to React to Password Expiration**

The following procedure assumes you _have not_ performed the steps outlined in Examples A or C. If, however, you have already performed either procedure, you need to be careful not to overwrite any trigger/response pairs previously mapped. The safest way to proceed is to select or set up the same test user for all procedures.

Step 1. Select or set up a test user.

Step 2. As the test user, access the database.

Step 3. In the UT application, access the User Interface Response Map (UIRM) form.

Step 4. In the Change Password Strings field, enter the trigger string sent by the password expiration warning.
For instance, suppose that the warning ends with the prompt “Change Password Now? (Y/N)”; that is the string the Application Server sends to the workstation, so it is the trigger. You could therefore enter:

```
  Change Password Now? Y/N
```

(or any unique subset of that string) in the Change Password Strings field. You can enter several strings if your system issues a variety of prompts for password expiration (such as a series of successive warnings), but be sure to enter each string on its own separate line.

UI pauses while the change-of-password procedure runs.

Step 5. In order to test your changes on just the test user’s copy of UI, enter Y in the box labeled “Reload Current Session Immediately.”

This will cause the copy of UI to which you point to automatically reload your changes on exit from this form. If you are using a shared copy of UI, be aware that your changes will impact everyone who uses that copy.

Step 6. Exit UI.

Step 7. Arrange for your test user’s password to expire.

Step 8. Restart the test user’s copy of UI.

UI pauses while the change-of-password procedure runs.

Step 9. Return to the UIRM form and enter Y in the box labeled Flag for Global Reload.

Step 10. Save your work, exit the form, and close UI.

The next time each copy of UI is started, it will automatically reload your trigger/response map. (This will also apply to all subsequently installed copies.)
Example C: Mapping the UIRM Form to Bypass a Login Menu

**Note:** This procedure applies only if you are using the UNIX operating system.

The object of this procedure is to enable UI to bypass a login menu invoked by users’ .profile files and continue loading. The following instructions assume the most likely scenario for using this feature, that is, that the .profile file is already set up and you need to adapt UI to its requirements. The general strategy of this procedure will be to add a hidden option—one that users will never see—to the menu and map the response in the UIRM form. Follow the steps below.

**Note:** Perform this procedure in the main remote account.

**Step 1.** If you have not already done so, edit your own .profile by commenting out the menu.

You will be able to load UI and access the UIRM form.

**Step 2.** Select or create a test user. In the test user’s .profile, comment out the menu.

You will be able to load UI on the test user’s workstation.

**Step 3.** As the test user, access the database.

**Step 4.** In the UT application, access the User Interface Response Map (UIRM) form.

**Step 5.** In a separate session, log in as yourself and access the test user’s .profile. Remove the comment characters from the menu. Then add a non-displaying menu option to the “case” portion of the menu definition.

This step makes it possible for UI on the test user’s workstation to bypass the menu.
This *hidden* menu choice should be very elaborate, because you don’t want users to enter it accidentally. For example, you could define the choice as “28646918” or some other long and complex number that users are not likely to enter. Define this option so that choosing it causes an exit to UNIX. (Once again: It is important that this option *does not get displayed*, because you don’t want users who log into the system in character mode to access the UNIX prompt!)

**Step 6.** Return to the test user’s UIRM form. In the paired fields labeled String/Response Map, enter (a) the trigger string sent by the Application Server to the workstation; and (b) the response that the workstation must send back.

The triggers that the Application server sends to UI will match the responses UI must send back in order for the load to proceed.

For instance, suppose that the menu invoked by .profile ends with the prompt “Enter Menu Choice: >”. That is the string the Application Server actually sends to the workstation, so it is the *trigger* to which UI must respond. You could therefore enter *Choice: >* in the first of the paired lines. For a Response, let’s stay with the example above and suppose that the menu option for loading UI will be “28646918.” (Remember, this will be a *hidden* menu choice; it should be very elaborate, because you don’t want users to enter it accidentally.) You would therefore enter `28646918\r` on the second of the paired lines. (If a return were not required, you would enter `28646918`.)

It is possible that you have different menus for different users on your system. It would be simplest to make all menus end with the same prompt and designate UI as the same numerical option in each menu. If that’s not possible, you can map several trigger/response pairs in the UIRM form, but you will need to make sure that you map a unique string for each prompt.

**Note:** The UIRM form’s default UNIX Prompt characters are $, >, %, and #. You can include others by adding extra lines to the Default UNIX Prompts group.

**Step 7.** Return to the test user’s UI session. In order to test your changes on just the test user’s copy of UI, enter *Y* in the box labeled “Reload Current Session Immediately.”

This will cause the test user’s copy of UI to automatically reload your changes on exit from this form. If you are using a shared copy of UI, be aware that your changes will impact everyone who uses that copy.

**Step 8.** Exit the test user’s UI session.
Step 9. Restart the test user’s copy of UI.

Confirm that UI bypasses the menu and is loaded.

Step 10. Return to the test user’s UIRM form and enter \texttt{Y} in the box labeled Flag for Global Reload.

Step 11. Save your work, exit the form, and close UI.

The next time each copy of UI is started, it will automatically reload your trigger/response map. (This will also apply to all subsequently installed copies.)

Step 12. Return to your own session and edit the .profile files for every user who will be using UI, adding the hidden UI option, just as you did for the test user in Step 4.

This step causes all users’ copies of UI to bypass the menu.

You may want to test a few more copies of UI before going on to the next step.

Step 13. Access your own .profile and reestablish the login menu, which you commented out earlier. Add the hidden UI option to the menu, if you have not done so already. Save your work and exit.
Index

A
Add/remove databases 4-7
Administer databases 4-8
Administrative installation
administrative menu options
  enabling 4-10
  understanding 4-6
  enabling the multi-line text editor 4-15
FTP transfers 4-20
  considerations 4-21
  setting up 4-22
  installing 3-2
  limiting user access to features 4-41
Administrative menu options
  enabling 4-10
  global access 4-10
  understanding 4-6

C
Certificates
  installing 5-16
  viewing 5-32
Colon prompt access A-1
Custom forms A-2
Custom report browser A-2

E
Exit button, enabling 4-18

F
Features, limiting user access to 4-41

Forms
  custom A-2
  Operator Definition (SOD) 4-36
  Query Builder Computed Column (QBCC) 6-7
  Sec Class QueryBuilder Access (SCQA) 6-5
  Security Class Definition (SCD) 4-6
  UI Administration Parameters (UIPR) 4-6, 6-4
  UI Certificate Inquiry (UICI) 5-32
  UI Certificate Request (UICR) 5-8, 5-16
  UI Security Context Record (USCR) 5-13
  UI Usage Parameters (UIPM) 4-36
  User Interface Databases (UIDB) 9-8
  User Interface Response Map (UIRM) 7-2

FTP transfers
  considerations 4-21
  setting up 4-22

G
Global access 4-10

H
Hardware requirements 2-1

I
Installation overview
  components installed 1-5

M
Master client. see Administrative installation
Multi-line text editor, enabling 4-15

O
Operating system startup sequence
  defined 7-4
  examples B-1 to B-7
Operator Definition (SOD) form 4-36

P
Preparing for User Interface
  hardware and software requirements 2-1
  Private key, defined 5-2
Procedures
adding a database
  options menu 9-6, 9-7
creating a security context record 5-14, 5-29
creating the unregister batch file 10-3
defining the startup sequence 7-7
enabling a secure connection 4-25
enabling the administrative menu options 4-10
global access 4-10
enabling the multi-line text editor 4-17
installing a certificate 5-16
setting the startup directory 7-10
setting up FTP transfers 4-22
uninstalling a full local install 10-4
uninstalling a shared install 10-4
uninstalling the master client software 10-5
updating local installs with changes to the startup sequence 7-9
using the report browser with query paragraphs
  A-2
viewing certificates 5-33
Public key, defined 5-2

Q
QBCC form 6-7
Query Builder Computed Column (QBCC) form 6-7
Query paragraphs, using the report browser with
  A-2

R
Report browser
  custom A-2
  query paragraphs and A-2

S
SCD form 4-6
SCQA form 6-5
Screens. see Forms
Sec Class QueryBuilder Access (SCQA) form 6-5
Security
  installing a certificate 5-16
  private key, defined 5-2
  public key, defined 5-2
  setting up 5-3
  understanding 5-2
  viewing certificates 5-32
Security Class Definition (SCD) form 4-6
SHEL A-1
SOD form 4-36
Software requirements 2-1
Startup sequence
  database 7-4
  defining 7-7
  operating system (UNIX) 7-4
  prompts 7-6
  setting the startup directory 7-10
  strings 7-6
  understanding 7-2
  updating local installs with changes 7-9

U
UI Administration Parameters (UIPR) form 4-6, 6-4
UI Certificate Inquiry (UICI) form 5-32
UI Certificate Request (UICR) form 5-8, 5-16
UI Security Context Record (USCR) form 5-13
UI Usage Parameters (UIPM) form 4-36
UI Web
  installing 3-10
  UICI form 5-32
  UICR form 5-8, 5-16
  UIDB form 9-8
  UIPM form 4-36
  UIPR form 4-6, 6-4
  UIRM form 7-2
Uninstalling User Interface
  creating the unregister batch file 10-3
  master client 10-5
  users
    full local install 10-4
    shared install 10-4
Unregister batch file, creating 10-3
USCR form 5-13
User installation and setup
  adding a database
    options menu 9-6, 9-7
    viewing a user’s databases 9-8
User Interface Databases (UIDB) form 9-8
User Interface Response Map (UIRM) form 7-2