Johnson Controls

P2000

Security Management System

Web Access Manual

Version 3.11 and higher, September, 2011
24-10618-163 Revision –

P2000

Security Management System

Web Access Manual

Version 3.11 and higher, September, 2011

24-10618-163 Revision –

Johnson Controls
Security Solutions
(805) 522-5555
www.johnsoncontrols.com

Acknowledgment

TABLE OF CONTENTS

Chapter 1: Introduction

Chapter 2: Web Badging Configuration

Chapter 3: Using Web Access

Chapter 4: System Administration

Index

INTRODUCTION

P2000 Web Access is a suite of applications that enables users to perform various P2000 tasks from any Web-ready computer, tablet, or compatible Personal Digital Assistant (PDA) device. Using Web Access has many advantages, such as its flexibility. Operators were previously required to edit most P2000 data directly on site using P2000 servers and workstations. Users can now submit P2000 requests via the Web using a remote computer, saving the customer costs on equipment and personnel. Essentially, the Web Access interface offers a simple, flexible alternative to working on a P2000 workstation.

Web Access offers many features such as employee, visitor, and contractor management applications; badge activity tracking and synchronization; alarm monitoring; emergency access disable; Web badging capabilities; and a customizable user interface. For more information, see "Web Access Features" on page 1-2.

Web Access also supports different permission levels for each user, and requests can be approved and validated prior to being implemented, helping to prevent unauthorized operations or changes to the P2000 system. When a user submits a request, the P2000 system sends it to the request queue for processing. Administrators can establish rules to determine how the request is submitted. For example, if a request requires approval, a pre-defined approver must approve or reject the request. If validation is also required, a user with the proper permissions must confirm the validity of the request before it can be fully processed.

NOTE

The screen captures shown in this manual may differ slightly, depending on the software version you are using.

CHAPTER SUMMARIES

- ***Chapter 1: Introduction*** describes the purpose of this document, manual conventions, software requirements, recommended computer display settings, logging instructions, and the sequence of steps for deploying, configuring and using Web Access.
- ***Chapter 2: Web Badging Configuration*** covers the steps necessary to configure a Web Access client computer as a Web Badging station.
- ***Chapter 3: Using Web Access*** provides operator instructions for using the Web Access interface, including descriptions of the application features.

- ***Chapter 4: System Administration*** covers system deployment and customization of the Web Access application.

MANUAL CONVENTIONS

The following items are used throughout this manual to indicate special circumstances, exceptions, important points regarding the equipment or personal safety, or to emphasize a particular point.

NOTE

Notes indicate important points or exceptions to the information provided in the main text.

IMPORTANT

Important messages remind you that certain actions, if not performed exactly as stated, may cause damage to equipment or make your system non-operational.

WEB ACCESS FEATURES

- **Employee Management**
  Manage P2000 employee data via the Web. Add, edit or delete cardholder records, badges, and journals. Badges can also be re-synchronized if out-of-sync.
- **Visitor Requests**
  Make visitor badge requests, so badges are ready when visitors arrive at the building.
- **Web Badging**
  Use the Web Access computer as a badging station for capturing cardholder images (portraits and signatures), and encoding and printing cardholder badges. For more information, see “Chapter 2: Web Badging Configuration”.
- **User Permissions**
  P2000 administrators can assign Web Access users to permission groups, which keep unauthorized users from performing high-level actions, such as deleting cardholder records or rejecting requests.
- **Contractor Requests**
  Send a request to change the validation period of one or more cardholder badges. The user sending this request must be assigned to the same company as the cardholder whose badge validation period will be changed.

- **Request Approval and Validation**
  Configure Web Access to require approval and/or validation before requests can be fully processed. An approver can approve or reject a request. A rejected request can be edited for re-submittal.
- **Badging Activities**
  Quickly and easily track the badge activities of P2000 cardholders. When a cardholder presents a badge to a reader to enter or exit a secured area, you can view the record of the cardholder, the area the cardholder currently occupies (based on the location of the reader where the badge was last presented) and the date and time when the badge was presented to the reader.
- **Guard Services**
  Monitor, acknowledge and remove P2000 alarms, activate or deactivate output points (for example, turn on/off lights), and lock or unlock doors.
- **Emergency Access Disable**
  Disable the account of a single cardholder, which disables all of the cardholder's badges and his/her ability to log into Web Access.
- **Customizable User Interface**
  The Web Access interface is built with XML (Extensible Markup Language) and can be customized using the Altova® StyleVision software tool.

IMPORTANT NOTE ON APPLICATIONS AND CUSTOMIZATION

Web Access consists of a number of applications that enable you to send P2000 requests. For example, the *Add Cardholder* application enables you to send a request to add a cardholder to the P2000 database. For ease of use, these applications are organized into logical groups on the Web Access interface, which a Web Access administrator can customize.

Web Access supports multiple styles, each with its own potential set of applications, fields, colors, and images. A style has a limited number of applications (see Table 1-1), but they can be grouped in different ways, according to the administrator in charge of customizing Web Access.

In the default **jci** style, the applications are organized into four logical groups: Employee Services, Guard Services, Management Services, and Visitor Management. Table 1-1 lists all of the Web Access applications and the group(s) to which they are assigned.

Table 1-1: Web Access Applications

Application (Listed in Alphabetical Order)	Group (jci style)	See . . .
Add Badge	Management Services	page 3-42
Add Cardholder	Management Services	page 3-26
Add Journal	Management Services	page 3-39

Table 1-1: Web Access Applications

Application (Listed in Alphabetical Order)	Group (jci style)	See . . .
Alarm Monitoring	Guard Services	page 3-16
Area Search	Employee Services	page 3-10
Badge Print and Encode	Employee Services	page 3-8
Badge Resync	Employee Services	page 3-14
Cardholder Search	Employee Services	page 3-1
Command Outputs	Guard Services	page 3-19
Contractor Request	Visitor Management	page 3-52
Door Commands	Guard Services	page 3-20
Edit Badge	Management Services	page 3-42
Edit Cardholder	Management Services	page 3-36
Edit Journal	Management Services	page 3-40
Emergency Access Disable	N/A	page 3-54
In/Out Status Display	Employee Services	page 3-11
Request Approval	Management Services	page 3-23
Request Status	Management Services; Visitor Management[1]	page 3-21
Validation	Management Services	page 3-44
View Cardholder Information	Employee Services	page 3-5
View Badge Information	Employee Services	page 3-6
Visitor Request	Visitor Management	page 3-50
WebBadging Setup	Management Services	page 2-1

1. The Request Status application is available in either group.

Important: If you are using a custom style, the applications available on your Web Access interface, including the fields, captions, images, colors, and buttons, may vary. The screen captures and instructions in this document reflect the default **jci** style. For more information, contact the Web Access administrator.

GETTING STARTED

Software Requirements

The Web Access interface can be accessed via an Internet-connected computer, tablet, or PDA device installed with the following minimum software:

Computer or Tablet

- **Browser:** Microsoft® Internet Explorer® version 6.0.2900 or higher

- **Microsoft .NET Framework:** Version 2.0.xxxxx or higher (required only for the Web Badging feature; see "Chapter 2: Web Badging Configuration")
- **Screen Resolution:** The Web Access interface has been optimized for a screen resolution of 1024 x 768.

PDA

- **Operating System:** Windows Mobile® version 5.0/6.0
- **Browser:** Opera Mobile version 8.65 or higher or Minimo™ version 0.2 or higher
- **Screen Resolution:** The Web Access PDA interface has been optimized for a screen resolution of 240 x 320.

PDA Users

The PDA version of Web Access has a limited number of features, which are:

- Cardholder Search
- Area Search
- Alarm Monitor
- Badge Resync
- Door Control
- Output Control
- Emergency Access Disable

This manual only covers the computer version of Web Access; it does not cover the PDA version. However, the instructions for both versions are similar in that they share some of the same functionality. But because the PDA's screen size is smaller, the screens and components (for example, the location of the fields, buttons, etc.) are structured differently.

Sequence of Steps

The following sequence of steps describe the process of deploying, customizing, configuring and using Web Access. Only the P2000 System Administrator, Security Manager, or other qualified professional in charge of administering Web Access should perform these administrative tasks.

- **Deploy Web Access**
  Web Access can be deployed two different ways, which are described in "Web Access Deployment" on page 4-1.

- **Customize the Web Access user interface (Optional)**
  The Web Access user interface can be customized using the Altova® StyleVision XML editing tool. See "Customizing the Web Access Interface" on page 4-30 for more information.

NOTE

Customizing the interface can occur at any time, before or after Web Access is deployed.

- **Create and assign menu permissions to perform Web Access functions**
  A P2000 operator or system administrator must create or edit menu permission groups, which are assigned to Web Access users, to prevent unauthorized users from performing high-level actions such as deleting cardholder records or rejecting requests. Refer to the *P2000 Software User Manual* for detailed information on creating and assigning menu permissions.
- **Define Web Access options**
  The P2000 system allows operators to set up system-wide settings to define how Web Access requests are managed. Use P2000 to define the default Web Access options, approval levels, and processing method for Web Access requests. See "Request Process Flow Chart" on page 1-11 for information on the request process work flow. Refer to the *P2000 Software User Manual* for specific instructions on defining Web Access options.
- **Define request approvers**
  Depending on settings defined in P2000, each Web Access request may require up to three active approvers. The approver is a cardholder assigned Web Request Approval menu permissions. The approvers are ordered in a sequence and approve requests in the same order. Refer to the *P2000 Software User Manual* for specific instructions on defining request approvers.
- **Configure the Web Access Computer for Web Badging (Optional)**
  If you will use the Web Access client computer for Web Badging (capturing cardholder photos and signatures, and printing and encoding badges), follow the instructions in "Chapter 2: Web Badging Configuration".
- **Submit requests using Web Access**
  Web Access users can submit a number of different requests (see "Chapter 3: Using Web Access" for detailed information). Depending on how Web Access is configured, the system can process a submitted request with or without approvers and validation.

NOTE

As a simple precaution, check the Request Queue after each request you submit to verify that it was submitted successfully.

- **View the status of a request**
  Users can view the status of requests using the Request Queue. Users can cancel their own requests, if desired. They cannot, however, cancel requests submitted by other users.

- **Approve or reject the request**
  Approvers may approve or reject a submitted request before it is committed (finalized). For information on defining request approvers, refer to the *P2000 Software User Manual*. For specific instructions on approving, see "Approving or Rejecting Requests" on page 3-23.

- **Validate the request**
  All visitor badge requests and other requests set for manual processing must be validated. Users can validate a request only if their menu permission group is configured to allow it.

Logging On

➤ To log on to Web Access:

1. From a Web browser, enter the following in the Address bar, replacing *Server Name or IP Address* with the name or IP address of the Web Access server:

   http://Server Name or IP Address/P2000

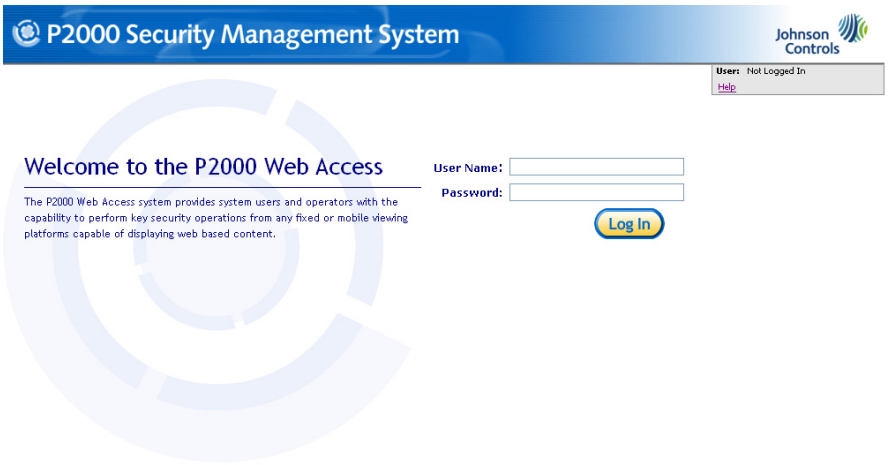
   Or enter the following if the Web Access Administrator has configured the P2000 server as a secure server:

   https://Server Name or IP Address/P2000

NOTE

If you do not know the Web Access server name, or if you cannot successfully log on to the application, consult your Web Access Administrator for assistance.

The Login page appears.



2. Enter your **Username** (`firstname.lastname`) and **Password**.

   The Username is based on the cardholder first and last name (for example, *john.smith*). The Password is an alphanumeric code (combination of letters and/or numbers) used for user authentication.

3. Click **Log In** or press **<Enter>** on your keyboard.

4. The Welcome page appears.

➤ To log off of Web Access:

1. Click the **Log Out** link at the upper-right corner of any Web Access page.

2. The Login page appears.

THE WELCOME PAGE

The Web Access Welcome page provides links to the following Web Access services. Some features, such as viewing status requests, can be performed from multiple service options.

- **Employee Services**
  Select to track the badge activities of P2000 cardholders, request a Badge Resync, which returns a badge to its correct state if it is out-of-sync, or print and encode a badge.
- **Guard Services**
  This service enables you to view, acknowledge, and discard P2000 alarms, activate or deactivate output points (for example, sirens, lights, etc.), and send door commands such as lock, unlock, timed unlock, and resume normal operation.
- **Management Services**
  Select to view and/or approve requests, add or edit a cardholder record, or validate requests. To approve or validate requests, you must have proper permissions configured.
- **Visitor Management**
  This feature allows you to request a visitor badge or request to extend the validation period of a cardholder badge. You may also view the status of your requests.

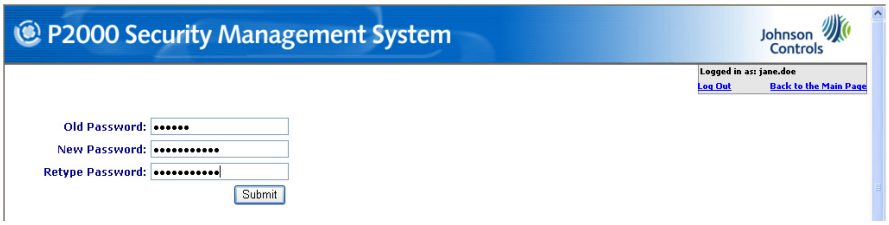
Changing Your Password

The Welcome Page also enables you to change your password used to log on to Web Access.

➤ **To change your Web Access password:**

1. Click the **Change Password** link in the upper-right corner of the Welcome page.

2. In the **Old Password** field, enter your existing Web Access password.
3. Enter your new password in the **New Password** and **Retype Password** fields.



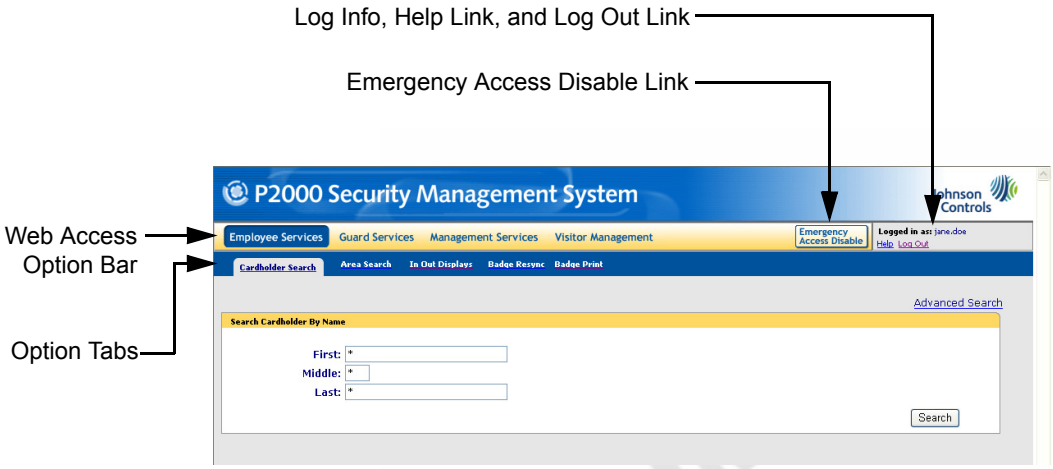
4. Click **Submit**.

   The Welcome page appears. If the change was successful, the following message appears in the upper-right corner of the page:

   `Your password is updated successfully!`

THE WEB ACCESS WORKSPACE

This section describes the Web Access Workspace, which consists of the Web Access Option bar, Option Tabs, the Emergency Access Disable link, and the Help and Log Out links.



- **Web Access Option Bar**
  Each option on this bar reveals a different set of tabs. Each tab enables you to perform a Web Access function. For descriptions of the bar's options, see "The Welcome Page" on page 1-9.

- **Option Tabs**
  These tabs are a collection of features associated with the option selected on the Web Access Option bar.
- **Emergency Access Disable**
  Use to immediately disable a cardholder account, which will disable all of the cardholder's badges and his/her ability to log into Web Access. This option is available on all Web Access pages. See "Emergency Access Disable" on page 3-54 for detailed information.
- **Help Link**
  Opens the P2000 Web Access online help system.
- **Log Out Link**
  Click to log out of Web Access.

REQUEST PROCESS FLOW CHART

Figure 1-1 outlines the request process once an operator submits a request. The following rules govern how Web Access processes the request:

- When an operator submits a request, if the system administrator has defined one or more approvers, the request must be approved before it can be validated or processed. If the system administrator has not defined an approver, the request can be validated (if the request type is set to *manual*) and processed.
- An approver can reject or approve a request. The status of a rejected request is *Rejected*. An operator can edit a rejected request and resubmit it for processing. An approved request can be validated (if the request type is set to *manual*) and processed.
- If validation is required, an authorized user must validate the request before the system can process it. Until an operator validates the request, it will have a status of *Validation*.
- During the validation process, an authorized user can reject a request or approve it for processing. The status of a rejected request is *Rejected*. An operator can edit a rejected request and resubmit it for processing. An approved request during validation will be processed.

NOTE

A requestor can cancel his/her request at any time during the approval or validation process. A cancelled request will be archived into the Request History and cannot be edited for re-submittal. A user cannot cancel a request submitted by another user.

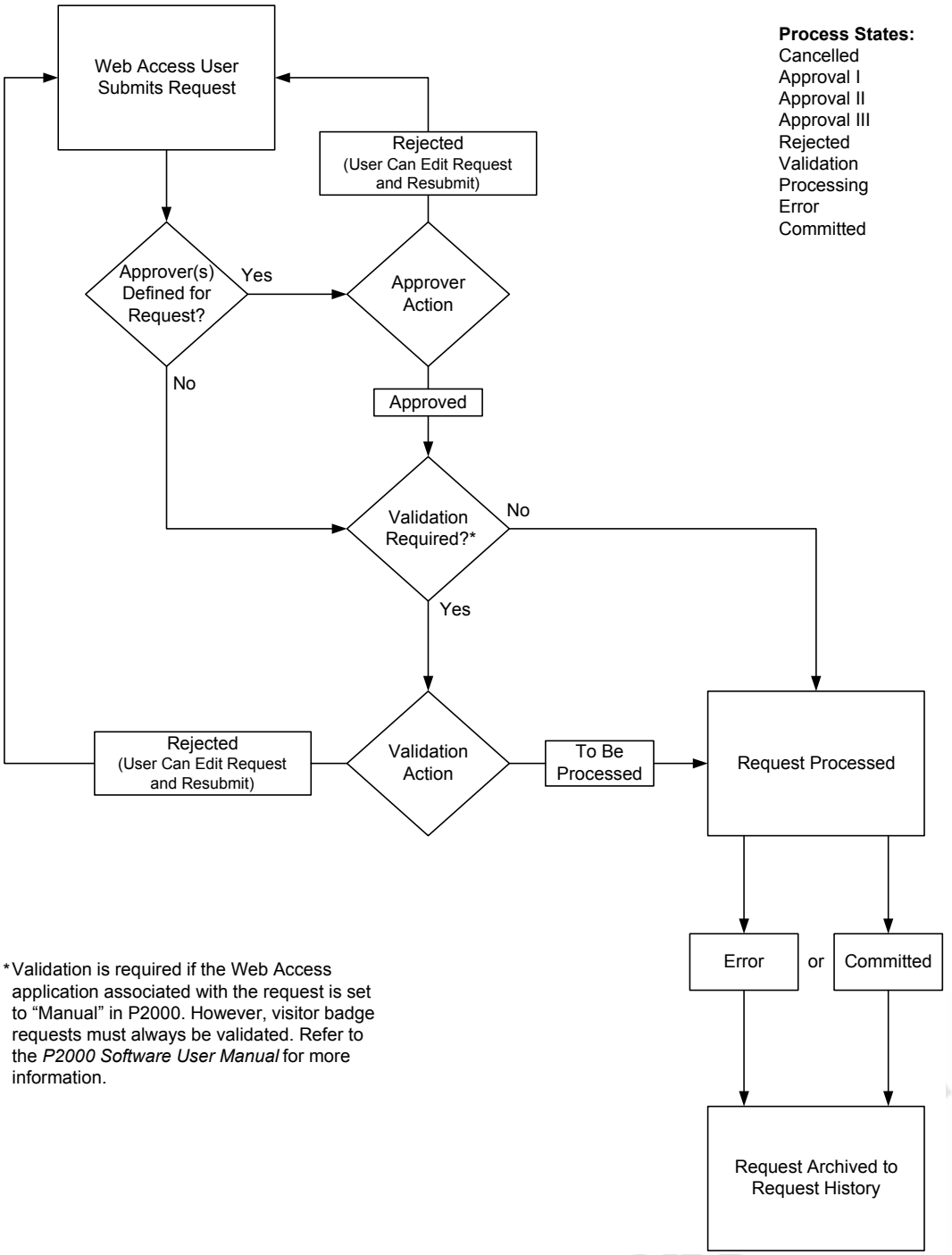


Figure 1-1: Request Process Flow Chart

Process States

As the system processes a request, the status changes to reflect the request's current state. The different states are described below:

- **Cancelled** – The request was cancelled before being processed. A cancelled request is archived into the Request History and cannot be edited for re-submittal.
- **Approval 1** – The request is waiting to be approved by the required approver.
- **Approval 2** – The request was approved by Approver 1, and requires approval of a second approver.
- **Approval 3** – The request was approved by Approvers 1 and 2, and requires approval of a third approver.
- **Rejected** – The request was rejected. A rejected request can be edited and resubmitted for processing.
- **Validation** – The request is waiting to be validated by an authorized user.
- **Processing** – The request is currently being processed.
- **Error** – There is an error in the request.
- **Committed** – The request has been completed.

WEB ACCESS SCENARIOS

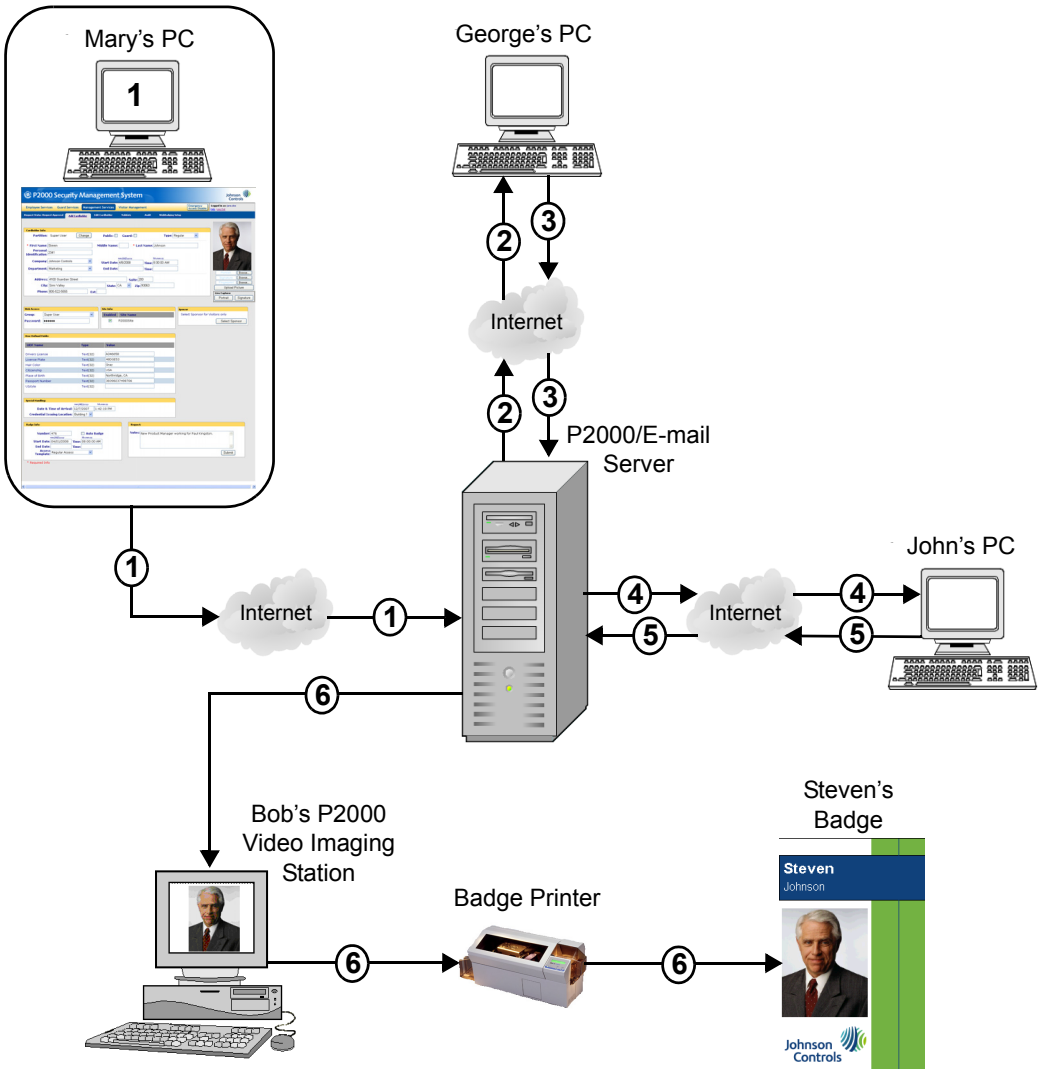
This section consists of fictitious scenarios that illustrate how the request and approval process works. The scenarios cover only two types of requests: add cardholder and visitor requests. As you are reading a scenario, refer to the corresponding number on the illustration.

NOTE

The following scenarios do not illustrate the use of the Web Badging feature, which can be used to capture cardholder images, and print and encode badges, directly from a Web Access client computer. See "Chapter 2: Web Badging Configuration" for more information.

Adding a Cardholder

Mary, a Human Resources Manager for ABC Industries, has just hired Steven. She is responsible for preparing what he needs for his first day of work. She starts by using Web Access' Add Cardholder application to submit a request to add a cardholder record for him.

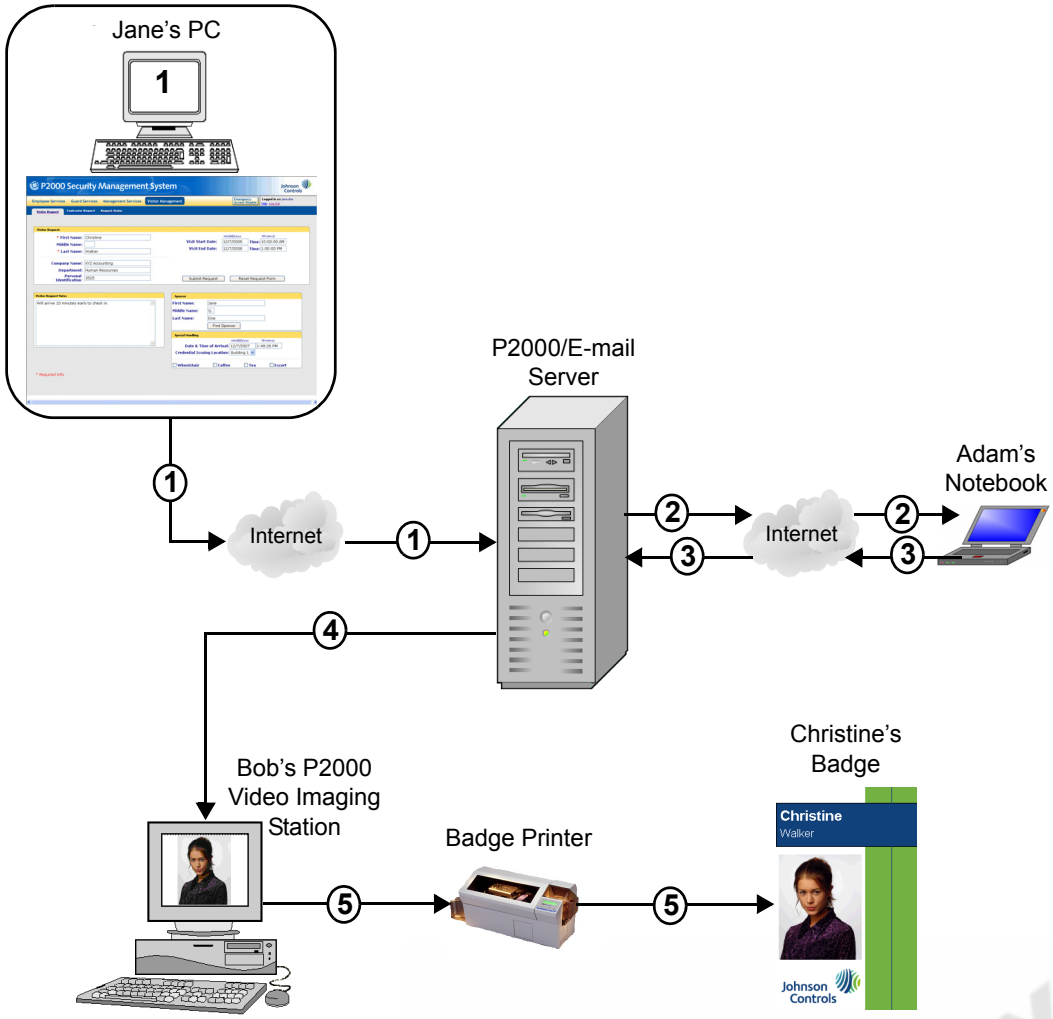


1. Mary enters Steven's data, uploads his picture, and adds a request note stating that he is a new Engineer working for George, an Engineering Manager. She submits the request to add Steven as a cardholder.
2. The P2000 system is set to require two approvals for cardholder requests, first from the cardholder's direct manager (George) and the second from the facility manager (John). George receives the first e-mail notification that there is a request pending for approval.
3. When George clicks the request hyperlink, the Web Access application opens the request. George approves the request for Steven and adds approval notes that Steven will need full-time access to the facility.
4. After George approves the request, John, the Facility Manager, receives an e-mail notification that there is a pending request. John clicks the request hyperlink to see the request.
5. John approves the request and notices that the request was originated by Mary and has already been approved by George.
6. The request is processed. When Steven arrives for work at the reception desk, he identifies himself to Bob, the security officer. Bob locates Steven's name in the Cardholder database. Bob then saves and prints the badge with Steven's picture.

Figure 1-2: Scenario 1 (Adding a Cardholder)

Requesting a Visitor Badge

Jane has invited Christine, a business colleague, to her facility for a tour. She arrives next week. Jane needs to request a visitor badge for her arrival.



1. Jane uses Web Access to request a visitor badge for Christine. The request is submitted to the Web Access Request Queue, where it will remain with a state of "Pending" until it is approved. The P2000 system administrator has configured P2000 to require a single approval for visitor requests.
2. The authorized approver, Adam, is away from the office and receives an E-mail notification on his Notebook PC informing him of Jane's visitor request.
3. Adam clicks on the request hyperlink in the E-mail, which links to the Web Access Request Approval application. After Adam logs into Web Access, he views the details of the visitor request. Adam approves the request, but enters an approval note that the visitor (Christine) should only have rights to visit between 9 A.M and 5 P.M.
4. Bob, the security officer, notices that Adam has approved the request. Bob adds Christine as a visitor to the P2000 database and assigns a badge according to Adam's instructions.
5. When Christine arrives at the reception desk, she identifies herself to the Security Officer, who prints and hands her the badge.

Figure 1-3: Scenario 2 (Requesting a Visitor Badge)

USING BROWSER FAVORITES/BOOKMARKS IN WEB ACCESS

Standard browsers enable you to save or bookmark URL addresses as *Favorites*, so you can quickly access a previously visited Web page by selecting its bookmark. Favorites or bookmarks can help you save time in Web Access as well, by allowing you to do the following:

- **Quickly open a particular application**
  Instead of navigating the interface each time to find a frequently-used application, simply add the application page to your favorites list.
- **Save a particular search**
  If you frequently perform a search with specific criteria, you can save the search page with the criteria for future use. For example, you can save a search that will filter the results based on a specific company (for example, Johnson Controls) and a specific department (for example, Engineering), saving you from entering search criteria each time you want to perform this search.
- **Quickly see who's In or Out of the facility**
  Bookmarking a page that displays the In-Out status of a particular cardholder enables you to quickly view the status again later, without having to locate the cardholder again and re-add him/her to the In-Out display. See "In/Out Status" on page 3-11 for more information.

For information on how to add a link to the Favorites list (or to bookmark a page), refer to your browser's online help.

Chapter 2

WEB BADGING CONFIGURATION

This chapter describes the steps necessary to configure your Web Access client computer as a Web Badging station. The Web Badging feature enables you to perform the following tasks from any computer running Web Access:

- Capture cardholder portrait images using any USB-compatible Webcam
- Capture cardholder signature images using the Topaz™ model T-S261-HSB signature pad
- Encode MIFARE® contactless smart cards with the ACS™ ACR120 encoder
- Print badges

To accomplish these tasks, you must first install and configure the proper hardware and software components as described in this chapter.

SYSTEM ARCHITECTURE

Figure 2-1 shows a P2000 Web Access Web Badging system.

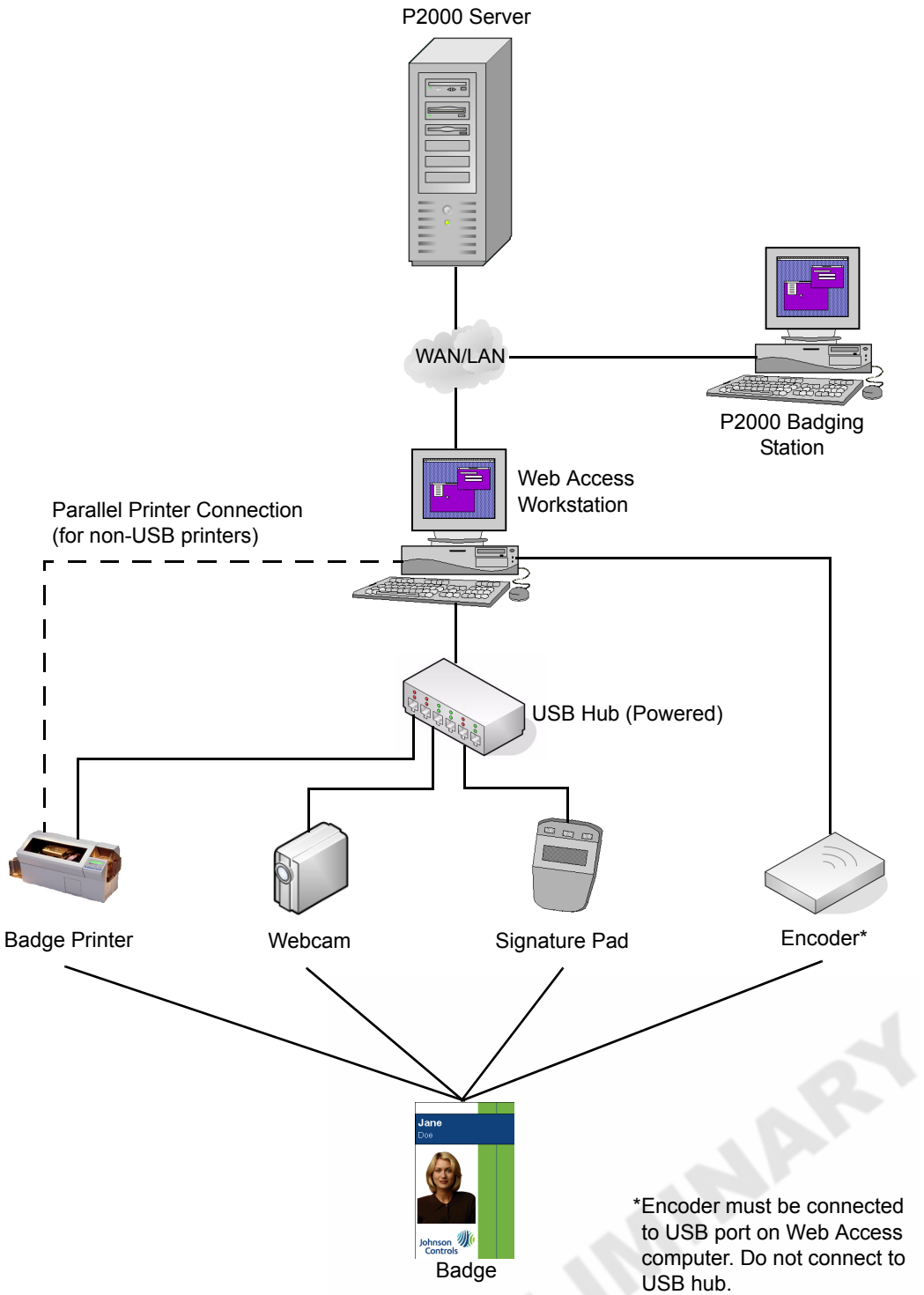


Figure 2-1: P2000 Web Access Web Badging Configuration

INSTALLATION AND CONFIGURATION

This section describes how to install and configure the hardware and software used on a P2000 Web Access Web Badging station.

IMPORTANT

When installing badging devices, follow the manufacturer's instructions for proper device and driver installation. The device may not function properly if you fail to follow the manufacturer's instructions during installation.

NOTE

Johnson Controls strongly recommends using a powered USB hub as the communications interface between the Web Access computer and the badging devices (excluding the encoder).

Before installing any badging hardware, download and run the **WebBadgingSetup.exe** file according to the instructions in "Installing and Running the WebUSB Application".

Installing and Running the WebUSB Application

The WebUSB application enables you to use USB-compatible badging devices via the P2000 Web Access interface. When you launch this application (by downloading and running the **WebBadgingSetup.exe** file), a WebUSB service runs in the background. This service must be running on the client computer running Web Access or the badging devices cannot be controlled.

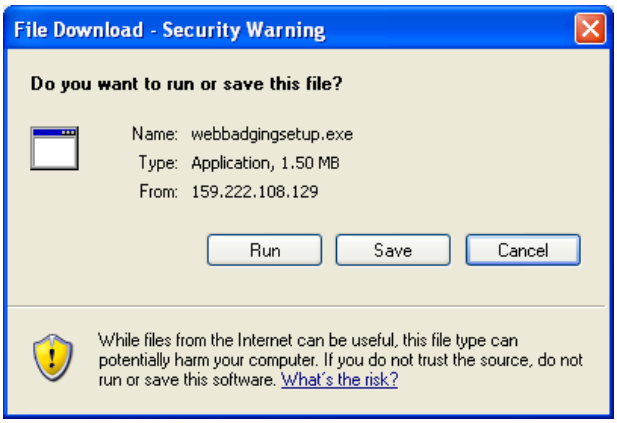
NOTE

*You only need to run the **WebBadgingSetup.exe** file once per client computer. Once this application is installed, the WebUSB service runs automatically, even after restarting the client computer.*

➤ **To install and run the WebUSB application:**

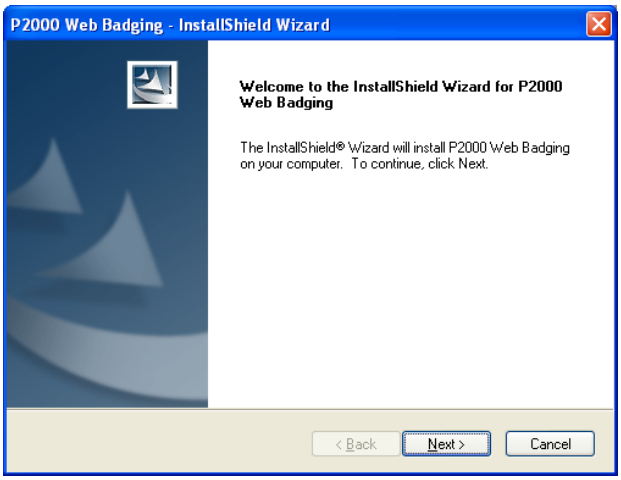
1. Select the **Management Services** option.
2. Select the **WebBadging Setup** tab.

3. Click the **WebBadgingSetup.exe** link. The File Download - Security Warning dialog box appears.

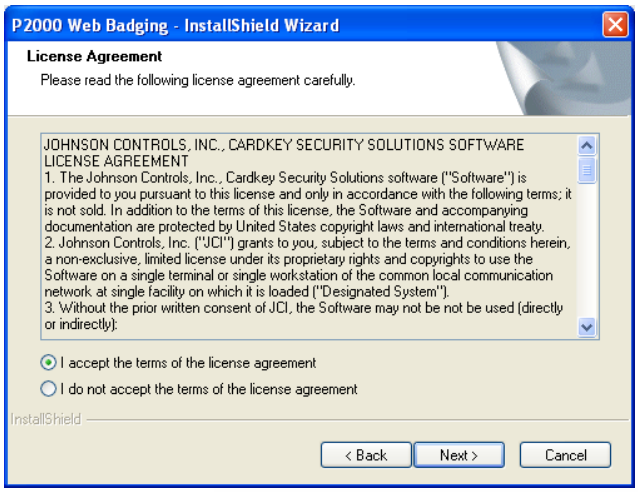


4. Click **Run**. The Internet Explorer - Security Warning dialog box appears.

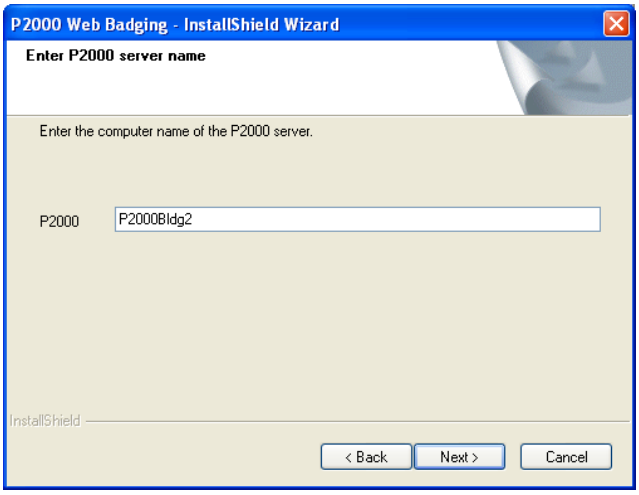
5. Click **Run**. The P2000 Web Badging - InstallShield Wizard dialog appears.



6. Click **Next**.
7. On the License Agreement page, select the **I accept the terms of the license agreement** check box and click **Next**.

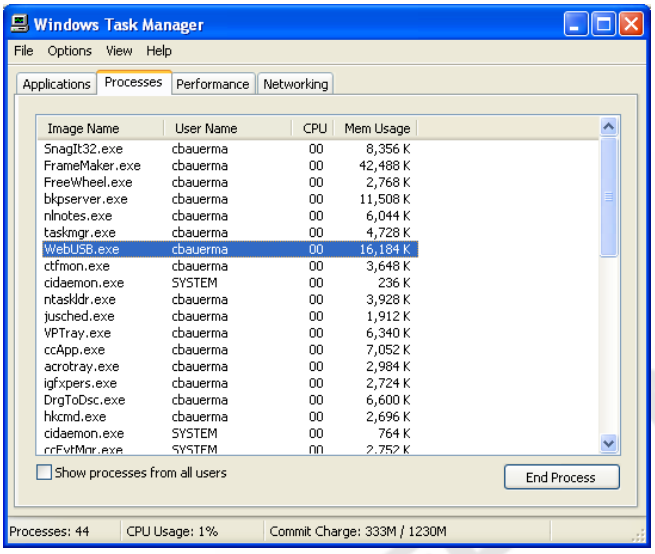


8. On the Enter P2000 server name page, enter the name assigned to the P2000 server and click **Next**.



9. Click **Install**.
10. Wait for the installation to finish. Then verify that the WebUSB service is running; the following icon in the Windows® system tray (bottom-right corner of screen) indicates that the service is running.

11. You can also verify that the service is running by accessing the Windows Task Manager (Processes tab). To access the Windows Task Manager, right-click on the digital clock in the Windows system tray and select **Task Manager**. Select the **Processes** tab. Under the **ImageName** column, verify the **WebUSB.exe** file is listed.



12. See “Important Web Badging Installation and Configuration Notes” on page 2-7.

Important Web Badging Installation and Configuration Notes

- If the WebUSB service fails to start or stops for any reason, to start the service, simply double-click the **WebUSB.exe** file located at: *Local Disk:\Program Files\Johnson Controls\CARDKEY P2000\WebBadging*
- If you receive an error when attempting to manually start the WebUSB service, verify you have the correct version of Microsoft® .NET Framework installed on your computer. See "Software Requirements" on page 1-4.
- Before using the Web Badging feature, close the Microsoft Internet Explorer® browser window running Web Access. Then re-launch the browser and log into Web Access.
- To use the Web Badging feature, your Windows account must have **administrator** or **power user** privileges. You *cannot* use this feature on a Windows account with limited or restricted privileges.
- If connecting to the P2000 server from the Web Access client using the server's IP address (see "Logging On" on page 1-7), add the server's IP address as a trusted site in Internet Explorer. For instructions on adding an address as a trusted site, refer to the Internet Explorer documentation.
- To connect to a different P2000 server than the one defined during the WebUSB application installation (see page 2-6), add the server's IP address and computer name as trusted sites in Internet Explorer. For instructions on adding an address as a trusted site, refer to the Internet Explorer documentation.

Installing the Webcam

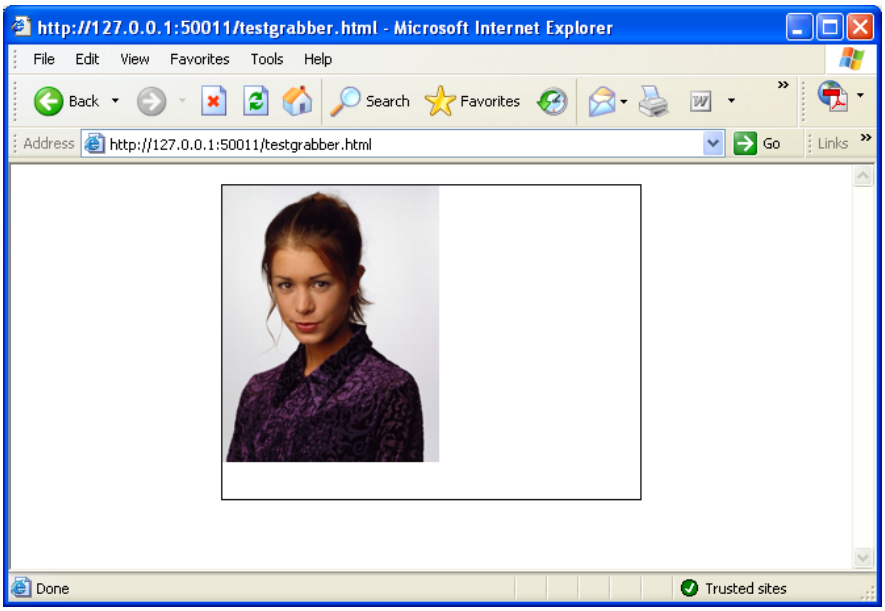
The Webcam requires a simple USB cable connection from the camera to the USB hub.

➤ **To install the Webcam:**

1. Install the camera driver software that comes with the Webcam. Refer to the manufacturer's documentation.
2. Connect the camera's USB cable to one of the USB hub's available USB ports.
3. Use the Windows® Device Manager to verify that the operating system recognizes the Webcam. To access Device Manager, select **Start>Control Panel**, double-click the **System** icon, select the **Hardware** tab, and click **Device Manager**.
4. Test the Webcam by opening a browser instance and entering the following address:

   `http://127.0.0.1:50011/testgrabber.html`

The Webcam image should appear.



5. If the image from the device fails to appear, see “Troubleshooting” on page 2-11 for assistance.

Installing the Signature Pad

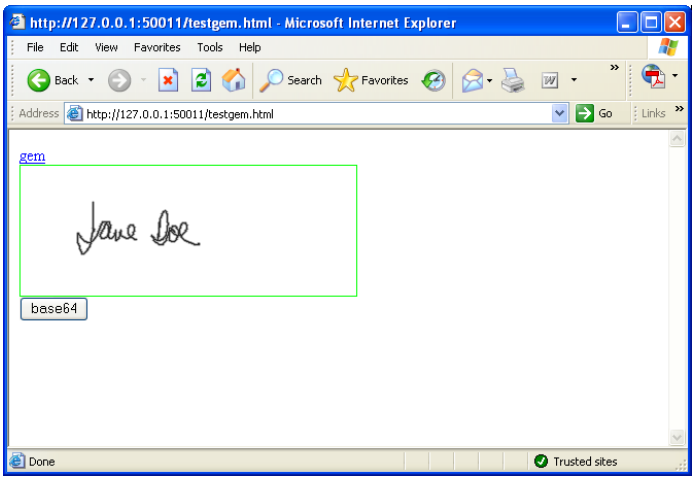
The P2000 Web Access Web Badging feature supports the Topaz™ model T-S261-HSB signature pad. The signature pad requires a simple USB cable connection from the pad to the USB hub.

➤ To install the signature pad:

1. Install the driver software that comes with the signature pad. Refer to the manufacturer’s documentation.
2. Connect the signature pad’s USB cable to one of the USB hub’s available USB ports.
3. Use the Windows Device Manager to verify that the operating system recognizes the signature pad. To access Device Manager, select **Start>Control Panel**, double-click the **System** icon, select the **Hardware** tab, and click **Device Manager**.
4. Test the signature pad by opening a browser instance and entering the following address:

   `http://127.0.0.1:50011/testgem.html`

For testing purposes, sign a name using the signature pad. The signature image should appear.



5. If the image from the device fails to appear, see “Troubleshooting” on page 2-11 for assistance.

Installing the Encoder

The P2000 Web Access Web Badging feature supports the ACS™ Model ACR120 MIFARE® smart card encoder. The encoder requires a simple USB cable connection from the device to the Web Access computer.

➤ To install the encoder:

1. Install the driver software that comes with the encoder. Refer to the manufacturer’s documentation.
2. Connect the encoder’s USB cable to one of the available USB ports on the Web Access computer.

NOTE

Do not connect the encoder to a USB hub. Connect the USB cable directly to the computer running Web Access.

---

3. Use the Windows Device Manager to verify that the operating system recognizes the encoder. To access Device Manager, select **Start>Control Panel**, double-click the **System** icon, select the **Hardware** tab, and click **Device Manager**.
4. Verify that the green LED on the front of the encoder is lit. If it is not lit, see “Troubleshooting” on page 2-11 for assistance.

Installing the Badge Printer

The P2000 Web Access Web Badging feature supports most standard Windows-compatible printers, including non-card/label printers.

The badge printer requires a simple cable connection from the printer to the USB hub (for USB-compatible printers) or to the computer's LPT1 parallel port (for parallel printers).

NOTE

Before using a badge printer, check with the printer manufacturer for current printer drivers.

➤ **To install the badge printer:**

1. Install the printer driver software that comes with your printer. Refer to the manufacturer's documentation.
2. **USB Printers:** Connect the printer's USB cable to one of the USB hub's available USB ports.
3. **Parallel Printers:** Connect one end of the parallel cable to the back of the printer and the other end to the computer's parallel port (LPT1).

   Refer to your printer documentation for more information on the installation, operation, and maintenance of your badge printer.
4. Select **Start>Printers and Faxes** and verify that the Windows operating system recognizes the printer.

WEB BADGING NOTES AND LIMITATIONS

If you are using Imageware® Systems, Inc.'s ID Server or EPI Builder badge design software to create your badge layouts, and you will be using Web Access to print your badges, we recommend creating the badge layout's static graphic elements (e.g. badge background, colors, lines, shapes, etc.) using a 3rd-party graphics application, such as Adobe® Photoshop®, and importing the badge elements into ID Server or EPI Builder as a single static image into the badge layout. If you create static graphic elements using ID Server or EPI Builder, some elements may not appear in Web Access when previewing and printing the badge.

Important ID Server Note

All static image files on the badge layout must be copied to the *C:\Badgemaster\bmaster* directory on the P2000 server or workstation. If an image file is not added to this directory, the image appears as a gray box when previewing or printing the badge.

Bar Code Limitations

The following bar code types are **not** supported in Web Access on badge layouts created with EPI Builder:

- Code 16K A
- Code 16K B
- Code 16K C
- Code 49
- Code 16K Auto
- Extended Code 3 of 9
- Extended Code 93

On badge layouts designed with ID Server, Web Access does **not** support any bar codes.

TROUBLESHOOTING

Use the following information to troubleshoot any issues with the Web Badging feature.

Table 2-1: Web Badging Troubleshooting

Issue	Action
General USB Device Issues	• Do not connect multiple USB badging devices directly to the Web Access client, as they may draw too much power from the computer. Use a powered USB hub as the interface between the Web Access client and the USB badging devices (excluding the encoder). • Verify that each USB cable is securely connected to each device. • Verify the USB hub's power cord is securely connected to a proper power outlet (120/220 VAC).
Encoder Green LED Not Lit, or Web Access Displays Error During Encoding	• Did you install the device driver? • Has Windows correctly identified the device in Device Manager? Verify that the device is using the manufacturer's driver and not a standard Windows driver. • Is the WebUSB application currently running? See page 2-3. • Verify the USB cable is connected to an available USB port on the Web Access client computer. Do not plug the cable into a USB hub.

Table 2-1: Web Badging Troubleshooting

Issue	Action
No Image from Webcam or Signature Pad	• Did you install the device driver? • Has Windows correctly identified the device in Device Manager? Verify that the device is using the manufacturer's driver and not a standard Windows driver. • Does the device software include a test application? If so, test the device using the manufacturer's software to verify that the device is functioning properly. • Is the WebUSB application currently running? See page 2-3. • Close and re-launch the Web browser. Then log on to Web Access and confirm whether you can view the Webcam or signature pad image. • Add the P2000 server's IP address and computer name as trusted sites in Internet Explorer on the Web Access client computer. Refer to the Internet Explorer documentation for assistance. • Are you logged into a Windows account with administrator or power user privileges? You *cannot* use the Web Badging feature on a Windows account with limited or restricted privileges. • Uninstall the WebUSB application using the Windows Control Panel. Then reinstall the application according to the instructions in "Installing and Running the WebUSB Application" on page 2-3.
Card Not Printing	• Is the printer powered on? • Verify the printer's power cord is securely connected to a proper power outlet (120/220 VAC). • Verify the printer's communication cable (USB or parallel) is securely connected.
Card Not Printing Properly	• Does the printer's ribbon need replacing? • Refer to the printer manufacturer's documentation for troubleshooting tips.
Static image appears as a gray box when previewing or printing a badge	• Copy all static image files on the badge layout to the *C:\Badgemaster\bmaster* directory on the P2000 server or workstations.
Bar code does not appear on badge preview or on printed badge	• Bar codes are not supported on badge layouts designed with ID Server. • Some bar codes are not supported with badges designed with EPI Builder.

Chapter 3

USING WEB ACCESS

This chapter provides details about the Web Access features and instructions for using the Web-friendly interface. Depending on your permissions, you may not have access to all of the features available on the interface. For example, the Web Access Security Manager having full permissions will be able to approve or deny Web Access requests, whereas a low-level user may only be able to request visitor badges or extend the validation period of cardholder badges. This chapter covers all of the features available from the Web interface.

NOTE

For information on configuring Web Access permissions, refer to the P2000 Software User Manual.

EMPLOYEE SERVICES

These services allow you to perform a number of cardholder-related actions, such as:

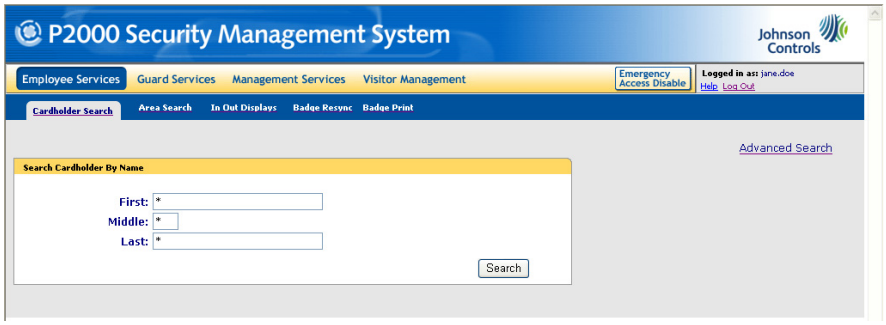
- Locating cardholder records in the P2000 database
- Viewing detailed cardholder and badge data (see page 3-5)
- Printing and encoding cardholder badges (see page 3-8)
- Determining the location of cardholders within P2000 defined areas (see page 3-10)
- Tracking the In-Out status of selected cardholders in specific P2000 defined areas (see page 3-11)
- Synchronizing your badge (see page 3-14)

Searching Cardholder Records

Web Access allows you to locate one or more cardholder records in the P2000 database. You may search by such criteria as cardholder name, badge number, personal identification number, department, and company. Use this feature to view cardholder and badge information of a particular cardholder record.

➤ To search for cardholder records:

1. Select the **Employee Services** option. The Cardholder Search page appears.



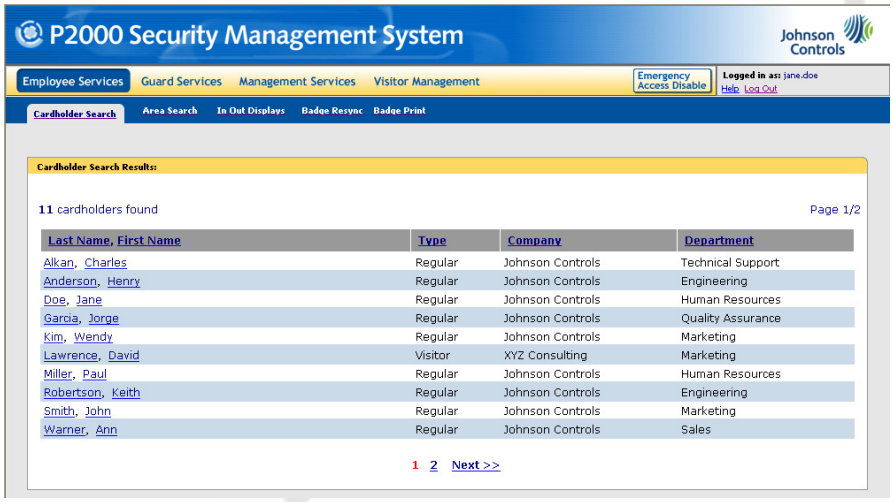
2. Enter the cardholder's first, middle and/or last name or click the **Advanced Search** link to search by other cardholder criteria listed below:
   - Personal Identification Number
   - Badge Number
   - Department
   - Company
   - Drivers License or License Plate, if defined as user-defined fields (UDF) in P2000

NOTE

The Drivers License and License Plate fields will only appear on the Cardholder Search page if they have been added as UDFs in P2000. For information on adding UDFs, refer to the P2000 Software User Manual.

---

3. Click **Search**. The Cardholder Search Results page appears, listing the cardholders that were located based on your search criteria.



Search Tools

If necessary, use the following search tools to help you locate cardholders. This information applies to all cardholder search fields in Web Access.

The Asterisk Wildcard (*)

This wildcard represents a string of characters during text searches. Use it to locate a range of values. For example, to search for everyone whose first name starts with "J", enter "J*" in the First name field.

The Question Mark Wildcard (?)

This wildcard represents a single character during text searches. For example, searching for "J??e" might return "Jane" or "Jude", searching for Jan?e might return "Janie", etc.

The Comma (,)

The Comma "," allows you to separate search values. For example, to search for cardholders of two companies (for example, Johnson Controls® and ABC Supplies), enter "Johnson Controls, ABC Supplies" in the Company field.

NOTE

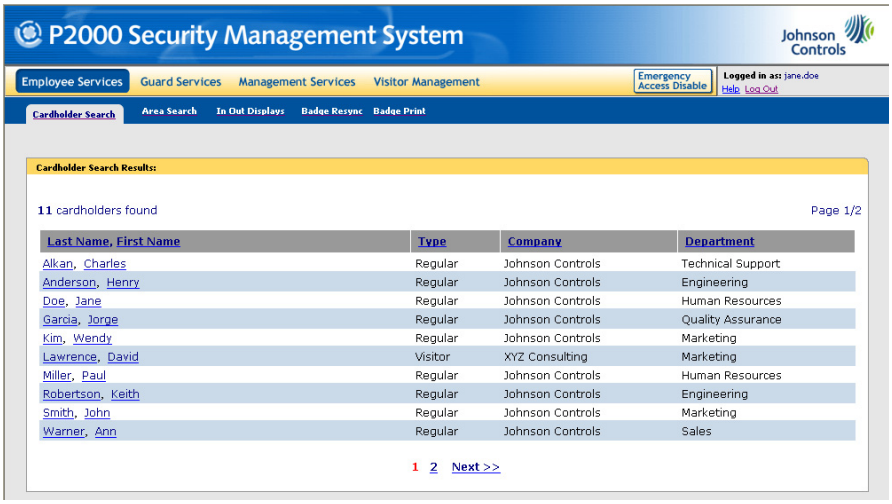
You may also combine search tools. For example, if you enter "J, William" into the First name field, Web Access will return all first names of "William"* ***and*** *names that start with "J".*

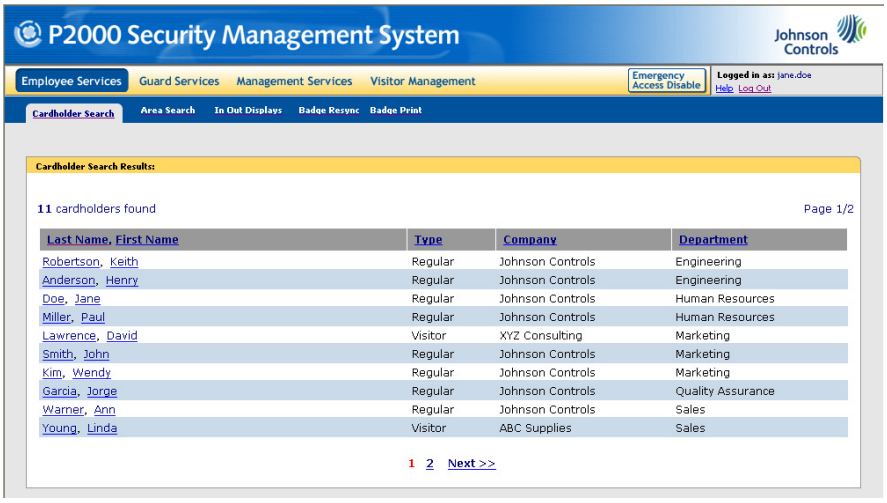
Sorting Columns

Many record tables in Web Access have sortable columns. Sorting a column allows you to re-order the values listed in the column alphabetically (A to Z, or Z to A) or numerically (date/time), which re-orders the values in the other columns accordingly.

For example, you may re-order a list of cardholder records based on the department. If cardholders belonging to four different departments are displayed (for example, Marketing, Engineering, Technical Support and Human Resources), sorting the Department column will list the cardholders in order of the department to which they belong (alphabetically, A to Z), so every cardholder belonging to Engineering will be displayed first, followed by Human Resources, Marketing and Technical Support respectively.

To re-order a column, simply click the column header. The first screen capture displayed below shows the cardholders listed alphabetically according to the cardholder Last Name. The second screen capture shows the list sorted alphabetically (A to Z) after clicking the Department column.





Changing the Number of Cardholders Listed Per Page

If the number of cardholders listed per page is too few or too many, you can temporarily modify the number displayed by appending the following to the end of the URL:

`&ipp=n`

where *n* equals the number of cardholders you wish to display per page.

Example:

*http://150.243.108.101/p2ktc/we/app/bactivity/cardholderlist.aspx?search=&span=1&time=12:00:00%20AM**&ipp=20***

In the previous example, 20 cardholders will be displayed per page.

NOTE

Changing the cardholders listed per page in this manner is only temporary. Once you access a different Web page, the cardholders listed per page setting returns to its default value.

NOTE

This feature can also be used on the Cardholder List page when searching for cardholders on the Edit Cardholder tab.

Viewing Cardholder Information

To view cardholder information, click the name of the cardholder on the Cardholder Search Results page. The Cardholder Info page appears.

The following information is displayed on this page:

- **Cardholder Information**
  Lists general cardholder information such as cardholder name, company name and address, department assigned to the cardholder, the cardholder record's start and end date, and the phone number.
- **Site Information**
  Displays the site to which the selected cardholder is assigned.

- **Badge Last Activity**
  Displays badge last activity information such as the terminal where the badge was last presented, the time it was presented, and the area the cardholder currently occupies (based on the location of the terminal where the badge was last presented).

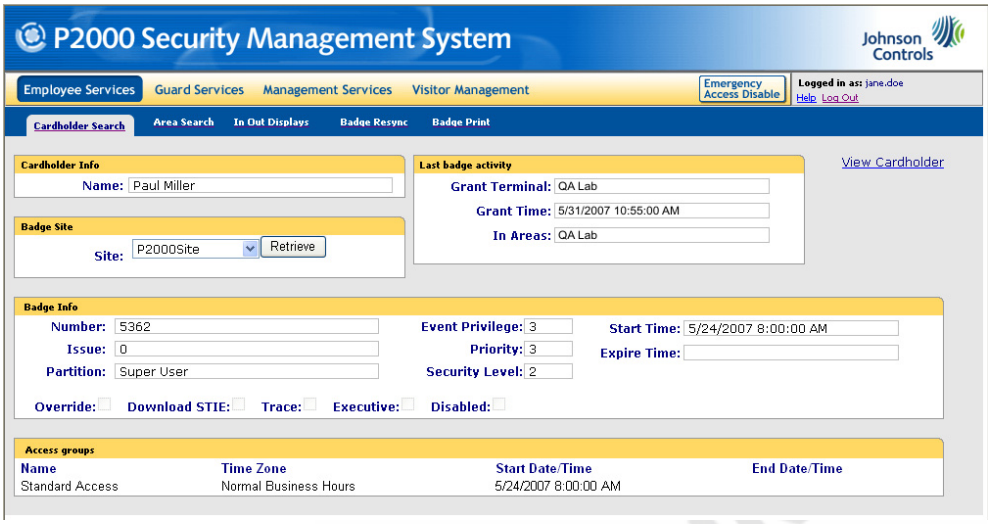
- **Cardholder Journal Entries**
  Lists the title, text, create date/time and last modified date/time of the cardholder journal entries. For more information on journals, refer to the *P2000 Software User Manual*.

Viewing Badge Information

You may view the cardholder's badge information by clicking the **View Badge Details** link on the upper-right corner of the Cardholder Info page. The Badge Info page appears.

NOTE

*If the cardholder has not been assigned a badge, the **View Badge Details** and **Print & Encode Badge** links will not be visible. Also, if the cardholder has multiple badges, you may only view information on the first badge (the badge with the lowest number), as listed in P2000.*



The following information is displayed on this page:

- **Cardholder Information**
  Displays the cardholder name.

- **Badge Site**
  Displays the name of the site associated with the badge. To retrieve badge information for another site, select a site from the drop-down list and click **Retrieve**.

- **Badge Information**
  See "Badge Info Field Definitions" on page 3-7.
- **Last Badge Activity**
  Displays badge last activity information such as the terminal where the badge was last presented, the date and time it was presented, and the area the cardholder currently occupies (based on the location of the terminal where the badge was last presented).
- **Access Groups**
  Displays the access group(s) assigned to the cardholder badge, consisting of the access group name, time zone, start date/time, and end date/time.

Badge Info Field Definitions

Number – Displays the number assigned to the badge.

Issue – Displays the badge's issue level. If a cardholder loses a badge, he/she receives the next available issue level and retains the same badge number. The number of badge issue levels supported depends on the panel type.

Partition – Displays the partition associated with this badge.

Event Privilege – Displays the badge's event privilege level, ranging from 0 to 7, with zero as the lowest level.

Priority – This number, ranging from 1 to 99, determines which guard tours the selected cardholder can perform.

Security Level – In order for the cardholder to obtain access at a door, this number must be equal to or greater than the security level set up at the terminal. If the security level at the terminal is greater, the cardholder will be denied access, unless the badge has the Executive privilege enabled.

Start/Expire Time – Displays the badge validation period. The Start Time displays the date and time when the badge became or will become active. The Expire Time displays the date and time when the badge expired or will expire.

The following information describes security options assigned to a badge. Refer to the *P2000 Software User Manual* for additional information.

Override – If enabled, the cardholder can unlock any door controlled by a keypad reader that has the Cardholder Override/Shunt option enabled.

Download STI E – This option applies only to legacy panels using STI-E terminal interfaces. If selected, the badge is downloaded to the STI-E terminal. The STI-E terminal can save up to 1,000 badges in a resident database for use if the panel becomes inactive.

Trace – If enabled, all badge transactions for the cardholder will be printed, as they occur, on any printer configured to print trace transactions, as long as the Badge Trace and Print options are selected in the Real Time List window in P2000.

Executive – If enabled, the cardholder will have unlimited access to all operational doors controlled by the access control system, regardless of any other privileges programmed for this badge. (If a specific terminal requires the use of a PIN code with a badge, the PIN code is still required.) Not available for P900 panels.

Disabled – When a badge is created, the system automatically enables it. If you select this check box, the system temporarily disables the badge.

Printing and Encoding Badges

Cardholder badges can be printed or encoded from a Web Access client if the computer has been configured as a Web Badging station. See "Chapter 2: Web Badging Configuration" for more information.

NOTE

Badge encoding must be enabled and configured in the P2000 software before you can encode a badge with Web Access. Refer to the P2000 Software User Manual for assistance.

➤ **To print and/or encode a badge:**

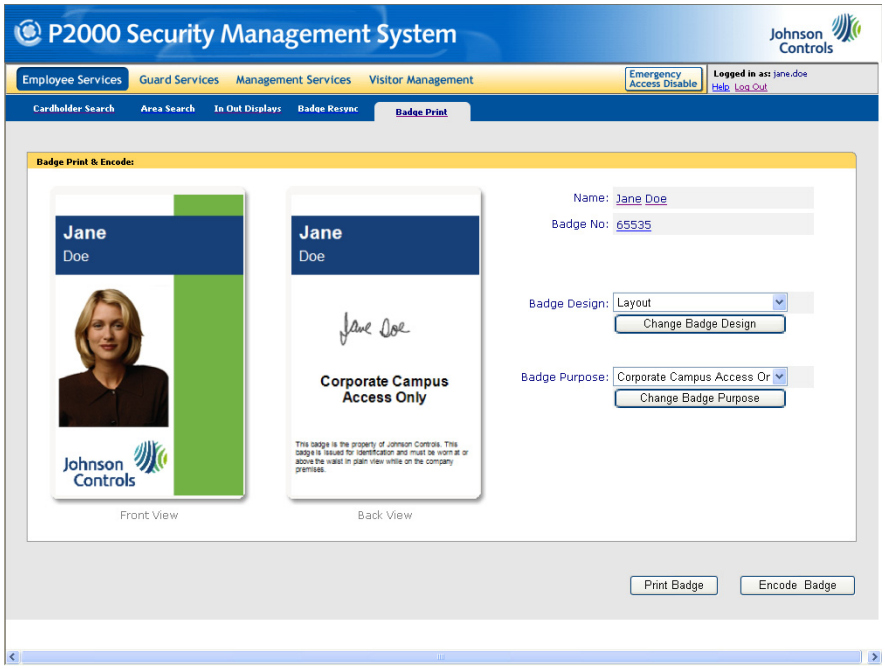
1. Use the Cardholder Search feature to locate the cardholder whose badge you wish to print and/or encode. See "Searching Cardholder Records" on page 3-1.

NOTE

*You may also search for cardholder records for purposes of printing and encoding badges by selecting the **Badge Print** tab (see page 3-15).*

2. On the Cardholder Info page, click **Print & Encode Badge**.

   The Badge Print & Encode page appears.



This screen displays the following:

- A preview of the badge (front and back) as it will appear when printed.
- The name of the associated cardholder. Clicking the name returns you to the Cardholder Info page.
- The badge number, which when clicked opens the Badge Info page.
- The current badge design assigned to the cardholder. To change it, select a new design from the **Badge Design** drop-down list and click **Change Badge Design**. The badge preview refreshes and displays the badge with the new design.
- The current purpose assigned to the badge (if the **BadgePurpose** field has been added to the badge layout). You can assign a different purpose to the badge, if desired. To assign a different purpose, select the new purpose from the **Badge Purpose** drop-down list and click **Change Badge Purpose**.

3. Click **Print Badge** to print the badge.

NOTE

The badge printer must be set as the default printer. Refer to your Microsoft Windows documentation for instructions on setting a default printer.

4. If encoding a badge, place the card on top of the encoder.
5. Click **Encode Badge**. If the card was encoded successfully, a message appears to indicate it.

NOTE

If you receive an error, see "Troubleshooting" on page 2-11 for assistance.

Area Search

Use this feature to view which P2000 cardholders currently occupy a specific area controlled by the P2000 Security Management System. Results are based on where the cardholder's badge was last presented.

NOTE

Only areas controlled by both an entry and exit reader can be used to determine whether someone actually occupies the area. If the area does not have an exit reader, you will be unable to use Web Access to determine when the cardholders leave, unless they badge at another reader.

With the Area Search feature, you may view all of the cardholders in a selected area, or you may search for specific cardholders in an area based on basic or advanced search criteria.

➤ To search an area:

1. Select the **Area Search** option. The Area Search page appears.

2. Perform one of the following actions:
   - Select one or more areas and click **Search** to view all of the cardholders who currently occupy the selected area(s).
   - To search for a specific cardholder in an area, enter the cardholder's first, middle and/or last name, select an area, and click **Search**.
   - Click the **Advanced Search** link, search by other area and cardholder criteria listed below, and click **Search**:
     - Cardholder ID
     - Badge Number
     - Department
     - Company

- Drivers License or License Plate, if defined as user-defined fields (UDF) in P2000 (see note on page 3-2)

3. The Area Search Results page appears, displaying the cardholder(s) in the selected area(s).

4. You may view information on a particular cardholder listed in your search by clicking the cardholder name (see “Viewing Cardholder Information” on page 3-5 for details).

In/Out Status

This feature enables you to see which P2000 cardholders are currently **In** or **Out** of the facility, or specific areas of the facility, based on their badge activity. If a cardholder has badged at the facility today (assuming the reset time is set to 12:00 AM), his/her status will be *In*. If a cardholder has not badged at the facility today, his/her status will be *Out*.

NOTE

Depending on your system’s configuration, you may or may not be able to assign areas when viewing the In/Out status of cardholders.

The In/Out status is determined by the time a cardholder badges at the facility or area and the reset time. If the reset time is set to 12:00 AM (the default setting), all cardholders who badge at the facility will be listed as *In*. At 12:00 AM, all the cardholders’ status will be reset to *Out*. See Figure 3-1.

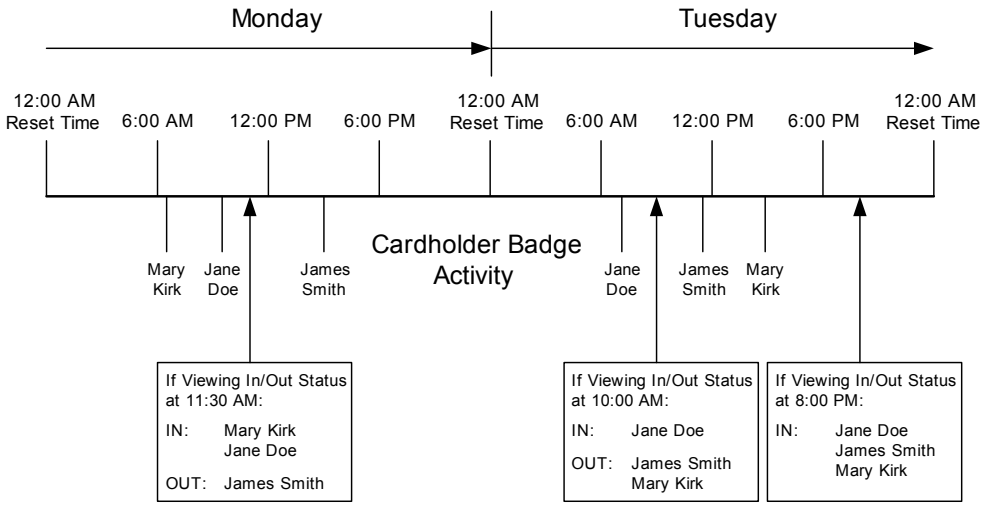
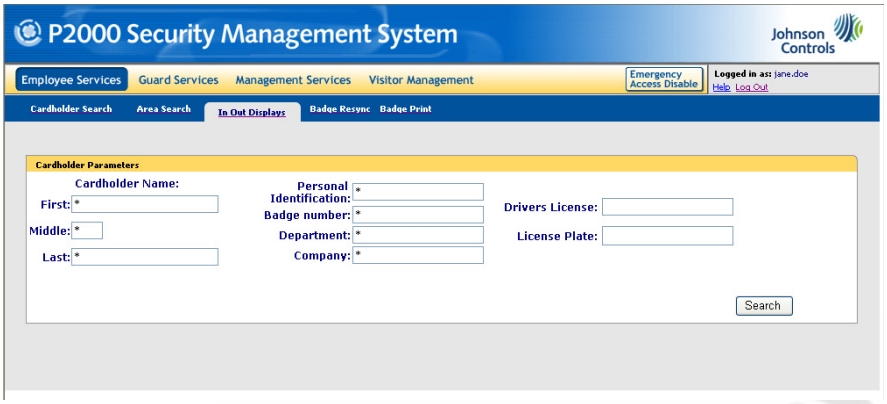


Figure 3-1: In/Out Status Reset - How it Works

➤ To view the in/out status of cardholders:

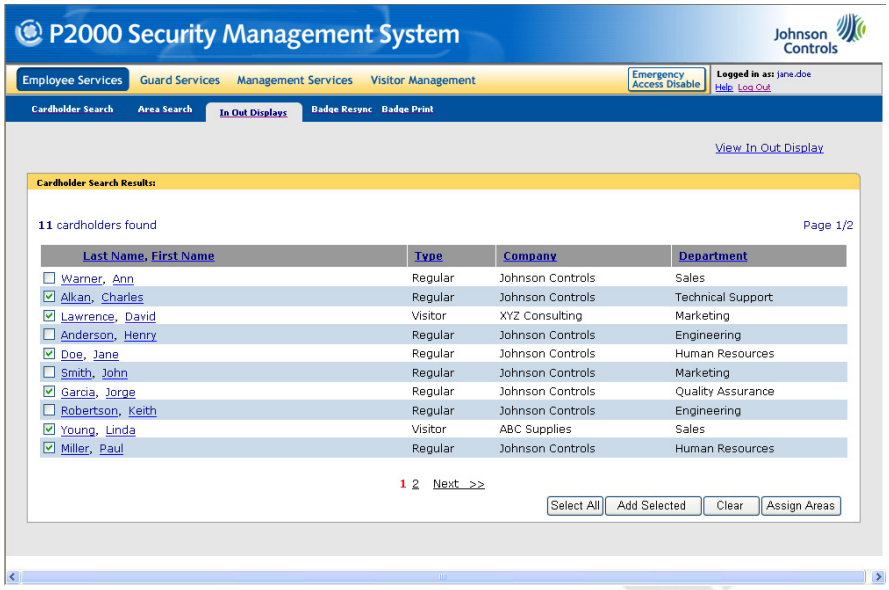
1. Select the **Employee Services** option.
2. Select the **In Out Displays** tab. The Cardholder Search page appears.



3. To locate specific cardholders, enter data into the search criteria fields (for example, cardholder name, badge number, etc.).
4. Click **Search**. The Cardholder Search Results page appears.
5. Click the **Add Cardholders to In Out Display** link. Check boxes appear next to the each cardholder's name.

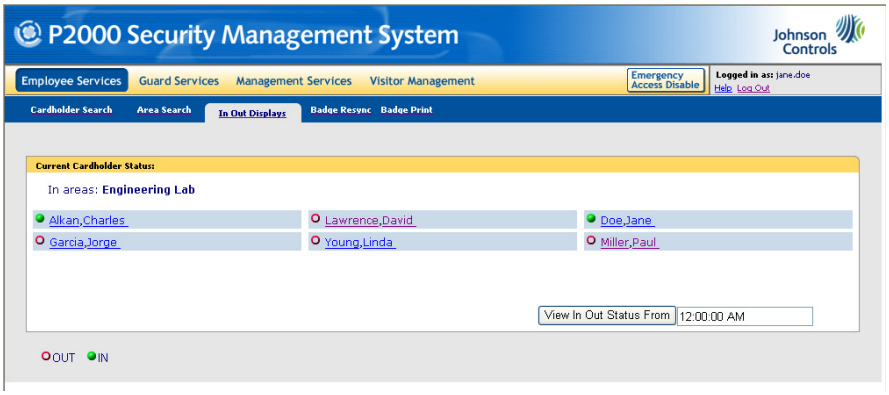
6. Select the check box next to each cardholder whose In/Out status you wish to view.

7. Click the **Add Selected** button, or click the **Select All** button to select all of the cardholders located in the search.



8. To assign areas, click the **Assign Areas** button, select the check box next to the area(s) you wish to assign, and click **Add Selected Areas to In Out Display**. By assigning areas, you can view which cardholders currently occupy a specific area of the facility.

9. Click the **View In Out Display** link. The Current Cardholder Status page appears.



- If the system detected badge activity from any of the selected cardholders from the **View In Out Status From** time to the current time, the cardholders will be listed as *In* (a green bullet will appear next to their name).
- If the system **did not** detect badge activity from any of the selected cardholders from the **View In Out Status From** time to the current time, the cardholders will be listed as *Out* (a red bullet will appear next to their name).

NOTE

*The View In Out Status From time resets the cardholder In/Out status. For example, if the View In Out From time is 12:00:00 AM and Cardholder A badges at 08:00:00 AM that same day, he/she will be **In**. The next day (starting at 12:00:00 AM), Cardholder A will be **Out** until he/she badges again (presumably at 8:00:00 AM).*

- To change the View In Out Status From time, enter the new time and click the **View In Out Status From** button. Enter the time in the following format: hh:mm:ss, where hh = hour, mm = minutes, and ss = seconds.
- To view cardholder data, click the cardholder's name to open the Cardholder Info page. See "Viewing Cardholder Information" on page 3-5 for more information.

Badge Resync

Entry and Exit terminals require cardholders to enter and exit an area in sequence. That is, when cardholders badge in at an entry terminal to enter a secured area, they must badge out to exit the secured area. If, for example, they follow another cardholder out without swiping their badge, it will remain in the *In* state

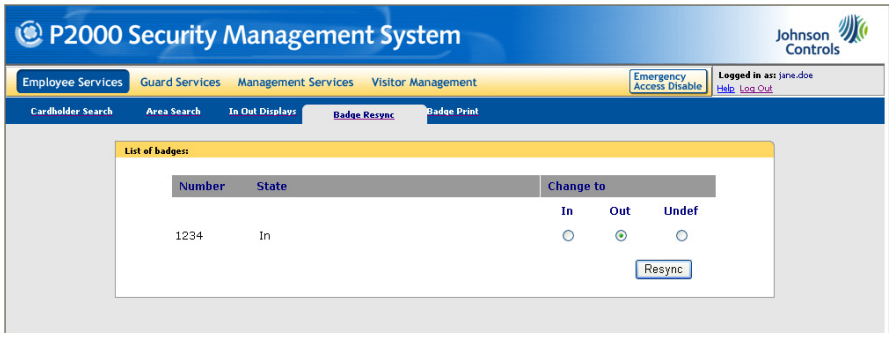
(out-of-sync). When they attempt to badge back into the area, they will be denied access. The Web Access Badge Resync enables you to request a Badge Resync, which will return your badge to its correct state if it is out-of-sync.

NOTE

You can only resynchronize your own badge (not the badge of another cardholder).

➤ To resync your badge(s):

1. Select the **Employee Services** option.
2. Select the **Badge Resync** tab. The Badge Resync page appears, displaying a record of each badge assigned to you.



3. Select the appropriate radio button, **In** or **Out**, to change the status of the badge, or select **Undefined** so that next badge swipe will redefine the badge for the appropriate action. For example, if you are outside of the secured area and your badge is set to **Undefined**, the next time you badge to enter the secured area, your badge status will automatically change to **In**.
4. Click **Resync**.

NOTE

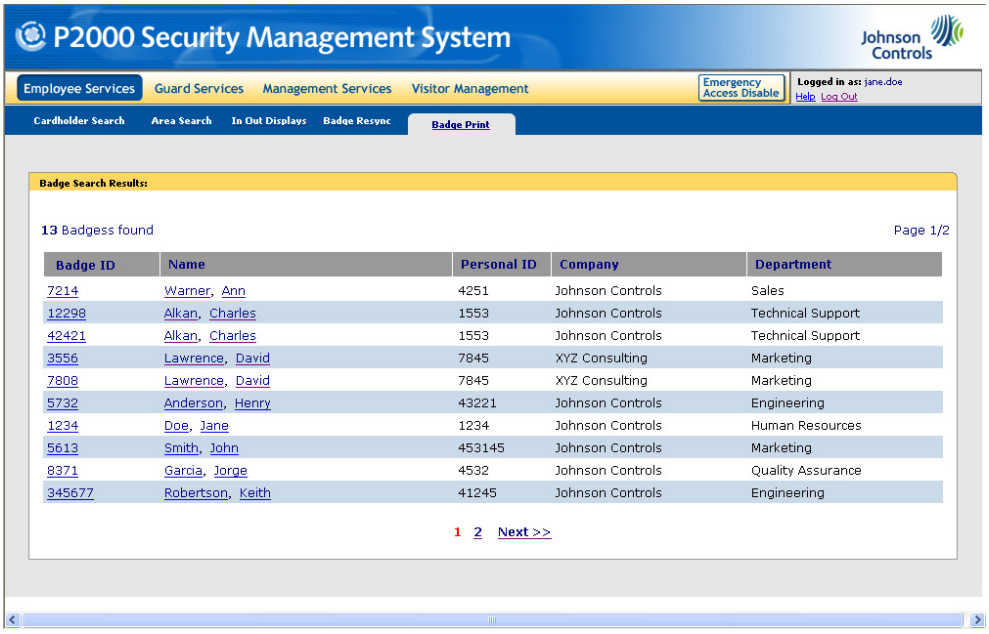
After you click Resync, you must refresh your browser screen for the Badge Resync page to display the updated badge state.

Badge Print

Similar to the Cardholder Search tab, the Badge Print tab enables you to locate cardholder records using various search filters. After you perform a search, Web Access lists the badge ID number, cardholder name, personal identification number, company, and department of each cardholder record located in the search.

- To preview, print, and/or encode a cardholder's badge, click the cardholder's badge ID number. See "Printing and Encoding Badges" on page 3-8 for more information.

- To view cardholder information, click the cardholder's name. See "Viewing Cardholder Information" on page 3-5 for more information.



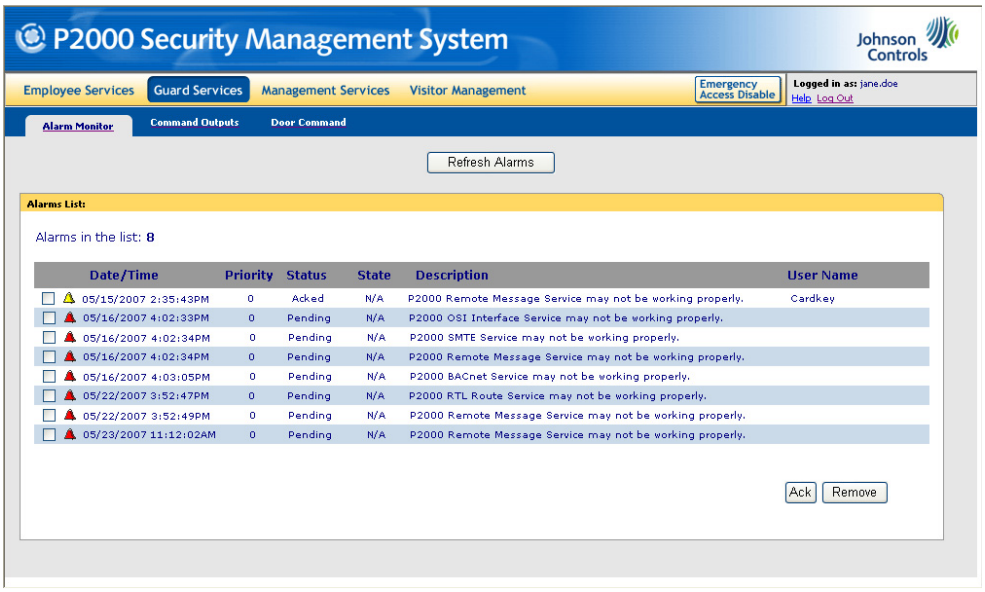
GUARD SERVICES

These services allow you to perform a number of guard-related actions, such as:

- Monitoring, acknowledging and discarding alarms
- Manually activating or deactivating output points (for example, turning on lights, activating a siren, etc.) (see page 3-19)
- Locking or unlocking doors, or timing the doors to lock/unlock after a user-defined number of minutes (see page 3-20)

Alarm Monitoring

P2000 alarms can be monitored, acknowledged and removed from the Web Access Alarm Monitor page. To access this page, select the **Guard Services** option. The **Alarm Monitor** page will appear by default.



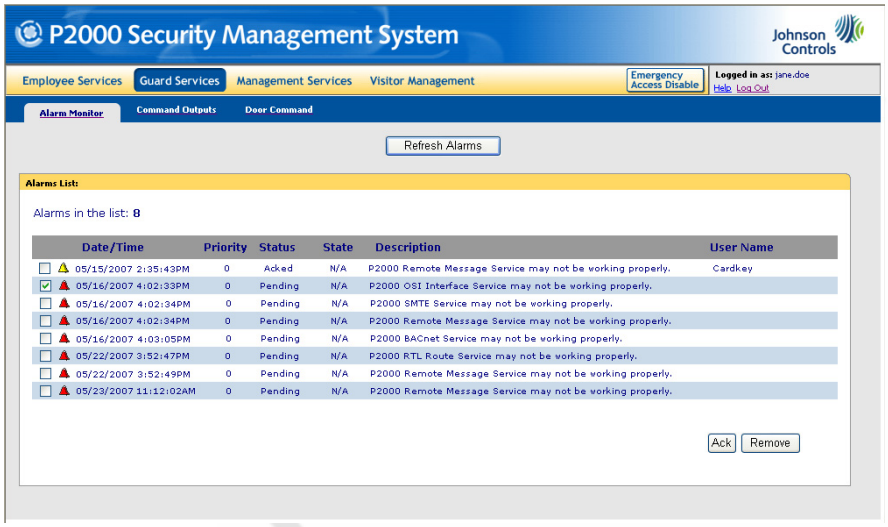
All pending alarm messages remain in the Alarm Queue until acknowledged and removed by a P2000 operator or Web Access user. You may only remove alarms in a *Secure* or *N/A* state.

Acknowledging an Alarm

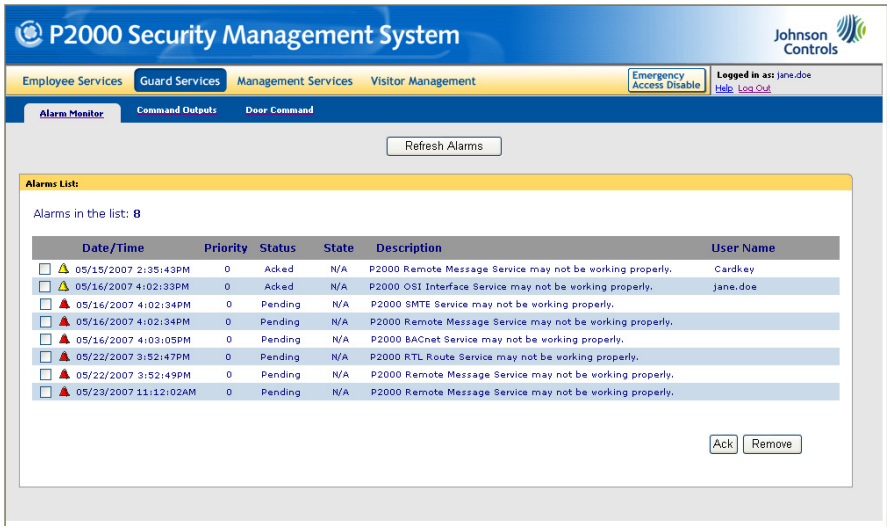
A P2000 operator or Web Access user may be required to acknowledge a new alarm as soon as it is received. They may do so and then return later to actually remove the alarm, depending on company policy and the priorities assigned to that alarm. The time and date of the acknowledgment is recorded in the P2000 alarm history.

➤ To acknowledge an alarm:

1. Select the check box next to the alarm you wish to acknowledge.



2. Click **Ack**. The red bell icon next to the alarm message will change to a yellow bell.



Removing an Alarm

According to company policy, Web Access users may remove completed alarms from the alarm queue. The alarm response sequence will remain in the P2000 alarm history record.

➤ To remove an alarm:

1. Select the check box next to the alarm you wish to remove. This alarm must be in a *Secure* or *N/A* state.
2. Click **Remove**. The alarm message will be removed from the Alarm Queue.

Alarm Monitor Definitions

Date/Time – Displays the date and time the alarm was reported to the system. Alarms that are originated at remote sites with different geographical time zones display the actual time at the remote site.

Priority – Displays the Alarm Priority set in P2000 (the highest is "0").

Status – Displays the status of the alarm.

- **Pending** – Not yet acknowledged.
- **Acked** – Acknowledged but no action taken.
- **Responding** – Acknowledged and response action in progress.

NOTE

You cannot respond to or complete an alarm from Web Access. These actions can only be performed in P2000.

State – Indicates one of the following alarm states: Secure, Alarm, Open, or Short.

Description – Description of the element that activated the alarm.

User Name – Name of the Web Access user or P2000 operator who handles the alarm.

Refreshing the Alarm Monitor Page

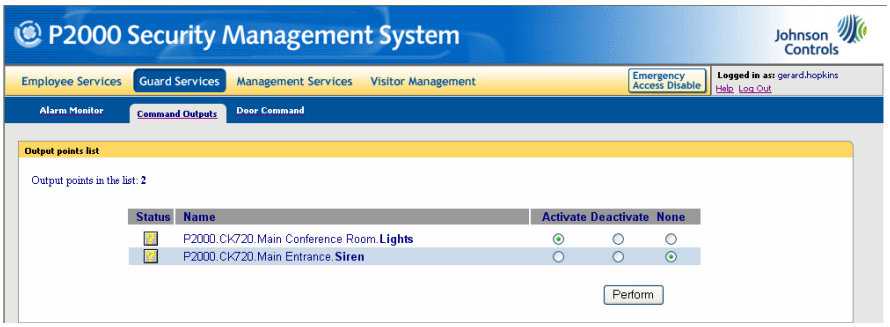
Click the **Refresh Alarms** button to display the current list of alarms in P2000 that have not been removed from the alarm queue.

Activating or Deactivating Output Points

Output Points are switches that control devices connected to them such as lights, air conditioning, alarm annunciators, parking barriers, and so on. Output Points can be activated (energized) or deactivated (de-energized) from Web Access.

➤ **To activate or deactivate an output point:**

1. Select the **Guard Services** option.
2. Select the **Command Outputs** tab. The Command Outputs page appears.



3. Select the **Activate** or **Deactivate** radio button next to the output point to be affected.
4. Click **Perform** to energize (activate) or de-energize (deactivate) the output point relay.

Output Point Definitions

Status – Displays the current status of the output point.

Status Unknown – Output relay status is unknown.

Output Reset – Output point relay is energized.

Output Set – Output relay is de-energized.

Name – Displays the site, panel, area, and output point affected.

Example: *P2000.CK720.Main Conference Room.Lights*

Site = P2000

Panel = CK720

Area = Main Conference Room

Output Point = Lights

Sending Door Commands

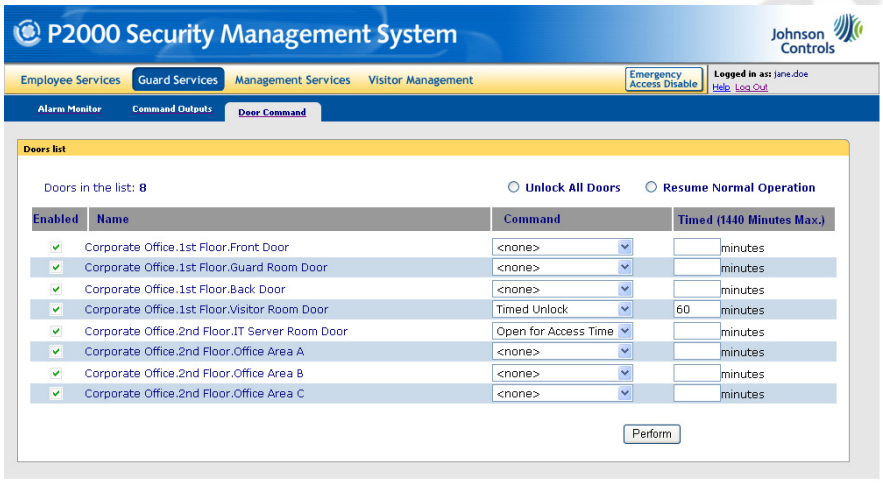
There may be instances when you may want to manually lock or unlock one or more doors of your building. For example, a cardholder has misplaced his card and wishes to access the building during off hours. You can manually unlock an entrance door via Web Access' door command feature to permit entry into the building.

The door commands available in Web Access are:

- **Unlock All Doors**
  Unlocks all of the doors controlled by the P2000.
- **Resume Normal Operation**
  Returns all of the doors controlled by the P2000 to their original state.
- **Lockout**
  Prevents access by all badges at the door (supported only by OSI controllers).
- **Open for Access Time**
  Unlocks the door for the amount of time set in the P2000 software as the door's Access Time. This time is not configurable using Web Access.
- **Timed Unlock**
  Unlocks the selected door for the number of minutes specified in the **Timed (1440 Minutes Max.)** field. Once the time expires, the door relocks.

➤ To perform a door command:

1. Select the **Guard Services** option followed by the **Door Command** tab. The Door Command page appears.



2. Select the desired door command(s). If selecting a Timed Unlock command for a specific door, enter the number of minutes the door will remain unlocked.

NOTE

The Name column lists each door according to the associated site, panel and terminal (for example, P2000.CK720.Cafeteria).

3. Click **Perform**.

MANAGEMENT SERVICES

These services allow you to perform a number of Web Access management-related actions, such as:

- Viewing and/or canceling requests
- Approving or rejecting requests (see page 3-23)
- Editing a rejected request (see page 3-26)
- Adding a cardholder (see page 3-26)
- Editing or deleting a cardholder (see page 3-35)
- Validating requests (see page 3-44)
- Auditing operator actions (see page 3-49)
- Installing and running the WebUSB application (see page 2-3)

Viewing and Canceling Requests

When Web Access operators submit requests, the system sends them to the Request Queue and assigns a status. The status varies, depending on whether approvers are defined for the request, or whether validation is required. For example, a request with no defined approvers and set to automatic processing will be added to the queue with a status of *Committed*. The request has been processed and finalized.

Other requests may require approvers and/or validation before they can be finalized. For a more thorough description of the request process, see the "Request Process Flow Chart" on page 1-11 and "Process States" on page 1-13.

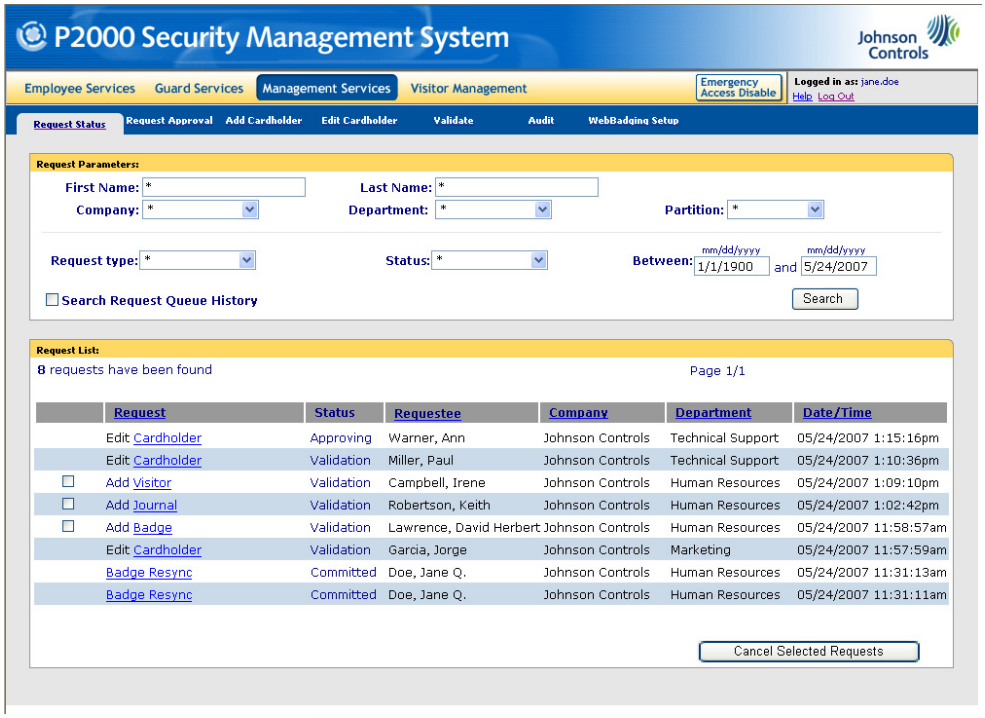
This section describes how to view and/or cancel requests in the Request Queue.

NOTE

Depending on how the P2000 menu permission groups are defined, requests submitted by a Web Access user assigned to a different company and/or department may not be visible. Refer to the P2000 Software User Manual for more detailed information on menu permission groups.

Viewing Requests

To view requests in the Request Queue, select the **Management Services** option. The Request Status page appears.



The requests are listed in the Request List box. The table in this box includes the following columns of data:

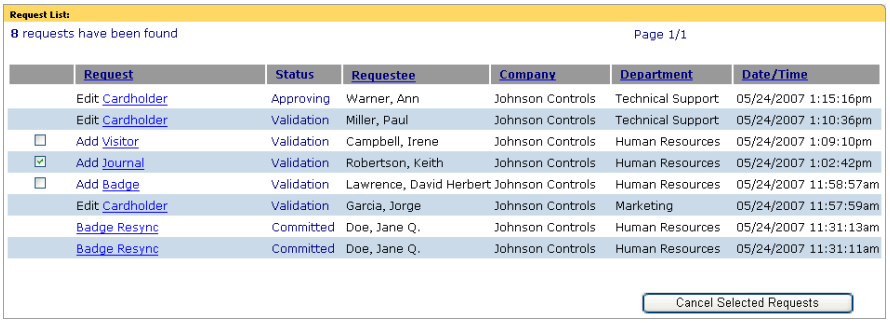
- **Request** – Type of request. Click the link to view detailed request information.
- **Status** – Request status. For a description of the different request states, see "Process States" on page 1-13.
- **Requestee** – Cardholder or visitor affected by the request.
- **Company** – Company assigned to the user who submitted the request.
- **Department** – Department assigned to the user who submitted the request.
- **Date/Time** – Date and time the request was submitted.

Canceling Requests

You may cancel a request you submitted before the system processes it. The system adds a cancelled request to the Request History, where it remains with a status of *Cancelled*. You cannot edit a cancelled request for re-submittal.

➤ **To cancel a request:**

1. Select the **Management Services** option. The Request Status page appears.
2. In the Request List box, select the check box next to the request you wish to cancel.



NOTE

You cannot cancel requests submitted by another user.

3. Click the **Cancel Selected Requests** button. The system changes the status of the request to *Canceled*.

Approving or Rejecting Requests

Depending on settings defined in P2000, each Web Access request may require up to three active approvers. The approver is a cardholder assigned Web Request Approval menu permissions. Approvers are ordered in a sequence and approve requests in the same order.

Administrators can define up to three approvers to approve a request before it can be validated and processed. For example, P2000 has three approvers defined: John (Level 1), Mary (Level 2), and Bob (Level 3). When a request is submitted, John approves the request first via Web Access or E-mail (if E-mail notification is enabled in P2000). After John approves the request, Mary can approve it by the same means. Once Mary approves the request, Bob can approve it to complete the approval process.

NOTE

For information on configuring approval levels, refer to the P2000 Software User Manual.

Any one of the three approvers can reject the request, which changes the request status to *Rejected*. A rejected request can be edited for re-submittal. An approved request must then be validated (if required) before it can be processed. If validation is not required, an approved request will be processed.

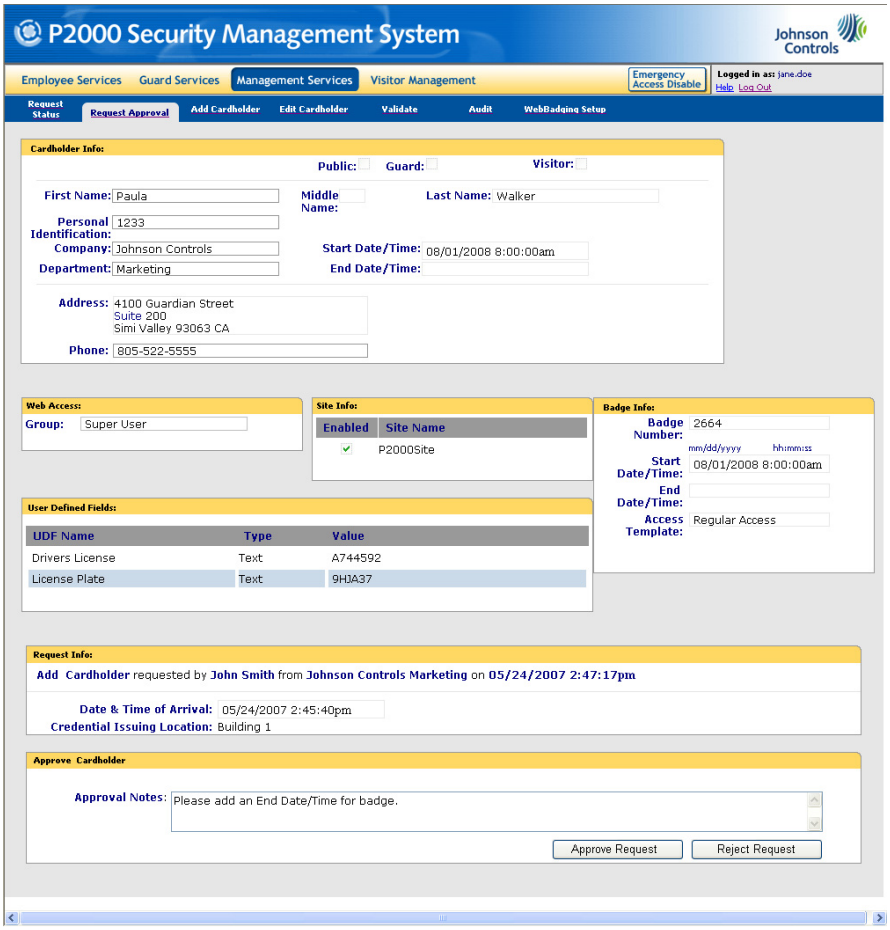
Requests can be approved via Web Access or E-mail notification. If E-mail notification is used, an E-mail is sent to an approver when a qualifying request is submitted. This E-mail allows the recipient approver to link to the Approval page of the specific request, where the approver can review the request and approve or reject it. Whether approved or rejected, another E-mail is sent to the requestor, notifying him/her of the approver action.

For a more thorough description of the request process, see the "Request Process Flow Chart" on page 1-11 and "Process States" on page 1-13.

➤ To approve or reject a request via Web Access:

1. Select the **Management Services** option.
2. Click the **Request Approval** tab. If any requests require your approval, they will appear on the Request Approval page. You will only see requests that you are allowed to approve.

3. Click **Select** next to the request you wish to approve or reject.
4. Review the request and enter any **Approval Notes,** if applicable. Approval Notes are especially useful if you wish to explain why you are rejecting a request or to request additional information.



5. Click **Approve Request** or **Reject Request**. The request will be removed from the Pending Approval List box.

➤ To approve or reject a request via E-mail notification:

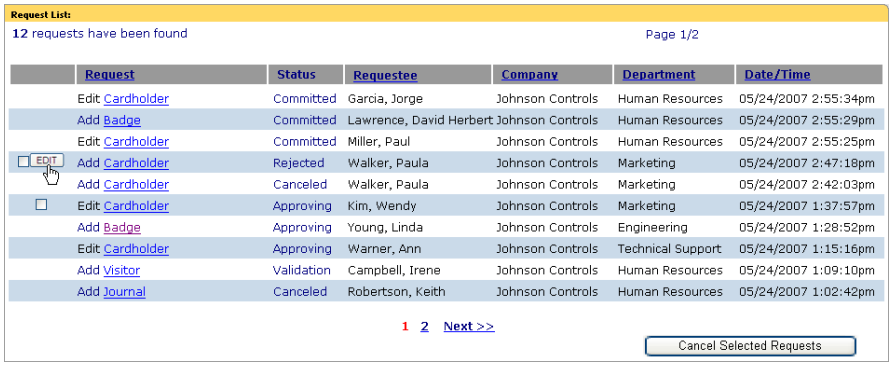
1. Open the E-mail notification.
2. Click the hyperlink provided in the E-mail.
3. Log in to Web Access, if prompted.

   The Approval page appears, displaying information specific to the request.
4. Review the request and enter any **Approval Notes,** if applicable. Approval Notes are especially useful if you wish to explain why you are rejecting a request.
5. Click **Approve Request** or **Reject Request**. The request will be removed from the Pending Approval List box.

Editing a Rejected Request

If a request is rejected, the requestor can edit the request for re-submittal. To edit a rejected request:

1. Select the **Request Status** tab.
2. Click the **Edit** button next to the rejected request you wish to edit and re-submit.



3. Edit the request and re-submit it.

Adding a Cardholder

Every person who needs access to the facility must have a cardholder and badge record entered into the P2000 system. This includes regular cardholders, such as full-time workers or contractors, and visitors. Web Access enables you to send a request to add a cardholder to the P2000 system. Security Managers with the proper permissions can approve or deny the request.

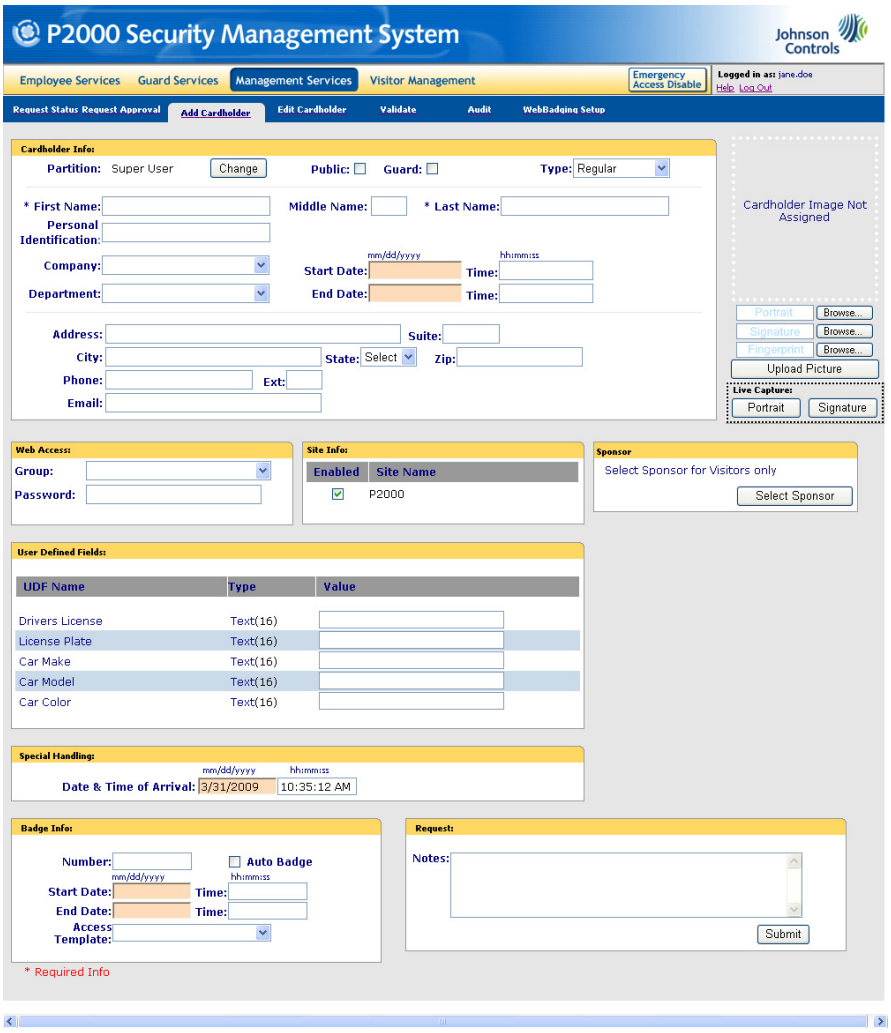
NOTE

All fields marked with an asterisk require data to be entered before the request can be submitted. Required fields for the Add Cardholder application are defined using the P2000 host software. For more information, refer to the P2000 Software User Manual.

➤ To add a cardholder:

1. Select the **Management Services** option.

2. Click **Add Cardholder**. The New Cardholder page appears.



3. Enter data into the **Cardholder Info** box, as described in "Cardholder Info Field Definitions" on page 3-29.
4. To import a cardholder image, such as a portrait, fingerprint, or signature image, click one of the **Browse** buttons to the right of the **Cardholder Info** box. See "Uploading a Cardholder Image" on page 3-30 for more information.

   If your Web Access computer is configured for Web badging, click the **Portrait** or **Signature** button inside the **Live Capture** box to capture a cardholder portrait or signature image. See "Capturing a Live Cardholder Image" on page 3-31 for more information.
5. To give the cardholder rights to use Web Access, in the **Web Access** box, select a **Group** and enter a **Password**.

   The Group field determines the Web Access permission group (the access rights) of the cardholder. The cardholder will use the password entered to log on to Web Access. To restrict the cardholder from having access to the Web Access application, leave these fields blank.

6. The **Site Info** box appears only with Enterprise Systems. By default, the site is enabled, meaning the new cardholder record will be visible in Web Access. Do not clear the **Enabled** check box unless you want to add the cardholder record into the site's database as disabled.
7. If the cardholder is a visitor, click the **Select Sponsor** button in the Sponsor box to assign a sponsor. The sponsor is the cardholder who is responsible for the visitor. See "Selecting a Sponsor" on page 3-32 for more information.

NOTE

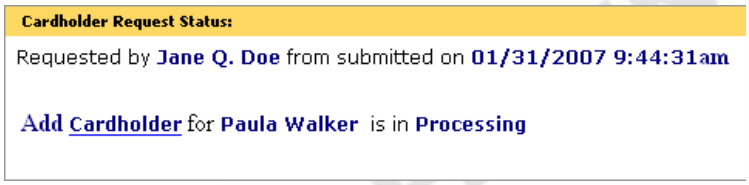
*In order to select a sponsor, the **Visitor** option must be selected from the **Type** drop-down list.*

8. Enter values in the **User Defined Fields** box, if applicable. See "User-Defined Fields (UDF)" on page 3-33 for more information.
9. In the **Special Handling** area, enter the cardholder's date and time of arrival. If the P2000 has multiple badging locations, select the **Credential Issuing Location** (the badging station that will be used to print the cardholder's badge.

NOTE

Badging stations are defined in the P2000 host software on the System Configuration window. To define a badging location, a workstation must be defined as a badging station and a description must be entered in the Location field. If no badging location is entered, the Credential Issuing Location field does not appear. Refer to the P2000 Software User Manual for more information on defining a P2000 workstation as a badging station.

10. Enter badge information into the **Badge Info** box. See "Entering Badge Information" on page 3-34 for more information.
11. Enter additional information or instructions about the request into the **Notes** field, if applicable.
12. Click **Submit**. If the cardholder is successfully submitted, the Cardholder Request Status box appears, showing request details such as the cardholder's name, the request type, and the current processing status.



Cardholder Info Field Definitions

Partition – If this is a partitioned system, click the **Change** button and select the Partition to assign to the cardholder. This field is not visible in a non-partitioned system.

Public – Select to make the cardholder record visible to all partitions. This field is not visible in a non-partitioned system.

Guard – Used to assign Tour Badges to cardholders who will participate in guard tour operations.

Type – Select Regular or Visitor. If you select Visitor, the Sponsor box becomes activated.

First Name – (Required) Enter the cardholder's first name.

Middle Name – Enter the cardholder's middle initial.

Last Name – (Required) Enter the cardholder's last name.

Personal Identification – Enter a unique ID for this individual (up to 25 characters).

Company / Department – Assign a company and department to the cardholder. Companies and departments are created in P2000. Refer to the *P2000 Software User Manual* for detailed information.

Start Date/Time – Date and time when all badges for this cardholder become active. To enter a date, click inside the field and select the date from the drop-down calendar. Enter the time in the following format:

hh:mm:ss AM or PM
hh = hour, mm = minutes, ss = seconds
Example: 08:00:00 AM

End Date/Time – Date and time when all badges for this cardholder expire. Enter the date and time as described in Start Date/Time above.

The End Time field is typically used for Visitor badges, but can also be edited, as needed, to void badges for a terminated employee or similar application. The system automatically voids the badge(s) on the date and time specified.

NOTE
If you create a Visitor badge and do not enter an End Date/Time, the date and time defaults to the Visitor Validity Period value specified in P2000's Site Parameters setting. Refer to the P2000 Software User Manual for detailed information.

Address – These entries are optional. Enter the suite, street, city, state, zip, phone number, and extension, if desired.

Email – Enter the cardholder's email address.

Uploading a Cardholder Image

Web Access allows you to upload a cardholder image, such as a portrait, fingerprint, and signature, for the new record. These images are visible when viewing the cardholder record in Web Access or P2000, and can be printed on the cardholder's badge from a P2000 Video Imaging station or from the Web Access computer (if configured for Web Badging – see "Chapter 2: Web Badging Configuration"). Refer also to the *P2000 Video Imaging Manual* for more information.

P2000 Web Access supports the following image formats: JPEG, GIF, and BMP. If Web Access does not support the format of the image you wish to import, use an image editing program to convert the image to a supported format.

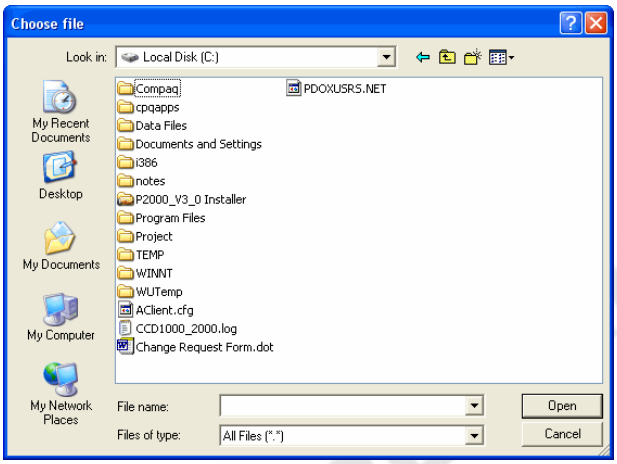
NOTE

The file size of each image cannot exceed 1 MB. Also, Web Access displays the imported image in an aspect ratio of 164 x 200 pixels for portraits and fingerprints and 320 x 160 pixels for signatures. If the image does not fit this ratio, Web Access will resize it accordingly. After the resizing occurs, the image may appear distorted. If this occurs, use an image editing application to edit the image, as necessary.

➤ **To upload a cardholder image:**

1. Click one of the **Browse** buttons to the right of the Cardholder Info box. You may import up to three cardholder images.
   - Click the top Browse button to import a **portrait** image.
   - Click the middle Browse button to import a **signature** image.
   - Click the bottom Browse button to import a **fingerprint** image.

   The Choose File dialog box appears.



2. Locate and select the image file to import.
3. Click **Open**. The directory path to the file appears in the field next to the **Browse** button.

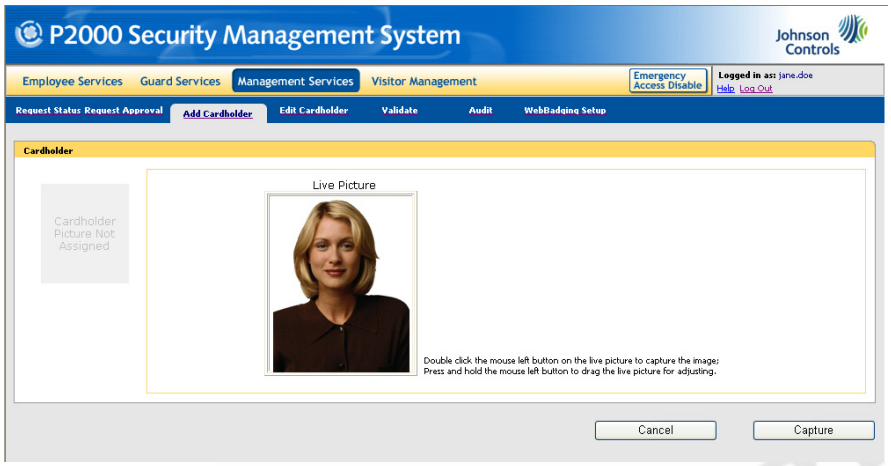
4. Repeat steps 1-3 for each image you wish to upload.
5. Click **Upload Picture**.
6. View the appearance of each uploaded image for approval before continuing. Use a bitmap editing program to edit an image, if necessary, and re-upload it until you are satisfied with its appearance.

Capturing a Live Cardholder Image

Web Access supports the ability to capture live cardholder portrait and signature images directly from the Web Access computer. To capture a live cardholder image, first configure your Web Access computer for Web Badging. See "Chapter 2: Web Badging Configuration" for more information.

➤ **To capture a live cardholder *portrait* image:**

1. On the Add Cardholder screen, click the **Portrait** button in the **Live Capture** box. The Live Capture page appears.
2. Wait until the cardholder's face is correctly positioned and aligned with the camera. To adjust the position of the image, with your mouse, click and drag inside the picture frame. To freeze the image, double-click inside the picture frame. To clear the image, double-click inside the picture frame.



NOTE

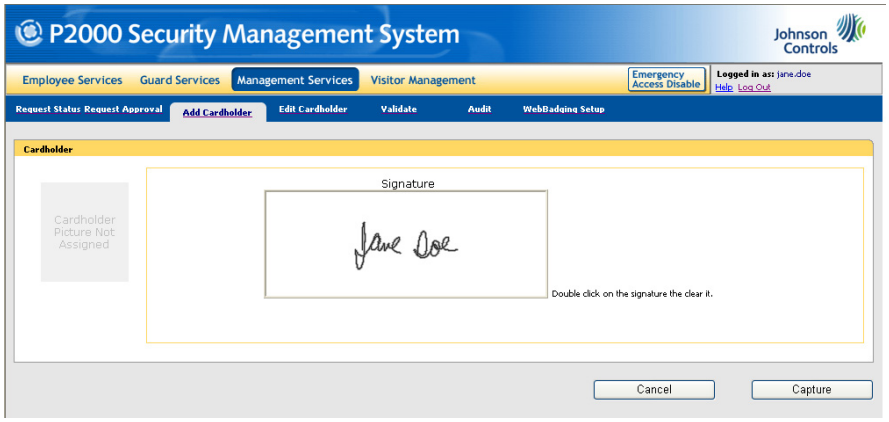
If the capture device fails to capture the desired image, see "Troubleshooting" on page 2-11 for assistance.

3. Click **Capture** to capture the image or **Cancel** to return to the Add Cardholder page. The captured image appears on the Add Cardholder page, above the associated Browse button.

➤ **To capture a live cardholder *signature* image:**

1. On the Add Cardholder screen, click the **Signature** button in the **Live Capture** box. The Live Capture page appears.

2. Click inside the signature frame. Then instruct the cardholder to sign his/her name on the signature pad. A signature image should appear in the signature frame. To clear the image, double-click inside the Signature frame.



NOTE

If the capture device fails to capture the desired image, see "Troubleshooting" on page 2-11 for assistance.

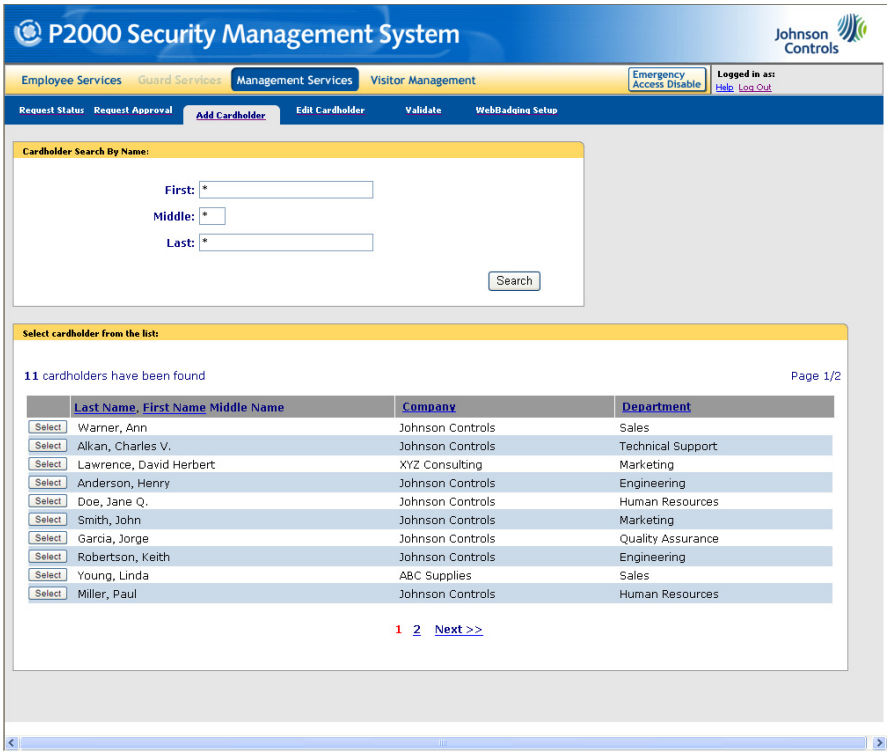
3. Click **Capture** to capture the image or **Cancel** to return to the Add Cardholder page. The captured images appear on the Add Cardholder page, above the associated Browse button.

Selecting a Sponsor

You can select a sponsor when requesting to add a visitor. A sponsor is a cardholder who is responsible for the visitor.

1. Verify that **Visitor** is selected in the **Type** drop-down list when adding or editing a cardholder. You cannot assign a sponsor to a regular cardholder.

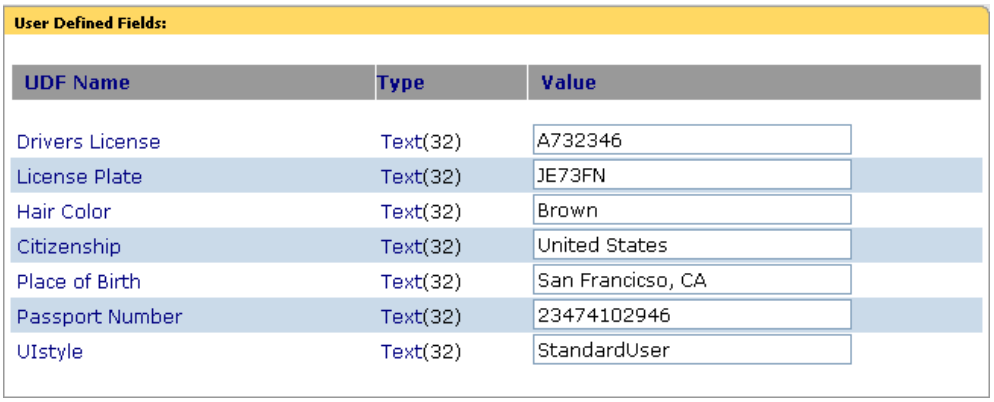
2. In the **Sponsor** box, click the **Select Sponsor** button. The Cardholder List page appears.



3. Locate the cardholder whom you will assign as the sponsor. Use the name search fields, if necessary.
4. Click the **Select** button next to the sponsor. The selected cardholder will be listed in the **Sponsor** box.

User-Defined Fields (UDF)

UDFs created in P2000 appear on the Add Cardholder and Edit Cardholder pages. Enter a value, if applicable, for the UDFs listed in the **User Defined Fields** box.



User Defined Fields:

UDF Name	Type	Value
Drivers License	Text(32)	A732346
License Plate	Text(32)	JE73FN
Hair Color	Text(32)	Brown
Citizenship	Text(32)	United States
Place of Birth	Text(32)	San Francicso, CA
Passport Number	Text(32)	23474102946
UIstyle	Text(32)	StandardUser

Each UDF consists of a name, field type (for example, text, numeric, etc.), field width (the number of characters allowed) and a user-entered value.

NOTE

The number next to the UDF type (for example, Text(32)) determines the maximum number of characters that can be entered for that UDF value.

NOTE

When a P2000 operator processes a visitor from the P2000 host software using the Visitor Request Management application, P2000 automatically creates the following UDFs: ***Approved Visits****,* ***Most Recent Visit****,* ***Second Most Recent Visit****, and* ***Third Most Recent Visit****. These UDFs allow P2000 operators to monitor the visits associated with a selected visitor. If these UDFs appear on the Add Cardholder page in Web Access, ignore them (do not enter any values). These UDFs are automatically updated based on the P2000 operator actions with the Visitor Request Management application.*

Entering Badge Information

Refer to the following information when entering badge information for a cardholder.

Number – Enter a badge number in this field or use the Auto Badge feature.

Auto Badge – If your facility is set up to use the AutoBadge Management feature, select the Auto Badge check box to insert the next available badge number in the Number field. The AutoBadge Management feature allows you to control and manage badge numbers within a defined pool. Once the pool of numbers is defined and you are issuing a badge, you can select the Auto Badge check box to insert the next available badge number in the Number field.

Start Date/Time – Date and time when this badge becomes active. To enter a date, click inside the field and select the date from the drop-down calendar. Enter the time in the following format:

hh:mm:ss AM or PM
hh = hour, mm = minutes, ss = seconds
Example: 08:00:00 AM

End Date/Time – Date and time when this badge expires. Enter the date and time as described in Start Date/Time above.

The End Time field is typically used for Visitor badges, but can also be edited as needed to void the badge for a terminated employee or similar application. The system automatically voids the badge on the date and time specified.

NOTE
If you create a Visitor badge and do not enter an End Date/Time, the date and time defaults to the Visitor Validity Period value specified in P2000's Site Parameters setting. Refer to the P2000 Software User Manual for detailed information.

Access Template – You may assign a badge to an Access Template, which contains preset badge options, access groups, and time zones. For detailed information, refer to the *P2000 Software User Manual*.

Editing a Cardholder

Follow the instructions in this section to edit a cardholder record using Web Access. Specifically, this section describes the following:

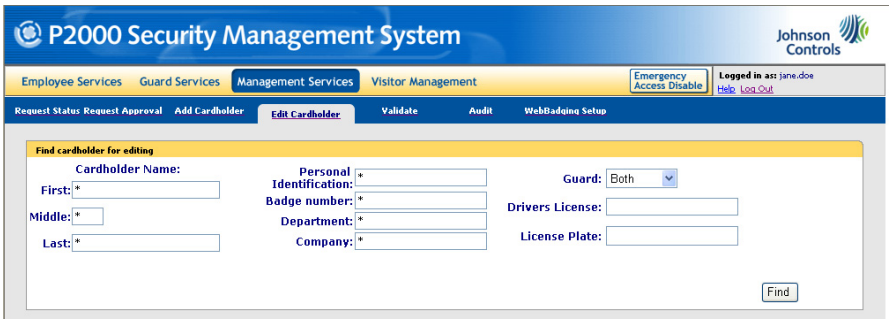
- Locating a cardholder record (see page 3-35)
- Editing or deleting a cardholder record (see page 3-36)
- Adding, editing or deleting cardholder journals (see page 3-38)
- Adding, editing or deleting a cardholder badge (see page 3-42)

Locating a Cardholder Record

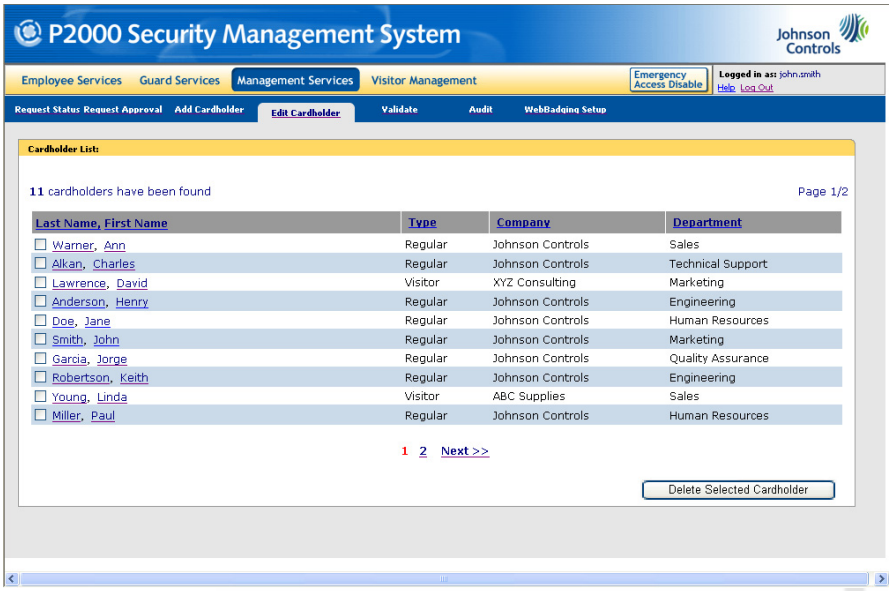
➤ **To locate a cardholder record:**

1. Select the **Management Services** option.

2. Click the **Edit Cardholder** tab. The Find Cardholder for Editing page appears.



3. Use the search fields to filter your search and locate the cardholder(s) you wish to edit.
4. Click **Find**. The Cardholder List page appears and displays a list of the located cardholders.

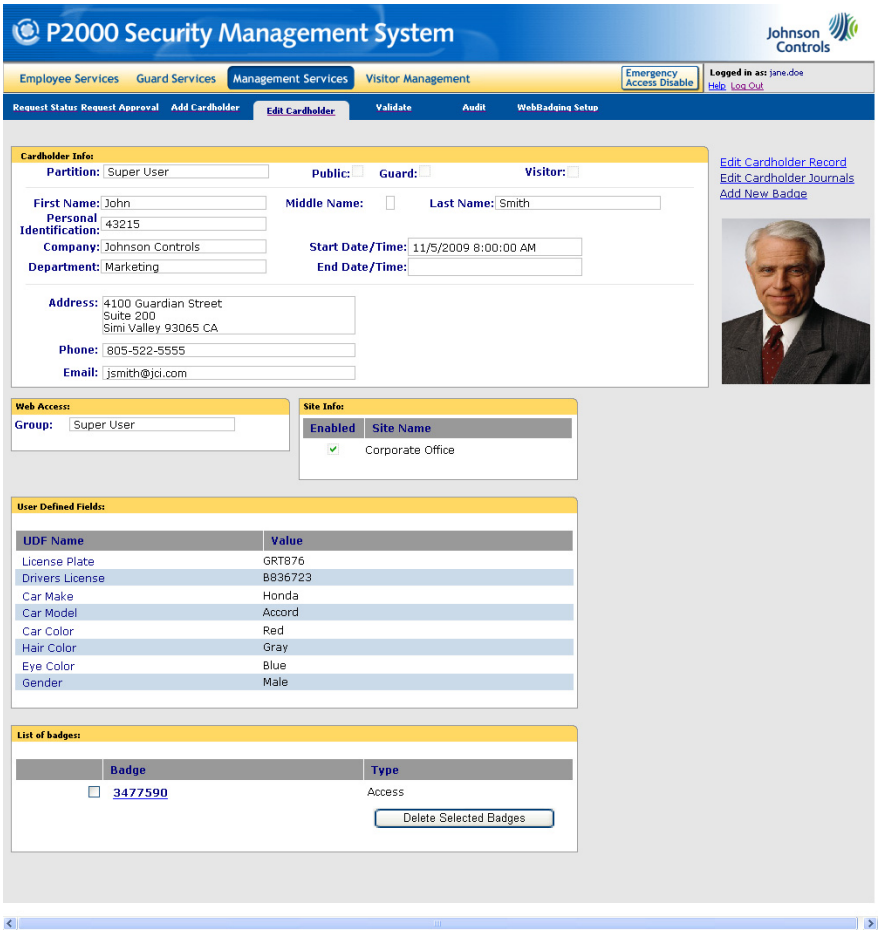


Editing or Deleting a Cardholder Record

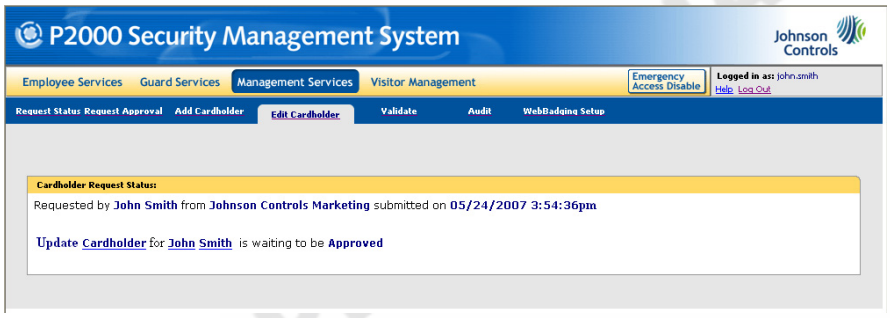
➤ To edit a cardholder record:

1. Locate a cardholder record to edit according to the instructions in “Locating a Cardholder Record” on page 3-35.

2. On the Cardholder List page, click the name of the cardholder you wish to edit. The Edit Cardholder page appears.



3. Click the **Edit Cardholder Record** link in the upper-right corner of the page.
4. Edit the cardholder record, as needed. See "Adding a Cardholder" on page 3-26 and its subsections for information on the cardholder fields.
5. Click **Submit Request**. The Cardholder Request Status box appears, displaying request specifics (for example, date and time submitted, requestor, request type, etc.).



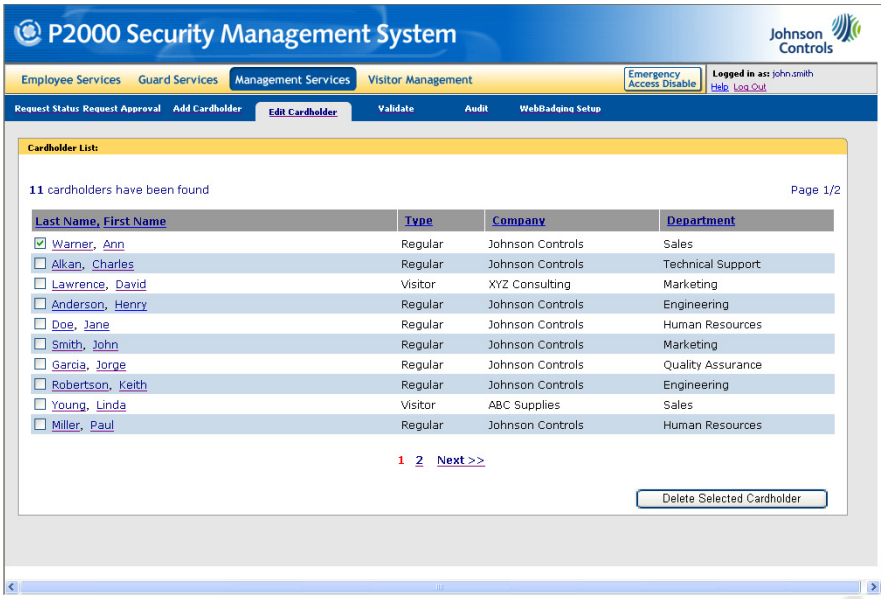
➤ **To delete a cardholder record:**

NOTE

When deleting a cardholder record from Web Access on a P2000 Enterprise system, the cardholder record and all associated badges will be deleted from all sites within the Enterprise system.

Refer to the P2000 Software User Manual for more information on managing cardholder records on multiple sites in a P2000 Enterprise system.

1. Locate a cardholder to delete according to the instructions in "Locating a Cardholder Record" on page 3-35.
2. On the Cardholder List page, select a check box next to each cardholder you wish to delete.



3. Click the **Delete Selected Cardholder** button. The check box is removed next to the cardholder(s) you have selected for deletion.

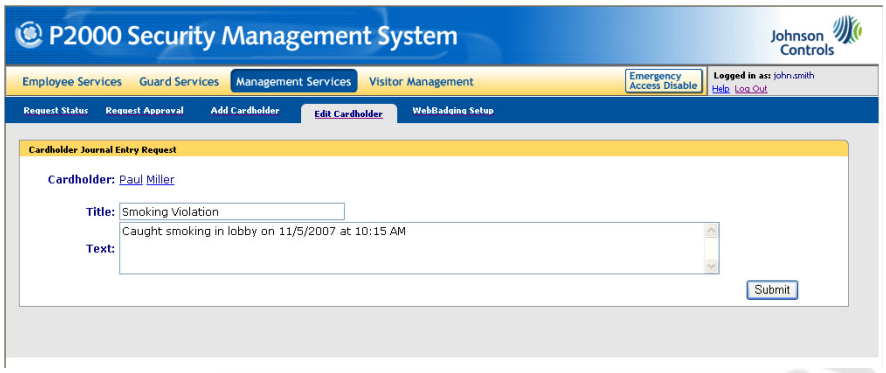
Adding, Editing or Deleting Cardholder Journal Entries

Journal entries supplement cardholder information by storing notes associated with each cardholder. For example, you can keep track of persons with parking violations, or keep a record of employees that attended specific company training, or record in writing suspicious behavior exhibited by tenants.

➤ To add a cardholder journal entry:

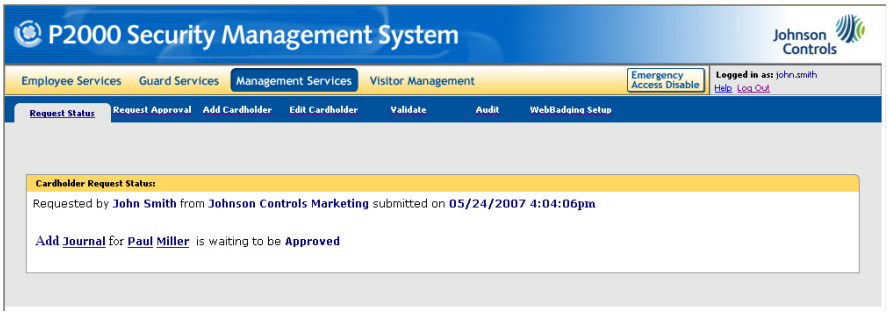
1. Locate a cardholder for whom you wish to add a journal entry. See “Locating a Cardholder Record” on page 3-35.
2. On the Cardholder List page, click the name of the cardholder for whom you will add a journal entry. The Edit Cardholder page appears (see page 3-37).
3. Click the **Edit Cardholder Journals** link in the upper-right corner of the page. The Cardholder Journal List page appears.

4. Click **Add New Journal**. The Cardholder Journal Entry Request page appears.



5. Enter a **Title** for the journal.
6. In the **Text** box, enter a description for the journal.

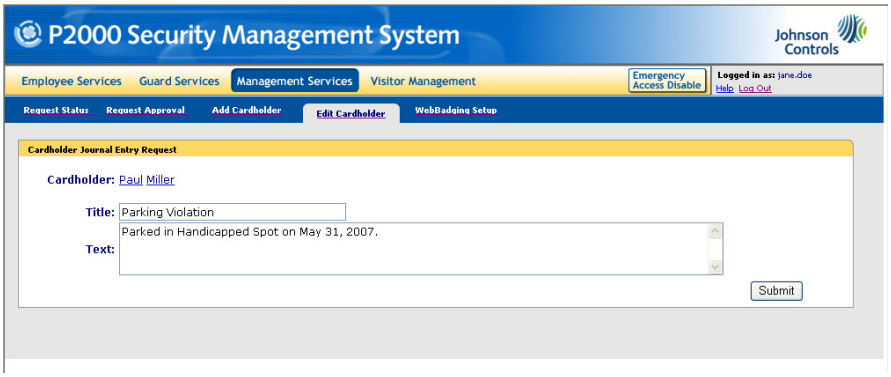
7. Click **Submit**. The Cardholder Request Status box appears, displaying request specifics (for example, date and time submitted, requestor, request type, etc.).



➤ To edit a cardholder journal entry:

1. Locate a cardholder whose journal entry you wish to edit. See “Locating a Cardholder Record” on page 3-35.
2. On the Cardholder List page, click the name of the cardholder whose journal entry you wish to edit. The Edit Cardholder page appears (see page 3-37).
3. Click the **Edit Cardholder Journals** link in the upper-right corner of the page. The Cardholder Journal List page appears.
4. Under the **Title** column, click the title of the journal you wish to edit.

The Cardholder Journal Entry Request page appears.



5. Edit the **Title** and/or **Text** of the journal and click **Submit**. The Cardholder Request Status box appears, displaying request specifics (for example, date and time submitted, requestor, request type, etc.).

➤ To delete a cardholder journal entry:

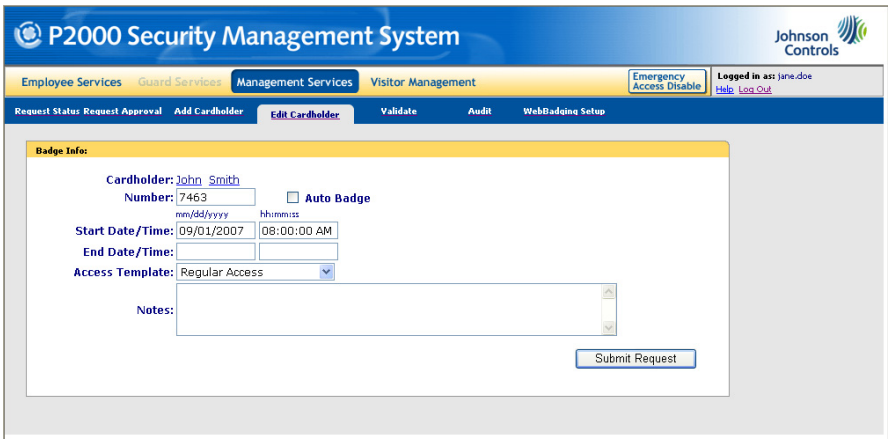
1. Locate a cardholder whose journal entry you wish to delete. See “Locating a Cardholder Record” on page 3-35.
2. On the Cardholder List page, click the name of the cardholder whose journal entry you wish to delete. The Edit Cardholder page appears (see page 3-37).
3. Click the **Edit Cardholder Journals** link in the upper-right corner of the page. The Cardholder Journal List page appears.
4. Select the check box next to each journal you wish to delete.

5. Click **Deleted Selected Journals**. A request submitted message appears below the Cardholder Journal List box.

Adding, Editing or Deleting Cardholder Badges

➤ To add a cardholder badge:

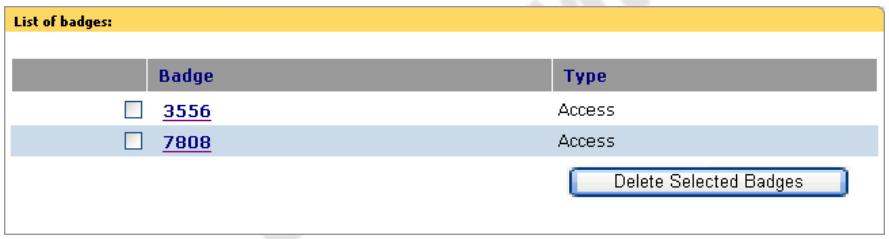
1. Locate a cardholder for whom you wish to add a badge. See “Locating a Cardholder Record” on page 3-35.
2. On the Cardholder List page, click the name of the cardholder for whom you will add a badge. The Edit Cardholder page appears (see page 3-37).
3. Click the **Add New Badge** link in the upper-right corner of the page. The Badge Info page appears.



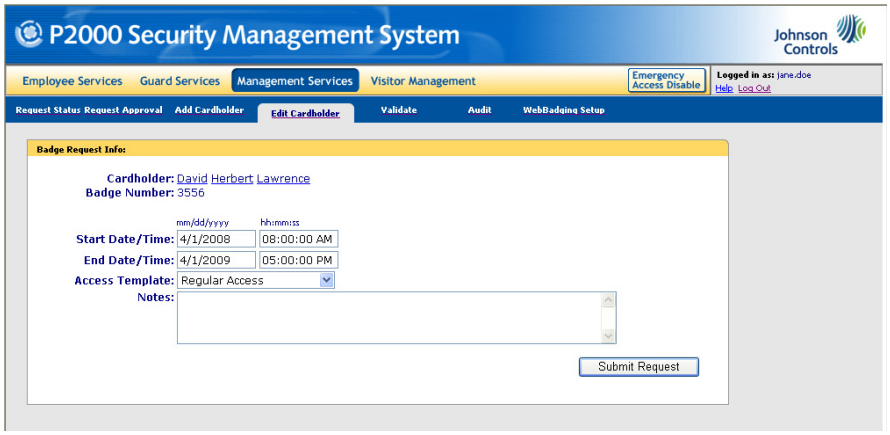
4. Enter badge information into the Badge Info fields. See “Entering Badge Information” on page 3-34 for detailed information about these fields.
5. Enter additional information or instructions about the request into the **Notes** field, if applicable.
6. Click **Submit Request**. The Cardholder Request Status box appears, displaying request specifics (for example, date and time submitted, requestor, request type, etc.).

➤ To edit a cardholder badge:

1. Locate a cardholder whose badge you wish to edit. See “Locating a Cardholder Record” on page 3-35.
2. On the Cardholder List page, click the name of the cardholder whose badge you wish to edit. The Edit Cardholder page appears (see page 3-37).
3. Scroll down to the **List of Badges** box.



4. Click the number of the badge you wish to edit. The Badge Request Info page appears.



5. Edit the badge information accordingly. See "Entering Badge Information" on page 3-34 for detailed information about the badge fields.
6. Click **Submit Request**. The Cardholder Request Status box appears, displaying request specifics (for example, date and time submitted, requestor, request type, etc.).

➤ To delete a cardholder badge:

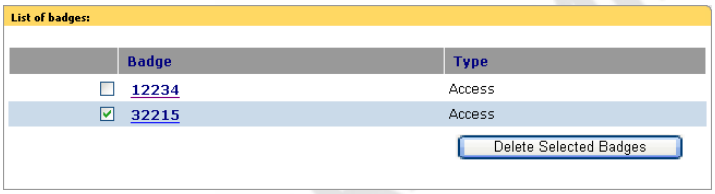
NOTE

When deleting a badge from Web Access:

- *On P2000 **non**-Enterprise systems, the badge will be deleted.*
- *On P2000 Enterprise systems, the badge will be **disabled** (not deleted).*

Refer to the P2000 Software User Manual for more information on managing badges on multiple sites in a P2000 Enterprise system.

1. Locate a cardholder whose badge you wish to delete. See "Locating a Cardholder Record" on page 3-35.
2. On the Cardholder List page, click the name of the cardholder whose badge you wish to delete. The Edit Cardholder page appears (see page 3-37).
3. Scroll down to the **List of Badges** box.



4. Select the check box next to each badge you wish to delete.
5. Click **Delete Selected Badges**.

Validating Requests

During the validation stage, users with proper menu permissions can process (approve) or reject a request configured for manual processing. Before processing the request, however, the same users may edit the request, if required. For example, if someone submits an Add Badge request without a start or end date, the user validating the request can add the dates before processing the request.

If the request is approved, the system will process and finalize it. A rejected request can be edited for re-submittal.

Before a request is approved or rejected, the requestor can cancel it. A cancelled request is stored in the Request History and cannot be edited for re-submittal.

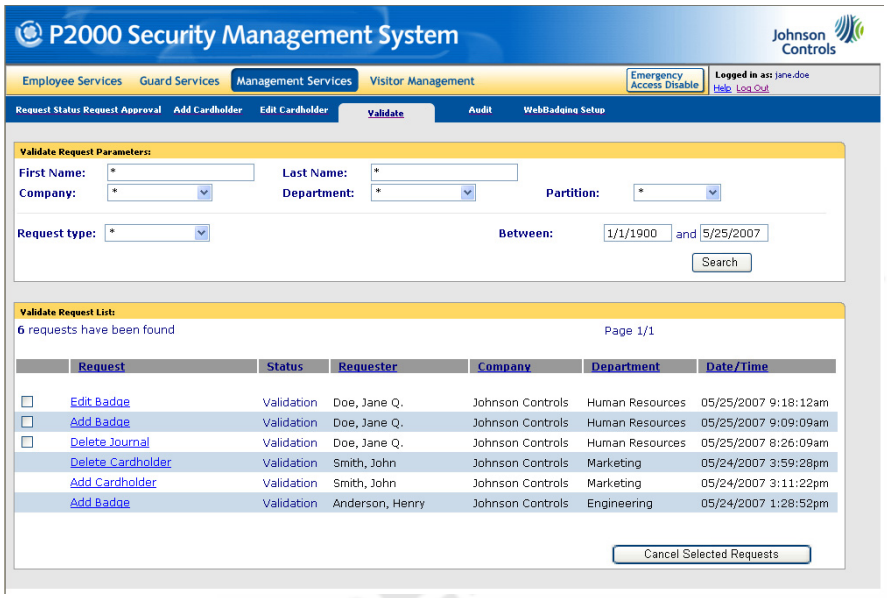
For a more thorough description of the request process, see the "Request Process Flow Chart" on page 1-11 and "Process States" on page 1-13.

NOTE

All requests to add a visitor must be validated by an authorized P2000 user from a P2000 server or workstation. Visitor requests cannot be validated using Web Access. Once an authorized user validates a visitor request, the system removes it from the Web Access Request Status page.

➤ To validate (process) or reject a request:

1. Click the **Management Services** option.
2. Select the **Validate** tab. The Validate page appears.

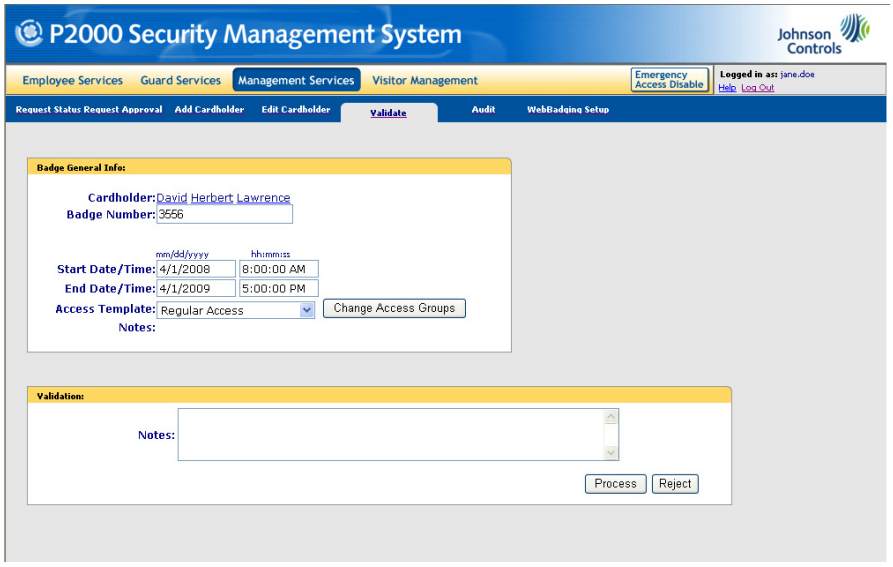


3. Locate the request you wish to validate. If necessary, enter the request information into the search fields and click **Search**. You may search by the following criteria:
   - First/Last Name

- Company
- Department
- Partition
- Request Type
- Request Submittal Date

4. Under the **Request** column, click the request type text of the request you wish to validate.

   A page displaying the request specifics appears (Edit Cardholder Badge shown).



5. Edit the request, if necessary.

   You may also edit the Access Groups associated with the Access Template for badge-related requests (see “Editing Access Groups During Validation” on page 3-46 for more information).

6. Enter validation **Notes**, if applicable. Validation Notes can be used, for example, to explain why you are rejecting a request or to request additional information.

7. Click **Process** or **Reject**.

➤ To cancel a request:

1. On the Validate page, select the check box next to each request you wish to cancel.
2. Click **Cancel Selected Requests**. The request is removed from the Validate page and stored in the Request History with a status of *Cancelled*.

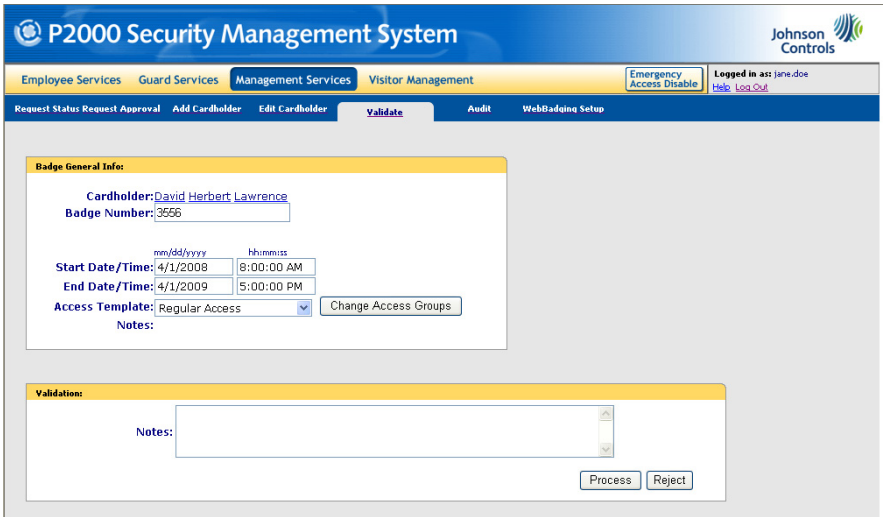
Editing Access Groups During Validation

When a Web Access user submits a badge or add cardholder request, he/she can assign an access template, which contains preset badge and security options, access groups, and time zones. During the validation process, users may edit the security options, access groups, and time zones associated with the selected access template.

For example, Joe (a Web Access user) submits a request to add a badge to an existing cardholder record (Jane). Joe assigns an access template, but adds a note that the badge should also allow Jane to access the Engineering lab. Currently, the access template assigned to the lab *would not* allow Jane to access the lab. Before processing the request, the person validating the request adds the access group that provides access to the Engineering lab.

➤ **To edit a badge's access groups and time zones during validation:**

1. Click the **Change Access Groups** button.

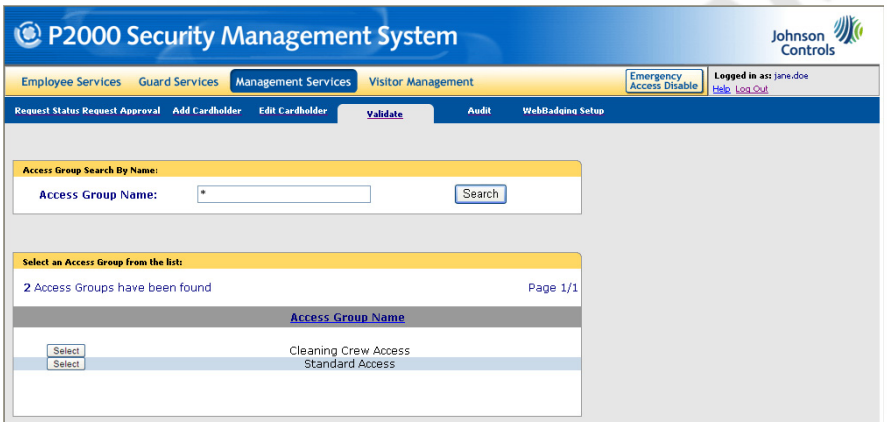


The Access Groups page appears.

NOTE

If the badge has one or more access groups and time zones assigned, they will be listed on the Access Groups page if no access template is selected on the Validation page.

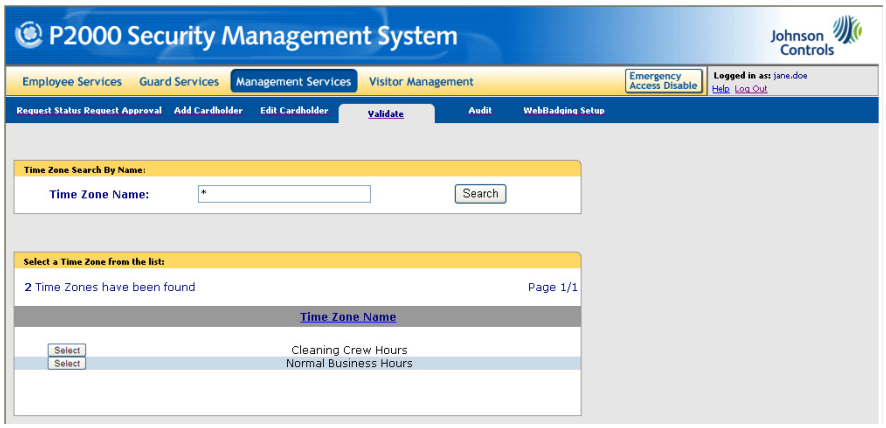
2. Select one or more check boxes at the top of the box to assign security options to the badge. For information on the P2000 security options, refer to the *P2000 Software User Manual*.
3. Select the check box next to the row where you will add or edit the access group and time zone.
4. Click **Select AccessGroup**. The Select Access Group page appears.



5. Locate the access group you wish to assign to the badge and click **Select**.

   The access group name will appear on the Access Groups page next to the selected check box.

6. Click **Select TimeZone**. The Select Time Zone page appears.



7. Locate the time zone you wish to assign to the access group and click **Select**.

   The time zone name will appear on the Access Groups page next to the access group.

8. Repeat steps 2 through 7 for each access group you wish to assign.

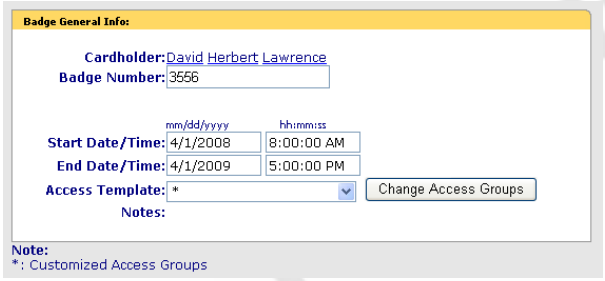
9. Use the Up/Down arrows to re-order the access groups and time zones accordingly.

   To re-order a row, select the check box next to the row you wish to re-order and click the Up or Down arrow in the row header.

NOTE

The order of the access groups determines which ones will be downloaded to the panel, starting with the group in the first row. If a panel can only receive two access groups per badge, then the access groups defined on rows 1 and 2 will be downloaded. For more information on the ordering of access groups, contact your P2000/Web Access administrator.

10. Click **Save and Return**. The Access Template field has an asterisk to denote that the access template has been customized.

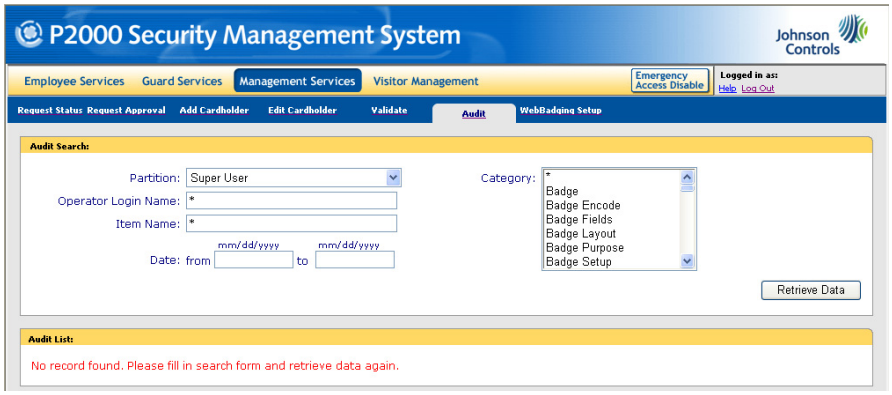


Auditing User Actions

Use this feature to track changes to the software based on who performed the action, the data affected by the action, the date and time the action occurred, and the action itself.

➤ To view audit data:

1. Click the **Management Services** option.
2. Select the **Audit** tab. The Audit page appears.



3. Select at least one item in the **Category** box. To select multiple items, hold down **<Shift>** or **<Ctrl>** on your keyboard.
4. Use the other search fields to restrict your search further, as necessary.
5. Click **Retrieve Data**.

   The Audit List box displays the results of the data retrieval.

6. Move from page to page with the links at the bottom of the grid. To increase or decrease the number of items in the list, click the up/down arrows on the right side of the column header bar.

VISITOR REQUESTS

Web Access allows you to request a badge for a visitor, so that it is ready upon his/her arrival. Simply enter the appropriate visitor data into the system, assign a visitor sponsor, and enter the date and time period of the scheduled visit. You can also enter notes relating to the visitor or request special handling (for example, wheelchair, coffee, tea, etc.).

Once a user submits a visitor request, Web Access adds it to the Request Queue. You may cancel your request from the queue, if necessary, but only an authorized person can approve and validate it. See “Request Process Flow Chart” on page 1-11 for more information on the request process.

NOTE

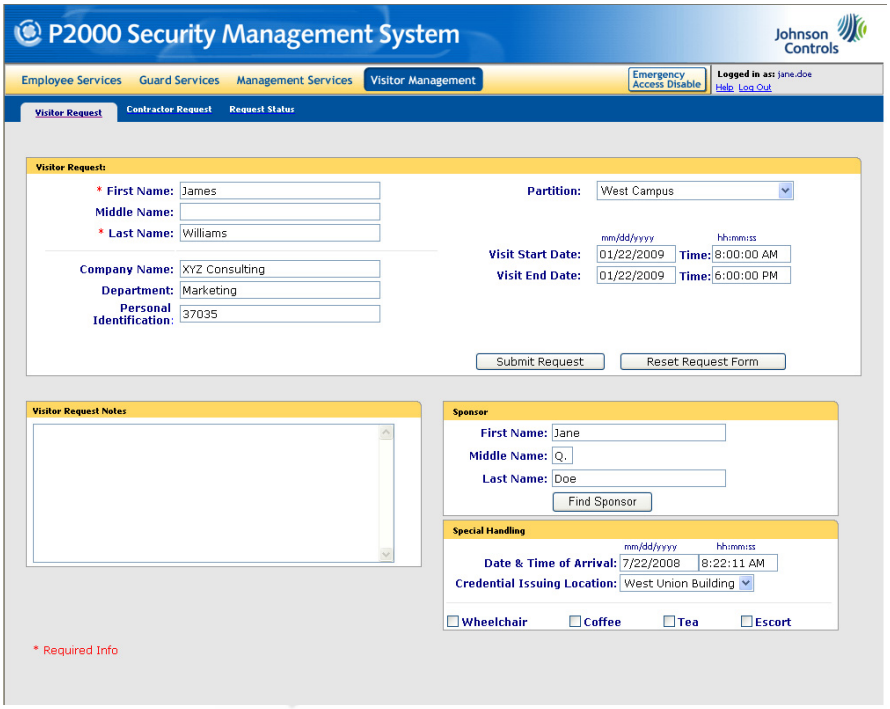
All requests to add a visitor must be validated by an authorized P2000 user from a P2000 server or workstation. Visitor requests cannot be validated using Web Access. Once a visitor request is validated, it is removed from the Web Access Request Status page.

NOTE

Users can add visitors using the New Cardholder page. See “Adding a Cardholder” on page 3-26 for detailed information.

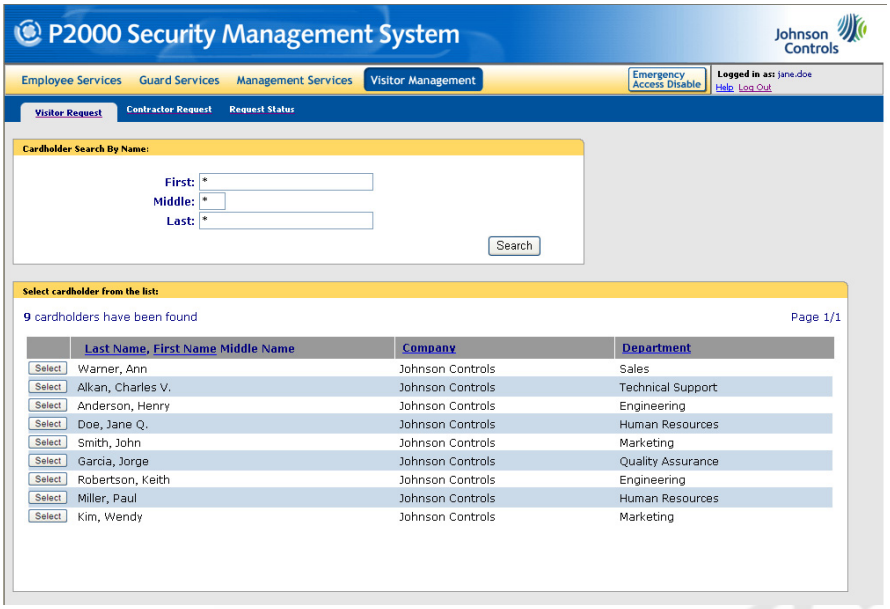
➤ To submit a visitor request:

1. Click the **Visitor Management** option. The Visitor Request page appears.



2. In the **Visitor Request** area, enter the visitor's name in the appropriate fields. The **First Name** and **Last Name** fields are required.
3. Enter the visitor's **Company Name**, **Department** and **Personal Identification** number, if applicable.
4. Select the **Partition** you wish to assign to the visitor.
5. Enter the visit period in the **Visit Start Date/Time** and the **Visit End Date/Time** fields. To enter a date, click inside the field and select the date from the drop-down calendar. Enter the time in the following format:

   hh:mm:ss AM or PM
   hh = hour, mm = minutes, ss = seconds
   Example: 08:00:00 AM
6. Enter any **Visitor Request Notes**, if applicable.
7. In the Sponsor area, Web Access adds your name as the default sponsor. You may select a different sponsor by clicking the **Sponsor** button and clicking the **Select** button next to the cardholder you wish to assign as the sponsor.



8. In the **Special Handling** area, enter the visitor's date and time of arrival. If the P2000 has multiple badging locations, select the **Credential Issuing Location** (the badging station that will print the badge for the visitor).

NOTE

*Badging stations are defined in the P2000 host software on the System Configuration window. To define a badging location, the P2000 administrator must define a workstation as a badging station and must enter a description in the **Location** field. If the administrator does not enter a badging location, the **Credential Issuing Location** field does not appear. Refer to the P2000 Software User Manual for more information on defining a P2000 workstation as a badging station.*

9. Select one or more check boxes that correspond to the type of handling the visitor requires (for example, Wheelchair, Coffee, Tea, Escort).
10. Click **Submit Request**.

    If successful, you will see the following message at the bottom-left corner of the page:

    "The request has been submitted successfully. You may make another visitor request."
11. To reset the request form to submit another visitor request, click the **Reset Request Form** button.

CONTRACTOR REQUESTS

Web Access enables you to send a request to change the validation period of one or more cardholder badges. Once you submit the request, Web Access adds it to the Request Queue. You may cancel your request from the queue, if necessary, but only an authorized person can approve and/or validate it. See "Request Process Flow Chart" on page 1-11 for more information on the request process.

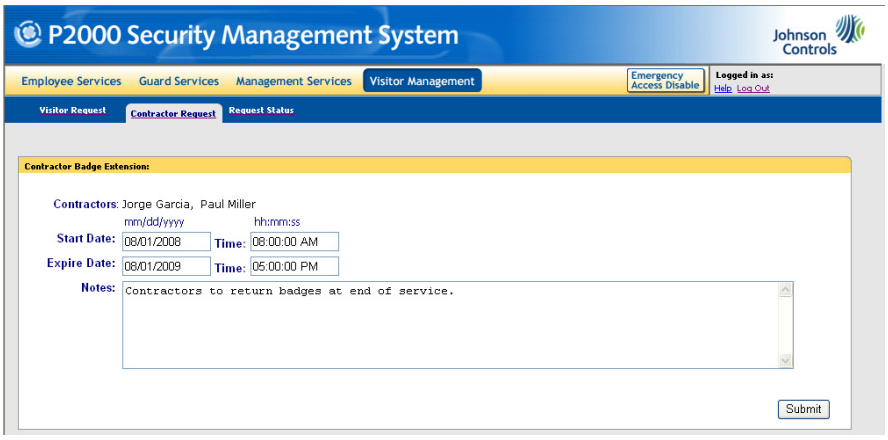
NOTE

You may only request to change the validation period of a cardholder badge if both you and the cardholder are assigned to the same company.

➤ To change a badge validation period:

1. Click the **Visitor Management** option. The Visitor Request page appears.
2. Click the **Contractor Request** tab to view a list of the cardholders in your company.

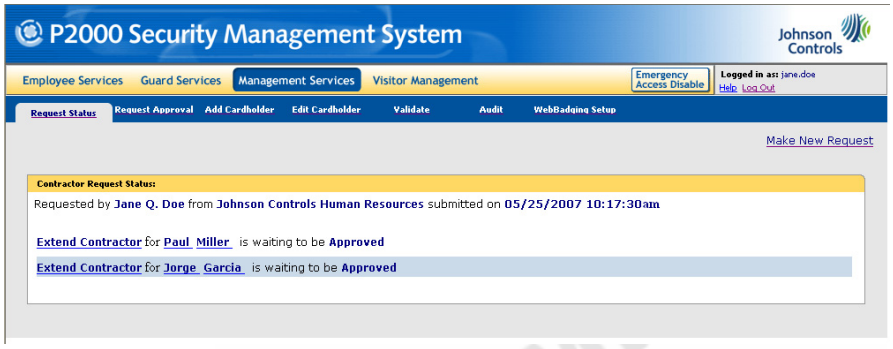
3. Select the check box(es) next to the cardholder(s) whose badge validation period you wish to extend.
4. Click **Proceed**. The Contractor Badge Extension page appears.



5. Enter the new validation period in the **Start Date/Time** and the **Expire Date/Time** fields. To enter a date, click inside the field and select the date from the drop-down calendar. Enter the time in the following format:

   hh:mm:ss AM or PM
   hh = hour, mm = minutes, ss = seconds
   Example: 08:00:00 AM
6. Enter any applicable notes.
7. Click **Submit**.

   The Contractor Request Status page appears and displays request information such as the requestor, department, date and time of request (in military time format), contractor, and request status (for example, Processing).



8. To submit a new request, click the **Make New Request** link in the upper-right corner of the page.

EMERGENCY ACCESS DISABLE

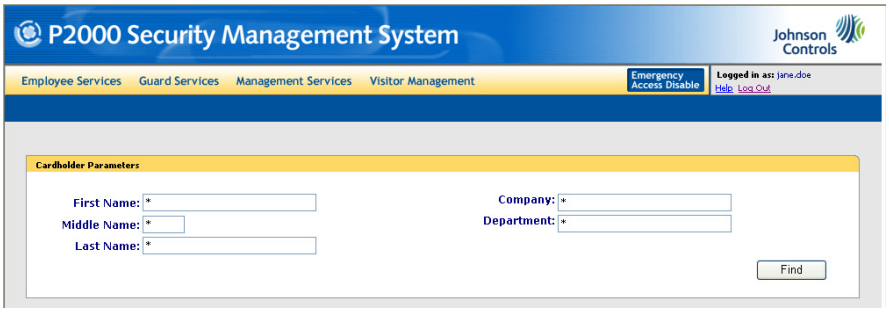
This feature enables you to immediately disable the account of a single cardholder, which disables all of the cardholder's badges and his/her ability to log into Web Access. A P2000 alarm is also generated. You can use this feature in various emergency situations. For example, if a worker threatens someone in the company, you can disable his account to prevent him from accessing the company building or complex.

NOTE

The Emergency Access Disable feature does not require approval or validation. Once a user submits the request, the selected cardholder account is immediately disabled.

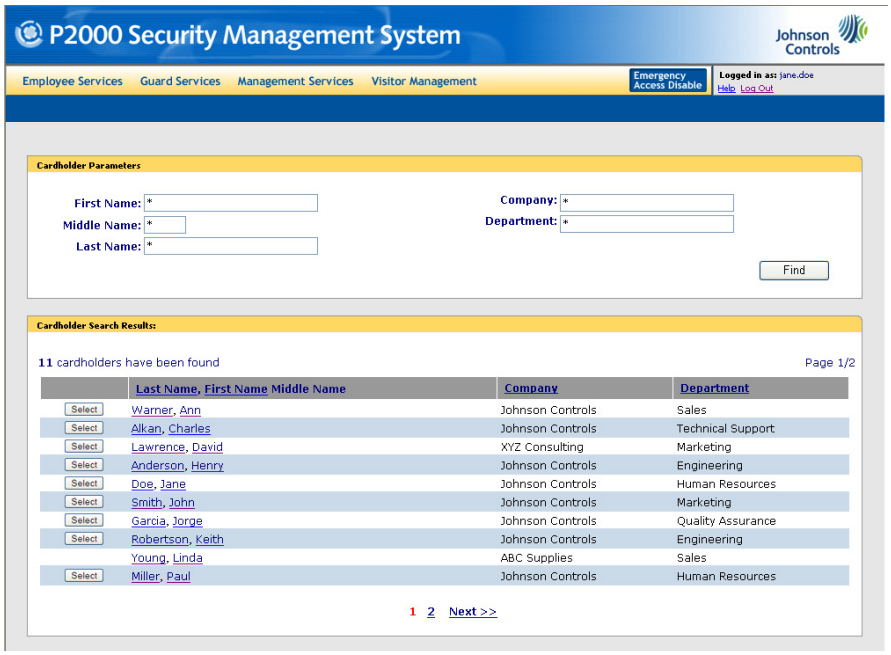
➤ To use the Emergency Access Disable feature:

1. On the Web Access Option bar, click **Emergency Access Disable**. The Cardholder Search page appears.

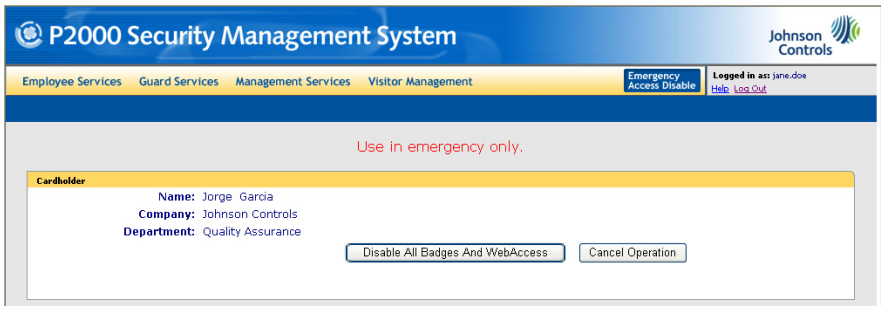


2. Enter data into the **Cardholder Parameters** text boxes to filter your search for the cardholder.

3. Click **Find**. The Cardholder Search Results box appears.



4. Click the **Select** button next to the cardholder account you wish to disable. The Disable Cardholder page appears.



5. Click the **Disable All Badges And WebAccess** button to disable the selected cardholder account.

   The words “Operation Completed Successfully” appear at the left-side of the page. You have successfully disabled the cardholder account.

NOTE

After performing an emergency access disable function on a particular cardholder, you can only re-enable badges from the P2000 host software. However, you can re-enable the Web Access access permissions from Web Access, if needed.

Chapter 4

SYSTEM ADMINISTRATION

This chapter covers the system deployment and customization of the P2000 Web Access application. It is intended for use by the P2000 System Administrator, Security Manager or other qualified professional in charge of deploying or customizing the P2000 Web Access application.

NOTE

Unless specified otherwise, the Microsoft® Windows Server® 2008 Operating System (OS) was used in the development of this chapter. If using a different Windows® OS, the screens and instructions may differ slightly.

NOTE

On 64-bit Microsoft Windows OSs supported by P2000, the Johnson Controls directory is located in Program Files (x86).

WEB ACCESS DEPLOYMENT

There are two methods to deploy the Web Access application, one which uses the P2000 server only (Option #1), and the other which also uses a separate front-end Web server (Option #2).

Deployment Option #1: P2000 Server Only

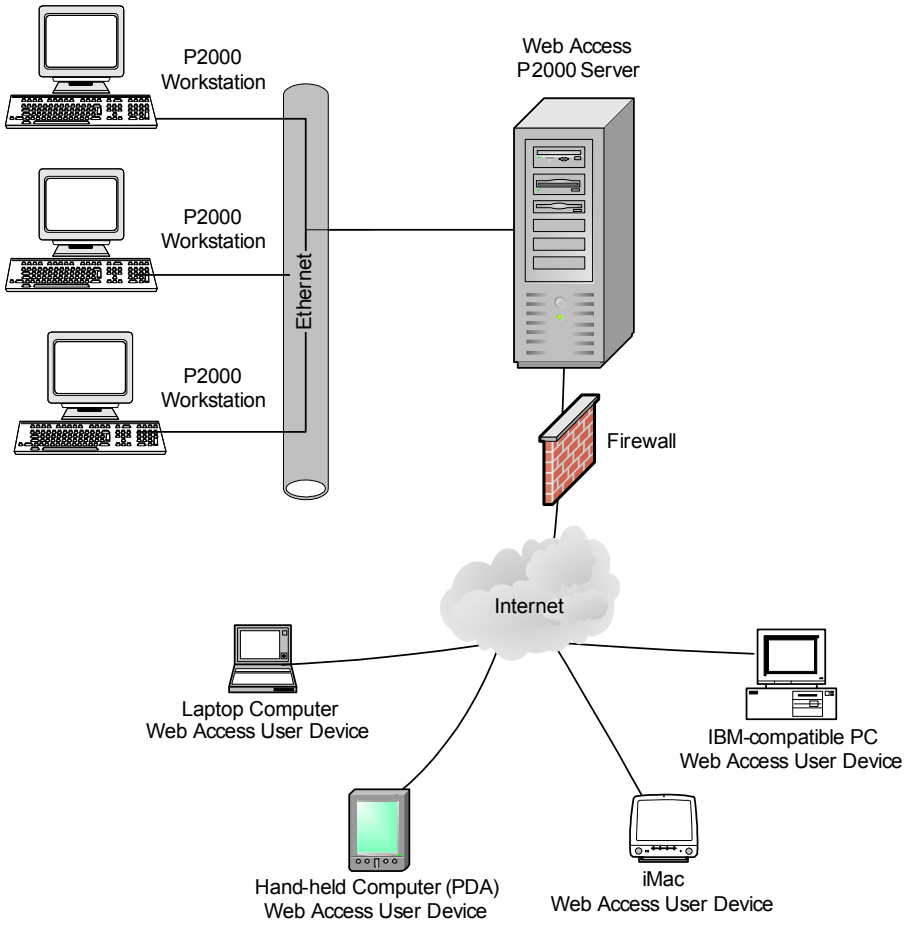


Figure 4-1: Web Access Deployment Option #1 (P2000 Server Only)

In this configuration, the P2000 server runs the Web Access front-end and back-end services. Essentially, the P2000 server is also used as the Web server. The Web Access front-end services handle the Web browser HTTP requests, while the Web Access back-end services handle the application's XML requests from the front end.

Before continuing with the instructions for this deployment option, install and configure all software applications required for the P2000 server according to the instructions in the *P2000 Server/Workstation Software Installation Manual*.

Once you have installed the P2000 software, follow the instructions in "Internet Information Services (IIS) Verification" on page 4-4.

Deployment Option #2: P2000 Server and Front-end Web Server

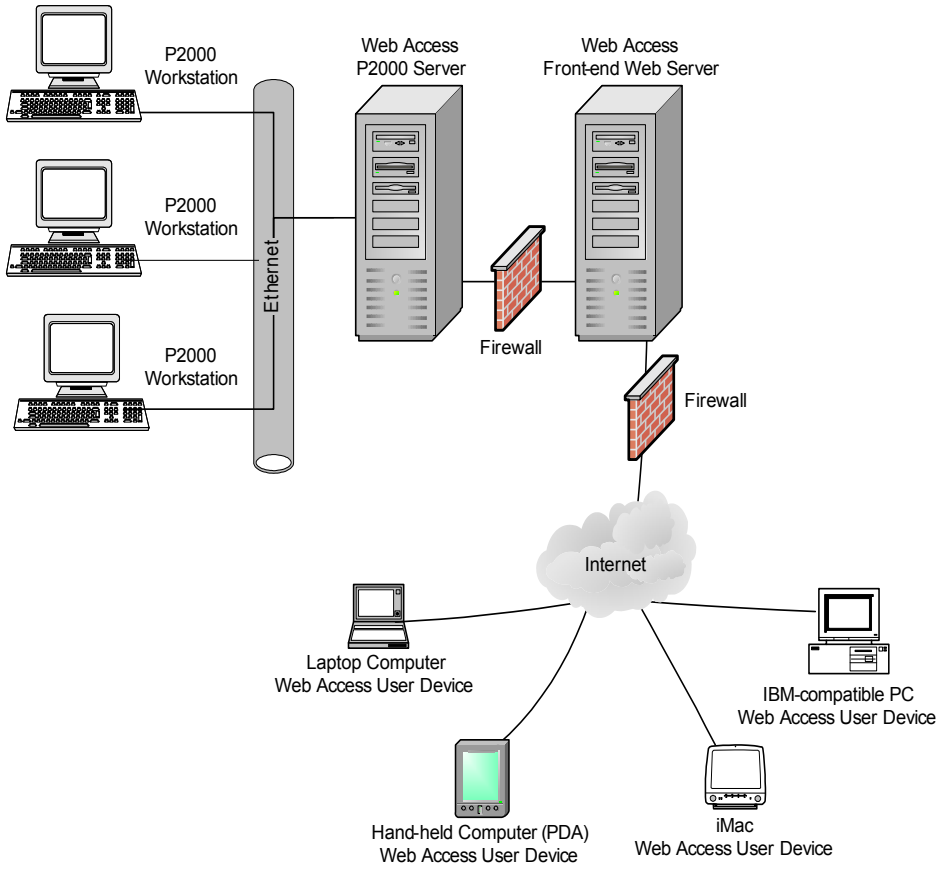


Figure 4-2: Web Access Deployment Option #2 (P2000 Server and Front-end Web Server)

In this scenario, the P2000 server runs the Web Access back-end services, and a separate server runs the front-end Web services.

Before continuing with the instructions for this deployment option, install and configure all software applications required for the P2000 server according to the instructions in the *P2000 Server/Workstation Software Installation Manual*. Then install all required software on the front-end Web server. The front-end Web server requires the following:

- One of the following operating systems:
  - Microsoft Windows Server 2008 OS or Windows Server 2008 R2 OS
  - Microsoft Windows Server 2003 OS or Windows Server 2003 R2 OS
  - Microsoft Windows Vista® OS
  - Microsoft Windows XP® OS
- Microsoft .NET Framework 4.0

- Microsoft Internet Information Services (IIS) 5.*x*, 6.*x*, or 7.0
- Digital Certificate for IIS

NOTE
If multiple front-end Web servers will be employed, install the required software on each computer.

The front-end Web server requires the same hardware as the P2000 workstation hardware, which is also specified in the software installation manual.

Once the required software is installed on the P2000 server and front-end Web server, follow the instructions in "Internet Information Services (IIS) Verification".

Internet Information Services (IIS) Verification

Verify that IIS has been installed and configured correctly on the P2000 server in accordance with the instructions in the *P2000 Server/Workstation Software Installation Manual*. Perform the instructions in the following sections according to the operating system installed on the P2000 server.

NOTE
When deploying a front-end Web server with the Windows Server 2008 or Windows Server 2003 operating system, IIS and ASP.NET must be installed on the server according to the instructions in the P2000 Server/Workstation Software Installation Manual. Then follow the instructions in this section to verify IIS was properly installed.

NOTE
*If using the S321-IP Interface Service on a P2000 computer running Microsoft Windows XP®, then you must configure Windows IIS service (if installed) to **not** start.*

If IIS was not installed and configured correctly, refer to the *P2000 Server/Workstation Software Installation Manual* for assistance.

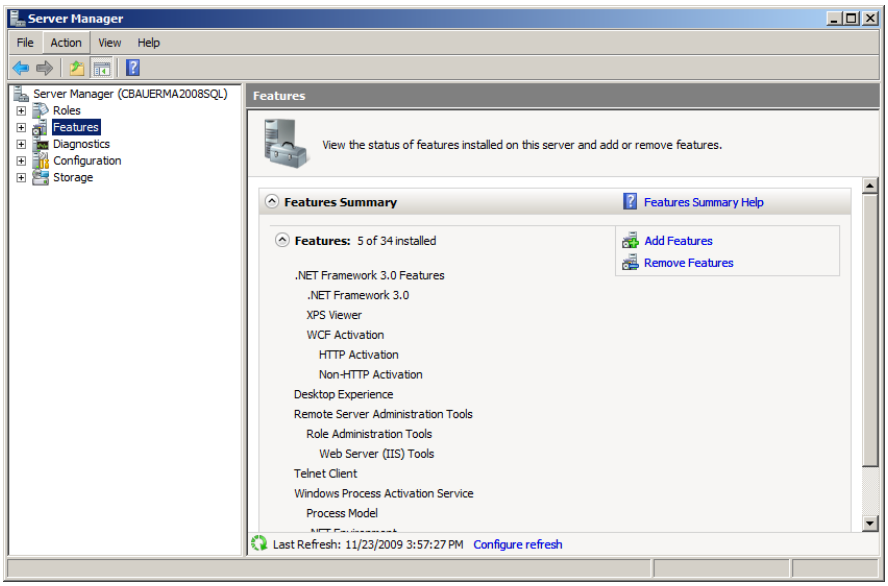
Windows Server 2008

➤ **To verify the IIS installation and configuration for Windows Server 2008:**

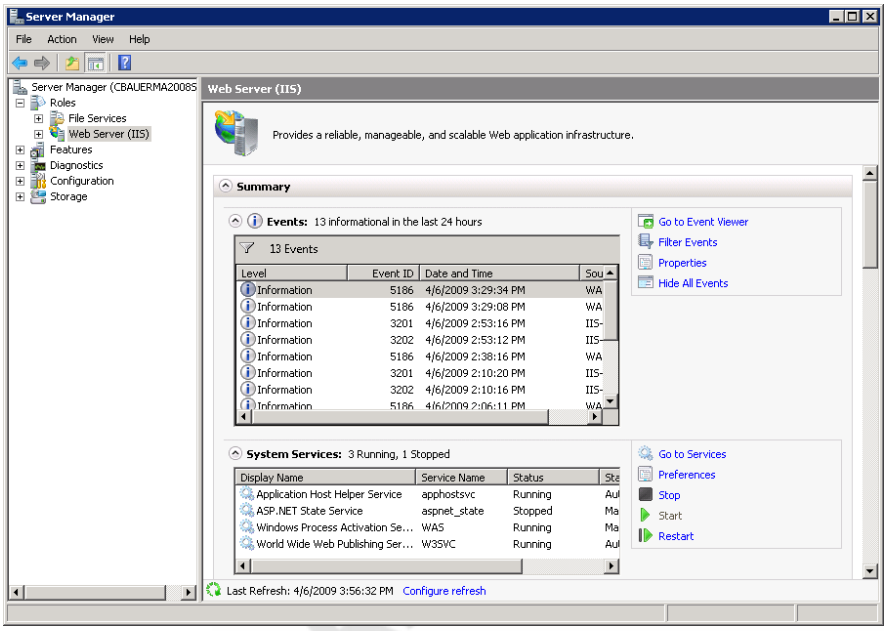
1. From the Windows **Start** menu, select **Administrative Tools>Server Manager**.

   The Server Manager window appears.
2. In the left pane, select **Features**.

3. Verify the following features are installed:
   - .NET Framework 3.x Features
   - Desktop Experience
   - Telnet Client



4. In the left pane, expand **Roles** and select **Web Server (IIS)**.
   The IIS Summary page appears.



5. Scroll down to **Roll Services** and verify the following services are installed:

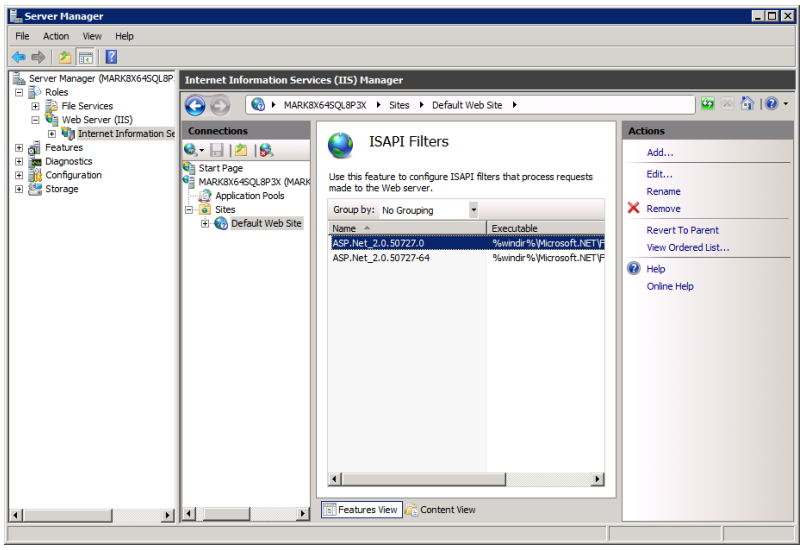
   Web Server
   - **Common HTTP Features**
     - Static Content
     - Default Document
     - Directory Browsing
     - HTTP Errors
     - HTTP Redirection
   - **Application Development**
     - ASP.NET
     - .NET Extensibility
     - ISAPI Extension
     - ISAPI Filters
   - **Health and Diagnostics**
     - HTTP Logging
     - Logging Tools
     - Request Monitor
     - Tracing
     - Custom Logging
     - ODBC Logging
   - **Security**
     - Basic Authentication
     - Windows Authentication
     - Request Filtering

   Management Tools
   - **IIS Management Console**
   - **IIS 6 Management Compatibility**
     - II 6 Metabase Compatibility
     - II 6 WMI Compatibility
     - II 6 Scripting Tools
     - II 6 Management Console

6. Install any required role service listed in step 5 if currently not installed. Refer to the IIS online documentation for assistance. Refer also to the *P2000 Server/Workstation Software Installation Manual* for additional help.

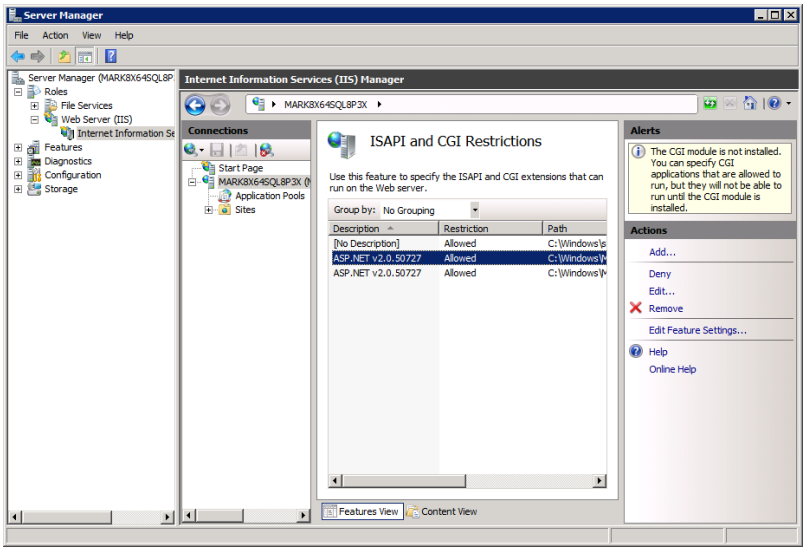
7. Verify that the **ASP.Net_2.0 ISAPI** filters are added in IIS Manager for **v2.0.xxxxx** (required for IIS Version 7.0 or later). To do this:
   - Launch Windows Server Manager.
   - In the left pane under Server Manager, expand **Roles** and **Web Server (IIS)**.
   - Select **Internet Information Services (IIS) Manager**.
   - In the **Connections** pane, expand **[server name]** and **Sites**.
   - Select **Default Web Site**.

- In the Default Web Site Home pane, double-click **ISAPI Filters**. A list of filters appears.



- Add the required filters, if necessary.
- For information on how to add ISAPI filters in IIS, refer to the Microsoft Windows documentation.

8. Verify that the **ASP.NETv2.0.xxxxx** ISAPI and CGI Restrictions are set to **Allowed**.
   - Launch Windows Server Manager.
   - In the left pane under Server Manager, expand **Roles** and **Web Server (IIS)**.
   - Select **Internet Information Services (IIS) Manager**.
   - In the **Connections** pane, select **[server name]**.
   - In the **[server name] Home** pane, double-click **ISAPI and CGI Restrictions**.



- Set the required extensions to **Allowed**, if necessary.
- For information on how to modify this setting, refer to the Microsoft Windows documentation.

9. If you are using the single server deployment option #1 (no Web server), you have completed the steps to deploy Web Access.

   If you are using the front-end Web server option #2, continue with the instructions in “Configuring the P2000 Server and Front-end Web Server (Front-end Web Server Deployment Option Only)” on page 4-11.

Windows Server 2003

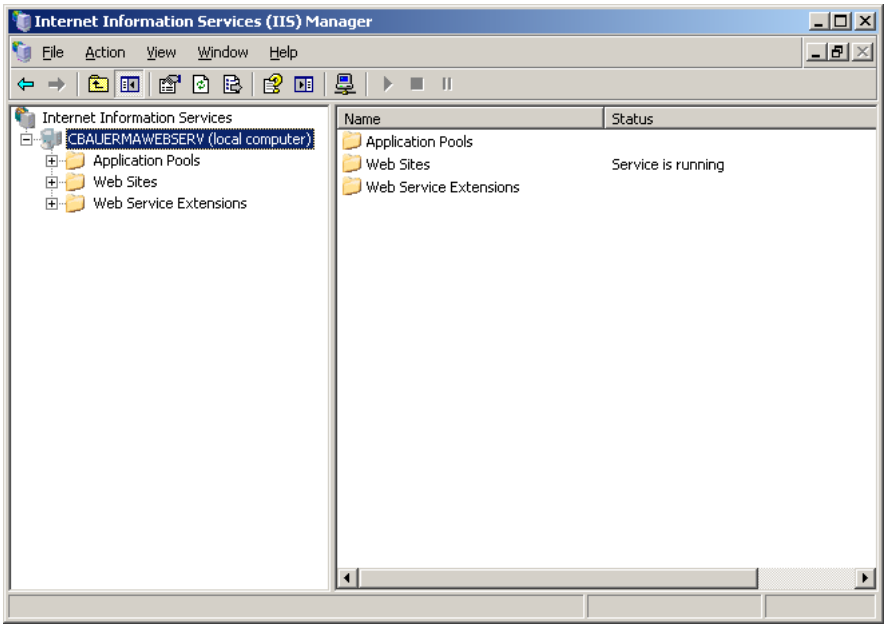
If P2000 is installed on a server running Microsoft Windows Server 2003, follow the IIS verification instructions in this section.

➤ To verify the IIS installation and configuration for Windows Server 2003:

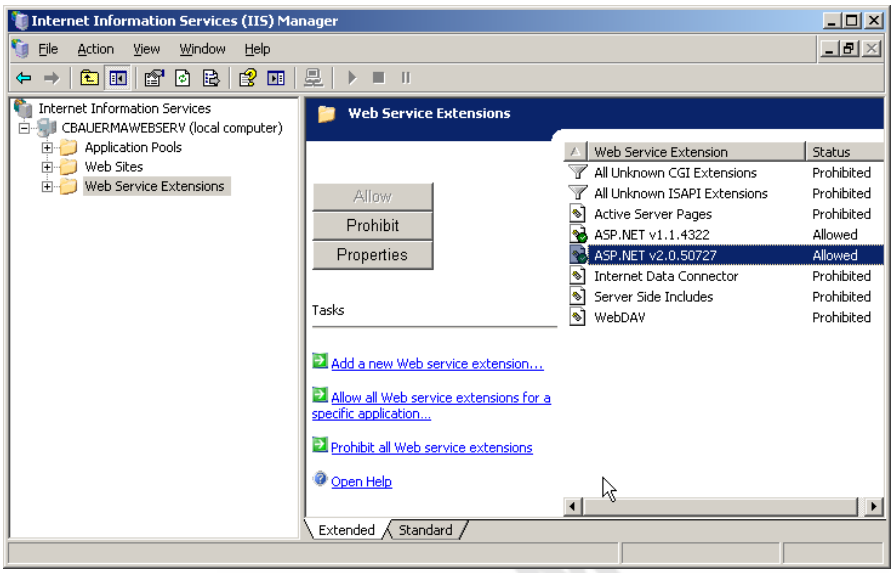
1. From the Windows taskbar, select **Start>Programs>Administrative Tools>Internet Information Services (IIS) Manager**.

   The Internet Information Services (IIS) Manager window appears.

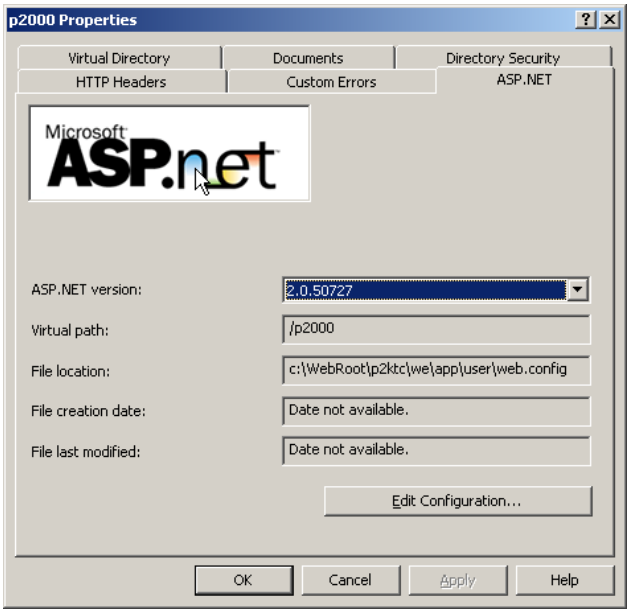
2. In the left pane, expand the directory tree labeled with the computer name.



3. In the left pane, select **Web Service Extensions**.
4. In the right pane, verify that the **ASP.NET v2.0.xxxx** web service extension status is set to **Allowed**. If the status is currently set to **Prohibited**, click the **Allow** button.



5. In the left pane, select **Web Sites>Default Web Site**.
6. Right-click over **p2000** and select **Properties**. The p2000 Properties dialog box appears.
7. Select the **ASP.NET** tab.
8. Verify that the **ASP.NET version** is **v2.0.xxxx**.



If another version is listed, refer to the *P2000 Server/Workstation Software Installation Manual* for assistance.

Windows Vista

If P2000 is installed on a computer running Microsoft Windows Vista, follow the IIS verification instructions in this section.

➤ **To verify the IIS installation for Windows Vista:**

1. Go to **Start>Settings>Control Panel** and double-click **Programs and Features**.
2. In the left window pane under **Tasks**, click on the **Turn Windows features on or off** link.
3. Select the **Internet Information Services** check box if currently not selected.
4. Click **OK**.

Windows XP

If P2000 is installed on a computer running Microsoft Windows XP, follow the IIS verification instructions in this section.

➤ **To verify the IIS installation for Windows XP:**

1. Go to **Start>Settings>Control Panel**.
2. In the Control Panel window, double-click the **Add/Remove Programs** icon.
3. Click the **Add/Remove Windows Components** button.

4. When the Windows Components Wizard opens, if the **Internet Information Services (IIS)** check box is selected, IIS has been installed on the computer. Click **Cancel** and close the Add or Remove Programs window.
5. If the **Internet Information Services (IIS)** check box is *not* selected, refer to the *P2000 Server/Workstation Software Installation Manual* for instructions on installing IIS.

Configuring the P2000 Server and Front-end Web Server (Front-end Web Server Deployment Option Only)

Using a separate computer to run the Web Access front-end services requires additional configuration steps, which are described in this section. These include:

- Verifying the P2000 Server Has Version 3.11 or Higher Installed (see page 4-11)
- Verifying Web Access Runs Properly on the P2000 Server (see page 4-12)
- .p2k Application Extension Mapping (P2000 Server) (see page 4-12)
- Copying and Running the FrontEnd Script (see page 4-17)
- Creating and Configuring the P2000Apps Application Pool (Windows Server 2008 or Server 2003 Only) (see page 4-19)
- Setting the Front-end Web Server's RemoteAppEnd, InstallationKey, and RegistrationKey Configuration Parameters (see page 4-27)
- Setting the P2000 Server's FrontEnd Configuration Parameter (see page 4-28)
- Validating Web Server Operation with Web Access (see page 4-29)

Because the P2000 server will not be used as the front-end Web server with this deployment option, you will need to edit the **Web.config** file for both the P2000 server and front-end Web server, which will enable the two computers to communicate and handle Web Access HTTP and XML requests. This procedure is described in this chapter.

Verifying the P2000 Server Has Version 3.11 or Higher Installed

➤ **To verify the P2000 server has Version 3.11 or higher installed:**

1. From the P2000 Main menu, select **Help>About P2000**.
2. On the About P2000 dialog box, verify the current version of P2000 meets the minimum requirement.
3. If the server does not meet the requirement, install P2000 Version. 3.11 or higher.

Verifying Web Access Runs Properly on the P2000 Server

Before continuing with the configuration instructions, verify that you can successfully launch and log on to P2000 Web Access from the P2000 server or client computer. See “Getting Started” on page 1-4.

.p2k Application Extension Mapping (P2000 Server)

The **p2ktc** virtual directory must be configured to accept the **.p2k** file extension. Perform the instructions in the following sections according to the operating system installed on the P2000 server.

Windows Server 2008

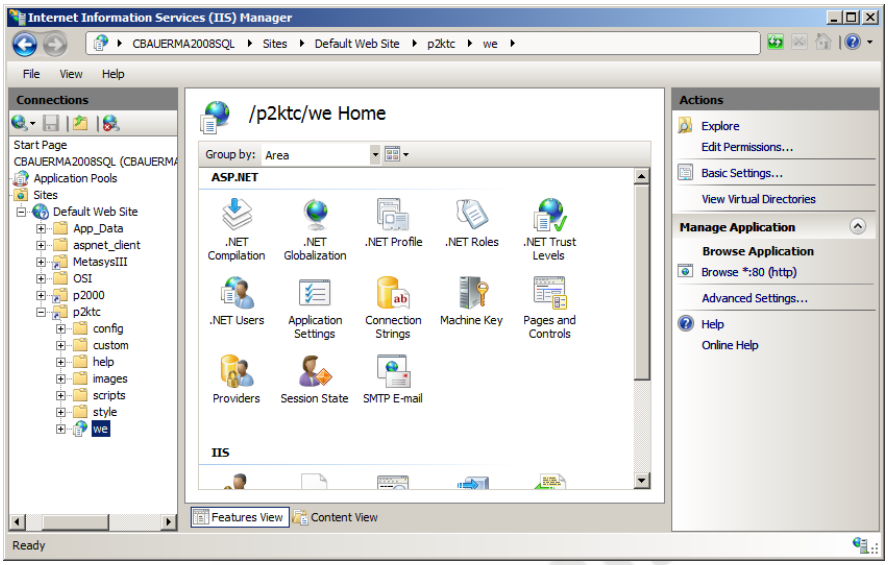
➤ **To configure the *p2ktc* virtual directory to accept the *.p2k* file extension:**

1. From the P2000 server, go to **Start>All Programs>Administrative Tools>Internet Information Services (IIS) Manager**.

   The Internet Information Services (IIS) Manager window appears.

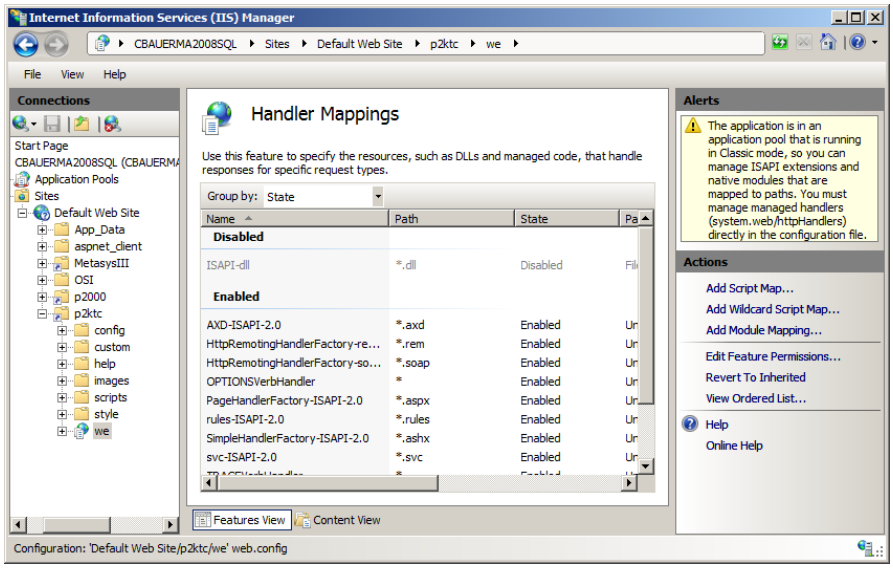
2. In the left pane, expand the directory tree to the following location:

   ***server name*>Sites>Default Web Site>p2ktc>we**



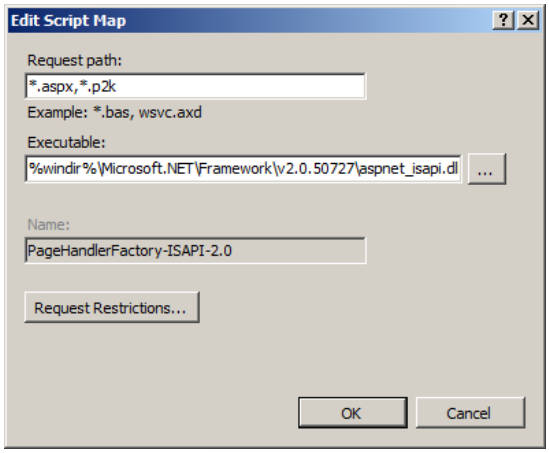
3. If the window is currently in Content View, select the **Features View** tab at the bottom of the screen.

4. In the middle pane, double-click **Handler Mappings**. The Handler Mappings page appears.

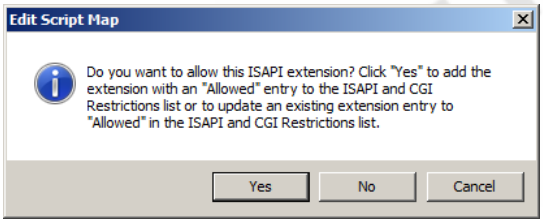


5. Double-click **PageHandlerFactory-ISAPI-2.0**. The Edit Script Map dialog box appears.
6. In the Request Path field, enter `,*.p2k` at the end of the text string.

   Example: *.aspx,*.p2k



7. Click **OK**.
8. Click **Yes** on the Edit Script Map dialog box.



Windows Server 2003

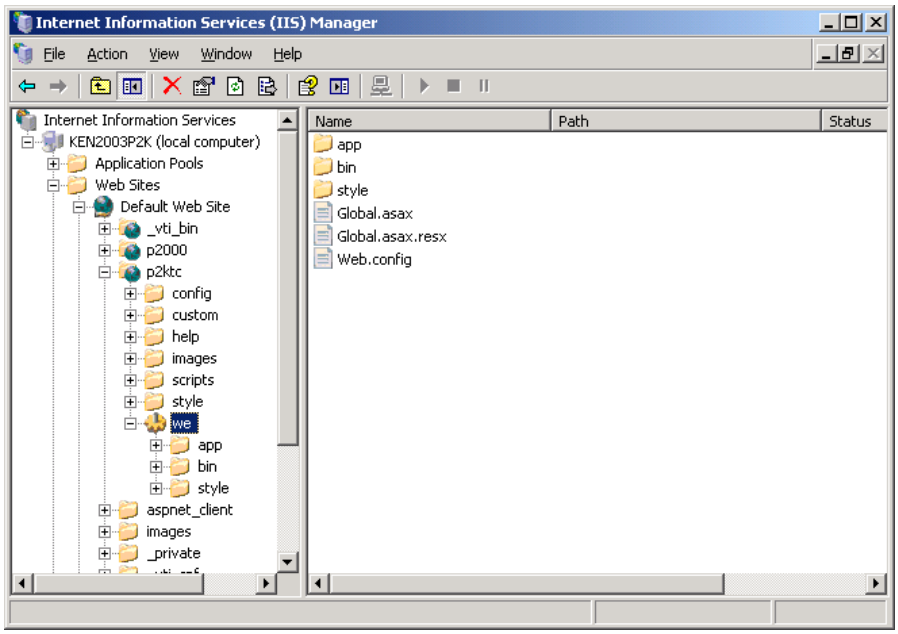
If P2000 is installed on a server running Microsoft Windows Server 2003, follow the IIS .p2k extension mapping instructions in this section.

➤ **To configure the *p2ktc* virtual directory to accept the *.p2k* file extension:**

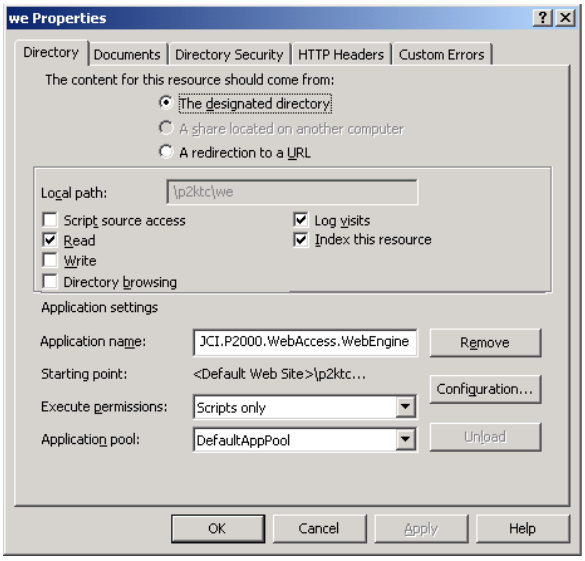
1. From the P2000 server, go to **Start>Programs>Administrative Tools>Internet Information Services (IIS) Manager**.

   The Internet Information Services (IIS) Manager window appears.

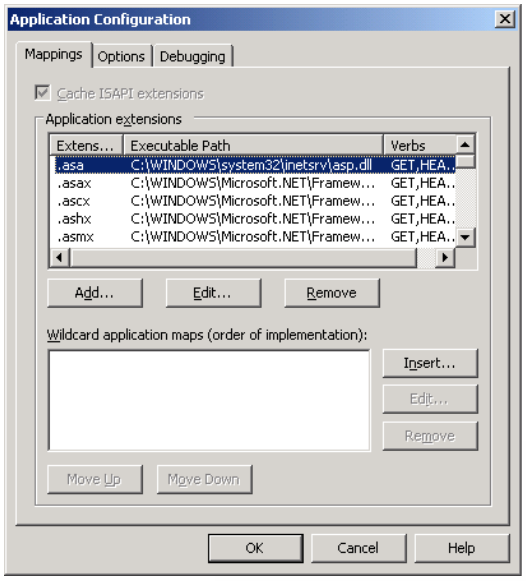
2. In the left pane, expand the directory tree to the following location: ***server name*>Web Sites>Default Web Site>p2ktc>we**.



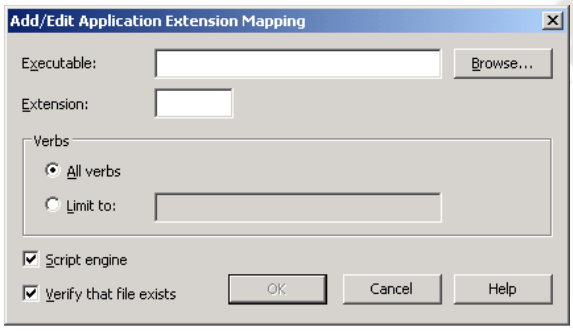
3. Right-click on **we** and select **Properties**. The we Properties dialog box appears.



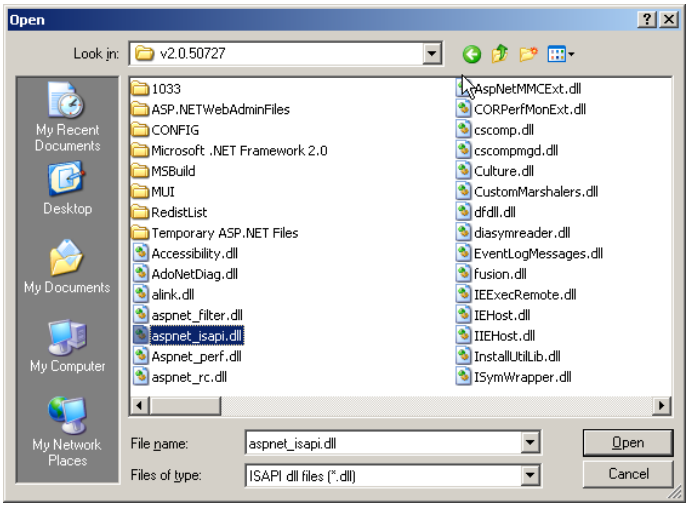
4. Click **Configuration**.The Application Configuration window appears.



5. Click **Add**. The Add/Edit Application Extension Mapping dialog box appears.

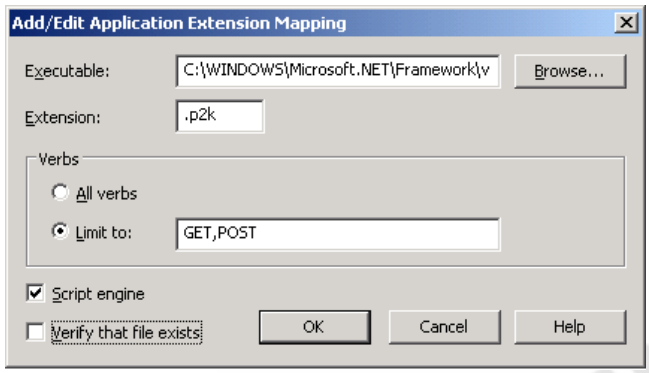


6. Click **Browse** and locate to the following directory: *Local Disk:\WINNT (or WINDOWS)\Microsoft.NET\Framework\v.2.0.xxxxx*
7. From the **Files of type** drop-down list, select **(*.dll)**. Select the **aspnet_isapi.dll** file and click **Open**.



The path will appear in the **Executable** field on the Add/Edit Application Extension Mapping dialog box

8. Enter `.p2k` in the **Extension** field.
9. In the **Verbs** area, select the **Limit to** radio button and enter `GET,POST` in the text box.
10. Clear the **Verify that file exists** check box.



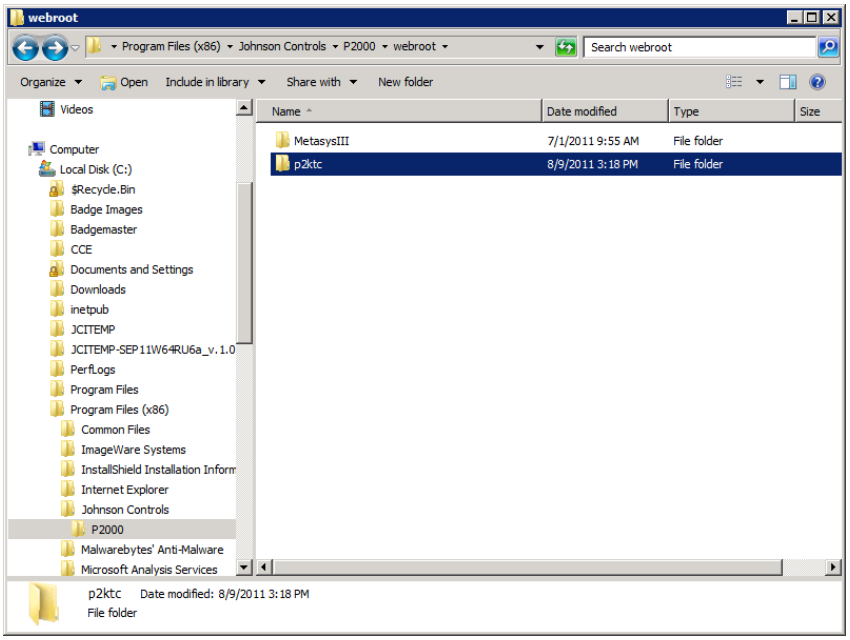
11. Click **OK**. Scroll the Application extensions table and verify that the .p2k extension appears in the table.
12. Click **OK**.
13. Click **OK** on the we Properties window.
14. Close the Internet Information Services (IIS) Manager window.

Copying and Running the FrontEnd Script

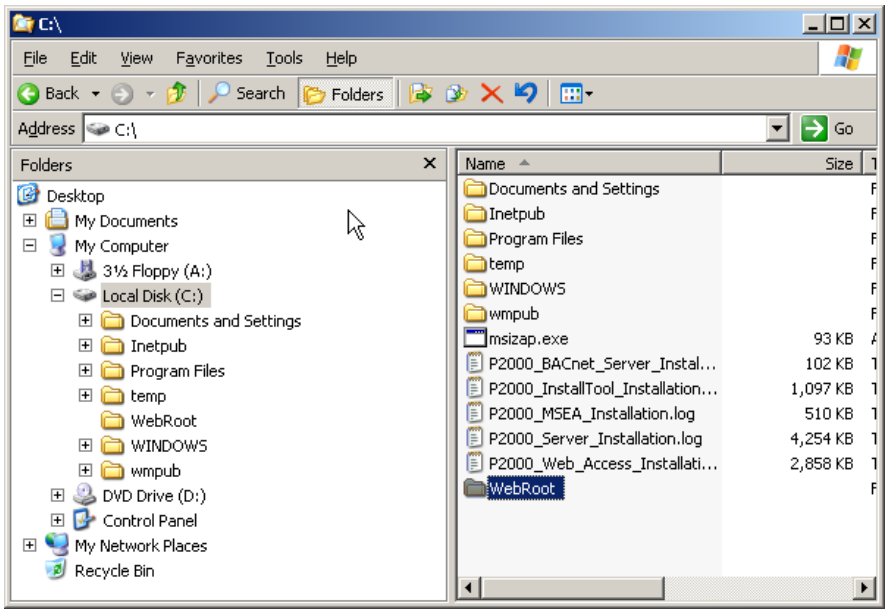
The next step to configure the front-end Web server consists of copying the **p2ktc** folder from the P2000 server to the front-end Web server, and running **ii7frontsetup.bat** (for front-end Web servers running IIS7) or **frontsetup.bat** (for all other versions of IIS).

➤ **To copy and run the FrontEnd script:**

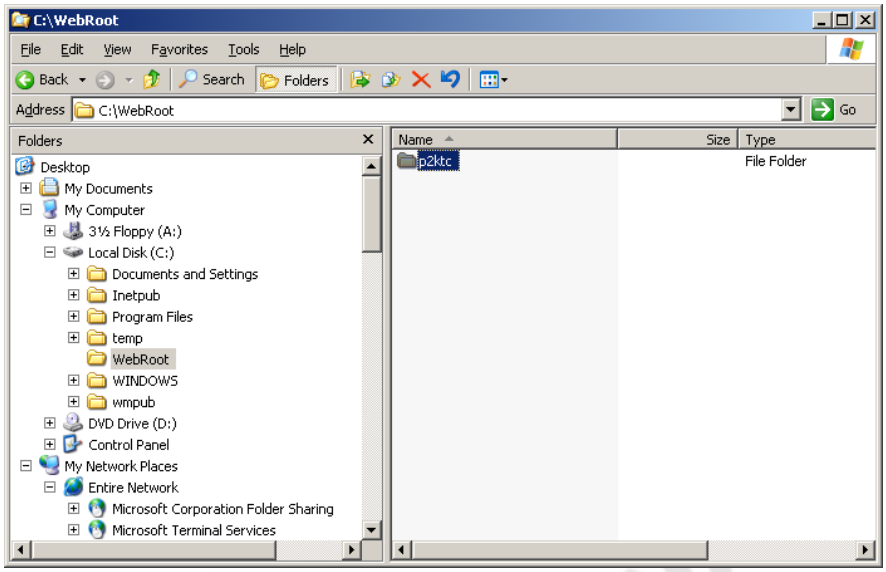
1. Copy the **p2ktc** folder from the following location on the P2000 server:
   LocalDisk:\Program Files\Johnson Controls\P2000\webroot



2. On the front-end Web server, create a new folder titled **WebRoot** at the root **C:** directory: *C:\WebRoot*.



3. Paste the copied directory into the *C:\WebRoot* directory on the front-end Web server.

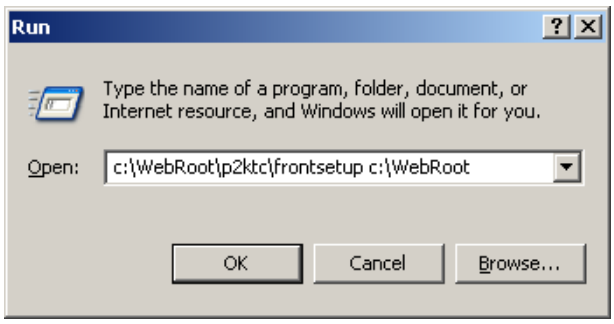


4. On the front-end Web server, from the Windows taskbar, select **Start>Run**.
5. In the **Open** field:

   If running **IIS 7.x**, enter *c:\webroot\p2ktc\iis7_frontsetup c:WebRoot*

   If running **IIS 6.x or earlier**, enter *c:\webroot\p2ktc\frontsetup c:WebRoot*

   A space separates *frontsetup* and the second path.



6. Click **OK**.
7. If the Windows Script Host dialog box appears, disregard the message and click **OK**.
8. If a dialog box appears asking whether you would like to register Cscript as your default host for VBscript, click **Yes**.
9. If you receive a successfully registered dialog box, click **OK**.

Creating and Configuring the P2000Apps Application Pool (Windows Server 2008 or Server 2003 Only)

Perform the following steps on each front-end Web server **only** if the server is running the Windows Server 2008 or Server 2003 operating system.

For front-end Web servers running other supported operating systems (see page 4-3), skip to "Setting the Front-end Web Server's RemoteAppEnd, InstallationKey, and RegistrationKey Configuration Parameters" on page 4-27.

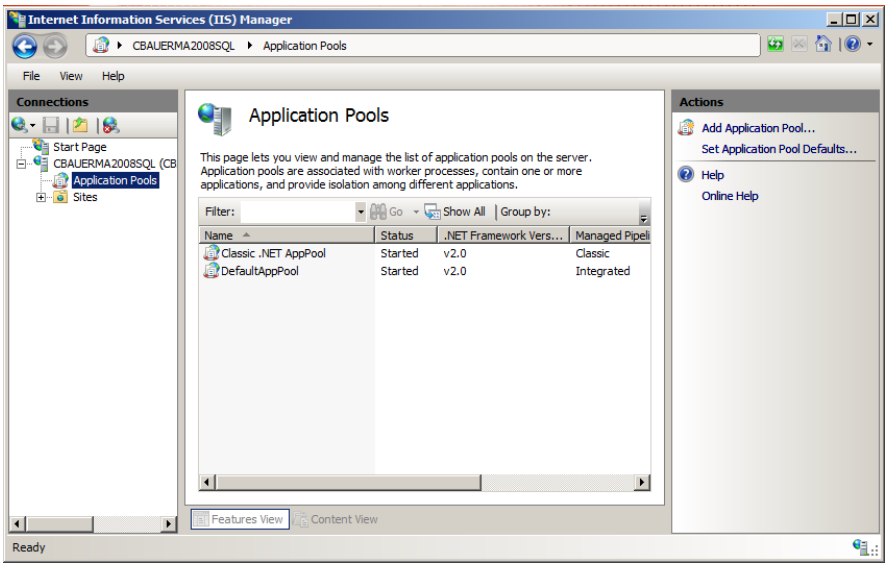
Windows Server 2008

➤ To create and configure the *P2000Apps* Application Pool:

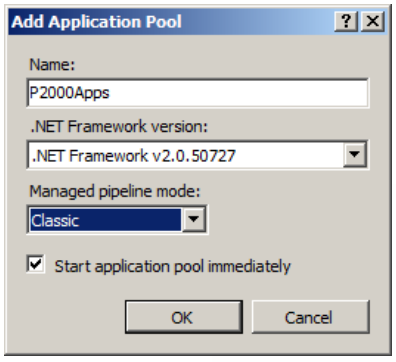
1. From the Windows taskbar, select **Start>All Programs>Administrative Tools>Internet Information Services (IIS) Manager**.

   The Internet Information Services (IIS) Manager window appears.
2. Expand the directory tree labeled with the computer name.

3. Select **Application Pools**.

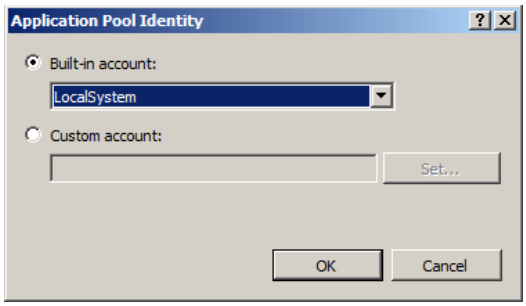


4. Under the **Actions** tab, select **Add Application Pool**. The Add Application Pool dialog box appears.
5. In the **Name** field, enter `P2000Apps`.
6. In the **.NET Framework version** drop-down list, select **.NET Framework v.2.0.xxxx**.
7. In the **Managed Pipeline Mode** drop-down list, select **Classic**.

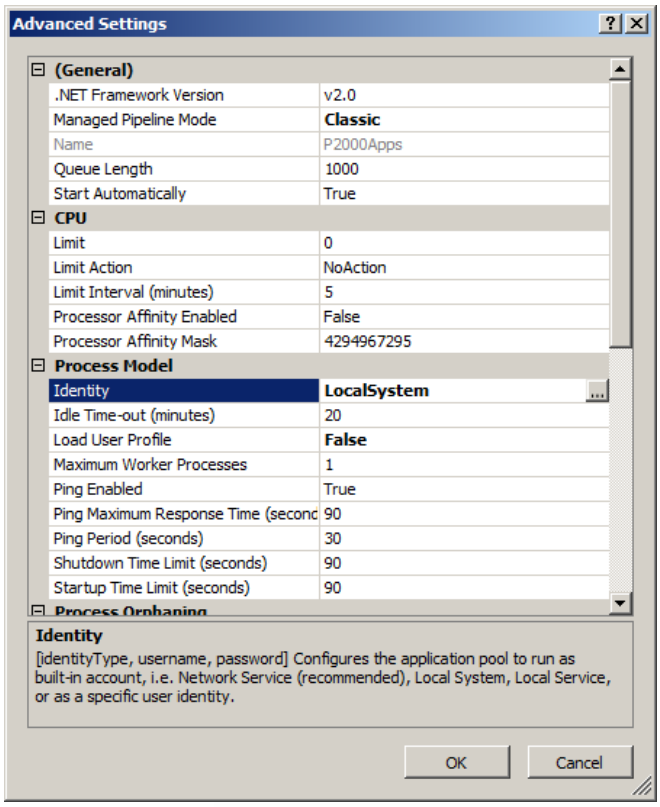


8. Click **OK**.
9. Select the **P2000Apps** application pool from the list and click **Advanced Settings**. The Advanced Settings dialog box appears.
10. Under **Process Model**, select the **Identity** row. Click the browse button to the right. The Application Pool Identity dialog box appears.

11. Select the **Built-in account** radio button. Then select **LocalSystem** in the drop-down list.



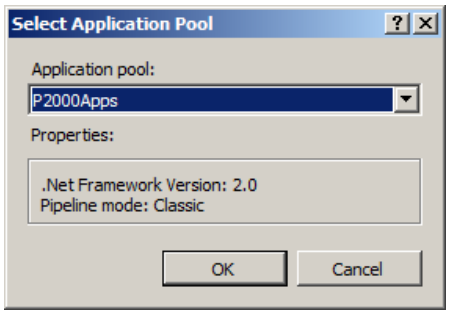
12. Click **OK**.



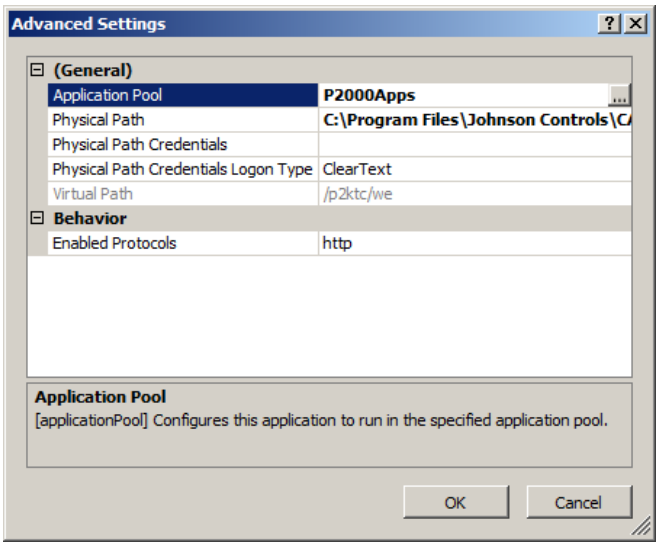
13. On the Advanced Settings dialog box, click **OK**.
14. In the left pane of the Internet Information Services (IIS) Manager window, expand the directory tree to the following location:

    ***server name*>Sites>Default Web Site>p2ktc>we**
15. Under the **Actions** tab, select **Advanced Settings**. The Advanced Settings dialog box appears.
16. Under **General,** select the **Application Pool** row. Click the browse button to the right. The Select Application Pool dialog box appears.

17. Select **P2000Apps** in the drop-down list.



18. Click **OK**.



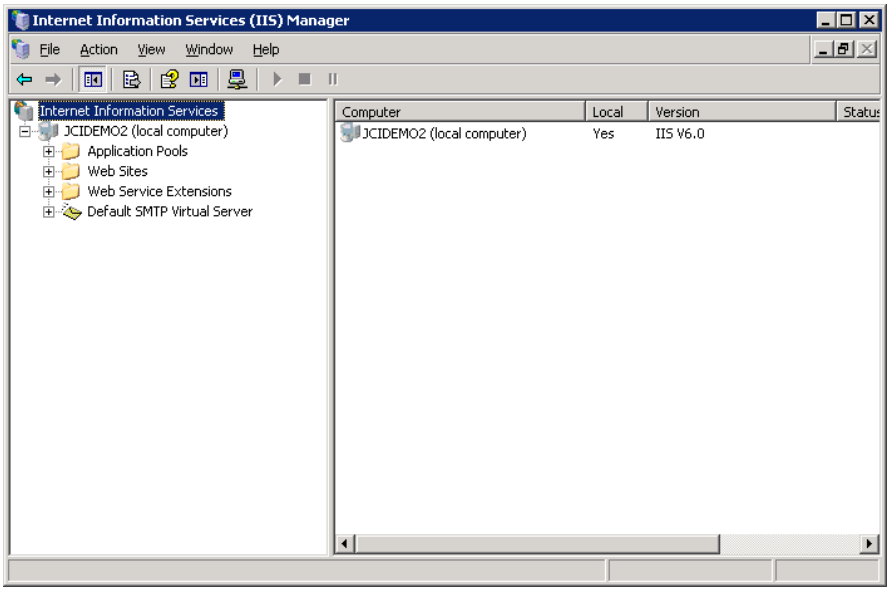
19. On the Advanced Settings dialog box, click **OK**.

Windows Server 2003

1. From the Windows taskbar, select **Start>All Programs>Administrative Tools>Internet Information Services (IIS) Manager**.

   The Internet Information Services (IIS) Manager window appears.

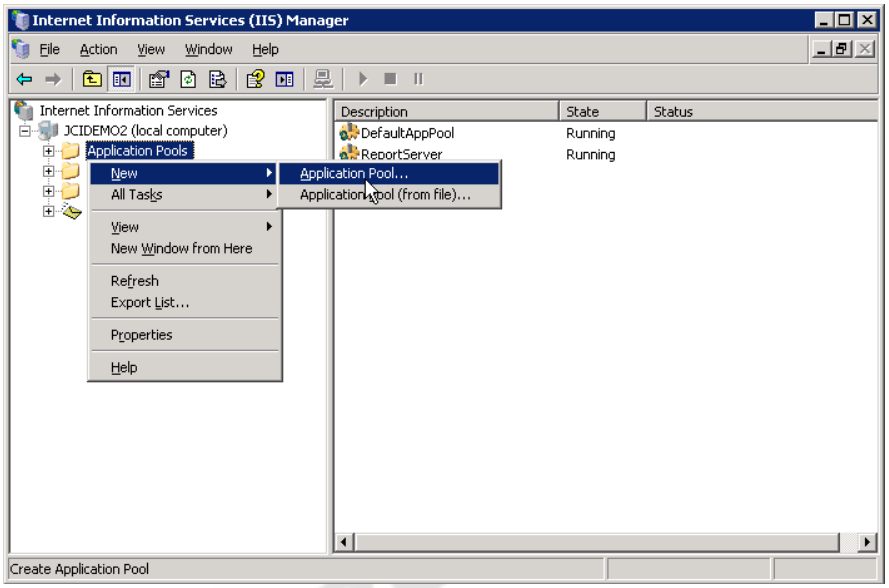
2. Expand the directory tree labeled with the computer name.



3. Verify the **Application Pools** directory appears under the computer name.

   If the Application Pools directory does not appear in the left pane, your server may be running IIS in isolation mode. To disable IIS isolation mode, right-click **Web Sites** and select **Properties**. Select the **Service** tab and clear the **Run WWW service in IIS 5.0 isolation mode** check box.

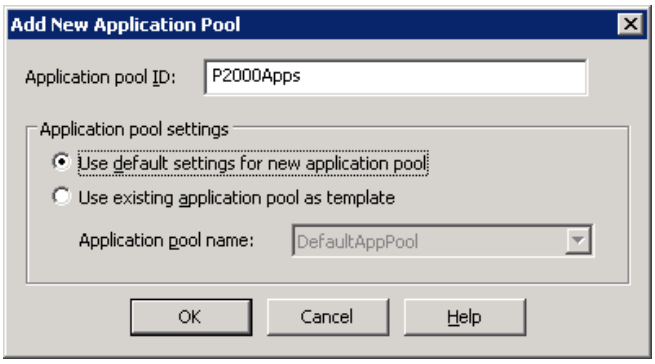
4. Right-click over **Application Pools** and select **New>Application Pool** from the pop-up menu.



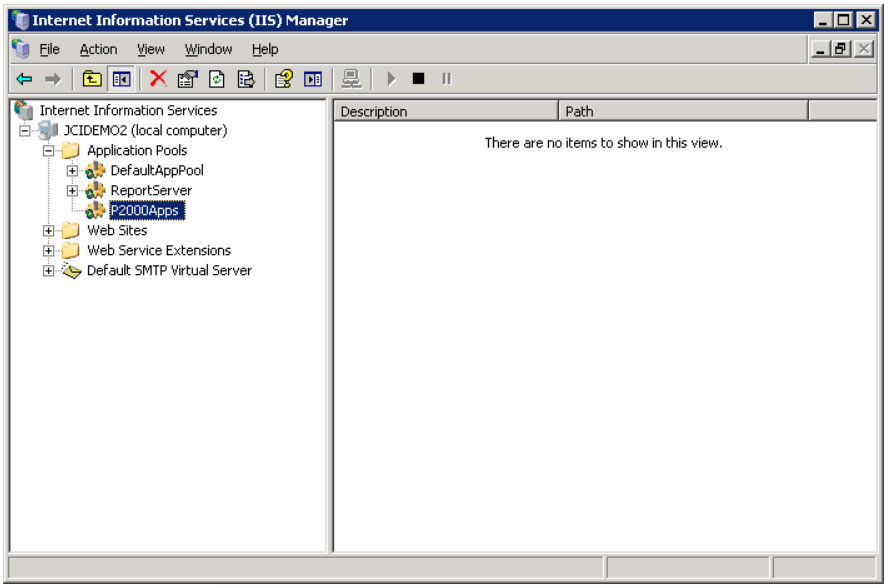
   The Add New Application Pool window appears.

5. Enter `P2000Apps` in the **Application pool ID** text box.

6. Select the **Use default settings for new application pool** radio button.



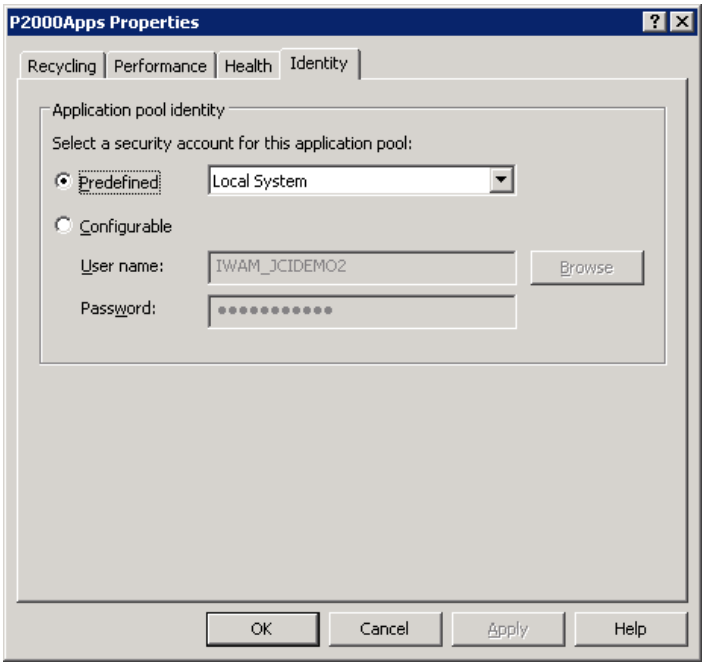
7. Click **OK**. The newly created application pool should appear as a subdirectory under the Application Pools directory.



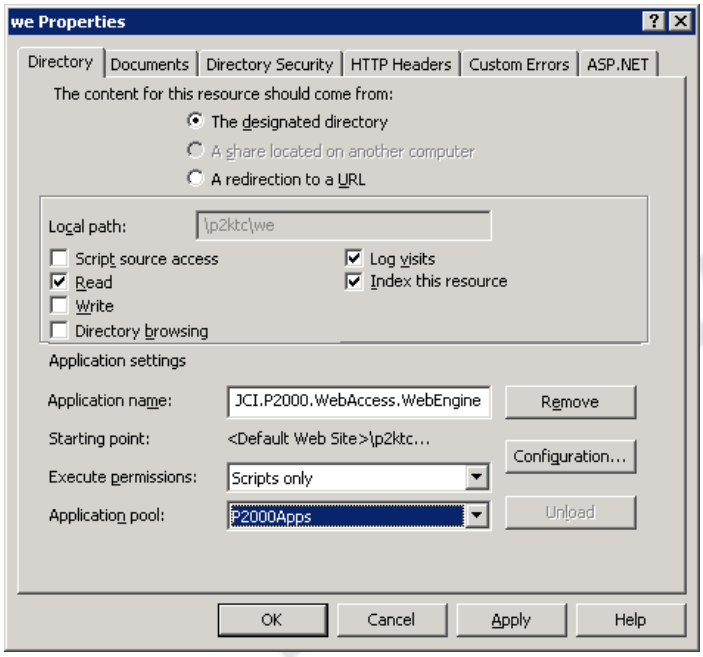
8. Right-click on **P2000Apps** and select **Properties**.

   The P2000Apps Properties dialog box appears.

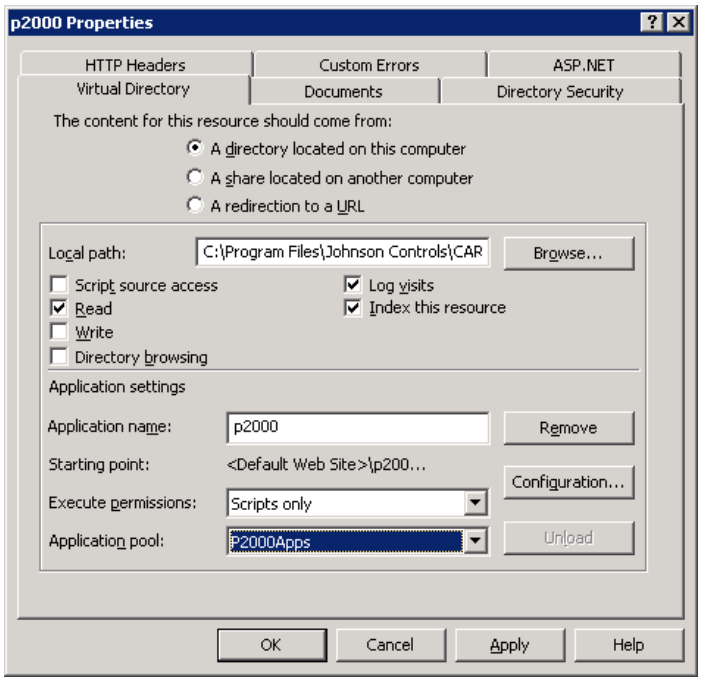
9. Select the **Identity** tab.
10. Select the **Predefined** radio button and select **Local System** from the drop-down list.



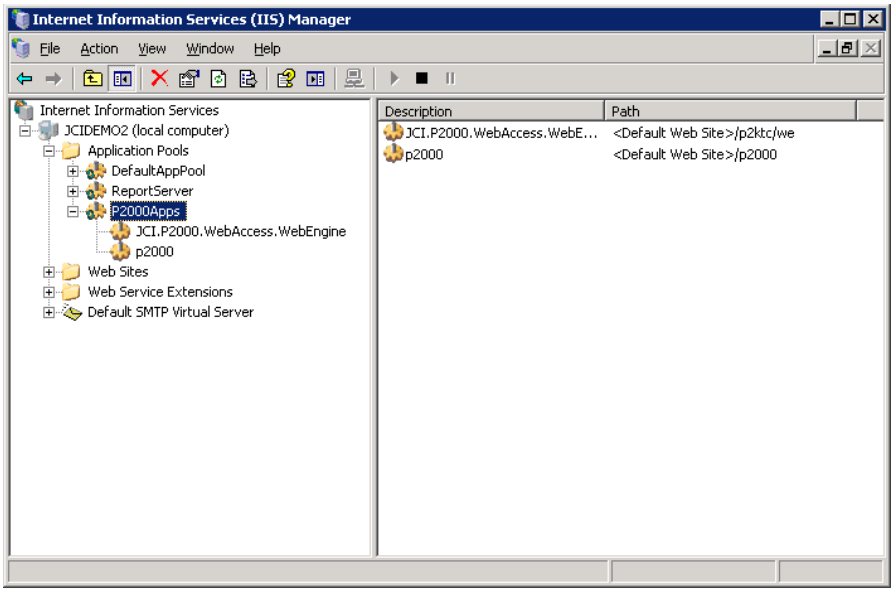
11. Click **OK**.
12. In the left pane of the Internet Information Services (IIS) Manager window, access the following directory: *Web Sites>Default Web Site>p2ktc>we*.
13. Right-click over the **we** directory and select **Properties**. The we Properties dialog box appears.
14. On the **Directory** tab, select **P2000Apps** in the **Application pool** drop-down list.



15. Click **OK**.
16. In the left pane of the Internet Information Services (IIS) Manager window, access the following directory: *Web Sites>Default Web Site>p2000*.
17. Right-click over the **p2000** directory and select **Properties**. The p2000 Properties dialog box appears.
18. On the Virtual Directory tab, click the **Create** button. The **Create** button caption changes to **Remove**.
19. Select **P2000Apps** in the **Application pool** drop-down list.



20. Click **OK**.
21. Confirm that the following items have been added to the **P2000Apps** directory:
    - JCI.P2000.WebAccess.WebEngine
    - p2000



Setting the Front-end Web Server's RemoteAppEnd, InstallationKey, and RegistrationKey Configuration Parameters

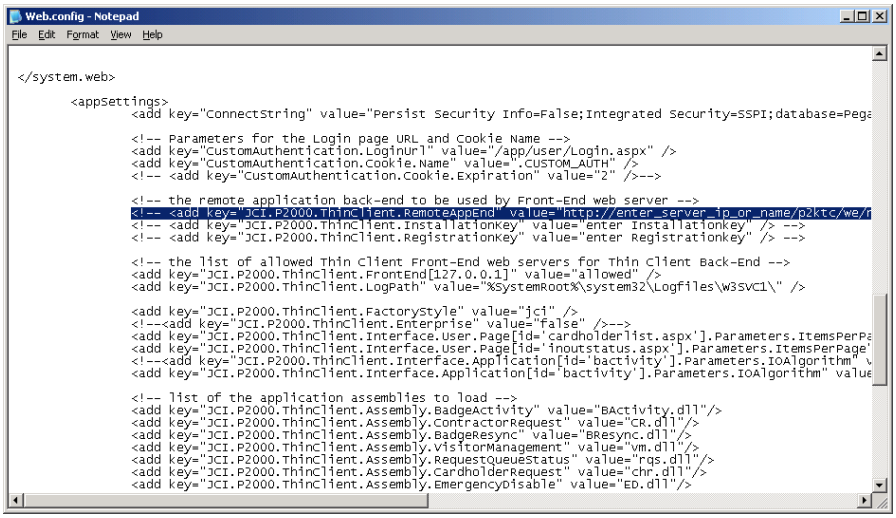
This section describes how to edit the **Web.config** file, which enables the front-end Web server to communicate with the P2000 server. Perform the following instructions for each front-end Web server.

➤ To set up the front-end Web server's *RemoteAppEnd*, *InstallationKey*, and *RegistrationKey* configuration parameters:

1. From the front-end Web server, open Windows Explorer.
2. Access the following directory:

   C:\webroot\p2ktc\we
3. Open the **Web.config** file in Microsoft Notepad or other text editor.
4. Locate the following text:

   <!--<add key="JCI.P2000.ThinClient.RemoteAppEnd" value="http://enter_server_ip_or_name/p2ktc/we/request.p2k" />-->



5. Replace "*enter_server_ip_or_name*" with the IP address or name of the P2000 server.
6. Remove the HTML comments from the beginning (**<!--**) and the end (**-->**) of the line.

   Example:

   <add key="JCI.P2000.ThinClient.RemoteAppEnd" value="http://158.322.104.7/p2ktc/we/request.p2k" />
7. If the P2000 server was configured as a secure server using Microsoft IIS, add an "s" after "http:".

   Example:

   *<add key="JCI.P2000.ThinClient.RemoteAppEnd" value="**https**://158.322.104.7/p2ktc/we/request.p2k" />*

   Refer to Microsoft's IIS documentation for information on setting up a secure server.
8. From the menu bar, select **File>Save**.
9. Reboot the front-end Web server or restart IIS.

Setting the P2000 Server's FrontEnd Configuration Parameter

The **Web.config** file must also be edited on the P2000 server, which allows the front-end Web server(s) to communicate and transfer data with the P2000 server.

NOTE

Whenever you install a new P2000 Service Pack, you may need to modify the Web.config file according to these instructions.

Perform the following instructions on the P2000 server:

1. Open Windows Explorer.
2. Access the following directory:

Local Disk:\Program Files\Johnson Controls\P2000\webroot\p2ktc\we

3. Open the **Web.config** file in Microsoft Notepad or other text editor.
4. Locate the following text:

<add key="JCI.P2000.ThinClient.FrontEnd[127.0.0.1]" value="allowed" />

5. If you will employ a single front-end Web server, skip to Step 6. If multiple front-end Web servers are employed, copy the entire line of text, place your cursor at the end of the line, press **<Enter>** on your keyboard, and paste the copied line of text beneath the first line. Repeat for each front-end Web server you will employ. You should have a FrontEnd text line for each front-end Web server.

   Example:

*<add key="JCI.P2000.ThinClient.FrontEnd[*127.0.0.1*]" value="allowed" />*
*<add key="JCI.P2000.ThinClient.FrontEnd[*127.0.0.1*]" value="allowed" />*
*<add key="JCI.P2000.ThinClient.FrontEnd[*127.0.0.1*]" value="allowed" />*

6. Replace "127.0.0.1" with the IP address of the front-end Web server. If employing multiple front-end Web servers, use the additional lines to define the IP addresses of the other front-end Web servers.

   Example:

*<add key="JCI.P2000.ThinClient.FrontEnd[*154.333.574.7*]" value="allowed" />*
*<add key="JCI.P2000.ThinClient.FrontEnd[*199.780.434.6*]" value="allowed" />*
*<add key="JCI.P2000.ThinClient.FrontEnd[*143.932.144.5*]" value="allowed" />*

NOTE

If at any time after the deployment of the front-end Web servers you wish to disable the connection between the P2000 server and a front-end Web server, simply change the ***value="allowed"*** to ***value="disallowed"***.

7. From the menu bar, select **File>Save**.
8. Reboot the P2000 server or restart IIS.

Validating Web Server Operation with Web Access

➤ **To validate Web server operation with Web Access:**

1. Launch a Web browser instance.
2. Enter the following in the Address bar, substituting *Web Server Name or IP* with the name or IP address of the Web server:

   http://Web Server Name or IP/P2000

Or enter the following if the Web Access Administrator has configured the P2000 server as a secure server:

https://Web Server Name or IP/P2000

3. Press <Enter> on your keyboard.

   When initially launching Web Access, you will have to wait approximately five minutes for the system to build the Web Access Web pages. Afterwards, the Login page appears.

CUSTOMIZING THE WEB ACCESS INTERFACE

Every Web Access interface page is fully customizable. The interface is built with XML (Extensible Markup Language) and can be customized using the Altova StyleVision software tool (Version 2005). The following Web Access interface components can be customized with this tool:

- Caption name, font size, type and color
- Images (for example, company logo)
- Background colors
- Field type (for example, combo box, text box, etc.), location and size
- Button types

Displaying pages in different languages can also be handled with the customization feature. See “Language Support” on page 4-36 for more information.

NOTE

This manual does not provide instructions on the installation and use of the Altova StyleVision XML editing tool. Refer to the Altova documentation for assistance.

Definition of Key Terms

This section describes some of the key terms and concepts discussed in this chapter. However, the information is basic in nature and specifically relates to the customization of the P2000 Web Access interface; it does not provide an in-depth discussion of the subjects. We invite you to research more on the subjects covered.

Extensible Markup Language (XML)

XML is a simplified version of the Standard Generalized Markup Language (SGML), and has been designed specifically for use on the Web. XML can be compared to Hypertext Markup Language (HTML) in that both are markup languages (they both use markup symbols to describe the contents of a page or file).

However, HTML was designed to define what data to display and how it should appear, while XML was designed to define how to structure and store the data. For example, an HTML tag will define how the name “Jane Doe” will appear on a Web page (for example, the font size, color, etc.). The XML data will describe the data contents as First Name (Jane) and Last Name (Doe). XML helps simplify the process of transmitting data across dissimilar platforms.

Using data structures (or schemas), XML enables the P2000 Security Management System to interpret the data (that is, identify the content) generated via the Web Access application.

XML Schema Definition (XSD)

XSD is a description of the structure of the contents and the rules of XML documents. In Web Access, XSD files define the data elements for each page of the application. You can only customize the Web Access elements as they are defined in the XML Schema.

Schema information for each Web Access page is provided in separate HTML files. See “Viewing Web Access Schema Information” on page 4-45 for more information.

Altova StyleVision Power Stylesheet (SPS)

The Altova StyleVision 2005 tool enables you to customize the Web Access interface by editing proprietary XSLT-based stylesheets called StyleVision Power Stylesheets (SPS). Johnson Controls provides the SPS source files for each page of the Web Access interface.

Extensible Stylesheet Language Transformation (XSLT)

XSLT is a language used to transform XML documents into other documents. Upon completion of the Web Access interface customization, standard XSLT files are generated from the SPS files, and are copied to a designated P2000 folder.

Overview of Customization Steps

Customizing the Web Access interface consists of the following steps:

1. Determine how the customized interface(s) will be deployed. Will you use a single interface? Will you have multiple interfaces? Will you only be customizing selected pages? Will you customize the interface for PDA devices? Do you want the interface to support languages other than English? How many users (cardholders) will be using the new interface?
2. Make a backup copy of the default style. See page 4-39.
3. Create one or more new style folders (for multiple interfaces only) to store the SPS files used to customize the Web Access interface. See page 4-39.

4. Launch Altova StyleVision and edit the SPS source files, as needed. See page 4-44.
5. Generate XSLT files from the edited SPS files using StyleVision and save them to a designated P2000 directory and subdirectories, as applicable. See page 4-46.
6. If using multiple interfaces, create a UIstyle user-defined field (UDF) in P2000 and assign users (cardholders) to the new style. See page 4-47.

Interface Customization Options

The Web Access application can be customized for different purposes. For example, you may want two interfaces for two different groups of Web Access users. This section describes the different customization options to aid you in your decision, since selecting a particular option has specific requirements.

NOTE

You may deploy one or more of the options described in this section (they are not mutually exclusive). For example, you may customize a single interface for desktop viewing, customize the interface for PDA devices, and create styles that support multiple languages.

Single Interface (Standard PC Viewing)

The Web Access default interface can be customized and deployed for all users for viewing on standard PCs. This is the most common choice for those wishing to customize the Web Access interface.

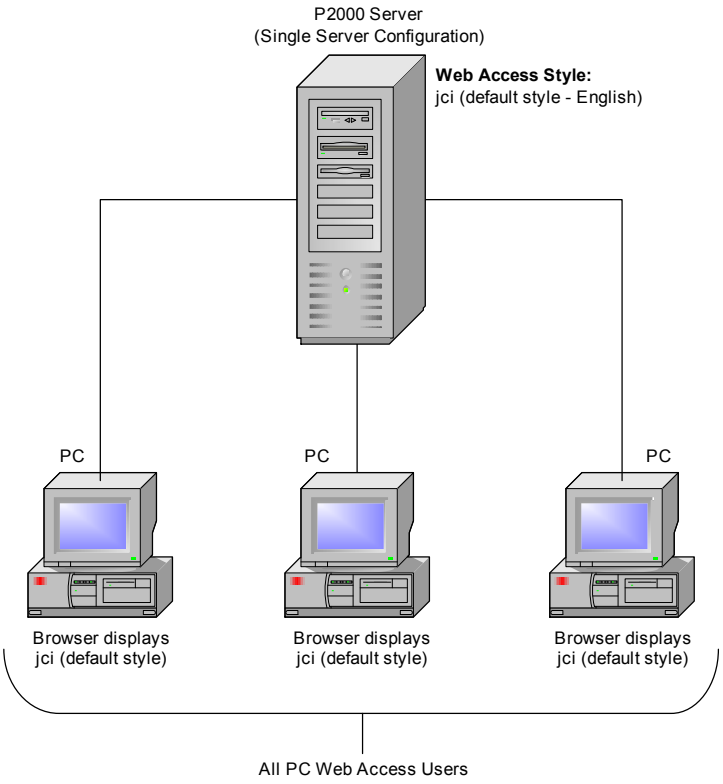


Figure 4-3: Single Interface Deployment

The SPS source files used to generate this interface can be edited once a backup copy of the files have been saved to another location (see “Backing Up the JCI Default Interface Style” on page 4-39).

Multiple Interfaces (Standard PC Viewing)

This option enables you to a create multiple Web Access interfaces for specific users. This is accomplished by creating a style folder for each additional style you wish to deploy. Each user not using the default style must be assigned to the new style(s) via a "UIstyle" user-defined field (UDF). See "Assigning Users to a New Style (Multiple Interfaces Only)" on page 4-47 for more information.

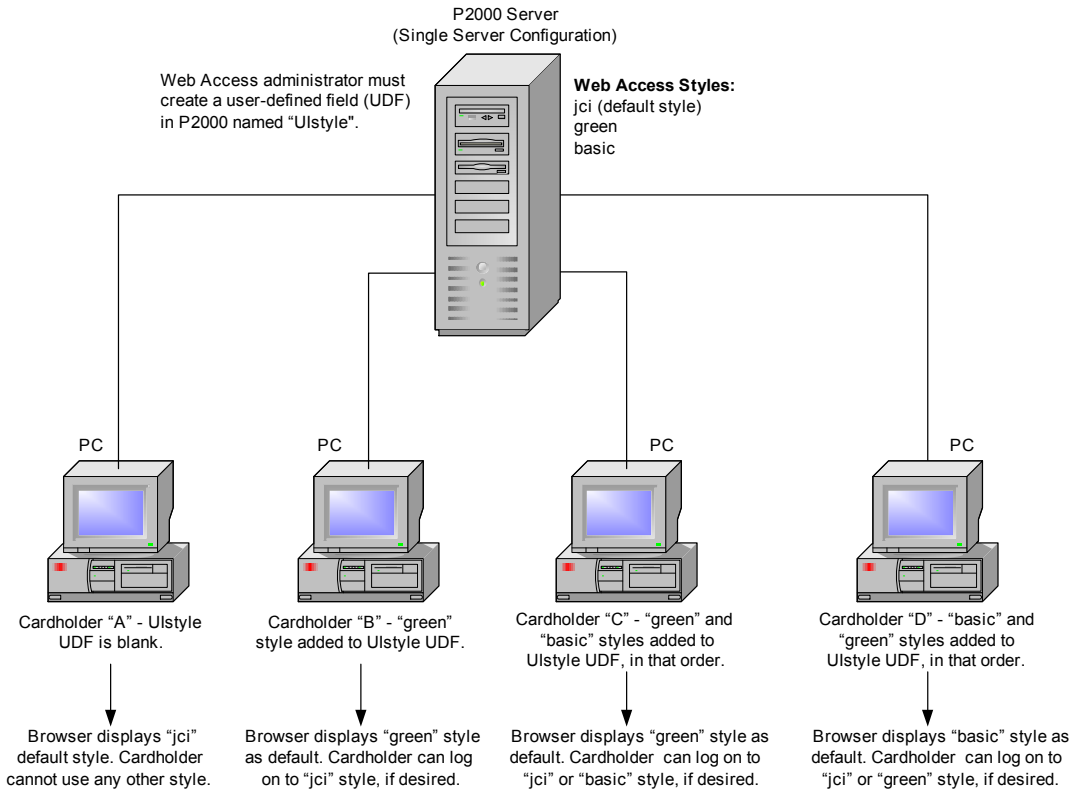


Figure 4-4: Deployment of Multiple Interfaces

All P2000 Web Access users/cardholders are automatically assigned to the default interface. If you create a new interface for a group of users, each user within that group must be manually assigned to it via the "UIstyle" UDF. This can be time consuming if you plan to add fifty or more users to a new interface.

PDA Device Interface

Web Access includes separate SPS files for Web pages viewed on Personal Digital Assistant (PDA) devices. This enables you to customize different Web Access interfaces for PCs and PDAs. See “The Web Access Directory and File Structure” on page 4-37 for information on how the files are structured for the different platforms.

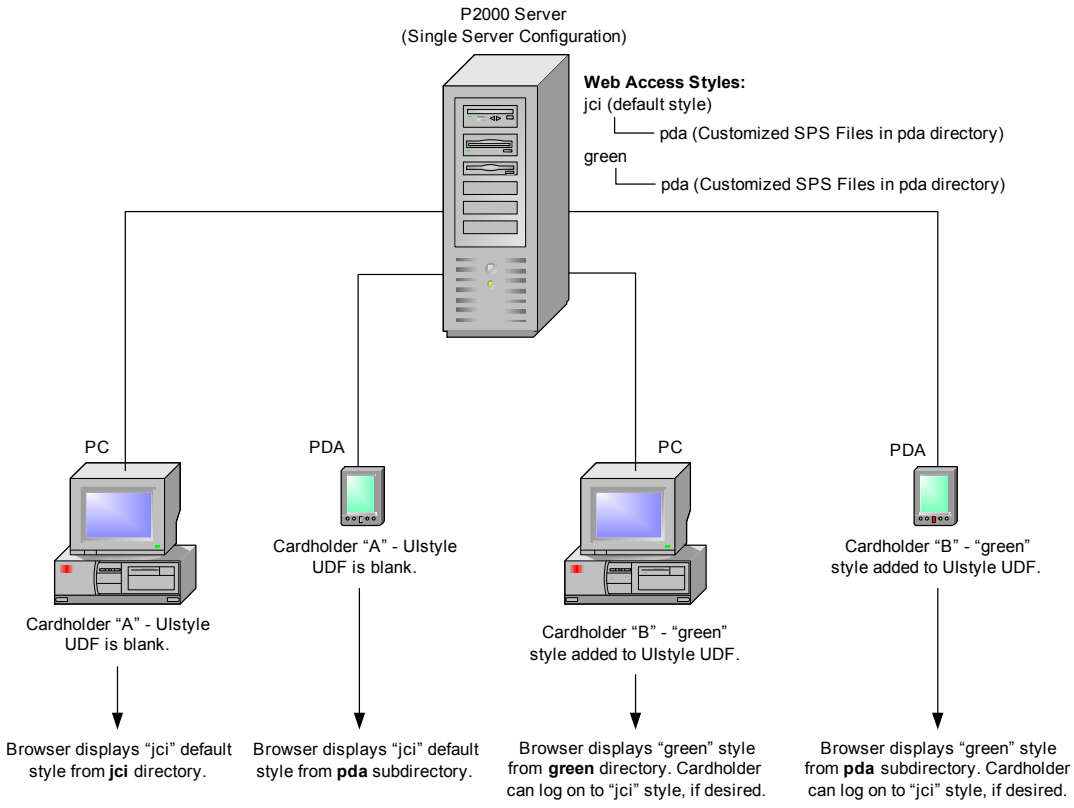


Figure 4-5: PDA Deployment

Language Support

Web Access can be configured to display an interface style based on the language setting of the end user's browser. This is accomplished by creating a style and suffixing it with a dash ("-") and a two-digit language code (for example, "jci-fr," where "jci" is the style name and "fr" is the language code for French).

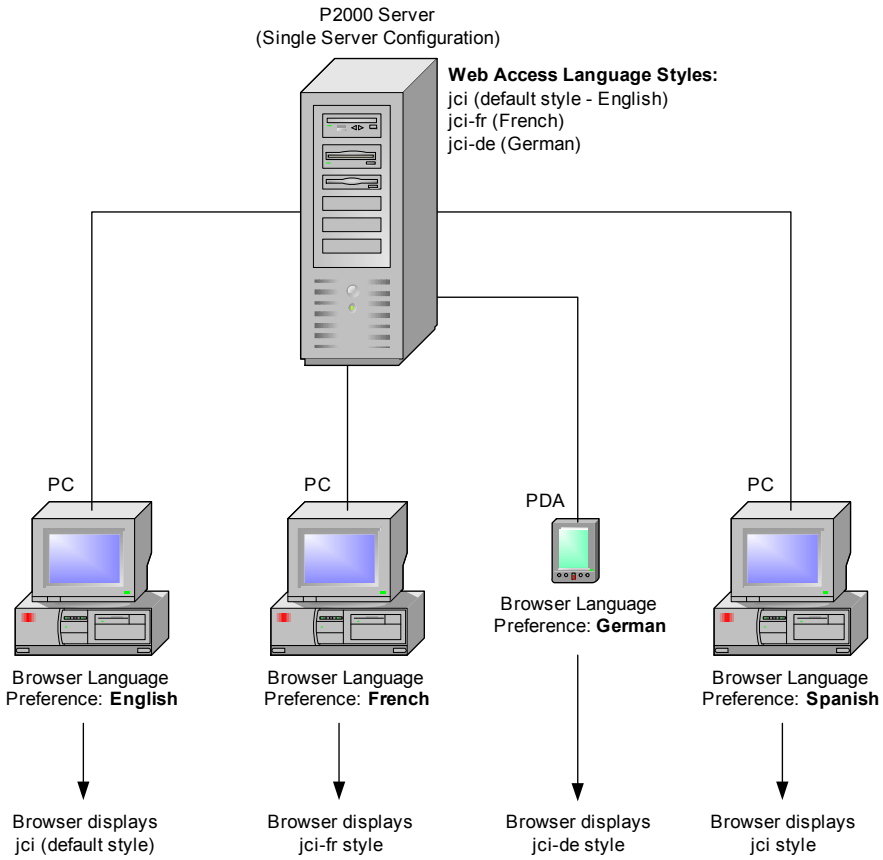


Figure 4-6: Language Styles

The default language is English. Johnson Controls also provides interface styles for French and German. The customer is responsible for translating the interface text into other desired languages. We simply enable you to set a style to display according to the language setting of the user's browser. If a user's browser is set to a language that does not have a corresponding Web Access language style, the default style (jci) will be displayed in English (see the PC set to Spanish in Figure 4-6).

NOTE

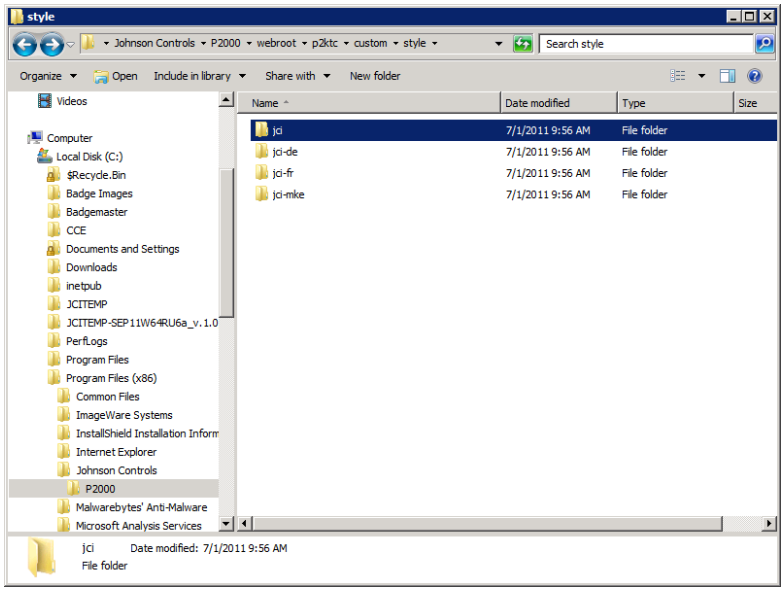
The P2000 Web Access application does not support language variants (for example, Canadian French, Mexican Spanish, etc.), which requires a four digit language code (for example, "fr-ca" for Canadian French). Web Access supports only the first two digits (for example, "fr" for French from France).

The Web Access Directory and File Structure

Understanding the Web Access directory structure is necessary to successfully deploy the customization options. Read the following information to learn more about the directories, subdirectories and files used to customize the Web Access interface.

p2ktc\custom\style\jci

Path: *Local Disk:\Program Files\Johnson Controls\P2000\webroot\p2ktc\custom\style\jci*

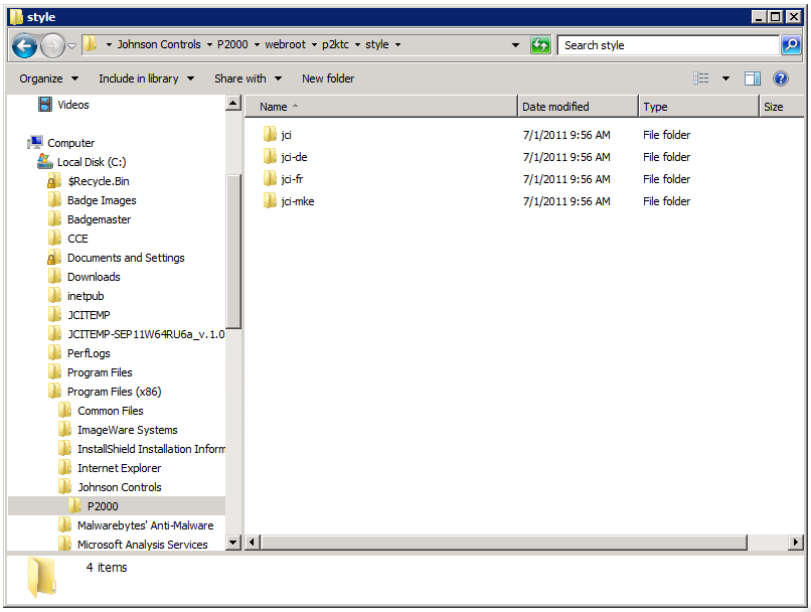


- The *p2ktc\custom\style\jci* directory stores the SPS source files used for the Web Access default interface.
- Before editing the default interface, make a backup copy of the **jci** directory and save it in secure location, preferably in a directory that is backed up regularly. See “Backing Up the JCI Default Interface Style” on page 4-39.
- If you are using a single interface, you may edit files directly in the *p2ktc\custom\style\jci* directory once a backup of the directory has been saved.
- If you are using multiple styles, copy the **jci** directory and save it in the same or another location. Rename the folder according to the type of style you are creating (for example, “green”). If a different language will be supported, rename the folder “*stylename-xx*”, where stylename is the name you have assigned to the folder, and *xx* is the language code your browser uses to determine language preference (for example, “jci-ja” for the jci style displayed in Japanese).

- The **jci** directory includes subdirectories containing SPS files. Each SPS file corresponds to a Web Access page and determines how the page will appear on standard PC monitors. The subdirectories organize the SPS files according to page type. For example, the **CHR** subdirectory groups the SPS files associated with cardholder-specific pages (for example, Cardholder Search page, Add Cardholder page, Edit Cardholder page, etc.).
- Each **jci** subdirectory includes a **pda** subdirectory, which contains SPS files for viewing Web Access pages on a PDA device. Editing the SPS files in the PDA subdirectory will only affect how the pages appear on a PDA device. It will not affect how pages appear on a standard PC monitor. Conversely, editing the SPS files in the jci subdirectories will not affect the pages viewed on a PDA device.

p2ktc\style

Path: *Local Disk:\Program Files\Johnson Controls\P2000\webroot\p2ktc\style*



- The *p2ktc\style* directory stores the XSLT files generated using the Altova StyleVision software tool.
- When using a single interface, you will be replacing the XSLT files in the **jci** subdirectory with the updated XSLT files. The XSLT files are located in subdirectories in the **jci** directory.
- When using multiple interfaces, save a copy of the **jci** directory and rename it according to the style you have created (for example, “green”). Then replace the existing XSLT files in the directory with the ones generated in StyleVision. The new folder must retain the same subdirectory and file structure as the **jci** directory, which is why you will be working with a copy of the **jci** directory.

Getting Started

Installing Altova StyleVision

Install the Altova software on a computer that will be used to edit the SPS source files. Refer to Altova's user documentation for installation assistance.

Backing Up the JCI Default Interface Style

Create a backup copy of the default Web Access interface. This will enable you to use the default interface at any time in the future, regardless of the changes you make to the SPS files in the *\Local Disk:\Program Files\Johnson Controls\P2000\webroot\p2ktc\custom\style\jci* directory.

To create a backup copy of the default style:

1. Open Windows Explorer and access the following directory:

   Local Disk:\Program Files\Johnson Controls\P2000\webroot\p2ktc\custom\style
2. Right-click over the **jci** subdirectory and select **Copy** from the pop-up menu.
3. Paste the **jci** directory into a location where you wish the backup source files to reside. You may save the directory in the **style** folder if desired.
4. (Optional) Rename the directory to better describe it (for example, jci backup, default interface, etc.).

Directory Management

The following subsections describe how to set up the directories needed to edit and deploy the Web Access interface style(s).

Creating Source and Deployment Directories for the New Interface Style

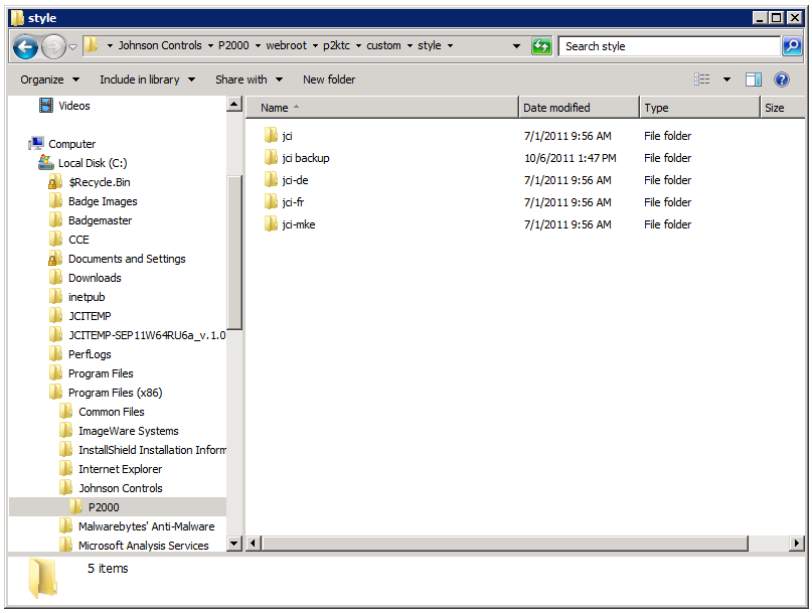
Follow the steps in this section if you are deploying more than one Web Access interface style. The source directory will be used to store the SPS files of the new style. The deployment directory will be used to store the generated XSLT files.

If using a single interface, you will be editing the files in the **jci** directory and therefore, you will not need to create a new directory (skip to "Editing the SPS Web Access Source Files" on page 4-44). If you will create a language-specific style directory, see "Creating Source and Deployment Directories for a Language-specific Style" on page 4-42.

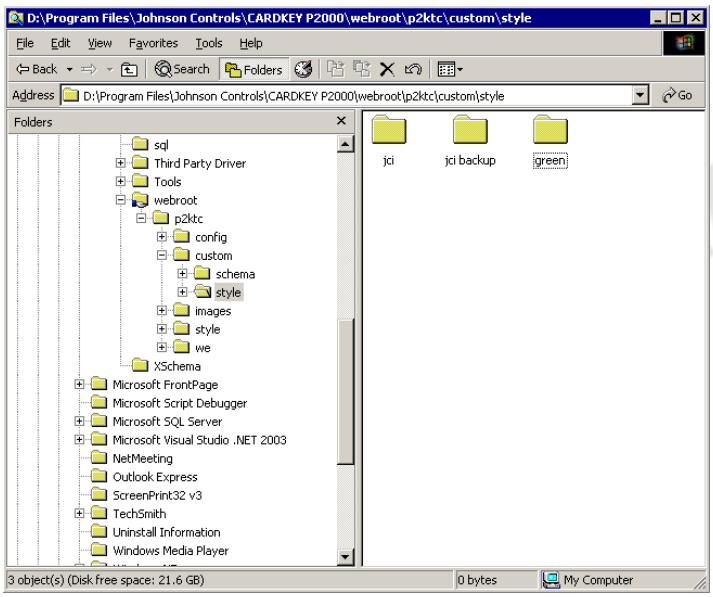
➤ **To create a source directory for the new interface style:**

1. Open Windows Explorer and access the following directory:

   Local Disk:\Program Files\Johnson Controls\P2000\webroot\p2ktc\custom\style



2. Right-click over the **jci** subdirectory and select **Copy** from the pop-up menu.
3. Paste the **jci** directory into a location where you wish the new style folder and source files to reside. You may save the directory in the **style** folder.
4. Rename the directory to better describe the new style (for example, “green”, “basic”, etc.).

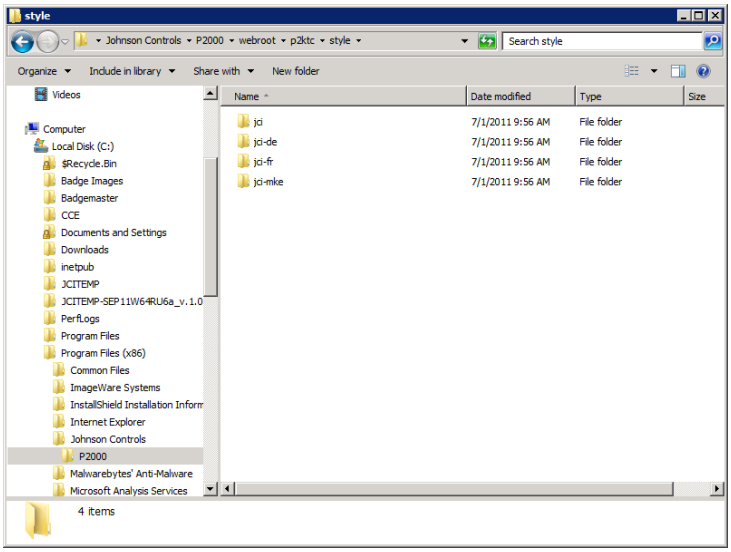


5. Repeat the steps for each style you wish to create.

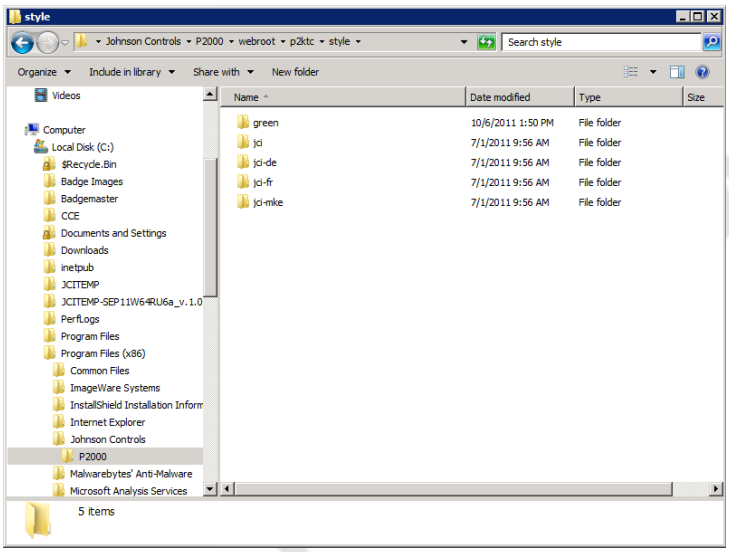
➤ To create a deployment directory for the new interface style:

1. Access the following directory:

   Local Disk:\Program Files\Johnson Controls\P2000\webroot\p2ktc\style



2. Right-click over the **jci** subdirectory and select **Copy** from the pop-up menu.
3. Paste the **jci** directory into the same **style** directory.
4. Rename the **copy of jci** directory to the same name given to the style created in the *Local Disk:\Program Files\Johnson Controls\P2000\webroot\p2ktc\custom\style* directory (for example, “green”).



The XSLT files in the new style folder will be replaced with the files you generate from the new style's edited SPS source files.

5. Repeat the steps for each style you have created.

Creating Source and Deployment Directories for a Language-specific Style

Follow the steps in this section if deploying one or more Web Access interface styles edited to display a language other than English, French, or German. The source directory will be used to store the SPS files of the new style. The deployment directory will be used to store the generated XSLT files. See "Language Support" on page 4-36 for more information.

➤ **To create a source directory for a language-specific style:**

1. Access the directory where the source subdirectories for your styles reside.
2. Right-click over the directory that will be used to create a language-specific style and select **Copy** from the pop-up menu. For example, copy the **jci** directory if you will create a **jci** style for a language other than English.
3. Paste the directory and its contents into the directory where the other source subdirectories reside.
4. Rename the directory by adding a dash ("-") and a two-digit language code to the directory name.

   Examples:

   - "jci-zh" (default style for browsers set to Chinese)
   - "green-es" (style with name "green" for browsers set to Spanish)

   Refer to the following list for various language codes. For additional codes, refer to your browser documentation.

   Language (code)

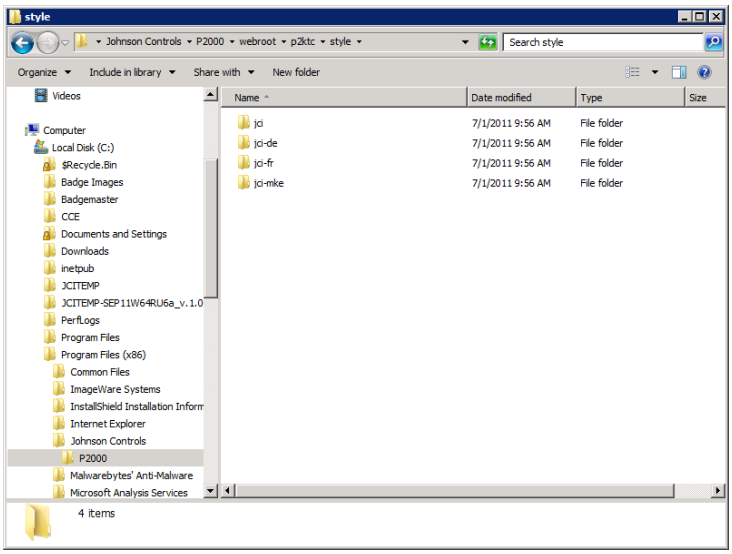
   Arabic (ar)
   Italian (it)
   Japanese (ja)
   Korean (ko)
   Russian (ru)
   Portuguese (pt)
   Swedish (sv)

5. Repeat the steps for each language-specific style you wish to create.

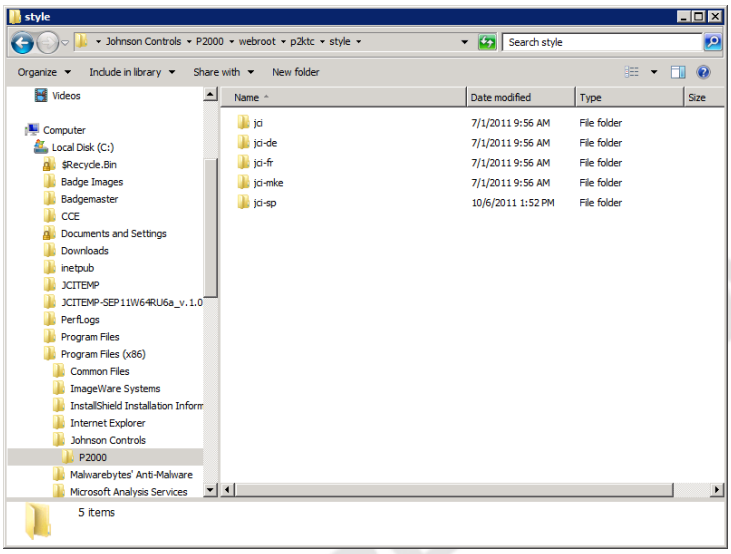
➤ To create a deployment directory for a language-specific style:

1. Access the following directory:

   Local Disk:\Program Files\Johnson Controls\P2000\webroot\p2ktc\style



2. Right-click over the **jci** subdirectory and select **Copy** from the pop-up menu.
3. Paste the **jci** directory into the same **style** directory.
4. Rename the **copy of jci** directory to the same name given to the language-specific source style (for example, “jci-sp”).



   The XSLT files in the new style folder will be replaced with the files you generate from the new style’s edited SPS source files.

5. Repeat the steps for each language-specific style you have created.

Editing the SPS Web Access Source Files

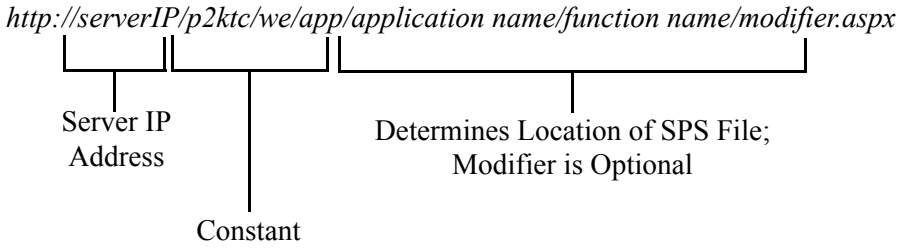
To customize the interface style(s), use the Altova StyleVision XML editing tool to edit the SPS source files. If you are simply editing a single interface, edit the SPS source files in the following directory:

Local Disk:\Program Files\Johnson Controls\P2000\webroot\p2ktc\custom\style\jci

Determining which SPS files to edit is the next step. As stated earlier, each SPS and XSLT file correspond to a Web Access page. For example, the Cardholder Search page has a single source file (CardholderSearch.sps) and a single deployment file (CardholderSearch.xslt) of the same name. If you want to edit this page, use StyleVision to open and edit the CardholderSearch.sps file (SPS files are proprietary StyleVision files).

FAQ: *How do I locate the source file for a specific Web Access page?*

Log on to Web Access and navigate to the page you'd like to edit. The address in the Address bar displays the location of the page's SPS file according to the following structure:



Application Name: Corresponds to the subdirectory (for example, bactivity, BResync, CHR, MC, etc.) located in the style directory.

Function Name: Corresponds to the SPS file name (for example, /cardholdersearch.aspx corresponds to the CardholderSearch.sps file).

Modifier: Some pages have modifiers such as "adv", "bio", etc. The Function Name and Modifier correspond to the SPS file name (for example, /cardholdersearch.adv.aspx corresponds to the CardholderSearch.adv.sps file).

Examples:

- *http://138.522.109.254/p2ktc/we/app/bactivity/cardholdersearch.aspx*

  PC Interface: Edit the CardholderSearch.sps file in the *stylename**bactivity* directory.

  PDA Interface: Edit the CardholderSearch.sps file in the *stylename**pda**bactivity* directory.

- *http://138.522.109.254/p2ktc/we/app/bactivity/cardholdersearch.adv.aspx*

  PC Interface: Edit the CardholderSearch.adv.sps file in the *stylename**bactivity* directory.

  PDA Interface: Edit the CardholderSearch.adv.sps file in the *stylename**pda**bactivity* directory.

- *http://138.522.109.254/p2ktc/we/app/vm/vmrequest.aspx*

  PC Interface: Edit the VMRequest.sps file in the *stylename**vm* directory.

  PDA Interface: Edit the VMRequest.sps file in the *stylename**pda**vm* directory.

Viewing Web Access Schema Information

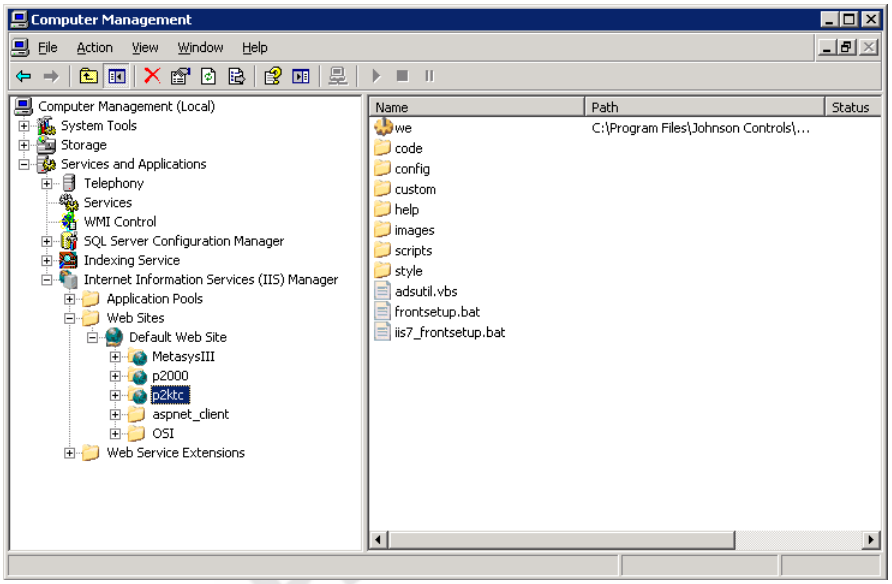
Schema information (for example, data elements and attributes) for each Web Access page is provided in separate HTML files. To view this information:

NOTE

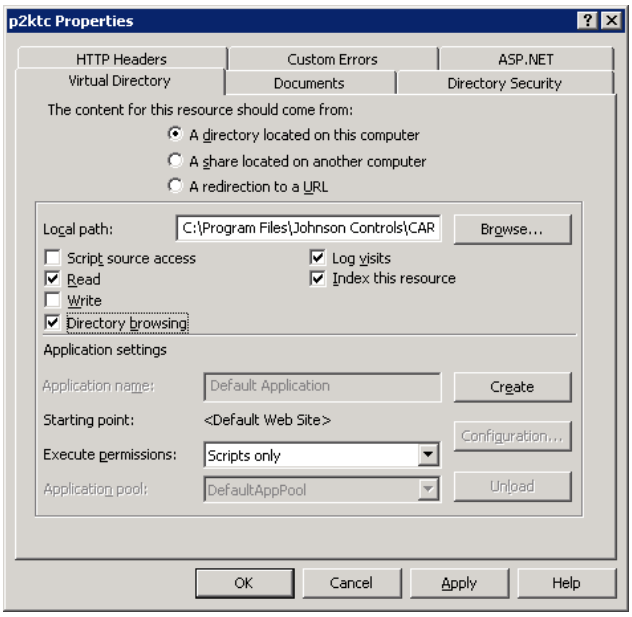
If P2000 is installed on a server running Windows Server 2008, skip to step 7.

1. From the P2000 server's desktop, right-click over **My Computer** and select **Manage**.
2. In the left pane, navigate to the following folder:

   *Computer Management (Local)**Services and Applications**Internet Information Services (IIS) Manager**Web Sites**Default Web Site*



3. Right-click over **p2ktc** and select **Properties**. The p2ktc Properties dialog box appears.
4. Select the **Virtual Directory** tab.
5. Select the **Directory browsing** check box.



6. Click **OK**.
7. Enter the following URL:

   *http://***P2000 Server Name or IP Address***/p2ktc/custom/schema*

   Examples:

   - **Using IP Address:** *http://122.43.78.54/p2ktc/custom/schema*
   - **Using Server Name:** *http://b7p2kserver1/p2ktc/custom/schema*

The index page that appears consists of links for each Web Access page. Each link opens an HTML file consisting of schema information for the selected page.

Generating XSLT Files

When you are finished editing the SPS files, use StyleVision to generate XSLT files for each Web Access page you have edited. Replace the corresponding XSLT files in the correct directory. For example:

If you update the following SPS source file:

Local Disk:\Program Files\Johnson Controls\P2000\webroot\p2ktc\custom\style\jci\bactivity\CardholderSearch.sps

Then you will replace the following XSLT file with the updated copy:

Local Disk:\Program Files\Johnson Controls\P2000\webroot\p2ktc\style\jci\bactivity\CardholderSearch.xslt

Assigning Users to a New Style (Multiple Interfaces Only)

When using multiple styles, each Web Access user who will use the new style must have it assigned to him/her via the UIstyle user-defined field (UDF). Start by creating this UDF with the following minimum settings:

- **Name:** UIstyle
- **Type:** Text
- **Width**: 32

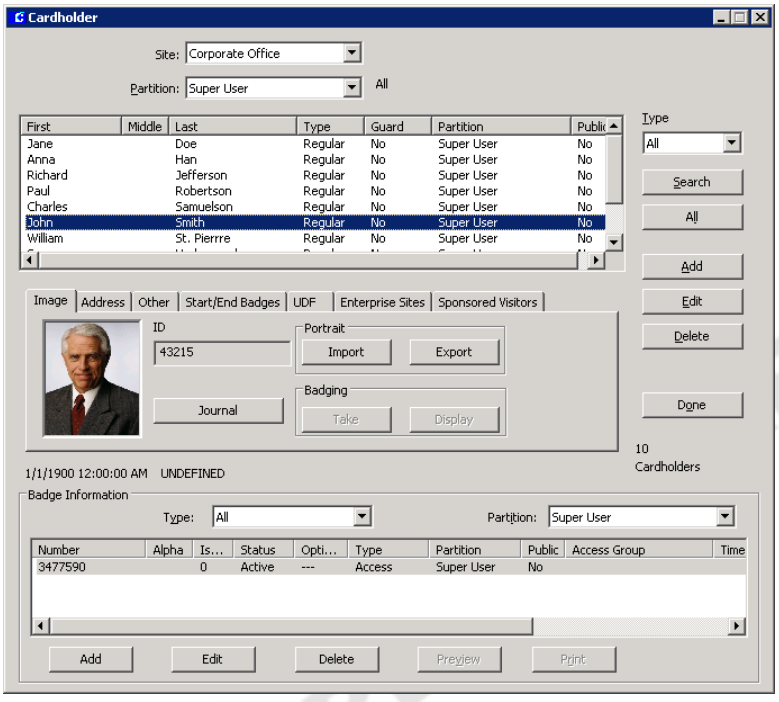
Enter the Name text exactly as shown. The letter case must match: **UI** should be uppercase letters and **style** should be lowercase letters. Do not add spaces.

For detailed information on creating a UDF, refer to the *P2000 Software User Manual*.

Once you have created the UIstyle UDF, assign the desired users (cardholders) to one or more of the new styles.

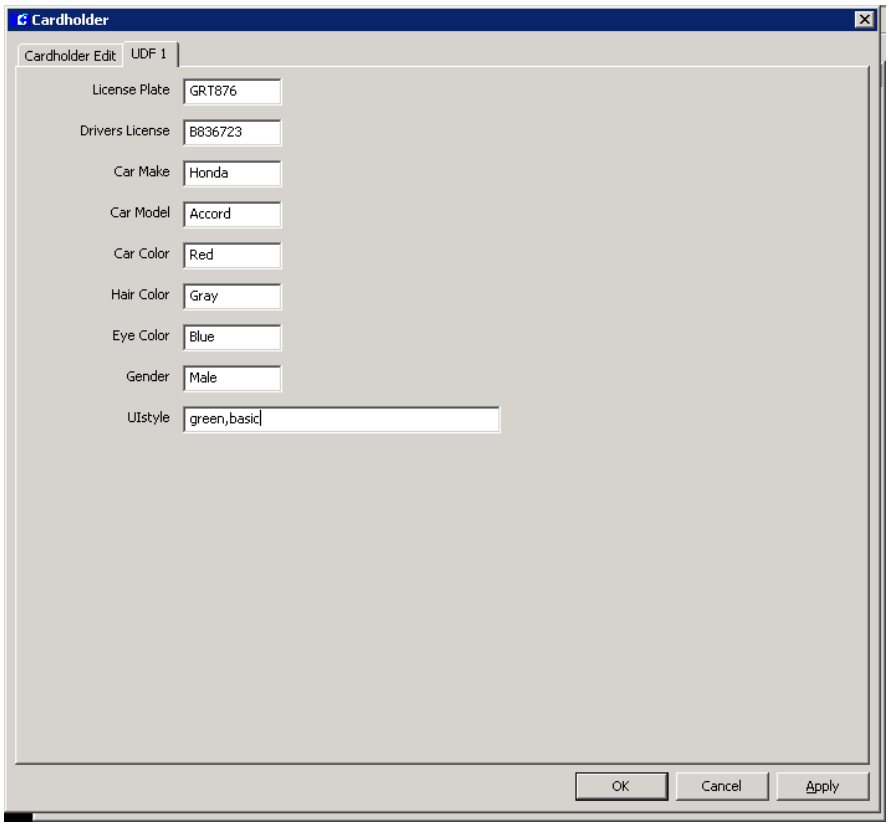
➤ To assign users to a new style:

1. In P2000, click the **Access Cardholder** button on the toolbar, or select **Access>Cardholder** from the Main menu bar. The Cardholder window appears.
2. Select the user (cardholder) whom you will assign to the new style(s).



3. Click **Edit** on the right side of the window. The Cardholder Edit dialog box appears.
4. Select the **UDF** tab.

5. To assign a style to the user (cardholder), enter the style name into the **UIstyle** field. The name must match the directory style name (for example, green).
6. If multiple new styles will be assigned to the user, enter the names of the styles separated with a comma (for example, `green,blue`).



7. Click **OK**.

Selecting a Different Style During Login

A user who has been assigned multiple styles can select a particular one during login by entering the **Username** as:

`firstname.lastname@stylename`

Example: *john.smith@green*, where "green" is the style name.

If the user simply enters `firstname.lastname` (without `@stylename`), the system will display the default style.

Setting a New Default Style

The factory default style is “jci”. Any user not assigned a different style will use this interface. Typically, there is no need to change the default style. If you need to change the interface for most or all of the Web Access users, simply edit the “jci” style files. Follow the instructions in this section to set a new default style.

➤ **To set a new default style:**

1. Access the following directory: *Local Disk:\Program Files\Johnson Controls\P2000\webroot\p2ktc\we*
2. Open the **Web.config** file in a text editor, such as Microsoft Notepad.
3. Locate the following text:
   <add key="JCI.P2000.ThinClient.FactoryStyle" value="jci" />
4. Replace ***jci*** with the name of the new default style.
   Example:
   <add key="JCI.P2000.ThinClient.FactoryStyle" value="green" />
5. Click **File>Save**.

OTHER CONFIGURATION OPTIONS

This section describes how to edit various configuration options in Web Access. These options allow you to change the operation or behavior of certain Web Access applications. Specifically, these options allow you to do the following:

- Change the session time-out period. See page 4-50.
- Edit the maximum number of cardholders to display on the Cardholder Search Results page and on the Current Cardholder Status page (In-Out Display application). See page 4-51.
- Enable users to assign areas when viewing the in-out status of cardholders. See page 4-54.
- Disallow users from changing the badge resync setting to In, Out and/or Undefined. See page 4-55.
- Change the default Visit Start and End Date/Time settings on the Visitor Management application. See page 4-56.
- Configure the system to send an E-mail when a visitor request is submitted. See page 4-58.
- Configure the system to use Active Directory Authentication. See page 4-63.

Changing the Session Time-out Period

This configuration option allows you to change the number of minutes until a Web Access session times out due to user inactivity.

Default Setting = 5 minutes

Maximum Setting Allowed = 20 minutes

➤ To change the time-out period:

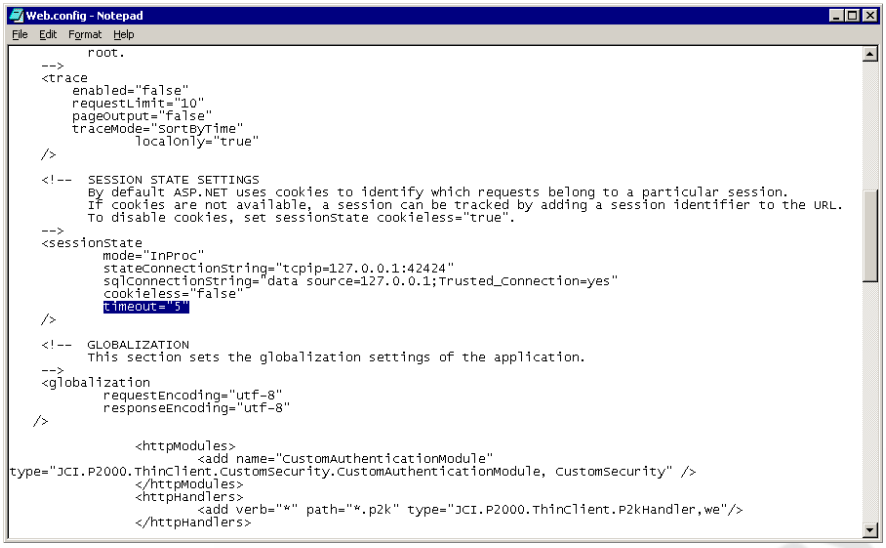
1. Access the following directory on the P2000 server:

   <Local Disk>:\Program Files\Johnson Controls\P2000\webroot\p2ktc\we

2. Open the **Web.config** file in a text editor, such as Microsoft Notepad.
3. Locate the following text:

   timeout="n"

   n is a variable number.



4. Edit the number accordingly.

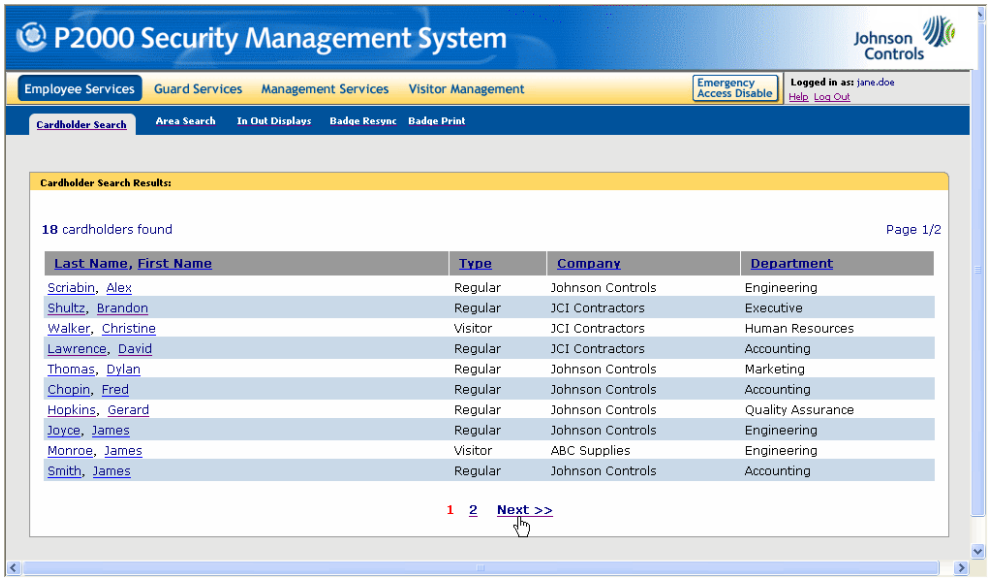
   Examples:

   - `timeout="10"` (session will time out after ten minutes of inactivity)
   - `timeout="20"` (session will time out after twenty minutes of inactivity)

5. Click **File>Save**.

Changing the Maximum Number of Cardholders to Display

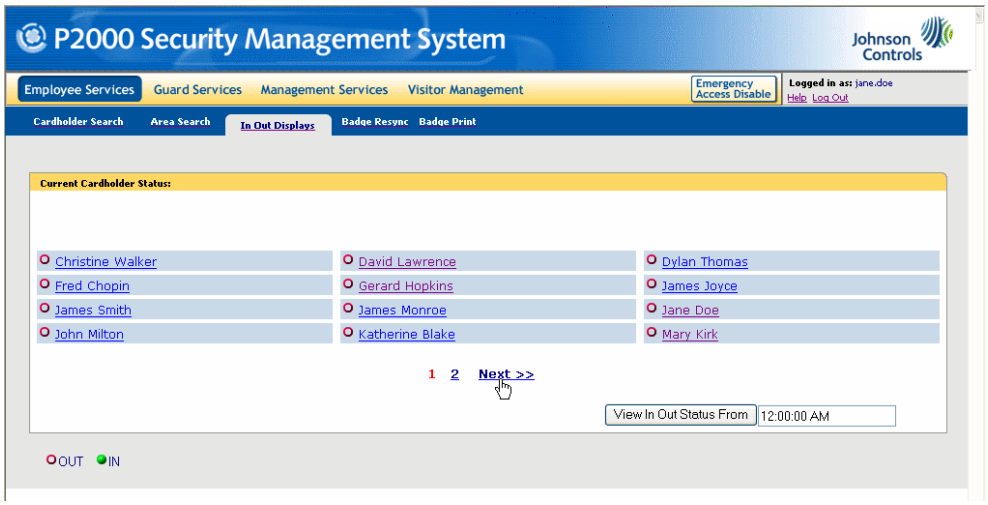
Web Access allows you to configure the maximum number of cardholders you wish to display at a time on the Cardholder Search Results page and the Current Cardholder Status page (In-Out Display application). For example, if the default number of cardholders listed for the Cardholder Search Results page is 10 and your search yields 50 cardholders, only a maximum of 10 cardholders can be listed at a time on the page. Clicking the **Next** link displays the remaining cardholders, 10 at a time.



The Current Cardholder Status page for the In-Out Display application lists the cardholders who are *In* or *Out* of the facility based on their badge activity.

For more information on the Cardholder Search Results page, see “Searching Cardholder Records” on page 3-1.

For more information on the Current Cardholder Status page, see “In/Out Status” on page 3-11.



There are three ways to modify the number of cardholders listed per page during a cardholder search or when viewing cardholders with the In-Out Display application. The following methods are listed in hierarchical order; the first method listed takes precedence over the next bulleted method, and so on.

- Appending `&ipp=n` to the page's URL (Temporary) (see "Changing the Number of Cardholders Listed Per Page" on page 3-4 for more information)
- Modifying the ItemsPerPage parameter in the page's associated XSLT file (this parameter is removed by default, but could be added manually)
- Modifying the ItemsPerPage parameters in the **We.config** file located at:

  <Local Disk>:\Program Files\Johnson Controls\P2000\webroot\p2ktc\config\WE

For example, if the We.config file's ItemsPerPage parameter is set to 10 and the system administrator adds an ItemsPerPage parameter value of 5 to the page's XSLT file, the page will display 5 cardholders at a time (the XSLT file takes precedence over the We.config file). If the user appends `&ipp=20` to the page's URL, the page will temporarily display 20 cardholders at a time (appending `&ipp=n` to the URL takes precedence over all other ItemsPerPage parameters).

Default Setting of We.config File's ItemsPerPage Parameter (Cardholder Search Results page) = 10 cardholders listed per page

Default Setting of We.config File's ItemsPerPage Parameter (Current Cardholder Status page) = 81 cardholders listed per page

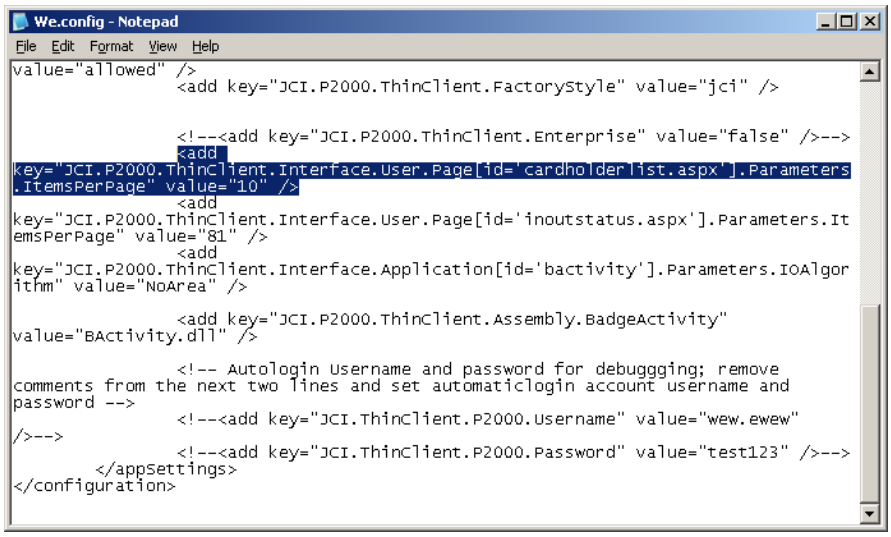
➤ To change the maximum number of cardholder search results by modifying the ItemsPerPage parameter in the We.config file:

1. Access the following directory on the P2000 server:

   <Local Disk>:\Program Files\Johnson Controls\P2000\webroot\p2ktc\WE
2. Open the **We.config** file in a text editor, such as Microsoft Notepad.

3. Locate the following text:

   <add key="JCI.P2000.ThinClient.Interface.User.Page[id='cardholderlist.aspx'].Parameters.ItemsPerPage" value="10" />



4. Edit the number (`value="10"`) accordingly.

   Example:

   - `value="20"` (page will display up to 20 cardholders at a time)

5. Click **File>Save**.

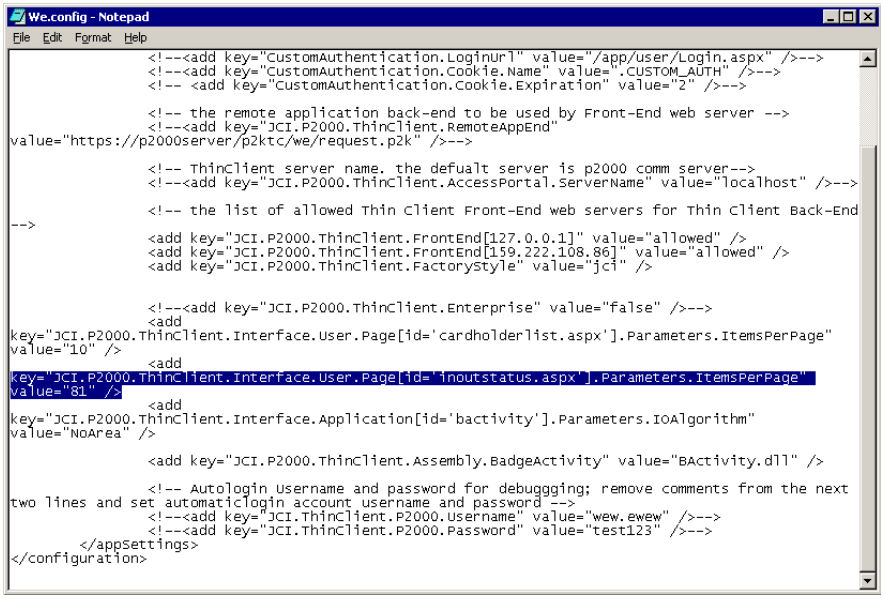
➤ To change the maximum number of cardholder status results:

1. Access the following directory on the P2000 server:

   <Local Disk>:\Program Files\Johnson Controls\P2000\webroot\p2ktc\WE

2. Open the **We.config** file in a text editor, such as Microsoft Notepad.
3. Locate the following text:

   <add key="JCI.P2000.ThinClient.Interface.User.Page[id='inoutstatus.aspx'].Parameters.ItemsPerPage" value="81" />



4. Edit the number (`value="81"`) accordingly.

   Example:

   - `value="25"` (page will display up to 25 cardholders at a time)

5. Click **File>Save**.

Enabling Users to Assign Areas for Viewing In-Out Status

By default, the system allows users to view the In-Out status of cardholders for the entire facility. That is, if a cardholder badges to enter any door in the facility, his/her status will be “In” until the In-Out status time resets. However, you may change the In-Out setting so that users can view the status of cardholders for one or more areas of the facility. For example, if “Training Room” is a defined area in P2000, a Web Access user can select this area when viewing In-Out status to see who has badged to enter the room today.

The In-Out status configuration option can be set to “WithArea” or “NoArea.”

- “WithArea” **allows** users to assign areas when viewing the In-Out status.
- “NoArea” **does not allow** users to assign areas when viewing the In-Out status.

Default Setting = NoArea

➤ To change the In-Out Status Assign Area setting:

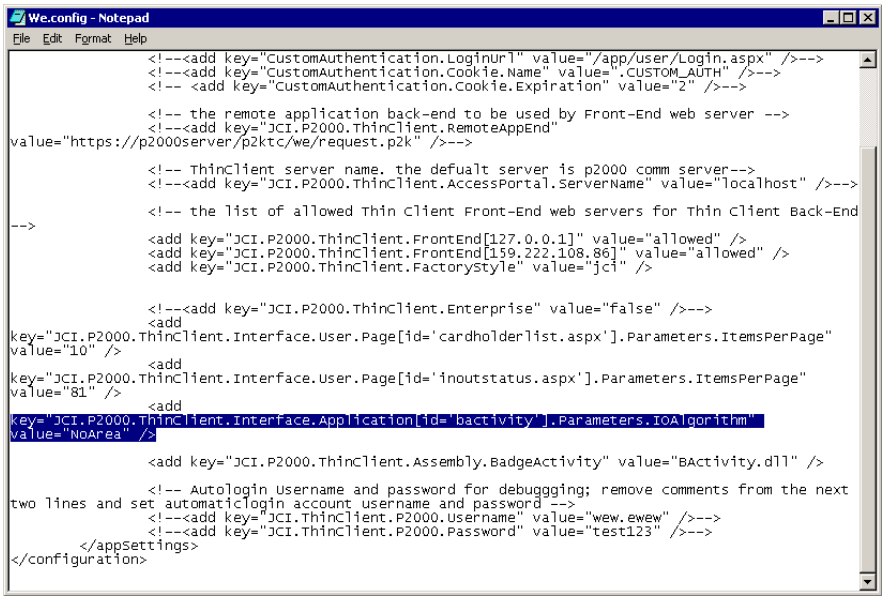
1. Access the following directory on the P2000 server:

   <Local Disk>:\Program Files\Johnson Controls\P2000\webroot\p2ktc\config\WE

2. Open the **We.config** file in a text editor, such as Microsoft Notepad.

3. Locate the following text:

   <add key="JCI.P2000.ThinClient.Interface.Application[id='bactivity'].Parameters.IOAlgorithm" value="NoArea" />



4. Change the "`NoArea`" text to "`WithArea`" or vice versa, depending on the current setting.
5. Click **File>Save**.

Changing the Badge Resync Setting

This option can be configured to disallow users from changing the badge resync setting to In, Out and/or Undefined. For additional information on the Badge Resync feature, see page 3-14.

Default Setting = True (allow)

➤ To change the Badge Resync setting:

1. Access the following directory on the P2000 server:

   <Local Disk>:\Program Files\Johnson Controls\P2000\webroot\p2ktc\config\Bresync

2. Open the **Application.config** file in a text editor, such as Microsoft Notepad.
3. Locate the following text:

   <add key="JCI.P2000.ThinClient.BResync.AllowResyncIn" value="true">

4. To disallow users from changing the badge state to “In,” change "`true`" to "`false`".

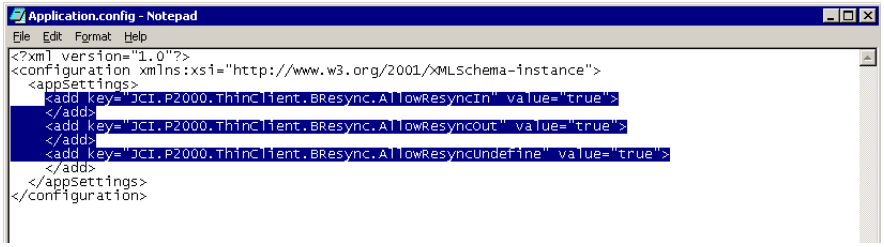
5. Locate the following text:

   <add key="JCI.P2000.ThinClient.BResync.AllowResyncOut" value="true">

6. To disallow users from changing the badge state to “Out,” change `"true"` to `"false"`.

7. Locate the following text:

   <add key="JCI.P2000.ThinClient.BResync.AllowResyncUndefine" value="true">



8. To disallow users from changing the badge state to “Undefined,” change `"true"` to `"false"`.

9. Click **File>Save**.

Changing the Default Visit Start and End Date/Time Settings

The Visitor Management application allows users to request a visitor badge. During this process, they can edit the default Visit Start Date/Time and Visit End Date/Time (the date/time when the visitor will arrive to, and leave from, the facility). This is the time period during which the badge will be valid.

The following settings associated with these fields may be configured:

- **Maximum Visit Period**
  You can define the maximum number of days between the Visit Start Date and Visit End Date. That is, you can control the maximum number of days a visitor can use his/her badge at your facility. For example, if the option is set to 3 days and the user enters a Visit Start Date of 12/1/2009, he/she cannot enter a Visit End Date past 12/3/2009.

  Default Setting = 5 days

- **Default Visit Start and End Times**
  When a user opens the Visitor Management application to request a visitor badge, the system will automatically add a default Visit Start Time and Visit End Time according to the following rules:

  - If the current time is later than [Time AM or PM], then the default Visit Start Time will be [Time AM or PM] tomorrow. If the current time is before [Time AM or PM], the system will display the current time in the Visit Start Time field.

Default Setting = 4 PM and 8 AM
If the current time is later than 4 PM when a user opens the Visitor Management application to request a visitor badge, then the default Visit Start time will be 8 AM tomorrow.

- The default Visit End Time will be [x] number of hours ahead of the default Visit Start Time.

  Default Setting = 1 hour
  Example: If the Visit Start Time is 8:00 AM, the Visit End Time will be 9:00 AM.

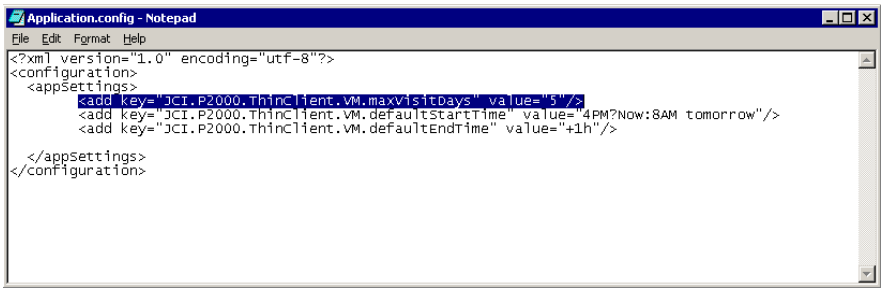
➤ To set the maximum visit period:

1. Access the following directory on the P2000 server:

   <Local Disk>:\Program Files\Johnson Controls\P2000\webroot\p2ktc\config\VM

2. Open the **Application.config** file in a text editor, such as Microsoft Notepad.
3. Locate the following text:

   <add key="JCI.P2000.ThinClient.VM.maxVisitDays" value="5"/>



4. Edit the number (`value="5"`) accordingly.

   Example:

   - `value="3"` (Visitor badges cannot exceed a 3-day validity period)

5. Click **File>Save**.

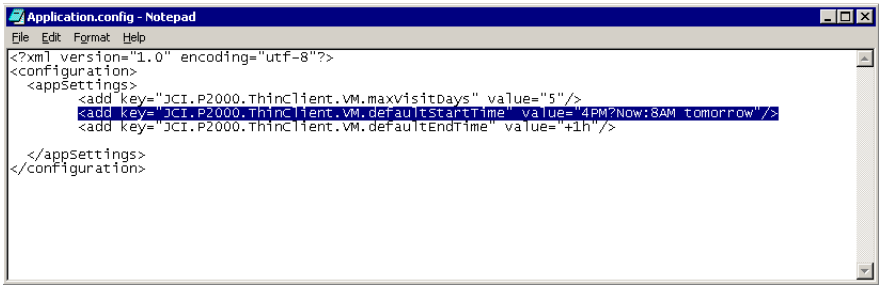
➤ To set the default visit start and end times:

1. Access the following directory on the P2000 server:

   <Local Disk>:\Program Files\Johnson Controls\P2000\webroot\p2ktc\config\VM

2. Open the **Application.config** file in a text editor, such as Microsoft Notepad.
3. Locate the following text:

   <add key="JCI.P2000.ThinClient.VM.defaultStartTime" value="4PM?Now:8AM tomorrow"/>



4. Edit the `4PM` and `8AM` values accordingly. See the following example:

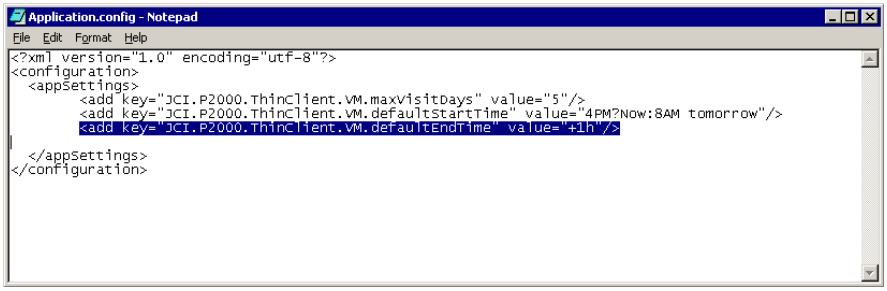
   Example:

   *<add key="JCI.P2000.ThinClient.VM.defaultStartTime" value="**3PM**?Now:**9AM** tomorrow"/>*

   If the current time is later than 3 PM when a user opens the Visitor Management application to request a visitor badge, then the default Visit Start time will be 9 AM tomorrow.

5. Locate the following text:

   <add key="JCI.P2000.ThinClient.VM.defaultEndTime" value="+1h"/>



6. Edit the `+1h` value accordingly. See the following example:

   Example:

   *<add key="JCI.P2000.ThinClient.VM.defaultEndTime" value="+**5**h"/>*

   The Visit End Time will default to five hours after the Visit Start Time.

7. Click **File>Save**.

Configuring the System to Send a Visitor Request E-mail

This feature allows you to configure the system to send an E-mail to specific individuals when a visitor request is submitted; the E-mail can be used to inform them of the request and provide specific instructions.

NOTE

This configuration option only allows you to inform individuals that a visitor request has been submitted, and to provide additional instructions. However, Web Access provides a different feature that allows you to configure the system to send an E-mail to an approver when a visitor request is submitted, allowing the approver to link to the request and approver or reject it (see "Approving or Rejecting Requests" on page 3-23 for more information).

➤ To configure the system to send a visitor request E-mail:

1. Enable E-mail notification in P2000. Refer to the *P2000 Software User Manual* for information.

NOTE

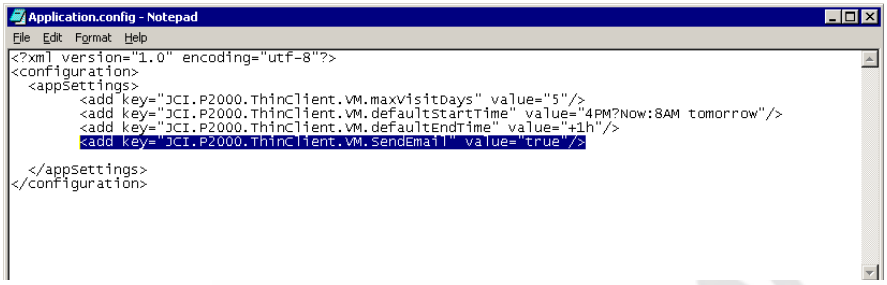
The P2000 server must also be configured as an E-mail server. For more information, contact an IT professional.

2. Access the following directory on the P2000 server:

   <Local Disk>:\Program Files\Johnson Controls\P2000\webroot\p2ktc\config\VM

3. Open the **Application.config** file in a text editor, such as Microsoft Notepad.
4. Add the following text:

   <add key="JCI.P2000.ThinClient.VM.SendEmail" value="true"/>



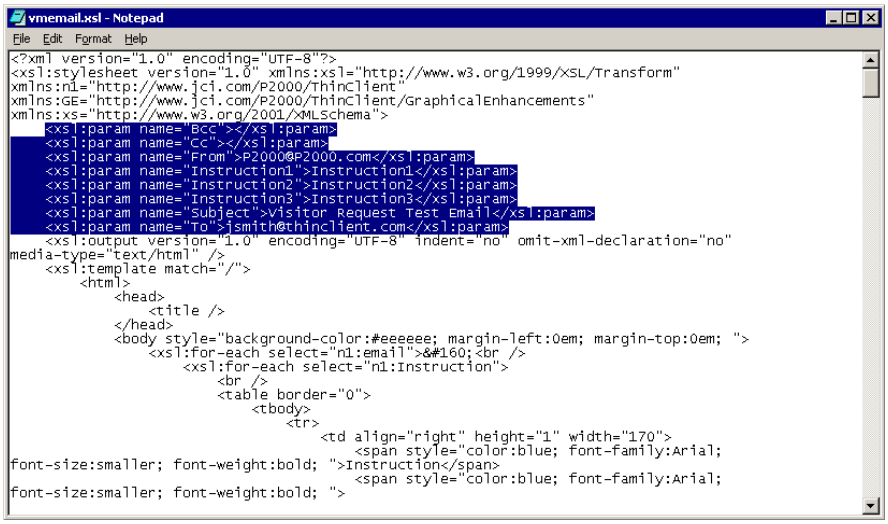
5. Click **File>Save**, and close the file.
6. Open the **vmemail.xsl** file in a text editor, such as Microsoft Notepad.

NOTE

For styles that use a language other than English (see "Language Support" on page 4-36), open the file using a unicode text editor such as EditPad Lite or Lekho.

7. Locate the following text:

   <xsl:param name="Bcc"></xsl:param>
   <xsl:param name="Cc"></xsl:param>
   <xsl:param name="From">P2000@P2000.com</xsl:param>
   <xsl:param name="Instruction1">Instruction1</xsl:param>
   <xsl:param name="Instruction2">Instruction2</xsl:param>
   <xsl:param name="Instruction3">Instruction3</xsl:param>
   <xsl:param name="Subject">Visitor Request Test Email</xsl:param>
   <xsl:param name="To">jsmith@thinclient.com</xsl:param>



8. Edit the text according to information below, which describes the elements line by line. See also “E-mail Notification Configuration Example” on page 4-61.

   <xsl:param name="Bcc"></xsl:param>

   This text element allows you to enter an E-mail address that will be used to send a Blind Carbon Copy (BCC) of the E-mail to the recipient.

   Example: *<xsl:param name="Bcc">**jane.doe@yahoo.com**</xsl:param>*

   <xsl:param name="Cc"></xsl:param>

   This text element allows you to enter an E-mail address that will be used to send a Carbon Copy (CC) of the E-mail to the recipient.

   Example: *<xsl:param name="Cc">**joe.smith@hotmail.com**</xsl:param>*

   <xsl:param name="From">P2000@P2000.com</xsl:param>

   Enter the return address assigned in P2000 (Site Parameters>Edit Site Parameters dialog box>Email tab) by replacing the **P2000@P2000.com** text.

   <xsl:param name="Instruction1">Instruction1</xsl:param>
   <xsl:param name="Instruction2">Instruction2</xsl:param>
   <xsl:param name="Instruction3">Instruction3</xsl:param>

You may add up to three different sets of instructions that will appear in the body of the E-mail. Edit the Instruction1, 2 or 3 text accordingly.

xsl:param name="Subject">Visitor Request Test Email</xsl:param>

This text element allows you to change the E-mail's subject text. The default text is "Visitor Request Test Email."

<xsl:param name="To">jsmith@thinclient.com</xsl:param>

This text element allows you to edit the "To" recipient of the E-mail. The default recipient is "jsmith@thinclient.com."

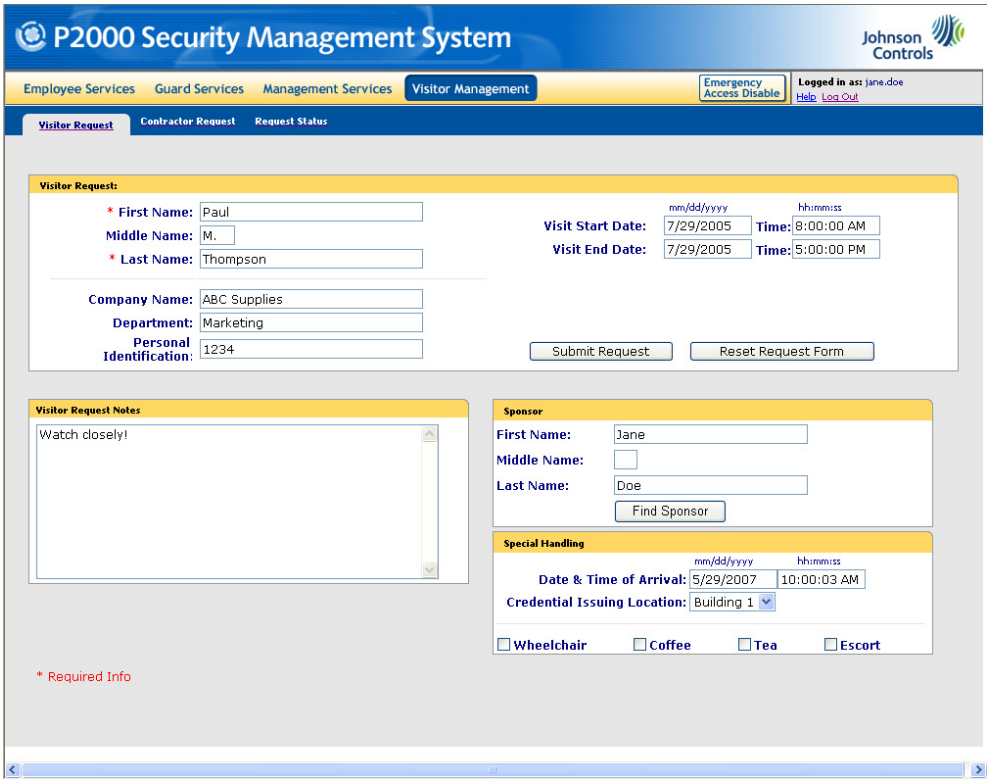
9. Click **File>Save**.

E-mail Notification Configuration Example

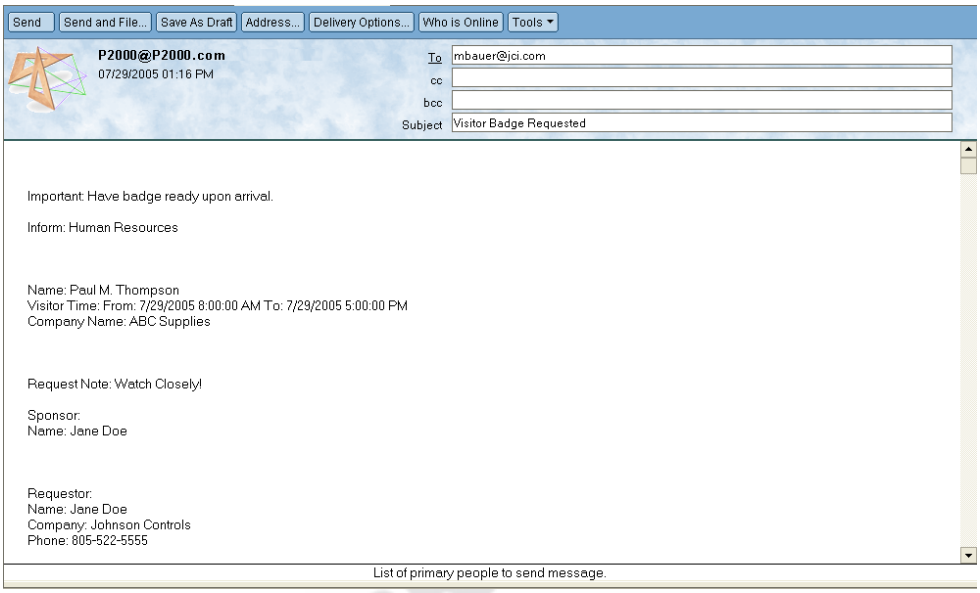
The Visitor Management E-mail notification feature is configured as shown below:

<xsl:param name="Bcc">cwalker@yahoo.com</xsl:param>
<xsl:param name="Cc">mkirk@hotmail.com</xsl:param>
<xsl:param name="From">P2000@P2000.com</xsl:param>
<xsl:param name="Important">Have badge ready upon arrival.</xsl:param>
<xsl:param name="Inform">Human Resources</xsl:param>
<xsl:param name="Instruction3">Instruction3</xsl:param>
<xsl:param name="Subject">Visitor Badge Requested</xsl:param>
<xsl:param name="To">mbauer@jci.com</xsl:param>

A Web Access user enters the following visitor request:



The following E-mail will be sent to mbauer@jci.com (default Visitor Request E-mail template shown):



Customizing the Visitor Request E-mail Template

If you plan to customize the Visitor Request E-mail template for personal layout preferences or for language translation purposes, do the following:

1. Edit the Visitor Request E-mail Template file (**VMEmail.sps**) using the Altova Stylevision stylesheet editor, as needed (see "Altova StyleVision Power Stylesheet (SPS)" on page 4-31).

   The **VMEmail.sps** file is located at:

   *Local Disk:\Program Files\Johnson Controls\P2000\webroot\ p2ktc\custom\style***<style name>***\VM*

   The ***<style name>*** directory varies, depending on the style you wish to edit.
2. Generate an XSLT file (**VMEmail.xslt**). See "Extensible Stylesheet Language Transformation (XSLT)" on page 4-31.
3. Remove the "t" at the end of the file extension, (**VMEmail.xsl**), and copy the file to the following location on the P2000 server:

   Local Disk:\Program Files\Johnson Controls\P2000\webroot\ p2ktc\config\VM

Directory Services Authentication

P2000 Web Access operator passwords can be authenticated against a directory service such as Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP). This eliminates operator passwords from the P2000 database.

This feature is useful in situations where passwords are periodically changed and therefore, eliminates the need to update passwords in the P2000 system and also passwords that are used to log on to Windows.

To use directory service password validation, the following elements must be set up in the P2000 system:

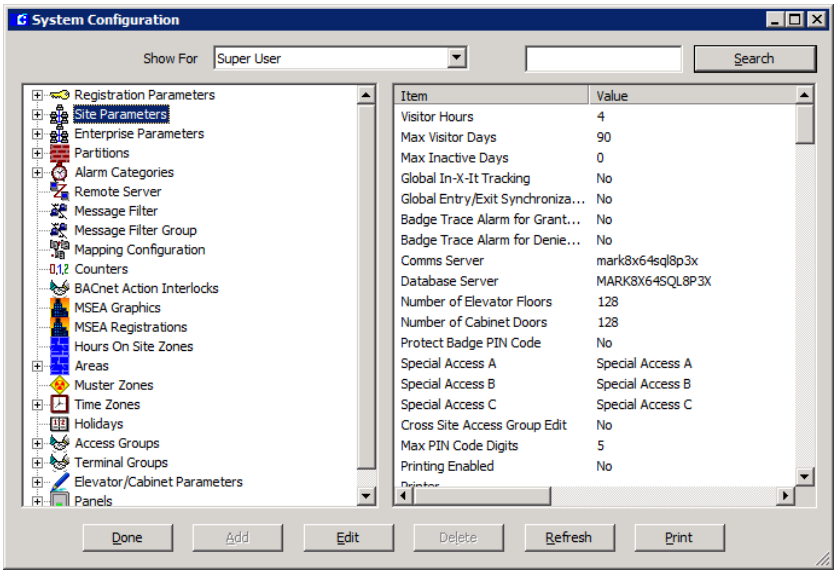
- The **Directory Services Path** field must be set in the Password Policy tab of Site Parameters. The actual value to use for the Directory Services Path is unique to your specific network configuration and needs to be obtained from the network administrator.
- Select the **Directory Services Password Validation** check box in the Edit Operator dialog box for each P2000 Web Access operator whose password will be verified by directory services.

Refer to the *P2000 Software User Manual* for information on defining the **Directory Services** path and editing the **Directory Services Password Validation** field.

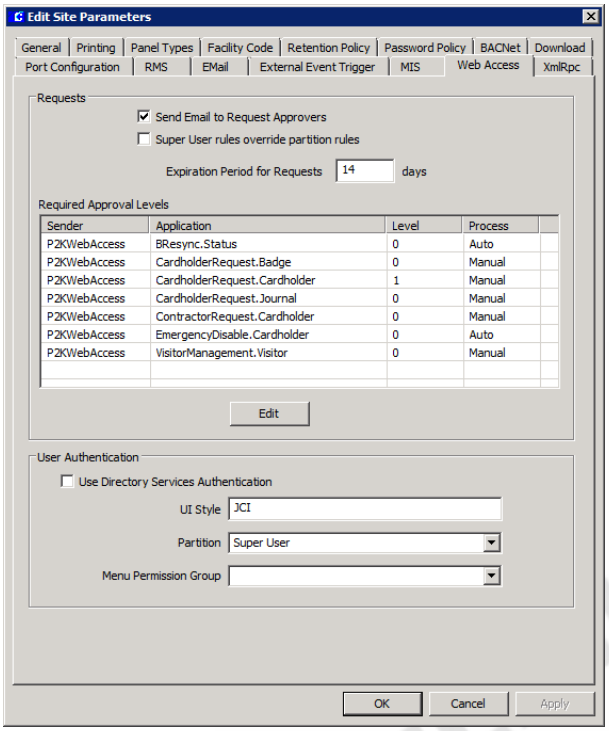
Once the previous elements are configured, perform the following steps to set up directory services for Web Access:

1. Using the P2000 software, select **System>Config** on the menu bar.
2. If prompted, enter your P2000 login password and click **OK**.

   The System Configuration window appears.



3. In the left pane, select **Site Parameters**.
4. Click **Edit**. The Edit Site Parameters window appears.
5. Select the **Web Access** tab.



6. In the User Authentication box, select the **Use Directory Services Authentication** check box.
7. In the **UI Style** field, enter the Web Access user interface style users will be assigned when logging in using directory services authentication.

8. In the **Partition** drop-down list, select the Web Access partition users will be assigned when logging in using directory services authentication.
9. In the **Menu Permission Group** drop-down list, select the Web Access group users will be assigned when logging in using directory services authentication.

NOTE

The UI Style, Partition, and Menu Permission Group assigned affects all P2000 operators whose accounts are enabled for directory services authentication. These parameters cannot be assigned individually (you cannot assign styles, partitions, or groups to specific users).

10. Click **OK**.

INDEX