Johnson Controls

P2000AE

Security Management System

Web Access Option

Version 4.1 and higher, December, 2008
24-10241-127 Revision B

P2000AE

Security Management System

Web Access

Version 4.1 and higher, December, 2008

24-10241-127 Revision A

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

Acknowledgment

TABLE OF CONTENTS

Chapter 1: Introduction

Chapter 2: Using Web Access

Chapter 3: System Administration

INTRODUCTION

P2000AE Web Access is a suite of applications that enables users to perform various P2000AE tasks from any web-ready Personal Computer (PC) or compatible Personal Digital Assistant (PDA) device. Using Web Access has many advantages; chief among them is its flexibility. Operators were previously required to edit most P2000AE data directly on site using P2000AE servers and workstations. Users can now submit P2000AE requests via the web using a remote PC or PDA, potentially saving the customer costs on equipment and personnel. Essentially, the Web Access interface offers a simple, flexible alternative to working on a P2000AE workstation.

Web Access offers many features such as employee, visitor, and contractor management applications, entity activity tracking and synchronization, alarm monitoring, emergency access disable, 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/or validated prior to being implemented, helping to prevent unauthorized operations or changes to the P2000AE system. When a request is submitted, it is sent to the request queue for processing. Rules can be established 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 and instructions in this manual may differ slightly, depending on the installation media and the software version you are using.

NOTE

"P2000AE" is also referred to as "P2000" throughout this manual.

CHAPTER SUMMARIES

- ***Chapter 1: Introduction*** describes the purpose of this document, manual conventions, software requirements, recommended PC display settings, instructions on how to log on and off, and the sequence of steps for deploying, configuring and using Web Access.

- ***Chapter 2: Using Web Access*** provides operator instructions for using the Web Access interface, including descriptions of the application features.
- ***Chapter 3: System Administration*** covers the 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.

CAUTION

Cautions remind you that certain actions, if not performed exactly as stated, can cause damage to equipment, security problems, or cause the system to operate incorrectly due to errors in system setup or programming.

WEB ACCESS FEATURES

- **Customizable User Interface**
  The Web Access interface is built with XML (Extensible Markup Language) and can be customized using the Altova StyleVision software tool.
- **User Roles**
  P2000 administrators can assign Web Access users to a particular user role with specific web access permissions, which can keep unauthorized users from performing high-level actions, such as deleting entity records or rejecting requests.
- **Entity Management**
  Web Access can be used to manage P2000 employee data and company assets via the web. Add, edit or delete entity records, identifiers and journals. An entity's In/Out status can also be re-synchronized if out-of-sync, including the entity status in areas controlled by Anti-Passback, Anti-Loitering, and Occupancy objects (CK722 controllers only).
- **Visitor Requests**
  Web Access allows you to add a visitor to the P2000 system, so that an identifier can be 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.

- **Contractor Requests**
  Use the application to send a request to change the validation period of an entity's access profile. The user sending this request must be assigned to the same entity category and partition as the entity whose access profile validation period will be changed.

- **Request Approval and Validation**
  Requests can be configured to require approval and/or validation before they can be processed. An approver can approve or reject a request. A rejected request can be edited for re-submittal. Validation allows the system administrator to make any necessary changes to the record before it is fully processed.

- **Entity Activity**
  Quickly and easily track the activities of P2000 entities and their In/Out status. For example, when an identifier is presented to a reader to enter or exit a secured area, you can view the record of the entity, the area the entity currently occupies (based on the location of the reader where the identifier was last presented), and the date and time when the identifier was presented to the reader.

- **Guard Services**
  Web Access can be used to monitor, acknowledge and remove P2000 alarms, activate or deactivate output points (e.g. turn on/off lights), and lock or unlock doors.

- **Time and Attendance Tracking**
  The P2000 Time and Attendance system is designed to record and track an entity's work schedule and attendance record, which can be integrated with a 3rd-party application, such as a payroll system. Using Web Access, you can define a particular work schedule for an entity, broadcast a message that appears on the Time and Attendance terminal where the entity signs-on, and monitor the entity's Time and Attendance status.

- **System Audit**
  Auditing the P2000 software enables you 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 (e.g Add Entity Group, Edit Entity, Execute Application, etc.).

- **Record Change Tracking**
  The P2000 Record Change Tracking option is an enhanced record tracking and operator auditing system that enables authorized users to view detailed reports of record value changes to the P2000 database based on numerous search parameters.

- **Emergency Access Disable**
  This feature enables an operator to disable the account of a single entity, which disables all of the entity's identifiers and his/her ability to log into Web Access.

- **WebBook Favorites**
  WebBook Favorites provides an enhanced method of saving Web Access web page links in a central location for quicker access later on. Links may be shared by a select group of Web Access users or by all Web Access users. Special tags can also be defined for a particular favorite page, allowing you to group like pages according to their tags.

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 Entity” application enables you to send a request to add an entity (person or asset) to the P2000 database. For ease of use, these applications are organized into logical groups on the Web Access interface, which can be customized by a Web Access administrator.

Web Access supports multiple styles, each with its own potential set of applications, fields, colors, images, etc. 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 the following logical groups: Employee Services, Guard Services, Management Services, Visitor Management, and Work Scheduler. 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 (In Alphabetical Order)	Group (“jci” style)	See Page No.
Add Entity	Management Services	2-29
Add Identifier	Management Services	2-48
Add Journal	Management Services	2-45
Alarm Monitor	Guard Services	2-18
Area Monitor	Work Scheduler	2-81
Area Search	Employee Services	2-8
Asset Finder	Employee Services	2-13
Broadcast Message	Work Scheduler	2-80
Change Partition	User Preferences	2-83
Change Password	User Preferences	2-83
Change Preferences	User Preferences	2-83
Command Outputs	Guard Services	2-20
Contractor Request	Visitor Management	2-75
Current (Work Schedule)	Work Scheduler	2-77
Door Command	Guard Services	2-21
Edit/Delete Entity	Management Services	2-41
Edit Journal	Management Services	2-46
Emergency Access Disable	N/A	2-82
Entity Activity	Employee Services	2-10
Entity Resync	Employee Services	2-14
Entity Search	Employee Services	2-1

Table 1-1: Web Access Applications

Application (In Alphabetical Order)	Group ("jci" style)	See Page No.
Monthly (Work Schedule)	Work Scheduler	2-77
Record Change Tracking	Management Services	2-69
Request Approval	Management Services	2-25
Request Status	Management Services; Visitor Management[1]	2-23
Validate	Management Services	2-66
Visitor Request	Visitor Management	2-73
WebBook Favorites	WebBook Favorites	2-85
Weekly (Work Schedule)	Work Scheduler	2-77

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 your Web Access administrator.

GETTING STARTED

User PC/PDA Software Requirements

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

PC

- **Browser:** Microsoft® Internet Explorer version 6.0 or higher
- **Screen Resolution:** The Web Access PC 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:

- Entity Search
- Area Search
- Alarm Monitor
- Entity Resync
- Door Command
- Command Outputs
- Emergency Access Disable

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

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

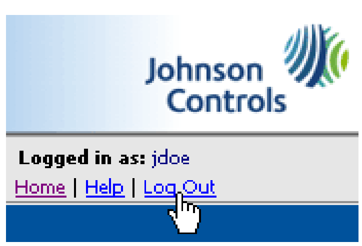
If you do not know the Web Access server name, or if you cannot successfully log on to the application, consult your Web Access Administrator for assistance.

The Login page appears.

2. Enter your **User Name** and **Password**, as defined in your P2000 user account.
3. Click **Log In**. 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 or simply close the browser window.



In addition, Web Access will automatically log off the current user if the system does not detect any activity for a defined number of minutes (the default is 20 minutes).

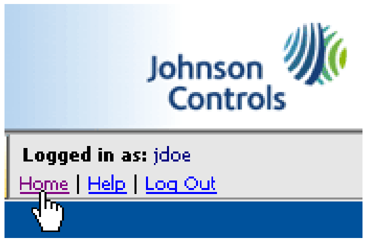
THE WELCOME PAGE

This page provides links to the following Web Access feature sets.

- **Employee Services**
  Select to track the activities of P2000 entities, perform an area or asset search, or request an entity resync, which will modify your in/out status if it is out-of-sync (legacy controllers). For CK722 controllers, you may modify your in/out status associated with an area controlled by Anti-Passback, Anti-Loitering, and/or Occupancy objects.
- **Guard Services**
  This service enables you to view, acknowledge, and discard P2000 alarms, activate or deactivate output points (e.g. 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 an entity record, validate requests, or audit user actions. To approve or validate requests, you must have proper permissions configured. Refer to the *P2000AE Software User Manual* for information on configuring Web Access permissions.
- **Visitor Management**
  This feature allows you to add a visitor to the system or request to extend the validation period of an entity's access profile. You may also view the status of requests.
- **Work Scheduler**
  This feature allows you can define a particular work schedule for an entity, broadcast a message that appears on the Time and Attendance terminal where the entity signs-on, and monitor the entity's Time and Attendance status.
- **User Preferences**
  The links in the User Preferences box allow you to change the password for your current user account (i.e. the account you used to log on to Web Access), your default login partition, and the default login Web Access style. These features are described in detail in "User Preferences" on page 2-83.
- **WebBook Favorites**
  This feature provides a way to bookmark Web Access pages you use most often and either use them for yourself, or create a "community" with which to share them. This feature is described in detail in "Using WebBook Favorites" on page 2-85.

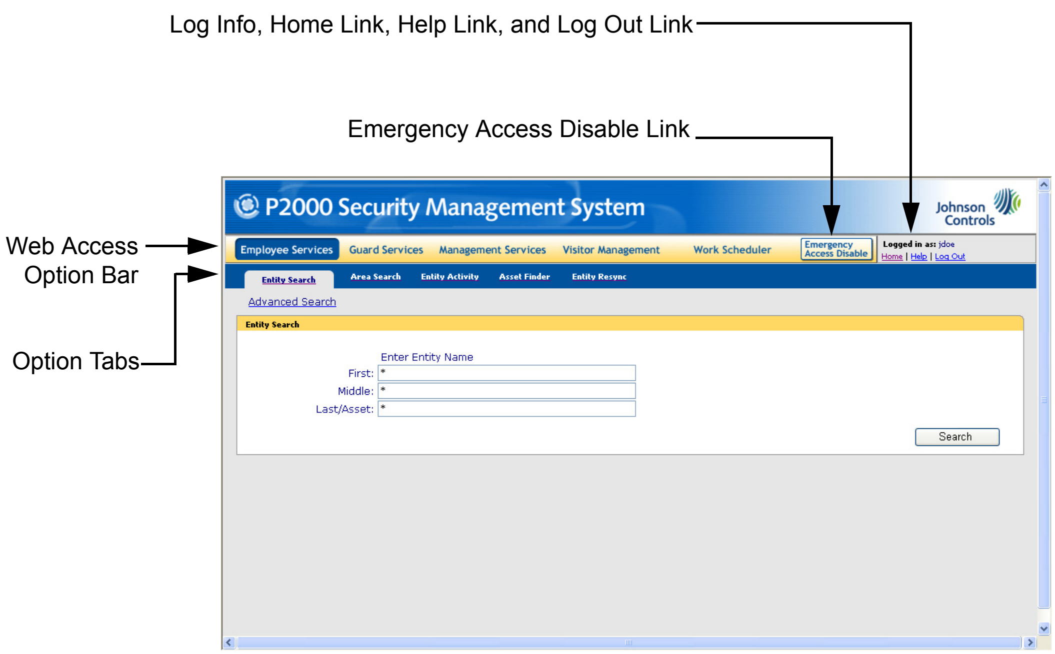
NOTE

*To return to the Welcome page from most pages, click the **Home** link in the upper-right corner of the page.*



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, the Home link, the Help link, and the Log Out link.



- **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 1-8.
- **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 an entity account, which will disable all of an entity's identifiers and his/her ability to log into Web Access. This option is available on most Web Access pages. See "Emergency Access Disable" on page 2-82 for detailed information.

- **Log Info**
  Displays the user name of the user currently logged on to Web Access.

- **Home Link**
  Returns you to the Welcome page (see page 1-8).

- **Help Link**
  Click to open the P2000 Web Access online help.

- **Log Out Link**
  Click to log out of Web Access.

SEQUENCE OF STEPS

The following sequence of steps are involved in the process of deploying, customizing, configuring and using Web Access. The administrative tasks should be performed by the P2000 System Administrator, Security Manager or other qualified professional in charge of administering Web Access.

- **Deploy Web Access**
  Deployment instructions are provided in "Web Access Deployment" on page 3-1.

- **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 3-16 for more information.

NOTE

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

- **Create and assign user roles to perform Web Access functions**
  By default, P2000 users are not permitted to log into Web Access until they are assigned at least one user role configured with the proper web permissions.

NOTE

Even the Super User role, by default, does not have web permissions enabled.

User roles prevent unauthorized users from performing high-level actions, such as deleting entity records or rejecting requests. Refer to the *P2000AE Software User Manual* for detailed information on creating and assigning user roles.

- **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 1-12 for information on the request process work flow. Refer to the *P2000AE 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 an entity whom has been assigned Web Request Approval permissions. The approvers are ordered in a sequence and they approve requests in the same order. Refer to the *P2000AE Software User Manual* for specific instructions on defining request approvers.

- **Submit requests using Web Access**
  Web Access users can submit a number of different requests (see “Chapter 2: Using Web Access” for detailed information). Depending on how Web Access is configured, a submitted request can be processed 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 Status feature. 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 (i.e. finalized). For information on defining request approvers, refer to the *P2000AE Software User Manual*. For specific instructions on approving, see “Approving or Rejecting Requests” on page 2-25.

- **Validate the request**
  All requests set for manual processing must be validated. Users can validate a request only if the P2000 host software is configured to allow it.

Request Process Flow Chart

Figure 1-1 outlines the request process once a request has been submitted. The following rules govern how the request is processed:

- When a request is submitted, if one or more approvers are defined and active, the request must be approved before it can be validated or processed. If no approvers are defined, 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 will change to “Rejected.” A rejected request can be edited and resubmitted by the user who originally submitted the request. An approved request can be validated (if the request type is set to manual) and processed.
- If validation is required, the request must be validated by an authorized user before it can be processed. Until the request is validated, it will have a status of “Validation.”
- During the validation process, a request can be rejected or approved for processing. The status of a rejected request will change to “Rejected.” A rejected request can be edited and resubmitted by the user who originally submitted the request. An approved request 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.

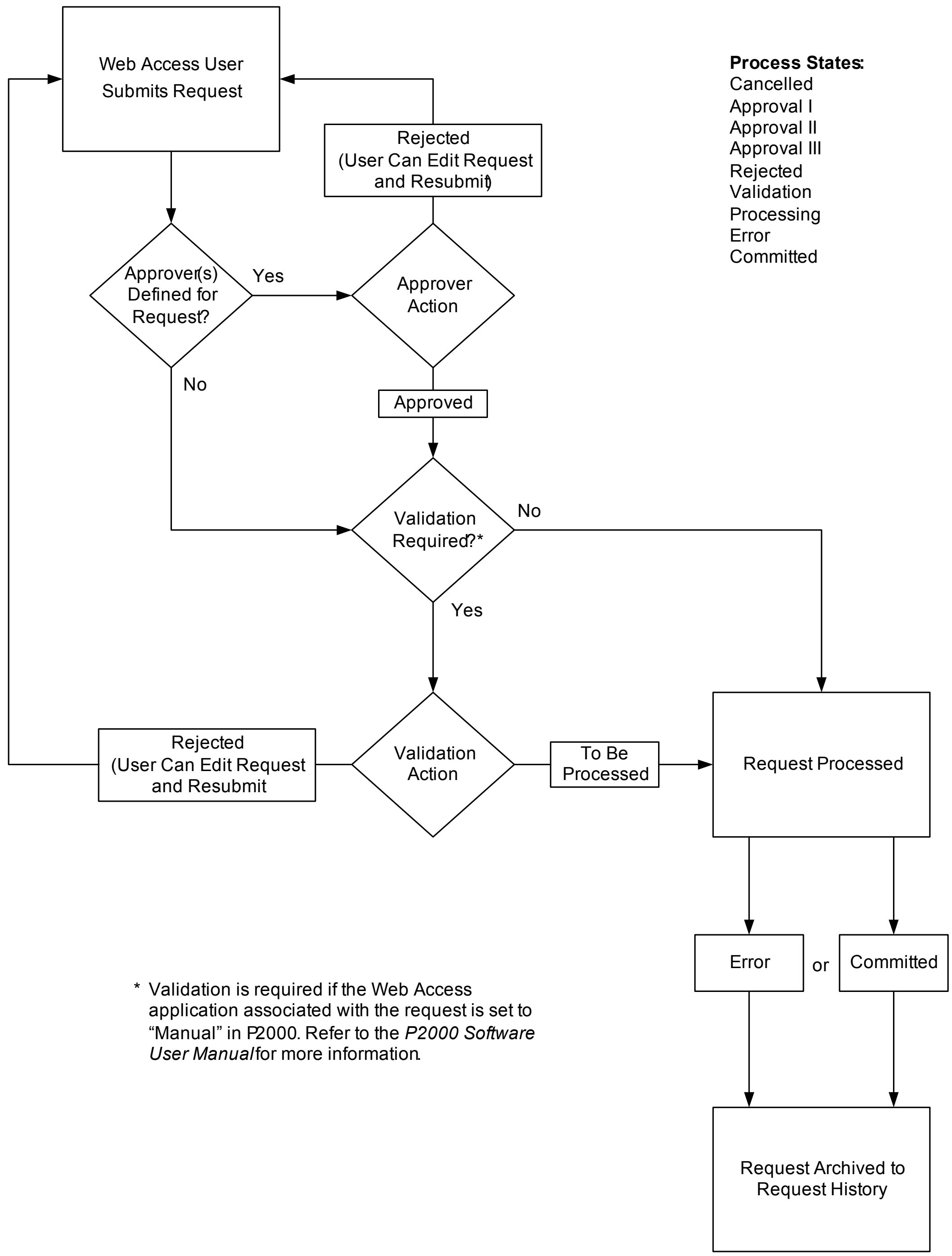


Figure 1-1: Request Process Flow Chart

 12/3/08

Process States

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

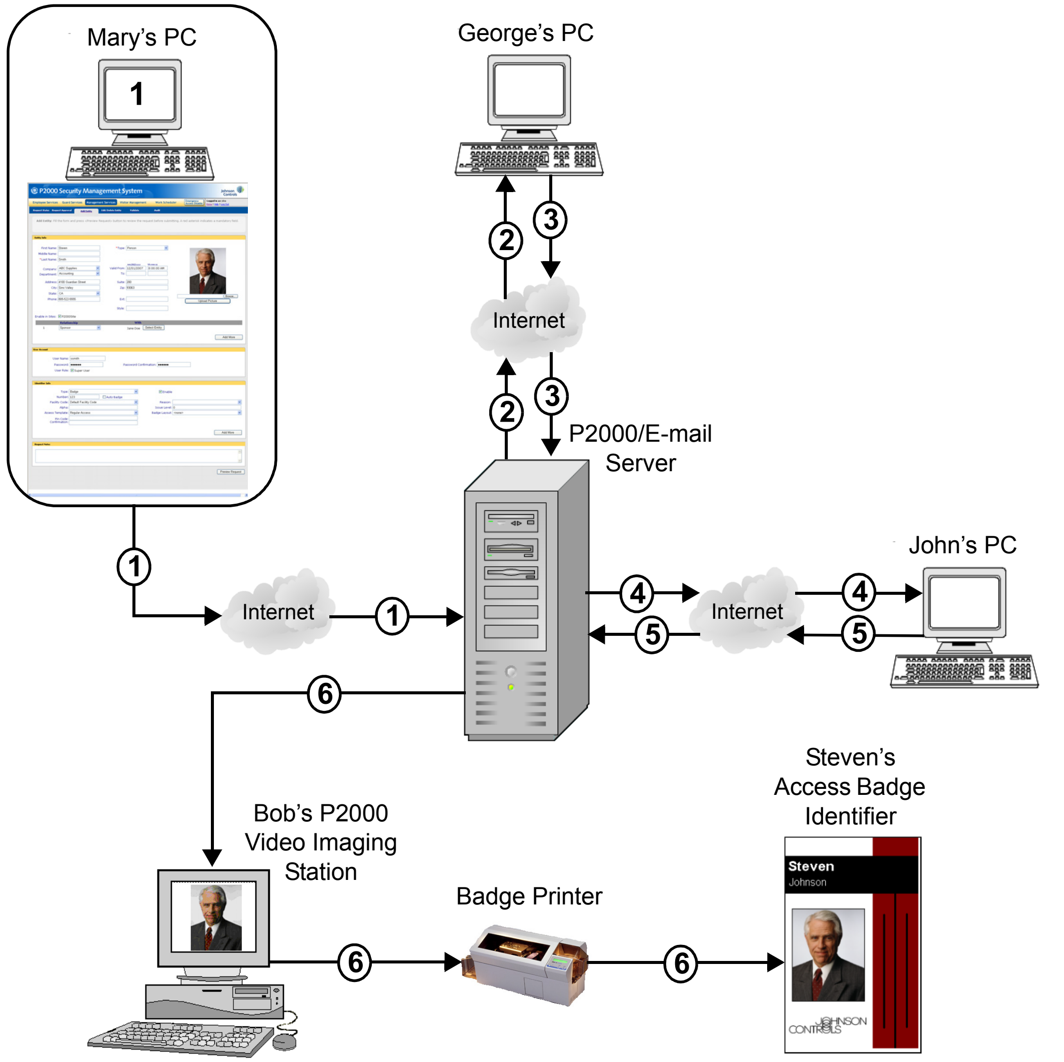
- **Cancelled** – The request was cancelled before being processed. A cancelled request is archived into the Request History and cannot be edited for re-submittal.
- **Approval 1** – The request is waiting to be approved by the required approver.
- **Approval 2** – The request was approved by Approver 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 by the user who originally submitted the request.
- **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 entity (person type) and visitor request. As you are reading a scenario, refer to the corresponding number on the illustration.

Adding an Entity

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 Entity application to submit a request to add an entity record for him.

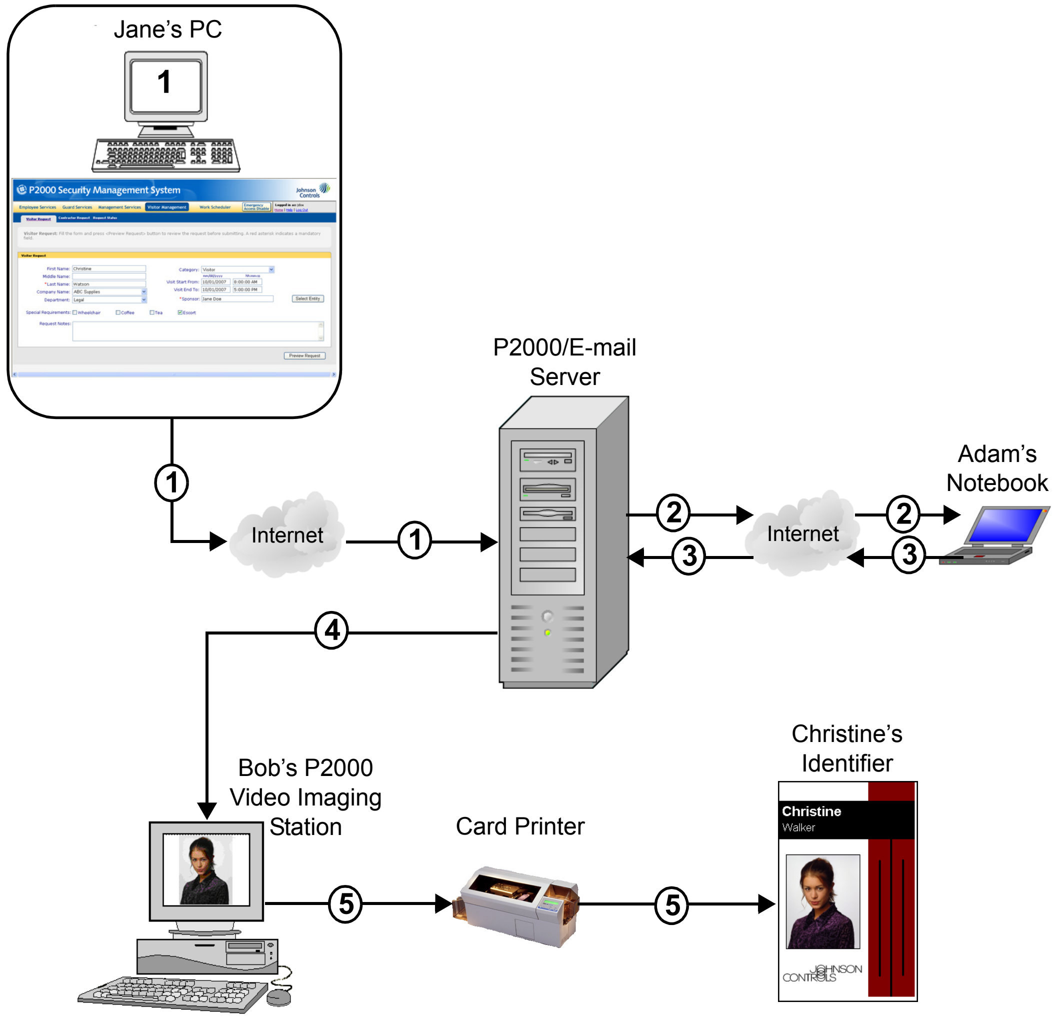


1. Mary enters Steven's data, uploads his picture, and adds a request note stating that he is a new Engineer working for George, an Engineering Manager. She submits the request to add Steven as an entity.
2. The P2000 system is set to require two approvals for entity requests, first from the person's 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 entity database. Bob then prints an access badge identifier with Steven's picture.

Figure 1-2: Scenario 1 (Adding an Entity)

Visitor Request

Jane has invited Christine, a business colleague, to her facility for a tour. She arrives next week. Jane needs to add Christine to the P2000 system as a visitor.



1. Jane uses Web Access to add Christine to the P2000 system as a visitor. 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 Christine has been added to the system as a visitor. Bob assigns an access badge identifier to Christine's entity record 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 access badge identifier.

Figure 1-3: Scenario 2 (Visitor Request)

USING BROWSER AND WEBBOOK FAVORITES

You can use any standard browser to bookmark favorite pages in Web Access; however, you may prefer to use the WebBook Favorites feature built-in to Web Access (see “Using WebBook Favorites” on page 2-85 for a list of advantages). The WebBook Favorites feature is specifically designed to help you make use of Web Access quickly and efficiently.

The following examples describe the benefits of using Browser Favorites or the Web Access WebBook feature. For complete steps to configure and use WebBook Favorites, see “Using WebBook Favorites” on page 2-85.

- **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 entity type (e.g. person), a specific company (e.g. Johnson Controls), and a specific category (e.g. Full-time Employee), saving you from entering search criteria each time you want to perform this search.
- **Quickly see who’s “In” or “Out” of the facility**
  Bookmark the Web Access page that displays the “In-Out” status of a particular entity to quickly view the status again later, without having to locate the entity again and re-add him/her to the “In-Out” display. See “Entity Activity” on page 2-10 for more information.

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

Chapter 2

USING WEB ACCESS

This chapter provides details about the Web Access features and instructions for using the web-friendly interface. Depending on your web 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 perform a visitor request or extend the validation period of an entity's access badge identifier. This chapter will cover all of the features available on the web interface.

NOTE

For information on configuring Web Access web permissions, refer to the P2000AE Software User Manual.

EMPLOYEE SERVICES

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

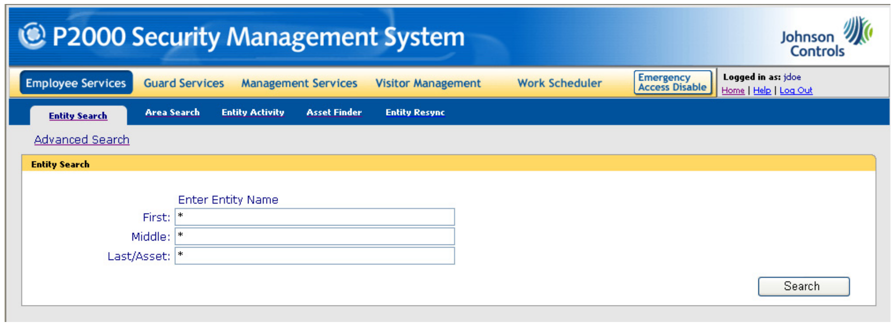
- Locating entity records in the P2000 database
- Viewing detailed entity and identifier data (see page 2-7)
- Determining the location of entities within P2000 defined areas (see page 2-8)
- Tracking entity activity, such as In-Out status, in specific P2000 defined areas (see page 2-10)
- Changing your In/Out status if out-of-sync, including the entity status in areas controlled by Anti-Passback, Anti-Loitering, and Occupancy objects (CK722 controllers only) (see page 2-14)

Entity Search

An entity is a person or asset that P2000 tracks in the database. Web Access allows you to search and locate one or more entity records in the P2000 database. You may search by such criteria as entity or asset name, badge number, department, company, category, type, and partition. Use this feature to view information of a particular entity record.

➤ To search for entity records:

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



2. If the entity is a person, enter the first, middle and/or last name; if the entity is an asset, enter the asset name in the **Last/Asset** field. You can click the **Advanced Search** link to search by the following criteria:
   - Badge Number
   - Department
   - Company
   - Partition
   - Category
   - Type
   - Drivers License and/or License Plate, if defined as user-defined fields (UDF) in P2000

NOTE

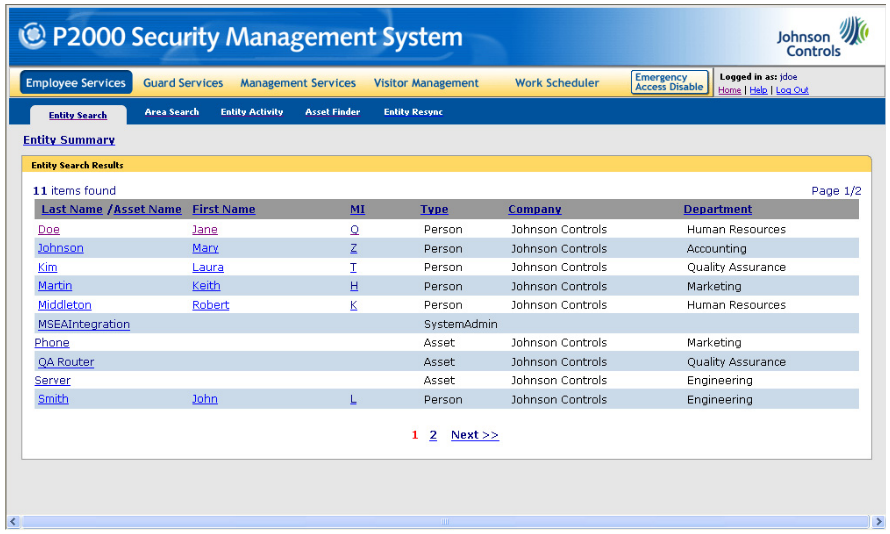
The Drivers License and License Plate fields will only appear on the Entity Search (Advanced) page if they have been added as UDFs in P2000. For information on adding UDFs, refer to the P2000AE Software User Manual.

NOTE

See “Search Tools” on page 2-3 for information on using wildcards and commas to help you locate entity records.

---

3. Click **Search**. The Entity List page appears, listing the entities that were located based on your search criteria.



Search Tools

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

The Asterisk Wildcard (*)

This wildcard represents a string of characters in 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 in 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 entities of two companies (e.g. 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 ones that start with "J".*

Temporarily Changing the Number of Entities Listed Per Page

If the number of entities 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 entities you wish to display per page.

Example:

*http://129.212.109.38/p2ktc/we/app/bactivity/EntityList.aspx?search=4QjvuKLVJaXPdTPr%2fTgIQcZJTIn6HKn9BbuH6na%2bKdSjGk7oFN0kL8ms2xjp1GjBlGU8sCGbEF652J2bNvDR8Q%3d%3d**&ipp=20***

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

NOTE

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

NOTE

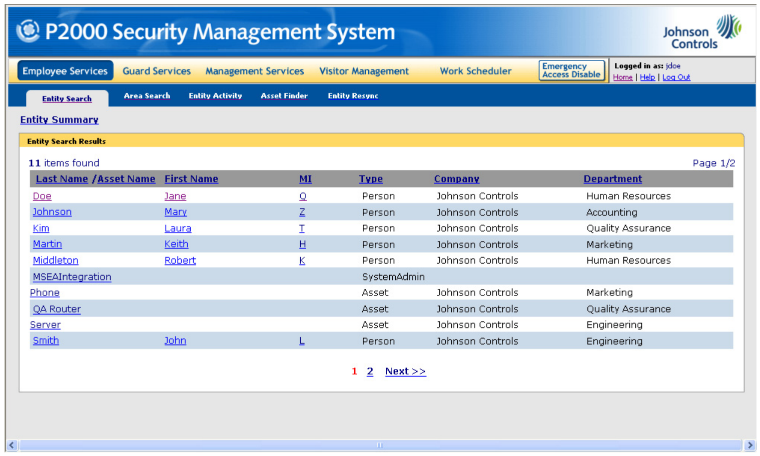
This feature can also be used on the Entity List page when searching for entities on the Edit/Delete Entity tab.

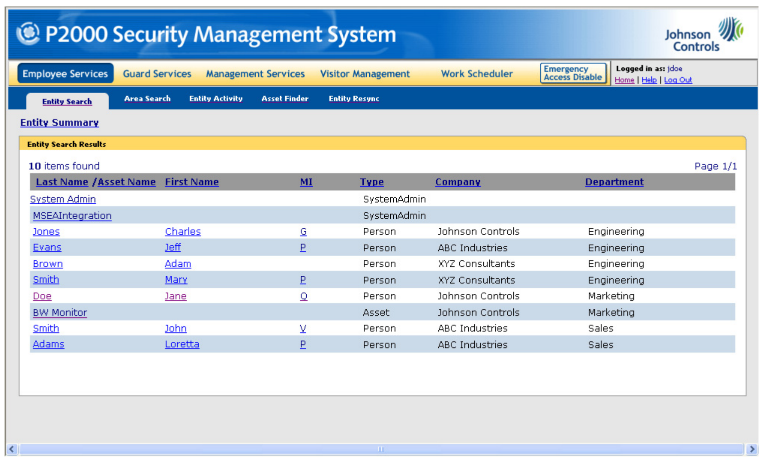
Sorting Columns

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 entity records based on the department. If entities belonging to four different departments are displayed (e.g. Marketing, Engineering, Technical Support and Human Resources), sorting the Department column will list the entities in order of the department to which they belong (alphabetically, A to Z), so every entity 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 entities listed alphabetically according to the entity Last/Asset Name. The second screen capture shows the list sorted alphabetically (A to Z) after clicking the Department column.

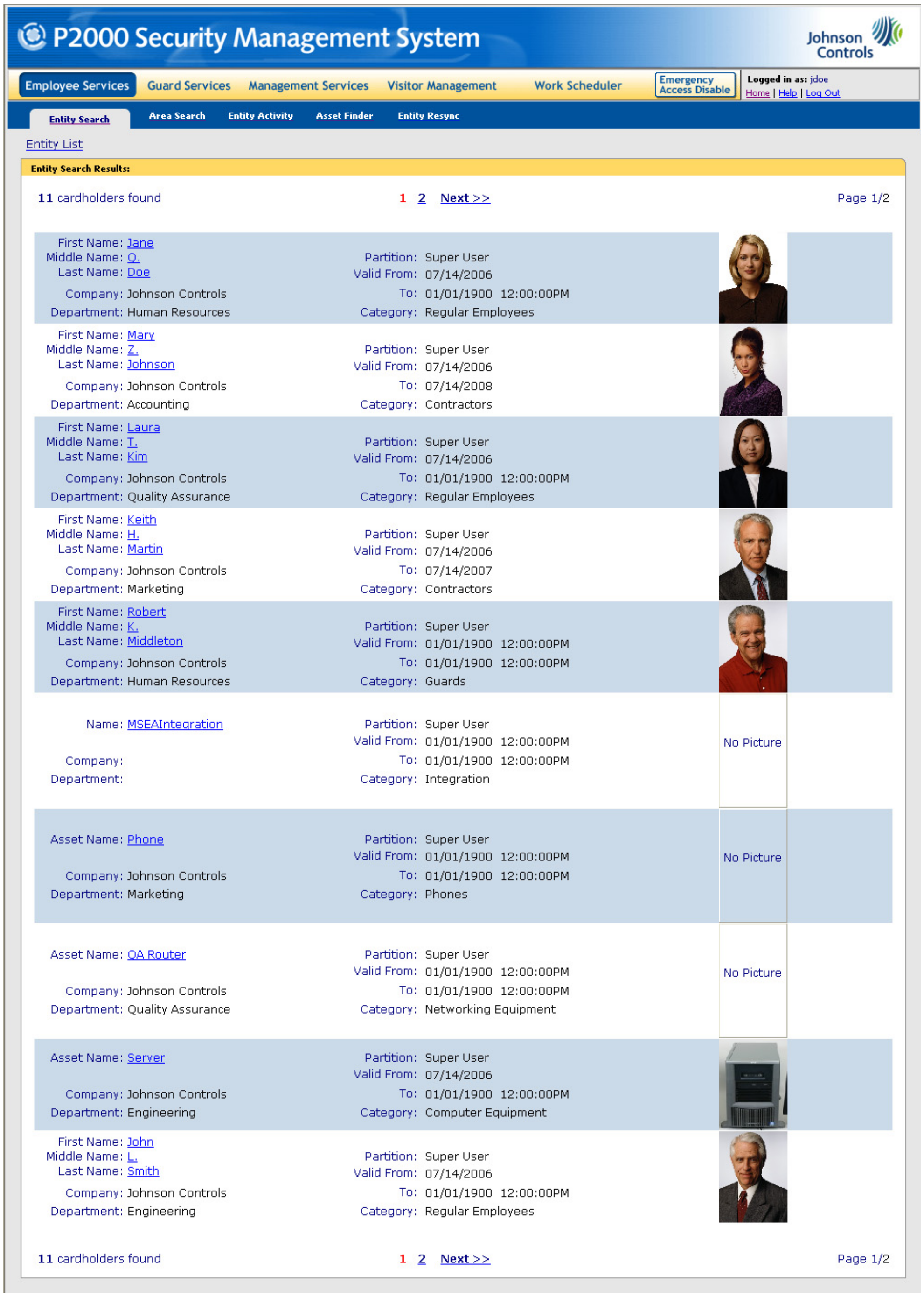




Viewing Entity Summary Information

Use the **Entity Summary** link on the Entity List page to view a summary of the entities located in your search. This summary includes additional information about each entity located in the search, including a portrait photo (if applicable).

- To view additional information about a particular entity, click the name of the entity.
- To return to the Entity List page, click the **Entity List** link.


P2000 Security Management System
Johnson Controls
Employee Services
Guard Services
Management Services
Visitor Management
Work Scheduler
Emergency Access Disable
Logged in as: jdoe
Home | Help | Log Out
Entity Search
Area Search
Entity Activity
Asset Finder
Entity Resync
Entity List
Entity Search Results:
11 cardholders found
1 2 Next >>
Page 1/2
First Name: Jane
Middle Name: Q.
Last Name: Doe
Company: Johnson Controls
Department: Human Resources
Partition: Super User
Valid From: 07/14/2006
To: 01/01/1900 12:00:00PM
Category: Regular Employees
First Name: Mary
Middle Name: Z.
Last Name: Johnson
Company: Johnson Controls
Department: Accounting
Partition: Super User
Valid From: 07/14/2006
To: 07/14/2008
Category: Contractors
First Name: Laura
Middle Name: T.
Last Name: Kim
Company: Johnson Controls
Department: Quality Assurance
Partition: Super User
Valid From: 07/14/2006
To: 01/01/1900 12:00:00PM
Category: Regular Employees
First Name: Keith
Middle Name: H.
Last Name: Martin
Company: Johnson Controls
Department: Marketing
Partition: Super User
Valid From: 07/14/2006
To: 07/14/2007
Category: Contractors
First Name: Robert
Middle Name: K.
Last Name: Middleton
Company: Johnson Controls
Department: Human Resources
Partition: Super User
Valid From: 01/01/1900 12:00:00PM
To: 01/01/1900 12:00:00PM
Category: Guards
Name: MSEAIntegration
Company:
Department:
Partition: Super User
Valid From: 01/01/1900 12:00:00PM
To: 01/01/1900 12:00:00PM
Category: Integration
No Picture
Asset Name: Phone
Company: Johnson Controls
Department: Marketing
Partition: Super User
Valid From: 01/01/1900 12:00:00PM
To: 01/01/1900 12:00:00PM
Category: Phones
No Picture
Asset Name: QA Router
Company: Johnson Controls
Department: Quality Assurance
Partition: Super User
Valid From: 01/01/1900 12:00:00PM
To: 01/01/1900 12:00:00PM
Category: Networking Equipment
No Picture
Asset Name: Server
Company: Johnson Controls
Department: Engineering
Partition: Super User
Valid From: 07/14/2006
To: 01/01/1900 12:00:00PM
Category: Computer Equipment
First Name: John
Middle Name: L.
Last Name: Smith
Company: Johnson Controls
Department: Engineering
Partition: Super User
Valid From: 07/14/2006
To: 01/01/1900 12:00:00PM
Category: Regular Employees
11 cardholders found
1 2 Next >>
Page 1/2

Viewing Entity Information

To view detailed information about a particular entity, click the name of the entity. The Entity Info page appears.

NOTE

Information and categories that appear on the Entity Info page depend on the information that has been configured for the entity. For example, if there are no journal entries for an entity, the Journal Title and Content bar will not appear.

The following categories list information associated with the selected entity:

- **Entity General Information**
  Lists general entity information, such as entity name, company, address, department, category, validation start/end dates, phone number, and any user-defined fields.

- **Other Info**
  Lists other entity information, such as the entity's sponsor, access profile, group membership, user account, identifiers, and journal entries. Click a link to view more information about the entity's sponsor, identifier, or journal entry.

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

Area Search

This feature enables you to view which P2000 entities currently occupy a specific area controlled by the P2000 Security Management System. This is based on where a person's identifier was last presented.

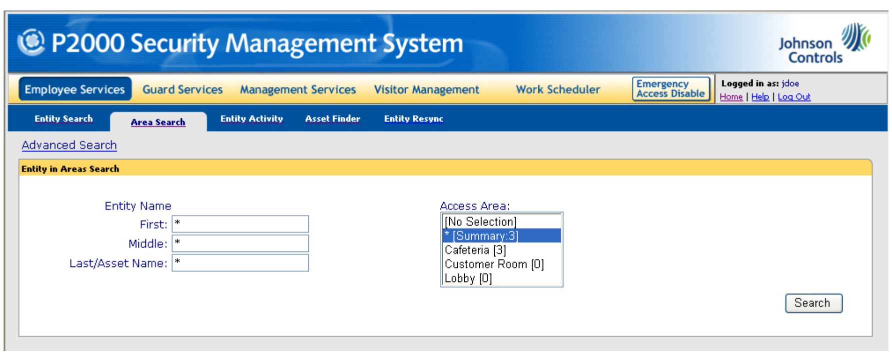
NOTE

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 entities leave, unless they use their identifier at another reader.

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

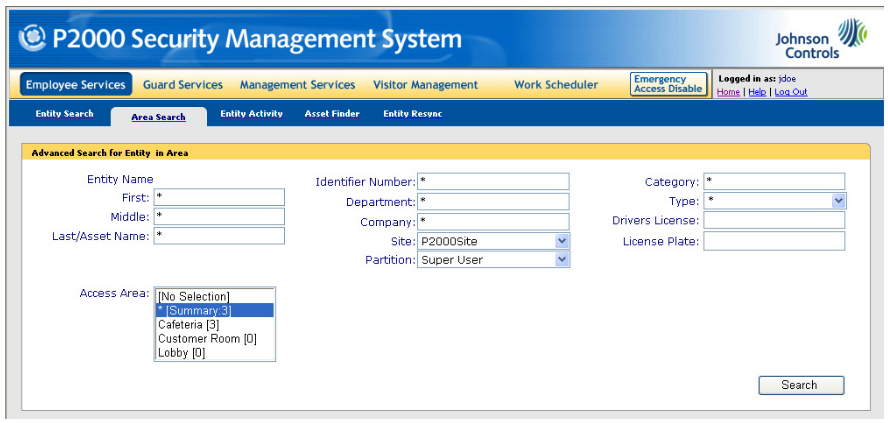
➤ To search an area:

1. Select the **Area Search** tab. The Entity in Areas Search page appears.

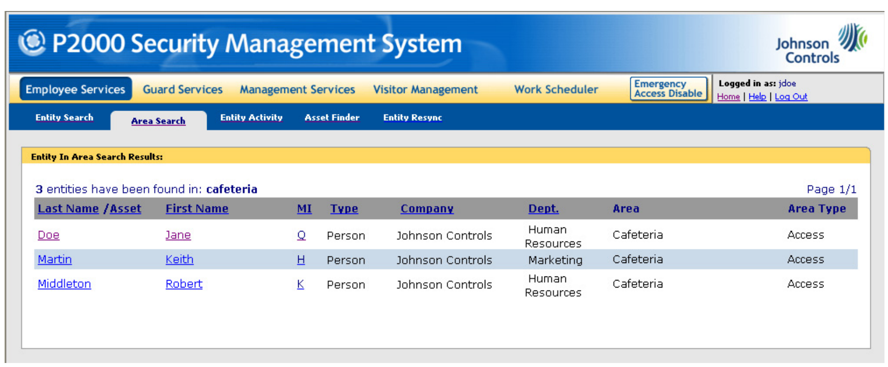


2. Perform one of the following actions:
   - Select an area and click **Search** to view all of the entities who currently occupy an area.
   - To search for a specific entity in an area, enter the person's first, middle and/or last name, (or asset name), select an area or the asterisk (*) for all areas, and click **Search**.

- Click the **Advanced Search** link to search by additional area criteria, such as:
  - Identifier Number
  - Department
  - Company
  - Site
  - Partition
  - Category
  - Type
  - Drivers License and/or License Plate (if these UDFs are defined in P2000)



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



You may view information on a particular entity listed in your search by clicking the entity name link (see “Viewing Entity Information” on page 2-7 for details).

Entity Activity

This feature enables you to see which P2000 entities (persons or assets) are “in” or “out” of the facility, or in specific areas of the facility today, based on their identifier activity. You may also view information on the last transaction recorded for an entity, allowing you to determine where the transaction occurred, the transaction date and time, and any companion and relation data.

Viewing In/Out Status Information

If an entity has presented his/her identifier to enter the facility today (assuming the reset time is set to 12:00 AM), his/her status will be “In”. If an entity has not presented his/her identifier to enter 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 entities.

The In/Out status is determined by the time an entity uses an identifier to enter the facility or area and the reset time. If the reset time is set to 12:00 AM (the default setting), all entities who use their identifier to enter the facility will be listed as “In.” At 12:00 AM, their status will be reset to “Out.” See Figure 2-1.

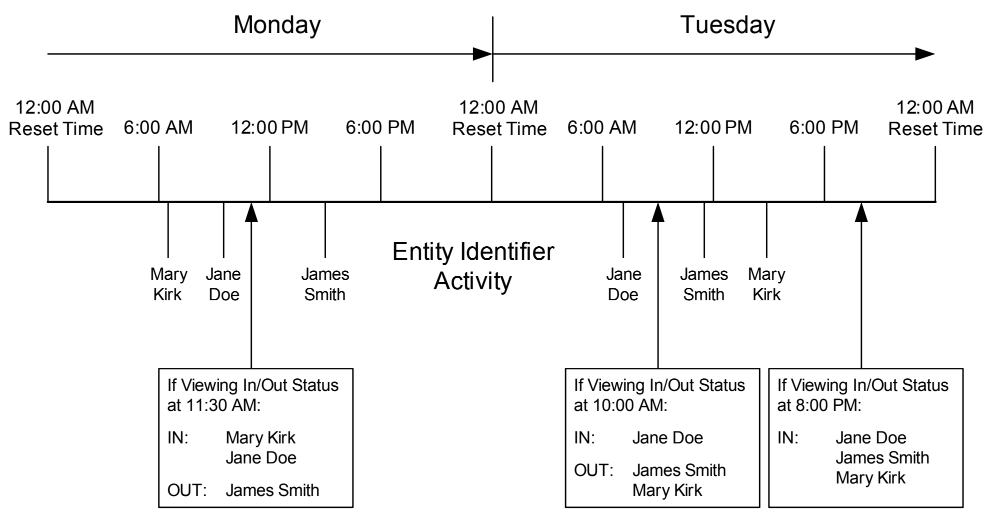
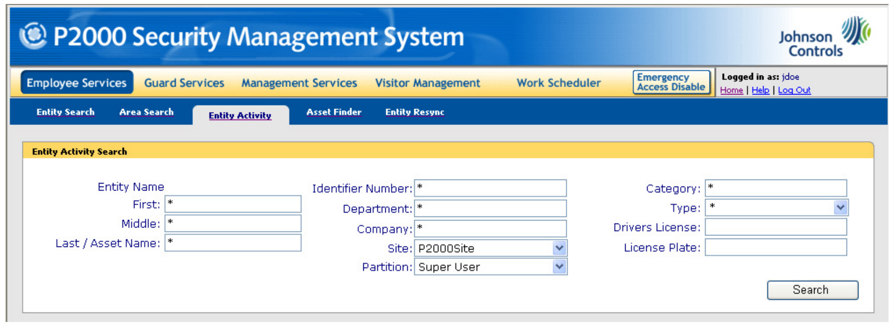


Figure 2-1: In/Out Status Reset - How it Works

➤ To view the in/out status of entities:

1. Select the **Employee Services** option.

2. Select the **Entity Activity** tab. The Entity Activity Search page appears.



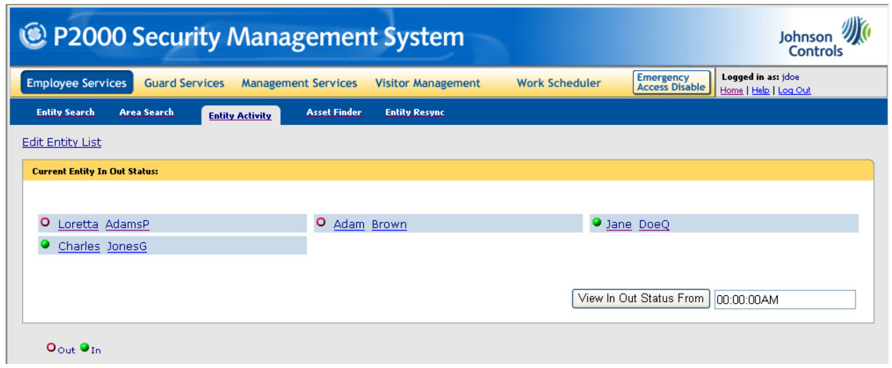
3. To locate specific entities, enter data into the search criteria fields (e.g. Entity, Identifier Number, etc.).
4. Click **Search**. The Entity List page appears, displaying the entities that match your search criteria.
5. Select the check box next to each entity whose In/Out status you wish to view or click the **Select All** button to select all of the entities located in the search.

6. Click **Create Group**.

NOTE

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****.*

7. Click the **View In Out Display** link at the top of the list. The Current Entity In-Out Status page appears.



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

NOTE

The View In Out Status From time resets the entity In/Out status. For example, if the View In Out From time is 12:00:00 AM and Entity A uses an identifier at 08:00:00 AM that same day, he/she will be "In". The next day (starting at 12:00:00 AM), Entity A will be "Out" until he/she uses an identifier 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 entity data, click the entity's name to open the Entity General Info page. See "Viewing Entity Information" on page 2-7 for more information.

Viewing Transaction Data

➤ To view entity last transaction information:

1. Select the **Employee Services** option.
2. Select the **Entity Activity** tab. The Entity Activity Search page appears.
3. To locate specific entities, enter data into the search criteria fields (e.g. Entity, Identifier Number, etc.).

4. Click **Search**. The Entity List page appears, displaying the entities that match your search criteria.
5. Select the check box next to each entity whose last transaction information you wish to view, or click the **Select All** button to select all of the entities located in the search.
6. Click **Create Group**.
7. Click the **View Last Transaction** link at the top of the list.

NOTE

*To view the last transaction information of a single entity, click the **View** link under the **Last Transaction** column.*

The last transaction information for the selected entities appears on the Entity Last Transaction List page.

8. To modify the entity search, click the **Modify Entity List** link and repeat steps 5 through 7.
9. Click one of the following links to view additional information associated with the transaction:
   - **Entity Name** – Click to access the Entity Information page for the selected entity. See "Viewing Entity Information" on page 2-7.
   - **Location** – Click to view additional badging activities at the selected location.
   - **Companion** – Click to access the Entity Information page for the selected companion. See "Viewing Entity Information" on page 2-7.
   - **View** – Click to view the entity's badging history.

Asset Finder

Using the Asset Finder feature, you can quickly locate assets within the facility using minimal search criteria, or find all assets in the facility. Once you locate an asset record, you may view transaction information associated with the asset.

➤ To view asset transaction information:

1. Select the **Employee Services** option.
2. Select the **Asset Finder** tab. The Asset Search page appears.
3. To locate specific assets, enter data into the search criteria fields (e.g. Asset Name, Category, etc.).
4. Click **Search**. The Entity List page appears, displaying the entities that match your search criteria.
5. Select the check box next to each asset whose last transaction information you wish to view, or click the **Select All** button to select all of the assets located in the search.

6. Click **Create Group**.
7. Click the **View Last Transaction** link at the top of the list.

NOTE

*To view the last transaction information of a single asset, click the **View** link under the **Last Transaction** column.*

The last transaction information for the selected assets appears.

8. Click one of the following links to view additional information associated with the transaction:
   - **Asset Name** – Click to access the Entity Information page for the selected asset. See “Viewing Entity Information” on page 2-7.
   - **Location** – Click to view additional badging activities at the selected location.
   - **Companion** – Click to access the Entity Information page for the selected companion. See “Viewing Entity Information” on page 2-7.
   - **View** – Click to view the asset’s badging history.

Entity Resync

This feature allows you to resynchronize your In/Out status if out-of-sync, including your status in areas controlled by Anti-Passback, Anti-Loitering, and Occupancy objects (CK722 controllers only).

NOTE

You can only resynchronize your own In/Out status (not the In/Out status of another entity).

Entity Status Resync in Legacy Panels

Entry and Exit terminals require entities to enter and exit an area in sequence. That is, when entities badge in at an entry terminal, they must badge out at the next badging. If, for example, they follow another entity out without swiping their badge identifier, their badge will remain in the “In” state (out-of-sync). When they attempt to badge back into the area, they will be denied access.

The Entity Resync feature allows you to manually re-synchronize your In/Out status by adjusting the status of your identifiers and returning them to the correct state if they are out-of-sync. You can also reconfigure them as Undefined to clear the Entry/Exit status until the next badging.

➤ To re-synchronize your in/out status:

1. Select the **Employee Services** option.

2. Select the **Entity Resync** tab. The Entity Resync page appears.

3. In the Legacy box, select the appropriate radio button, **In** or **Out**, to change your In/Out status, or select **Undefined** so that the next identifier presented will redefine the identifiers for the appropriate action.

   For example, if you are outside of the secured area and your status is set to **Undefined**, the next time you use your identifier to enter the secured area, your status will automatically change to **In**.

4. Click **Submit**.

Entity Status Resync in CK722 Controllers

With Entity Resync you can issue commands to change your in/out status in an area controlled by Anti-Passback, Anti-Loitering, and Occupancy objects (CK722 controllers only).

The **Anti-Passback object** enforces the use of entry and exit readers in accordance with the anti-passback rule by time, and the anti-passback rule by location (also known as the entry-exit rule). The Entity Resync function allows you to change your status if you were denied access because you violated one of the anti-passback rules.

The **Anti-Loitering object** monitors the time individual entities spend in an anti-loitering area. If an entity exceeds the area's anti-loitering time, an anti-loitering notification is generated. The Entity Resync function allows you to change your status if you violated the defined anti-loitering rules.

The **Occupancy object** monitors the number of entities in an occupancy space. The Entity Resync function allows you to change your status if you violated the defined occupancy rules.

NOTE

Some entity resync options, such as Reset All, allow you to change the status of all entities in the area controlled by a selected object.

For more information on these objects, refer to the following manuals:

- *CK722 Network Controller Commissioning Guide*
- *Anti-Passback Object Manual*
- *Anti-Loitering Object Manual*
- *Occupancy Object Manual*

➤ To modify the entity status in the area controlled by an Anti-Passback object, Anti-Loitering object, and/or Occupancy object:

1. Select the **Employee Services** option.
2. Select the **Entity Resync** tab. The Entity Resync page appears.

3. To modify the entity status in an area controlled by an **Anti-Passback** object, select one of the following radio buttons:
   - **In** – Changes your status to “In” in the area controlled by the selected Anti-Passback object in an entry/exit application, so you can make exit requests again in the area.
   - **Out** – Changes your status to “Out” in the area controlled by the selected Anti-Passback object in an entry/exit application, so you can make entry requests again in the area.

- **Undefined** – Changes your status to “Undefined” in the area controlled by the selected Anti-Passback object in an entry/exit application, so you can make entry or exit requests again in the area.
- **Entry Time** – Resets your entry time in the area controlled by the selected Anti-Passback object in a timed application, so you can make entry requests again in the area. For example, the Anti-Passback Entry Time attribute is set to 2 hours and you present your badge identifier at 8:00 AM to enter the facility. When you attempt to enter the facility again at 9:00 AM, the system denies you access. However, if you reset the entry time, you can make an entry request and enter the facility, after which your entry time will start over.
- **Exit Time** – Resets your exit time in the area controlled by the selected Anti-Passback object in a timed application, so you can make exit requests again in the area. For example, the Anti-Passback Exit Time attribute is set to 30 minutes and you present your badge identifier at 5:00 PM to exit the facility. When you attempt to exit the facility again at 5:15 PM, the system denies your exit request. However, if you reset the exit time, you can make an exit request and exit the facility, after which your exit time will start over.
- **Reset All** – Changes the status of ALL entities in the area controlled by the selected Anti-Passback object in an entry/exit application to that which is defined in the selected Anti-Passback object’s Default Status attribute (In, Out, or Undefined). For example, if the Anti-Passback object’s Default Status attribute is set to *In* and you select Reset All in Web Access, the entry/exit status of all entities will change to *In*.

CAUTION

Use the Reset All function cautiously, since it changes the entry/exit status of ALL entities in the area controlled by the selected Anti-Passback object. Misuse of this function may result in entities being mistakenly locked out of or locked in the facility.

- **Reset Entry Time (All)** – Resets the entry time of ALL entities in the area controlled by the selected Anti-Passback object in a timed application, so they can make entry requests again in the area.
- **Reset Exit Time (All)** – Resets the exit time of ALL entities controlled by the selected Anti-Passback object in a timed application, so they can make exit requests again in the area.

4. To modify the entity status in an area controlled by an **Anti-Loitering** object, select one of the following radio buttons:
   - **In** – Change your status to “In” in the area controlled by the selected Anti-Loitering object.
   - **Out** – Change your status to “Out” in the area controlled by the selected Anti-Loitering object.

5. To modify the entity status in an area controlled by an **Occupancy** object, select one of the following radio buttons:
   - **In** – Change your status to “In” in the area controlled by the selected Occupancy object.
   - **Out** – Change your status to “Out” in the area controlled by the selected Occupancy object.
6. Click **Submit**.

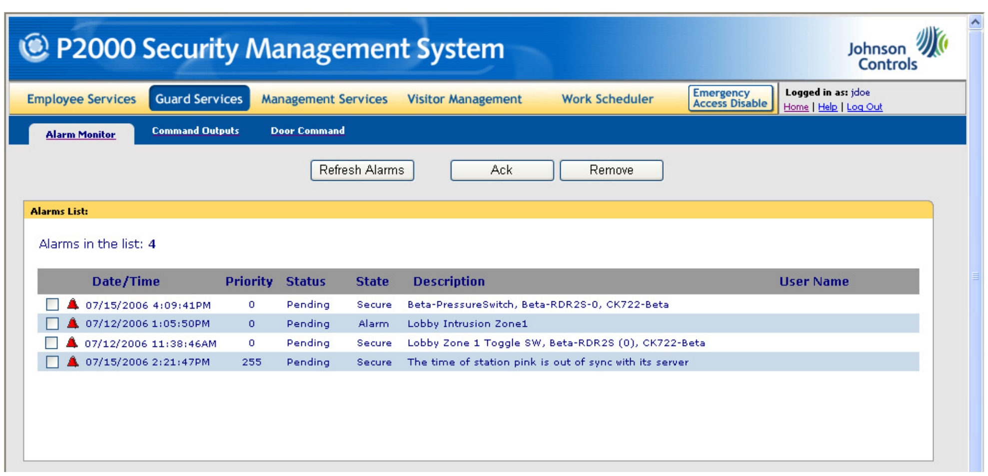
GUARD SERVICES

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 (e.g. turning on lights, activating a siren, etc.) (page 2-20)
- Locking or unlocking doors, or timing the doors to lock/unlock after a user-defined number of minutes (page 2-21)

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.



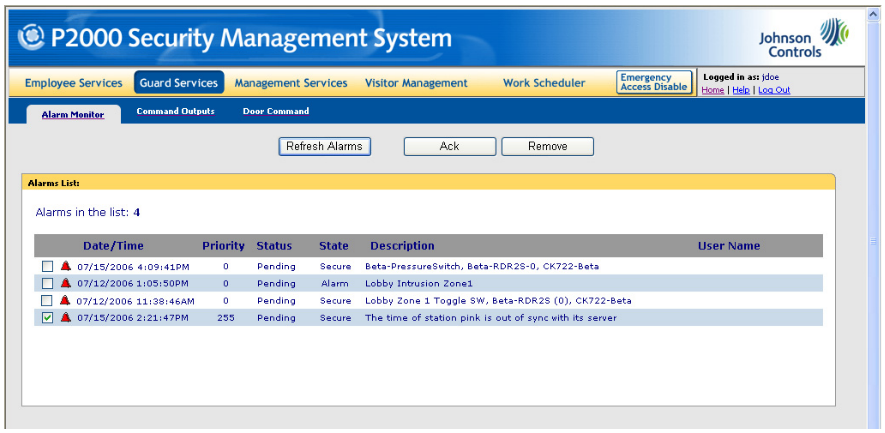
All pending alarm messages remain in the Alarm Queue until acknowledged and removed by a P2000 operator or Web Access user. You may only remove alarms in a “Secure” or “N/A” state.

Acknowledging an Alarm

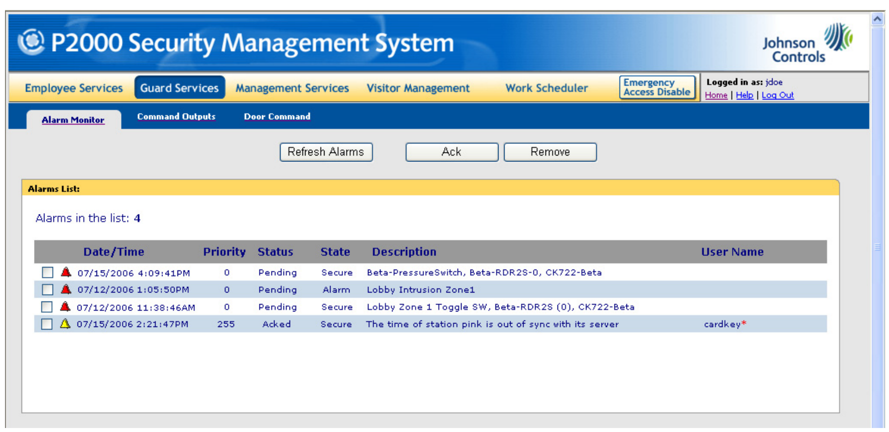
A P2000 operator or Web Access user may be required to acknowledge a new alarm as soon as it is received. They may do so and then return later to actually remove the alarm, depending on company policy and the priorities assigned to that alarm. The time and date of the acknowledgment is recorded in the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

➤ To acknowledge an alarm:

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



2. Click **Ack** at the top of the page. 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 the one of the following alarm states: Secure, Alarm, Open, or Short.

Description – A description of the element that activated the alarm.

User Name – The 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.

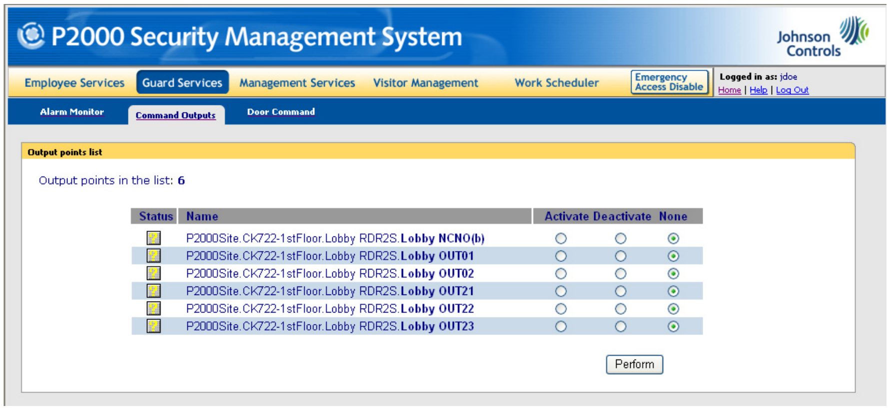
Activating or Deactivating Output Points

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: *P2000Site.CK722-1stFloor.Lobby RDR2S.Lobby OUT01*

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 person has misplaced his access badge identifier 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.

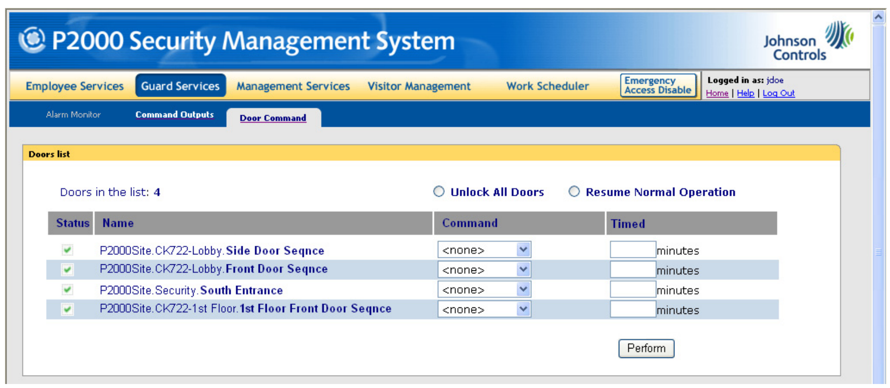
The door commands available in Web Access are:

- **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.

- **Lock Command**
  Locks the selected door until it returns to its normal state or is manually unlocked.
- **Unlock Command**
  Unlocks the selected door until it returns to its normal state or is manually locked.
- **Timed Unlock Command**
  Locks the selected door for a specified number of minutes. Once the time expires, the door will relock.

➤ To perform a door command:

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



3. 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, controller, and terminal (for legacy controllers) or Door Sequence object (for CK722 controllers).

Example: *P2000Site.1stFloor.Main Entrance Seqnce*

---

4. 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 (page 2-23)
- Approving or rejecting requests (page 2-25)
- Editing a rejected request (page 2-28)
- Adding an entity (page 2-29)
- Editing or deleting an entity (page 2-41)
- Validating requests (page 2-66)
- Auditing operator actions (page 2-68)
- Record change tracking (page 2-69)

Viewing and/or Canceling Requests

When Web Access requests are submitted, they are sent to the Request Queue and assigned a status. The status will vary, 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 1-12 and “Process States” on page 1-14.

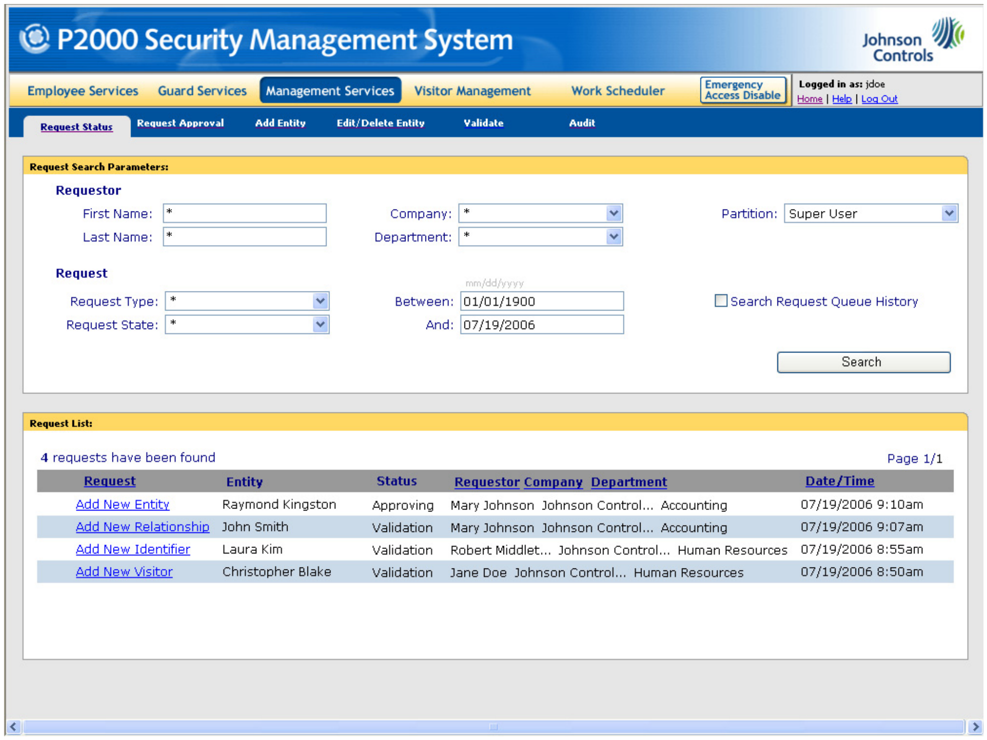
This section will describe how to view and/or cancel requests in the Request Queue.

NOTE

Depending on how the P2000 user roles 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 User Roles.

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:

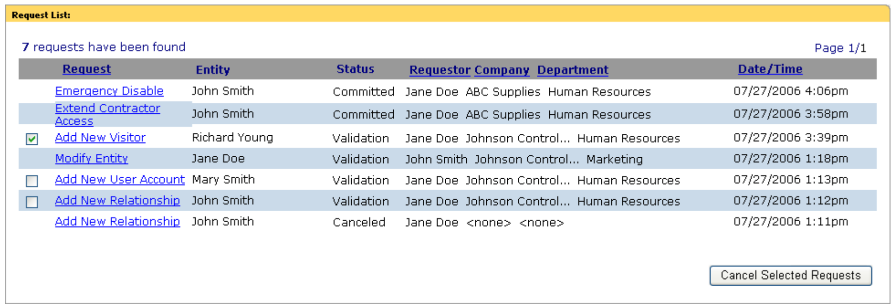
- **Request** – Displays the request type. Click the link to view detailed request information.
- **Entity** - Displays the name of the entity whose record will be modified by the request.
- **Status** – Displays the status of the request. For a description of the different request states, see "Process States" on page 1-14.
- **Requestor** – Displays the user who submitted the request.
- **Company** – Displays the company assigned to the user who submitted the request.
- **Department** – Displays the department assigned to the user who submitted the request.
- **Date/Time** – Displays the date and time the request was submitted.

Canceling Requests

You may cancel a request you submitted before it is validated and processed, but not after it has been committed. A cancelled request will be added to the Request History, where it will remain with a status of "Canceled." A cancelled request cannot be edited 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 status of the request will change to “Canceled.”

Approving or Rejecting Requests

Depending on the settings defined in P2000, each Web Access request may require up to three active approvers. The approver is an entity who has been assigned Web Request Approval permissions. The approvers are ordered in a sequence and they receive and approve requests in the same order.

Up to three approvers can be defined 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 P2000AE 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.

12/3/08

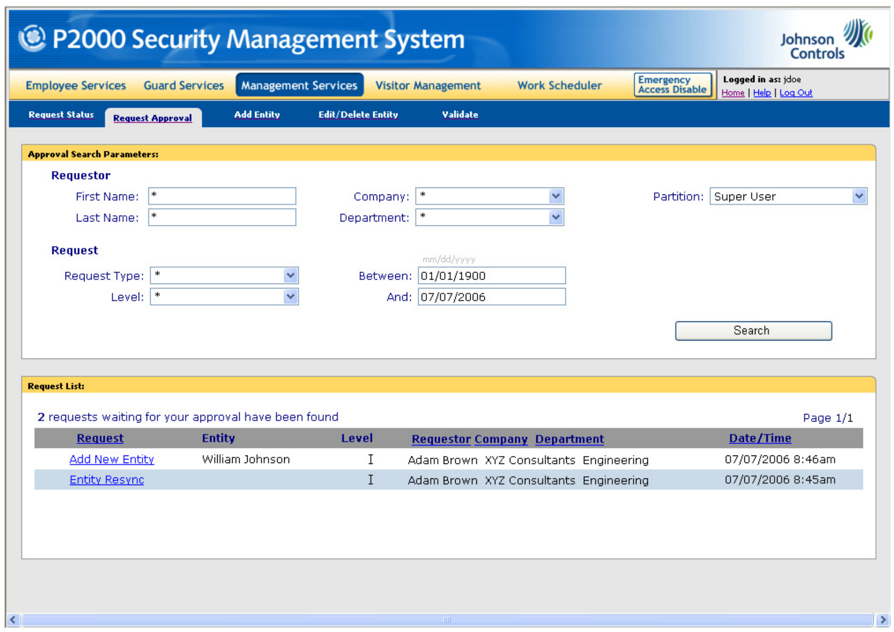
Requests can be approved via Web Access or E-mail notification. If E-mail notification is used, an E-mail will be sent to an approver when a qualifying request is submitted. This E-mail will allow the recipient approver to link to the Approval page of the specific request, where the approver can review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

For a more thorough description of the request process, see the “Request Process Flow Chart” on page 1-12 and “Process States” on page 1-14.

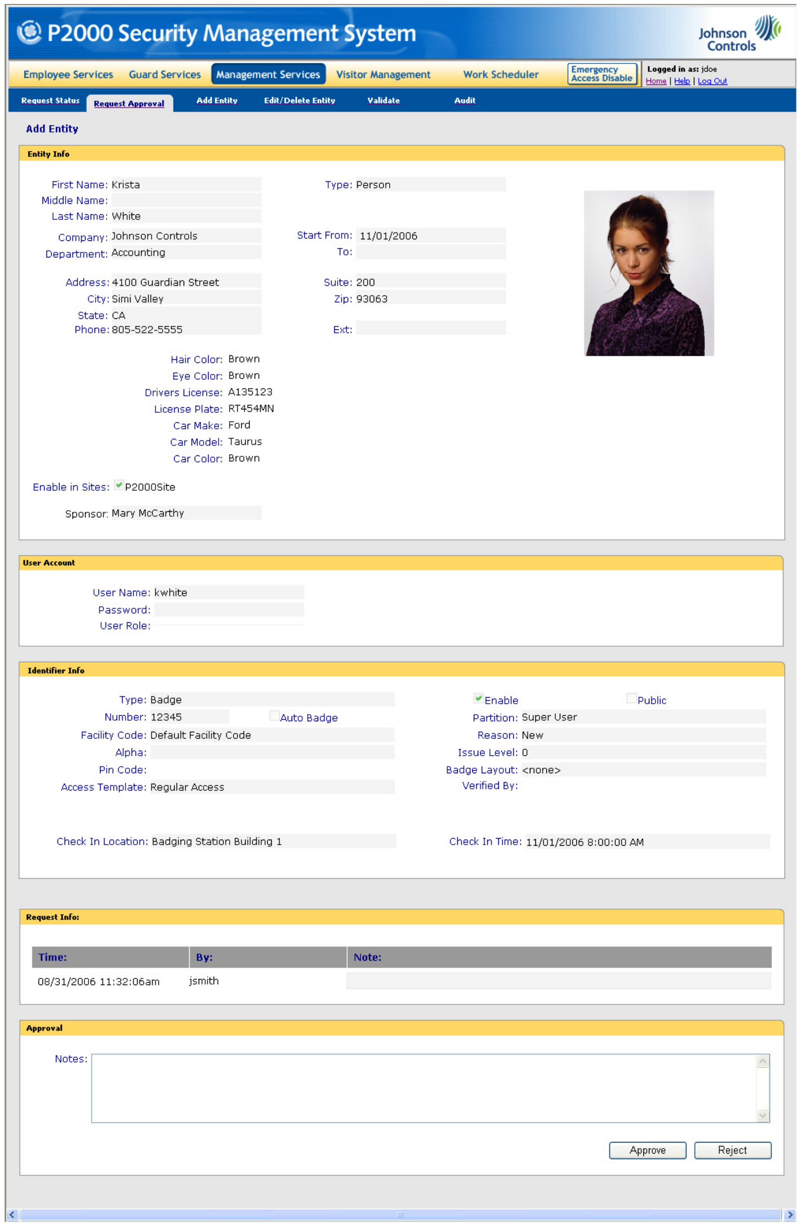
➤ To approve or reject a request via Web Access:

1. Select the **Management Services** option.
2. Click the **Request Approval** tab.

   If any requests require your approval, they will appear in the Request Approval page. You will only see requests that you have been assigned permission to approve.



3. Under the Request column, click the link of the request you wish to approve or reject. The Request Approval Summary page opens.



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** or **Reject**. The request will be removed from the Request List box on the Request Approval page.

➤ 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 Request 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** or **Reject**. The request will be removed from the Request List box on the Request Approval page.

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.

Edit button

3. Edit the request and re-submit it.

Adding an Entity

Web Access enables you to send a request to add an entity (person or asset) to the P2000 system. Every person who needs access to the facility must have an entity and identifier record entered into the P2000 system. This can include full-time employees, contractors, temporary employees, and visitors. For visitors, you may enter them on the Visitor Management page (see “Visitor Management” on page 2-73). You may also add assets and track them in the system. Security Managers with the proper permissions in P2000 can approve or deny the request.

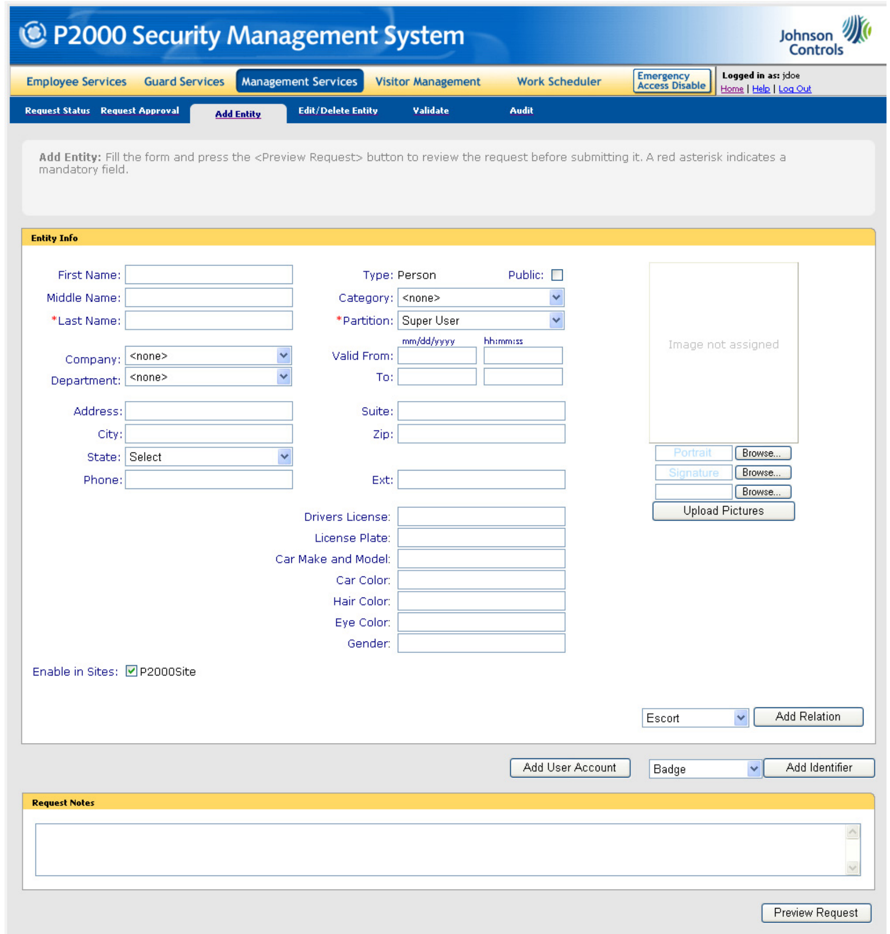
NOTE
You cannot add a System Administrator entity type using Web Access. To add this type of entity to the P2000 database, you must use the P2000 host software (see the P2000AE Software User Manual for details).

➤ To add an entity:

1. Select the **Management Services** option.
2. Click **Add Entity**. The Select Entity Type page appears.
3. Select whether the new entity is a **Person** or **Asset**.

NOTE
The data fields available will be different, depending on your selection.

The Add Entity page appears (person entity type shown).



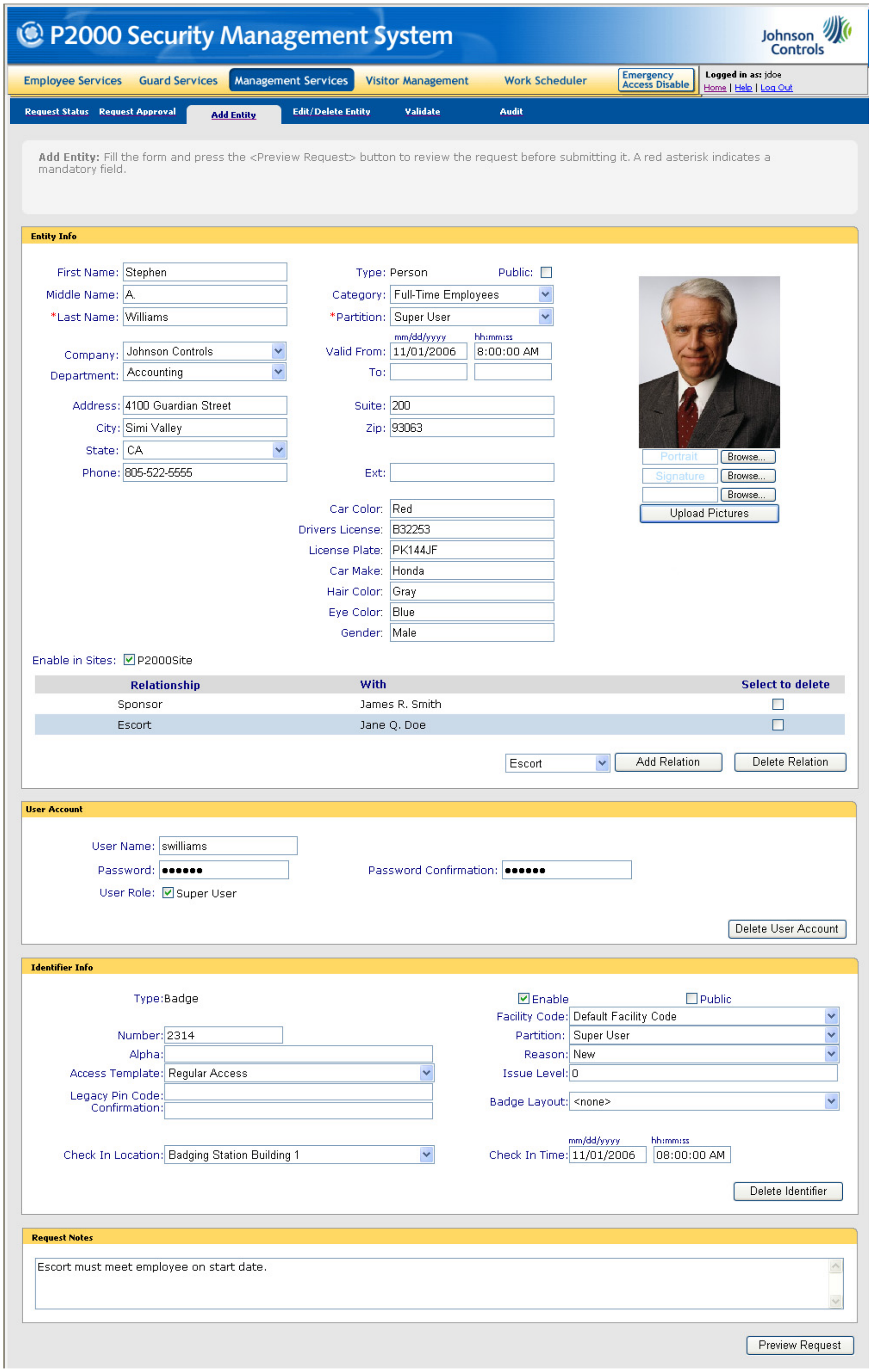
4. Enter data into the **Entity Info** box, as described in “Entity Info Field Definitions” on page 2-32.
5. To import an entity image, such as a portrait, fingerprint, or signature image, click one of the **Browse** buttons on the right side of the **Entity Info** box. See “Uploading an Entity Image” on page 2-34 for more information.
6. Enter values in any user-defined fields, if applicable. See “User-Defined Fields (UDF)” on page 2-35 for more information.
7. To add one or more relationships associated with the new entity, next to the **Add Relation** button, select the relationship type and click **Add Relation**. See “Assigning a Relationship” on page 2-35 for more information.
8. To add a user account for the new entity, click **Add User Account**. A user account enables the entity to have user access rights to the P2000 host software and Web Access. After clicking Add User Account, in the User Account box, enter a **User Name** and **Password** for the new entity. Re-enter the password to confirm.
9. If adding a user account, select a **User Role** for the user account (e.g. Super User, Limited Access, etc.). User roles are defined in the P2000 host software.

10. To assign an identifier to the new entity, next to the **Add Identifier** button, select the identifier type and click **Add Identifier**. See “Entering Identifier Info” on page 2-38 for more information.
11. Enter additional information or instructions about the request into the **Request Notes** box, if applicable. These notes are not saved with the entity record; they simply provide additional information about the request for persons approving or validating the request.
12. Click **Preview Request**.

    The Request Preview page appears, displaying the data you entered for the new entity.
13. Review the data for accuracy and do one of the following:
    - To submit the request, click **Submit Request**.
    - To modify the request, click **Modify Request**.
    - To cancel the request, click **Cancel**.

    If the entity is successfully submitted, a request submitted successfully message appears.

Entity Info Field Definitions



Type – Displays the entity type: Person or Asset. The type cannot be changed once it is selected.

NOTE

For Asset entity types, some of the following fields will not be available. For example, instead of First Name, Middle Name and Last Name, only the Name field is available.

Name - (Required) If the entity is an Asset, enter a name for the asset.

First Name – Enter the first name of the person.

Middle Name – Enter a middle initial.

Last Name – (Required) Enter the last name of the person.

Public – Select this check box if you wish this entity record to be visible to all partitions. This field will not be visible in a non-partitioned system.

Category – Select a category to assign to this entity. Examples of entity categories are Full-time Employees, Contractors, and Visitors. Categories are created using the P2000 host software. Refer to the *P2000AE Software User Manual* for detailed information.

Partition – If this is a partitioned system, select the Partition to which this entity will be assigned. This field will not be visible in a non-partitioned system.

Company / Department – Assign a company and department to the entity. Companies and Departments are created in the P2000 host software. Refer to the *P2000AE Software User Manual* for detailed information.

Valid From – Date and time when all identifiers for this entity become active. Enter the date in the following format:

> **mm/dd/yyyy**
> mm = month, dd = day, yyyy = year
> Example: 08/22/2007

Enter the time in the following format:

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

Valid To – Date and time when all identifiers for this entity expire. Enter the date and time in the same format as described in Valid From above.

The Valid To field is typically used for Visitor identifiers, but can also be edited as needed to void identifiers for a terminated employee or similar application. The system will automatically void the identifier(s) on the date and time specified.

Address and Phone Information – These entries are optional. Enter the suite, street, city, state, zip, phone number, and extension associated with the entity.

Enable in Sites – Select a check box next to each site that will be enabled for the new entity. If a site is not enabled, the person will not be able to access any areas in that site.

Uploading an Entity Image

Web Access allows you to upload an entity image, such as a portrait, fingerprint, and signature, for the new record. These images are visible when viewing the entity record in Web Access or P2000, and can be printed on the entity's badge identifier from a P2000 Video Imaging station. Refer to the *P2000AE Integrated Video Imaging Installation and Operation Manual* for more information.

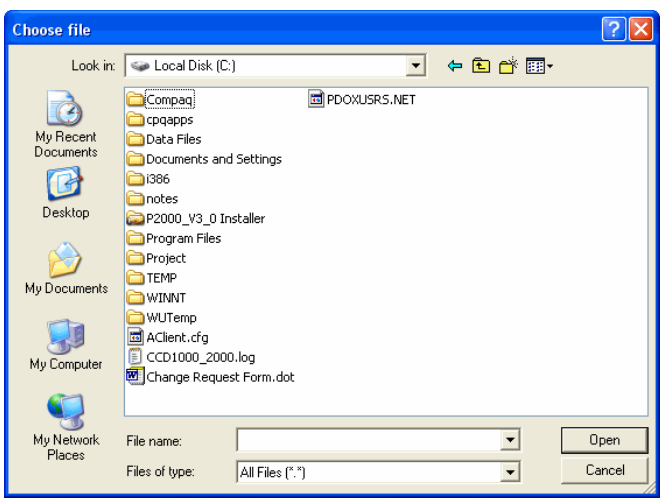
P2000 Web Access supports the following image formats: JPEG, GIF, and BMP. If the format of the image you wish to import is not supported, use an image editing program to convert to a supported format.

NOTE

The file size of each image cannot exceed 1 MB. Also, the imported image will be displayed 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, it will be resized 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 an entity image:

1. Click one of the **Browse** buttons on the right side of the Entity Info box. The Choose File dialog box appears.

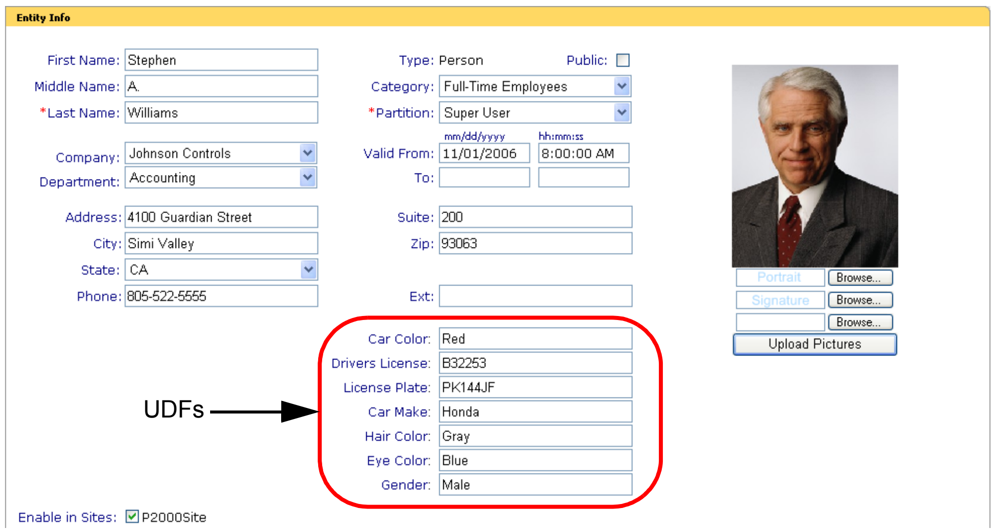


2. Locate and select the image file that will be imported.
3. Click **Open**. The directory path to the file will appear in the field next to the **Browse** button.

4. Click **Upload Pictures**. View the appearance of each uploaded image for approval before submitting the request. Use a bitmap editing program to edit an image, if necessary, and re-upload it until you are satisfied with its appearance.

User-Defined Fields (UDF)

If UDFs were created in P2000, they will appear on the Add Entity and Edit Entity pages. Enter a value, if applicable, for the UDFs listed in the Entity Info box.



NOTE

If the P2000 is configured to use the Time and Attendance feature, the system administrator may configure a UDF for the employee message that appears on the Time and Attendance terminal. If this is the case, in the designated UDF, enter the message you wish the employee to see from the terminal.

Assigning a Relationship

The entity relationship application enables you to assign one or more sponsors, escorts, or owners to the entity. You may also assign the current entity to a particular group.

About Entity Sponsors/Owners

A sponsor is someone who sponsors an entity, thereby accepting some level of responsibility for the entity. A typical example of a sponsor is an employee who invites a visitor to the facility to conduct business. In this example, the employee is the sponsor of the visitor. You may also assign regular employees as sponsors of temporary employees.

Since entities can also be assets, you can assign an entity (person) as the owner of an entity (asset). For example, if an employee is assigned a particular piece of electronic equipment, this equipment is added to the P2000 SMS as an asset, and the employee is assigned as the owner of that asset.

A sponsored entity may also be assigned an entity group as the sponsor. If this case, everyone within the entity group is the sponsor/owner of the entity (person or asset).

About Entity Escorts

You may assign one or more escorts to an entity, if the entity requires some level of supervision inside the facility. If properly configured, the P2000 Security Management System can deny access to an escorted entity until the system identifies that each escort is present. An escort must present an identifier, such as an access badge, at the controlled location for the system to verify whether he/she is present.

An escort can be one of the following:

- **A single entity unassociated with an entity group.** An escorting entity does not have to be assigned to an entity group. A escorted entity can have one or more escorts assigned to him/her, and each entity does not have to be assigned to an entity group.
- **A single member of an entity group.** Entities who are members of this group are able to escort a non-group member (the escorted person or asset) through the building. In order for the escorted entity to be granted access, one member of the escort group must be present and identify him/herself within a defined period of time.
- **All members of the entity group.** Entities that are members of this group are required to enter a controlled area together. All entities must present and identify themselves within a defined period of time to be granted access.

➤ To assign a relationship:

1. Next to the **Add Relation** button, select the relationship type and click **Add Relation**.
2. Under the **Relationship With** column heading, select a relationship type.
   - **Escort** – The person you select will serve as an escort for the entity and will be required to present an identifier together with the entity in order to gain access at a door (depending on the Access Profiles assigned). Escort operation depends on the CK722 Access Control object (ACO) configuration. For more information, refer to the *CK722 Network Controller Commissioning Guide*.
   - **Sponsor** – The selected person will take responsibility of the entity while in the facility.
   - **Accompanied By** – The entity is not a member of the group, but in order for the entity to be granted access, the entity must be escorted by at least one member of the selected Entity Group.

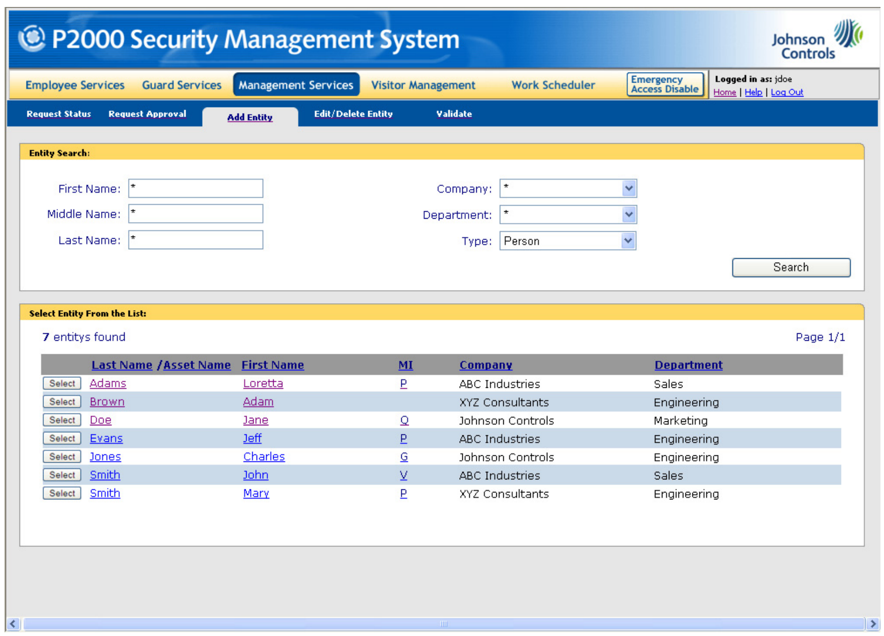
- **Escorted By All** – The entity is a member of the group, and in order for the entity to be granted access, the entity must be escorted by all members of the selected Entity Group. Entities that are members of this group are required to enter a controlled area together. All entities must present and identify themselves within a defined period of time to be granted access.

NOTE

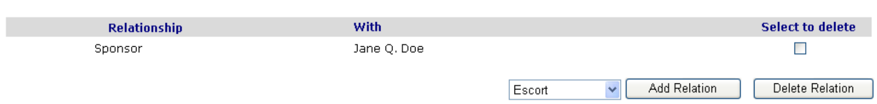
Escort operation depends on CK722 Access Control object configuration and the Access Profiles assigned to the entity. Refer to the CK722 Network Controller Commissioning Guide.

- **Member Of** – The entity is assigned to the selected Entity Group.

3. If you selected Escort of Sponsor, click the **Select Entity** button. Locate the entity whom you will assign as the escort or sponsor. Use the name search fields, if necessary. Click the **Select** button next to the entity.



The selected entity will be listed under the **Relationship With** column heading.



4. If you selected Accompanied By, Escorted By All, or Member Of, select the entity group from the drop-down list.
5. To add more relationships to the entity, click the **Add Relation** button.
6. To remove a relationship, select the check box under the **Select to delete** column next to the relationship you wish to remove and click **Delete Relation**.

Entering Identifier Info

The Identifier application allows you to add identifiers associated with the entity. An entity may have multiple identifiers. You can define access badge identifiers, which use access profiles to restrict access to authorized areas at authorized times. Some facilities require that the entity present an access badge at a door, and immediately enter a PIN code at a keypad, for the system to grant access to a controlled area.

You can also define ID badges that can be created strictly for identification purposes.

The following identifier types are available:

- Access Badge
- Card ID
- Common PIN
- ID Badge
- PIN Code

NOTE
The identifier fields available are determined by the identifier type selected.

Access Badge, Card ID, and ID Badge Identifiers

The following fields are available when adding Access Badge, Card ID, and ID Badge identifiers:

Type – Displays the identifier type selected. Once you select an identifier type, you cannot modify this field.

- **Badge** – Select this option to assign an access badge identifier to the entity. Access badge identifiers allow entities to access a controlled area by presenting an access badge to a portal's reader. In addition, when an entity uses an access badge, the P2000 system can identify and track the location of the entity in the facility. Access profiles are assigned to access badge identifiers to define the access rights assigned to the entity.
- **Card ID** – This is a code of a particular badge that users enter on a keypad to prompt the system to grant them access to a controlled area. This code is typically printed on the badge itself. With this option selected, users must enter the Card ID without presenting an access badge to access a controlled area.
- **Badge / Card ID** – If this option is selected, users can either present their badge to a reader or enter their Card ID on a keypad to enter a controlled area of the facility.
- **ID Badge** – This badge visually identifies an entity but does not provide access control capabilities – it cannot be used to access a controlled area of a facility.

NOTE

Some of the following fields are not available for ID badge identifiers.

Number – Enter the number of the access badge identifier (the number of allowed characters depends on the parameters defined in the P2000 host software). This number is usually pre-assigned to badges provided by Johnson Controls. This number is also the Card ID that users enter on keypads to access a controlled area.

NOTE

You can assign any number of badge identifiers to an entity; however, if your facility uses legacy panels, each badge identifier must have a unique number.

Alpha – Some custom badge identifiers may provide space for alpha characters. If so, enter them here. (Limited to 4 characters.)

Access Template – Select from the drop-down list the Access Template that provides the access rights of the entity. When the entity record is created, P2000 will assign the selected template to the entity's access profile. See "Managing Entity Access Profile Data" on page 2-59 for information on access templates and access profiles.

Legacy PIN Code / Confirmation – Enter the entity's personal identification number (PIN) to be used with PIN readers connected to legacy panels. If an algorithmic PIN is used, leave this field blank. For PIN readers connected to CK722 panels, use the identifier type PIN Code described in "PIN Code Identifiers" on page 2-41. In the Confirmation field, enter the PIN you entered into the PIN code field.

Enable – When a badge identifier is created, it is automatically enabled. Select this check box to temporarily disable this identifier. This function is useful when you wish to temporarily disable a badge identifier, but do not wish to re-issue or redefine the identifier.

Public – Select this check box for this badge identifier to be visible to all partitions.

Facility Code – Select from the drop-down list the type of facility code to be assigned to this badge identifier. Facility codes are provided by Johnson Controls and identify the badges that belong to your particular site. Facility codes for legacy panels are defined in the P2000 host software. Facility codes for CK722 panels are defined in the P2000 System Configuration Tool (SCT).

Partition – If this is a partitioned system, select the Partition in which this Access Badge identifier will be active.

Reason – Select a Reason from the drop-down list to indicate why the badge identifier is being issued. The choices are: New, Reissue, Damaged, Lost, Not Returned, Returned, Stolen, Temporary, or Visitor.

Issue Level – Select an issue level per badge identifier number. If an entity loses a badge, you would give him/her the next available issue level and retain the same badge number. The number of badge issue levels supported depends on the panel/controller type you use.

Badge Layout – If you have created a number of badge designs using your Video Imaging software, you can select a badge layout from the drop-down list. (Badge design instructions are provided in the *P2000AE Integrated Video Imaging Installation and Operation Manual*.)

Check In Location – If this field is visible, select the location where the entity will check in. The badging station location is defined in the P2000 host software (System Configuration>Workstation>Description field).

Check In Time – If this field is visible, enter the time when the entity will check in.

Common PIN Identifiers

Formerly called "Air Crew PIN," a Common PIN is a personal identification number users enter at a keypad to access a controlled area. When entering a Common PIN at the keypad, users must enter *2 before entering the assigned PIN. If they do not enter *2, the P2000 system will treat the data entry as an Access PIN entry request (see "PIN Code Identifiers" on page 2-41). Presenting a badge identifier is not required when using Common PINs.

The following fields are available when adding Common PIN identifiers:

Type – Displays the identifier type selected. Once you select an identifier type, you cannot modify this field.

Common PIN – Enter the Common PIN code in this field.

Access Template – Select from the drop-down list the Access Template that provides the access rights of the entity. When the entity record is created, P2000 will assign the selected template to the entity's access profile. See "Managing Entity Access Profile Data" on page 2-59 for information on access templates and access profiles.

Enable – When a Common PIN identifier is created, it is automatically enabled. Select this check box to temporarily disable this identifier. This function is useful when you wish to temporarily disable a Common PIN identifier, but do not wish to re-issue or redefine the identifier.

Public – Select this check box if you wish this identifier to be visible to all partitions.

Partition – If this is a partitioned system, select the Partition in which this identifier will be active.

Reason – Select a Reason from the drop-down list to indicate why the identifier is being issued. The choices are: New, Reissue, Damaged, Lost, Not Returned, Returned, Stolen, Temporary, or Visitor.

Check In Location – If this field is visible, select the location where the entity will check in. The badging station location is defined in the P2000 host software (System Configuration>Workstation>Description field).

Check In Time – If this field is visible, enter the time when the entity will check in.

PIN Code Identifiers

You can create PIN Code identifiers that can be assigned to entities for authentication purposes. These PIN Code identifiers can only be used on keypads connected to CK722 controllers. The P2000 system will grant or deny access to a controlled area based on the validity of the entered PIN code.

The following fields are available when adding PIN Code identifiers:

Type – Displays the identifier type selected. Once you select an identifier type, you cannot modify this field. PIN Code identifier types consist of the following:

- **Access PIN** – Identifier used for access requests.
- **Intrusion PIN** – Identifier used for intrusion requests.
- **Universal PIN** – Identifier used for access *and* intrusion requests.

Name – Enter a name to describe the selected PIN Code identifier.

Number – Enter the access, intrusion, or universal personal identification number to be used with PIN readers connected to CK722 panels. Enter the same PIN code into the Confirmation field.

Access Template – Select from the drop-down list the Access Template that provides the access rights of the entity. When the entity record is created, P2000 will assign the selected template to the entity's access profile. See "Managing Entity Access Profile Data" on page 2-59 for information on access templates and access profiles.

Check In Location – If this field is visible, select the location where the entity will check in. The badging station location is defined in the P2000 host software (System Configuration>Workstation>Description field).

Check In Time – If this field is visible, enter the time when the entity will check in.

Editing or Deleting an Entity

This section describes how to edit or delete an entity record using Web Access.

NOTE

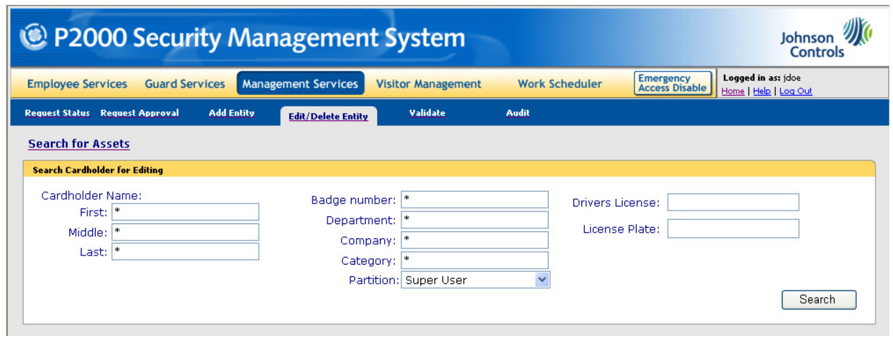
You may only edit or delete a person or asset entity type. You cannot edit or delete a system administrator entity type. To edit or delete this type of entity, you must use the P2000 host software (refer to the P2000AE Software User Manual for details).

Locating an Entity to Edit or Delete

To edit or delete an entity record, you must first locate the record in the P2000 database using the search feature on the Edit/Delete Entity page.

➤ To locate an entity to edit or delete:

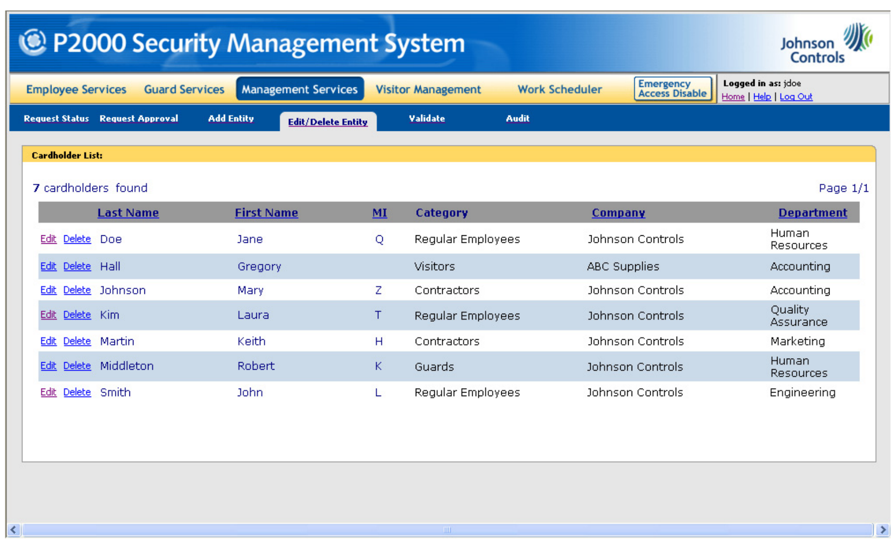
1. Select the **Management Services** option.
2. Click the **Edit/Delete Entity** tab. The Entity Search page (for person entities) appears.



3. If you wish to locate a *person*, enter any search criteria on this page and click **Search**.

   If you wish to locate an *asset*, click **Search for Assets** to display search fields applicable to finding an asset. Enter search criteria and click **Search**.

   The Entity Search Results page appears.



Editing or Deleting an Entity

➤ To edit an entity:

1. Locate an entity to edit using the instructions in “Locating an Entity to Edit or Delete” on page 2-41.
2. From the Entity Search Results page, click **Edit** next to the record you wish to edit.

The Edit Entity page appears (person entity type shown).

3. Click the link that applies to the data you wish to add, edit, or delete.

   Depending on the data associated and configured for this entity, you can add, edit, or delete the following:

   - **General Information** – Click this link in the Entity Editing Choices box to edit general information associated with the entity, such as name, company, department, address, phone, category, validation period, and UDFs. You may also modify the entity's images. For field definitions, see "Entity Info Field Definitions" on page 2-32.

   - **Relationship** – If the entity currently has a relationship, it will appear as a link in the Entity Editing Choices box. Clicking this link allows you to modify the relationship. The Add Relationship link at the top of the page enables you to add a relationship to the entity record. For information on adding, editing, or deleting relationships, see page 2-63.

   - **Access Profile** – If the entity currently has an access profile, it will appear as a link in the Entity Editing Choices box. Clicking this link allows you to modify the access profile. The Add Access Profile link at the top of the page enables you to add an access profile to the entity record. For information on adding, editing, or deleting access profiles, see page 2-56.

NOTE

If an access template was selected when the entity record was added, an access profile name will be automatically generated by the P2000 system. This name will appear as "Template Name+random string of characters and numbers".

- **User Account** – If the entity currently has a user account, it will appear as a link in the Entity Editing Choices box. Clicking this link allows you to modify the user account. The Add User Account link at the top of the page enables you to add a user account to the entity record. For information on adding, editing, or deleting user accounts, see page 2-51.
- **Identifier** – If the entity currently has an identifier, it will appear as a link in the Entity Editing Choices box. Clicking this link allows you to modify the identifier. The Add Identifier link at the top of the page enables you to add an identifier to the entity record. For information on adding, editing, or deleting identifiers, see page 2-48.
- **Journal** – If the entity currently has a journal, the title, content, and last modified date and time appear for each entry in the Entity Editing Choices box. Clicking the link under the Journal Title column allows you to modify the selected journal.The Add Journal link at the top of the page enables you to add a journal entry to the entity record. For information on adding, editing, or deleting entity journals, see page 2-45.

4. Edit the entity record, as needed.
5. If you are adding or editing data, when you are finished with your data entry or modifications, click **Preview Request**.

   If you are deleting a relationship, access profile, use account, identifier, or journal, click the **Delete** button.
6. Perform one of the following actions:
   - Click **Submit Request** if you are satisfied with the request and you are ready to submit it for processing.
   - Click **Modify Request** if modifications are still needed prior to submittal.
   - Click **Cancel** to cancel the request. Clicking this button does not save the request data and will open the Edit/Delete Entity page.

➤ To delete an entity:

CAUTION

When you delete an entity, ALL data associated with the entity, such as identifiers, relationships, user accounts, journals, and access profiles, will also be deleted. You cannot undo this action.

NOTE

When deleting a entity record from Web Access on a P2000 Enterprise system, the entity record will be deleted from all sites within the Enterprise system. Refer to the P2000AE Software User Manual for more information on managing entity records on multiple sites in a P2000 Enterprise system.

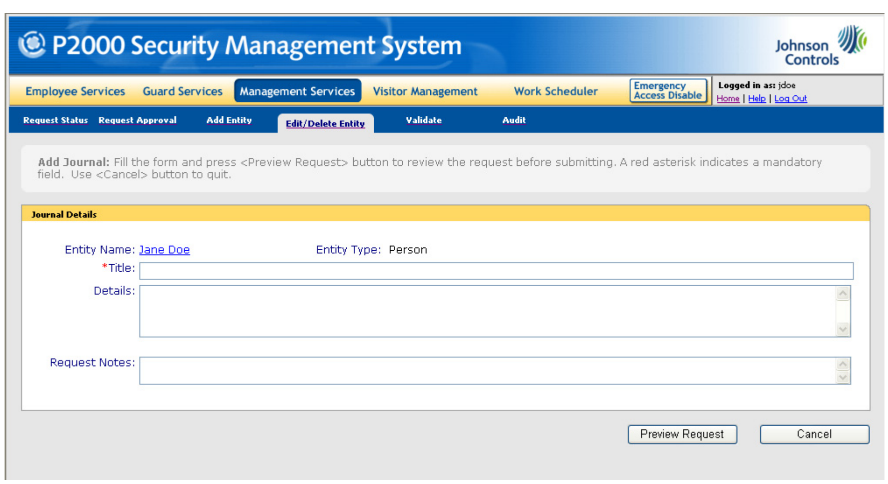
1. Locate an entity to delete using the instruction in "Locating an Entity to Edit or Delete" on page 2-41.
2. From the Entity Search Results page, click **Delete** next to the record you wish to delete. The Delete Entity page appears.
3. Click the **Preview Delete** button. Verify that you have selected the correct record you wish to delete.
4. Click **Submit Request for Delete.** The record and all associated data are deleted.

Adding, Editing or Deleting Entity Journals

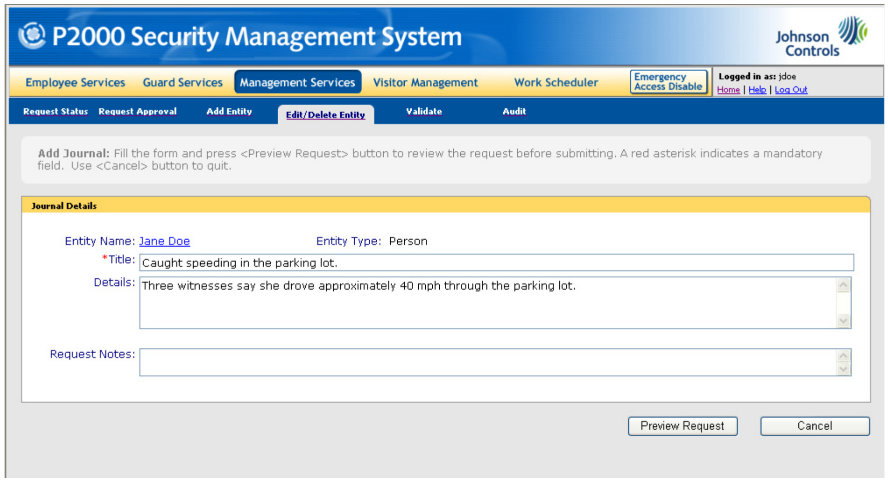
Journal entries supplement entity information by storing notes associated with each entity. For example, you may want to keep track of persons with parking violations, or keep a record of employees that attended specific company training, or track tenants with suspicious behavior.

➤ To add a journal:

1. Locate an entity for whom you wish to add a journal entry. See "Locating an Entity to Edit or Delete" on page 2-41.
2. From the Entity Search Results page, click **Edit** next to the entity for whom you will add a journal entry. The Entity Edit page appears.
3. Click the **Add Journal** link at the top of the page. The Journal Details page appears, displaying the entity name and type.



4. Enter a journal title in the **Title** box.
5. In the **Details** box, enter the details of the journal entry.

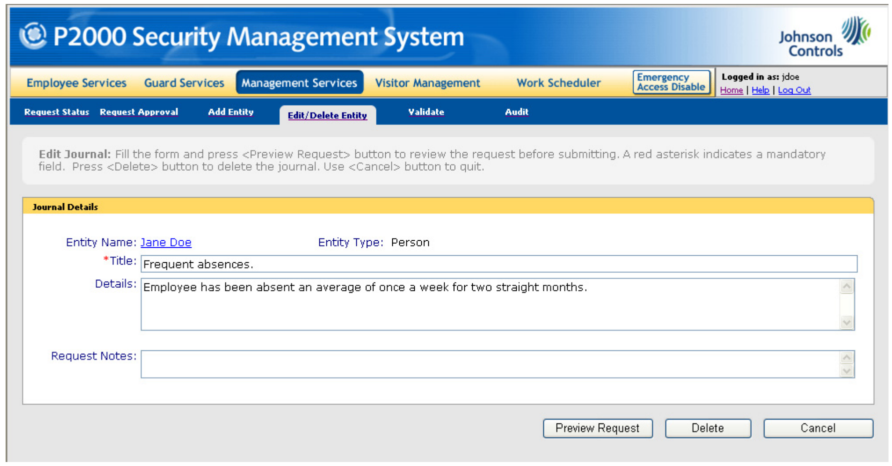


6. Enter any **Request Notes**, if applicable. These notes are not saved with the entity record; they simply provide additional information about the request for persons approving or validating the request.
7. Click **Preview Request**.
8. Perform one of the following actions:
   - Click **Submit Request** if you are satisfied with the request and you are ready to submit it for processing.
   - Click **Modify Request** if modifications are still needed prior to submittal.
   - Click **Cancel** to cancel the request. Clicking this button does not save the request data and will open the Edit/Delete Entity page.

➤ To edit a journal:

1. Locate an entity for whom you wish to edit a journal entry. See “Locating an Entity to Edit or Delete” on page 2-41.
2. From the Entity Search Results page, click **Edit** next to the entity for whom you will edit a journal entry. The Edit Entity page appears.

   Existing journal entries are listed in the Entity Editing Choices box at the bottom of the page.
3. Click the title of the journal you wish to edit. The Journal Details page appears.

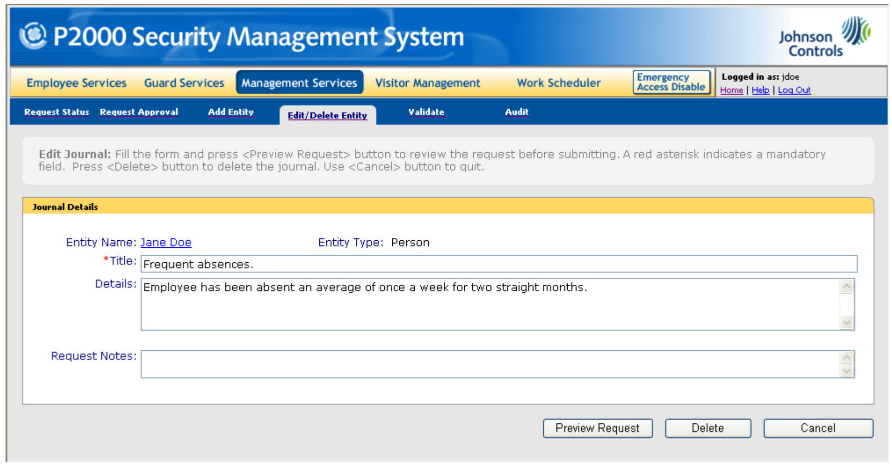


4. Edit the journal's **Title** and **Details**, as necessary.
5. Enter any **Request Notes**, if applicable. These notes are not saved with the entity record; they simply provide additional information about the request for persons approving or validating the request.
6. Click **Preview Request**.
7. Perform one of the following actions:
   - Click **Submit Request** if you are satisfied with the request and you are ready to submit it for processing.
   - Click **Modify Request** if modifications are still needed prior to submittal.
   - Click **Cancel** to cancel the request. Clicking this button does not save the request data and will open the Edit/Delete Entity page.

➤ To delete a journal:

1. Locate an entity for whom you wish to delete a journal entry. See "Locating an Entity to Edit or Delete" on page 2-41.
2. From the Entity Search Results page, click **Edit** next to the entity for whom you will delete a journal entry. The Edit Entity page appears.

   Existing journal entries are listed in the Entity Editing Choices box at the bottom of the page.
3. Click the title of the journal you wish to delete. The Journal Details page appears.



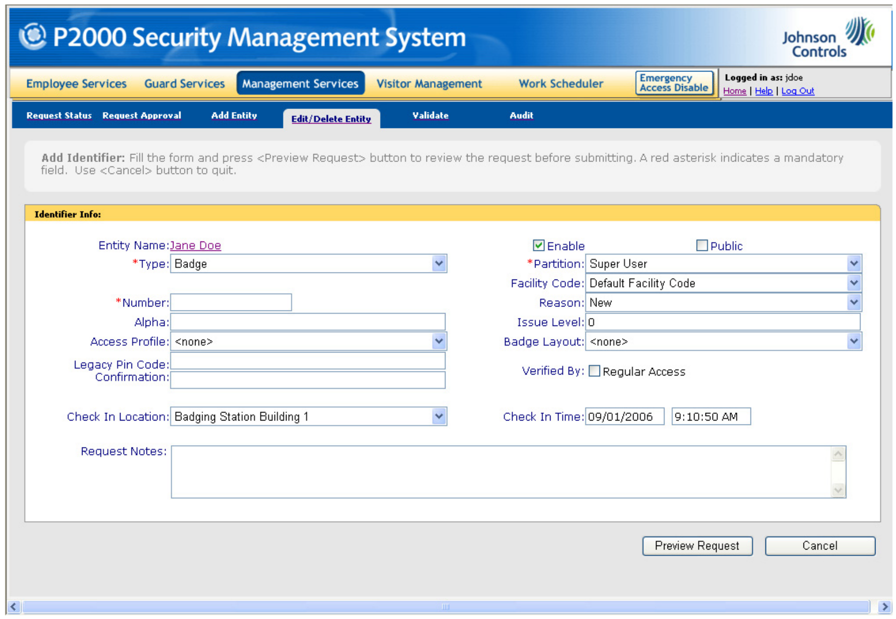
4. Enter any **Request Notes**, if applicable. These notes are not saved with the entity record; they simply provide additional information about the request for persons approving or validating the request.
5. Click **Delete**.
6. Perform one of the following actions:
   - Click **Submit Request** if you are satisfied with the request and you are ready to submit it for processing.
   - Click **Modify Request** if modifications are still needed prior to submittal.
   - Click **Cancel** to cancel the request.

Adding, Editing or Deleting Identifiers

➤ To add an identifier:

1. Locate an entity for whom you wish to add an identifier. See “Locating an Entity to Edit or Delete” on page 2-41.
2. On the Entity Search Results page, click **Edit** next to the name of the entity for whom you will add an identifier. The Edit Entity page appears.

3. Click the **Add Identifier** link on the top of the page. The Identifier Info page opens.



4. Enter identifier information into the Identifier Info fields. See "Entering Identifier Info" on page 2-38 for detailed information about these fields.
5. Enter any **Request Notes**, if applicable. These notes are not saved with the entity record; they simply provide additional information about the request for persons approving or validating the request.
6. Click **Preview Request**.
7. Perform one of the following actions:
   - Click **Submit Request** if you are satisfied with the request and you are ready to submit it for processing.
   - Click **Modify Request** if modifications are still needed prior to submittal.
   - Click **Cancel** to cancel the request. Clicking this button does not save the request data and will open the Edit/Delete Entity page.

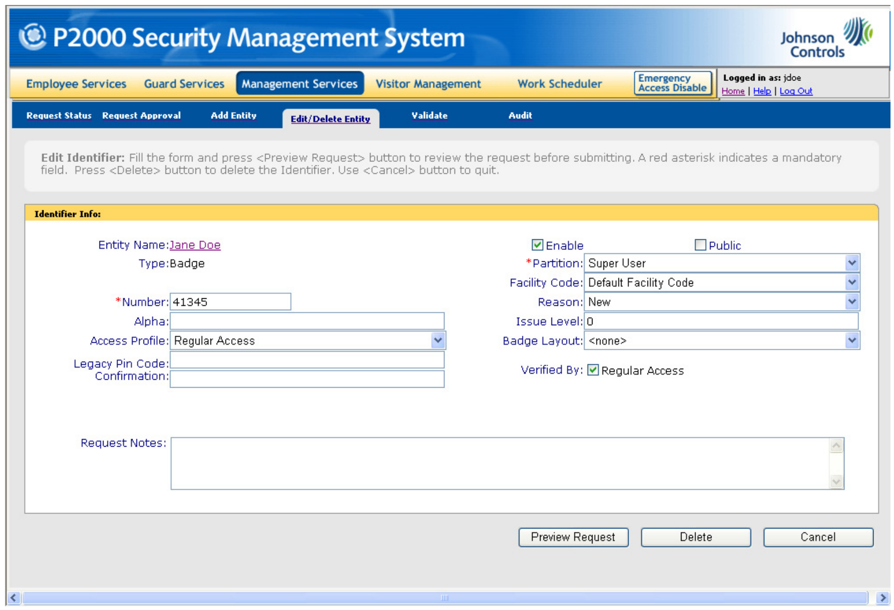
➤ To edit an identifier:

1. Locate an entity for whom you wish to edit an identifier. See "Locating an Entity to Edit or Delete" on page 2-41.
2. On the Entity Search Results page, click **Edit** next to the name of the entity for whom you will edit an identifier. The Edit Entity page appears.

   Existing identifiers are listed in the Entity Editing Choices box at the bottom of the page.

12/3/08

3. Click the identifier you wish to edit. The Identifier Info page appears.



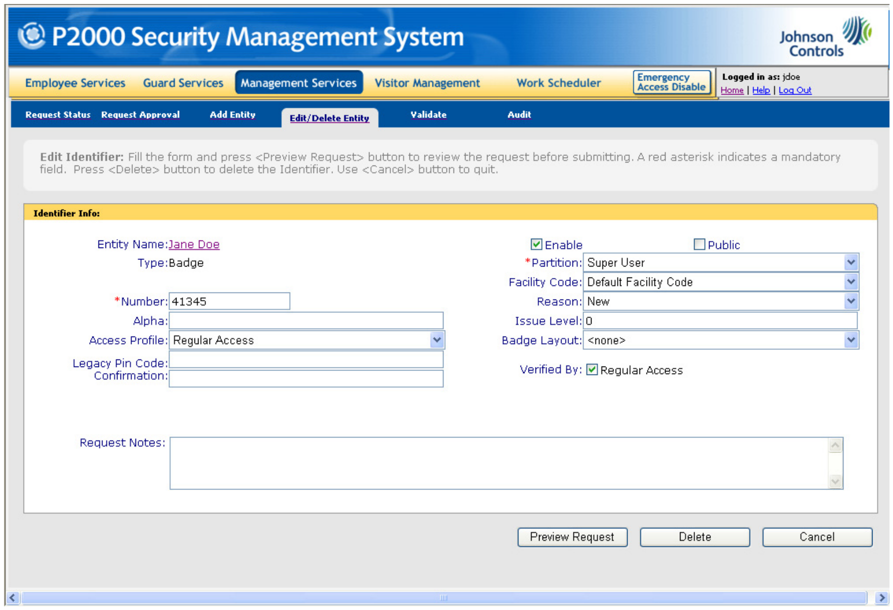
4. Edit identifier information as needed. See “Entering Identifier Info” on page 2-38 for detailed information about these fields.
5. Enter any **Request Notes**, if applicable. These notes are not saved with the entity record; they simply provide additional information about the request for persons approving or validating the request.
6. Click **Preview Request**.
7. Perform one of the following actions:
   - Click **Submit Request** if you are satisfied with the request and you are ready to submit it for processing.
   - Click **Modify Request** if modifications are still needed prior to submittal.
   - Click **Cancel** to cancel the request. Clicking this button does not save the request data and will open the Edit/Delete Entity page.

➤ To delete an identifier:

1. Locate an entity for whom you wish to delete an identifier. See “Locating an Entity to Edit or Delete” on page 2-41.
2. On the Entity Search Results page, click **Edit** next to the name of the entity for whom you will delete an identifier. The Edit Entity page appears.

   Existing identifiers are listed in the Entity Editing Choices box at the bottom of the page.

3. Click the identifier you wish to delete. The Identifier Info page appears.



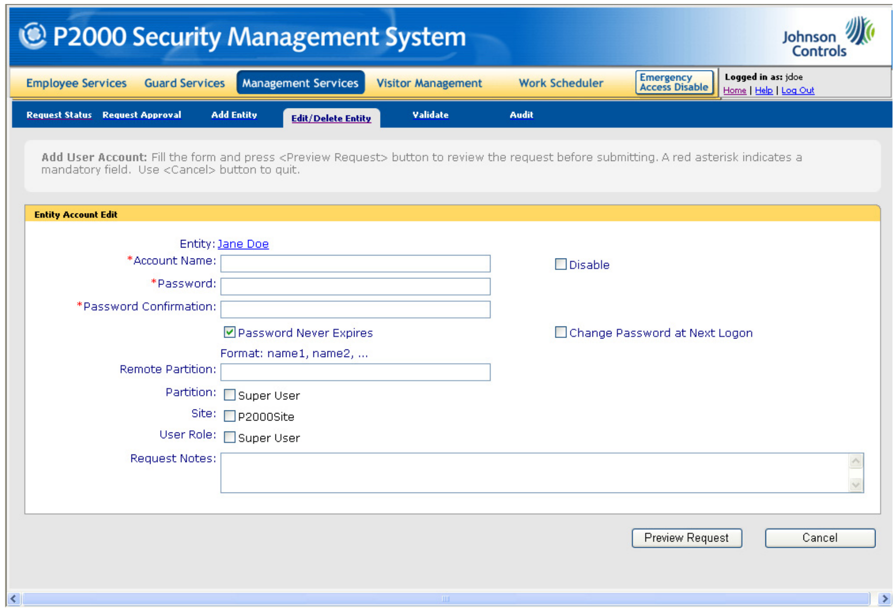
4. Enter any **Request Notes**, if applicable. These notes are not saved with the entity record; they simply provide additional information about the request for persons approving or validating the request.
5. Click **Delete**.
6. Perform one of the following actions:
   - Click **Submit Request** if you are satisfied with the request and you are ready to submit it for processing.
   - Click **Modify Request** if modifications are still needed prior to submittal.
   - Click **Cancel** to cancel the request.

Adding, Editing, or Deleting User Accounts

➤ To add a user account:

1. Locate an entity for whom you wish to add a user account. See “Locating an Entity to Edit or Delete” on page 2-41.
2. On the Entity Search Results page, click **Edit** next to the name of the entity for whom you will add a user account. The Edit Entity page appears.

3. Click the **Add User Account** link on the top of the page. The Entity Account Edit page opens.



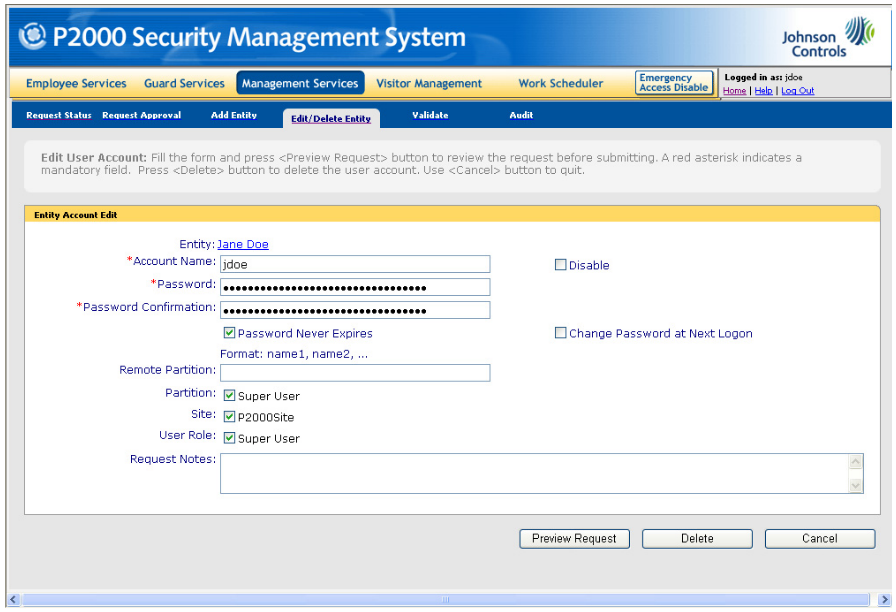
4. Enter user account information into the Entity Account Edit fields. See "Entity Account Edit Field Definitions" on page 2-54 for detailed information about these fields.
5. Enter any **Request Notes**, if applicable. These notes are not saved with the entity record; they simply provide additional information about the request for persons approving or validating the request.
6. Click **Preview Request**.
7. Perform one of the following actions:
   - Click **Submit Request** if you are satisfied with the request and you are ready to submit it for processing.
   - Click **Modify Request** if modifications are still needed prior to submittal.
   - Click **Cancel** to cancel the request. Clicking this button does not save the request data and will open the Edit/Delete Entity page.

➤ To edit a user account:

1. Locate an entity for whom you wish to edit a user account. See "Locating an Entity to Edit or Delete" on page 2-41.
2. On the Entity Search Results page, click **Edit** next to the name of the entity for whom you will edit a user account. The Edit Entity page appears.

   Existing user accounts are listed in the Entity Editing Choices box at the bottom of the page.

3. Click the user account you wish to edit. The Entity Account Edit page appears.



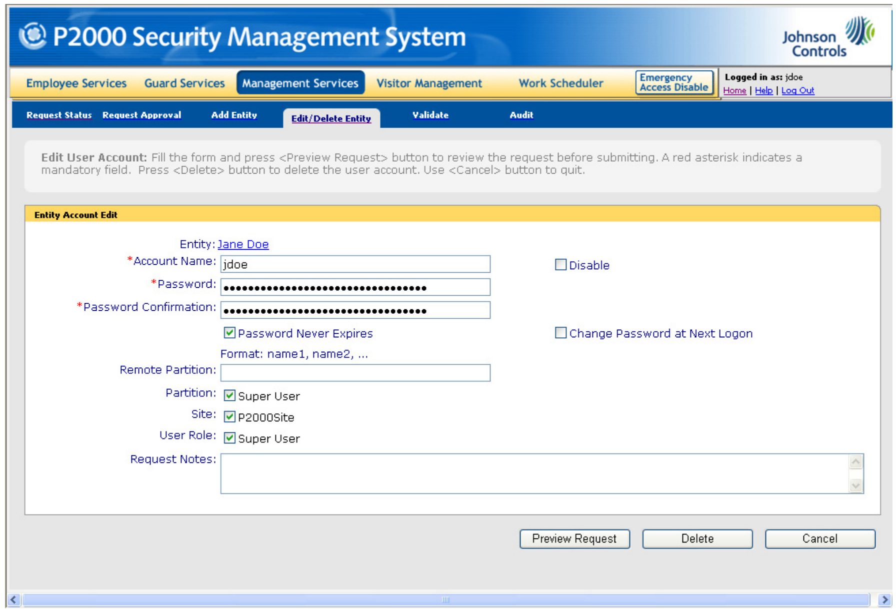
4. Edit user account information on the Entity Account Edit page. See "Entity Account Edit Field Definitions" on page 2-54 for detailed information about the fields on this page.
5. Enter any **Request Notes**, if applicable. These notes are not saved with the entity record; they simply provide additional information about the request for persons approving or validating the request.
6. Click **Preview Request**.
7. Perform one of the following actions:
   - Click **Submit Request** if you are satisfied with the request and you are ready to submit it for processing.
   - Click **Modify Request** if modifications are still needed prior to submittal.
   - Click **Cancel** to cancel the request. Clicking this button does not save the request data and will open the Edit/Delete Entity page.

➤ To delete a user account:

1. Locate an entity for whom you wish to delete a user account. See "Locating an Entity to Edit or Delete" on page 2-41.
2. On the Entity Search Results page, click **Edit** next to the name of the entity for whom you will delete a user account. The Edit Entity page appears.

   Existing user accounts are listed in the Entity Editing Choices box at the bottom of the page.

3. Click the user account you wish to delete. The Entity Account Edit page appears.



4. Enter any **Request Notes**, if applicable. These notes are not saved with the entity record; they simply provide additional information about the request for persons approving or validating the request.
5. Click **Delete**.
6. Perform one of the following actions:
   - Click **Submit Request** if you are satisfied with the request and you are ready to submit it for processing.
   - Click **Modify Request** if modifications are still needed prior to submittal.
   - Click **Cancel** to cancel the request.

Entity Account Edit Field Definitions

This section describes the fields on the Entity Account Edit page.

Entity – Name of the entity whose user account will be edited or deleted.

Account Name – Name of the user account that will be entered when logging on to the P2000 system.

Password – Enter the password that will be entered when logging on to the P2000 system. The system will display an asterisk for each character or number (****).

Password Confirmation – Enter the password again to confirm.

Password Never Expires – Select this option to define passwords that never expire, for system administrator users for example.

Remote Partition – If the user will be monitoring remote messages, use this field to define the partitions to which the user will have access. If you do not enter any remote partition names, the user can monitor all messages from the remote site.

Remote partitions are partitions from other Enterprise systems – not from other P2000 sites within the Enterprise System.

NOTE

Remote messages are any alarm or transaction messages originated at another P2000 site. Refer to the P2000AE Software User Manual for details.

Partition – Select the check box next to each partition to which this user will have access. The Partition field will appear only if your system has the Partition option. Users can be assigned to single or multiple partitions and have unique access restrictions, such as the ability to add, modify, or view database information within their assigned partitions. Partitions are defined in P2000. Refer to the *P2000AE Software User Manual* for more information.

Site – Select the check box next to each Enterprise site to which this user will have access. The Site field will appear only if your system has the Enterprise option, and displays the different sites within the P2000 Enterprise. Users can only modify and manage records that belong to a site that the user can access. Enterprise sites are defined in P2000. Refer to the *P2000AE Software User Manual* for more information.

User Role – Select the check box next to each User Role you wish to assign to the entity. User roles define the applications and/or database items that the user can view or change. Each user account can be associated with different rights to applications.

NOTE

A user can perform any function if at least one user role assigned to the user allows permission to that function.

Disable – Select this option if you wish to disable this account. Once this option is selected, this account can no longer be used for logging into P2000, until the account is enabled again.

Change Password at Next Logon – If a user forgets his or her password, the system administrator may grant a temporary password and force the user to change the password at the beginning of the next login. A password cannot be changed for MIS or XML RPC users.

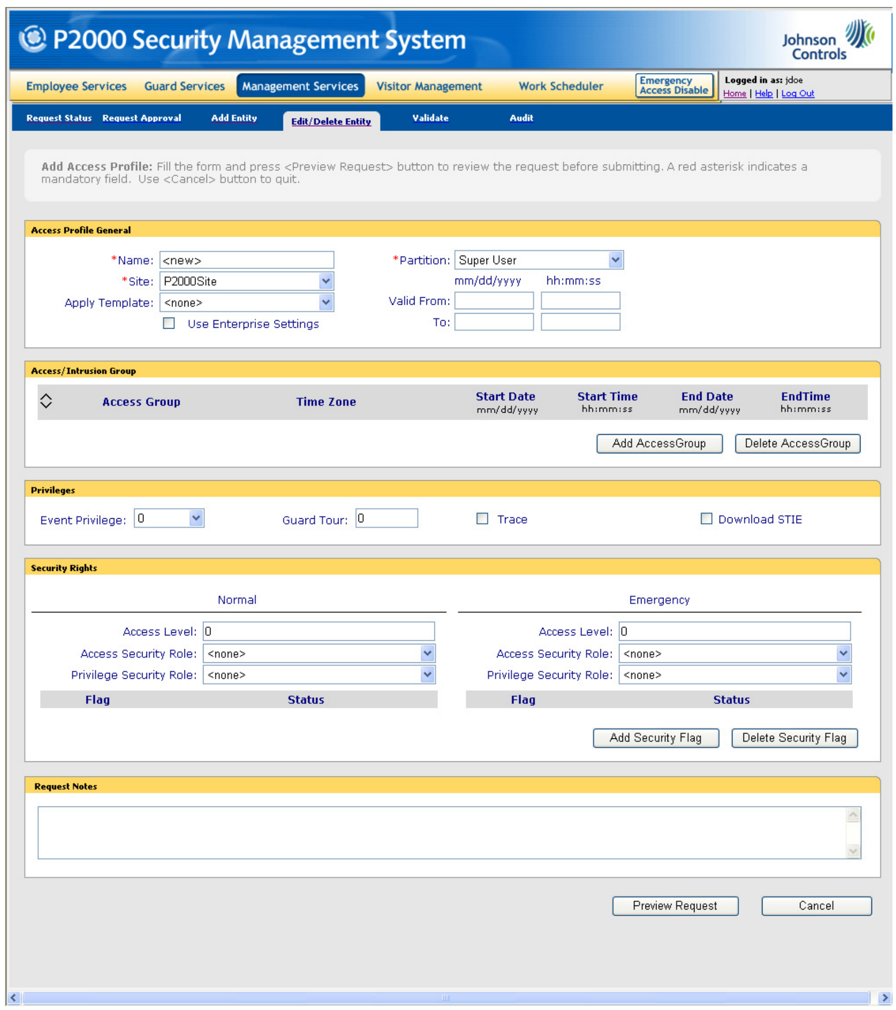
Adding, Editing, or Deleting Access Profiles

Access Profiles define the access rights of an entity. You can define access profiles for a person or asset, and then associate their identifiers with the access profile. If an entity loses an identifier, the administrator will not be required to define new access rights, but associate the replacement identifier with the defined access profile.

Multiple access profiles can be associated with one entity, and one access profile can be applied to multiple identifiers.

➤ To add an access profile:

1. Locate an entity for whom you wish to add an access profile. See “Locating an Entity to Edit or Delete” on page 2-41.
2. On the Entity Search Results page, click **Edit** next to the name of the entity for whom you will add an access profile. The Edit Entity page appears.
3. Click the **Add Access Profile** link on the top of the page. The Add Access Profile page opens.



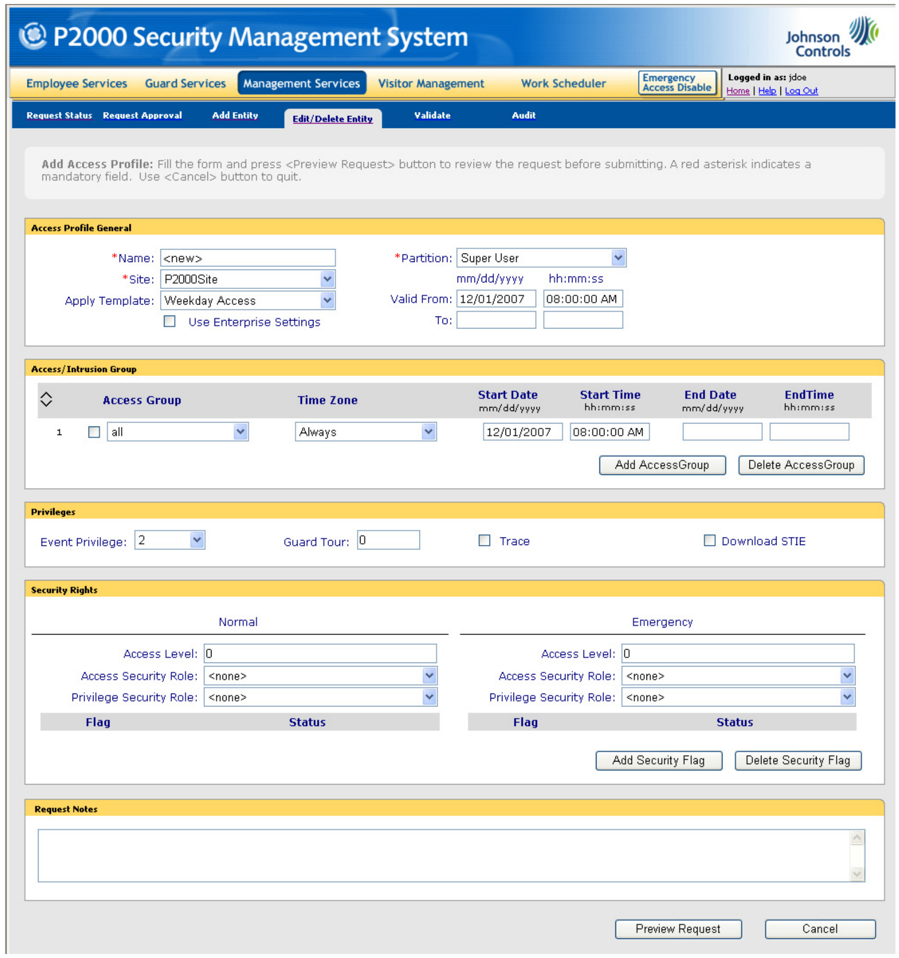
4. Enter access profile information on the Add Access Profile page. See "Managing Entity Access Profile Data" on page 2-59 for detailed information about the fields on this page.
5. Enter any **Request Notes**, if applicable. These notes are not saved with the entity record; they simply provide additional information about the request for persons approving or validating the request.
6. Click **Preview Request**.
7. Perform one of the following actions:
   - Click **Submit Request** if you are satisfied with the request and you are ready to submit it for processing.
   - Click **Modify Request** if modifications are still needed prior to submittal.
   - Click **Cancel** to cancel the request. Clicking this button does not save the request data and will open the Edit/Delete Entity page.

➤ To edit an access profile:

1. Locate an entity for whom you wish to edit an access profile. See "Locating an Entity to Edit or Delete" on page 2-41.
2. On the Entity Search Results page, click **Edit** next to the name of the entity for whom you will edit an access profile. The Edit Entity page appears.

   Existing access profiles are listed in the Entity Editing Choices box at the bottom of the page.

3. Click the access profile you wish to edit. The Edit Access Profile page appears.



4. Edit access profile information on the Edit Access Profile page. See “Managing Entity Access Profile Data” on page 2-59 for detailed information about the fields on this page.
5. Enter any **Request Notes**, if applicable. These notes are not saved with the entity record; they simply provide additional information about the request for persons approving or validating the request.
6. Click **Preview Request**.
7. Perform one of the following actions:
   - Click **Submit Request** if you are satisfied with the request and you are ready to submit it for processing.
   - Click **Modify Request** if modifications are still needed prior to submittal.
   - Click **Cancel** to cancel the request. Clicking this button does not save the request data and will open the Edit/Delete Entity page.

➤ To delete an access profile:

1. Locate an entity for whom you wish to delete an access profile. See “Locating an Entity to Edit or Delete” on page 2-41.
2. On the Entity Search Results page, click **Edit** next to the name of the entity for whom you will delete an access profile. The Edit Entity page appears.

   Existing access profiles are listed in the Entity Editing Choices box at the bottom of the page.
3. Click the access profile you wish to delete. The Edit Access Profile page appears.
4. Enter any **Request Notes**, if applicable. These notes are not saved with the entity record; they simply provide additional information about the request for persons approving or validating the request.
5. Click **Delete**.
6. Perform one of the following actions:
   - Click **Submit Request** if you are satisfied with the request and you are ready to submit it for processing.
   - Click **Modify Request** if modifications are still needed prior to submittal.
   - Click **Cancel** to cancel the request.

Managing Entity Access Profile Data

The Access Profile page consists of numerous functions associated with assigning and defining access profile data for an entity. The data is divided into the following categories:

- Access Profile General
- Access/Intrusion Group
- Privileges
- Security Rights
- Action Interlocks (BACnet option only)

Access Profile General

Name – Enter a descriptive name for this access profile. Names must be unique within each entity. This is a required field.

Site – Select the site associated with the access profile. This is a required field.

Apply Template – If a large number of entities will use access profiles with the same options, you can set all these options at once by applying an Access Profile Template. The Access Profile Template contains preset access options, access groups, time zones, etc. All entities that use the same Access Profile Template will use the same options and you can edit the options individually after the template is applied to suite the needs of individual entities; however, if you re-select the template, the settings will again mirror the access template options.

NOTE

Access Profile Templates must first be created in P2000 before they are available in the Apply Template drop-down list. For more information, refer to the P2000AE Software User Manual.

If you wish to override the settings applied from the Access Profile Template, edit the data in the following boxes;

- Access/Intrusion Group
- Privileges
- Security Rights

Use Enterprise Settings – Applies the access profile settings from the Enterprise site. Valid only if your facility has purchased the Enterprise option.

Partition – If this is a partitioned system, select the Partition in which this access profile will be active.

Valid From – Enter the date and time that the access profile becomes active. All identifiers using this access profile will be activated on this date and time.

Valid To – Enter the date and time this access profile will be automatically voided. All identifiers using this access profile will be voided on this date and time.

Access/Intrusion Group

Use this box to assign one or more Access/Intrusion Groups and corresponding Time Zones to this access profile. You can assign an unlimited number of access/intrusion groups, but P2000 will only download up to 100 groups if using CK722 panels; up to eight access groups if using CK720/CK705 panels; and up to two access groups if using S321 panels.

NOTE

S321 panels are not supported in this release.

➤ To assign an access/intrusion group:

1. In the Access/Intrusion Group box, click **Add Access Group**.

   The left-most column displays the number automatically assigned to the entry. This number indicates the sequence order in which the access/intrusion group will be downloaded to the panel.

NOTE

If you wish to insert a group between two existing groups, select the check box next to the group you wish to move and click the up/down arrow in the column header.

2. Under the **Access Group** column, select the Access Group you wish to assign to this access profile.
3. Under the **Time Zone** column, select the Time Zone that will be assigned to the selected access/intrusion group.
4. If you wish to define a temporary access period for the selected group, under **Start Date** and **Start Time**, enter the date and time when permission for access will be granted. If no date and time is entered, access will be allowed immediately.
5. Under **End Date** and **End Time**, enter the date and time when permission for access will be denied.

NOTE

For example, if the reader doors included in the Access Group normally grant access from 8:00 A.M. to 5:00 P.M., you can set up temporary access on a selected date and time period that will grant the entity permission for limited access within the normal time zone. This feature is performed by the Smart Download service and therefore, you can use it only when Smart Download is running. Refer to the P2000AE Software User Manual for information on the Smart Download feature.

Enter the date in the following format:

mm/dd/yyyy
mm = month, dd = day, yyyy = year
Example: 08/22/2007

Enter the time in the following format:

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

To remove an access/intrusion group, select the check box next to the group you wish to remove and click **Delete Access Group**.

Privileges

Event Privilege – Every access badge identifier has an event privilege level, ranging from 0 to 7, with zero as the lowest level. If an entity's badge is to initiate a card event, his/her event privilege level must be equal to or greater than the privilege level defined in the Panel Card Event dialog box.

Guard Tour – This field is used if you have purchased the Guard Tour option. Enter a priority number from 1 (lowest) to 99. This number determines which tours the selected guard can perform. Only tour badges with equal to or greater than this priority can perform a tour.

Trace – If enabled, all identifier transactions for the entity 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 (P2000 host software). Refer to the *P2000AE Software User Manual* for details.

Download STIE – This option applies only to panels using STI-E terminal interfaces. If selected, the badge identifier 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.

Security Rights

Security rights determine whether or not an access request made by the entity will be granted or denied. The panels will make the access decision based on the rights assigned to the entity. This box allows you to define the access rights of an entity under normal and under emergency circumstances. In emergency situations, the system will switch the entity's normal access privilege to a set of alternative privileges without having to change the entity's rights, which may be time consuming during an emergency.

Access is granted or denied based on access levels and/or security roles.

Access Levels

Normal Access Level – Enter a normal access level from 0 (lowest) to 99. To obtain access at a door, this number must be equal to or greater than the Security Level set up for the terminal. If the Security Level at the terminal is raised, entities will be denied access, unless the access profile has the Executive privilege defined. Normal Access Level is considered an alternative access mode and is available only for CK722 controllers.

Emergency Access Level – Enter an emergency access level from 0 (lowest) to 99. To obtain access at a door, this number must be equal to or greater than the Security Level set up for the terminal. If the Security Level at the terminal is raised, entities will be denied access, unless the access profile has the Executive privilege defined. Emergency Access Level control provides a rapid method of restricting access in case of an emergency.

Security Roles

Entities can be assigned through their access profiles, two sets of security roles, one set for standard (Normal) operation and one set for elevated security (Emergency) operation.

Normal security roles are defined for normal daily access. Emergency security roles are defined for temporary emergency situations. When an emergency is declared, the selected Emergency security roles become active and are used instead of the Normal roles.

To assign Security Roles through this access profile, select an Access or Privilege Security Role from the associated drop-down lists.

Access Security Role – Select an Access Security Role from the drop-down list. Select one for Normal and, if you wish, one for Emergency operation.

Privilege Security Role – Select a Privilege Security Role from the drop-down list. Select one for Normal and, if you wish, one for Emergency operation.

Security Flags – You can define security flags that override roles defined in the Access and Privilege security roles.

➤ To add a security flag:

1. Click **Add Security Flag**.
2. From the **Flag** drop-down list, select the flag you wish to override.
3. From the **Status** drop-down list, select whether you wish to Deny or Grant the access based on the flag selected.

   To delete a security flag, select the check box next to the flag you wish to delete and click **Delete Security Flag**.

Action Interlocks

Action Interlocks initiate actions in BACnet devices. A typical use of an Action Interlock includes turning on lights and air conditioning at a person's office that has been granted access at a door.

Once Action Interlocks are configured in P2000, you may assign them to the access profile. When an access profile is assigned to an identifier, the object property defined in the Action Interlock will be written with the value associated with the badge identifier. Each badge identifier can be configured to activate up to two Action Interlocks that will be triggered when that badge is granted access.

Action Interlocks are configured from the P2000 host software. Refer to the *P2000AE Software User Manual* for details.

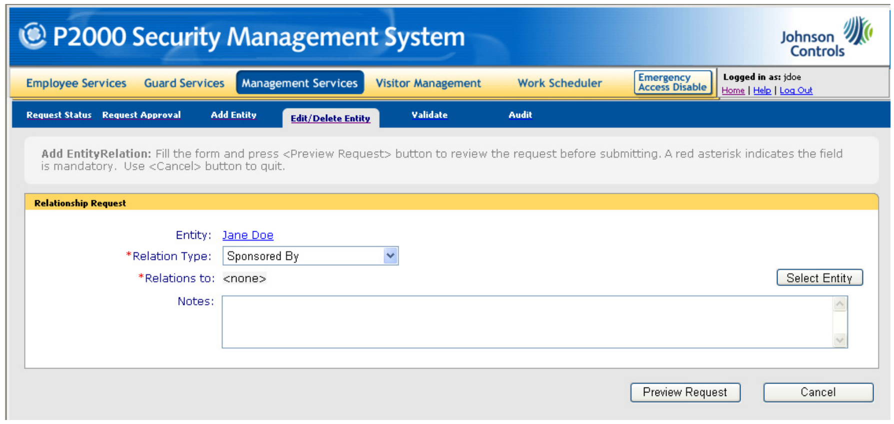
Adding, Editing, or Deleting Relationships

For a description of entity relationships, see "Assigning a Relationship" on page 2-35.

➤ To add a relationship:

1. Locate an entity for whom you wish to add a relationship. See "Locating an Entity to Edit or Delete" on page 2-41.
2. On the Entity Search Results page, click **Edit** next to the name of the entity for whom you will add a relationship. The Edit Entity page appears.

3. Click the **Add Relationship** link on the top of the page. The Add Relationship page opens.



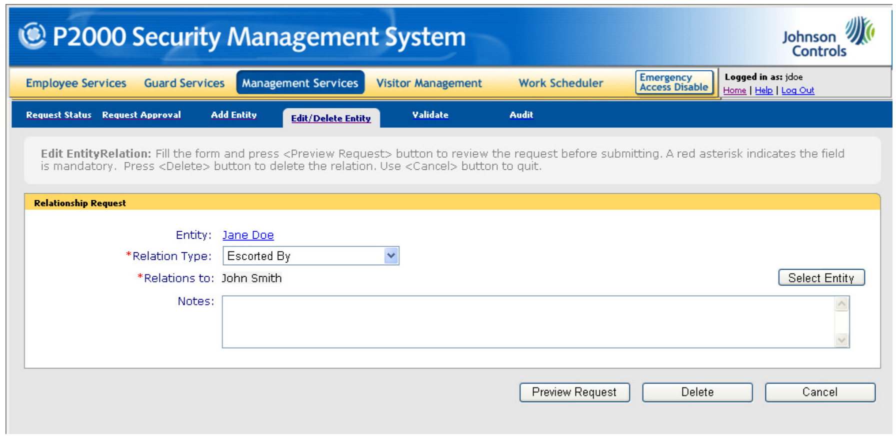
4. Select a **Relationship Type**.
5. Depending on the relationship type selected, assign an entity (or entities) or an entity group using the **Relations To** field.
6. Enter any **Request Notes**, if applicable. These notes are not saved with the entity record; they simply provide additional information about the request for persons approving or validating the request.
7. Click **Preview Request**.
8. Perform one of the following actions:
   - Click **Submit Request** if you are satisfied with the request and you are ready to submit it for processing.
   - Click **Modify Request** if modifications are still needed prior to submittal.
   - Click **Cancel** to cancel the request. Clicking this button does not save the request data and will open the Edit/Delete Entity page.

➤ To edit a relationship:

1. Locate an entity for whom you wish to edit a relationship. See “Locating an Entity to Edit or Delete” on page 2-41.
2. On the Entity Search Results page, click **Edit** next to the name of the entity for whom you will edit a relationship. The Edit Entity page appears.

   Existing relationships are listed in the Entity Editing Choices box at the bottom of the page.

3. Click the relationship you wish to edit. The Edit Relationship page appears.



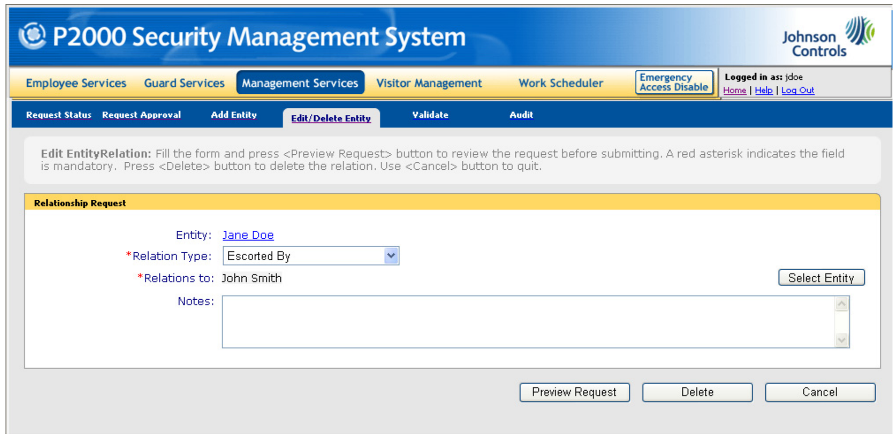
4. Edit relationship information on this page.
5. Enter any **Request Notes**, if applicable. These notes are not saved with the entity record; they simply provide additional information about the request for persons approving or validating the request.
6. Click **Preview Request**.
7. Perform one of the following actions:
   - Click **Submit Request** if you are satisfied with the request and you are ready to submit it for processing.
   - Click **Modify Request** if modifications are still needed prior to submittal.
   - Click **Cancel** to cancel the request. Clicking this button does not save the request data and will open the Edit/Delete Entity page.

➤ To delete a relationship:

1. Locate an entity for whom you wish to delete a relationship. See “Locating an Entity to Edit or Delete” on page 2-41.
2. On the Entity Search Results page, click **Edit** next to the name of the entity for whom you will delete a relationship. The Edit Entity page appears.

   Existing relationships are listed in the Entity Editing Choices box at the bottom of the page.

3. Click the relationship you wish to delete. The Edit Relationship page appears.



4. Enter any **Request Notes**, if applicable. These notes are not saved with the entity record; they simply provide additional information about the request for persons approving or validating the request.
5. Click **Delete**.
6. Perform one of the following actions:
   - Click **Submit Request** if you are satisfied with the request and you are ready to submit it for processing.
   - Click **Modify Request** if modifications are still needed prior to submittal.
   - Click **Cancel** to cancel the request.

Validating Requests

During the validation stage, users with proper web access permissions can process (i.e. approve) or reject a request configured for manual processing. Before processing the request, however, the same users may edit the request, if needed. For example, if someone submitted an Add Entity request without a badge identifier number, the user validating the request can add a badge identifier number before processing the request.

If the request is approved, it will be processed and finalized. A rejected request can be edited for re-submittal. Before a request is approved or rejected, the requestor can cancel it.

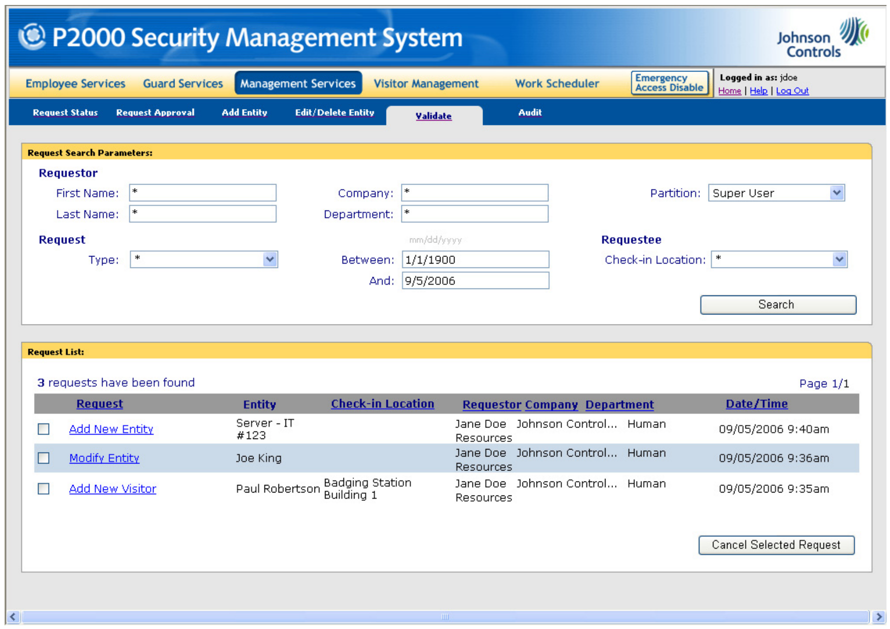
Note

*A **Rejected** request can be edited and resubmitted. A **Canceled** 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 1-12 and “Process States” on page 1-14.

➤ 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**.
4. Under the **Request** column, click the link of the request you wish to validate. The Entity Info page for that request opens.
5. Edit the request, if necessary.
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 Request**.The request is removed from the Validate page and stored in the Request History with a status of “Cancelled.”

Auditing User Actions

P2000 Web Access includes an auditing feature that allows you 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 (e.g Add Entity Group, Edit Entity, Execute Application, etc.).

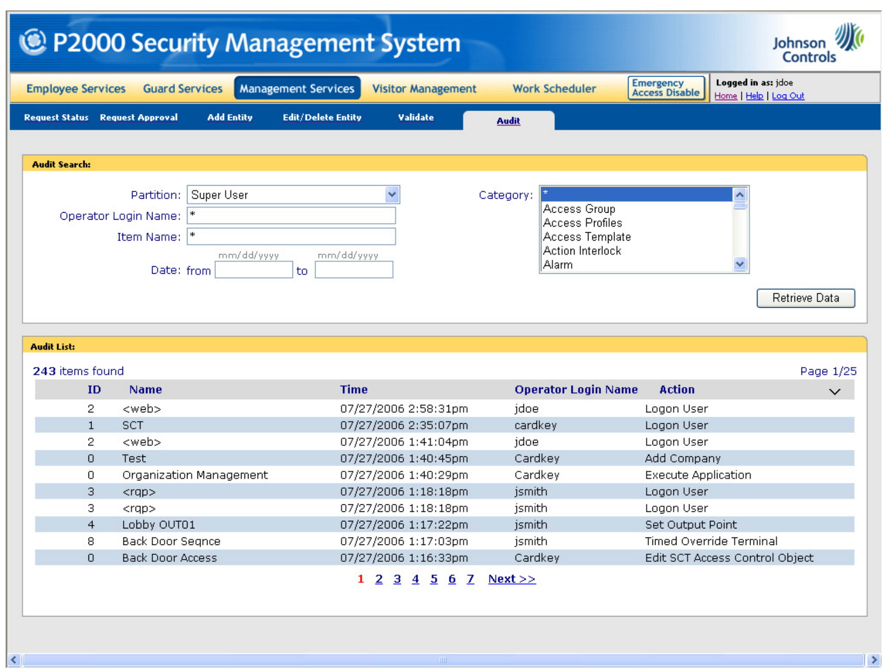
NOTE

The Audit feature does not provide record change tracking capabilities (record retention and persistence). See page 2-69 for information on using the P2000 Record Change Tracking option.

➤ 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 the **<Shift>** or **<Ctrl>** key 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.

Record Change Tracking

The P2000 Record Change Tracking option is an enhanced record tracking and operator auditing system that enables authorized users to view detailed reports of record changes to the P2000 database based on numerous search parameters.

The Record Change Tracking option consists of the following features:

- **Audit Trail**
  This enables the P2000 system to trace actual value changes, allowing the system to provide time-stamped reports to monitor day-to-day operator activity, such as how hardware is controlled, when alarms are acknowledged, or when records are changed.
- **User Authorization**
  The P2000 software limits system access to authorized individuals. Authorized users are identified by their unique combination of user name and password. The passwords for these individuals can be configured to change periodically and have a minimum password length. Additionally, the software disables user access upon multiple invalid login attempts, and provides automatic user logoff after a pre-defined period of user inactivity.
- **Record Validation**
  The Record Change Tracking option provides a tampering tool to detect unauthorized record modifications.
- **Record Retention**
  Through the P2000 software, system administrators can define the parameters to backup and retrieve records in order to ensure the availability of all records for a specified period.
- **Record Persistence**
  All original records are saved in the P2000 database, even if the records are subsequently modified. The P2000 software generates detailed, time-stamped, audit trail reports, assuring that all records changed maintain the original recorded information, and thereby protecting all previous data.
- **Backups**
  Periodic backups are performed to maintain data integrity.

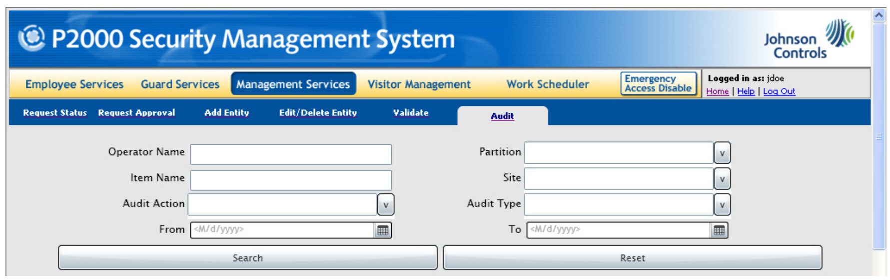
NOTES

- *The Record Change Tracking option is designed to meet the compliance requirements of the Food and Drug Administration (FDA) Title 21, Code of Federal Regulation (CFR) Part 11 standard.*
- *The P2000 Record Change Tracking option must be registered with the P2000 software before you can use it from Web Access. If it is not registered, or you do not have proper user permissions, the Record Change Tracking button on the Home page will not be available.*

- *The Record Change Tracking option from Web Access requires that the Microsoft® Silverlight™ software be installed on the client computer. If your computer does not have the software installed, Web Access will prompt you to install it.*
- *For more information on the Record Change Tracking option, including configuration instructions, refer to the P2000AE Software User Manual.*

➤ To access the Record Change Tracking option:

1. Click the **Home** link in the upper right-hand corner to access the Home page.
2. Click the **Record Change Tracking** button. If you have the Microsoft Silverlight software installed, the Record Change Tracking Search page appears. See “Running a Record Change Tracking Report” on page 2-71.



3. If you are prompted to Install the Microsoft Silverlight software, click the link to begin the installation.

When the File Download dialog box appears, click **Run**. Click **Run** again when prompted.

When the Silverlight Installation window appears, click **Install Now**.

When the installation is completed, click **Close**. Then click your browser’s refresh button.

4. You can now run a record change tracking report.

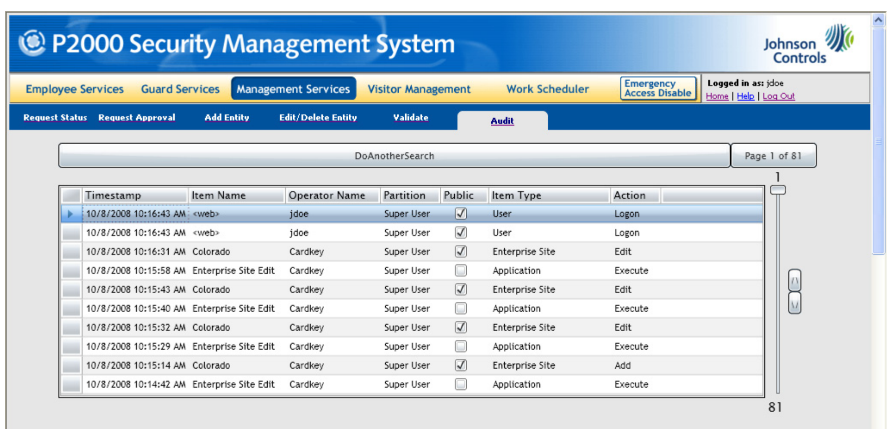
Running a Record Change Tracking Report

The Record Change Tracking Search page enables you to enter various search filters when generating the report. The following filters are available:

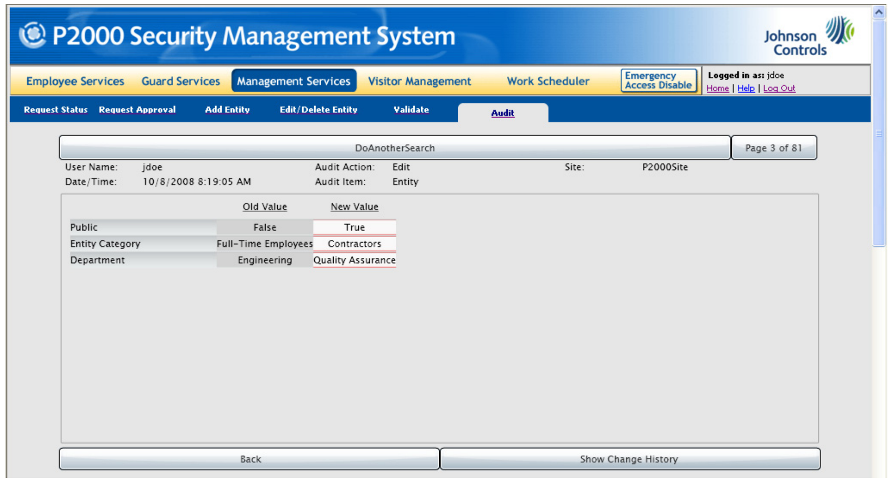
- **Operator Name** – Filters your search based on the operator who performed the action. Enter the User Name assigned to the operator.
- **Item Name** – Filters your search based on the item or record that was modified.
- **Audit Action** – Filters your search based on the type of action performed. For example, the Add option displays all add actions, such as Add Entity.
- **From / To** – Filters your search based on the date or range or dates during which the action(s) occurred.
- **Partition** – Filters your search based on partition assigned to the operator who performed the action(s).
- **Site** – Filters your search based on the Enterprise site associated with the action(s). You may only select a different site if the P2000 Security Management System is configured as an Enterprise system.
- **Audit Type** – Filters your search based on the type of record or item that was modified.

➤ To run a Record Change Tracking report:

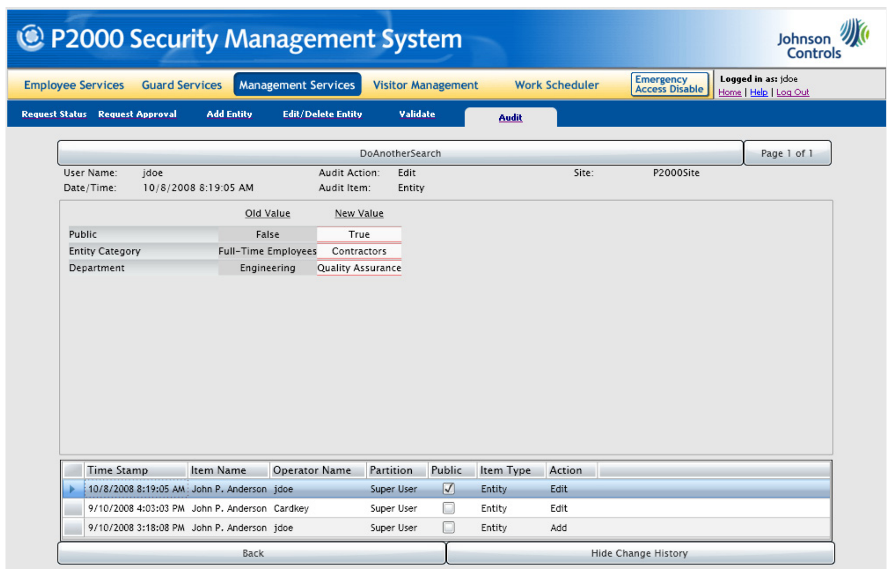
1. On the Record Change Tracking Search page, enter your search filter criteria.
2. Press **Search** to receive the results of your search.



3. Click on the row of a listed audit record to view detailed information.



4. To view the change history of the selected audit record, click **Show Change History**.



5. To view an audit record from the Change History list, click the record.

6. To hide the Change History list, click **Hide Change History**.

   To perform another search, click **DoAnotherSearch**.

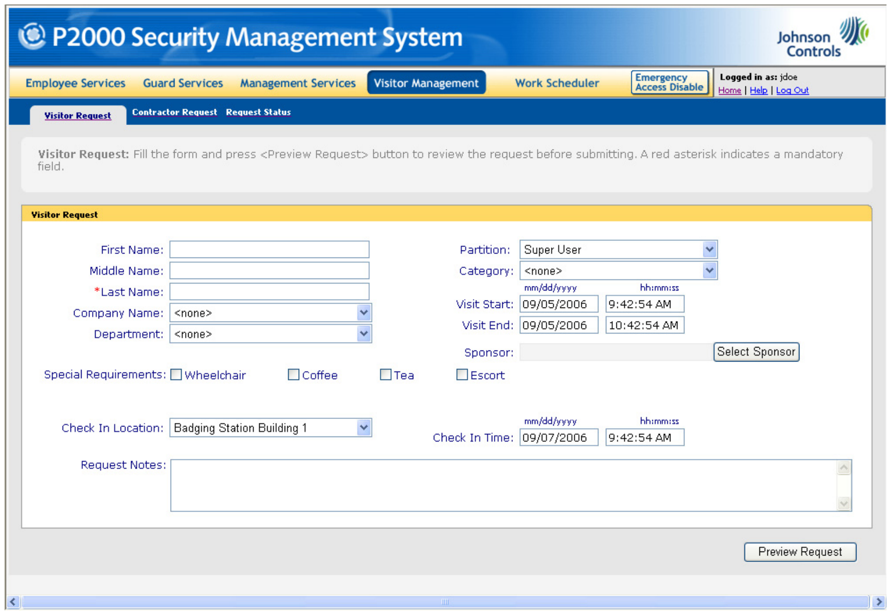
VISITOR MANAGEMENT

Web Access allows you to add a visitor to the P2000 system, so that an identifier can be 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 (e.g. wheelchair, coffee, tea, etc.).

Once a visitor request has been submitted, it is added 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 1-12 for more information on the request process.

➤ To add a visitor to the P2000 database:

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



2. In the **Visitor Request** box, enter the visitor's name in the appropriate fields. The **Last Name** field is required.
3. Enter the visitor's **Company Name** and **Department**, if applicable.
4. Select one or more **Special Requirements** associated with the visitor.
5. If this is a partitioned system, select the **Partition** to which this entity will be assigned. This field will not be visible in a non-partitioned system.
6. From the **Category** drop-down list, select an entity category to assign to the entity.
7. Enter the visit period in the **Visit Start From** and the **Visit End To** fields.

   Enter the date in the following format:

   > **mm/dd/yyyy**
   > mm = month, dd = day, yyyy = year
   > Example: 08/22/2007

   Enter the time in the following format:

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

8. You must enter a sponsor to complete a visitor request. Click the **Sponsor** button and **Select** button next to the entity you wish to assign as the sponsor.
9. If the **Check In Location** field is visible, select the location where the visitor will check in. The badging station location is defined in the P2000 host software (System Configuration>Workstation>Description field).

   If the **Check In Time** field is visible, enter the time when the visitor will check in.

10. Enter any **Request Notes**, if applicable. These notes are not saved with the entity record; they simply provide additional information about the request for persons approving or validating the request.
11. Click **Preview Request**.
12. Perform one of the following actions:
    - Click **Submit Request** if you are satisfied with the request and you are ready to submit it for processing.
    - Click **Modify Request** if modifications are still needed prior to submittal.
    - Click **Cancel** to cancel the request. Clicking this button does not save the request data and will open the Edit/Delete Entity page.

Contractor Requests

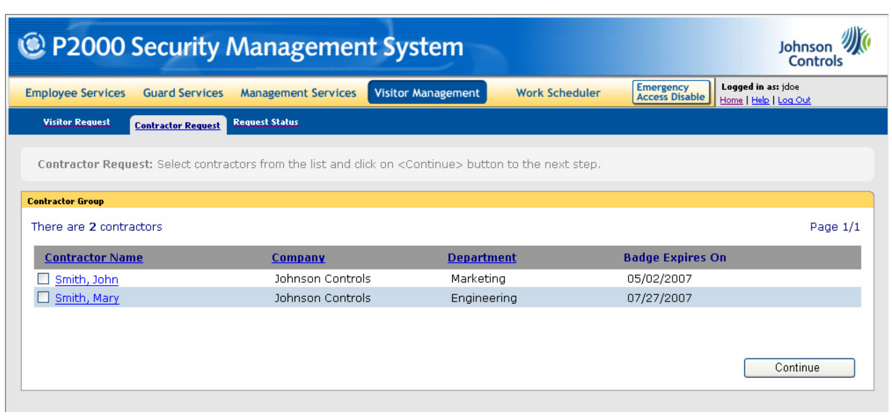
Web Access enables users to send a request to change the validation period of an entity's access profile. Once the request has been submitted, the request is added to the Request Queue. You may cancel your request from the queue, if necessary, but only an authorized person can approve and/or validate it. See "Request Process Flow Chart" on page 1-12 for more information on the request process.

Note

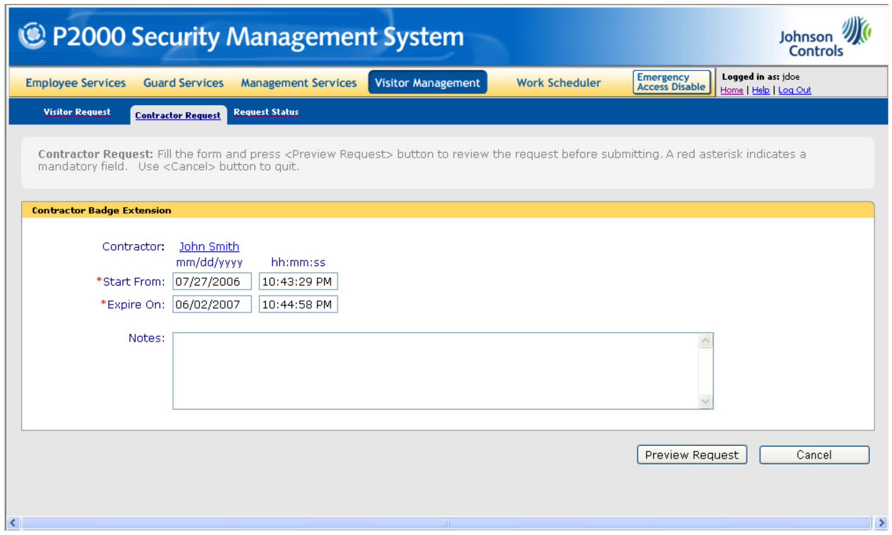
To modify the validation period of an entity's access profile, you must be in the same partition and be a part of the same entity category as the entity.

➤ To change the validation period of an entity's access profile:

1. Click the **Visitor Management** option. The Visitor Request page appears.
2. Click the **Contractor Request** tab to view a list of entities who are in the same partition and are assigned to the same entity category as you.



3. Select the check box next to each entity whose access profile validation period you wish to extend.
4. Click **Continue**. The Contractor Badge Extension page appears.



5. Enter the new validation period in the **Start From** and the **Expire On** date/time fields.

   Enter the date in the following format:

   > **mm/dd/yyyy**
   > mm = month, dd = day, yyyy = year
   > Example: 08/22/2005

   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 request **Notes**, if applicable. These notes are not saved with the entity record; they simply provide additional information about the request for persons approving or validating the request.
7. Click **Preview Request**.
8. Perform one of the following actions:
   - Click **Submit Request** if you are satisfied with the request and you are ready to submit it for processing.
   - Click **Modify Request** if modifications are still needed prior to submittal.
   - Click **Cancel** to cancel the request. Clicking this button does not save the request data and will open the Edit/Delete Entity page.

WORK SCHEDULER

The P200 Work Scheduler feature is a Time and Attendance system designed to record and track an entity's work schedule and attendance record, which can be integrated with a 3rd-party application, such as a payroll system. Using this feature in Web Access, you can define a particular work schedule for an entity, broadcast a message that appears on the Time and Attendance terminal where the entity signs-on, and monitor the entity's Time and Attendance status.

NOTE
For more information on the Work Scheduler feature, including configuration instructions, refer to the P2000AE Software User Manual.

Defining a Work Schedule

You can define a work schedule simply by adding one or more time periods to a day on the calendar for the selected entity. Once you have configured a work schedule, the P2000 system can track when the entity signs in for work and compare it to the current work schedule assigned to that entity for any discrepancies.

The following Work Scheduler tabs allow you to define and view an entity's work schedule:

- **Current** – This tab displays the current work schedule of each entity for the current week. The column listing the schedule of the current day is highlighted in pink. When accessing this tab, the current day always appears in the middle of the week.
- **Weekly** – This tab displays the current week's work schedule starting with the day of the week defined as the schedule start day (determined by the **Schedule start on** field value of the Work Schedule object, which is defined using the P2000 software; refer to the *P2000AE Software User Manual* for more information). Unlike the Current tab, this tab enables you to view the work schedule of a different week by selecting the **Next Week** and **Previous Week** links.
- **Monthly** – This tab provides a month-to-month view of each entity's work schedule. Days with a green sphere icon indicate that the entity has a schedule defined for those days. Days with a dash indicate that the entity does not have a schedule defined on those days.

NOTE
*Web Access lists the entities as **Employee** or **Leased Employee**. A Leased Employee is an entity whose assigned Department matches the name of the P2000 site. All other entities are listed as Employee.*

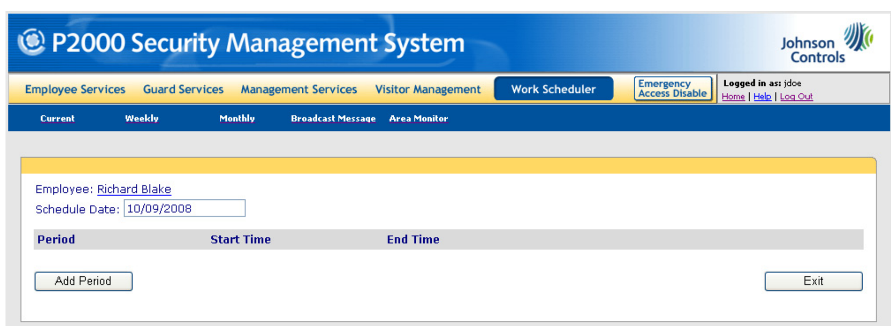
➤ To define a work schedule:

1. Click the **Work Scheduler** option. The Current tab appears.

> ## NOTE
> *The following instructions can also be performed from the Weekly and Monthly tabs.*

2. Select a schedule date for the desired entity.

   The Add Period page appears.



3. Click **Add Period**.
4. Enter the **Start Time** and **End Time** of the time period.

   Enter the time in the following format:

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

   You may also enter the time in the 24-hour format (e.g. 17:00 for 5:00 PM).

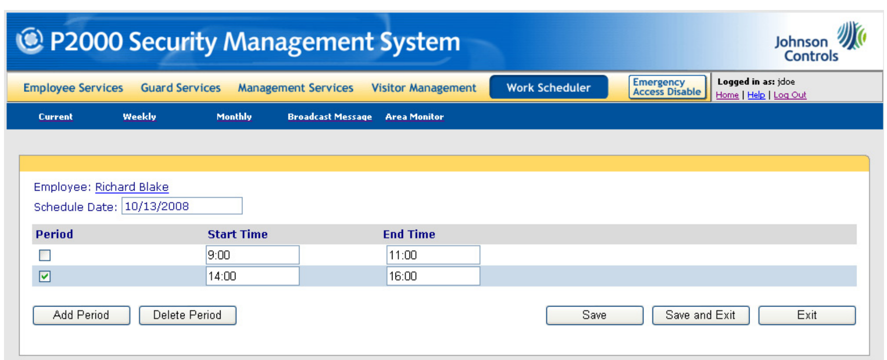
5. Select one of the following options:
   - **Save** – Saves the current time period without exiting the current page. Select this option if you wish to enter another time period.
   - **Save and Exit** – Saves the current time period and exits the current page. Select this option if you do not need to enter another time period.
   - **Exit** – Cancels the current action and exits the current page.
6. If you need to add another time period, repeat steps 3-5.
7. After exiting the page, the defined time periods appear on the Work Schedule calendar, visible on the **Current**, **Weekly**, and **Monthly** tabs.

➤ To edit a work schedule:

1. Click the **Work Scheduler** option. The Current tab appears.
2. Select the schedule date you wish to modify. Select the **Monthly** tab if the desired date does not appear on the Current tab.
3. Enter the new **Start Time** and/or **End Time**.
4. Click **Save** or **Save and Exit**.

➤ To delete a time period:

1. Click the **Work Scheduler** option. The Current tab appears.
2. Select the schedule date that includes the time period you wish to delete. Select the **Monthly** tab if the desired date does not appear on the Current tab.
3. Select the check box(es) next to the period(s) you wish to delete.



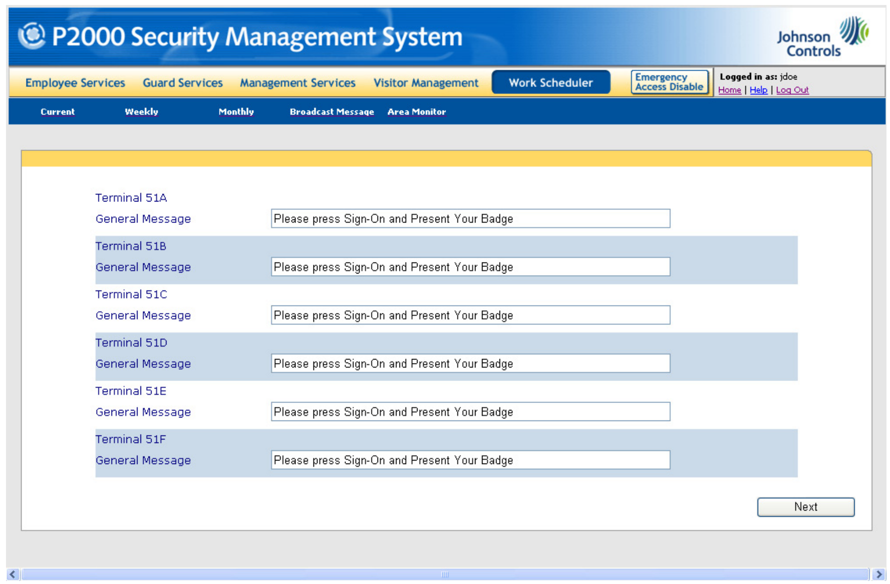
4. Click **Delete Period**.
5. Click **Save** or **Save and Exit**.

Broadcasting a General Message

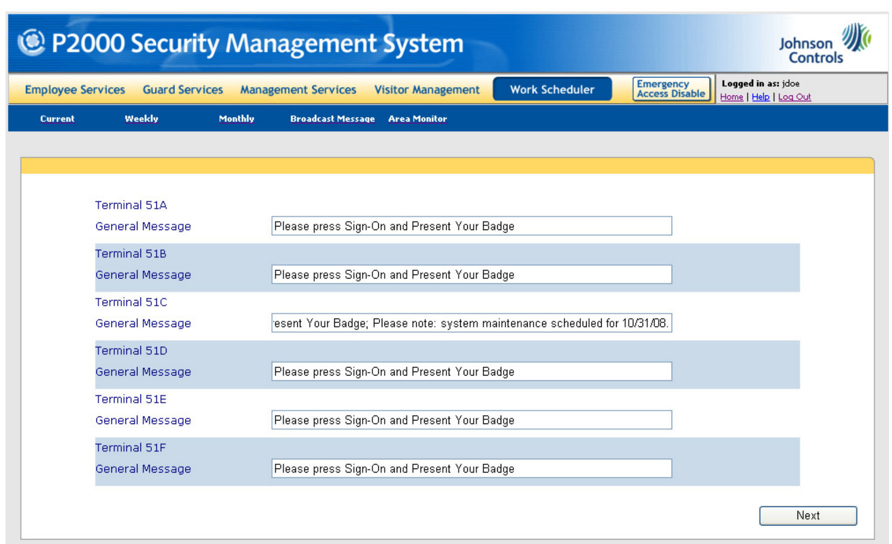
Web Access allows you to modify the general message broadcasted to Time and Attendance terminals.

➤ To modify the general message for one or more Time and Attendance terminals:

1. Click the **Work Scheduler** option. The Current tab appears.
2. Select the **Broadcast Message** tab. The Broadcast Message page appears.



3. Modify the general message for each desired Time and Attendance terminal.



4. Click **Next**.
5. Click **Save**.

Modifying the Employee Message

You may also use Web Access to modify the employee message that appears on the Time and Attendance terminal if the system administrator has configured a UDF for this purpose. See “User-Defined Fields (UDF)” on page 2-35 for information on entering data into UDFs.

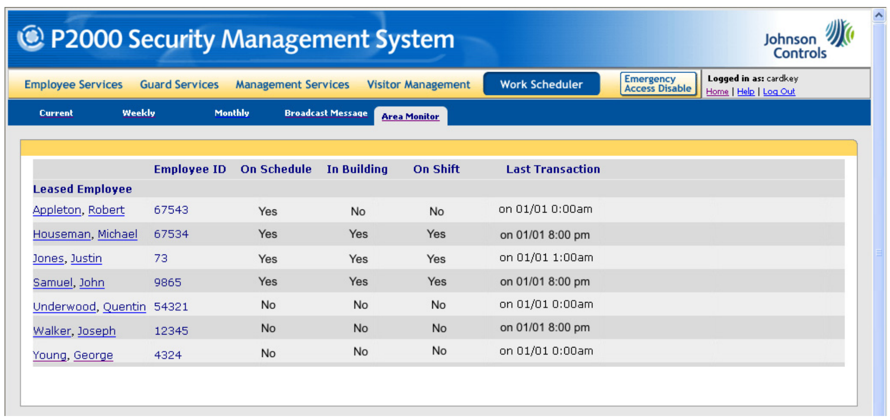
Monitoring an Entity’s Time and Attendance Status

The Area Monitor tab on the Work Scheduler option enables you to view an entity’s current Time and Attendance status such as the whether the entity is scheduled to work for the current day, whether he has presented a valid identifier to enter the building, and whether he has checked in for work according to his schedule.

➤ To view an entity’s Time and Attendance status:

1. Click the **Work Scheduler** option. The Current tab appears.
2. Select the **Area Monitor** tab.

   On this tab, each entity is listed in alphabetical order based on his/her last name.



The following Time and Attendance information is presented:

- **On Schedule** – Indicates whether or not the entity is scheduled to work for the current day according to the schedule defined on the Current, Weekly, and Monthly tabs.
- **In Building** – Indicates whether or not the entity has presented a valid identifier to enter the building on the current day.
- **On Shift** – Indicates whether or not the entity is currently checked in for work according to the Time and Attendance schedule defined on the Current, Weekly, and Monthly tabs.
- **Last Transaction** – Indicates the date and time the entity last presented an identifier to one of the readers.

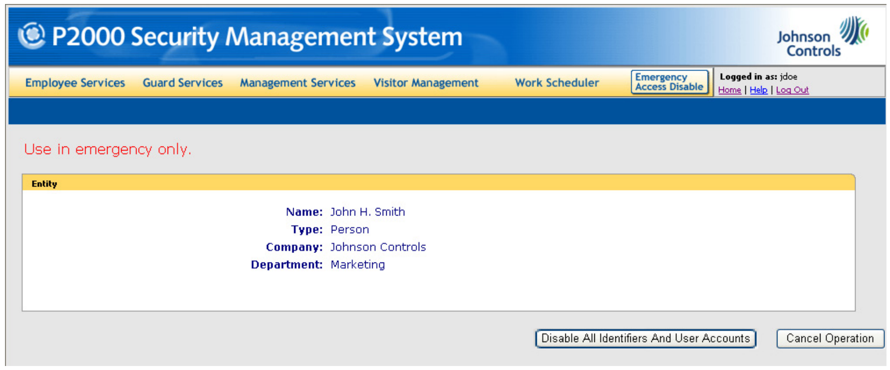
EMERGENCY ACCESS DISABLE

This feature enables you to immediately disable the account of a single entity, which disables all of the entity's identifiers and his/her ability to log into Web Access. A P2000 alarm will also be generated. This feature can be used in various emergency situations. For example, if a worker has threatened someone in the company, his/her account can be disabled to prevent him/her from accessing the company building or complex.

➤ To use the Emergency Access Disable feature:

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

2. Use the **Entity Parameters** fields and **Search** button to quickly locate a specific entity, or refer to the Entity Search Results list, which will automatically display all entities.
3. Click the **Select** button next to the entity account you wish to disable. The Disable Entity page appears.



4. Click the **Disable All Identifiers And User Accounts** button.

   The words "Operation Completed Successfully" appears at the left-side of the page. You have successfully disabled the entity account.

NOTE

*Until you click the **Disable All Identifiers and User Accounts** button, you have the option to cancel the operation by clicking **Cancel Operation**.*

User Preferences

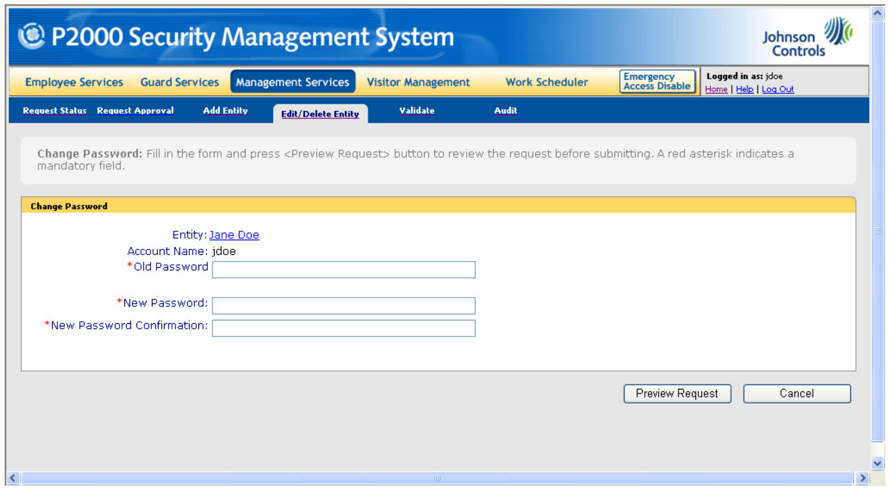
The Web Access Welcome page has user preference links that allow you to configure your default login preferences. You may change the following for your account:

- Login password
- Partition
- Web Access user interface style

➤ To change your login password:

1. From the Welcome page, click the **Change Password** link inside the User Preferences box.

The Change Password page appears.



2. In the **Old Password** field, enter the current password.
3. In the **Password** field, enter the new password.
4. In the **New Password Confirmation** field, enter the new password again.
5. Click **Preview Request**.
6. Perform one of the following actions:
   - Click **Submit Request** if you are satisfied with the request and you are ready to submit it for processing.
   - Click **Modify Request** if modifications are still needed prior to submittal.
   - Click **Cancel** to cancel the request. Clicking this button does not save the request data and will open the Edit/Delete Entity page.

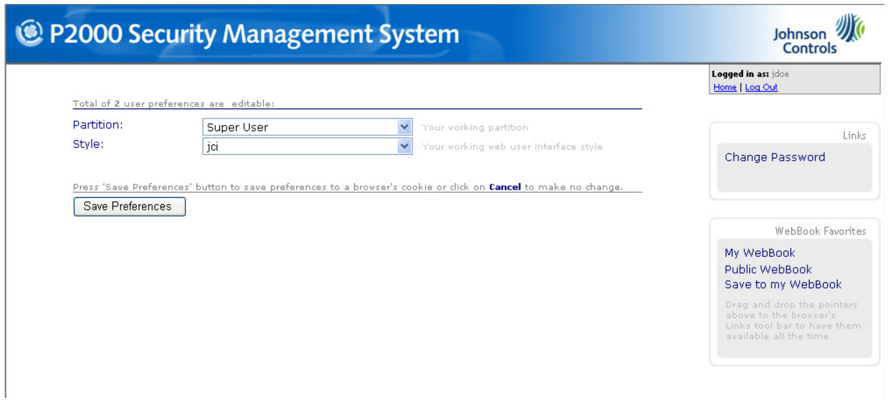
NOTE

Once you change your password, you need to log in again.

➤ To change your partition and/or Web Access user interface style:

1. From the Welcome page, click the **Change Preferences** link inside the User Preferences box.

The Change Preferences page appears.



2. In the **Partition** drop-down list, select a new partition.
3. In the **Style** drop-down list, select a new user interface style.
4. Click **Save Preferences** to save your changes, or click **Cancel** to cancel your changes.

Using WebBook Favorites

Use the WebBook Favorites feature to bookmark the Web Access pages you use most often and save them in a central location. When you wish to access a saved page quickly, you simply open your WebBook and click the link that represents the page you wish to access. In addition, using the Web Access WebBook has some distinct advantages to simply using your browser's Favorites feature, such as:

- **Creating Tags**
  Tags are keywords associated with a particular WebBook page and enable you to group multiple WebBook pages based on a particular tag. Once you create a tag, all Favorites defined with that tag will be listed under the tag on the Tags tab in your WebBook. For example, if you add the Add Entity and Edit/Delete Entity pages to your WebBook and assign the tag "Entity" to each page, these two pages are grouped together on the Tags tab under the "Entity" tag item.
- **Sharing WebBook Favorites**
  You may set up a sharing community and view favorite pages saved by other Web Access users or allow them to view pages you have saved.
- **Favorites Accessible from Multiple Computers**
  When saving favorite Web Access pages using a browser's Favorites feature, they can only be selected from the same computer from which they were saved. However, because the Web Access WebBook is saved in the P2000 database, WebBook favorites can be selected from any computer.

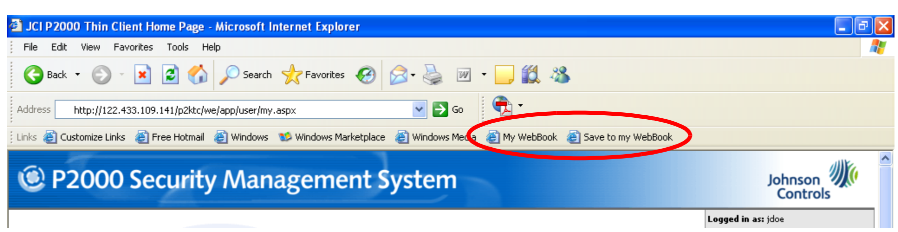
Setting Up WebBook Favorites

Setting up WebBook Favorites is a simple drag-and-drop operation on the Web Access Welcome page. Once you set up the WebBook feature, your WebBook links will be available on your browser's Links toolbar.

➤ To set up WebBook Favorites:

1. Launch Web Access and log in. The Welcome page opens.

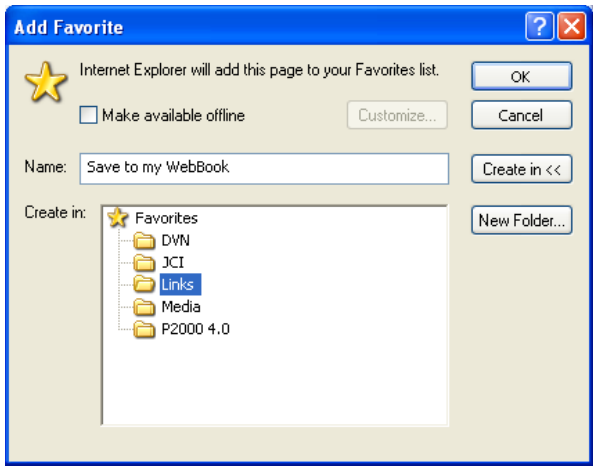
2. Verify that your Links toolbar is selected to display in your web browser. For example, in Microsoft® Internet Explorer, right-click on the toolbar and select **Links**.
3. In the WebBook Favorites box on the right of the page, left-click and drag the **My WebBook** link to the Links toolbar.
4. In the WebBook Favorites box on the right of the page, left-click and drag the **Save to my WebBook** link to the Links Toolbar. The links are added to the toolbar.



NOTE

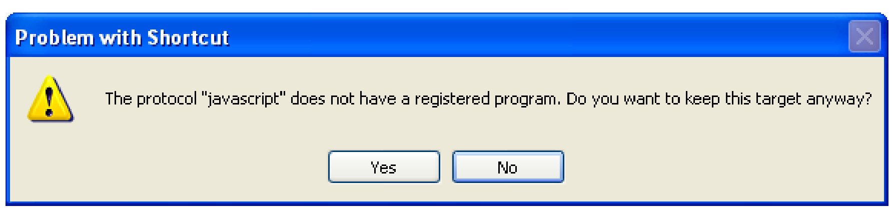
Your Microsoft® Internet Explorer security settings may not allow you to drag-and-drop the Save to my WebBook link because it uses a Java® script. If this is the case with your browser, perform the following instructions:

1. In the WebBook Favorites box, right-click over the **Save to my WebBook** link and select **Copy Shortcut**.
2. From the browser's menu bar, select **Favorites>Add to Favorites**.
3. In the **Name** field, enter `Save to my WebBook`.
4. In the **Create in:** box, select **Links**.



5. Click **OK**.

   The new link will be added to the Links toolbar.
6. Right-click over the **Save to my WebBook** link that you added to the **Links** toolbar and select **Properties**.
7. Paste the URL that you copied onto your clipboard into the **URL** field and click **OK**.
8. If you receive the following message, click **Yes**.



 12/3/08

Saving Web Access Pages to Your WebBook

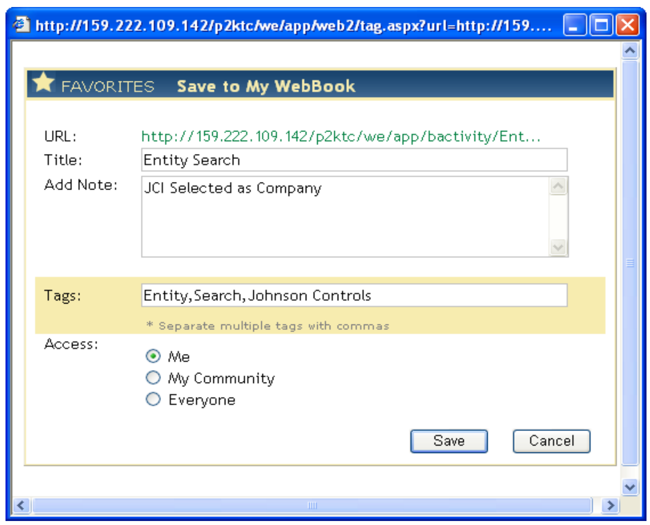
You can save any pages from Web Access to your WebBook. You can make these pages available to yourself only, or you can share them with every Web Access user or a selected community of users. You can also create tags to organize your pages under keyword categories.

Once you save pages to your WebBook, you can use it to quickly locate and manage your saved pages.

➤ To save a Web Access page to your WebBook:

1. In Web Access, access a page you want to bookmark.
2. Click **Save to My WebBook** on your browser's Links toolbar.

   The Favorites dialog box opens with the URL to the saved page displayed at the top.

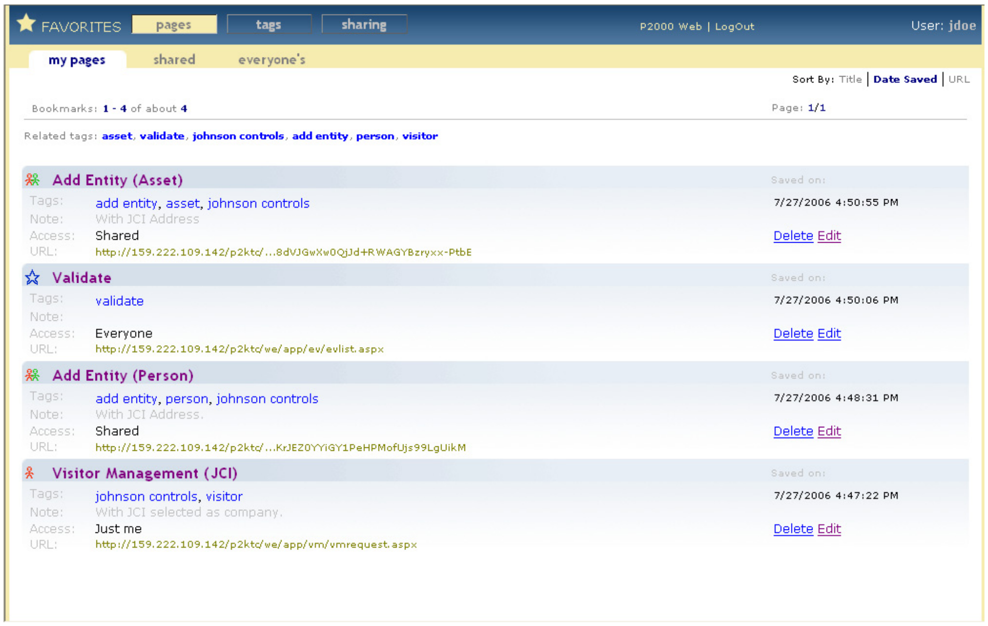


3. In the **Title** field, enter a title for the page. This will identify your saved page when you open your WebBook.
4. Add a note, if needed.
5. In the **Tags** field, enter one or more tags if you intend to create a number of pages that you want organized under a particular keyword.

   If entering multiple tags, separate each tab with a comma. Example: *Entity,Search,Johnson Controls*.
6. Under **Access**, select whether you wish the page to be available to just yourself, your community, or to everyone (i.e. all Web Access users).
7. Select **Save**. The page will now be available in your WebBook.

Using the WebBook

To open your WebBook, simply click **My WebBook** on your browser's Links toolbar.



The WebBook Favorites application is divided into three main tabs:

- **pages** – This tab displays the favorites pages that you saved, including those saved in the Shared and Everyone's categories.
- **tags** – This tab displays a list of tags associated with the saved favorites pages. Clicking a tag allows you to select the saved pages associated with the selected tag.
- **sharing** – This tab allows you to set up a shared community and to view the communities of which you are currently a member.

Pages Tab

The Pages tab has the following subordinate tabs:

- **My Pages** – Displays the details of the pages saved, such as the title, any tags associated with it, and whether it is shared or private. You can also edit or delete a saved page from this tab.
- **Shared** – Displays only those pages you and others in your defined community have defined as "Shared."
- **Everyone's** – Displays all pages saved into the Everyone's category.

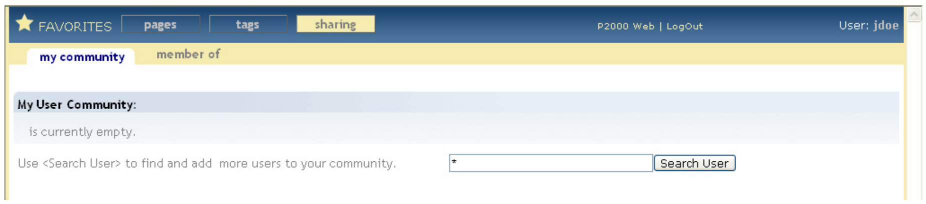
To access a page, simply click on the name. You may also view tag pages by clicking on a particular tag.

Sharing Favorites with Your Community

Once you have created some useful Favorites, you may want to share them with others that perform similar operations. To do this, you create a Community, then either create new or edit existing pages to have Community access.

➤ To create a community:

1. From the WebBook, select **Sharing** at the top of the page. The page opens at the My community tab.



2. To create a community, use the search field and **Search User** button to locate a user you wish to add to your community.
3. From the Search results, select the check box next to each entity whom you wish to add to your community.
4. Click **Add to My Community**.

➤ To remove an entity from your community:

1. From the WebBook, select **Sharing** at the top of the page. The page opens at the My community tab.
2. Under **My User Community**, select the check box next to each entity whom you wish to remove from your community.
3. Click **Remove Selected**.

Chapter 3

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.

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

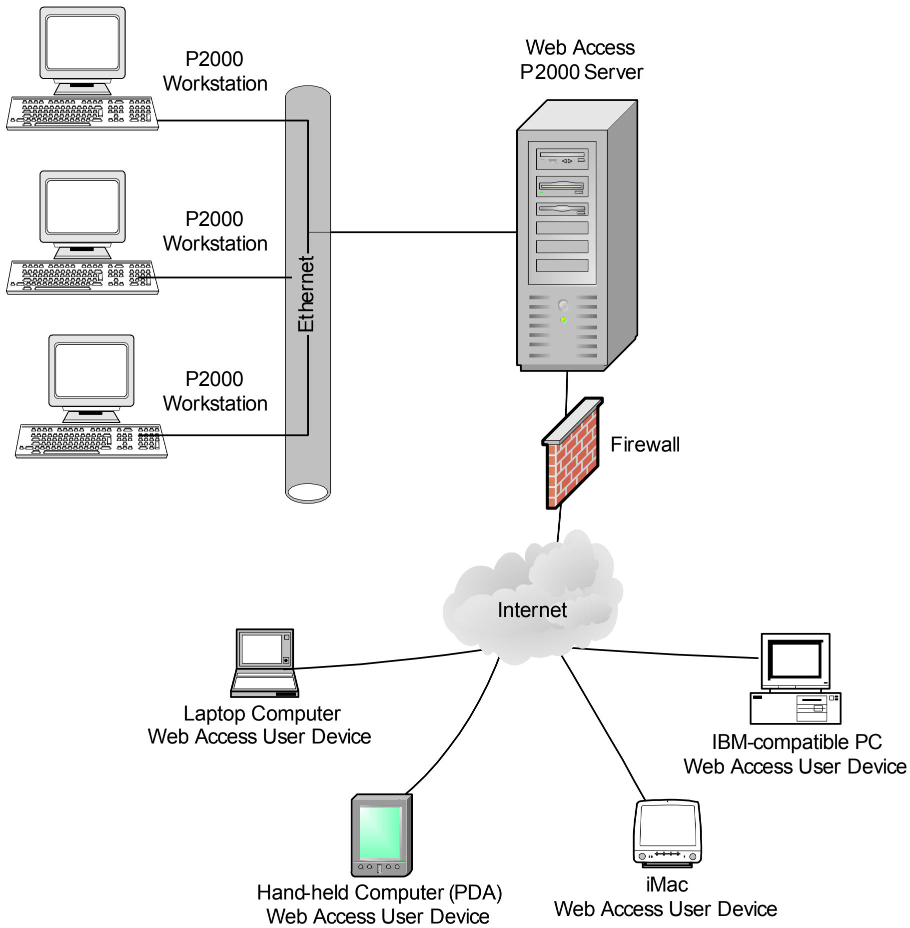


Figure 3-1: Web Access Deployment Option #1 (P2000 Server Only)

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.

The following minimum software must be installed when using the single server Web Access configuration:

- Microsoft Windows Server 2003 R2, Windows Server 2003, or Windows Server 2000
- P2000 Host Prerequisites
- P2000 Host Software Version 4.1 or higher
- P2000 Thin Client Server Software (see "P2000 Web Access Option Software Installation" on page 3-4)
- Microsoft Internet Information Services (IIS) 6.0 or higher

- .NET Framework 1.1
- Digital Certificate for IIS

NOTE
IIS, .NET Framework and the IIS Digital Certificate will automatically be installed during the P2000 Host and Prerequisites installation process.

Once the software is installed, follow the instructions in "Internet Information Services (IIS) Verification" on page 3-7. For information on the P2000 server system requirements, refer to the *P2000AE Server/Workstation Software Installation Manual*.

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

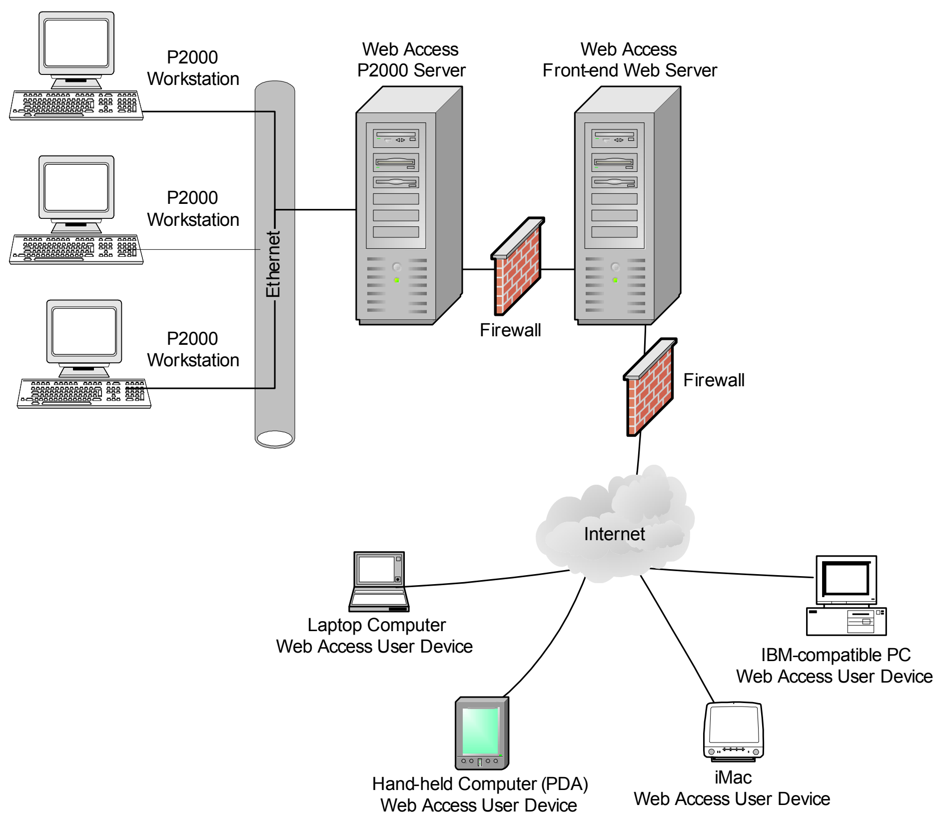


Figure 3-2: Web Access Deployment Option #2 (P2000 Server and Front-end Web Server)

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

The following minimum software must be installed on the P2000 server when using this configuration:

- Microsoft Windows Server 2003 R2, Windows Server 2003, or Windows Server 2000
- P2000 Host Prerequisites
- P2000 Host Software Version 4.1 or higher
- P2000 Thin Client Server Software (see “P2000 Web Access Option Software Installation” on page 3-4)
- Microsoft Internet Information Services (IIS) 6.0 or later
- Digital Certificate for IIS

NOTE

IIS, .NET Framework and the IIS Digital Certificate will automatically be installed during the P2000 Host and Prerequisites installation process.

The web server requires the following:

- Microsoft Windows 2003 Server, Windows 2000 Server, Windows Vista, or Windows XP
- P2000 Thin Client Front End Software (see “P2000 Web Access Option Software Installation” on page 3-4)
- .NET Framework 1.1
- Microsoft® Internet Information Services (IIS) 5.0 or higher
- Digital Certificate for IIS

NOTE

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

For information on the P2000 server system requirements, refer to the *P2000AE Server/Workstation Software Installation Manual*. 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, you must follow the instructions in “Internet Information Services (IIS) Verification” on page 3-7.

P2000 Web Access Option Software Installation

When installing Web Access on the P2000 server, install the front-end *and* back-end components, regardless of the deployment option you are using. When prompted to select the setup type during the installation, select **Typical**.

If you are using a front-end Web server (see page 3-3), install only the front-end components on the Web server. When prompted to select the setup type during the installation, select **Custom**.

NOTE

When installing Web Access on the P2000 server, install it after installing the P2000 server software.

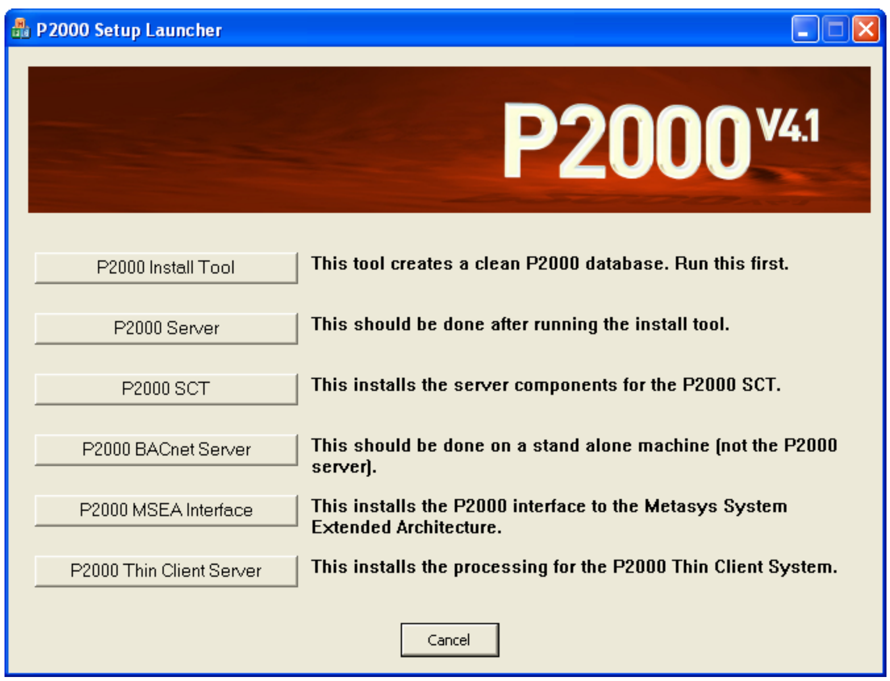
You will need:

- P2000 Server Applications and Services CD

➤ To install the P2000 Thin Client Server software:

1. Insert the CD.

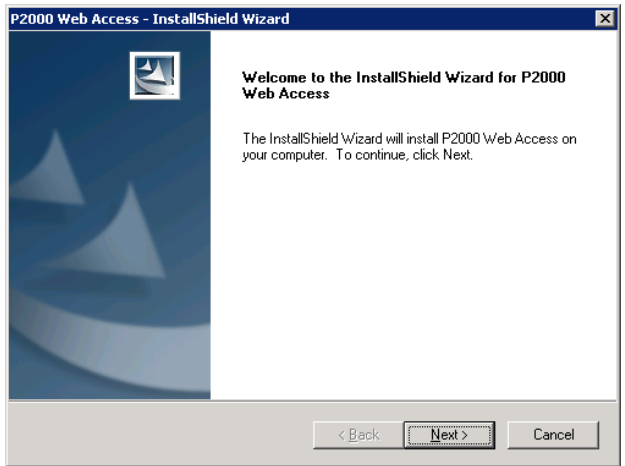
   The P2000 Setup Launcher window appears.

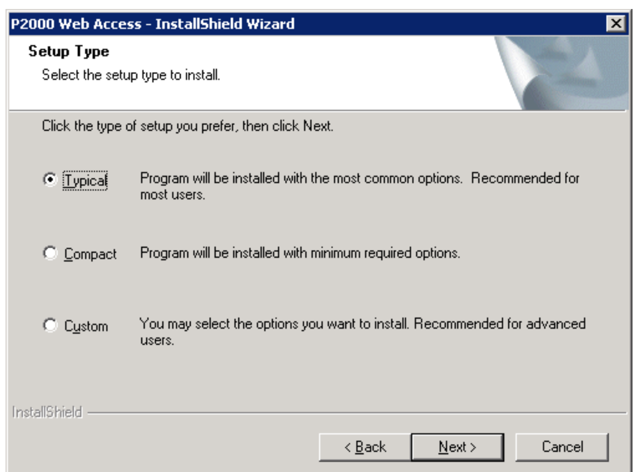
   If this window does not appear, from Windows Explorer, double-click to run the **Setup.exe** file, located at the root level of the CD.

2. On the P2000 Setup Launcher window, click the **P2000 Thin Client Server** button.

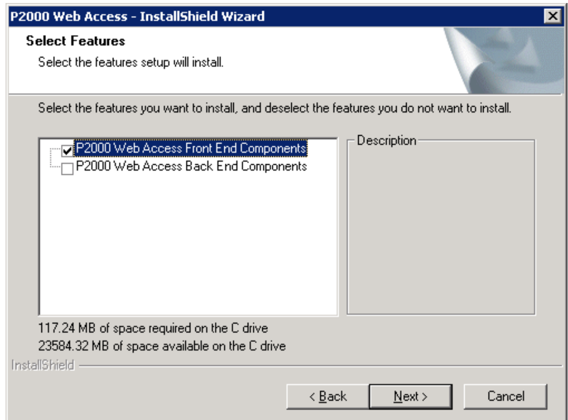
3. The P2000 Web Access Install Wizard starts. Click **Next**.



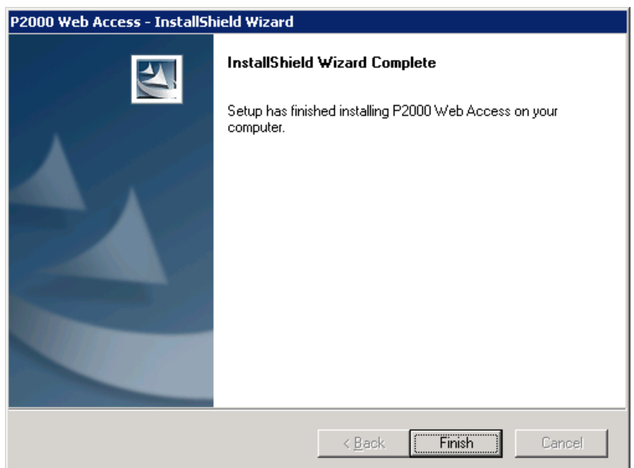
4. On the Setup type screen, select one of the following options:
   - **Typical** – Select if installing Web Access on the P2000 server. Click **Next**. Then skip to step 6.
   - **Custom** – Select if installing Web Access on a front-end Web server and continue with step 5.



5. If you selected the **Custom** setup type, *de*select the **P2000 Web Access Back End Components** check box. Install only the front-end components on the Web server. Click **Next**.



6. On the Start Copying Files screen, click **Next**.
7. When the process is complete, click **Finish**.



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 *P2000AE 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 2003 operating system, IIS and ASP.NET must be installed on the server according to the instructions in the P2000AE Server/Workstation Software Installation Manual. Then follow the instructions in this section to verify IIS was properly installed.

If IIS was not installed and configured correctly, refer to the *P2000AE Server/Workstation Software Installation Manual* for assistance.

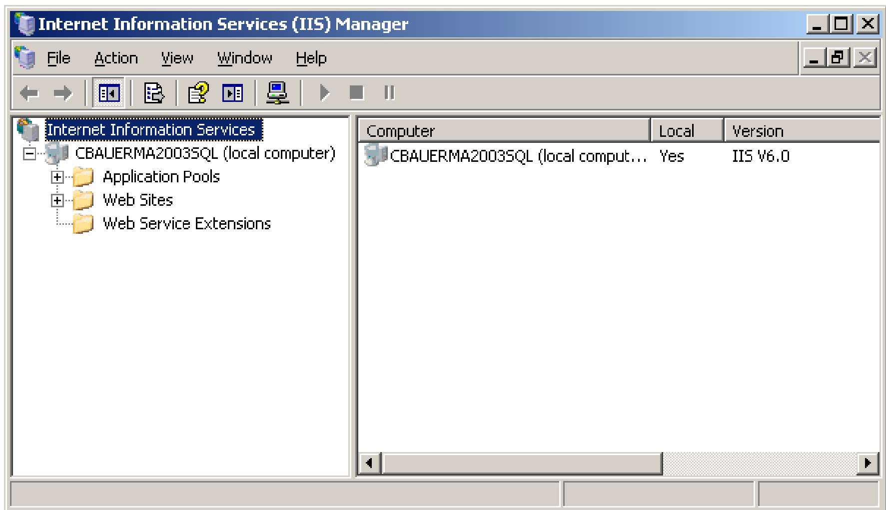
Windows Server 2003

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

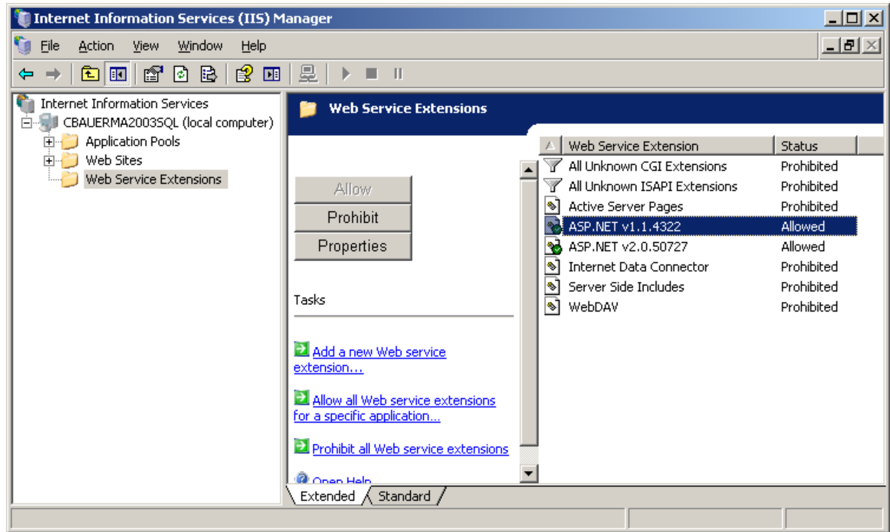
1. From the Windows taskbar, select **Start>Programs>Administrative Tools>Internet Information Services (IIS) Manager**.

   The Internet Information Services (IIS) Manager window appears.

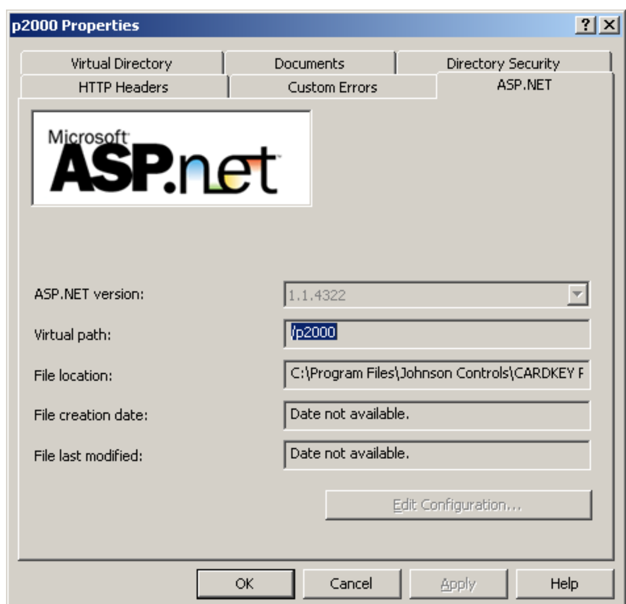
2. In the left pane, expand the directory tree labeled with the computer name.



3. In the left pane, select **Web Service Extensions**.
4. In the right pane, verify that the **ASP.NET v1.1.4322** 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 **1.1.4322**.



If another version is listed, refer to the *P2000AE Server/Workstation Software Installation Manual* for assistance.

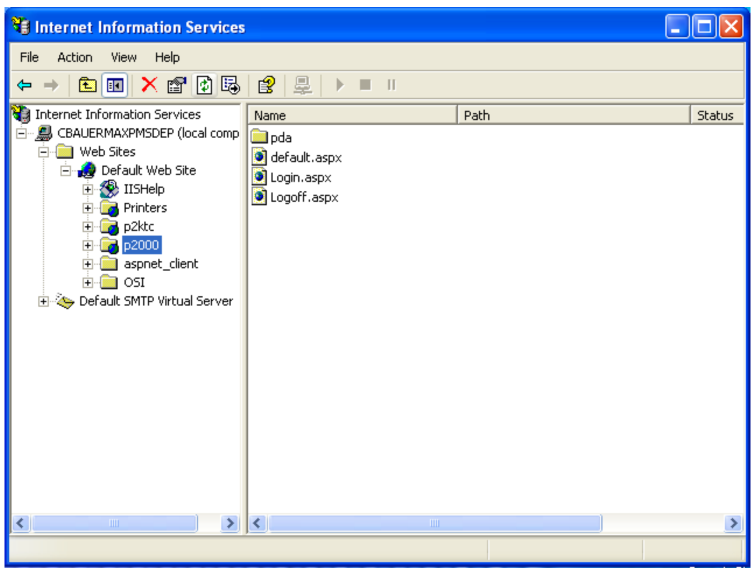
9. If you are using the single server deployment option #1 (no web server), you have completed the steps to deploy Web Access.

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 3-11.

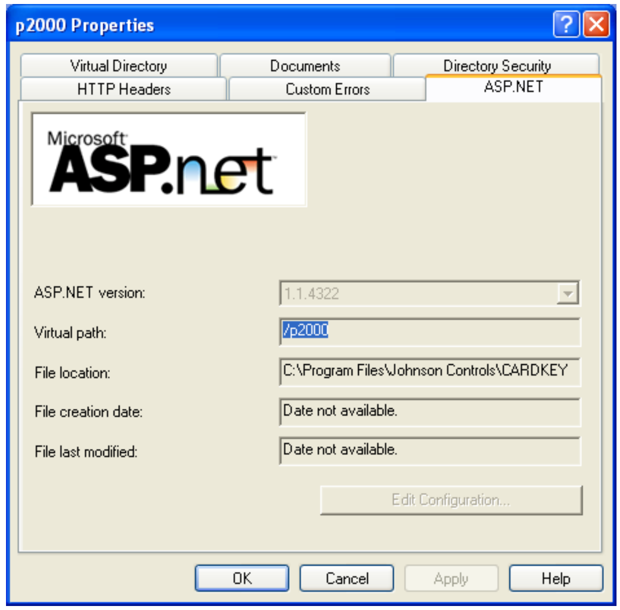
Windows Server 2000 or Windows XP

➤ **To verify the IIS installation and configuration for Windows Server 2000 or Windows XP:**

1. From the Windows taskbar, select **Start>Settings>Control Panel**.
2. Double-click **Administrative Tools**.
3. Double-click **Internet Information Services**. The Internet Information Services window appears.
4. In the left pane, expand the directory tree labeled with the computer name.
5. Expand **Web Sites>Default Web Site** on the directory tree.



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 **1.1.4322**.



If another version is listed, refer to the *P2000AE Server/Workstation Software Installation Manual* for assistance.

9. Click **OK**.
10. Close the Internet Information Services window.
11. 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 the "Configuring the P2000 Server and Front-end Web Server (Front-end Web Server Deployment Option Only)" section.

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 Web Access Runs Properly on the P2000 Server (see page 3-12)
- Configuring the P2000 Server's xe.config File (see page 3-12)
- Configuring the Front-end Web Server's Web.config File (see page 3-13)
- Validating Web Server Operation with Web Access (see page 3-15)

Configuring both the front-end web server's **Web.config** file and the P2000 server's **xe.config** file will enable the two computers to communicate and handle Web Access HTTP and XML requests.

12/3/08

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 1-5.

Configuring the P2000 Server’s xe.config File

This section describes how to edit the P2000 server’s **xe.config** file, which will enable the P2000 server to communicate and transfer data with the front-end web server. Perform the following instructions on the P2000 server:

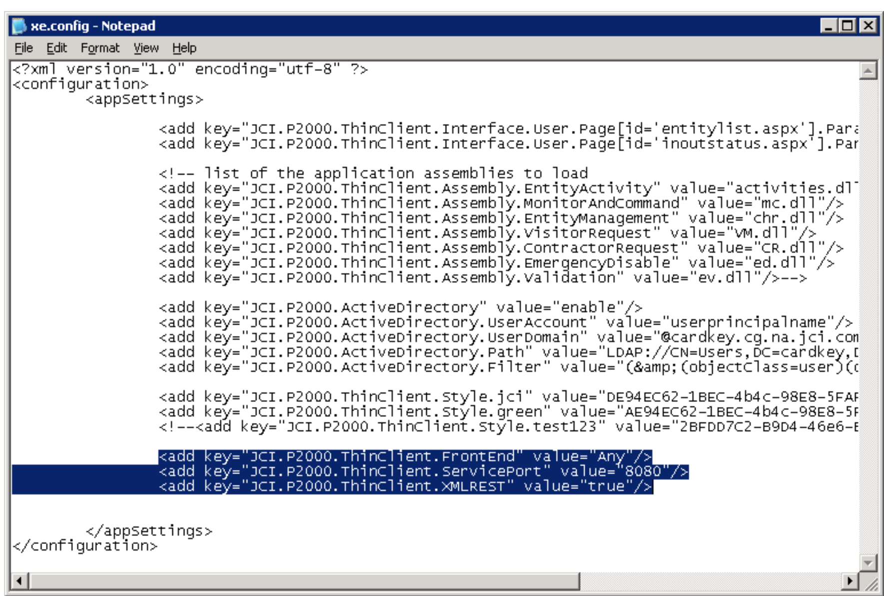
1. Open Windows Explorer.
2. Access the following directory: *Local Disk:\Program Files\Johnson Controls\P2000 Web Access\xerver\xe*
3. Double-click the **xe.config** file and open it in Microsoft Notepad or other text editor.
4. Add the following lines of text if not currently present (see highlighted section in the following screen capture):

NOTE

In the following lines of text, note the bold text for the following steps.

---

*<add key="JCI.P2000.ThinClient.FrontEnd" value="**Any**"/>*
*<add key="JCI.P2000.ThinClient.ServicePort" value="**Service Port Number**"/>*
<add key="JCI.P2000.ThinClient.XMLREST" value="true"/>



5. (Optional) For added security, on the first line of inserted text, replace the word "Any" with the IP address of the front-end web server.

Example:

*<add key="JCI.P2000.ThinClient.FrontEnd" value="**123.222.165.211**"/>*

The P2000 server will only communicate with a front-end web server having the specified IP address. If you specify "Any," the P2000 server will not verify a specific IP address before communicating with the front-end web server.

6. On the second line of inserted text, replace the **Service Port Number** text with a service port number that the P2000 server is not using.

   Example: *<add key="JCI.P2000.ThinClient.ServicePort" value="**8181**"/>*

NOTE

Write down this number, as you will have to enter the same number when configuring the front-end Web server's Web.config file (see "Configuring the Front-end Web Server's Web.config File" on page 3-13.

---

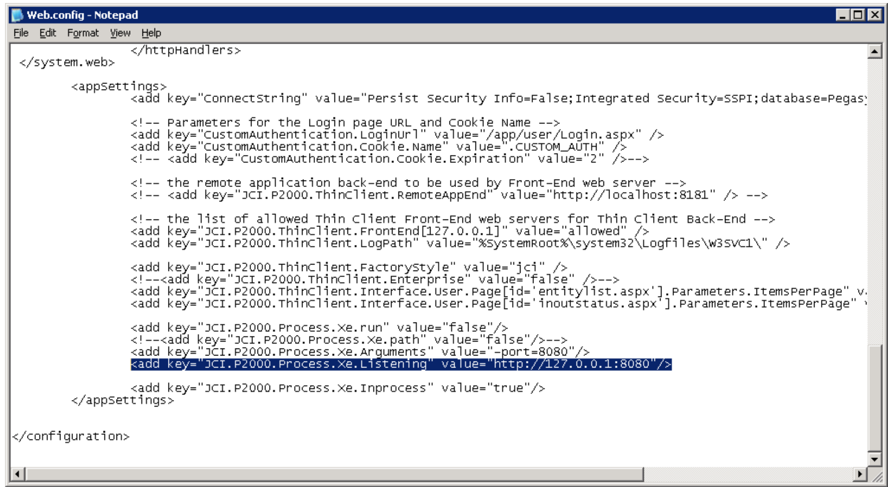
7. On the third line of inserted text, verify that the value is set to "true".
8. Remove any HTML comments from the beginning (<!--) and the end (-->) of the lines of text listed in Step 4.
9. From the menu bar, select **File>Save**.
10. Reboot the P2000 server or restart IIS.

Configuring the Front-end Web Server's Web.config File

This section describes how to edit the front-end Web server's **Web.config** file, which will enable the front-end Web server to communicate with the P2000 server. Perform the following instructions on the front-end Web server.

1. From the front-end Web server, open Windows Explorer.
2. Access the following directory: *Local Disk:\Program Files\Johnson Controls\P2000 Web Access\p2ktc\we*
3. Double-click the **Web.config** file and open it in Microsoft Notepad or other text editor.
4. Scroll to the bottom of the page.
5. Locate the following text:

   <add key="JCI.P2000.Process.Xe.Listening" value="http://127.0.0.1:8080"/>



```
Web.config - Notepad
File  Edit  Format  View  Help
            </httpHandlers>
    </system.web>

        <appSettings>
            <add key="ConnectString" value="Persist Security Info=False;Integrated Security=SSPI;database=Pegas

            <!-- Parameters for the Login page URL and Cookie Name -->
            <add key="CustomAuthentication.LoginUrl" value="/app/user/Login.aspx" />
            <add key="CustomAuthentication.Cookie.Name" value=".CUSTOM_AUTH" />
            <!-- <add key="CustomAuthentication.Cookie.Expiration" value="2" />-->

            <!-- the remote application back-end to be used by Front-End web server -->
            <!-- <add key="JCI.P2000.ThinClient.RemoteAppEnd" value="http://localhost:8181" /> -->

            <!-- the list of allowed Thin Client Front-End web servers for Thin Client Back-End -->
            <add key="JCI.P2000.ThinClient.FrontEnd[127.0.0.1]" value="allowed" />
            <add key="JCI.P2000.ThinClient.LogPath" value="%SystemRoot%\system32\Logfiles\W3SVC1\" />

            <add key="JCI.P2000.ThinClient.FactoryStyle" value="jci" />
            <!--<add key="JCI.P2000.ThinClient.Enterprise" value="false" />-->
            <add key="JCI.P2000.ThinClient.Interface.User.Page[id='entitylist.aspx'].Parameters.ItemsPerPage" v
            <add key="JCI.P2000.ThinClient.Interface.User.Page[id='inoutstatus.aspx'].Parameters.ItemsPerPage"

            <add key="JCI.P2000.Process.Xe.run" value="false"/>
            <!--<add key="JCI.P2000.Process.Xe.path" value="false"/>-->
            <add key="JCI.P2000.Process.Xe.Arguments" value="-port=8080"/>
            <add key="JCI.P2000.Process.Xe.Listening" value="http://127.0.0.1:8080"/>

            <add key="JCI.P2000.Process.Xe.Inprocess" value="true"/>
        </appSettings>

</configuration>
```

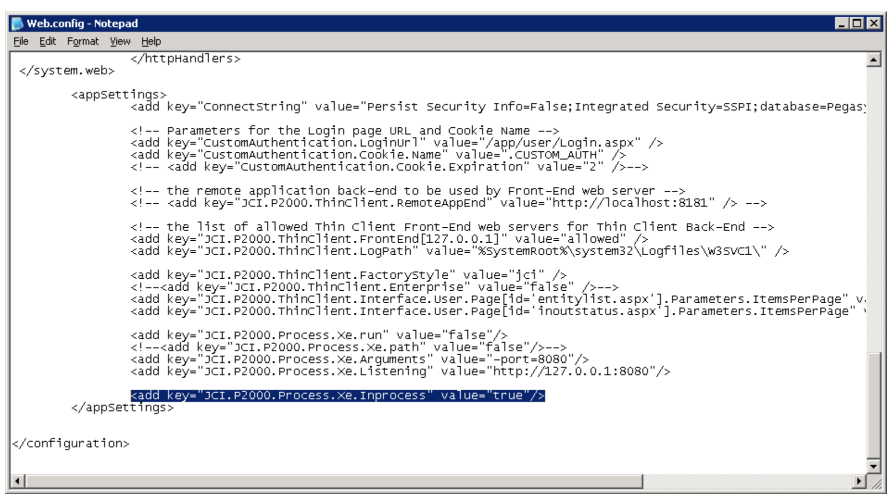
6. Replace the IP address with the IP address or computer name of the P2000 server.
7. Replace the **8080** text with the service port number defined in the P2000 server's **xe.config** file. See "Configuring the P2000 Server's xe.config File" on page 3-12.

   Example:

*<add key="JCI.P2000.Process.Xe.Listening" value="http://**145.122.345.322**:**8181**"/>*

   In the previous example, the P2000 server's IP address is 145.122.345.322 and the service port defined in the xe.config file is 8181.
8. Locate the following text:

   <add key="JCI.P2000.Process.Xe.Inprocess" value="true"/>



```
Web.config - Notepad
File  Edit  Format  View  Help
            </httpHandlers>
    </system.web>

        <appSettings>
            <add key="ConnectString" value="Persist Security Info=False;Integrated Security=SSPI;database=Pegas

            <!-- Parameters for the Login page URL and Cookie Name -->
            <add key="CustomAuthentication.LoginUrl" value="/app/user/Login.aspx" />
            <add key="CustomAuthentication.Cookie.Name" value=".CUSTOM_AUTH" />
            <!-- <add key="CustomAuthentication.Cookie.Expiration" value="2" />-->

            <!-- the remote application back-end to be used by Front-End web server -->
            <!-- <add key="JCI.P2000.ThinClient.RemoteAppEnd" value="http://localhost:8181" /> -->

            <!-- the list of allowed Thin Client Front-End web servers for Thin Client Back-End -->
            <add key="JCI.P2000.ThinClient.FrontEnd[127.0.0.1]" value="allowed" />
            <add key="JCI.P2000.ThinClient.LogPath" value="%SystemRoot%\system32\Logfiles\W3SVC1\" />

            <add key="JCI.P2000.ThinClient.FactoryStyle" value="jci" />
            <!--<add key="JCI.P2000.ThinClient.Enterprise" value="false" />-->
            <add key="JCI.P2000.ThinClient.Interface.User.Page[id='entitylist.aspx'].Parameters.ItemsPerPage" v
            <add key="JCI.P2000.ThinClient.Interface.User.Page[id='inoutstatus.aspx'].Parameters.ItemsPerPage"

            <add key="JCI.P2000.Process.Xe.run" value="false"/>
            <!--<add key="JCI.P2000.Process.Xe.path" value="false"/>-->
            <add key="JCI.P2000.Process.Xe.Arguments" value="-port=8080"/>
            <add key="JCI.P2000.Process.Xe.Listening" value="http://127.0.0.1:8080"/>

            <add key="JCI.P2000.Process.Xe.Inprocess" value="true"/>
        </appSettings>

</configuration>
```

9. Change the value to "false".

   *<add key="JCI.P2000.Process.Xe.Inprocess" value="**false**"/>*

10. Under the Xe.Inprocess line of text (see Step 9), add the following line of text and replace the *Enter Installation Key Here* text with the installation key of the P2000 server:

*<add key="JCI.P2000.Registration.InstallationKey" value="***Enter Installation Key Here***" />*

Example:

<add key="JCI.P2000.Registration.InstallationKey" value="FJASO597NDIJA235398"/>

To view the current installation key of the P2000 server, from the taskbar on the P2000 server, select *Start>Programs>Johnson Controls>P2000 Server>Launch Register*. The current installation key is listed on the Register dialog box.

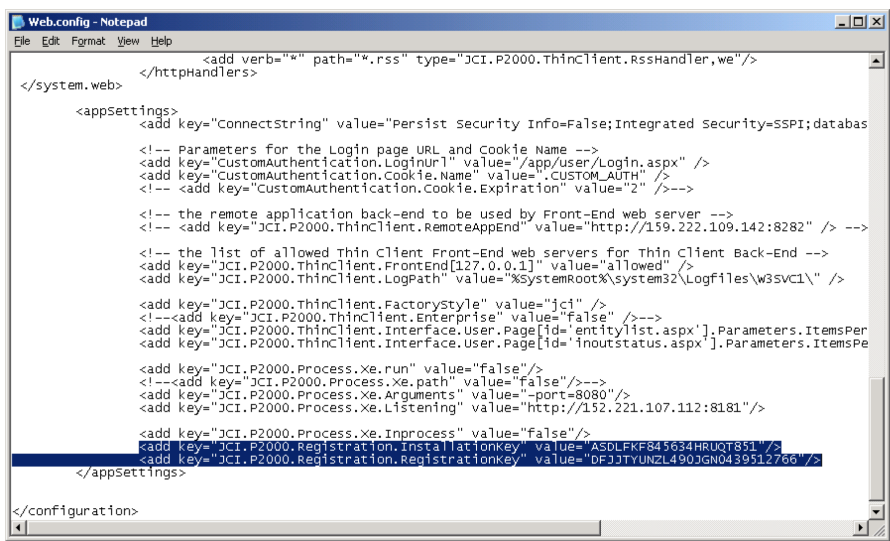
11. Under the InstallationKey line of text, add the following line of text and replace the *Enter Registration Key Here* text with the registration key of the P2000 server:

*<add key="JCI.P2000.Registration.RegistrationKey" value="***Enter Registration Key Here***" />*

Example:

<add key="JCI.P2000.Registration.RegistrationKey" value="FHEUYWNVNA35735NDAQIFU" />

To view the current registration key of the P2000 server, from the taskbar on the P2000 server, select *Start>Programs>Johnson Controls>P2000 Server>Launch Register*. The current registration key is listed on the Register dialog box.



12. From the menu bar, select **File>Save**.
13. Reboot the front-end web 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 (e.g. company logo)
- Background colors
- Field type (e.g. 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 3-22 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 (i.e. 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 (e.g. 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 (i.e. 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.

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:

- Determining 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 will be using the new interface?
- Making a backup copy of the default style. See page 3-25.

- Creating one or more new style folders (for multiple interfaces only) to store the SPS files used to customize the Web Access interface. See page 3-25.
- Opening Altova StyleVision and editing the SPS source files, as needed. See page 3-29.
- Generating XSLT files from the edited SPS files using StyleVision and saving them to a designated P2000 directory and subdirectories, as applicable. See page 3-30.
- If using multiple interfaces, configuring the **xe.config** file, which allows users to view and assign the new style in the P2000 host software interface. See page 3-30.
- If using multiple interfaces, assigning entities to Web Access user interface styles in P2000. See page 3-32.

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 (i.e. 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.

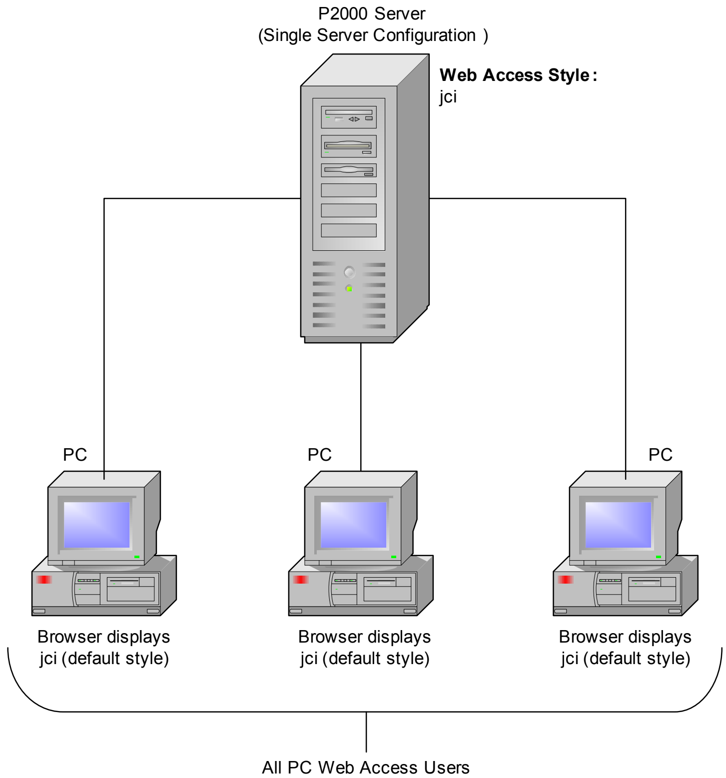


Figure 3-3: Single Interface Deployment

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 3-25).

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. Different styles are assigned to users via the Web UI Styles tab in the P2000 host software. See “Assigning Users to a New Style (Multiple Interfaces Only)” on page 3-32 for more information.

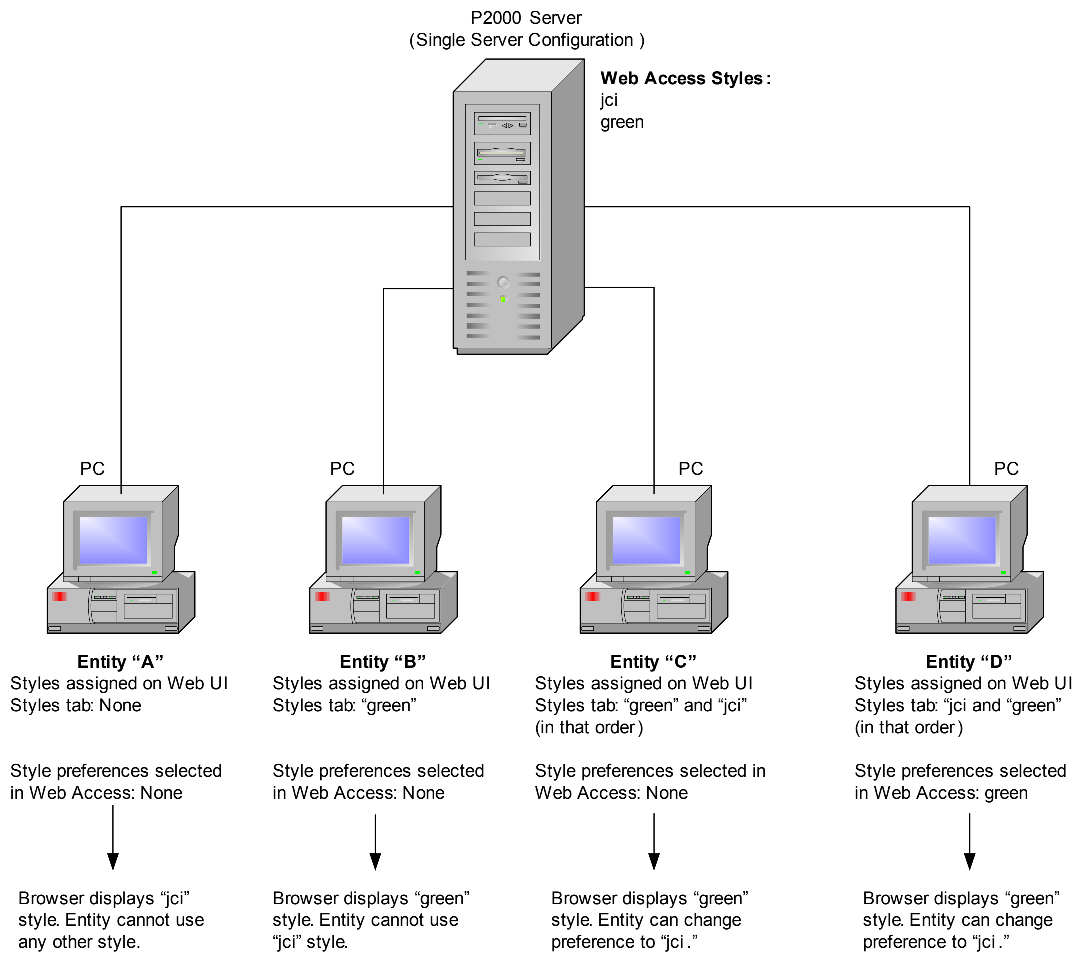


Figure 3-4: Deployment of Multiple Interfaces

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 3-23 for information on how the files are structured for the different platforms.

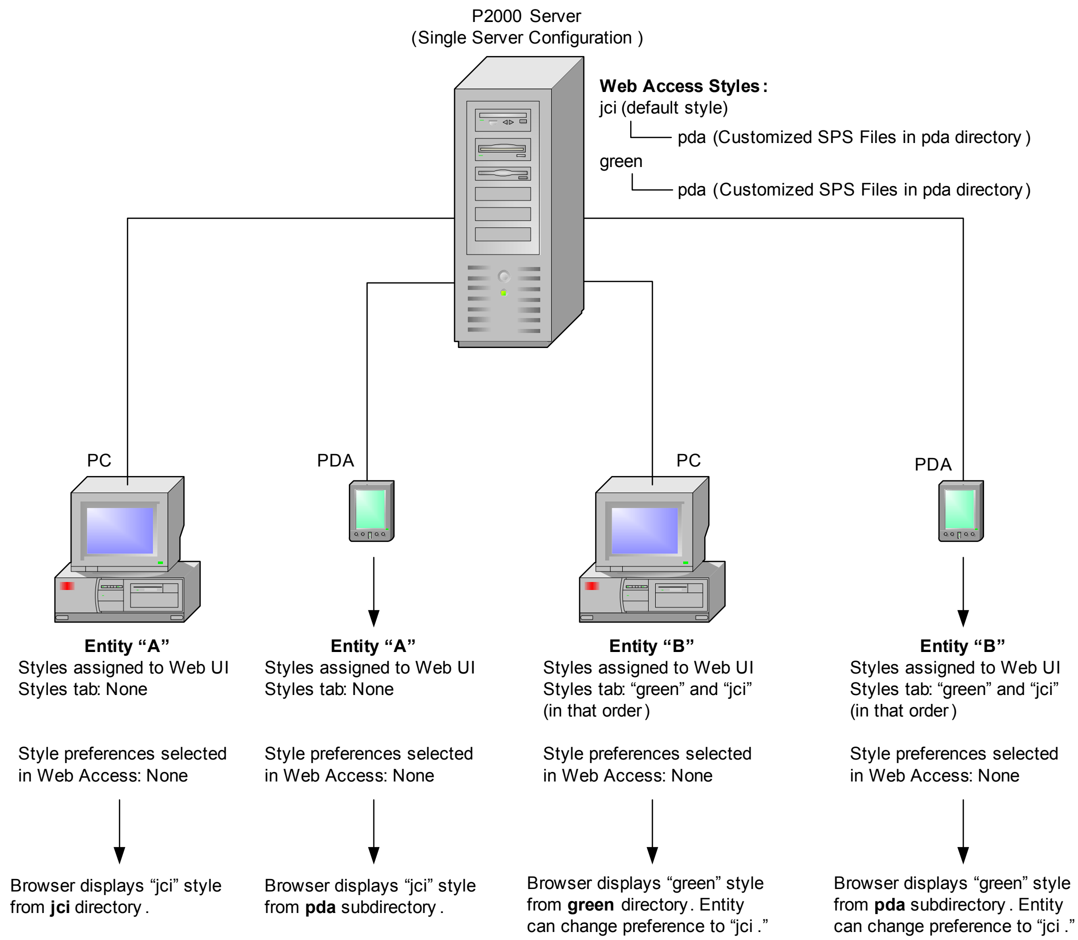


Figure 3-5: PDA Deployment

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 (e.g. "jci-fr," where "jci" is the style name and "fr" is the language code for French).

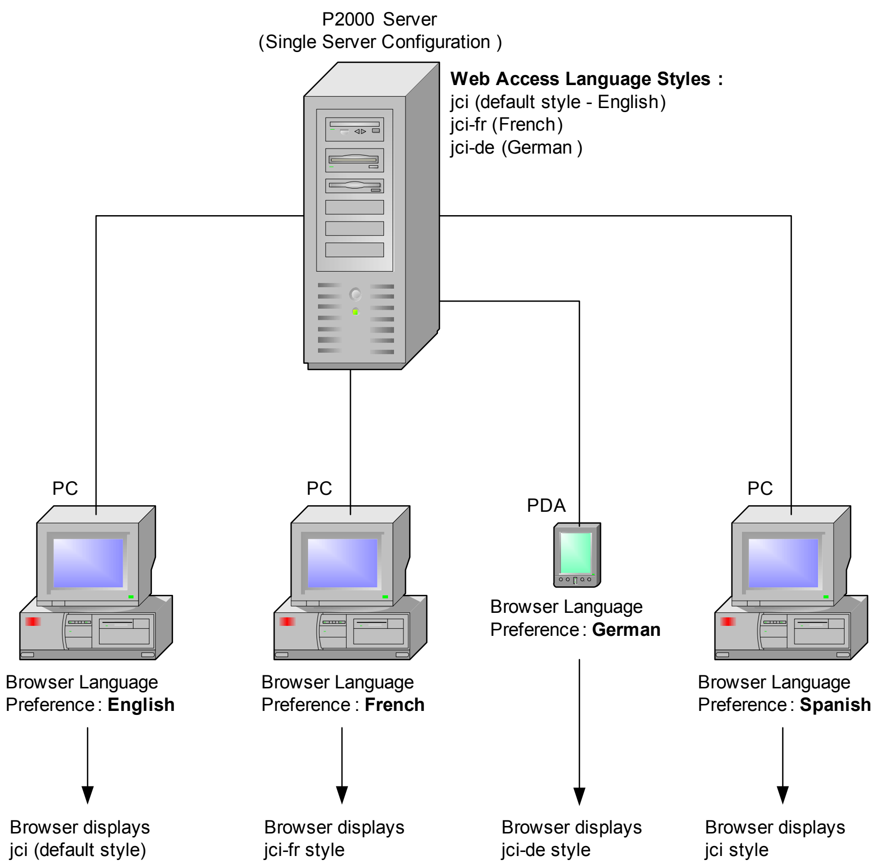


Figure 3-6: Language Styles

The default language is English. Johnson Controls does not provide interface styles translated into a language other than English. The customer is responsible for translating the interface text into the desired language. 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 3-6).

NOTE

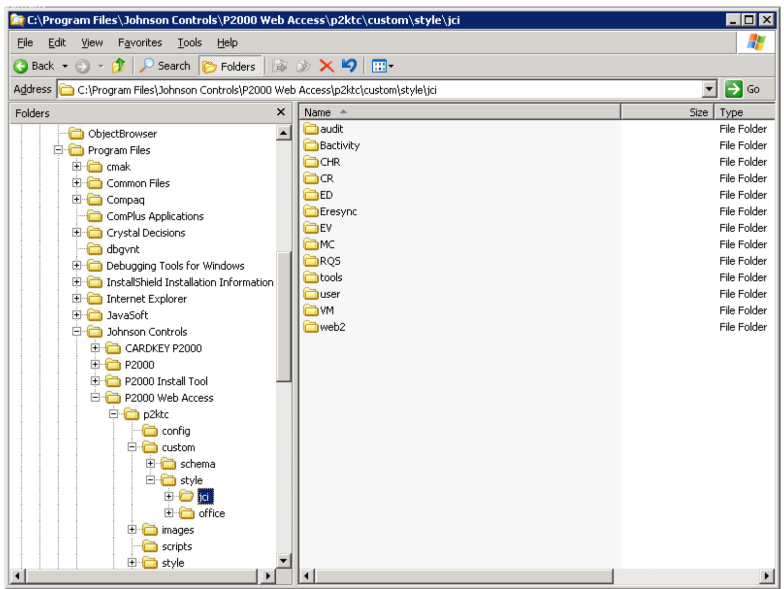
The P2000 Web Access application does not support language variants (e.g. Canadian French, Mexican Spanish, etc.), which requires a four digit language code (e.g. "fr-ca" for Canadian French). Web Access supports only the first two digits (e.g. "fr" for French from France).

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 Web Access\p2ktc\custom\style\jci*

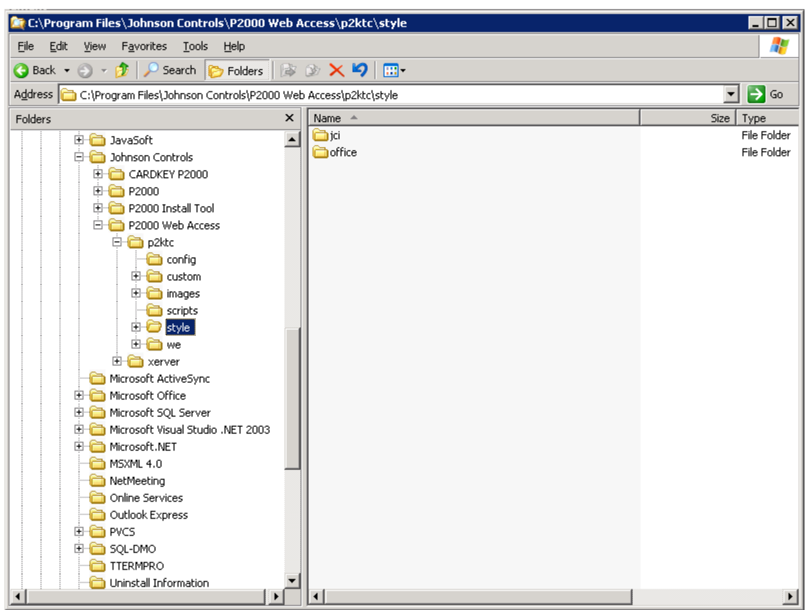


- The *p2ktc\custom\style\jci* directory stores the SPS source files used for the Web Access default interface.
- Before editing the default interface, make a backup copy of the **jci** directory and save it in secure location, preferably in a directory that is backed up regularly. See “Backing Up the JCI Default Interface Style” on page 3-25.
- 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 (e.g. “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 (e.g. “jci-de” for the jci style displayed in German).

- 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 entity-specific pages (e.g. Entity Search page, Add Entity page, Edit Entity 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 Web Access\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 (e.g. “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 Web Access\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 Web Access\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 (e.g. 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

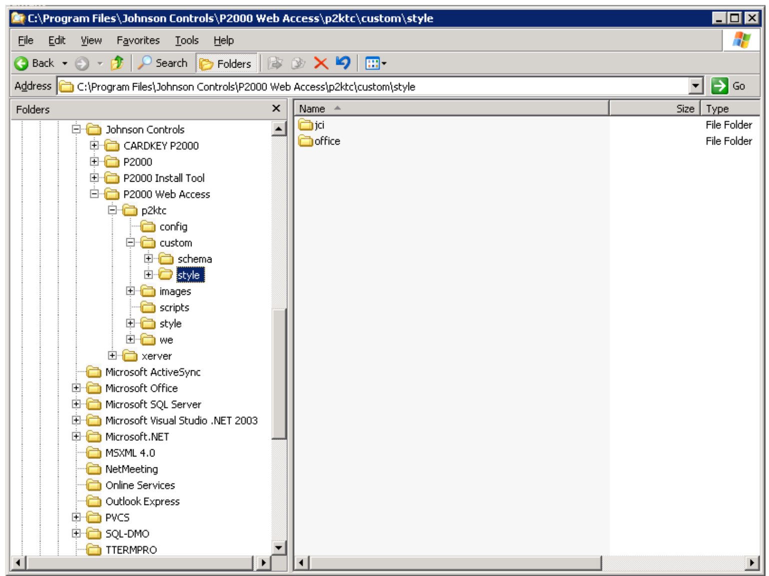
Follow the steps in this section if you are deploying more than one Web Access interface style. The source directory will be used to store the SPS files of the new style. The deployment directory will be used to store the generated XSLT files.

If you 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 3-29). If you will create a language-specific style directory, see "Creating Source and Deployment Directories for a Language-specific Style" on page 3-28.

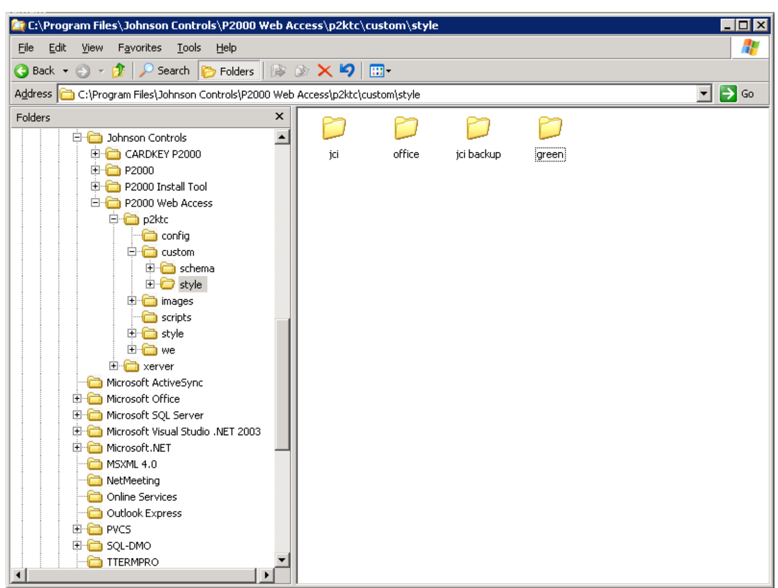
➤ To create a source directory for the new interface style:

1. Open Windows® Explorer and access the following directory:

   Local Disk:\Program Files\Johnson Controls\P2000 Web Access\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 (e.g. “green”, “basic”, etc.).

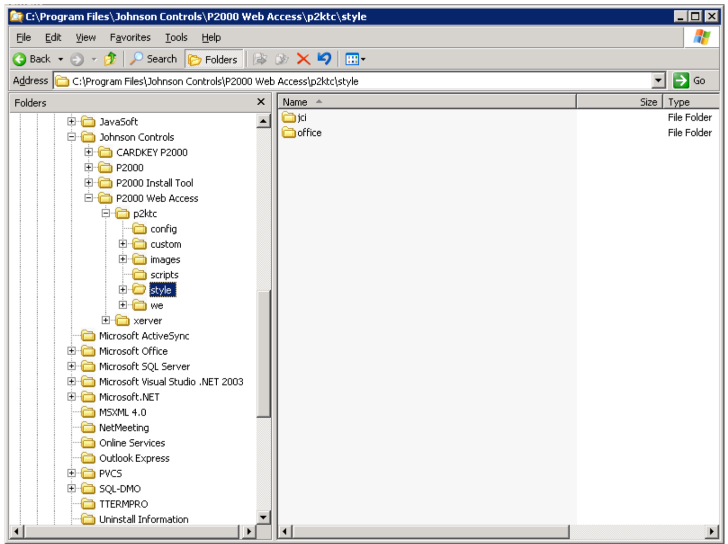


5. Repeat the steps for each style you wish to create.

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

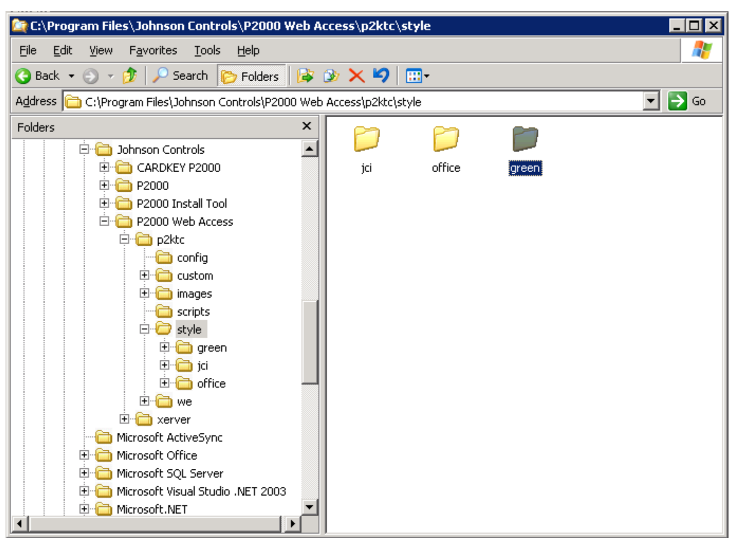
1. Access the following directory:

   Local Disk:\Program Files\Johnson Controls\P2000 Web Access\p2ktc\style



2. Right-click over the **jci** subdirectory and select **Copy** from the pop-up menu.
3. Paste the folder into a different 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 Web Access\p2ktc\custom\style* directory (e.g. “green”).
5. Paste the copied folder representing the new style into the following directory:

   Local Disk:\Program Files\Johnson Controls\P2000 Web Access\p2ktc\style



12/3/08

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.

6. 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. 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 3-22 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-de" (default style for browsers set to German)
   - "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)
   Chinese (zh)
   French (fr)
   German (de)
   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 Web Access\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 (e.g. “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 Web Access\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 Entity Search page has a single source file (EntitySearch.sps) and a single deployment file (EntitySearch.xslt) of the same name. If you want to edit this page, use StyleVision to open and edit the EntitySearch.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:

http://serverIP/p2ktc/we/app/application name/function name/modifier.aspx

Server IP Address

Determines Location of SPS File; Modifier is Optional

Constant

Application Name: Corresponds to the subdirectory (e.g. Bactivity, EResync, CHR, MC, etc.) located in the style directory.

Function Name: Corresponds to the SPS file name (e.g. /entitysearch.aspx corresponds to the EntitySearch.sps file).

Modifier: Some pages have modifiers such as “adv”, “bio”, etc. The Function Name and Modifier correspond to the SPS file name (e.g. /entitysearch.adv.aspx corresponds to the EntitySearch.adv.sps file).

Examples:

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

  PC Interface: Edit the EntitySearch.sps file in the *stylename\Bactivity* directory.

  PDA Interface: Edit the EntitySearch.sps file in the *stylename\Bactivity\pda* directory.

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

  PC Interface: Edit the EntitySearch.adv.sps file in the *stylename\Bactivity* directory.

  PDA Interface: Edit the EntitySearch.adv.sps file in the *stylename\Bactivity\pda* 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\VM\pda* directory.

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 Web Access\p2ktc\custom\style\jci\Bactivity\EntitySearch.sps

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

Local Disk:\Program Files\Johnson Controls\P2000 Web Access\p2ktc\style\jci\Bactivity\EntitySearch.xslt

Configuring the xe.config File

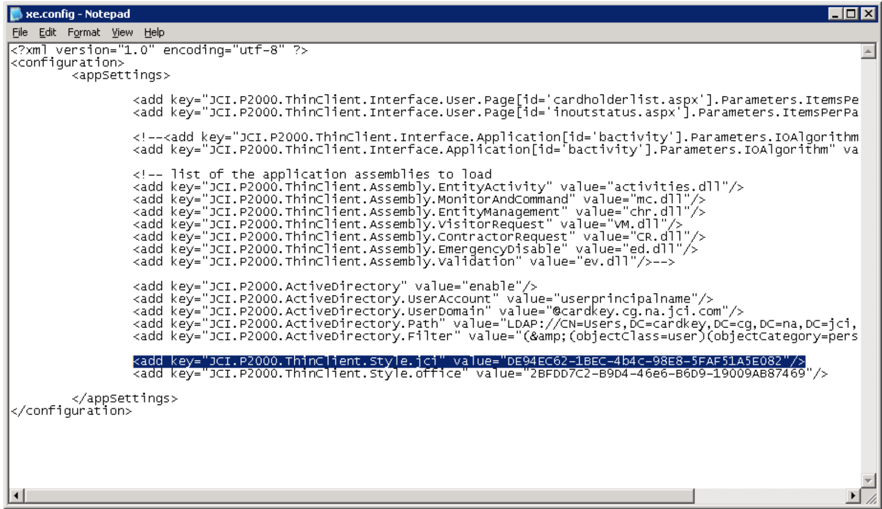
Before you can assign an interface to a user account, you must configure the **xe.config** file so that the interface is visible in the P2000 host software.

➤ To configure the xe.config file:

1. Access the following directory:
   Local Disk:\Program Files\Johnson Controls\P2000 Web Access\xerver\xe
2. Open the **xe.config** file in Notepad® or other text editor.

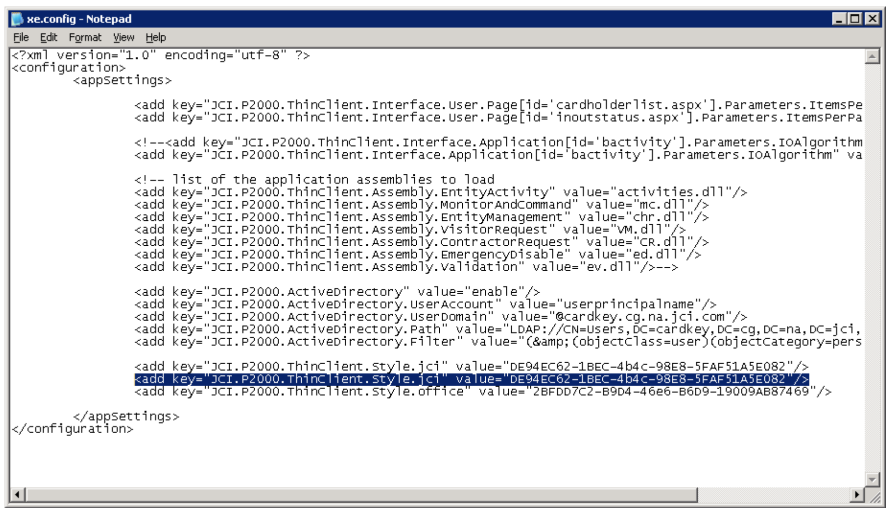
3. Locate the following text:

<add key="JCI.P2000.ThinClient.Style.jci" value="DE94EC62-1BEC-4b4c-98E8-5FAF51A5E082"/>



```
xe.config - Notepad
File  Edit  Format  View  Help
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
        <appSettings>

                <add key="JCI.P2000.ThinClient.Interface.User.Page[id='cardholderlist.aspx'].Parameters.ItemsPe
                <add key="JCI.P2000.ThinClient.Interface.User.Page[id='inoutstatus.aspx'].Parameters.ItemsPerPa

                <!--<add key="JCI.P2000.ThinClient.Interface.Application[id='bactivity'].Parameters.IOAlgorithm
                <add key="JCI.P2000.ThinClient.Interface.Application[id='bactivity'].Parameters.IOAlgorithm" va

                <!-- list of the application assemblies to load
                <add key="JCI.P2000.ThinClient.Assembly.EntityActivity" value="activities.dll"/>
                <add key="JCI.P2000.ThinClient.Assembly.MonitorAndCommand" value="mc.dll"/>
                <add key="JCI.P2000.ThinClient.Assembly.EntityManagement" value="chr.dll"/>
                <add key="JCI.P2000.ThinClient.Assembly.VisitorRequest" value="VM.dll"/>
                <add key="JCI.P2000.ThinClient.Assembly.ContractorRequest" value="CR.dll"/>
                <add key="JCI.P2000.ThinClient.Assembly.EmergencyDisable" value="ed.dll"/>
                <add key="JCI.P2000.ThinClient.Assembly.Validation" value="ev.dll"/>-->

                <add key="JCI.P2000.ActiveDirectory" value="enable"/>
                <add key="JCI.P2000.ActiveDirectory.UserAccount" value="userprincipalname"/>
                <add key="JCI.P2000.ActiveDirectory.UserDomain" value="@cardkey.cg.na.jci.com"/>
                <add key="JCI.P2000.ActiveDirectory.Path" value="LDAP://CN=Users,DC=cardkey,DC=cg,DC=na,DC=jci,
                <add key="JCI.P2000.ActiveDirectory.Filter" value="(&amp;(objectClass=user)(objectCategory=pers

                <add key="JCI.P2000.ThinClient.Style.jci" value="DE94EC62-1BEC-4b4c-98E8-5FAF51A5E082"/>
                <add key="JCI.P2000.ThinClient.Style.office" value="2BFDD7C2-B9D4-46e6-B6D9-19009AB87469"/>

        </appSettings>
</configuration>
```

4. Copy the text and paste one line below.



```
xe.config - Notepad
File  Edit  Format  View  Help
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
        <appSettings>

                <add key="JCI.P2000.ThinClient.Interface.User.Page[id='cardholderlist.aspx'].Parameters.ItemsPe
                <add key="JCI.P2000.ThinClient.Interface.User.Page[id='inoutstatus.aspx'].Parameters.ItemsPerPa

                <!--<add key="JCI.P2000.ThinClient.Interface.Application[id='bactivity'].Parameters.IOAlgorithm
                <add key="JCI.P2000.ThinClient.Interface.Application[id='bactivity'].Parameters.IOAlgorithm" va

                <!-- list of the application assemblies to load
                <add key="JCI.P2000.ThinClient.Assembly.EntityActivity" value="activities.dll"/>
                <add key="JCI.P2000.ThinClient.Assembly.MonitorAndCommand" value="mc.dll"/>
                <add key="JCI.P2000.ThinClient.Assembly.EntityManagement" value="chr.dll"/>
                <add key="JCI.P2000.ThinClient.Assembly.VisitorRequest" value="VM.dll"/>
                <add key="JCI.P2000.ThinClient.Assembly.ContractorRequest" value="CR.dll"/>
                <add key="JCI.P2000.ThinClient.Assembly.EmergencyDisable" value="ed.dll"/>
                <add key="JCI.P2000.ThinClient.Assembly.Validation" value="ev.dll"/>-->

                <add key="JCI.P2000.ActiveDirectory" value="enable"/>
                <add key="JCI.P2000.ActiveDirectory.UserAccount" value="userprincipalname"/>
                <add key="JCI.P2000.ActiveDirectory.UserDomain" value="@cardkey.cg.na.jci.com"/>
                <add key="JCI.P2000.ActiveDirectory.Path" value="LDAP://CN=Users,DC=cardkey,DC=cg,DC=na,DC=jci,
                <add key="JCI.P2000.ActiveDirectory.Filter" value="(&amp;(objectClass=user)(objectCategory=pers

                <add key="JCI.P2000.ThinClient.Style.jci" value="DE94EC62-1BEC-4b4c-98E8-5FAF51A5E082"/>
                <add key="JCI.P2000.ThinClient.Style.jci" value="DE94EC62-1BEC-4b4c-98E8-5FAF51A5E082"/>
                <add key="JCI.P2000.ThinClient.Style.office" value="2BFDD7C2-B9D4-46e6-B6D9-19009AB87469"/>

        </appSettings>
</configuration>
```

5. In the newly pasted text, replace the lower-case **jci** text with the name of the new style.

*<add key="JCI.P2000.ThinClient.Style.**jci**" value="DE94EC62-1BEC-4b4c-98E8-5FAF51A5E082"/>*

*<add key="JCI.P2000.ThinClient.Style.**green**" value="DE94EC62-1BEC-4b4c-98E8-5FAF51A5E082"/>*

6. Change the first letter of the value to a number between 0-9 or a letter between A-F.

*<add key="JCI.P2000.ThinClient.Style.jci" value="**D**E94EC62-1BEC-4b4c-98E8-5FAF51A5E082"/>*

*<add key="JCI.P2000.ThinClient.Style.green" value="**A**E94EC62-1BEC-4b4c-98E8-5FAF51A5E082"/>*

7. Click **File>Save**.

8. Restart Microsoft® Internet Information Services (IIS).

9. Launch Web Access.

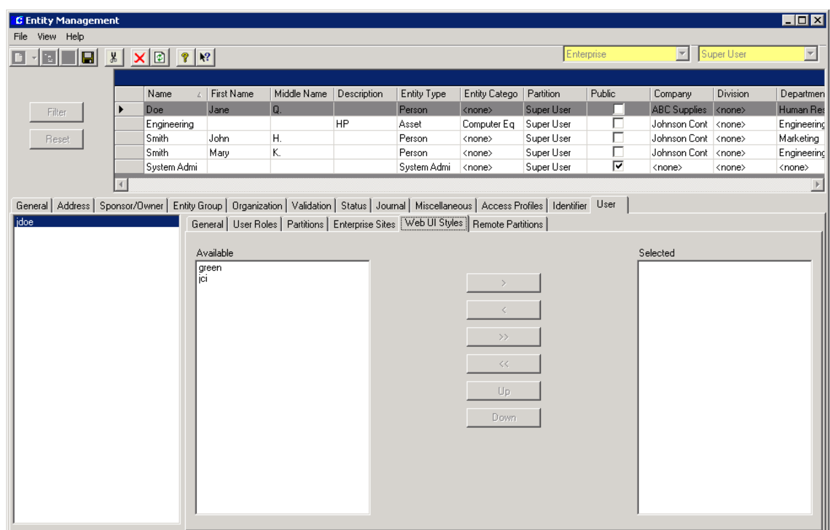
   You will now be able to assign the new style to users with the P2000 host software.

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 Web UI Styles tab on the P2000 host software's Entity Management window.

➤ To assign users to a new style:

1. In P2000, click the **Entity Management** button on the toolbar, or select **Access>Entity Management** from the Main menu bar. The Entity Management window appears.
2. Select the user (entity) whom you will assign to the new style(s).
3. Click the **User** tab.
4. In the left-hand pane, select the user account that will be assigned the Web Access interface style.
5. Select the **Web UI Styles** tab.



6. Click **Edit** on the toolbar.
7. To assign one or more styles to the user (entity), select one or more styles in the **Available** pane and click the right arrow button. The assigned style(s) appear in the **Selected** pane.
8. Use the **Up** or **Down** buttons to move the styles in the Selected box accordingly.

NOTE

The first style on the Selected box is the user's default style. If the user wishes to use a different style, then he or she will need to select a style preference using the Web Access user preferences feature. See "User Preferences" on page 2-83.

---

9. Click **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.
- Edit the maximum number of entities to display on the Entity Search Results page and the Current Entity In/Out Status page (Entity Activity application). See page 3-34.
- Change the default Visit Start and End Date/Time settings on the Visitor Management application. See page 3-37.
- Configure the system to use Active Directory Authentication. See page 3-40.

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.

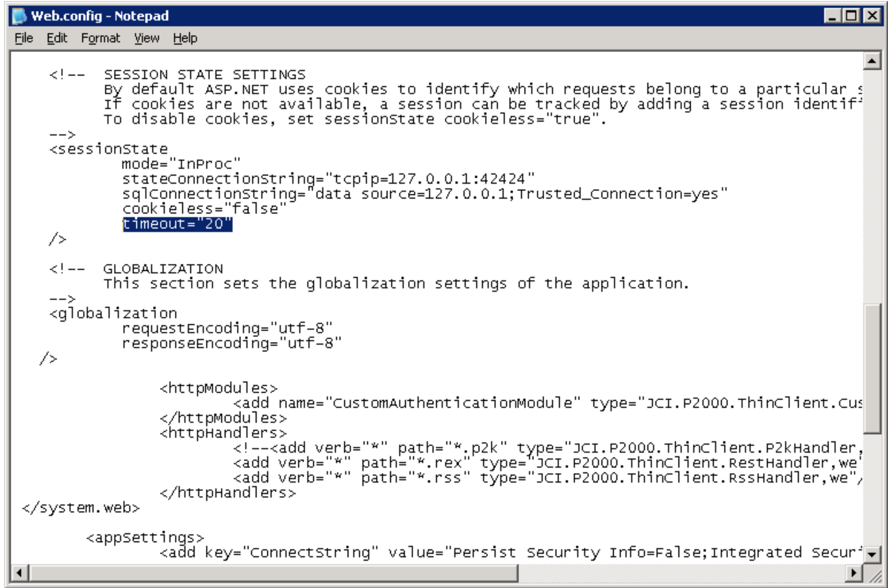
Default Setting = 20 minutes

➤ To change the time-out period:

1. Access the following directory on the P2000 server:

   <Local Disk>:\Program Files\Johnson Controls\P2000 Web Access\p2ktc\we
2. Open the **Web.config** file with a text editor such as Microsoft Notepad.
3. Locate the following text:

   timeout="20"



4. Edit the number accordingly.

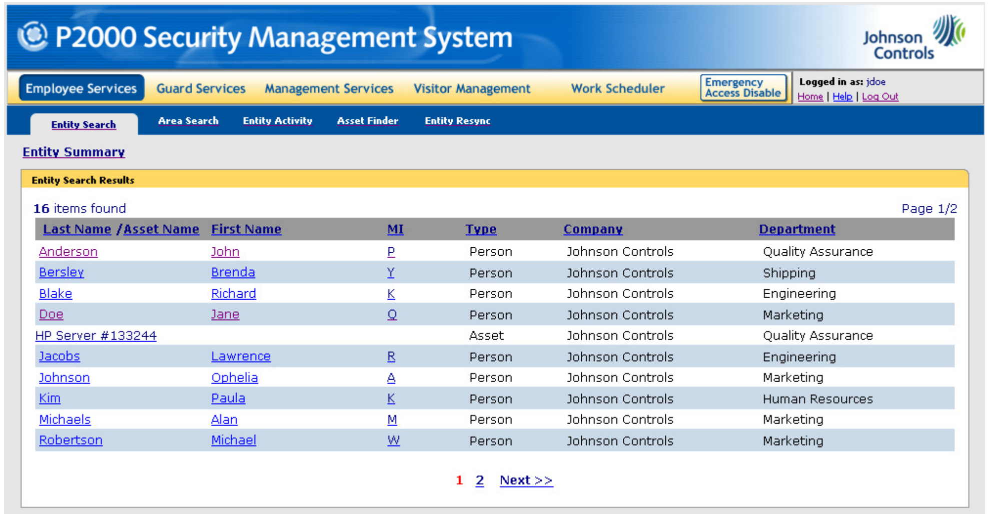
   Examples:

   - `timeout="10"` (session will time out after ten minutes of inactivity)
   - `timeout="60"` (session will time out after an hour of inactivity)

5. Click **File>Save**.

Changing the Maximum Number of Entities to Display

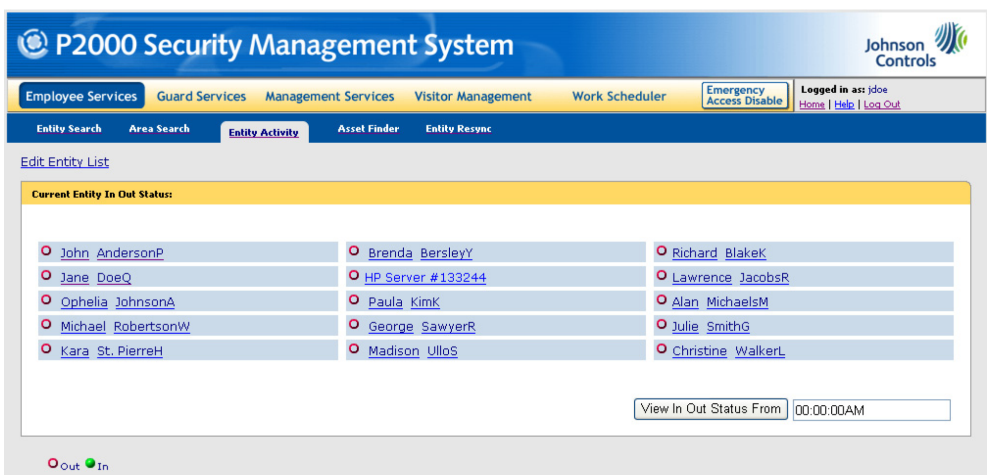
Web Access allows you to configure the maximum number of entities you wish to display at a time on the Entity Search Results page and the Current Entity In/Out Status page (Entity Activity application). For example, if the default number of entities listed for the Entity Search Results page is 10 and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



The Current Entity In/Out Status page for the Entity Activity application lists the entities who are “In” or “Out” of the facility based on their identifier activity.

For more information on the Entity Search Results page, see “Entity Search” on page 2-1.

For more information on the Current Entity In/Out Status page, see “Entity Activity” on page 2-10.



There are three ways to modify the number of entities listed per page during an entity search or when viewing entities with the Entity Activity 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 “Temporarily Changing the Number of Entities Listed Per Page” on page 2-4 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 **Web.config** file located at:

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

For example, if the **Web.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 entities at a time (the XSLT file takes precedence over the Web.config file). If the user appends `&ipp=20` to the page's URL, the page will temporarily display 20 entities at a time (appending `&ipp=n` to the URL takes precedence over all other ItemsPerPage parameters).

<u>Default Setting of Web.config File's ItemsPerPage Parameter</u> (Entity Search Results page) = 10 entities listed per page

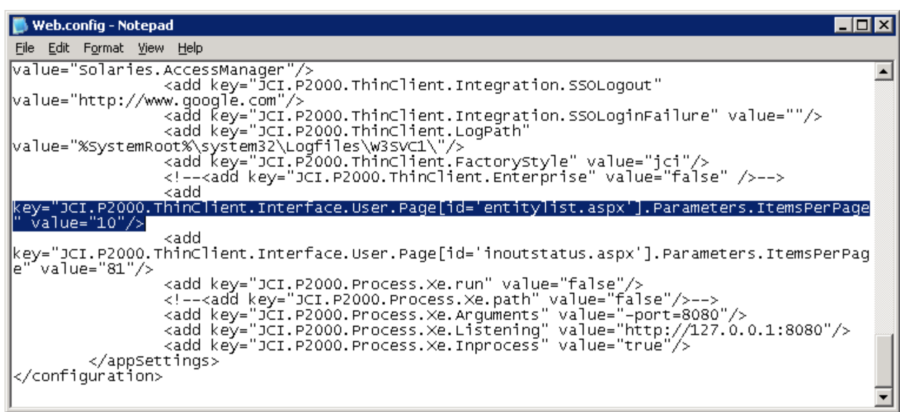
<u>Default Setting of Web.config File's ItemsPerPage Parameter</u> (Current Entity In/Out Status page) = 81 entities listed per page

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

1. Access the following directory on the P2000 server:

   <Local Disk>:\Program Files\Johnson Controls\P2000 Web Access\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.Interface.User.Page[id='entitylist.aspx']. Parameters.ItemsPerPage" value="10"/>



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

   Example:

   - `value="20"` (page will display up to 20 entities at a time)
5. Click **File>Save**.

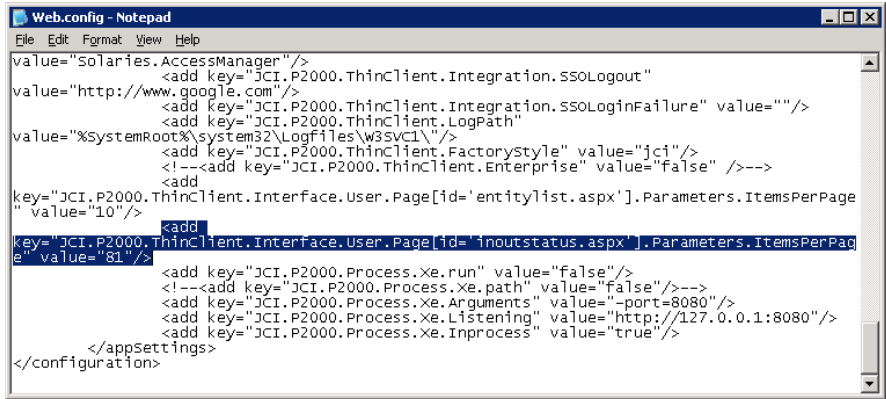
➤ To change the maximum number of entity in/out status results:

1. Access the following directory on the P2000 server:

   <Local Disk>:\Program Files\Johnson Controls\P2000 Web Access\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.Interface.User.Page[id='inoutstatus.aspx']. Parameters.ItemsPerPage" value="81"/>



```
Web.config - Notepad
File  Edit  Format  View  Help
value="Solaries.AccessManager"/>
                <add key="JCI.P2000.ThinClient.Integration.SSOLogout"
value="http://www.google.com"/>
                <add key="JCI.P2000.ThinClient.Integration.SSOLoginFailure" value=""/>
                <add key="JCI.P2000.ThinClient.LogPath"
value="%SystemRoot%\system32\Logfiles\W3SVC1\"/>
                <add key="JCI.P2000.ThinClient.FactoryStyle" value="jci"/>
                <!--<add key="JCI.P2000.ThinClient.Enterprise" value="false" />-->
                <add
key="JCI.P2000.ThinClient.Interface.User.Page[id='entitylist.aspx'].Parameters.ItemsPerPage
" value="10"/>
                <add
key="JCI.P2000.ThinClient.Interface.User.Page[id='inoutstatus.aspx'].Parameters.ItemsPerPag
e" value="81"/>
                <add key="JCI.P2000.Process.Xe.run" value="false"/>
                <!--<add key="JCI.P2000.Process.Xe.path" value="false"/>-->
                <add key="JCI.P2000.Process.Xe.Arguments" value="-port=8080"/>
                <add key="JCI.P2000.Process.Xe.Listening" value="http://127.0.0.1:8080"/>
                <add key="JCI.P2000.Process.Xe.Inprocess" value="true"/>
        </appSettings>
</configuration>
```

NOTE

The key (e.g. inoutstatus) must match the page name.

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

   Example:

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

5. Click **File>Save**.

Changing the Default Visit Start and End Date/Time Settings

The Visitor Management application allows users to request a visitor identifier. 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 identifier 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 identifier at your facility. For example, if the option is set to 3 days and the user enters a Visit Start Date of 12/1/2008, he/she cannot enter a Visit End Date past 12/3/2008.

  Default Setting = 50,000 days

- **Default Visit Start and End Times**
  When a user opens the Visitor Management application to request a visitor identifier, 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 identifier, 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.

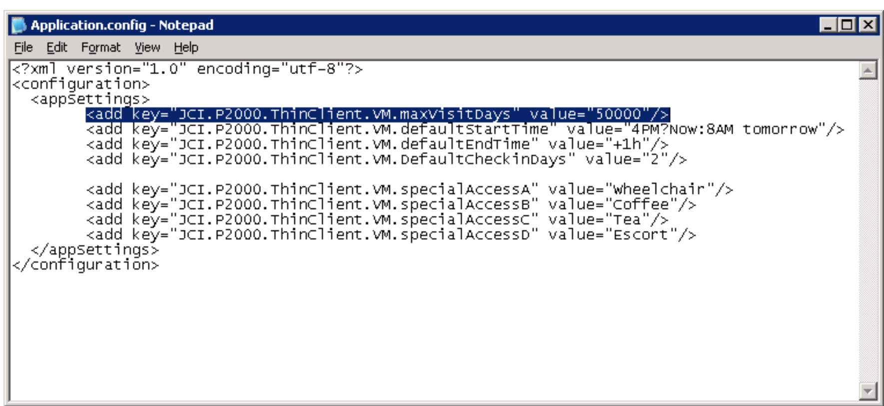
➤ To set the maximum visit period:

1. Access the following directory on the P2000 server:

   <Local Disk>:\Program Files\Johnson Controls\P2000 Web Access\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="50000"/>



```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
        <add key="JCI.P2000.ThinClient.VM.maxVisitDays" value="50000"/>
        <add key="JCI.P2000.ThinClient.VM.defaultStartTime" value="4PM?Now:8AM tomorrow"/>
        <add key="JCI.P2000.ThinClient.VM.defaultEndTime" value="+1h"/>
        <add key="JCI.P2000.ThinClient.VM.DefaultCheckinDays" value="2"/>

        <add key="JCI.P2000.ThinClient.VM.specialAccessA" value="wheelchair"/>
        <add key="JCI.P2000.ThinClient.VM.specialAccessB" value="Coffee"/>
        <add key="JCI.P2000.ThinClient.VM.specialAccessC" value="Tea"/>
        <add key="JCI.P2000.ThinClient.VM.specialAccessD" value="Escort"/>
  </appSettings>
</configuration>
```

4. Edit the number (`value="50000"`) 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:

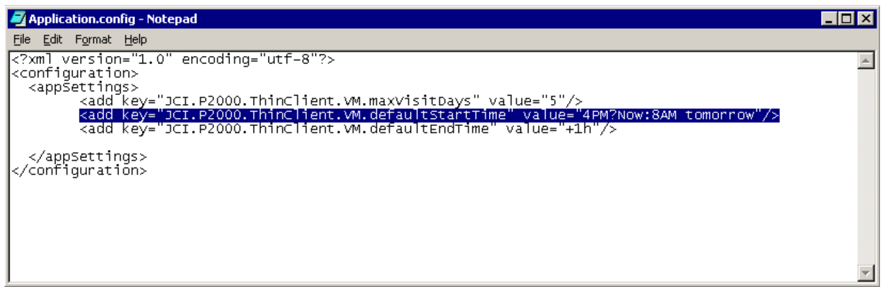
1. Access the following directory on the P2000 server:

   <Local Disk>:\Program Files\Johnson Controls\P2000 Web Access\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:

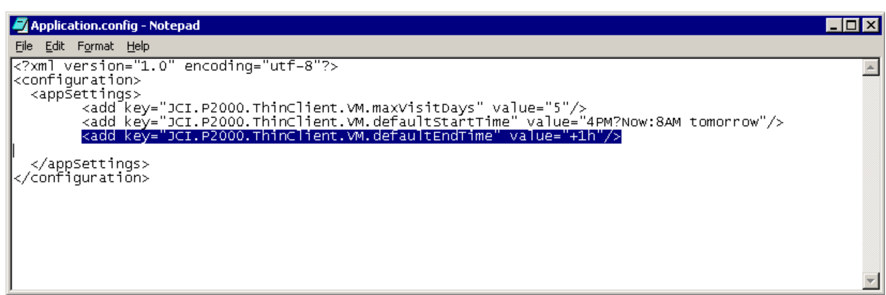
   Example:

   *<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**.

Active Directory Authentication

P2000 Web Access supports Active Directory Authentication.

NOTE

Configuring the system to use Active Directory Authentication should be performed by the System Administrator.

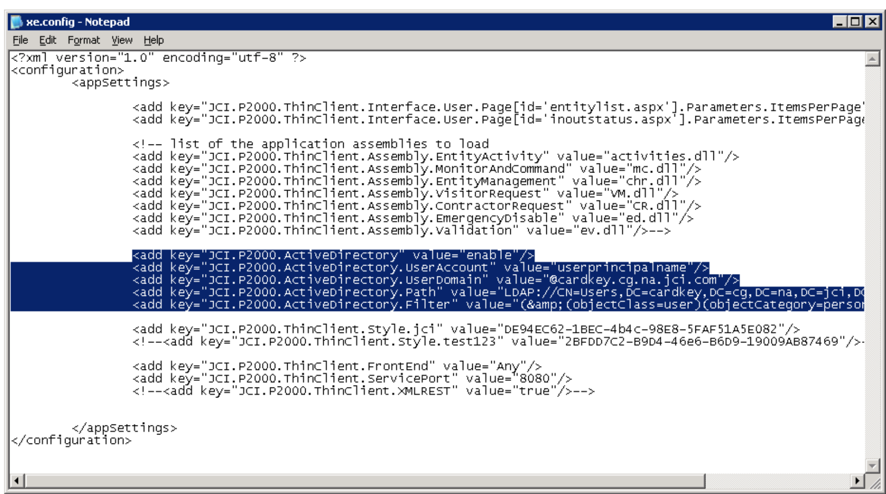
➤ To configure the system to use Active Directory Authentication:

1. Access the following directory on the P2000 server:

   <Local Disk>:\Program Files\Johnson Controls\P2000 Web Access\xerver\xe

2. Open the **xe.config** file with a text editor, such as Notepad.
3. Edit the following parameters according to your system configuration:

<add key="JCI.P2000.ActiveDirectory" value="enable"/>
<add key="JCI.P2000.ActiveDirectory.UserAccount" value="userprincipalname"/>
<add key="JCI.P2000.ActiveDirectory.UserDomain" value="@cardkey.cg.na.jci.com"/>
<add key="JCI.P2000.ActiveDirectory.Path"
value="LDAP://CN=Users,DC=cardkey,DC=cg,DC=na,DC=jci,DC=com"/>
<add key="JCI.P2000.ActiveDirectory.Filter"
value="(&(objectClass=user)(objectCategory=person)(samaccountname=%))"/>



```
xe.config - Notepad
File  Edit  Format  View  Help
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
        <appSettings>

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

                <!-- list of the application assemblies to load
                <add key="JCI.P2000.ThinClient.Assembly.EntityActivity" value="activities.dll"/>
                <add key="JCI.P2000.ThinClient.Assembly.MonitorAndCommand" value="mc.dll"/>
                <add key="JCI.P2000.ThinClient.Assembly.EntityManagement" value="chr.dll"/>
                <add key="JCI.P2000.ThinClient.Assembly.VisitorRequest" value="VM.dll"/>
                <add key="JCI.P2000.ThinClient.Assembly.ContractorRequest" value="CR.dll"/>
                <add key="JCI.P2000.ThinClient.Assembly.EmergencyDisable" value="ed.dll"/>
                <add key="JCI.P2000.ThinClient.Assembly.Validation" value="ev.dll"/>-->

                <add key="JCI.P2000.ActiveDirectory" value="enable"/>
                <add key="JCI.P2000.ActiveDirectory.UserAccount" value="userprincipalname"/>
                <add key="JCI.P2000.ActiveDirectory.UserDomain" value="@cardkey.cg.na.jci.com"/>
                <add key="JCI.P2000.ActiveDirectory.Path" value="LDAP://CN=Users,DC=cardkey,DC=cg,DC=na,DC=jci,DC
                <add key="JCI.P2000.ActiveDirectory.Filter" value="(&amp;(objectClass=user)(objectCategory=person

                <add key="JCI.P2000.ThinClient.Style.jci" value="DE94EC62-1BEC-4b4c-98E8-5FAF51A5E082"/>
                <!--<add key="JCI.P2000.ThinClient.Style.test123" value="2BFDD7C2-B9D4-46e6-B6D9-19009AB87469"/>-

                <add key="JCI.P2000.ThinClient.FrontEnd" value="Any"/>
                <add key="JCI.P2000.ThinClient.ServicePort" value="8080"/>
                <!--<add key="JCI.P2000.ThinClient.XMLREST" value="true"/>-->


        </appSettings>
</configuration>
```

4. Click **File>Save**, and close the file.