

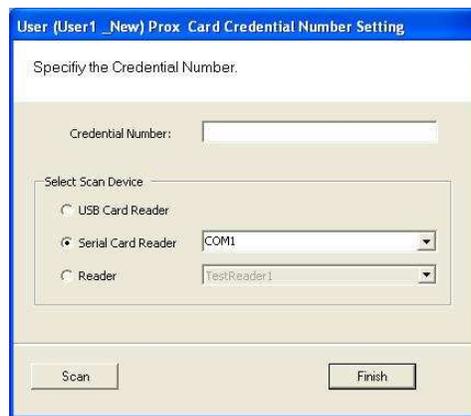
Reader

- You can use a local reader to scan the card credentials. Select **Reader**, and then use the drop-down list to navigate to the reader where the card will be scanned. When you are ready to scan the card, select the **Scan** button. You will have 30 seconds to scan the card. When recognized, the number will display in the Credential Number text box.
- Select **Finish** and return to the Credential Setup dialog box.

NOTE: You may need to expand the drop-down list to view all available readers. Use the highlighted area in the lower right corner.

To register a Prox Card Credential:

- Select **Prox Card** from the list on the left. The User Prox Card Credential Number dialog box opens.



- Enter a Credential Number manually (must be less than 16 characters, zeros will be prepended) or select a scan device:

USB Card Reader

- If you have a USB Card reader connected to your computer, select **USB Card Reader**.
- When you are ready to scan the card, select the **Scan** button. You will have 30 seconds to scan the card. When recognized, the number will display in the Credential Number text box.
- Select **Finish** and return to the Credential Setup dialog box.

Serial Card Reader

- If you have a Serial Card Reader connected to your computer, select **Serial Card Reader** and then select the appropriate com port from the drop-down list.
- When you are ready to scan the card, select the **Scan** button. You will have 30 seconds to scan the card. When recognized, the number will display in the Credential Number text box.
- Select **Finish** and return to the Credential Setup dialog box.

Reader

- You can use a local reader to scan the card credentials. Select **Reader**, and then use the drop-down list to navigate to the reader where the card will be scanned.
- When you are ready to scan the card, select the **Scan** button. You will have 30 seconds to scan the card. When recognized, the number will display in the Credential Number text box.
- Select **Finish** and return to the Credential Setup dialog box.

NOTE: You may need to expand the drop-down list to view all available readers. Use the highlighted area in the lower right corner.

3. In the Proximity Card category, review the Prox Card Type. If the default entry is not the one you will use, select the field and use the down-arrow to select the correct type from the list.

The screenshot shows a window titled "User (Fred Denver) Credentials Setup" with the subtitle "Add, Delete, and Modify User Credentials". On the left, there is a list box containing "Keypad" and "Proximity Card". The "Proximity Card" item is selected. On the right, there is a form with the following fields:

(ID)	
Credential ID	2
Credential Type	Proximity Card
Credential	
Number	000000000003456
Proximity Card	
Enforce Expiration Date	False
Prox Card Type	Prox 26-Bit Card

Below the form, there is a section labeled "Credential ID" with the text "The User Credential's ID Number." At the bottom of the dialog, there are four buttons: "Add", "Remove", "Update", and "Finish".

4. Select **Finish** and return to the Credential Setup dialog box.

To register a Smart Card credential:

1. Select **Smart Card** from the list on the left. The Users Smart Card Credential Number dialog box opens.
2. Enter a Credential Number manually (must be less than 16 characters, zeros will be prepended) or select a scan device:

Card Reader

- If you have a scanning device connected to your computer, select **Card Reader**. When you are ready to scan the card, select the **Scan** button. You will have 30 seconds to scan the card.
- When recognized, the number will display in the Credential Number text box.
- Select **Finish** and return to the Credential Setup dialog box.

Reader

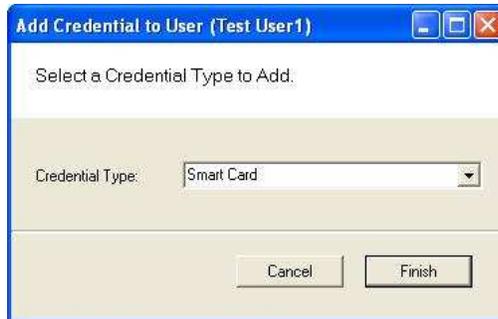
- You can use a local reader to scan the card credentials. Select **Reader**, and then use the drop-down list to navigate to the reader where the card will be scanned.
- When you are ready to scan the card, select the **Scan** button. You will have 30 seconds to scan the card. When recognized, the number will display in the Credential Number text box.
- Select **Finish** and return to the Credential Setup dialog box.

Adding a Credential Type

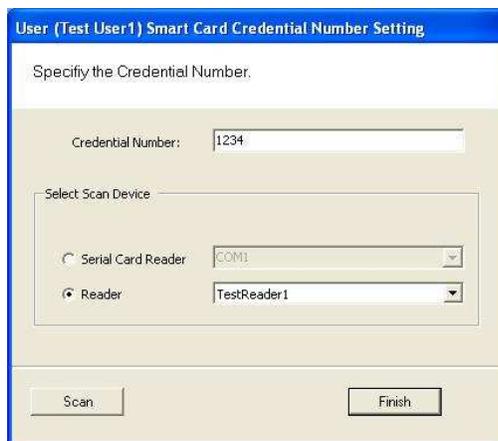
At least one credential type must be defined for the system. The default credential type in WAMS is Keypad. If you use other than keypad credential types, you can add them to the User Credentials Setup dialog box. For example, if your facility will use Smart cards, you can add Smart Card to the list.

To add a card type to the list:

1. In the Users Credentials Setup dialog box, select the **Add** button. The Add Credential to User dialog box opens.



2. Select the Credential Type from the drop-down list.
3. Select **Finish**. The User <Smart Card> Credential Number Setting dialog box opens. The default Credential Number displays in the text box at the top.



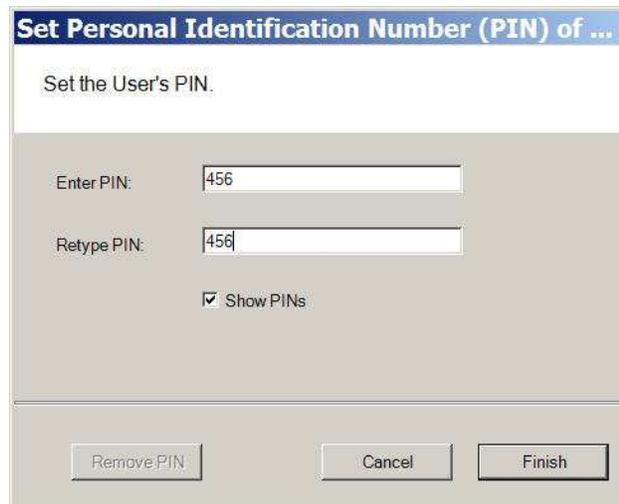
4. If you selected a user before you added the new type, you can enter or scan in the credential number. If you did not select a user, select **Finish** to return to the User Credentials Setup dialog box. The new credential type will display in the list of types.

PIN

You can add a level of security by requiring PIN numbers in addition to credentials for all users, or for specific Timezone Intervals. The default displays the PIN number as asterisks in the fields; however you can choose to show the actual PIN numbers.

To add a PIN Number for a User:

1. Under Credential Settings, click in the field next to PIN. The Set Personal Identification Number dialog box opens.



2. Select the Show PINs check box if you wish to view the numbers instead of asterisks as you type them in.
3. Enter a PIN number for the user.
4. Click Finish to save the PIN and exit the dialog box.

Settings

Each facility user will be assigned a user type and access type, depending on the tasks they perform and the access mode needed to perform those tasks. The system supports four different types of users: General Users, Managers, Programmers, and Service users. You can have up to 65,000 individual users in the system and they can be of any User Type. User types are briefly described in the following paragraphs.

General Users

The majority of users will be assigned as General Users. They are allowed entry only when the access level is set to ID Required. General Users never have access when the reader is in Lockout.

To assign User Type:

1. In the Settings category, select the field next to User Type.
2. Select a User Type from the drop-down list.

Manager

Managers are one of the most useful types of IDs. This User Type provides the capability to change the access level of a reader with a few simple key presses. These changes can and will be overridden by the time schedule or another manager or programmer. A user with Manager privileges is always allowed access to a reader. For example, when a facility requires an individual to have access at all hours of the day without giving any extra privileges, that individual will be assigned Manager Privileges.

Programmer

Programmers can scan all channels at the keypad reader as well as reset the reader to respond to keypad commands as in manager mode. The programmer must enter his or her specific programmer code then:

- Press #7 to scan all channels
- Or
- Press #8 to use manager codes.

NOTE: *Managers and programmers are indistinguishable from a general user when no keyboard is present.*

Reader Control

The system defaults the amount of time from the moment a reader unlocks until it relocks, and the amount of time a door can stay open before an alarm will be triggered. You can modify reader operate and shunt times for individual users. For example, to be ADA compliant, a user who is in a wheelchair, or uses a walker may need more time to pass through a door. You can increase the shunt time for this user.

To modify reader operate time:

In the Reader Control category, Operate Time, select the amount of time you wish to leave the reader in the unlocked position from the drop-down list.

To modify reader shunt time:

In the Reader Control category, Shunt Time, select the amount of time you wish to allow for passage before an alarm will be triggered.

USING WAMS TRANSACTIONS

Each time a user accesses the system, WAMS collects a transaction from the reader/portal gateway network. Once the system is signed on and users begin accessing the system, transactions begin including any alarm activity. You can monitor all this activity in WAMS Transactions. Access WAMS Transactions via the Windows Start button.

To Launch WAMS Transactions:

1. Select Start>All Programs>OSI Security Devices>WAMS>WAMS Transactions.
2. Enter your Login and Password. WAMS Transactions opens at the Transactions Tab.

From here you can view all transaction and alarm activity for the facility you select.

NOTE: *If you have been assigned the Manager or Administrator User Type, you can launch WAMS Transactions from the Applications menu in WAMS Configurator.*

WAMS Transactions Overview

As activity takes place throughout the facility, WAMS tracks each event as a transaction. The most obvious use of WAMS Transactions is to recognize and investigate when security has been compromised. You can immediately locate the source of the alarm and take the action necessary to respond according to your facility policy and procedure.

The WAMS gives each transaction in the database a unique ID, records the time and type of transaction, the reader where the transaction occurred and the User ID and Group name associated with the transaction. You can monitor all this activity, real time, from the WAMS Transactions application. The transactions can be organized and sorted according to how you want to use the data. In addition, you can temporarily pause data updating if you need to review a transaction in more detail.

Reader and Portal Controls

WAMS Version 2.0 now provides access to reader and portal controls from within the WAMS software. From here a user can override access levels of readers to unlock or lockout one or a whole related group of readers. To use this feature, simply right click on the portal or reader and select an option. For more information about this feature, see *Portal and Reader Controls* and *Portal and Reader Messaging* in the Administrator's Guide.

Transactions Tab

You can view all transactions as they occur in the Transactions Tab. Alarm transactions such as Forced Entry or Anti Tamper display in red. Access requests "attempted but not allowed" displays in yellow. Successful access requests display in black on a white background.

OSI Wireless Access Management System - Transactions

File Help

Facility: Secure, Inc. Refresh State
 Timespan: All Updating

Transactions Alarms

Secure, Inc.
 Portals
 Readers

Drag a column header here to group by that column.

ID	Time	Transaction	Reader	User	Group Name
20	2/7/2007 4:33:41 PM	Reader Offline	Reader (0014f5000121)		
21	1/1/1970 12:04:35 AM	Attempt	Reader (0014f5000121)	UNKNOWN <Keypad (...)	
22	1/1/1970 12:04:54 AM	Alarm Cleared (ALL)	Reader (0014f5000121)		
23	2/16/1972 5:21:06 PM	Set Clock	Reader (0014f5000121)		
24	2/7/2007 4:36:00 PM	Alarm Cleared (ALL)	Reader (0014f5000121)		
25	2/7/2007 4:36:26 PM	Attempt	Reader (0014f5000121)	UNKNOWN <Keypad (...)	
26	2/7/2007 4:41:42 PM	Attempt	Reader (0014f5000121)	UNKNOWN <Keypad (...)	
27	2/7/2007 4:48:59 PM	Reader Offline	Reader (0014f5000121)		
28	2/7/2007 4:49:29 PM	Portal Offline	PORTAL (Portal (0014...		
29	1/9/1970 2:40:29 PM	Attempt	Reader (0014f5000121)	UNKNOWN <Keypad (...)	
30	1/9/1970 2:40:29 PM	Attempt	Reader (0014f5000121)	UNKNOWN <Keypad (...)	
31	2/17/2007 8:04:59 AM	Set Clock	Reader (0014f5000121)		
32	2/17/2007 8:12:13 AM	Attempt	Reader (0014f5000121)	UNKNOWN <Keypad (...)	
33	2/17/2007 8:12:26 AM	Attempt	Reader (0014f5000121)	UNKNOWN <Keypad (...)	
34	2/17/2007 8:13:56 AM	Attempt	Reader (0014f5000121)	UNKNOWN <Keypad (...)	
35	5/11/2007 8:43:33 AM	Reader Offline	Reader (0014f5000121)		
36	5/11/2007 8:43:41 AM	Portal Offline	PORTAL (Portal (0014...		
37	5/11/2007 8:43:41 AM	Portal Offline	PORTAL (Portal (1111...		
38	6/13/2007 8:01:21 AM	Portal Offline	PORTAL (Portal (1111...		
39	10/1/2007 1:05:08 PM	Portal Offline	PORTAL (Portal (1111...		
40	10/25/2007 9:50:17 AM	Portal Offline	PORTAL (Portal (1111...		
41	11/1/2007 11:30:11 AM	Portal Login Attempt	UNKNOWN (0014f500...		
42	11/1/2007 11:30:21 AM	Portal Login Successful	UNKNOWN (0014f500...		
43	1/1/1970 12:00:31 AM	Alarm Cleared (ALL)	Reader (0014f5000121)		
44	1/1/1970 12:00:37 AM	Alarm Cleared (ALL)	Reader (0014f5000121)		
45	1/1/1970 12:01:52 AM	Logon	Reader (0014f5000121)	UNKNOWN <Keypad (...)	
46	11/1/2007 1:35:26 PM	Set Clock	Reader (0014f5000121)		
47	11/1/2007 1:36:36 PM	Configuration Updated...	Reader (0014f5000121)		
48	11/1/2007 1:36:41 PM	Configuration Updated...	Reader (0014f5000121)		
49	11/1/2007 1:36:50 PM	Configuration Updated...	Reader (0014f5000121)		
50	11/2/2007 7:48:57 AM	Reader Offline	Reader (0014f5000121)		
51	11/2/2007 7:49:01 AM	Portal Offline	PORTAL (Portal (0014...		
52	11/6/2007 10:37:16 AM	Portal Offline	PORTAL (Portal (1111...		
53	11/7/2007 6:55:18 AM	Portal Offline	PORTAL (Portal (0014...		
54	11/8/2007 6:44:54 AM	Portal Offline	PORTAL (Portal (0014...		

User: Admin

System transactions such as changing an access level or clearing an alarm display in blue on a white background. To review and respond to alarms, select the Alarms Tab.

Alarms Tab

When an alarm is triggered, such as a door is blocked open or forced entry, the system creates an alarm record. When you select the Alarms Tab, unanswered alarms display in red and activate an alarm sound .wav file on your computers sound system. When you “silence” an alarm in WAMS Transactions, you are simply telling the system that you have recognized the alarm condition. The alarm sound .wav file will stop on your computer system for that alarm and the display color changes to yellow. A log will be generated as to when the alarm was silenced. The user can add a comment to this log to further define the incident.

Remember, when you “Silence” an alarm in WAMS Transactions, you are only silencing a .wav file; you are not resolving the problem. It is important to establish Alarm Response protocols within your facility and follow up with action. See Responding to Alarms on page 24 for more information.

Transaction Types

The WAMS database records transactions by category. Under normal operating conditions, the most common transaction types will be Entry and Request to Exit. The system recognizes various alarm and status categories, such as:

- Alarm Cleared (All)
- Alarm Cleared (Forced Entry)
- Anti-Tamper

Organizing and Sorting Transactions

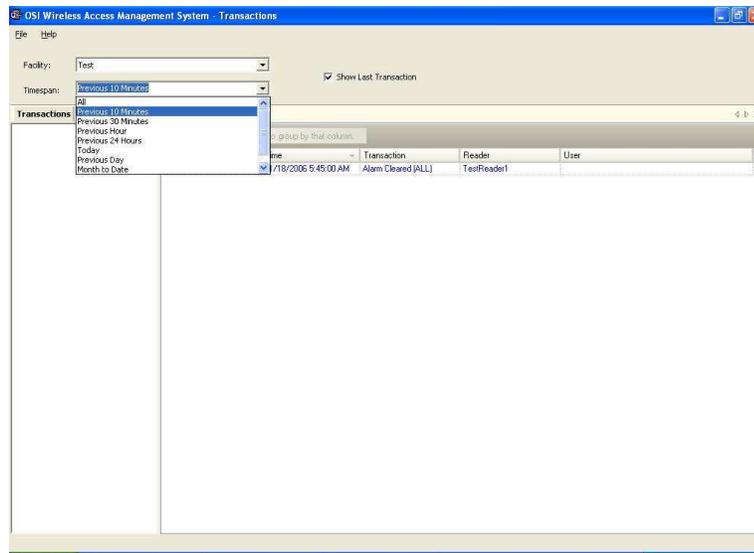
WAMS makes it easy to manage high transaction traffic. You could view every transaction in the system, real time. However, in large systems where hundreds of transactions can occur in a very short time, you may want to limit the transactions displayed, or group them in a way that makes sense for system activity. For example, you can limit the transactions list to only those that occurred in the last ten minute timespan; you can sort ascending or descending by column header; and you can arrange the columns in any order you wish. In addition, you can create a hierarchy, rather than a columnar view.

Display by Timespan

By default, WAMS Transactions displays all transactions in the order they occur. If you are monitoring all transactions, you may want to simply watch them as they occur. However, in large systems, your effort may best be served by limiting transactions to only those that have occurred in the previous ten minutes, or previous hour. WAMS gives you a number of options from All to year to date.

To set the display timespan:

1. In the Transactions Tab, select the Facility you wish to monitor.
2. Under Timespan, select the timespan you wish to display from the drop-down list. The display list on the right changes to reflect your selection.



NOTE: You can choose to always show the last transaction, no matter how you configure your display. Select *Show Transaction at the top of the display*.

Sort by Column Header

You can sort WAMS Transactions by column header in ascending or descending order. This is helpful, depending on what you are looking for. If you simply want to watch transactions in the order they occur, the default setting—sorted by ID, descending—will display the most recent transaction on the top line of the list. However, if you have an interest in viewing all the activity of a particular user, you can sort alphabetically by User credential. As with common database programs, you can move the columns in the column header to any order you wish. WAMS Transactions will remember your changes and display in the new order when you next open the program.

View Transactions in Tree Levels

You can display transactions similar to the way you view the Facility Tree in WAMS Configurator. This is useful to minimize and organize the amount of data you view at one time.

Transaction: Forced Entry

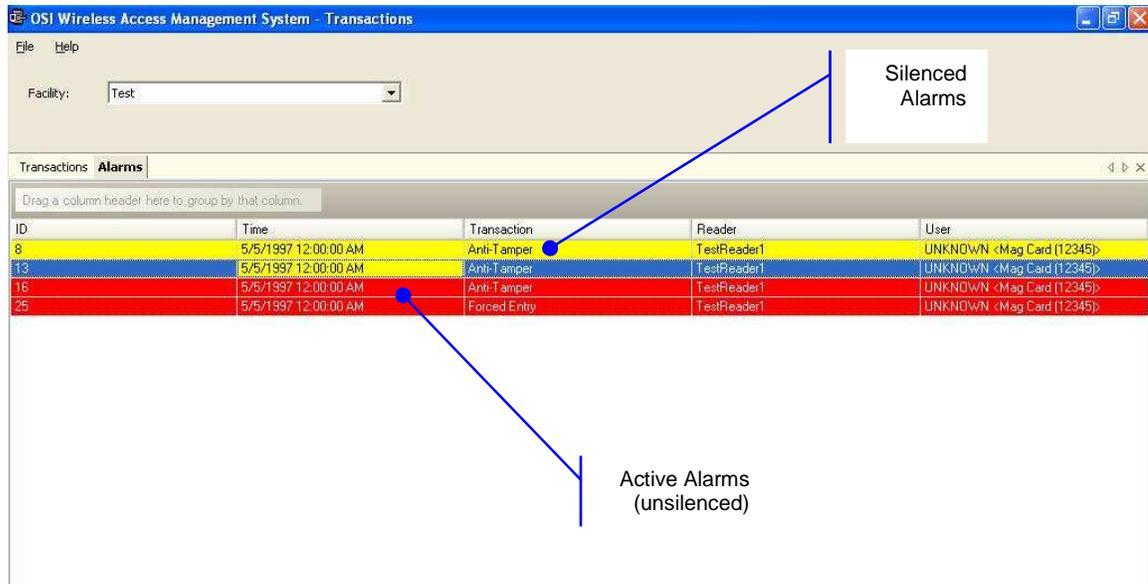
ID	Time	Transaction	Reader	Group Na...	User
25	5/5/1997 12:00:00 AM	Forced Entry	TestReader1		UNKNOWN <Mag Card (12345)>
3	5/5/1997 12:00:00 AM	Forced Entry	TestReader1		UNKNOWN <Mag Card (12345)>

In this example, we placed Transactions at the top of the tree; however, you can place them in any hierarchy you wish. When you select the plus sign next to the top level, the second and third level items expand to display. It's easy to create a Transactions Tree: simply drag and drop the column headers into position.

Responding to Alarms

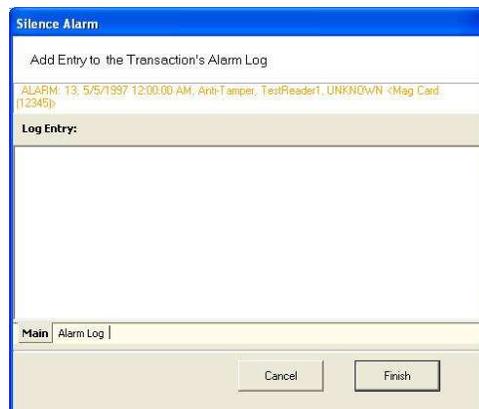
When an alarm occurs, the system immediately displays it in red in the Transactions Tab. The alarm will be categorized as either an Anti-Tamper or a Forced Entry type. At this point, you will take action according to your facility's security plan. In a small facility, you may simply dispatch a person to physically investigate the source of the alarm. In larger facilities with I/O devices in the system, the alarm may trigger a video recorder, a lighting plan, or other I/O device. In either case, you will respond to the alarm in WAMS Transactions using the alarms tab.

As with the Transactions Tab, you can sort the alarms in ascending and descending order with a column, and change the order in which the columns display, and create an Alarms Tree.



To respond and silence an alarm:

1. Select the Alarms Tab.
2. Double-click on an active alarm (displaying in red). The Silence Alarm text box opens at the Alarm Log tab. Alarm details display in the message area.
3. To add an entry to the log, select the Main tab.



4. Place the cursor in the text box and enter a comment; for example, dispatched technician to inspect reader.
5. Select **Finish**. In the Alarms tab, the alarm line changes from red to yellow and the alarm sound stops.

You can continue to add comments in the alarm's log until the condition is resolved.

To update or review the status of an alarm:

1. In the Alarms Tab, double click the alarm. The Silence Alarm text box opens.
2. Select the Alarm Log Tab. All comments regarding the alarm are recorded.
3. Select the Main Tab to enter a new comment.
4. Select **Finish** to close the text box and return to the Alarms Tab.

WAMS Statistics Monitor

The Statistics Monitor is a powerful tool that displays a real-time, color coded overview of system performance. When you set up your new system, and want to monitor ongoing system performance, you will use the WAMS Statistics Monitor. Statistics Monitor is primarily a System Administrator tool. For more information about this application, please see the WAMS Administrator's Guide.

USING WAMS REPORTS

You can view a wide variety of reports based on data collected in WAMS Configurator and WAMS Transactions. Access WAMS Reports from the Applications menu at the top of the WAMS Configurator Main Screen.

Reports Overview

WAMS provides seven reports that you can modify.

USER REPORTS

- **Users of Readers** – Generate a report that lists all readers and the users currently assigned to them, or you can specify a particular reader and view only the users for that reader.
- **Users of Groups** - Generate a report that lists all user groups and the users currently assigned to them, or you can specify a particular user group and view only the users for that group.
- **Users Entry Log** – Generate a report that lists user entry data for all users and all a readers, or you can specify which readers and users to list. You can also specify a timespan or Begin and End dates on which to report.
- **Users Entry/Exit Log** - Generate a report that lists user entry/exit data for all users and all a readers, or you can specify which readers and users to list. you can also specify a timespan or Begin and End dates on which to report.

ALARM REPORTS

- **Alarms Log** – Generate a report by alarm for all readers in all timespans, or specify which alarms, timespans, or Begin and End dates.
- **Readers Alarms Log** – Generates a report by reader for all alarms in all timespans, or specify which readers, timespans, or Begin and End dates.

TRANSACTION REPORTS

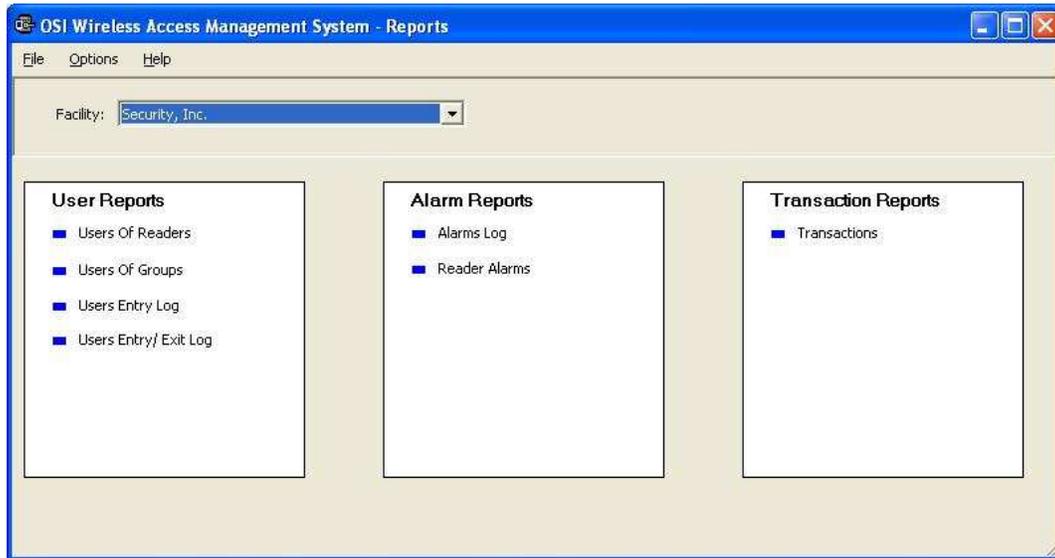
- **Transactions** – Generate a report for all transactions at all readers for all users during all timespans, or specify which transactions you wish to list.

Creating Reports in WAMS

The first step in creating reports in WAMS is to configure report settings. Here you can enter your company name and include a picture or logo that will be included in any files exported or printed from the application. Once you have configured your report settings you are ready to choose a report type and generate the report. From there you can print the report, or export the report to any number of file formats such as .doc, .rtf, .rpt, etc.

To get started, select Applications>WAMS Reports from the WAMS Configurator main menu.

Once you enter your login and password, the WAMS Reports main screen opens.



Configure Report Settings

You can include your company or organization name and logo with any report. WAMS supports both .bmp and .jpg image formats.

To configure report settings:

1. In the Facility box, select the Facility you wish to create the setting for.
2. Select **Options>Report Settings**. The Set Company Name and Logo for Reports dialog box opens.



3. In the Company Name box, type in the company name you wish to appear on your reports.

4. Under Company logo, click the **Change** link. Use the Select Logo browser to navigate the file you wish to include.
5. Click **Open**. The file is now uploaded to the WAMS Reports settings.
6. Click **Finish** to save your settings and begin working with Reports.

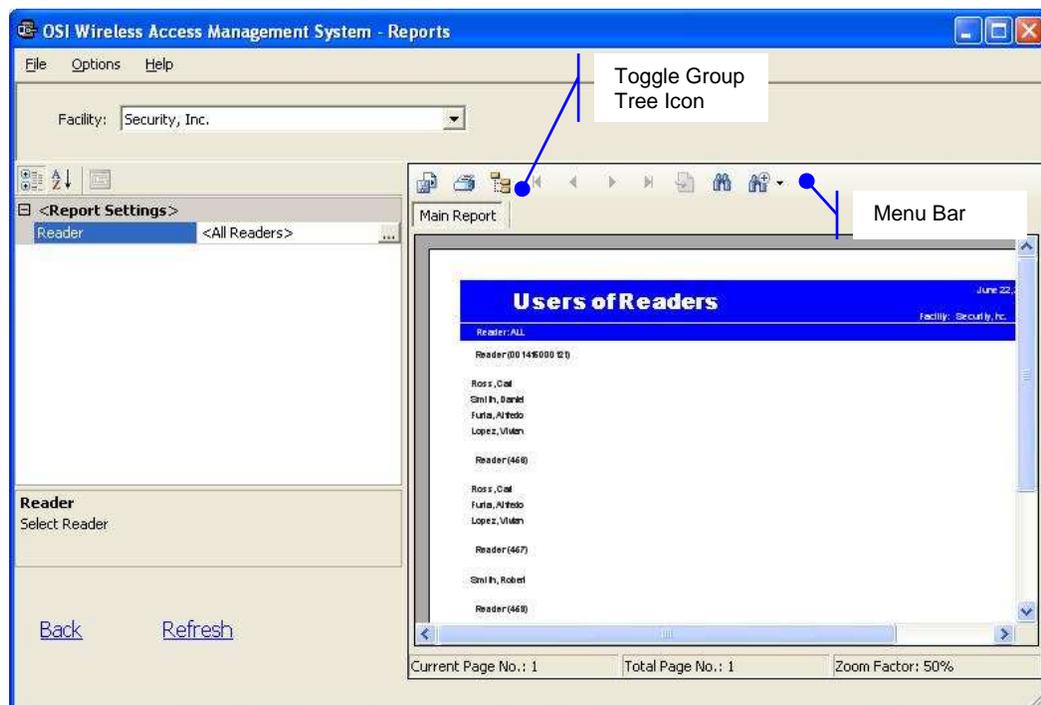
Generating a Report

This section presents steps to create some example reports. Once you are familiar with the basic operations, you will be able to create your own reports using the selections available in WAMS Reports. First we'll look at a Users of Readers report with All Users selected. Then we'll look at a filtered report using the options under the Report Settings categories.

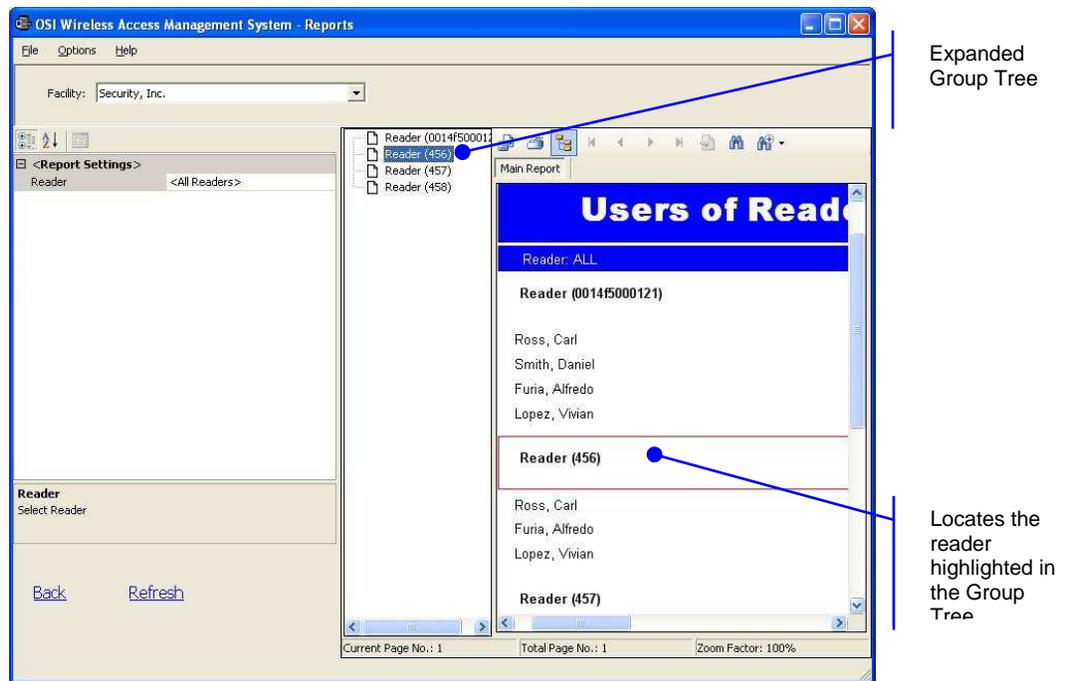
NOTE: *The Reports application won't show much data until you have configured your system, added Users and User Groups, and begun collecting transactions. Once this occurs, you can experiment with the options to get the reports that will be most significant for your operation.*

To Generate a Report:

1. In the WAMS Reports main screen, under the User Reports box, click on Users of Readers. WAMS Reports opens at the basic users of Readers Reports generator.
2. In the Facility box, select the Facility you wish to report on.
3. Available report settings are listed on the left, and the results are shown on the right. For this particular report, the default will be <All Readers>.



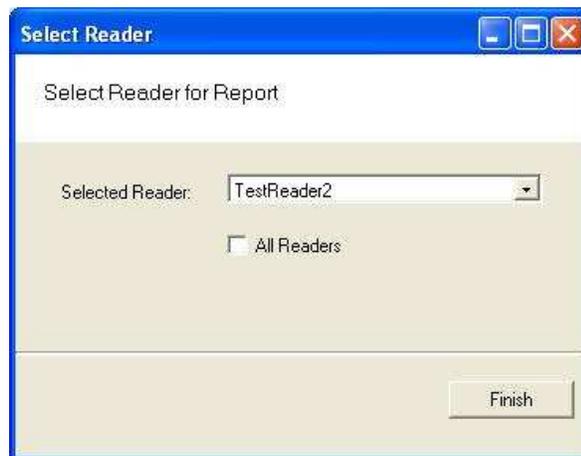
4. Use the scroll bars to view the data, use menu icons to export, print, scroll through multi-paged reports, or use the Zoom tools to get a closer look.
5. If you have a large number of readers, Click the Toggle Group Tree icon and highlight a specific reader to jump to its section in the report.



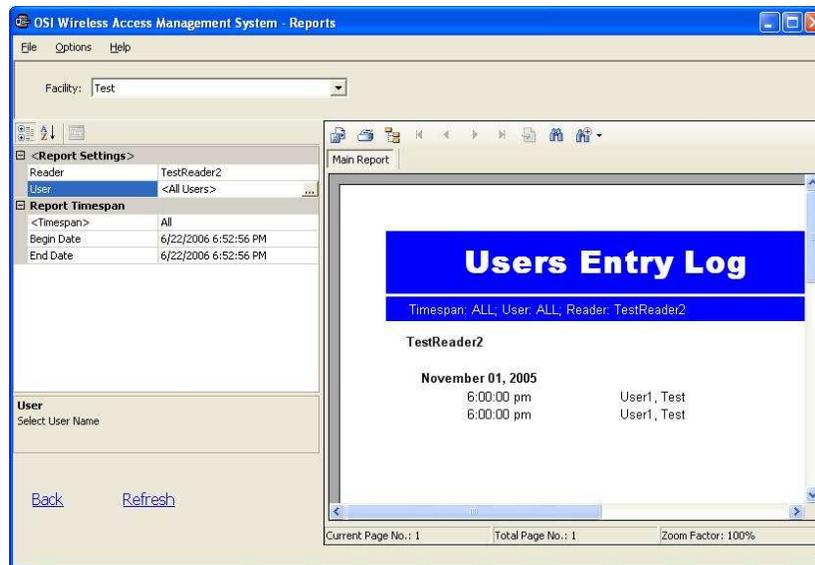
6. Click **Back** (bottom left of screen) to return to the Report Generator screen.

To create filtered report:

1. In the WAMS Reports main screen, select the Facility you wish to report on. In our example, we created a facility called Test.
2. Under the User Reports box, click on Users Entry Log. In this report set up, more selections are available for this report than for the Users of Readers report, including Reader, User, and Report Timespans. You can use any or all of these selections to filter your report. Each report type will have different selections available depending on the data available for the report. The defaults are always All. In the following example, we are filtering for Test Reader2, All Users, and All Timespans.
3. Under Report Settings, click on the Reader field then click the ellipsis button. The Select Reader dialog box opens.

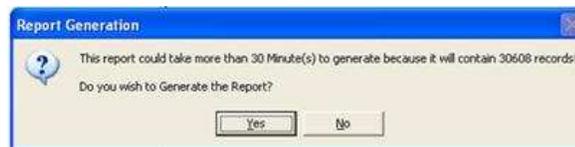


4. Clear the All Readers box just below the drop-down list box.
5. Select the reader you wish to filter for from the drop-down list.
6. Click **Finish**. The report results will display data for only the reader you selected.



Generating Larger Reports

The more records you include in your report, the longer the report will take to generate. During report generation, you can use other WAMS applications; however, you can generate only one report at a time in the Reports application. If you define a report that will take more than 30 minutes to generate based on the records included, WAMS will present the following message:



In the example, WAMS detects that the defined report contains about 30,000 records and will take more than 30 minutes to generate. If this is acceptable, simply select **Yes** and the report will be generated. Select **No** if this is an inconvenient time to generate the report, or review your report definitions to see if you can further filter the report and still get the information you need. When you select Yes, the report begins to generate and WAMS displays the Elapsed Time as the report runs.



Printing and Exporting Reports

Once you are satisfied with your report, you can print to a local or networked printer, or export the report in several formats. Your results will be determined by the options you select and how you wish to use the data. For example if you export to an Excel[®] file, you may get a different formatting result than if you export to an Adobe Acrobat[®] file or print directly from WAMS. However, you may wish to export to an Excel file and use the data in another format.

The following example was printed from an Adobe Acrobat .pdf file exported from WAMS reports. It retains all the formatting as displayed in WAMS Reports.

June 22, 2006
Users of Readers
Facility: Security, Inc.

Reader: ALL

Reader (0014f5000121)

Ross, Carl
Smith, Daniel
Furia, Alfredo
Lopez, Vivian

Reader (456)

Ross, Carl
Furia, Alfredo
Lopez, Vivian

Reader (457)

Smith, Robert

Reader (458)

Denver, Fred	Ross, Carl	Smith, Robert
Carlson, Betty	Furia, Alfredo	Lopez, Vivian


Wireless Access Management System
Page 1

To print a report:

1. Create the report using the features described in the previous sections.
2. Click the Printer icon in the menu bar.
3. Navigate to the printer you wish to use.
4. Print using the appropriate actions for the chosen printer.

To export a report:

1. Create the report using the features described in the previous sections.
2. In the menu bar, click the Export Report option.
3. In the Export Report dialog box, select a format type from the drop-down list. The available types are:
 - Crystal Reports (*.rpt)
 - Adobe Acrobat (*.pdf)
 - Microsoft Excel (*.xls)
 - Microsoft Excel Data Only (*.xls)
 - Microsoft Word (*.doc)
 - Rich Text Format (*.rtf)
4. Navigate to the location you wish to export to.
5. Enter a filename for the file.
6. Click **Save**.

Now you can use the report in any manner you wish, depending on the format exported.

Using Dialup Networking

Set up and use of Dialup Networking is described in Appendix A of the Administrator's Guide.

Using WAMS System Administrator

You can archive and restore data and import data from a legacy OFM Database or comma-delimited file using the System Administrator application. You must have Administrator privileges to use this tool. Complete instructions are presented in the Administrator's Guide.