Contents

Chapter 1: Getting Started with the Device Management Server ..................... 4
Management Server Product Overview .......................................................... 4
    Deployment ......................................................................................... 5
    Management ...................................................................................... 5
    Monitoring ....................................................................................... 5
    Logging/Tracking .............................................................................. 5
    Security ............................................................................................ 5
       Secure Access .............................................................................. 6
Device Enrollment ......................................................................................... 6
Logging On to the Management Server ......................................................... 6
Troubleshooting .......................................................................................... 7
Chapter 2: Monitoring and Managing Devices ............................................... 9
Chapter 2: Monitoring and Managing Devices ............................................... 9
Understanding the Reporting Page .............................................................. 9
    Report and Display Options ................................................................ 9
    Device Specific Information .............................................................. 11
Searching for Devices .................................................................................. 12
Filtering Devices by Merchant .................................................................... 12
Viewing Health Status and Activity Reports ............................................... 12
    Viewing Status Reports .................................................................... 13
    Viewing Activity Logs ..................................................................... 14
Viewing the Network History of Devices ..................................................... 15
    Polling History Page ....................................................................... 15
    Product Status Page ......................................................................... 16
    Firmware History Page ..................................................................... 17
    Config History Page ......................................................................... 17
    Diagnostics History Page .................................................................. 18
       Managing User Options for POSLynx Devices ................................ 20
Statistics History Page ............................................................................... 23
MID/TID Data Page .................................................................................... 23
Modifying Devices ....................................................................................... 24
<table>
<thead>
<tr>
<th>Chapter 3: Configuring Devices</th>
<th>28</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing Device-Specific Configuration Files</td>
<td>28</td>
</tr>
<tr>
<td>Modifying Configuration Files</td>
<td>29</td>
</tr>
<tr>
<td>Saving Configuration Files</td>
<td>30</td>
</tr>
<tr>
<td>Accessing Config Files: 3 Ways</td>
<td>30</td>
</tr>
<tr>
<td>Saving Configuration Files as Templates</td>
<td>30</td>
</tr>
<tr>
<td>Chapter 4: Managing Profiles and Users</td>
<td>31</td>
</tr>
<tr>
<td>Managing Profiles</td>
<td>31</td>
</tr>
<tr>
<td>Modifying Profiles</td>
<td>32</td>
</tr>
<tr>
<td>Changing Profile Passwords</td>
<td>33</td>
</tr>
<tr>
<td>Customizing Profile Logos</td>
<td>34</td>
</tr>
<tr>
<td>Managing Users</td>
<td>34</td>
</tr>
<tr>
<td>Adding New Users</td>
<td>34</td>
</tr>
<tr>
<td>Modifying Users</td>
<td>36</td>
</tr>
<tr>
<td>Deleting Users</td>
<td>36</td>
</tr>
<tr>
<td>Chapter 5: Managing Merchant Accounts</td>
<td>38</td>
</tr>
<tr>
<td>Adding New Merchants</td>
<td>38</td>
</tr>
<tr>
<td>Modifying Merchants</td>
<td>40</td>
</tr>
<tr>
<td>Deleting Merchants</td>
<td>40</td>
</tr>
<tr>
<td>Associating Devices to a Merchant</td>
<td>41</td>
</tr>
<tr>
<td>Associating One Device to a Merchant</td>
<td>41</td>
</tr>
<tr>
<td>Associating Multiple Devices to a Merchant</td>
<td>43</td>
</tr>
<tr>
<td>Adding a Merchant Logo to the Merchant View</td>
<td>46</td>
</tr>
</tbody>
</table>
Chapter 1: Getting Started with the Device Management Server

This document provides instructions for using the Device Management Server as an ISO Administrator and describes the following functions:

- Monitoring and Managing Devices
- Configuring Devices
- Managing Profiles and Users
- Managing Merchant Accounts

Management Server Product Overview

The Device Management Server is a web-based network configuration manager used by VARs, ISOs, and help desks to support merchants and to simplify device and network support of remote access. Its user interface guides the user through the steps required to provision, configure, and monitor IPocket232 devices. The management server tracks devices through their complete lifecycle as they move from manufacturing to a Partner’s inventory and onto the customer site.

The key benefits of the Management Server are:

- Common tasks are completed remotely.
- No on-site visits required for configuration, software upgrades, and deployment.
- Available 24/7 for any location.
- Improves reliability by monitoring network and terminal status, with alerts for failures.
- Features a security Audit log of all activities by users, contributing to the solution’s PCI DSS compliance.

The Management Server assigns products shipped by iPocket232 to the receiving Partner/ISO. These products are then associated to particular merchants by the Partner/ISO. The management server then allows for the provisioning of these appliances. The management server also manages the customer’s communication links, allowing help desks to quickly identify potential problems and assign resolution of the problem to the appropriate supplier.

Designed to work with POS Lynx series payment appliances and other IPocket232 products, such as the iPocket232 and the Ether232DUO, the management server is the driver behind our unique deployment, management, monitoring and security features.
Deployment
Recognizing that deployment of new technology can be a costly drain on technical resources, the Management Server was designed to streamline the process. Each POSLynx unit can be deployed easily by the IPocket232 Partner, without onsite technical assistance. When the POSLynx device is plugged in, it automatically calls the Management Server to download its configuration, which has been set up in the Management Server by the merchant’s service provider (ISO, dealer, processor, or network provider). This feature means installation is virtually plug-and-play for the merchant, and saves thousands of dollars in onsite technical support costs, particularly in larger deployments with multiple sites.

Management
By leveraging the data delivered by the Management Server, merchants and their support providers can resolve problems quickly and cost effectively, with minimal downtime. To simplify remote support, the Management Server has been designed to allow help desk applications to interface to this data through standard Web services. Additional management features offered by the Management Server include asset management and version control, configuration storage, search and download capabilities, and application downloads.

Monitoring
With the Management Server, VARs and other first line support providers are the first to know when a customer’s site is down, and can often identify the source of the problem before any significant downtime has occurred. The Management Server is always working in the background, monitoring the POSLynx device activities on the network. It collects data from the POSLynx device at regular pre-set intervals, which is used to monitor the health of the device and its network. Data collected by the Management Server includes network status, POSLynx device status, transaction data, log files of device activity, and details on users and their activities.

Logging/Tracking
The Management Server is an invaluable tool when an audit trail is needed to understand actions taken with respect to a device. The Management Server provides the following types of logging/tracking:

- **Audit log** - a comprehensive log of all activity on the system, including log on, log off, inventory, and configuration change activities.
- **Product Status** - displays a history of commands issued, and in-progress commands and their outcome, ordered by time and date. This page also displays details such as the IP address and network status changes issued to a selected device.

Security
Cardholder security is among the payment industry’s most critical issues. The Management Server has been designed to facilitate ongoing PCI compliance for merchants with two key features:
The Management Server does not store complete cardholder data. In addition, the POS Lynx device with the Management Server helps enforce PCI compliance, with features such as passwords which automatically expire in a set number of days.

The Management Server is updated on an ongoing basis, as cardholder security requirements change. If PCI DSS standards change, the Management Server helps users manage the updates or configuration changes easily.

As nearly all devices will be contacting the Management Server from within secure networks, The Management Server has been designed to receive calls from the end device, requesting new actions and updating the Management Server server. The actions requested by the products are stored in the Management Server by authorized users awaiting contact from the end device.

**Secure Access**

The Management Server provides several layers of access:

- **Administration:** With full access to all units (add units, feature keys). Typically reserved for IPocket232 users. Can be used by Partner Admin if the Management Server is hosted by Partner.
- **ISO Admin:** Can add new users within Partners.
- **ISO Users:** Can view diagnostics, statistics, add configurations, and upgrade firmware.
- **ISO Operations/ISO Dealers:** Same as ISO User but for only one group of merchants within an ISO account.
- **Merchant:** Access to Merchant data. Provides access to Merchant Reporting application.
- **Merchant Select:** Access to all stores enrolled in Merchant Reporting section.
- **Limit access to certain IP addresses:** Only allows access to the Management Server account from IP addresses listed.

**Device Enrollment**

When a device is shipped from the manufacturing facility or warehouse, it has been assigned a unique Serial# (MAC ID). The MAC ID from each device shipped in an order will be assigned by IPocket232 to the responsible Partner (that is the ISO, VAR, or other party responsible for deploying and configuring the devices), and will be accessible to the Partner as soon as they have been assigned, regardless of whether the devices have been received at their destinations. The Partner can only access those units with MAC IDs that have been assigned to them.

**Logging On to the Management Server**

After your IPocket232 product has been shipped to the IPocket232 Management Server, you will receive an email from sales@ipocket232.com indicating a URL, username, and temporary password for your account.

**To Log On to the Management Server**

1. In a browser, enter the URL provided in your confirmation email.
   The Login page appears.
2. Enter your **Username** and **Password**, and then click **Login**.

**IMPORTANT:** The first time a user logs on to the Management Server using these temporary credentials, they will be prompted to change their password. To be PCI-compliant, passwords must be at least seven (7) alphanumeric characters in length, contain at least one uppercase character, and one numeric character. Thereafter, in accordance with the PCI standard, the user will be prompted to change passwords every 90 days.

If you have problems logging in, your account may already have been logged in from somewhere else. In this case, you'll need to wait for the Management Server to disconnect that session. However, if you accidentally close a session while logged in, you can return to the login screen and press ‘Logout’ on the main menu. This will disconnect your previous session, allowing you to login again.

After changing passwords and logging in, the **Reporting Page** appears.

**Note:** To log off from the Management Server, click **Logout** on the main menu.

**Troubleshooting**

For assistance in solving problems with a POSLynx device and the Management Server, see the **Management Server Troubleshooting Guide** available on the Documentation page of [www.ipocket232.com](http://www.ipocket232.com) or contact sales@ipocket232.com.
Chapter 2: Monitoring and Managing Devices

You can monitor devices and manage devices in the Management Server as follows:

- Viewing device information
- Searching and filtering devices
- Viewing health status and activity reports
- Viewing the network history of devices
- Modifying device settings

Understanding the Reporting Page

After you log on to the Management Server, the Reporting page appears. The Reporting page is the main viewing portal for the lifecycle of your IPocket232 devices and has been designed to identify and prioritize devices with potential issues that require action. The default page provides details on your entire customer base, and lists the status of all devices assigned to you (or your assigned merchants) regardless of whether the devices have been received or powered at their destination.

**NOTE:** The Login as Merchant list allows you to login to the Merchant Reporting View.

On the Reporting page, you can track your device deployment, monitor devices after they are installed, and access information and data from devices. The Reporting page provides you with two types of information:

- Report and Display Options
- Device Specific Information

Note: To return to the main Reporting page from any other page, click Reporting on the main menu.

Report and Display Options

You can change the display and view reports on the Reporting page.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login as Merchant list</td>
<td>To log into the Merchant view as a merchant, select the merchant name from the dropdown menu.</td>
</tr>
<tr>
<td>Search by Serial Number box</td>
<td>To search for a specific device or a group of devices, enter any part of a MAC address (serial #), and then click Search. The Reporting page refreshes to display all devices containing the searched string. For more information, see Searching for Devices.</td>
</tr>
<tr>
<td>Choose a Report list</td>
<td>To filter the Reporting page to show only alerts, functional devices, inventory devices, or to select the audit report, select a report in the Choose a Report box. The Reporting page refreshes to display the selected option. For more information, see Viewing Health Status and Activity Reports.</td>
</tr>
<tr>
<td>Report by Merchant list</td>
<td>To display devices for all merchants or only for a specific merchant, select a merchant option in the Report by Merchant list. The Reporting page refreshes to display the selected option. For more information, see Filtering Devices by Merchant.</td>
</tr>
<tr>
<td>Location column</td>
<td>It is recommended you include a location description for each device to make it easier to identify a device. You can sort the Location column to quickly find a specific device or set of devices.</td>
</tr>
<tr>
<td>Sort by Column</td>
<td>To sort the rows in alphabetical order within a sortable column, right-click on a column heading. The Reporting page refreshes to show the selected column in ascending order. Note: You cannot manually sort the following columns: Report by Merchant Internal/External IP Diagnostics/Statistics Click again to switch the order (ascending/descending).</td>
</tr>
</tbody>
</table>
| Return to the default Reporting page view | To return to the default Reporting page from a specific view, do one of the following:  
  - Click Reporting on the main menu.  
  - Click the Back button on your browser. |
Device Specific Information
To get information related to a specific device, click on a row entry in a column in the ISO Admin view.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial # column</td>
<td>In the Serial # column, click on the serial number of a device. The Edit Product page appears where you can display and modify merchant, device, software, and configuration settings for the specified device. For more information, see Modifying Devices.</td>
</tr>
<tr>
<td>Internal IP column</td>
<td>You can choose between displaying the Internal IP address or the External IP address of devices. Internal IP: The IP Address on the WAN port of the device. External IP: The IP Address of the Internet gateway router. Click on a device for an Internal/External IP address to open the Polling History page. For more information, see Polling History Page.</td>
</tr>
<tr>
<td>Product column</td>
<td>The device identifier shows which device model or product is being used at a site. Click a device in the Product column to open the Product Status page where you can view a history of commands issued, commands in process, and their outcome, ordered by time and date. For more information, see Product Status Page.</td>
</tr>
<tr>
<td>Version column</td>
<td>The Version column shows the latest firmware download for a specific device. <strong>Note:</strong> A version number that is displayed inside brackets ie: (V2.13.053R) means that the command to download this firmware was not issued by the Management Server. Click a device in the Version column to open the Firmware History page where you can view a history of firmware application downloads to the selected device delivered via the Management Server. For more information, see Firmware History Page.</td>
</tr>
<tr>
<td>Config File column</td>
<td>The Config File column shows the latest configuration file imported in a device. <strong>Note:</strong> Configurations not performed through the Management Server will be displayed in the Config File column as &quot;Custom&quot; or &quot;Account Mismatch&quot;. Click a configuration (.cfg) file in the Config File column to open the Config History page where you can view a history of the configurations and the dates the .cfg files were sent to the selected device. For more information, see Config History Page.</td>
</tr>
<tr>
<td>Diagnostics column</td>
<td>The Diagnostic column displays the last date that a Diagnostic file was received by the Management Server. Click a date entry in this column and the Diagnostic History page appears, with the latest day’s diagnostics files. For more information, see Diagnostics History Page.</td>
</tr>
<tr>
<td>Statistics column</td>
<td>The Statistics column displays the last date that a Transaction Statistics file was received by the Management Server.</td>
</tr>
</tbody>
</table>
Attribute | Description
--- | ---
Click a date entry in this column to open the **Statistics History** page. For more information, see **Statistics History Page**.

**Searching for Devices**

You can search for a specific device or groups of devices.

**To search for a device**

1. On the main **Reporting** page, enter any part of a device's Serial# in the **Search by Serial #** box.
2. Click **Search**.

The **Reporting** page refreshes to display all devices containing the search string on the page.

*Note*: To return to the main **Reporting** page, click **Reporting** on the main menu.

**Filtering Devices by Merchant**

You can filter on the **Reporting** page to display only those devices assigned to a specific merchant.

**To filter devices by merchant**

- On the **Reporting** page, select an existing merchant in the **Report by Merchant** drop down list.

The pagerefreshes to display only those devices associated with the specified merchant.

**Viewing Health Status and Activity Reports**

Administrators can quickly and accurately locate problems on the network from the **Reporting** page. With the serial number and a standard web browser, you can view device activity, identify devices with potential issues that require action, and determine the location of a problem.

Each row on the **Reporting** page represents a device and is color coded to display the health status of the device at a glance. The devices are prioritized by status, with failures being displayed in **red** at the top of the page.

<table>
<thead>
<tr>
<th>Row Color</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Red** | Indicates a device that has failed to properly implement commands or has lost contact with the Management Server.  
*Note*: Select the IP address to open the **Polling History** page where you can view the networking history of the device. |
| **Black** | Indicates a device that has been enrolled (that is, assigned to a specific merchant) and is ready for deployment but is waiting for contact with the Management Server. |
| **Bold** | Indicates command(s) have been issued for device, and the Management Server is awaiting contact. New devices that are issued commands from inventory through the enroll products process will change to **Black Bold** after the changes are applied. |
You can filter the **Reporting** page to display two types of device information:

- The status of alerts, functional devices, unregistered devices, and devices in inventory. For more information, see [Viewing Status Reports](#).
- An audit log. For more information, see [Viewing Activity Logs](#).

### Viewing Status Reports

You can filter the **Reporting** page to display the following status reports:

- Alerts
- Functional devices
- Unregistered devices
- Inventoried devices

To view a status report

1. On the **Reporting** page, in the **Choose a Report** box, select one of the following:

   - **Select Status – Alerts**
     - The **Reporting** page refreshes to show a list of devices with existing (red and bold) alerts.

   - **Select Status – Functional**
     - The **Reporting** page refreshes to show a list of all active (green) devices.
Device Management Server Administrator Guide

- **Select Status - Unregistered**
  The **Reporting** page refreshes to show a list of any unregistered (purple) devices. Unregistered devices are in Inventory and make contact with the Management Server. The Management Server places these devices in an unregistered state.

- **Select Status - Inventory**
  The **Reporting** page refreshes to show a list of any (blue) devices in inventory.

**Viewing Activity Logs**

The Management Server maintains a comprehensive log of all activity on the system in the Audit log. You can view log on, log off, inventory, and configuration change activities within your account. You can view an Audit log to see activity in the Management Server or to drill down to a specific device and follow the trail of updates for the device.

In the Audit log, you can search on device details in two ways:

- By time. For more information, see **To search all events by time**.
- By MAC address. For more information, see **To search by MAC address**.

The following table describes the attributes of the Audit Log.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserID</td>
<td>The unique identification number of the user.</td>
</tr>
<tr>
<td>User Name</td>
<td>The name of the administrator who made the changes in the Management Server.</td>
</tr>
<tr>
<td>IP</td>
<td>The IP address of where the administrator who made the changes logged on from.</td>
</tr>
<tr>
<td>Serial #</td>
<td>The device that was modified.</td>
</tr>
<tr>
<td>Date</td>
<td>The date and time of day the device was modified.</td>
</tr>
<tr>
<td>Details</td>
<td>A description of the type of changes that were performed.</td>
</tr>
</tbody>
</table>

**To search all events by time**

1. On the **Reporting** page, in the **Choose a Report** box, select **Audit Log**.

The **Audit Log** page appears.

![Audit Log page screenshot]

---

14
2. In the **Search By** box, select a time/date criteria:
   - Today
   - Last Week
   - Last Month
3. Click **Search**.

   The **Audit Log** page refreshes to show a read-only report based on the selected time/date criteria.

   **Hint:** The Audit Log is useful for day to day operations. It provides detailed information on activities such as firmware upgrades (date, time, by whom) that help pinpoint the source of any problems.

To search by MAC address

1. On the **Reporting** page, in the **Choose a Report** box, select **Audit Log**.

   The **Audit Log** page appears.

   ![Audit Log Page](image)

   **Note:** The default view for the Audit Log page is for a single day.

2. In the **By Serial #** box, enter the MAC address or a portion of a MAC address for a device.
3. Click **Search**.

   The **Audit Log** page refreshes to show a read-only report based on the MAC address criteria.

### Viewing the Network History of Devices

For each device listed on the **Reporting** page, you can view the following historical details:

- Network status on the **Polling History page**
- Issued commands on the **Product Status page**
- Firmware downloads on the **Firmware History Page**
- Imported configurations on the **Config History Page**
- Diagnostic information on the **Diagnostics History Page**
- Statistical information on the **Statistics History Page**
- MID/TID information on the **MID/TID Data Page**

### Polling History Page

Internal IP is the IP Address on the WAN Port of the device and External IP is the IP Address of the Internet gateway router. Both IP Addresses are received from the poll messages sent by the device to the Management Server.
The Polling History page shows the history of polls – the current IP address of the device sent within each heartbeat message and listed on the page. Only commands that have been sent to the device are listed in this table. The polling history also shows if a unit is offline.

An entry in the Polling History table is made when:
- A device loses contact with the Management Server (that is, The Management Server does not receive a number of expected polls). The default setting is 3 missing heartbeats in a row.
- A device re-connects with the Management Server after having been ‘lost’.
- A new WAN IP address is assigned to the device.
- A change in status among those tracked in the Links Status column.

To view the Polling History page
1. On the Reporting page, click a device in either the Internal IP or External IP column. The Polling History page appears.
2. To view a status on the link, hover over WAN | NTP in the Link Status column.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPE</td>
<td>Displays the Management Server process running on device.</td>
</tr>
<tr>
<td>NTP</td>
<td>Displays whether the device has a time from the NTP server. Green=yes, Red=No.</td>
</tr>
<tr>
<td>WAN</td>
<td>Displays whether the device believes it has network connectivity. Green=yes, Red=No.</td>
</tr>
<tr>
<td>VXN</td>
<td>First Data connectivity.</td>
</tr>
</tbody>
</table>

Note: You can toggle between Polling History and Product Status by clicking on the associated link on each page.

Product Status Page
The Product Status page displays a history of commands issued, and in-progress commands and their outcome, ordered by time and date. The Product Status page displays details the IP address and network status changes issued to a selected device.

To view the Product Status page
- On the Reporting page, click a device in the Product column. The Product Status page appears.
Note: You can toggle between **Product Status** and **Polling History** by clicking on the associated link on each page.

**Firmware History Page**

The **Firmware History** page displays a history of firmware application downloads to the selected device delivered via the Management Server, and the time/date of the download when issued. It displays all firmware the Management Server becomes aware of via the version information on the device.

You can roll back to a previous firmware version. For more information, see [Modifying Devices](#).

**Note**: Firmware downloads not performed through the Management Server will be listed in the current **Version** status in parentheses.

To view the Firmware History page

- On the **Reporting** page, click a device in the **Version** column.

The **Firmware History** page appears.

**Config History Page**

The **Config History** page displays a history of the configurations sent to the device and the time/date they were accepted by the device.

**Note**: Configurations tagged as ‘Account Mismatch’, not performed through the Management Server are not displayed on the **Config History** page. "Custom" configurations may have been captured by the Management Server and stored under Diagnostics, within the precidia.cfg file of the diagnostic download.

To view the Config History page

- On the **Reporting** page, click a configuration (.cfg) file in the **Config File** column.

The **Config History** page appears.
For more information about device configuration, see Viewing Device-Specific Configuration Files.

Diagnostics History Page

The **Diagnostics History** page displays a list of zipped diagnostic (.gz) files and the time and date they were sent to the Management Server, either as a scheduled contact or other diagnostic file upload from the POSLynx device.

To view the Diagnostics History page

1. On the **Reporting** page, click a date in the **Diagnostics** column. The **Diagnostics History** page appears.

2. (Optional) To search across all displayed Diagnostics files, enter a pattern/string in the **Search** field, and click ‘Search’.

   The **Diagnostic File Search Results** page appears where you can select a file to view.
3. (Optional) To see the .gz file for a previous date, click **Previous Day**.

To return to the current date, click **Next Day**.

4. On the Diagnostics History page, click a Filename to open the Diagnostics Files page.

5. (Optional) To view all available files, select **Advanced**.

On the **Diagnostic Files** page, you can view a list of diagnostic files which provide you with important information to assist you in determining where breakdowns are occurring. These files can act as a resource in quickly resolving problems when they occur.

Some of the most common diagnostic files include:

- ***.cfg**: Displays current configuration of the device.
- **uid_pwd.file**: Manages POSLynx GUI users. For more information, see [Managing User Options on POSLynx Devices](#).
- **messages**: Displays system and application level log messages.
- **info.txt**: Displays the MAC ID and firmware version on the device at the time.
6. Click on any of the diagnostic files to open the Diagnostics File page for the selected file.

For example: Click **iptablesinfo.txt** and the following page appears.

![Diagnostics File Page](image)

**Note:** You can select a configuration (.cfg) file and save the file as a template or as a command. For more information, see [Saving Configuration Files](#).

### Managing User Options for POSLynx Devices

If the POSLynx Web GUI is temporarily not available, you can choose to modify the following POSLynx user options directly in the Management Server:

- Add a new POSLynx username and password
- Change an existing POSLynx username and password
- Set the permissions you want to assign to the username

For more information on the POSLynx Web GUI, see the appropriate user guide.

### To manage user options for a POSLynx device

1. On the **Reporting** page, click a date field in the **Diagnostics** column.
2. On the Diagnostics History page, select a Filename.

The Diagnostics Files page appears.
3. Click uid_pwd.file. The **Security – Change User** page appears.

4. In the **Change Username** box, do one of the following:
   - To select another existing username, select a username from the list.
   - To create a new username, select **New** and enter a unique username.

   **NOTE:** Username is not case sensitive. Password is case sensitive.

5. To change the password of an existing user or to add a password for a new user, enter **New Password** and **Confirm New Password**.

   **Note:** To be PCI-compliant, passwords must be at least seven (7) alphanumeric characters in length and contain at least one uppercase character and one numeric character.

6. In the **Capabilities** box, select the permissions you want to assign to the POSLynx user.

   The following table describes the configurable parameters of the **Capabilities** box.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View POSLynx Configuration</td>
<td>Allows a POSLynx user to view, but not change configuration parameters. Default: Checked. <strong>Note</strong>: If you clear this check box, the Change Port Configuration and Change System Configuration check boxes are not available.</td>
</tr>
<tr>
<td>Change Port Configuration</td>
<td>Allows a user to change port configurations, such as, devices, hosts, and TransNet links. Default: Checked.</td>
</tr>
<tr>
<td>Change System Configuration</td>
<td>Allows a user to view and change all parameters within System Configuration. Default: Checked.</td>
</tr>
<tr>
<td>View Logs</td>
<td>Gives the user access to Transaction logs on the GUI. Default: Checked.</td>
</tr>
<tr>
<td>Delete Logs</td>
<td>Allows a user to delete log files. Default: Unchecked.</td>
</tr>
<tr>
<td>Administer Other Users</td>
<td>Allows a user to add, delete, or administer users. Default: Unchecked. <strong>Note</strong>: You must select this check box to make the Persistent User option available.</td>
</tr>
<tr>
<td>Persistent User</td>
<td>Allows a user to be made persistent. The user will not be removed after 90 days of inactivity. <strong>Note</strong>: You must select this check box to make the Persistent Password option available. <strong>Important</strong>: Selecting this option will make the device non-compliant with PCI Guidelines and less secure.</td>
</tr>
<tr>
<td>Persistent Password</td>
<td>Allows the password of a user to be made persistent. The password will not expire after 90 days. <strong>Important</strong>: Selecting this option will make the device non-compliant with PCI Guidelines and less secure.</td>
</tr>
<tr>
<td>Transaction Operations</td>
<td>If selected, a Transactions Options box appears where you can select the payment options available for the user. In the Default Cash Register box, you can select the cash register (lanes) the user will be able to access and run transactions from. To allow the user to access all of the available lanes, select Any.</td>
</tr>
</tbody>
</table>

7. To save the changes, click **Save**.
8. Click Save As Command.

**Note**: If you click **Save As Command**, these changes will be downloaded the next time the device calls into the Management Server.

**WARNING:**
When configuring a user to access the web GUI in v 2.13, do not choose the ‘precidia’ user, since the user will be presented with the web GUI, and will no longer have access to Admin level functions. Instead, create a new user for web GUI access for payments.
Statistics History Page

The Statistics History page displays the latest statistics received by the Management Server for the posted date.

To view the Statistics History page

1. Click Reporting on the main menu bar.
2. In the Reporting page, toggle the ‘Diagnostic’ column to ‘Statistics’.
3. Click the date next to the device you want to view in the Statistics column. The Statistics History page appears.
4. (Optional) To view all transactions for a specific day, click the Calendar icon, choose a date and then click Submit.
5. (Optional) To export the transactions to a MS Excel file, click Excel Format.

MID/TID Data Page

The MID/TID Data page displays all details on the Merchant Identification (MID) and Terminal Identification (TID) data associated with a MAC Address (Serial#) for a specific ISO Admin user.

To view the MID/TID Data page

- On the ISO Admin tab, click View MID/TID on the left navigation bar.

The MID/TID Data page appears where you can view details for all merchant users in the ISO Admin user's group.
NOTE: This is very useful when you have merchants using multiple processors. The Protocol will tell you what merchants and devices are using which processors across your entire account.

Modifying Devices

Every device has a unique MAC address/Serial#. You can view and change settings for a specific device on the Edit Product page including:

- Modify assigned merchant and location
- Change the status of the device
- Upgrade to the latest firmware
- Choose a configuration template, edit it and store in the Management Server awaiting next device contact.
- Set or change intervals of contacts, polling, and statistics
- Reset commands on the device

Note: The modified settings will be sent to the device the next time it contacts the Management Server.

To modify a device

1. Do one of the following:
   - On the Reporting page, click an entry in the Serial # column.
   - On the ISO Admin tab, click Edit/Product on the left navigation bar, select a MAC ID from the list, and then click Continue.

The Edit Product page appears for the selected device.
2. To set commands and modify device settings, do any of the following on the **Edit Product** page:

<table>
<thead>
<tr>
<th>To</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Merchant Information box</strong></td>
<td></td>
</tr>
<tr>
<td>Change the merchant associated with a device</td>
<td>In the <strong>Merchant</strong> dropdown, select an existing merchant.</td>
</tr>
</tbody>
</table>
| Add or modify the location identifier of a device | In the **Location** box, enter the location of the device.  
*Note:* Including a location will help you quickly find a specific device or set of devices.  
*Hint:* You should always add a Location name that is specific to the Store/Lane, as Location is used to display and sort device transactions. |
| **Product Information box** | | |
| Change the status of the device | Select a status from the **Change Status** box.  
Options include:  
- *Move to Inventory* - Moves device into ISO’s general inventory.  
- *RMA Product* - Removes device from the ISO’s account.  
  *Note:* All data associated with this device will be lost to the ISO.  
- *Installation Pending* – Used if an ISO wishes to preconfigure a device and send to a merchant afterwards. Not useful for most accounts. |
| View the status history of a device | In the **Product Information** box, click **View Product Status**.  
The **Product Status** page appears. For more information, see **Product Status Page**.  
*Note:* You can toggle between the **Product Status** page and **Polling History** page by clicking on the associated link in each window. |
| View the networking history of a device | On the **Product Status** page, click **View Polling History**. |
To | Do this
--- | ---
device | The **Polling History** page appears. For more information, see [Polling History Page](#).

**Note**: You can toggle between the **Polling History** page and **Product Status** page by clicking on the associated link in each window.

**Command Panel**

<table>
<thead>
<tr>
<th>Change the firmware version,</th>
<th>In the <strong>Firmware</strong> box, select a version number of the application firmware you want to load on the device. <strong>NOTE</strong>: If the version number you require is not listed, contact IPocket232 Support at <a href="mailto:sales@ipocket232.com">sales@ipocket232.com</a> <strong>WARNING</strong>: Please contact IPocket232 if you are interested in using a new release you have not yet tried, as the load may include changes that alter some items or parameters you require.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Change the configuration file</th>
<th>In the <strong>Template</strong> box, select a configuration file/template (.cfg) to apply to the device. <strong>Important</strong>: It is critical that you select the correct configuration file. For more information, see <a href="#">Modifying Configuration Files</a>.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Change the predetermined interval of when the device sends diagnostic files (logs) and pulls updates</th>
<th>In the <strong>Contact</strong> box, select an interval. <strong>Note</strong>: The Contact interval for new installations should be set at shorter intervals until locations have stabilized, at which time they can be set to a less frequent interval. Recommended interval: 1 Hour.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Change the interval between polls (heartbeats) sent by the device to the Management Server</th>
<th>In the <strong>Polling</strong> box, select an interval. Recommended interval: 2 Min. <strong>NOTE</strong>: This setting will affect the duration that the location is down before the Management Server takes notice. If a 15 minute interval is chosen, the Management Server will alarm the device after 3 consecutive missed polls. If the device went offline just after the previous poll, the site could be down for nearly 60 minutes before it is alarmed on the Management Server.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Change the interval of when the transaction details are updated</th>
<th>In the <strong>Statistics</strong> box, select an interval. Recommended interval: 30 Min.</th>
</tr>
</thead>
</table>

**Device Reset Commands**

| Reset previously selected parameters for the device | Select a reset option. Options include:  
- Reboot Device  
- Restore Factory Defaults  
- Get Batch  
- Clear Batch |
|---|---|

3. To save all changes, click **Update**.
4. To return to the **Reporting** page, click **Reporting** on the main menu.
**Important:** Any device changes you have saved do not take effect immediately. The modified settings will be sent to the device the next time it contacts the Management Server, or upon next power cycle. The Polling Contact and Statistics periods are changed upon re-starting of the device.
Chapter 3: Configuring Devices

In the Management Server, you can:

- View all configuration files associated with a device
- Modify the settings of a configuration file
- Save a configuration file

Viewing Device-Specific Configuration Files

You can view all configuration files associated with a specific device in your network. The config files on the Management Server are the same as you would see if you logged into the device, with only a few specific exceptions.

To view all device-specific configuration files

1. On the ISO Admin tab, click View/Edit Config on the left navigation bar.
In the **Product Name** box, select a device type, and then click **Continue**.

The **Available <product> Configs** page displays all configuration files associated with the selected device type.

![Configuration Files Table]

**Note**: To modify the configuration files, see [Modifying Configuration Files](#).

## Modifying Configuration Files

You can modify the settings associated with a device's configuration file.

### To modify a configuration file

1. On the **ISO Admin** tab, click **View/Edit Config** on the left navigation bar.

![ISO Admin Tab]

**NOTE RE:** Other ISO Admin functions (inside red boxes above)

IPocket232 Inc. adds functionality that applies to specific customers or devices. For more information on this, please contact IPocket232 at sales@ipocket232.com.
In the **Product Name** box, select a device type, and then click **Continue**.

The **Available `<product>` Configs** page displays all of the configuration files associated with the selected device type.

**Important**: You must select a configuration (.cfg) file that matches the processing requirements of a specific device for a particular merchant user to ensure that you have the correct template set up. For assistance with setting up your configuration file, contact sales@ipocket232.com.

2. (Optional) To delete one or more configuration files, select the **Delete** check box for an associated .cfg file, and then click **Delete Checked**.

**Saving Configuration Files**

In the Management Server, you can save a configuration file in two ways:

- **Save as a Template**
- **Save as a Command**

**Accessing Config Files: 3 Ways**

There are three ways to access a config file in the Management Server:

1. In **ISO Admin**, choose **View/Edit Config**. In the next screen, choose the appropriate product from the 'Product Name' dropdown menu, and click 'Continue'. Click on the `.cfg` file from the list of **Available Configs**.

2. In the main **Reporting** screen, click on a config in the **Config File** column. In the **Config History** page, click on the `.cfg` config file.

3. In the main **Reporting** screen, click on a date in the **Diagnostics** column. In the **Diagnostics History** screen, click on a `.gz` file. In the **Diagnostics Files** screen, click on **precidia.cfg**.

**Saving Configuration Files as Templates**

You can make changes to an existing configuration (.cfg) file and then save it as a template for reuse and to be accessible for download into other devices.

Configuration files can be prepared as templates (as an example, one for each processor) and easily modified for unique Merchant IDs (MIDs) and Terminal IDs (TIDs).

To save a configuration file as a template

1. To open the **POSLynx device GUI** page, access the config using one of the methods in **Accessing Config Files: 3 Ways** above.
2. Once changes have been made (making sure to click Save button on each page), you can save as a template (choose Save as Template). **NOTE:** You can also save as a direct command to store the config and deliver to the device upon next contact. To do this, you would choose *Save as Command.*

3. Click **Save As Template.**

   The **Source Config** page appears.

   ![Source Config Page](image)

   - In the **New Filename** box, enter a name for the configuration file.
   - In the **Description** box, enter a unique description identifier for the file.
   - Click **Save As Template.**

   The .cfg file appears in the **Available Configs** list. The next time you open the **View/Edit Config** page, the new template will be available.

---

### Chapter 4: Managing Profiles and Users

#### Managing Profiles

In the Management Server, you can manage the following aspects of the ISO Admin user profile:
- Modify the profile
- Change the password of the administrative user for the account
- Customize the profile settings
Modifying Profiles
You can modify the Profile of the ISO Admin user.

To modify a profile
1. On the ISO Admin tab, click **Edit Profile** on the left navigation bar. The **Edit Profile** page appears.

2. To set commands and modify profile settings, do any of the following on the **Edit Profile** page:

<table>
<thead>
<tr>
<th>To</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contact Information box</strong></td>
<td>Modify the company associated with a profile</td>
</tr>
<tr>
<td>Modify the contact name for the company</td>
<td>In the <strong>Contact Name</strong> box, enter the name of the contact.</td>
</tr>
<tr>
<td>Add/modify the title of the contact</td>
<td>In the <strong>Contact Title</strong> box, enter a title for the contact.</td>
</tr>
<tr>
<td>Add/modify the shipping address of the company</td>
<td>Enter address information in the following fields:</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This information will be entered from the iPocket232 Customer Database, so it is important that Partners contact iPocket232 if this information</td>
<td>Shipping Address</td>
</tr>
<tr>
<td></td>
<td>City</td>
</tr>
<tr>
<td></td>
<td>State Prov.</td>
</tr>
<tr>
<td></td>
<td>Zip Postal Code</td>
</tr>
<tr>
<td>To</td>
<td>Do this</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| changes.                 | • Telephone
• Telephone 2
• Fax
• E-mail (NOTE: This email will receive any alerts sent by the Management Server) |
| Change the profile user password | See Changing Profile Password.                                         |

### Alerts Configuration box

| Send an email to the Profile user when specific alarms occur | Select the alarms that will trigger an email notification to the Profile user. Options include:
• **IP Address Change**
• **NTP Down/Up**
• **Dial-Backup** (triggered when dial back-up starts)
• **Batch Fail** (if a batch fails to close, an alert is sent to email in ISO Profile)
• **Batch Not Close (>3 Days)** (if a batch remains open for 3 days, an alert is sent to email in ISO Profile)
• **SN Changed** (for a Lane, if the serial number of the terminal has changed, an alert is sent to email in ISO profile) |
| Send an alert email when specific actions occur | These actions will always trigger an alert:
• **Firmware Download Failed**
• **Config Download Failed**
• **First Contact**
• **Device Contact Lost**
• **Device Contact Renewed** |
| Add a Source IP List (Restricts the Management Server access to select IP addresses) | In the Source IP List box, enter the logon IP address(es) from which valid users can log on to this account.
Note: If a logon IP address is not added to this list, the user/merchant user will receive an error message when they attempt to log on. The ISO Admin must add all logon IP address in this field.
Important: Multiple IP addresses must be separated by a comma (X.X.X.X,X.X.X.X).
WARNING: Adding only one incorrect IP address and saving this will disallow all user access to the account, as only access from this address will be allowed. |
| Customize the Profile with a logo | See Customizing Profiles. |

1. To save the profile changes, click **Update**.

### Changing Profile Passwords

You can change the password associated with a profile.

To change your Administrative account password

1. On the **ISO Admin** tab, click **Edit Profile** on the left navigation bar.
2. In the ISO Login Information box, click Change Password.

**Note:** To be PCI-compliant, passwords must be at least seven (7) alphanumeric characters in length, contain at least one uppercase character, and one numeric character.

**Note:** Usernames must be unique across the entire the Management Server and once assigned are not changeable by the user. Please contact IPocket232 Inc. if you wish to change your username.

4. Click Change Password.

The new password is saved.

**Customizing Profile Logos**

You can add or change the logo associated with a profile. The logo appears at the upper left hand side of the Management Server screens.

To customize a logo
1. On the ISO Admin tab, click **Edit Profile** on the left navigation bar.
2. At the bottom of the **Edit Profile** page is the **ISO Logo Configuration** field.
3. Click on the here link to add a custom logo.
4. In the **File Upload** box, select the graphic file for the logo, and then click **Submit**.

The logo appears on the **Reporting** page.

**NOTE:** If the logo is too large or does not appear as you would like it, please send the logo and the correct details to IPocket232 Support, requesting its addition to the ISO Profile.

### Managing Users

In the Management Server, you can manage the following aspects of user accounts:

- Add new users
- Modify existing users
- Delete users

#### Adding New Users

You can add a new user to the Management Server.

**To add a new user**

1. On the ISO Admin tab, click **Add/Edit User** on the left navigation bar.
2. In the **Select User** box, select **Add New User**, and then click **Continue**.
Enter the user contact details as appropriate.

In the **Password** box, a password is automatically generated for the new user. **Important:** The ISO Admin user should take note of the new username and password, as they must inform the new user of their **Username** and this temporary **Password**. When the new user logs on to the Management Server for the first time, they will be prompted to change their password. To be PCI-compliant, passwords must be at least seven (7) alphanumeric characters in length, and contain at least one uppercase character and one numeric character.

In the **User Type**, select one of the following user types:

- **ISO Operation**: Can access all devices in the ISO account.
- **ISO Dealer**: Can only access devices associated with a specific merchant user.

**Note:** If you select **ISO Dealer**, you must select an existing merchant in the **For ISO Dealer** list.

Click **Update**.

The new user is now available for selection on the **Add/Edit User** page.
Modifying Users
You can modify the contact details, password, and user type for an existing user.

To modify a user

On the ISO Admin tab, click Add/Edit User on the left navigation bar.
In the Select User box, select an existing user from the list, and then click Continue.
Modify the user information as required.

Note: Username is case sensitive.
To change the user password, click Change Password, enter a New Password and Confirm New Password, and then click Change Password.

Important: The ISO Admin user must inform the user of their Username and this new Password. The next time the user logs on to the Management Server using these credentials, they will be prompted to change their password. To be PCI-compliant, passwords must be at least seven (7) alphanumeric characters in length, contain an uppercase character, and one numeric character.

Click Update.
The user account is updated.

Deleting Users

1. On the ISO Admin tab, click Delete Merchant/User on the left navigation bar.
2. In the **Select Category** box, select **User**.

3. In the **Check Catalog** box, select the user you want to delete.
4. Click **Execute Delete**.

The page refreshes with the updated user list.
Chapter 5: Managing Merchant Accounts

Within the Management Server, merchant users are linked to a merchant account that provides access to the Merchant reporting view. There can only be one user per merchant account.

In the Management Server, you can manage the following aspects of merchant user accounts:

- Add new merchant
- Modify existing merchant accounts
- Delete merchant account
- Enroll products in merchant account

Adding New Merchants

You can create a new merchant account and then enroll the user in the Management Server. Once enrolled, the merchant can access transaction reporting and alerts on their products on the home page of the Merchant View application.

To add a new merchant

1. On the ISO Admin tab, click Add/Edit Merchant on the left navigation bar.
2. In Merchant Name box, select Add New Merchant, and then click Continue.

3. On the **Add Merchant** page, enter the contact details for the merchant to uniquely identify the merchant in the Management Server.

4. (Optional) To provide the merchant with access to the Merchant View application, select **Allow Merchant to view Report**, and do the following:

   - Enter a **Username**.
   - In the **Password** box, a password is automatically generated for the merchant user. **Important:** The ISO Admin user must inform the merchant user of their **Username** and this temporary **Password**. The first time the merchant user logs on to the Merchant View to see their devices using these credentials, they will be prompted to change their password. To be PCI-compliant, passwords must be at least seven (7) alphanumeric characters in length, contain at least one uppercase character and one numeric character.

   - In the **Reporting Style**, select either **Merchant View/Standard** or **Merchant View/Enterprise** depending on whether the user will have access to basic or advanced information. The default choice is **Merchant View/Standard**.

5. Click **Update** to save the new merchant user.
Modifying Merchants

You can modify the contact details, the password, and the user type for an existing merchant user.

To modify a merchant

1. On the ISO Admin tab, click Add/Edit Merchant on the left navigation bar.
2. In Merchant Name box, select an existing merchant from the list, and then click Continue.
3. Make any required changes, and then click Update.

Deleting Merchants

You can only delete a merchant that has no product association.

To delete a merchant

1. On the ISO Admin tab, click Delete Merchant/User/Alert on the left navigation bar.
2. In the Select Category box, select Merchant with No Product.
3. In the **Check Catalog** box, select the merchant you want to delete.
4. Click Execute Delete.
   The page refreshes with the updated merchant list.

**Associating Devices to a Merchant**

To prepare for installing a new device, you must first enroll the device in the merchant account.

You can associate devices to a merchant in two ways:
- Assign one device to one merchant. For more information, see **Associating One Device to a Merchant**.
- Assign multiple devices to one merchant. For more information see **Associating Multiple Devices to a Merchant**.

**Associating One Device to a Merchant**

You can select a single device and associate it to a merchant.

**To associate one device to a merchant user**

1. On the **Reporting** page, select a **Serial #** of an inventoried (blue) device.
   
   The Management Server ISO Administration page appears.

   ![Management Server ISO Administration](image)

   **Note**: To enroll a new device, you must first add the merchant to the Management Server. For more information, see **Adding New Merchants**.

2. In the **Merchant Name** box, select an existing merchant, and then click **Continue**.
   
   The **Device Enrollment** page appears.

   ![Device Enrollment](image)

   **Note**: To enroll a new device, you must first add the merchant to the Management Server. For more information, see **Adding New Merchants**.

3. On the **Device Enrollment** page, do the following:

<table>
<thead>
<tr>
<th>To</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add the location identifier of a merchant user</td>
<td>In the <strong>Location</strong> box, enter the location of the device. <strong>Note</strong>: Including a location will help you quickly find a specific device, especially in the Merchant view.</td>
</tr>
<tr>
<td>To</td>
<td>Do this</td>
</tr>
<tr>
<td>----</td>
<td>---------</td>
</tr>
<tr>
<td>Select the firmware version</td>
<td>In the <strong>Application Version</strong> box, select a version number of the application firmware you want to load on the device. <strong>Note</strong>: If the version number you require is not listed, contact iPocket232 Inc.</td>
</tr>
<tr>
<td>Select the configuration file</td>
<td>In the <strong>Config File</strong> box, select a configuration file/template (.cfg) to apply to the device. <strong>Important</strong>: It is critical that you select the correct configuration file. For more information, see <a href="#">Modifying Configuration Files</a>. <strong>WARNING</strong>: Configuration files chosen in this page cannot be viewed or edited prior to issuing the command. If you are at all unsure of the contents of the file, particularly the IP addressing scheme, do NOT choose the file here, but instead choose it from the Main Reporting screen, where it is viewable and editable prior to issuing to the device.</td>
</tr>
</tbody>
</table>
| To set a predetermined interval of when the device sends diagnostic files (logs) and pulls updates | In the **Scheduled Contact** box, select an interval. Options include:  
- 1 Hour  
- 3 Hours  
- 6 Hours  
- Daily  
- Never  
**Hint**: The Contact interval for new installations should be set at shorter intervals until locations have stabilized, at which time they can be set to a less frequent interval. Recommended interval: 1 Hour. |
| Set the interval between polls (heartbeats) sent by the device to the Management Server | In the **Polling** box, select an interval. Options include:  
- 2 Min  
- 5 Min  
- 15 Min  
- Never  
Recommended interval: 2 Min. |
| Set the interval when the device sends transaction statistics to the Management Server (and through the Merchant view) | In the **Statistics** box, select an interval. Options include:  
- 30 Min  
- 1 Hour  
- 2 Hours  
- 6 Hours  
- 12 Hours  
- Never  
Recommended interval: 1 Hour. |

4. Click Save Configuration.  
The device now appears as **Bold Black** on the **Reporting** page indicating that the device has been enrolled with a merchant (and, therefore, is no longer in inventory) and is waiting for contact with the Management Server.
You can confirm the status of the device (Awaiting Device Contact) in the Status Panel on the Edit Product page.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Status</th>
<th>Command</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware Upgrade</td>
<td>V2.12.755</td>
<td>Awaiting Device Contact</td>
<td>abort</td>
<td>abort</td>
<td></td>
</tr>
<tr>
<td>Configuration Download</td>
<td>Avh4.ini</td>
<td>Awaiting Device Contact</td>
<td>abort</td>
<td>abort</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** If you click **abort**, the aborted command will be removed.

### Associating Multiple Devices to a Merchant

If you have a number of devices you want to associate to a single merchant, you can enroll multiple devices at one time.

**Note:** To enroll one device to a merchant, see [Associating One Device to a Merchant](#).

To associate multiple devices to a merchant:

1. On the main menu, click **Enroll Products**.
   
The ISO Administration page appears.

2. In the **Merchant Name** box, select a previously created merchant.
   
   **Note:** To enroll a new merchant, you must first add the new merchant to the management server. For more information, see [Adding New Merchant](#).

3. In the **Product Name** box, select a device type (such as POSLynxDUO), and then click **Continue**. All available products of that device type are listed in the ‘Available’ box on the left hand side.

4. To allow the merchant to access a device, select all Available devices required using <Ctrl><Enter> to add single devices or <Shift><Enter> to select all products between the two selections. Click the **Associate** button for each device highlighted, and devices will appear in the **Associated** box.
Note: To remove a device from the Associated box, select the device in the Associated box, and then click Disassociate. The device moves to the Available box.

5. Click Continue, and then click Setup Config on the Association page.

6. To individually configure each device, select an existing merchant in the Merchant Name box, and then click Save Configuration. To configure all devices Associated in the previous steps, choose Copy to All Products.

The Device Configuration page appears.

**WARNING:** It is strongly recommended that when associating multiple devices with a merchant, ISO Admin users configure each device individually to ensure there are no errors in the configuration files. Alternatively, the ISO Admin can use a base template that ensures the correct IP addressing is assigned in the configs of all products.

**Hint:** If you are unsure about your configuration assignment, select all the other parameters, leaving Config File blank. This will set up all devices in the Merchant account, awaiting contact – and with the correct settings, in one step.
On the **Device Configuration** page, do the following:

<table>
<thead>
<tr>
<th>To</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add the location identifier of a merchant</td>
<td>In the <strong>Location</strong> box, enter the location of the merchant. <strong>Note</strong>: Including a location will help you quickly find a specific device, and is needed for the Merchant view sorting.</td>
</tr>
<tr>
<td>Select the firmware version</td>
<td>In the <strong>Application Version#</strong> box, select a version number of the application firmware you want to load on the device. <strong>Note</strong>: If the version number you require is not listed, contact IPocket232 Inc.</td>
</tr>
<tr>
<td>Select the configuration file</td>
<td>In the <strong>Config File</strong> box, select a configuration file/template (.cfg) to apply to the device. <strong>Important</strong>: It is critical that you select the correct configuration file. For more information, see Chapter 3: Configuring Devices.</td>
</tr>
</tbody>
</table>
| To set a predetermined interval of when the device sends diagnostic files (logs) and pulls updates | In the **Scheduled Contact** box, select an interval. Options include:  
- 1 Hour  
- 3 Hours  
- 6 Hours  
- Daily  
- Never  
**Hint**: The contact interval for new installations should be set at shorter intervals until locations have stabilized, at which time they can be set to a less frequent interval. Recommended interval: 1 Hour. |
| Set the interval between polls (heartbeats) sent by the device to the Management Server | In the **Polling** box, select an interval. Options include:  
- 2 Min  
- 5 Min  
- 15 Min  
- Never  
Recommended interval: 2 Min.                                                                 |
| Set the interval when the device sends transaction statistics to the Management Server | In the **Statistics** box, select an interval. Options include:  
- 30 Min  
- 1 Hour  
- 2 Hours  
- 6 Hours  
- 12 Hours  
- Never  
Recommended interval: 1 Hour.                                                                 |

7. **Click Save Configuration.**

The device now appears as **Bold Black** on the **Reporting** page indicating that the device has been enrolled with a merchant (and, therefore, is no longer in inventory) and is waiting for contact with the Management Server.

You can confirm the status of the device (Awaiting Device Contact) in the **Status Panel** box on the **Edit Product** page.
Adding a Merchant Logo to the Merchant View

The ISO User can add the merchant’s logo, so that it appears on their Merchant screens.

To add a merchant logo


2. Click on the here link under Merchant Logo Configuration at the bottom left.

   Merchant Logo Configuration:
   No logo specified.
   Click here to add a custom logo.

3. In the File Upload box, click Browse to select the graphic file for the logo, and then click Submit.

   The logo appears on the Merchant View screens for that Merchant User.