Intermec

Integration Guide

CK30/CK31 and Cisco® Aironet 1231/1242

Intermec Technologies Corporation

Worldwide Headquarters
6001 36th Ave.W.
Everett, WA 98203
U.S.A.

www.intermec.com

The information contained herein is proprietary and is provided solely for the purpose of allowing customers to operate and service Intermec-manufactured equipment and is not to be released, reproduced, or used for any other purpose without written permission of Intermec.

Information and specifications contained in this document are subject to change without prior noticed and do not represent a commitment on the part of Intermec Technologies Corporation.

The word Intermec, the Intermec logo, Norand, ArciTech, Beverage Routebook, CrossBar, dcBrowser, Duratherm, EasyADC, EasyCoder, EasySet, Fingerprint, i-gistics, INCA (under license), Intellitag, Intellitag Gen2, JANUS, LabelShop, MobileLAN, Picolink, Ready-to-Work, RoutePower, Sabre, ScanPlus, ShopScan, Smart Mobile Computing, SmartSystems, TE 2000, Trakker Antares, and Vista Powered are either trademarks or registered trademarks of Intermec Technologies Corporation.

Throughout this manual, trademarked names may be used. Rather than put a trademark (™ or ®) symbol in every occurrence of a trademarked name, we state that we are using the names only in an editorial fashion, and to the benefit of the trademark owner, with no intention of infringement.

There are U.S. and foreign patents pending.

Contents

About This Guide

Configuring your wireless network to work in an optimal way can be a difficult task. There are many requirements that need to be evaluated and balanced. Your company's needs for application performance, data throughput, battery life, network security, and radio range must all be balanced so that the system will meet the needs of everyone who must work with it.

This integration guide recommends a configuration based on testing that Intermec has performed between Cisco® Aironet access points and Intermec computers.

Scenario

Intermec performed testing using these devices:

- Cisco Aironet 1231 Access Points and Cisco Aironet 1242 Access Points
- Intermec CK30 Handheld Computers and CK31 Handheld Computers running the TE 2000™ terminal emulation application.

The testing involved using the Intermec computers to perform eight radio transactions per minute over TCP/IP during normal use while the computers frequently roamed between access points.

If your anticipated usage is different from this scenario (for example, you use voice or video applications) or if your location has unusual environmental characteristics, these recommendations may not be applicable.

Recommended Firmware and Software Versions

This table identifies the firmware and software versions that were current at the time this scenario was tested. Intermec recommends that you use these versions or later.

Recommended Versions

Product	Version
1231/1242 access point firmware	12.3(7)JA2
CK30/CK31 computer operating software (OS)	3.00.00.0732
CK30/CK31 computer IVA (Intermec Value Add) software	4.01.17.0597

Quick Configuration Tables

Intermec recommends that you use these settings when configuring the access points to communicate with the Intermec computers. For more details on the access point settings, see "Configuring the 1231/1242" on page 8.

Recommended Settings Summary for 1231/1242

Parameter	Recommended Setting	Default Setting
ARP Caching	Enable ARP Caching	Disable ARP Caching
Radio Settings		
Radio Transmit Power	**1231:** 50 mW CCK (802.11b), 30 mW OFDM (802.11g) **1242:** 17 dBm CCK, 17 dBm OFDM	**1231:** 100 mW CCK (802.11b), 30 mW OFDM (802.11g) **1242:** 20 dBm CCK, 17 dBm OFDM
Radio Channel Settings	1, 6, 11. If you are not using these channels, select your channels carefully to avoid overlap.	Access point selects the least loaded channel
Aironet Extensions	Enable Aironet extensions	Enable Aironet extensions
Public Secure Packet Forwarding (PSPF)	Enable PSPF	Disable PSPF
Multiple SSIDs		
SSID	Enable Guest mode on the SSID that is used by your client devices	Disable Guest mode

Recommended Settings Summary for 1231/1242 (continued)

Parameter	Recommended Setting	Default Setting
Cipher Suites		
Encryption	TKIP	No security
Authentication Types		
Authentication – Open	Open with EAP authentication	No security
Authentication – Network-EAP	Enabled	No security
Authentication – Key-Management	WPA	No security
802.1x Authentication	LEAP authentication with strong passwords	No security
RADIUS Servers		
Radius-server host	Enter the host name or the IP address of a Cisco Secure Access Control Server (ACS) or Funk Odyssey server.	No security
Key	Enter a shared secret key. This text string must match the encryption key used on the RADIUS server.	No security

Recommended Settings Summary for CK30/CK31

Setting	CK30 Computer and CK31 Computer
Network Name (SSID)	Enter the SSID that matches the appropriate access point SSID.
Power Management	Enabled
802.1x Security	LEAP
Association	WPA
Encryption	TKIP
User Name Password	Enter the user name and user password that the computer will use to authenticate to the access point.

Note: Before you configure the 802.11 radio settings, you should configure DHCP settings or TCP/IP communications settings.

Configuring the 1231/1242

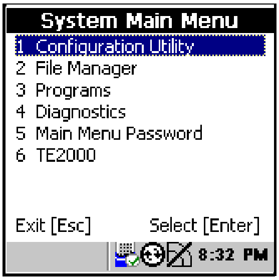
To configure the access point, you can use the web-browser interface or the command line interface (CLI). For help, see the documentation that shipped with the access point or the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

Configuring the CK30

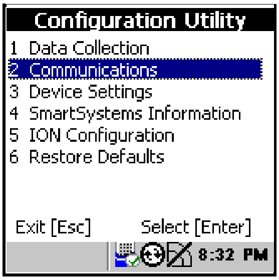
To configure the CK30, you use the menu-driven Configuration Utility. For help, see the *CK30 Handheld Computer User's Manual* (P/N 073528) and the *Intermec Computer Command Reference Manual* (P/N 073529).

To configure the CK30

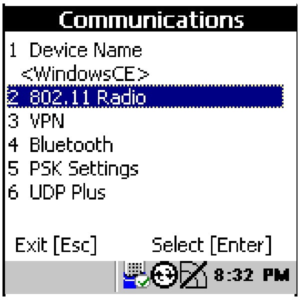
1 Press ▭■ and then ■▭. The System Main Menu appears.



2 Select the **Configuration Utility**. The Configuration Utility main menu appears.



3 Select **Communications**. The Communications menu appears.

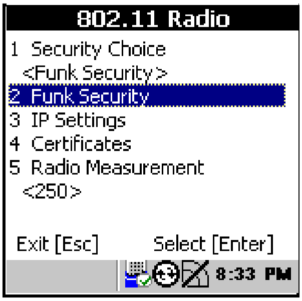


Communications

1 Device Name
<WindowsCE>
2 802.11 Radio
3 VPN
4 Bluetooth
5 PSK Settings
6 UDP Plus

Exit [Esc] Select [Enter]

4 Select **802.11 Radio**. The 802.11 Radio screen appears. Configure DHCP settings or TCP/IP information settings, as required.



802.11 Radio

1 Security Choice
<Funk Security>
2 Funk Security
3 IP Settings
4 Certificates
5 Radio Measurement
<250>

Exit [Esc] Select [Enter]

5 Configure the CK30 to communication with the access point. See the “Recommended Settings Summary for CK30/CK31” on page 7.

6 Press **Esc** until you return to the System Main Menu. If you have made any changes to the configuration, the Save Settings dialog box appears.

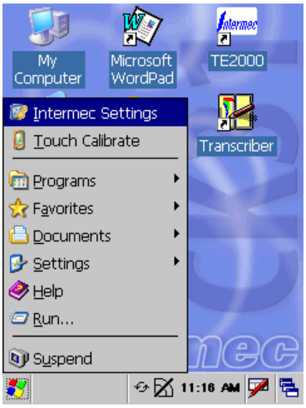
7 Press **Enter** to exit and save the changes through a cold boot. press **Esc** to exit without saving the changes through a cold boot.

Configuring the CK31

To configure the CK31, you use Intermec Settings as described next. For help, see the *CK31 Handheld Computer User's Manual* (P/N 075207) and the *Intermec Computer Command Reference Manual* (P/N 073529).

To configure the CK31

1 Tap the Start icon or press □■ and then ■□. The Start menu appears.



2 Tap **Intermec Settings**. The Intermec Settings application appears.

3 Tap **Communications**. The Communications menu opens.

4 Configure DHCP settings or TCP/IP information settings, as required.

5 Select **802.11 Radio** > **Security Settings**.

6 Configure the CK31 to communicate with the access point. See the "Recommended Settings Summary for CK30/CK31" on page 7.

To enter the LEAP user name and password, tap the **Prompt for Credentials** field and choose **Enter credentials now**.

7 Exit Intermec Settings. Tap **Yes** to save the changes.

About the 1231/1242 Settings

This section provides a brief description of the access point settings and Intermec's recommendation. For more information, see the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

ARP Caching

Intermec Recommends: Enable ARP Caching

Intermec recommends that you configure the access point to reply to ARP queries on behalf of any associated client devices whose IP address it knows. This feature helps to reduce the amount of broadcast traffic sent to all client devices, thereby improving battery life and reducing congestion on the wireless network.

Radio Transmit Power

Intermec Recommends:
1231: 50 mW CCK (802.11b), 30 mW OFDM (802.11g)
1242: 17 dBm CCK, 17 dBm OFDM

You should not set the radio transmit power of the access point higher than the maximum radio transmit power of the client device. The effective range between the access point and the client device is limited by the weaker of the two transmitters.

If you set the access point radio transmit power too high, it can cause unintended areas to be covered, which may present security and interference issues. You may even want to set the radio transmit power to lower power settings in particular areas of your facility in order to provide uniform coverage with minimum interference.

There are two different power settings. The CCK power setting is for 802.11b data rates, and the OFDM power setting is for 802.11g data rates. For the 1231, the maximum power output for OFDM is 30 mW. For the 1242, the maximum power output for OFDM is 17 dBm or 50 mW.

Radio Channel Settings

Intermec Recommends: In the U.S.A., the best choices are channels 1, 6, and 11. Select channels carefully to avoid overlap.

The number of radio channels that are available to set will depend on local regulations and the number of access points installed at your location. When choosing a radio channel for the access point, you should consider the radio channels that are being used by surrounding access points. Intermec recommends that you separate the channels of these access points by as large an amount as possible.

The spacing of the radio channels for the 802.11 radio in the 2.4 GHz band is such that channels separated by less than five channel numbers will overlap. In the U.S.A., where channels 1 through 11 are available, only channels 1, 6, and 11 do not interfere with each other. Make sure that you only use these channels and that neighboring access points do not also use these channels.

Aironet Extensions

Intermec Recommends: Enable Aironet extensions

Aironet extensions add fields to the radio management packets that allow the access point and client devices to exchange information beyond what is specified in the 802.11 standards.

Until recently these messages could only be used by devices that contained a Cisco Aironet radio. Now with the CCX program, CCX-capable clients can participate in this information-sharing feature. This feature helps to enable advanced network management features, such as wireless domain services (WDS) and the wireless LAN solution engine (WLSE).

Public Secure Packet Forwarding (PSPF)

Intermec Recommends: Enable PSPF

Public Secure Packet Forwarding (PSPF) prevents broadcast frames from being rebroadcast from the access point when the access point receives a broadcast frame from a client device. This feature improves security and battery life by decreasing the amount of broadcast traffic on the wireless network. Intermec recommends that you enable this setting if the client devices communicate only with hosts on the wired network.

You must disable this setting if client devices need to communicate directly (peer-to-peer) with other wireless devices. For example, you must disable PSPF for a wireless CK30 to communicate directly with a wireless printer.

Multiple SSIDs—Guest Mode

Intermec Recommends: Enable Guest mode on the SSID that is used by the client devices in your data collection network.

If you enable Guest mode on an SSID, the access point includes a guest SSID in its beacon message. Client devices can quickly determine which access points support their SSID, which access points they can roam to, and what level of security is being used. Therefore, enabling Guest mode will provide the wireless network with faster and more reliable roaming performance.

Enabling Guest mode also lets the access point allow associations from client devices that do not specify an SSID in their configuration.

Some experts recommend that you disable the SSID broadcast as a way to improve security. However, the security afforded by disabling Guest mode is minimal at best and may cause problems for some client devices. Also, it increases the amount of traffic that is required for roaming and therefore will have an adverse impact on roaming performance.

Cipher Suites—Encryption

Intermec Recommends: TKIP

Intermec recommends that you always use encryption in wireless networks to prevent unauthorized network access and to prevent transmitted data from being seen by unauthorized users. To enable Wi-Fi Protected Access (WPA), you must use a cipher suite. Cipher suites are sets of encryption and integrity algorithms designed to protect radio communication on your wireless network. Cipher suites that contain Temporal Key Integrity protocol (TKIP) provide the best security for your wireless network.

TKIP is a newer, stronger encryption algorithm that addresses some of the shortcomings of WEP. Unless your 123X needs to support very old devices in the same wireless network as the CK30s, Intermec recommends that you use WPA with TKIP encryption.

WPA-2 supports CCMP encryption using the AES cipher. However, CCMP support is still very limited and will provide very little benefit beyond that provided by TKIP.

Authentication Types

Intermec Recommends:

Open: Open with EAP authentication
Network-EAP: Enabled
Key Management: WPA

Before a client device can communicate on your network through the access point, it must authenticate to the access point using open or shared-key authentication.

Open with EAP authentication and Network-EAP authentication both allow any client device to associate with the access point and then immediately require 802.1x authentications to begin. There is no difference in functionality or security between Open with EAP authentication and Network-EAP authentication.

Shared key authentication requires that the access point and the client device each be configured with the same WEP key. Then during the association process, they exchange key information to determine if association is allowed. This type of authentication is less secure than open authentication because it is easy for an attacker to determine the correct key from the exchange between a legitimate client device and the access point.

802.1x Authentication

Intermec Recommends: LEAP authentication with strong passwords

The use of an 802.1x-based authentication protocol ensures that only authorized users are able to access your wireless network. The 802.1x protocol also produces the random keying material that is necessary to securely distribute WEP keys to client devices.

The Light Extensible Authentication protocol (LEAP) is easy to configure and requires a minimum amount of processor usage on the client device and authentication server. LEAP also has the advantage of not requiring certificates for either the client or the server. However, LEAP is vulnerable to some forms of password-cracking attacks, and passwords shorter than 10 characters may not be secure. When using LEAP, Intermec recommends that you choose strong passwords.

The Protected Extensible Authentication protocol (PEAP) is another a good option for installations that require stronger security than LEAP. Like LEAP, PEAP does not require a certificate for client authentications. It is based on a user name and password login. However, a certificate is used for server authentication and for setting up an encrypted tunnel for passing credentials from the client device to the authentication server.

RADIUS-Server Host

Intermec recommends: Use a Cisco Secure Access Control Server (ACS) or a Funk Odyssey server.

Before you can use LEAP authentication as your 802.1x authentication, you must configure the access point to communicate with a RADIUS server. To configure the access point, you must open the Security Server Manager page and enter the host name or IP address of the RADIUS server.

You must also select which RADIUS server you want to use for EAP authentication.

Key

Intermec recommends: Configure the key as the last item in the radius-server host command.

The access point and the RADIUS server use a shared secret key (text string) to encrypt passwords and exchange responses. You must enter the same key on the access point and on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.

Sample 1231/1242 Configuration File (CLI)

Here is a sample configuration file for a 1231 or a 1242 that uses the recommended settings of this integration guide. For each installation, you will need to change some settings such as IP information and configuration passwords.

Note: Intermec recommends that you use the sample configuration file as guides to help you identify differences between your access point’s configuration file and the recommended configuration. You should not use the Cisco IOS command line interface (CLI) to copy them directly to your access points.

```
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap1242-1
!
enable secret 5 $1$zq0f$YFiLnn6yDF28Ta0ea7tcC/
enable password 7 1505071F012F25252A3F30
!
ip subnet-zero
ip domain name cisco.boot.com
!
!
aaa new-model
!
!
aaa group server radius rad_eap
 server 192.168.200.90 auth-port 1812 acct-port 1813
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
 cache expiry 1
 cache authorization profile admin_cache
 cache authentication profile admin_cache
!
aaa group server tacacs+ tac_admin
 cache expiry 1
 cache authorization profile admin_cache
 cache authentication profile admin_cache
```

Sample 1231/1242 Configuration File (continued)

```
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
aaa cache profile admin_cache
 all
!
aaa session-id common
!
dot11 ssid DataCollection
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa
   guest-mode
   mbssid guest-mode
!
dot11 arp-cache optional
power inline negotiation prestandard source
!
!
username Cisco password 7 106D000A0618
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers tkip
 !
 ssid DataCollection
 !
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0
24.0 36.0 48.0 54.0
 power local cck 17
 channel 2437
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 port-protected
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
```

Sample 1231/1242 Configuration File (continued)

```
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 !
 encryption mode ciphers tkip
 !
 ssid DataCollection
 !
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 192.168.200.20 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.200.1
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/
prodconfig/help/eag
ip radius source-interface BVI1
!
snmp-server view basic iso included
snmp-server view basic ieee802dot11 included
snmp-server community public RO
radius-server attribute 32 include-in-access-req format %h
radius-server host 192.168.200.90 auth-port 1812 acct-port 1813 key 7
12180815
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
```

Sample 1231/1242 Configuration File (continued)

```
!
!
!
line con 0
 transport preferred all
 transport output all
line vty 0 4
 transport preferred all
 transport input all
 transport output all
line vty 5 15
 transport preferred all
 transport input all
 transport output all
!
end
```

Sample CK30 or CK31 XML File (for SmartSystems)

Here is a sample XML file for the CK30 or CK31 that you can use with the SmartSystems Server/Console. This XML file configures the CK30 or CK31 using the recommended settings of this integration guide. For each installation, you may need to change some settings such as IP information, radio settings (SSIDs), and configuration passwords.

```
<?xml version="1.0" encoding="UTF-8"?>
<DevInfo Action="Set">
   <Subsystem Name="Funk Security">
      <Group Name="802.11 Radio">
         <Field Name="ZeroConfig">Off</Field>
      </Group>
      <Field Name="ActiveProfile">Profile_1</Field>
      <Group Name="Profile" Instance="Profile_1">
         <Field Name="ProfileLabel">DataCollection</Field>
         <Field Name="NetworkType">Infrastructure</Field>
         <Field Name="DSChannel">1</Field>
         <Field Name="SSID">DataCollection</Field>
         <Field Name="PSMode">Enabled(Fast PSP)</Field>
         <Field Name="8021x">LEAP</Field>
         <Field Name="Association">WPA</Field>
         <Field Name="Encryption">TKIP</Field>
         <Field Name="PreSharedKey">******</Field>
         <Field Name="DefaultKeyID">1</Field>
         <Field Name="Key1"/>
         <Field Name="Key2"/>
         <Field Name="Key3"/>
         <Field Name="Key4"/>
         <Field Name="PasswordPrompt">Disabled</Field>
```

Sample CK30 or CK31 XML File (continued)

```
        <Field Name="UserName">anonymous</Field>
        <Field Name="UserPassword">******</Field>
        <Field Name="InnerAuthenticationTTLS">MS-Chapv2</Field>
        <Field Name="InnerEAP">EAP/Token Card</Field>
        <Field Name="InnerAuthenticationPEAP">EAP/MS-Chapv2</Field>
        <Field Name="SubjectName"/>
        <Field Name="ValidateServerCert">No</Field>
        <Field Name="CN1"/>
        <Field Name="CN2"/>
        <Field Name="MixedCell">On</Field>
        <Field Name="CCKM">Off</Field>
        <Field Name="DetectRogueAPs">Off</Field>
        <Field Name="Logging">Off</Field>
     </Group>
     <Group Name="Profile" Instance="Profile_2">
        <Field Name="ProfileLabel">Profile_2</Field>
        <Field Name="NetworkType">Infrastructure</Field>
        <Field Name="DSChannel">1</Field>
        <Field Name="SSID">INTERMEC</Field>
        <Field Name="PSMode">Enabled(Fast PSP)</Field>
        <Field Name="8021x">None</Field>
        <Field Name="Association">Open</Field>
        <Field Name="Encryption">None</Field>
        <Field Name="PreSharedKey">******</Field>
        <Field Name="DefaultKeyID">1</Field>
        <Field Name="Key1"/>
        <Field Name="Key2"/>
        <Field Name="Key3"/>
        <Field Name="Key4"/>
        <Field Name="PasswordPrompt">Disabled</Field>
        <Field Name="UserName">anonymous</Field>
        <Field Name="UserPassword">******</Field>
        <Field Name="InnerAuthenticationTTLS">MS-Chapv2</Field>
        <Field Name="InnerEAP">EAP/Token Card</Field>
        <Field Name="InnerAuthenticationPEAP">EAP/MS-Chapv2</Field>
        <Field Name="SubjectName"/>
        <Field Name="ValidateServerCert">No</Field>
        <Field Name="CN1"/>
        <Field Name="CN2"/>
        <Field Name="MixedCell">On</Field>
        <Field Name="CCKM">Off</Field>
        <Field Name="DetectRogueAPs">Off</Field>
        <Field Name="Logging">Off</Field>
     </Group>
     <Group Name="Profile" Instance="Profile_3">
        <Field Name="ProfileLabel">Profile_3</Field>
        <Field Name="NetworkType">Infrastructure</Field>
        <Field Name="DSChannel">1</Field>
        <Field Name="SSID">INTERMEC</Field>
        <Field Name="PSMode">Enabled(Fast PSP)</Field>
```

Sample CK30 or CK31 XML File (continued)

```
       <Field Name="8021x">None</Field>
       <Field Name="Association">Open</Field>
       <Field Name="Encryption">None</Field>
       <Field Name="PreSharedKey">******</Field>
       <Field Name="DefaultKeyID">1</Field>
       <Field Name="Key1"/>
       <Field Name="Key2"/>
       <Field Name="Key3"/>
       <Field Name="Key4"/>
       <Field Name="PasswordPrompt">Disabled</Field>
       <Field Name="UserName">anonymous</Field>
       <Field Name="UserPassword">******</Field>
       <Field Name="InnerAuthenticationTTLS">MS-Chapv2</Field>
       <Field Name="InnerEAP">EAP/Token Card</Field>
       <Field Name="InnerAuthenticationPEAP">EAP/MS-Chapv2</Field>
       <Field Name="SubjectName"/>
       <Field Name="ValidateServerCert">No</Field>
       <Field Name="CN1"/>
       <Field Name="CN2"/>
       <Field Name="MixedCell">On</Field>
       <Field Name="CCKM">Off</Field>
       <Field Name="DetectRogueAPs">Off</Field>
       <Field Name="Logging">Off</Field>
    </Group>
    <Group Name="Profile" Instance="Profile_4">
       <Field Name="ProfileLabel">Profile_4</Field>
       <Field Name="NetworkType">Infrastructure</Field>
       <Field Name="DSChannel">1</Field>
       <Field Name="SSID">INTERMEC</Field>
       <Field Name="PSMode">Enabled(Fast PSP)</Field>
       <Field Name="8021x">None</Field>
       <Field Name="Association">Open</Field>
       <Field Name="Encryption">None</Field>
       <Field Name="PreSharedKey">******</Field>
       <Field Name="DefaultKeyID">1</Field>
       <Field Name="Key1"/>
       <Field Name="Key2"/>
       <Field Name="Key3"/>
       <Field Name="Key4"/>
       <Field Name="PasswordPrompt">Disabled</Field>
       <Field Name="UserName">anonymous</Field>
       <Field Name="UserPassword">******</Field>
       <Field Name="InnerAuthenticationTTLS">MS-Chapv2</Field>
       <Field Name="InnerEAP">EAP/Token Card</Field>
       <Field Name="InnerAuthenticationPEAP">EAP/MS-Chapv2</Field>
       <Field Name="SubjectName"/>
       <Field Name="ValidateServerCert">No</Field>
       <Field Name="CN1"/>
       <Field Name="CN2"/>
       <Field Name="MixedCell">On</Field>
```

Sample CK30 or CK31 XML File (continued)

```
        <Field Name="CCKM">Off</Field>
        <Field Name="DetectRogueAPs">Off</Field>
        <Field Name="Logging">Off</Field>
     </Group>
   </Subsystem>
</DevInfo>
```

Intermec

Corporate Headquarters
6001 36th Avenue West
Everett, Washington 98203
U.S.A.

tel 425.348.2600

fax 425.355.9551

www.intermec.com

CK30/CK31 and Cisco Aironet 1231/1242 Integration Guide

P/N 944-621-002