Release Notes

PE15N

Version 3.4.4.0 *November 2017*

This document provides release notes for version 3.4.4.0 of the PE15N, EC15N, and EC25N radio software for Windows XP (Professional and Embedded).

Release notes are a summary of new and enhanced features, resolved issues, and known issues that are not resolved in this version. Consult the user's guide for details on the features of this software release.

SOFTWARE VERSION 3.4.4.0

Released November 2017

Package

This release package includes the following:

Component	Version
Windows Installer Package	3.04.04.00
NDIS 5 Device Driver	3.04.01.36
Summit Connection Utility	3.04.03.14
Laird 802.1x Supplicant	40.03.10.19
Supplicant Credential Dialog Helper	3.04.00.00
SDC Control Panel Applet	3.04.01.01
Single Sign On Module	3.04.00.00

New or Enhanced Features

None

Resolved Issues

The following issues are resolved with the 3.4.4.0 release:

- **WPA KRACK vulnerability** –The WPA supplicant shipped with the PE15N is no longer vulnerable to Key Reinstallation Attacks. (12108)

Known Issues

The following are known issues with the 3.4.3.0 release:

- **LRU unable to select TX antenna** – The driver transmits on the main antenna regardless of LRU TX antenna setting. (8374)
- **LRU continuous waive** – The driver does not support the continuous wave functionality. (8910)
- **pspDelay support (PE15N/EC15N/EC25N):** The pspDelay setting is not supported on the PE15N, EC15N, and EC25N.
- **LED Active state (PE15N)** – LED remains in a constantly Active state.
- **EAP Type errors** – When configuring profiles on the SCU that do not use EAP types, it is possible to select an EAP type from the EAP Type drop-down menu. Attempting to "Commit" a profile with an incorrect mix of Encryption type and EAP type correctly results in an error.
- **Disabling the radio** – If "Disable" is the focus on the Main tab of the SCU, changing to the Status tab and tapping the spacebar can disable the radio.
- **Manual WEP configuration option** – Scanning for an SSID set to "CKIP Auto" results in a configuration option of "Manual WEP".
- **Ad hoc mode/Channel mode support issue** – Ad Hoc mode does not support the BG Channel Mode setting in the Global tab.
- **SCU - Ad hoc connection shown before completed** – When the radio mode is Ad Hoc, SCU displays a connection five to ten seconds before the connection is actually established. This is consistent with the behavior of Windows Zero Config (WZC) when it is used instead of SCU.
- **Status window displays with Ad Hoc mode** – If the active profile uses an Ad Hoc radio mode, then SCU displays the IP address for the Summit radio on the Diags window but not on the Status window.
- **Imported profiles display** – Imported profiles do not display on the SCU Profile tab until SCU is restarted.
- **Incorrect stored credentials** – Incorrect stored credentials are not corrected when proper credentials are entered on the password prompt.
- **Pre-logon Settings** – Pre-logon settings (SCU/Global tab/Logon Options) are not retained during an Import/Export operation.
- **Wireless network icon display issues** – Mousing over the wireless network icon in the notification area in Windows may not show the correct/updated state of the radio. Use the SCU, Main tab or Status tab, to view the correct radio state.
- **Modified filepath settings issues** – Modified filepath settings are not saved after completing an Import or Export.
- **Device boot process authentication failures** – Client radios configured for EAP-TLS will see authentication failures recorded in the RADIUS server logs during the device boot process. The radio attempts to authenticate before the Microsoft Store, in which the user certificate is stored, is available. Once the MS Store is available the authentication will proceed.
- **Credential/Authentication issues** – When connecting to a wireless network with a profile configured to use Windows credentials for authentication with Active Directory, and the user is prompted to change their Active Directory password, the Active Directory password and the local Windows password on the device can get out of sync if, after changing the password, the device is rebooted prior to the user logging out and logging back into Windows. When the passwords are out of sync, the user is unable to log into Windows using the new password but is able to log into Windows using the old password. However, when logged in using the old password, network authentication repeatedly fails even if the new (changed) credentials are provided when prompted.

- To recover once in this state, the user must log into Windows using the old password and modify the wireless profile to prompt for credentials rather than use Windows credentials. When prompted for credentials to connect to the wireless network, provide the new password and the client will successfully connect to the network. Once connected to the network, log out of Windows and then log back in using the new password so that the local Windows password is in sync with the Active Directory password.
- To avoid encountering this issue, always log out of Windows and log back in prior to rebooting the device following an Active Directory password change.

SOFTWARE VERSION 3.4.3.0

Released January 2017

Package

This release package includes the following:

Component	Version
Windows Installer Package	3.04.03.00
NDIS 5 Device Driver	3.04.01.36
Summit Connection Utility	3.04.03.14
Laird 802.1x Supplicant	40.03.08.00
Supplicant Credential Dialog Helper	3.04.00.00
SDC Control Panel Applet	3.04.01.01
Single Sign On Module	3.04.00.00

New or Enhanced Features

802.1x Supplicant

The following supplicant features have been added or removed in this release.

- Upgraded supplicant's OpenSSL library to v1.0.1h
- Added full support for WFA2014 requirement
- Added the ability to configure the EAP-FAST outer identity

Resolved Issues

The following issues are resolved with the 3.4.3.0 release:

- **Reduced possible credential disclosure** –User password is stored in memory in encrypted format. (9747)
- **TLS middle certificate validation failures** – Fixed issue where some valid middle certificates would be rejected.(9598)
- **Memory Leak** – Fix memory leak of service handle on shutdown. (8172)
- **Disconnects due to incorrect broadcast key messages** – Added work-arounds for APs which send WPA2/TKIPS EAPOL-Key packets with the key field encapsulated or with incorrect AES-WRAP padding in the key data field. (8191/9475)

- **Authentication attempt delayed after authentication failure** – Resolved long delays due to EAP timing out before global configuration timer expires. (7438)
- **Delayed prompting immediately after windows logon** - Fixed issues causing the credential prompt to be delayed immediately after user logged in. (3329)
- **User prompt continues after supplicant exits** – The user will no longer be prompted for credentials after the supplicant stops running. (5544)
- **PEAP-TLS Phase 2 Certificate Cache** – cache certificate for phase 2 of PEAP-TLS (5641)
- **Supplicant stops running** – Fixed stack overflow causing supplicant to exit when prompting after a failed authentication attempt. (5604)
- **Supplicant stops running with EAP-FAST**- Fixed issue which caused suppliant to exit unexpectedly if EAP-FAST PAC refresh occurs and the old PAC is already deleted. (4603)
- **OPMK failures** –Fixed error in recalculation of PMKID which caused AP to discard PMKID and force full authentication. (5424)
- **Supplicant ignores TKIP countermeasures report** - Fixed issue where supplicant would continue to attempt to connect while TKIP countermeasures were invoked. (4868)
- **Support for Certificate Date Checking** – Added option to validate certificate date. The default continues to be off. (4505)
- **Removed 5 second connection attempt delay** – Upon a disconnect indication from the driver, which indicates connection has been lost for 10 seconds, the supplicant will no longer wait an additional 5 second before attempting to connect again. (2335)

Known Issues

The following are known issues with the 3.4.3.0 release:

- **LRU unable to select TX antenna:** The driver transmits on the main antenna regardless of LRU TX antenna setting. (8374)
- **LRU continuous waive:** The driver does not support the continuous wave functionality. (8910)
- **pspDelay support (PE15N/EC15N/EC25N):** The pspDelay setting is not supported on the PE15N, EC15N, and EC25N.
- **LED Active state (PE15N):** LED remains in a constantly Active state.
- **EAP Type errors:** When configuring profiles on the SCU that do not use EAP types, it is possible to select an EAP type from the EAP Type drop-down menu. Attempting to "Commit" a profile with an incorrect mix of Encryption type and EAP type correctly results in an error.
- **Disabling the radio:** If "Disable" is the focus on the Main tab of the SCU, changing to the Status tab and tapping the spacebar can disable the radio.
- **Manual WEP configuration option:** Scanning for an SSID set to "CKIP Auto" results in a configuration option of "Manual WEP".
- **Ad hoc mode/Channel mode support issue:** Ad Hoc mode does not support the BG Channel Mode setting in the Global tab.
- **SCU - Ad hoc connection shown before completed:** When the radio mode is Ad Hoc, SCU displays a connection five to ten seconds before the connection is actually established. This is consistent with the behavior of Windows Zero Config (WZC) when it is used instead of SCU.
- **Status window displays with Ad Hoc mode:** If the active profile uses an Ad Hoc radio mode, then SCU displays the IP address for the Summit radio on the Diags window but not on the Status window.
- **Imported profiles display:** Imported profiles do not display on the SCU Profile tab until SCU is restarted.

- **Incorrect stored credentials:** Incorrect stored credentials are not corrected when proper credentials are entered on the password prompt.
- **Pre-logon Settings:** Pre-logon settings (SCU/Global tab/Logon Options) are not retained during an Import/Export operation.
- **Wireless network icon display issues:** Mousing over the wireless network icon in the notification area in Windows may not show the correct/updated state of the radio. Use the SCU, Main tab or Status tab, to view the correct radio state.
- **Modified filepath settings issues:** Modified filepath settings are not saved after completing an Import or Export.
- **Device boot process authentication failures:** Client radios configured for EAP-TLS will see authentication failures recorded in the RADIUS server logs during the device boot process. The radio attempts to authenticate before the Microsoft Store, in which the user certificate is stored, is available. Once the MS Store is available the authentication will proceed.
- **Credential/Authentication issues:** When connecting to a wireless network with a profile configured to use Windows credentials for authentication with Active Directory, and the user is prompted to change their Active Directory password, the Active Directory password and the local Windows password on the device can get out of sync if, after changing the password, the device is rebooted prior to the user logging out and logging back into Windows. When the passwords are out of sync, the user is unable to log into Windows using the new password but is able to log into Windows using the old password. However, when logged in using the old password, network authentication repeatedly fails even if the new (changed) credentials are provided when prompted.
- To recover once in this state, the user must log into Windows using the old password and modify the wireless profile to prompt for credentials rather than use Windows credentials. When prompted for credentials to connect to the wireless network, provide the new password and the client will successfully connect to the network. Once connected to the network, log out of Windows and then log back in using the new password so that the local Windows password is in sync with the Active Directory password.
- To avoid encountering this issue, always log out of Windows and log back in prior to rebooting the device following an Active Directory password change.

SOFTWARE VERSION 3.4.2.1

Released 27 April 2016

Package

This release package includes the following:

Component	Version
Windows Installer Package	3.04.02.01
NDIS 5 Device Driver	3.04.01.36
Summit Connection Utility	3.04.03.14
Laird 802.1x Supplicant	3.04.07.04
Supplicant Credential Dialog Helper	3.04.00.00
SDC Control Panel Applet	3.04.01.01
Single Sign On Module	3.04.00.00

New or Enhanced Features

LRU

This package includes support for the Laird Regulatory Utility v47.3.2.8 and greater.

LMU

This package includes support for the Laird Manufacturing Utility v46.3.1.6 and greater.

ETSI Regulatory Compliance

This package is compliant with the ETSI EN300 1.9.1 requirements by disabling .11N rates for WW and ETSI regulatory domains.

FCC 594280 Compliance

This package is compliant with the FCC 594280 requirements ***with assistance from OEM manufacturers***. OEMs shipping products within the FCC territorial domain ***must perform additional steps during manufacturing in*** order to comply with all FCC regulations. Please contact Laird support for further information.

In order to comply with these requirements, support for the World Mode (WW) regulatory domain (specifically 802.11d) was removed. The WW regulatory domain is now a fixed subset of channels and power levels that are compliant across all supported regulatory domains.

Resolved Issues

The following issues are resolved with the 3.4.2.1 release:

- **FCC 594280 Regulatory Compliance -** This release complies with the FCC 594280 requirements. (7721)
- **Updated KCC Regulatory settings –** The channel set and TX power settings for KCC have been updated to correspond with the updated KCC regulatory requirements. (3950) (3558) (8119)
- **TX Power Levels –** The driver will now adopt the TX power level set by the configuration and report the estimated TX power usage in milliwatts. (7932)
- **Added support for newer versions of LRU –** The driver includes support for LRU versions 47.3.2.8 and newer. (5849)

Known Issues

The following are known issues with the 3.4.2.1 release:

- **LRU unable to select TX antenna:** The driver transmits on the main antenna regardless of LRU TX antenna setting. (8374)
- **LRU continuous waive:** The driver does not support the continuous wave functionality. (8910)
- **pspDelay support (PE15N/EC15N/EC25N):** The pspDelay setting is not supported on the PE15N, EC15N, and EC25N.

- **LED Active state (PE15N):** LED remains in a constantly Active state.
- **EAP Type errors:** When configuring profiles on the SCU that do not use EAP types, it is possible to select an EAP type from the EAP Type drop-down menu. Attempting to "Commit" a profile with an incorrect mix of Encryption type and EAP type correctly results in an error.
- **Disabling the radio:** If "Disable" is the focus on the Main tab of the SCU, changing to the Status tab and tapping the spacebar can disable the radio.
- **Manual WEP configuration option:** Scanning for an SSID set to "CKIP Auto" results in a configuration option of "Manual WEP".
- **Ad hoc mode/Channel mode support issue:** Ad Hoc mode does not support the BG Channel Mode setting in the Global tab.
- **SCU - Ad hoc connection shown before completed:** When the radio mode is Ad Hoc, SCU displays a connection five to ten seconds before the connection is actually established. This is consistent with the behavior of Windows Zero Config (WZC) when it is used instead of SCU.
- **Status window displays with Ad Hoc mode:** If the active profile uses an Ad Hoc radio mode, then SCU displays the IP address for the Summit radio on the Diags window but not on the Status window.
- **Imported profiles display:** Imported profiles do not display on the SCU Profile tab until SCU is restarted.
- **Incorrect stored credentials:** Incorrect stored credentials are not corrected when proper credentials are entered on the password prompt.
- **Pre-logon Settings:** Pre-logon settings (SCU/Global tab/Logon Options) are not retained during an Import/Export operation.
- **Wireless network icon display issues:** Mousing over the wireless network icon in the notification area in Windows may not show the correct/updated state of the radio. Use the SCU, Main tab or Status tab, to view the correct radio state.
- **Modified filepath settings issues:** Modified filepath settings are not saved after completing an Import or Export.
- **Device boot process authentication failures:** Client radios configured for EAP-TLS will see authentication failures recorded in the RADIUS server logs during the device boot process. The radio attempts to authenticate before the Microsoft Store, in which the user certificate is stored, is available. Once the MS Store is available the authentication will proceed.
- **Credential/Authentication issues:** When connecting to a wireless network with a profile configured to use Windows credentials for authentication with Active Directory, and the user is prompted to change their Active Directory password, the Active Directory password and the local Windows password on the device can get out of sync if, after changing the password, the device is rebooted prior to the user logging out and logging back into Windows. When the passwords are out of sync, the user is unable to log into Windows using the new password but is able to log into Windows using the old password. However, when logged in using the old password, network authentication repeatedly fails even if the new (changed) credentials are provided when prompted.

  To recover once in this state, the user must log into Windows using the old password and modify the wireless profile to prompt for credentials rather than use Windows credentials. When prompted for credentials to connect to the wireless network, provide the new password and the client will successfully connect to the network. Once connected to the network, log out of Windows and then log back in using the new password so that the local Windows password is in sync with the Active Directory password.

  To avoid encountering this issue, always log out of Windows and log back in prior to rebooting the device following an Active Directory password change.

SOFTWARE VERSION 3.4.0.3

Released 17 November 2014

Package

This release package includes the following:

Component	Version
Windows Installer Package	3.04.00.03
NDIS 5 Device Driver	3.04.00.26
Summit Connection Utility	3.04.03.14
Laird 802.1x Supplicant	3.04.07.04
Supplicant Credential Dialog Helper	3.04.00.00
SDC Control Panel Applet	3.04.01.01
Single Sign On Module	3.04.00.00

New or Enhanced Features

The following new features were added in the 3.4.0.3 release:

ETSI Regulatory Compliance

- This package is compliant with the ETSI EN300 requirements.

Resolved Issues

The following issues are resolved with the 3.4.0.3 release:

- **ETSI Compliance –** Removed N-Rates support for ETSI and World Mode regulatory domains in order to pass ETSI EN300 requirements. (6403)
- **UNII 2 & 3 Quiet Channels –** Resolved issue where driver may actively probe on a 5GHz channel which is marked as a quite channel. (6027)

Known Issues

The following are known issues with the 3.4.0.3 release:

- **pspDelay support (PE15N/EC15N/EC25N):** The pspDelay setting is not supported on the PE15N, EC15N, and EC25N.
- **LED Active state (PE15N):** LED remains in a constantly Active state.
- **EAP Type errors:** When configuring profiles on the SCU that do not use EAP types, it is possible to select an EAP type from the EAP Type drop-down menu. Attempting to "Commit" a profile with an incorrect mix of Encryption type and EAP type correctly results in an error.
- **Disabling the radio:** If "Disable" is the focus on the Main tab of the SCU, changing to the Status tab and tapping the spacebar can disable the radio.
- **Manual WEP configuration option:** Scanning for an SSID set to "CKIP Auto" results in a configuration option of "Manual WEP".

- **Ad hoc mode/Channel mode support issue:** Ad Hoc mode does not support the BG Channel Mode setting in the Global tab.
- **SCU - Ad hoc connection shown before completed:** When the radio mode is Ad Hoc, SCU displays a connection five to ten seconds before the connection is actually established. This is consistent with the behavior of Windows Zero Config (WZC) when it is used instead of SCU.
- **Status window displays with Ad Hoc mode:** If the active profile uses an Ad Hoc radio mode, then SCU displays the IP address for the Summit radio on the Diags window but not on the Status window.
- **Imported profiles display:** Imported profiles do not display on the SCU Profile tab until SCU is restarted.
- **Incorrect stored credentials:** Incorrect stored credentials are not corrected when proper credentials are entered on the password prompt.
- **Pre-logon Settings:** Pre-logon settings (SCU/Global tab/Logon Options) are not retained during an Import/Export operation.
- **Wireless network icon display issues:** Mousing over the wireless network icon in the notification area in Windows may not show the correct/updated state of the radio. Use the SCU, Main tab or Status tab, to view the correct radio state.
- **Modified filepath settings issues:** Modified filepath settings are not saved after completing an Import or Export.
- **Device boot process authentication failures:** Client radios configured for EAP-TLS will see authentication failures recorded in the RADIUS server logs during the device boot process. The radio attempts to authenticate before the Microsoft Store, in which the user certificate is stored, is available. Once the MS Store is available the authentication will proceed.
- **Credential/Authentication issues:** When connecting to a wireless network with a profile configured to use Windows credentials for authentication with Active Directory, and the user is prompted to change their Active Directory password, the Active Directory password and the local Windows password on the device can get out of sync if, after changing the password, the device is rebooted prior to the user logging out and logging back into Windows. When the passwords are out of sync, the user is unable to log into Windows using the new password but is able to log into Windows using the old password. However, when logged in using the old password, network authentication repeatedly fails even if the new (changed) credentials are provided when prompted.

  To recover once in this state, the user must log into Windows using the old password and modify the wireless profile to prompt for credentials rather than use Windows credentials. When prompted for credentials to connect to the wireless network, provide the new password and the client will successfully connect to the network. Once connected to the network, log out of Windows and then log back in using the new password so that the local Windows password is in sync with the Active Directory password.

  To avoid encountering this issue, always log out of Windows and log back in prior to rebooting the device following an Active Directory password change.