Outpost v3.1 Release Content Description

Jim Oberhofer KN6PE
29 December 2015

1. Introduction

This Release Content Description provides information about new or changed functionality that will be available in Outpost Packet Message Manager Release 3.1. This information is organized under the following sections:

- ***New Features:*** A new capability that did not exist in any prior version of Outpost in any form.
- ***Enhancements:*** A change to an existing feature that further improves the performance or usability of the application. Enhancements include minor changes, internal changes (that may not be evident to the user, but contribute to improved supportability increased stability, or application performance) and bug fixes.

***NOTE*:** This release is focused on supporting the changes planned by the Winlink Development team, specifically the Secure Logon. Due to the time sensitivity of the Winlink release (April 15, 2016), the Outpost v3.1 release will ensure Outpost users can be operational with Winlink once that application is released.

2. New Features

2.1. ER#1099: User Access Control (UAC) data restructuring

While Outpost continues to be an application focused on RF connectivity, there is also a need to ensure it remains compatible with telnet access to BBSs. Telnet access and Secure Logons mean *Password Management*.

Outpost originally implemented telnet logon features as an extension of the TNC comm port setup. When a TNC (in reality an Interface) was defined and it was declared as a telnet interface, the user provided, among other things, the telnet prompts and the user responses (logon and password). While this approach worked ok for single user environments, if multiple people used a single Outpost instance, a different TNC/Telnet configuration was needed for each user to access the BBS. This situation gets out of hand when Outpost is located in an EOC and different users were expected to work a shift at one Outpost instance.

This change does the following:

1. Removes all user logon and password data from the TNC / Telnet configuration and user interface. This means that the TNC/Telnet configuration is now exclusively describing how Outpost finds a BBS (hostname:port) and anticipates the logon sequence (logon and password prompts).
2. Creates a new data structure for Users and Tactical Calls.
3. Associates one or more BBS/Logon/Password entries with a specific user.
4. Addresses the special Winlink requirement for the secure user logon password (in addition to the telnet connect password).
5. Adds additional fields and controls to the Setup > Identification form to capture the BBS/Logon/ Password data.

What's not changing: AGWPE logon and passwords will not be a part of this change since these logon/passwords manage access to the AGWPE interface, not the BBS specifically. They will continue to be located on the TNC/AGWPE Tab.

Migration: A fully automated data migration of logons and passwords from the TNC data structure to the new user data structure is not planned. While more detailed instructions will be provided, the migration steps will essentially include:

1. Create a list of BBSs, logons, and passwords that you use.
2. Perform the upgrade to Outpost v3.1
3. For each logon, re-enter the BBS, Logon, and passwords. Multiple BBS/Logon/Password entries can be made for a given user.

This change simplifies the TNC Interface management by letting that data focus on navigation to the BBS, and then the new user data structure focus on the user and his/her credentials for access to the BBS.

2.2. ER#1278: Manage the Winlink Secure Logon interaction

The Winlink move to a Secure Logon is good for the ARES/RACES community with respect for our Served Agencies. Protecting their data (within the constraints of the FCC Rules) and access to that data continues to be critical for all communications responders.

If you are a Winlink user, you already received a message similar to this: "On April 15, 2016, the Winlink system will begin requiring the use of passwords and secure login for all users. This is being done to enhance the privacy and protection of the Winlink community. If you've already entered both a password and also turned on Secure Login, you don't have to make any other changes. The transition taking place on April 15, 2016, won't change your operation. If you have not set a password for your account, and also have not enabled Secure Login, we recommend you do it now so you won't be surprised on April 15, 2016."

Outpost will support this change as follows:

1. Manage and store a user's Winlink Secure Logon Password (see #1099 above).
2. Watch for and process all Winlink password challenges, and send back the appropriate response.
3. Provide Winlink Secure Logon support for both telnet and CMS/RF access.
4. Provide error messages to help the user figure out where a problem may reside.
5. Provide the necessary App Notes and user documentation to ensure a smooth transition.
6. Allows Tactical Calls to be treated like a "user" with their own BBS/Logon/Password entries.

The plan is to deliver this release to you in January 2016 to ensure you have time to get Outpost configured to work correctly with Winlink.

3. Enhancements

ER#1284: Remove Winlink Transparency Mode. Located on the TNC/Telnet Form, this mode was a legacy change that was introduced and removed by Winlink. The removal of this feature and control should not have any impact on any Winlink users.

ER#1285: Remove "Use Default Station ID" control. Located on the TNC/Telnet Form, this control allowed users to use the Station ID value instead of entering a Logon Value. This worked fine PROVIDED that all users had the same password; a bad assumption. This change removes this control and requires all telnet logons and passwords to be explicitly entered for each user (see #1099 above).

ER#1286: Correct Notification Form behavior. This change ensures that send/receive notifications are not lost by ensuring the Notification alert form pops to the top on receipt of a notification.

… and no others