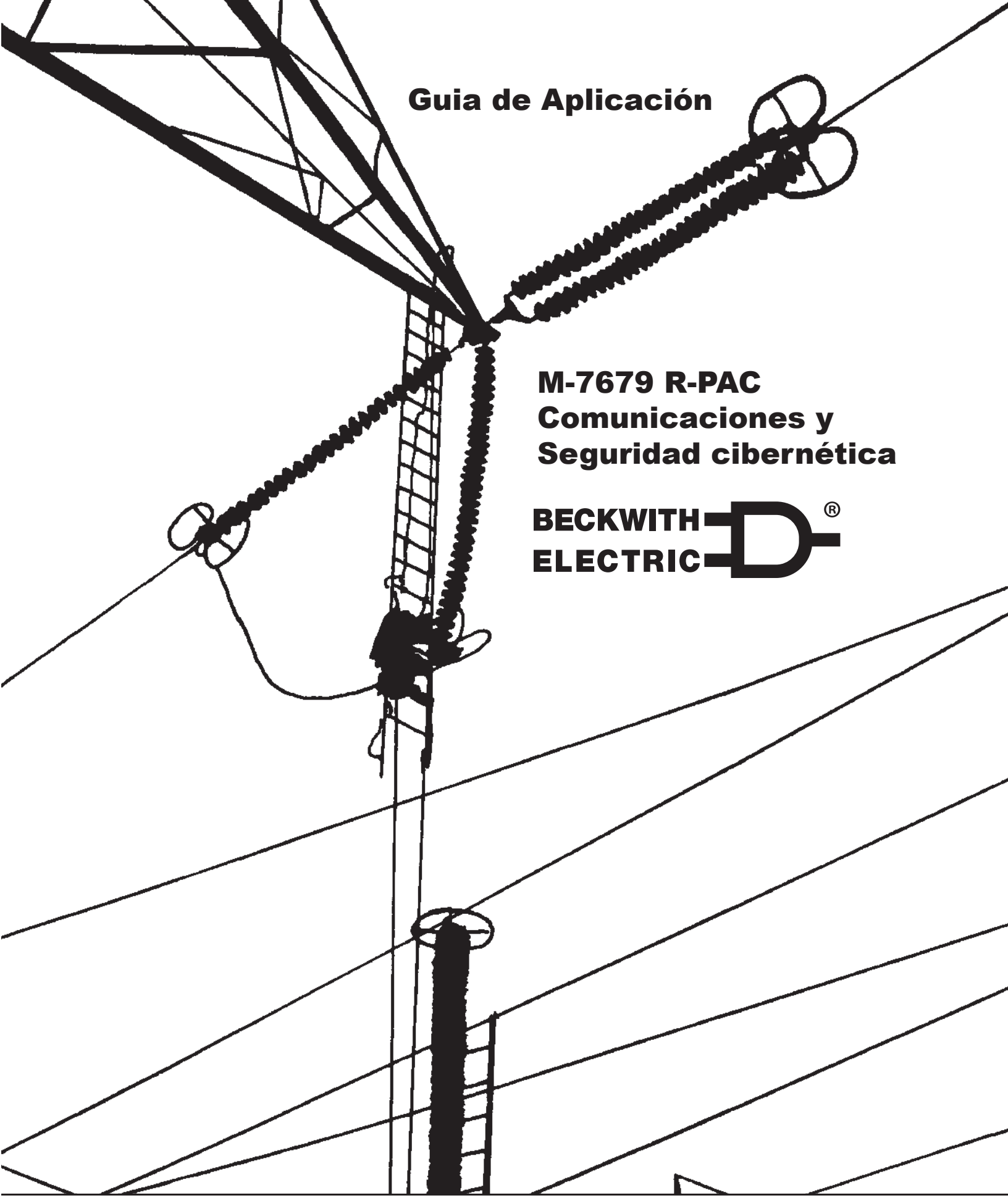
Guia de Aplicación

M-7679 R-PAC
Comunicaciones y Seguridad cibernética

BECKWITH ELECTRIC®



HUBBELL® Un orgulloso miembro de la familia Hubbell.

MARCAS COMERCIALES

Todas las marcas o nombres de productos mencionados en este documento pueden ser marcas comerciales o marcas registradas de sus respectivos propietarios.

El contenido de este manual de instrucciones se proporciona únicamente para uso informativo y está sujeto a cambios sin previo aviso. Beckwith Electric ha aprobado únicamente la versión en Inglés de este documento.

NOTA: Las ultimas actualizaciones del producto no se encuentran disponibles en la versión actual del documento. Verificar la versión del documento en idioma Inglés para obtener la información más actualizada del producto.

TABLA DE CONTENIDOS
M-7679 R-PAC
Comunicaciones y Seguridad cibernética

1.0 Editor de Configuración DNP

■ **NOTA DE SEGURIDAD CIBERNETICA:**
Cuando se habilita la Seguridad cibernética, el acceso a alguna de las funciones descritas en este Sección está sujeta a la política de permisos de acceso designadas por el administrador de la Política de seguridad.

El Editor de configuración DNP incluye las siguientes características y funciones:

Variaciones – La variación de un objeto da una representación diferente del mismo punto de datos, tales como el tamaño del objeto o si o no el objeto tiene información de indicador. Acordemente, la sección Variación configura los objetos listados con las variaciones deseadas y soportadas.

Direcciones Maestras usadas para respuestas No Solicitadas – Estas direcciones serán usadas como las direcciones a transmisiones de respuestas no solicitadas.

Módem de Ajuste No Solicitado – Se aplica a interfase TIA 232 conectado a un módem Ethernet. Ajuste no solicitados TCP/IP y UDP/IP se utilizan cuando DNP está siendo desplegado sobre una red ethernet. Los elementos de ajuste se describen a continuación:

- Permitir No Solicitados: Determina si las respuestas no solicitadas (nulas) serán enviadas cuando la sesión se detecte en línea. Si está activado, las respuestas no solicitadas posteriores estarán habilitadas a través del código de función 0x14 (habilitar respuestas no solicitadas) e inhabilita a través del código de función 0x15 (desactivar respuestas no solicitadas). Si "Allow Unsolicit" está desactivada, entonces los códigos de función 0x14 y 0x15 responderán con un error.
- Clase 1 Retardo Máximo (Seg): Si la respuesta no solicitada es habilitada, este parámetro especifica la cantidad de tiempo máximo después de que un evento en la clase correspondiente es recibido antes de que una respuesta no solicitada sea generada.
- Clase 1 Eventos Máximo: Si las respuestas no solicitadas están habilitadas, el parámetro especifica el número máximo de eventos en la clase correspondiente a ser permitido antes de generar una respuesta no solicitada.
- Clase 2 Retardo Máximo (Seg): Si la respuesta no solicitada es habilitada, este parámetro especifica la cantidad de tiempo máximo después de que un evento en la clase correspondiente es recibido antes de que una respuesta no solicitada sea generada.
- Clase 2 Eventos Máximos: Si las respuestas no solicitadas están habilitadas, el parámetro especifica el número máximo de eventos en la clase correspondiente a ser permitido antes de generar una respuesta no solicitada.

Selección de Puntos – la ventana de puntos disponibles es poblada cuando se abre un archivo fuente DNP. La selección de los puntos de las pestañas de Entradas Binarias, Entradas Analógicas, Salidas Binario/Control y Salidas Analógicas pueden llevarse a cabo por cualquiera seleccionar de forma individual, arrastrar y colocar puntos en la ventana de puntos seleccionados o utilizando la función "Copiar Todos". Esta característica copia únicamente los puntos en la carpeta abiertas a la ventana de puntos seleccionados. La característica "Eliminar Todo" elimina todos los puntos que se muestran en la ventana de puntos seleccionados para la pestaña que está abierta.

Buscar – los campos de búsqueda permiten al usuario buscar los puntos disponibles y los puntos seleccionados para conocer los términos específicos. Los puntos que contienen estos términos de búsqueda se enumeran en orden numérico.

Ordenamiento de puntos seleccionados – puntos seleccionado pueden ser reordenadas para que coincida con los de usuarios SCADA, RTU o configuración maestro seleccionando, arrastrando y soltando el punto deseado dentro de la ventana de puntos seleccionados.

Agregando puntos falsos (dummy) – el propósito del punto ficticio es permitir al usuario que coincida con otros mapas DNP de dispositivos que contienen puntos que no son compatibles con el control. Esta característica permita al usuario comunicarse con el Control M-7679 R-PAC cuando está conectado a una RTU que contiene otros tipo de controles y elimina la necesidad de re-configurar la RTU o los otros controles.

Para insertar un punto ficticio, seleccione **Insert Dummy**. El punto ficticio se insertará al final de la lista de Puntos Seleccionados. Para mover el punto Ficticio, seleccionar, arrastrar y soltar el punto en la ubicación deseada en la lista de Puntos Seleccionados. El punto Ficticio asumirá la posición de índice y los puntos seleccionados restantes serán modificados para acomodar el Punto Ficticio.

Insertar desplazamiento – esto permite crear un desplazamiento en el mapa DNP sin el número de punto de inicio para transmitir, lo que proporciona la capacidad de construir un perfil de DNP sin la necesidad de números consecutivos dentro de un grupo.

Edición de puntos de entrada binaria – el "Valor" y "Máscara" de una entrada binaria pueden ser editados con un doble clic izquierdo sobre el punto deseado en los elementos de Valor o Mascara. El valor predeterminado para los Valor es TRUE, lo que significa que el punto mostrara un Alto o Verdadero cuando el punto monitoreado se active en el control. Puede ser cambiado a "FALSO" para coincidir con una Maestra SCADA si es necesario. El valor de "Mascara" por defecto es "CLASS ONE" y define qué tipo de clase de recolección es asignada al punto mapeado. El valor de mascara también puede ser asignado a CLASE DOS o TRES haciendo doble clic en el elemento de mascara del punto deseado.

Edición de puntos de entrada análoga – la "Deadband (Banda Muerta)" y la "Mask" de una entrada análoga pueden ser editados con un doble clic izquierdo sobre el punto deseado en los elementos de Banda Muerta o Mascara. La Banda Muerta puede ser definida cuando el punto reportara por excepción a una maestra. Cuando el valor del punto excede el valor de banda muerta, iniciará un informe de excepción al maestro. El valor de "Mascara" por defecto es "CLASE DOS" y define qué tipo de clase de recolección es asignada al punto mapeado. El valor de mascara también puede ser asignado a CLASE UNO o TRES haciendo doble clic en el elemento de mascara del punto deseado.

Edición de Salidas Binarias de Control – Los Valores de "Crob", "Mascara" e "Inverso" de las Salidas Binarias de Control pueden ser editados con un doble clic izquierdo sobre el punto deseado en los elementos de Crob, Mascara o Inverso. El ajuste Crob (Control Relay Output Block) (Control de Relevador de Boque de Salida) se utiliza para definir el método que se usara para operar el punto. Los posibles ajustes de "Crob" se enlistan a continuación:

- Latch On
- Latch Off
- Latch OnOff
- Latch OnOff_TC
- Pulse On
- Pulse Off
- Pulse OnOff
- Pulse OnOff_TC
- Paired Close
- Paired Trip
- Paired TripClose

El valor por omisión de "Mask" es "CLASS ZERO" y define el tipo de clase de poleo en que el punto es mapeado. El valor del parámetro Mask se puede editar haciendo doble clic sobre el elemento deseado del punto Mask y configurando dicho parámetro como CLASS NONE.

Inverso define si el comando que se enviará se invierte, lo que significa que cuando se selecciona TRUE, enviando una Apertura, Cerrar, etc. este tendrá el efecto contrario. Esto se llevó a cabo debido a las variaciones observadas en la aplicación de varios fabricantes de RTU, de control directo con DNP para permitir la plena compatibilidad del mayor número posible de RTU.

Edición de Puntos de Salida Análogos – el valor de "Máscara" de Salida Análoga puede ser editado haciendo doble clic en el punto de elemento Máscara. El valor por omisión de "Mask" es "CLASS ZERO" y define el tipo de clase de poleo en que el punto es mapeado. El valor del parámetro Mask se puede editar haciendo doble clic sobre el elemento deseado del punto Mask y configurando dicho parámetro como CLASS NONE.

Edición de Contadores – el valor de Contadores "Mascara" puede ser editada con un doble clic izquierdo sobre el punto deseado en el elemento de Mascara. El valor por defecto "Máscara" a "CLASE TRES" y define que tipo de clase de búsqueda es mapeado. El valor de mascara también puede ser asignado a CLASE CERO, CLASE UNO, CLASE DOS, SIN CLASE, CLASE UNO NO CLASE 0, CLASE DOS NO CLASE 0 o CLASE TRES NO CLASE 0 haciendo doble clic en el elemento de mascara del punto deseado.

Seguridad DNP – la autentificación DNP está ahora disponible y puede ser habilitada independientemente en la pestaña de seguridad de DNP para las interfaces seriales o Ethernet (ambos tipos TCP o UDP).

Los conceptos de Código de Autentificación de Mensajes (HMAC) y desafío – respuestas como están definidas en la especificación DNP3 para Autentificación Segura Versión 2.0 están implementadas.

Cuando la Autentificación está habilitada, los siguientes ajustes deben ser seleccionados:

- Algoritmo HMAC y Clave de Actualización
- Tiempo Transcurrido de Respuesta a Desafíos
- Duración de sesión con Clave
- Modo Agresivo
- Códigos de Funciones de Solicitudes Críticas

■NOTA: Antes que el IPScom permita al usuario actualizar la clave, el usuario tendrá que introducir la clave anterior.

Algoritmo HMAC y Actualización de Clave – el algoritmo HMAC es cualquiera de estos SHA1 (4 OCT) o SHA1 (10 OCT). Una actualización de clave necesaria para proveer una clave de SESIÓN segura. Una vez una clave de SESIÓN es obtenida cualquier desafío/respuesta subsecuente empleara la clave de sesión. La clave de actualización puede tener hasta 32 caracteres hexadecimales (0123456789ABCDF) (128 bits).

Tiempo de espera de respuesta de desafío – el rango es de 0 – 100 segundos. Este es el tiempo de respuesta en el que el control está esperando una respuesta a un desafío.

Duración de Sesión con Clave – esta duración se debe configurar en minutos (0 – 100) y en cuentas de 0 – 65535. Esta duración representa el tiempo máximo o el número máximo de desafíos que una sesión particular con clave antes de que se realiza de nuevo la negociación de claves.

Modo Agresivo – Un intercambio de Desafío/Respuesta completo incrementa el número de mensajes en el protocolo, lo que afecta el rendimiento del procesamiento. Por lo tanto, la autentificación de seguridad de DNP ofrece un modo agresivo en el que los datos de un solo desafío se pueden utilizar para autenticar muchos mensajes posteriores. El remitente del mensaje crítico incluye el HMAC al final del mensaje crítico sin tener que ser desafiado. Al menos un desafío debe ocurrir, sin embargo, antes de que el modo agresivo puede ser utilizado.

Códigos de Funciones de solicitudes Criticas – esto representa los códigos de función que se requieren para la autentificación, si esta fue seleccionada. Si no hay ninguna seleccionada, la autenticación no se puede realizar en cualquier código de función de autenticación, aunque este activado.

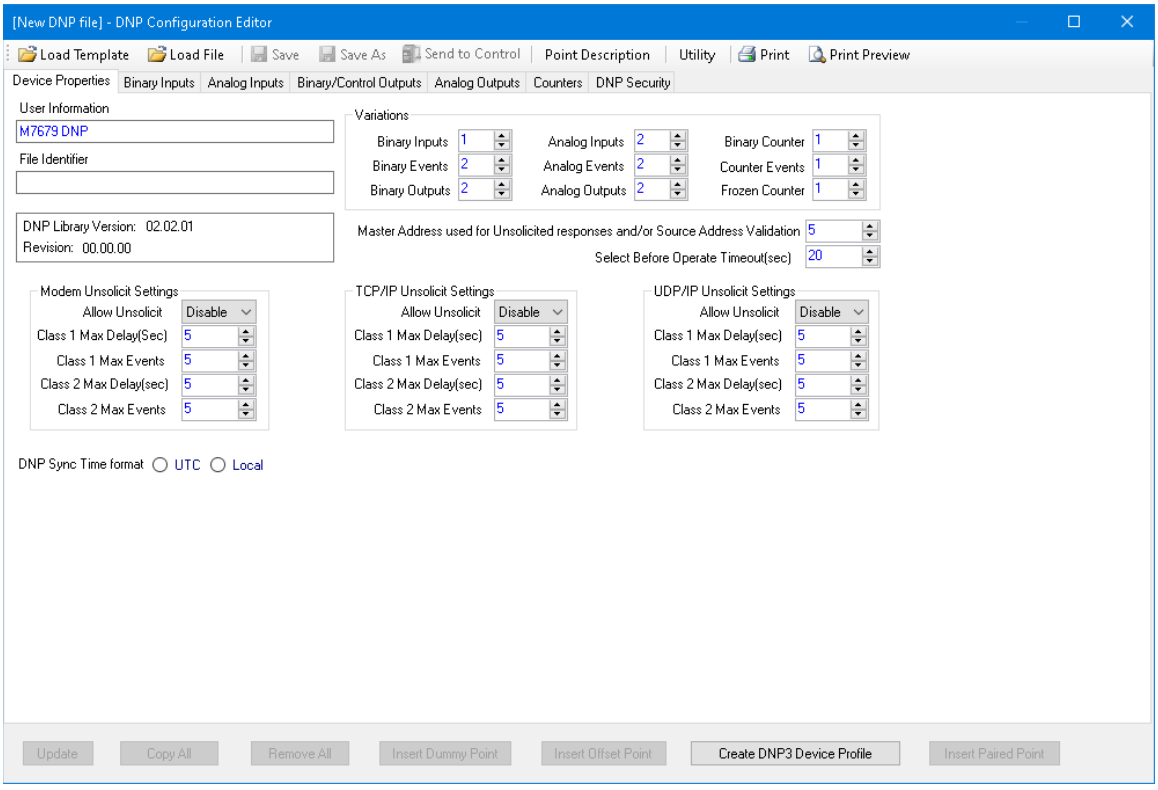


Figura 1-1 Pantalla de editor de configuración DNP

Pestañas de objetos del editor de configuración de DNP – cada objeto de DNP se puede configurar seleccionando la pestaña correspondiente en la ventana principal del editor: Entradas binarias, entradas analógicas, salidas binarias/control, salidas analógicas y contadores.

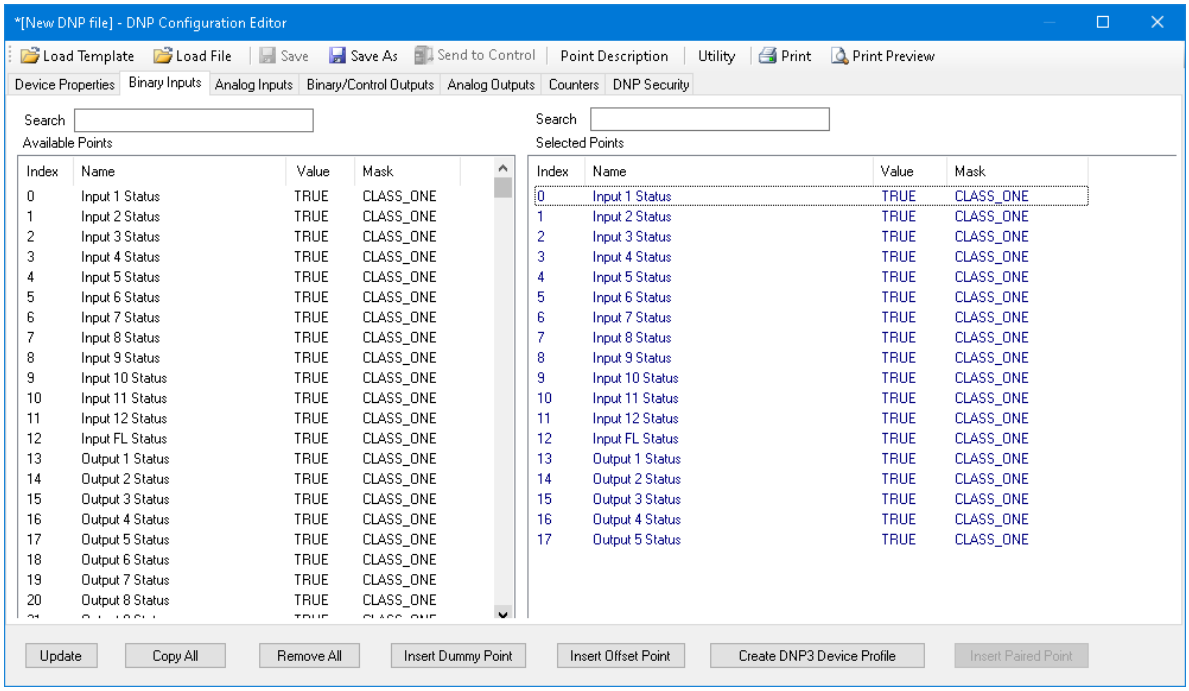


Figura 1-2 Editor de configuración DNP – Pestaña de Entradas binarias

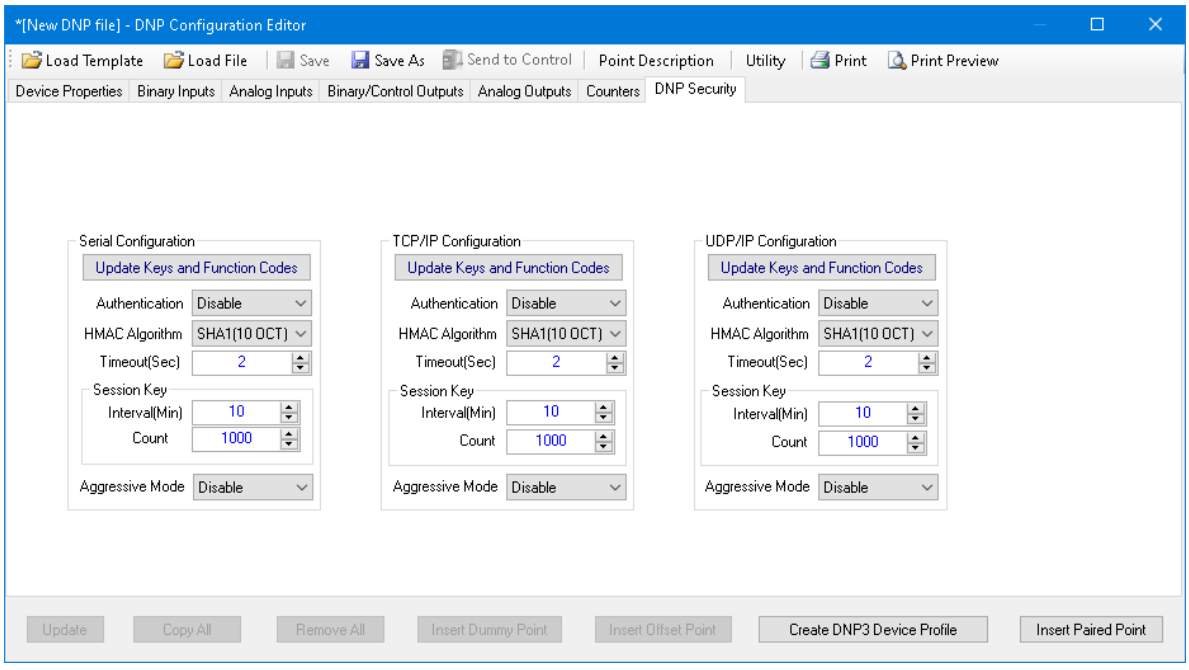


Figura 1-3 Editor de configuración DNP – Pestaña de seguridad DNP

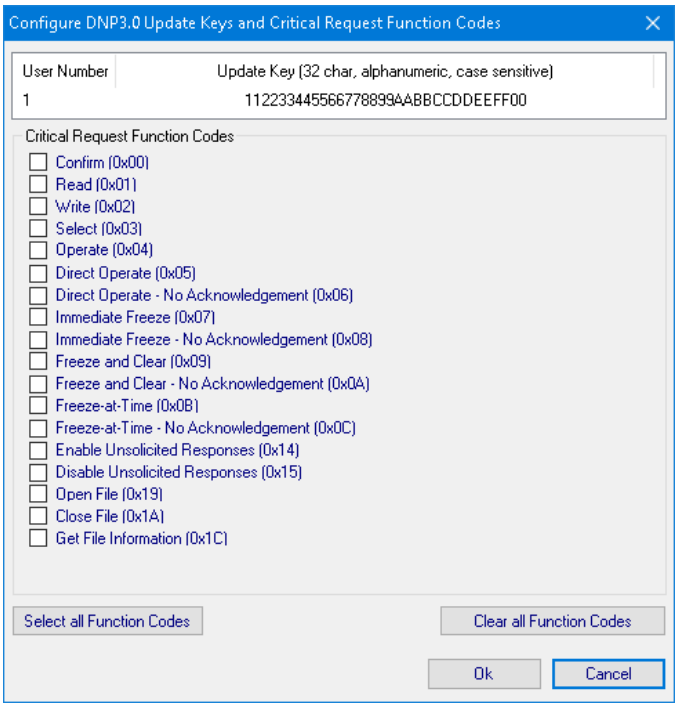


Figura 1-4 Pantalla de DNP actualizar claves y códigos de petición de función critica

Ejemplo de uso del Editor de Configuración DNP – la siguiente secuencia de pasos proporciona un ejemplo de la utilización del Editor de Configuración DNP.

1. Desde la Pantalla Principal de IPScom S-7600 Software de Comunicaciones seleccione **Communication/Protocol/DNP/DNP Configuration Editor**. IPScom mostrará la pantalla de Editor de Configuración DNP (Figura 1-1).
2. Seleccione **Load Template/M-7679 Default** desde la barra de menú configurador DNP. Seleccione la pestaña de **Binary Inputs**, Figura 1-2 es desplegada. La lista de Puntos Disponibles para cada Grupo de Puntos DNP también será poblado.
3. Seleccione los puntos de entradas binarias que desea incluir en el mapa DNP seleccionando Copiar Todo o arrastrando el (os) punto (s) deseado(s) a la ventana de Puntos Seleccionados.
4. Edite los puntos seleccionados para cada ficha si es necesario para que coincida con su SCADA, RTU o configuración Maestro.
5. Seleccione **Save File** (Guardar Archivo) de la barra de menú en el DNP Configurator. IPScom mostrará una pantalla de "Guardar Como" con una extensión de archivo *.xml.
6. Escriba el nombre del archivo y seleccione **Save** (Guardar).
7. Si IPScom está conectado al control destino entonces puede usar "Enviar al Control" desde el menú como sigue:
    a. Seleccione **Send to Control** (Enviar al Control). IPScom mostrará la pantalla de "Abrir Archivo" con una extensión *.xml.
    b. Seleccione el archive de a ser enviado al control, después seleccione **Open**. IPScom iniciará la transferencia de archivo como se indica en la pantalla de dialogo "Upload" (Figura 1-5), seguida por una pantalla de confirmación "Archivo DNP enviado con éxito".

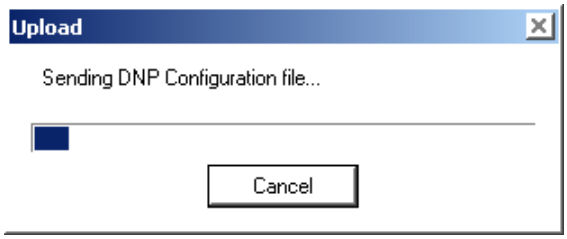


Figura 1-5 Pantalla de estado del archivo de configuración de envío DNP

2.0 S-1100 Utilidad de Actualización Ethernet Remota de Archivo (M-7679 R-PAC solamente)

■ NOTA DE SEGURIDAD CIBERNETICA:
Cuando se habilita la Seguridad cibernética, el acceso a alguna de las funciones descritas en este Sección está sujeta a la política de permisos de acceso designadas por el administrador de la Política de seguridad.

S-1100 Utilidad de Actualización Ethernet Remota de Archivo (REFU)

■NOTA: La utilidad REFU S-1100 solo está disponible para el M-7679 R-PAC.

La utilidad REFU es una aplicación de PC independiente. La utilidad REFU utiliza un algoritmo de transferencia de archivos que Beckwith Electric ha implementado en el firmware M-7679 para la transferencia de archivos como el Acceso de Usuarios, de Directivas IPsec y archivos de mapas dispositivo DNP. La utilidad REFU es capaz de funcionar detrás de cualquier firewall seguro o dentro de cualquier política de seguridad IT impuesta por un administrador local.

Figura 2-1 Icono del Programa de Utilería Ethernet de Actualización Remota de Archivo

Ethernet Actualización Remota de Firmware

El elemento de Ethernet Remota Actualización de Firmware de la aplicación Utilidad Ethernet de Actualización Remota de Firmware (REFU) permite al usuario actualizar el firmware de forma remota de uno o más controles a una nueva versión, utilizando una conexión Ethernet. La pantalla de Utilidad Ethernet de Actualización Remota de Archivo (REFU) se presenta en la Figura 2-2.

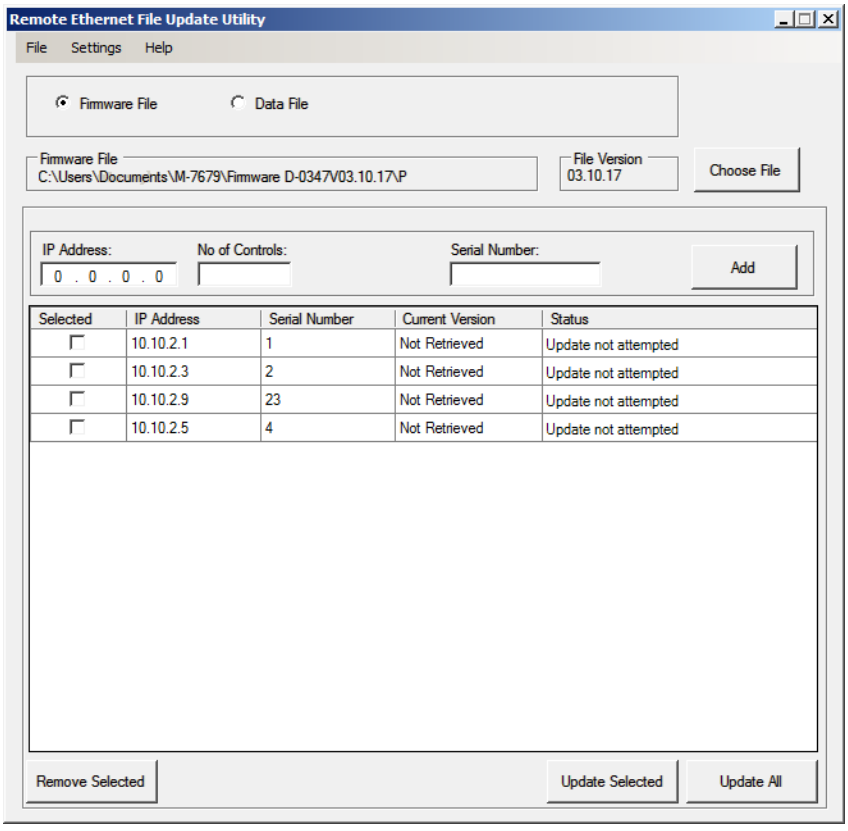


Figura 2-2 Pantalla de Utilidad Ethernet de Actualización Remota de Archivo (archivo de firmware)

Actualización Ethernet Remota de Firmware y Seguridad Cibernética

Para cumplir con los requerimientos de la Seguridad Cibernética, la utilidad REFU le pedirá una contraseña cuando se inicia. La contraseña por defecto es "BecoUpdate". Esta contraseña es configurable por el usuario (caracteres alfanuméricos y especiales) al iniciar el programa por primera vez, y también se puede cambiar en el menú **File/Password**.

Debido a la naturaleza sensible de esta utilidad, es altamente recomendable no distribuir esta aplicación para los usuarios no autorizados. Por lo tanto, esta aplicación no estará disponible para su descarga desde el sitio web de Beckwith Electric. Por otra parte, sólo está disponible previa solicitud por escrito del personal autorizado.

La aplicación Remote Ethernet Firmware Update permite al usuario actualizar de forma remota el firmware de los controles específicos.

Como medida de seguridad adicional, el protocolo REFU debe ser habilitado utilizando IPScom o desde el panel frontal IHM. Para activar el protocolo REFU en IPScom, vaya a la pantalla de Protocolo de Acceso **Communication/Setup/Comm Port Security/Protocol Access**. Seleccione **Enable REFU** (Figura 2-3).

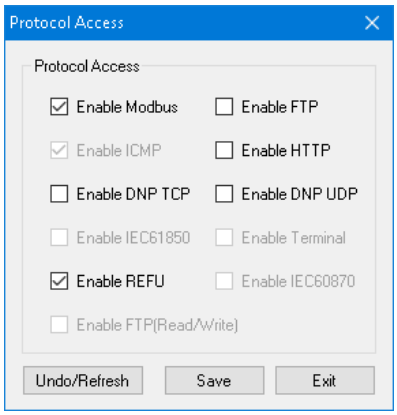


Figura 2-3 Pantalla de Seguridad de Puerto de Comunicaciones/Protocolo de Acceso

Para activar el protocolo REFU utilizando la IHM, vaya a pantalla del menú de **Actualización FW Remoto Communication/Comm Ports Security/Protocol Access**. Seleccione **ENABLE**.

```
Remote FW Update
ENABLE
```

Características Adicionales

Estas características se aplican tanto a los modos de Firmware y Archivos de Datos:

- El usuario puede seleccionar para cada control, qué archivo (s) se actualiza mediante la selección de las casillas de verificación correspondientes.
- La utilidad puede generar automáticamente las Direcciones IP consecutivas, dada una Dirección IP de inicio y el número de controles en ese rango de Direcciones IP. Es importante tener en cuenta que la verificación del número de serie por la utilidad no se realiza cuando se utiliza esta función.
- Los usuarios también pueden copiar y pegar la Dirección IP y el número de serie de una hoja de cálculo Microsoft® Excel® en la vista de cuadrícula de datos de la utilidad REFU. Los datos se pueden pegar usando la tecla "Ctrl + V" o utilizando el botón derecho del ratón y seleccionando "Pegar".

■**NOTA:** El usuario no puede Copiar/Pegar sólo el número de serie. La selección debe ser (dirección IP + número de serie) o (dirección IP solamente).

La información contenida en la hoja de cálculo debe ser almacenado como se muestra a continuación para utilizar la característica de Copiar/Pegar:

10.10.2.1	1
10.10.2.3	2
10.10.2.9	23
10.10.2.5	4

Procedimiento de Actualización Ethernet Remota de Firmware

■**NOTA:** Estas instrucciones describen los pasos necesarios para llevar a cabo una actualización del firmware de forma remota utilizando la interfaz de usuario proporcionada por la Utilidad de Actualización Ethernet Remota de Archivo. El diálogo real entre la utilidad REFU y el Control se describe en detalle en la sección de Secuencia de Actualización de Firmware de este Sección.

Para actualizar de forma remota el firmware de un control o una serie de controles en una red Ethernet proceder como sigue:

1. Verifique que existan las siguientes condiciones:
   - La Utilidad de Actualización Ethernet Remota de Archivos (REFU) está instalado y en ejecución en una computadora con acceso a la red Ethernet de destino.
   - Está disponible un archivo ".ppf" (Archivo de paquete de programa) que contiene el firmware que se actualizará.
2. Iniciar la Utilidad de Actualización Ethernet Remota de Archivo (REFU). Se mostrará la pantalla de REFU (Figura 2-2).
3. Seleccione "Firmware File".
4. Seleccione "Choose File". La utilidad mostrará la Figura 2-4 que permite al usuario seleccionar el producto aplicable.

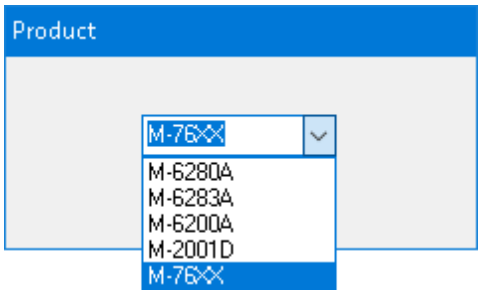


Figura 2-4 REFU Lista Desplegable de Seleccionar Producto

5. Seleccione el archivo ".ppf". La utilidad:
   - Rellene el campo "Archivo de Firmware" con el nombre de ruta/archivo
   - Abrir el archivo seleccionado y recuperar y descifrar la información de versión y rellenar el campo "Versión del Archivo" con la versión de firmware.
6. Introduzca la dirección IP y el número de serie del control a ser actualizado.
7. Seleccione "Add". La información se añadirá a la lista de controles a actualizarse. Repita el Paso 6 para cualquier otro control a ser actualizado.

   El usuario puede crear una lista de controles que tendrán su firmware actualizado. Esta lista puede ser guardada si se desea y puede ser recuperada para su uso en una fecha posterior. La lista de los controles y su información asociada (a excepción de la "Update to Version") se almacena en un formato codificado.

8. En el menú desplegable Settings seleccione el número de "Reintentos" para intentarse si hay alguna falla de actualización del firmware de algún control.

   El número máximo de reintentos es 10. El número predeterminado de reintentos es 3. El rango es de 0 a 10.

9. Seleccione los controles a ser actualizados.
10. Seleccione "Update Selected" o "Update All" para iniciar la secuencia de actualización.

    La Utilidad REFU iniciará la secuencia de actualización para cada control. La secuencia es descrita en detalle en la Secuencia de Actualización de Firmware más adelante en este documento.

Resumen de secuencia de actualización de firmware

1. La Utilidad REFU abre una conexión TCP en el puerto 62000.

■NOTA: Puerto 62000 debe estar disponible a través del firewall del usuario para que REFU funcione.

2. La Utilidad REFU inicia la sesión de Autenticación mediante el envío de una firma hash cifrado.
3. El Control verifica la cadena de hash cifrado recibido.
4. Si el control no puede verificar la cadena de hash cifrado recibido, a continuación, la conexión se cierra automáticamente por el Control.
5. Si la verificación de cadena de hash recibido es exitosa, entonces el Control pasa al modo de programación.
6. La Utilidad REFU entonces consulta el Control por la versión del firmware instalado en el Control y si se selecciona, el número de serie del Control.
7. La Utilidad REFU comparará la versión de firmware instalada recibida desde el Control y, si es seleccionado, el número de serie con el número y la versión del filtro de serie interno de la Utilidad REFU, y continúa de la siguiente forma:
   - Si se determina que la versión del firmware instalado es una versión de firmware que no admite la Actualización Ethernet Remota de Firmware, y/o si es seleccionado, el número de serie no coincide, entonces después de que el número seleccionado de intentos también han fallado entonces la Utilidad de REFU cerrará la conexión.
   - Si la comparación se realiza correctamente, entonces el procedimiento de actualización continúa.
8. La Utilidad REFU comienza la carga de archivos al control.
9. Cuando el archivo está completamente cargado al Control, el control va a verificar la firma digital del firmware.
10. Basándose en los resultados de la comprobación, el control se procederá como sigue:
    - Si la verificación de la firma digital no tiene éxito, entonces el Control enviará el mensaje de error apropiado a la Utilidad REFU y terminará la sesión de actualización.
    - Si la verificación de la firma digital es exitosa, entonces la secuencia de programación continuará.
11. Antes de programar la memoria flash, se toman las siguientes medidas:
    a. Un bloqueo de todas las operaciones automáticas y remotas se activa, dejando el estado del Control sin cambios.
    b. Todas las operaciones en curso se terminan.
    c. Todos los puntos de ajuste y datos de calibración se copian en la memoria flash interna de datos.

▲PRECAUCIÓN: El proceso de actualización, desde borrar el Programa Flash hasta completar la reprogramación tarda aproximadamente 15 segundos. Cualquier error o pérdida de energía después de que el flash se ha borrado serán fatales para el control.

12. La programación flash se inicia de la. Si por alguna razón el borrado o la programación del Programa Flash no tienen éxito, entonces el Control dará por terminado el proceso de actualización y volverá a la ejecución normal del programa sin necesidad de reiniciar.

    El Control también notificará a la Utilidad REFU enviando el mensaje de error apropiado cuando se les pregunta. Este tipo de error puede resultar en que el Programa Flash no está completamente programado. Por lo tanto, el usuario debe volver a intentar actualizar el firmware de nuevo. Una pérdida de energía en esta condición dará lugar a que el Control no sea capaz de reiniciar correctamente.

13. Cuando la quema del firmware en el programa flash se ha completado, el Control se Reiniciará.
14. Cuando el Control ha completado el proceso de reinicio, el Control comenzará su operación normal sujeto de los valores de puntos de ajustes previamente guardados y los datos de calibración.
15. Después de que el Control ha completado su proceso de reinicio la Utilidad REFU volverá a abrir una conexión TCP en el puerto 62000 y consultará para el número de versión del firmware.
16. Si el número de versión consultado no coincide con el número de versión programado, la aplicación de Utilidad REFU notificará al usuario del estado del proceso y permitirá al usuario repetir la actualización si se desea.
17. Si el número de versión consultado coincide con el número de versión programada, el proceso de programación ha sido exitosa.

Procedimiento de Actualización Remota del Archivo de Datos

Para actualizar de forma remota archivos de datos seleccionados de un control o una serie de controles en una red Ethernet proceder como sigue:

1. Verifique que existan las siguientes condiciones:
   - La Utilidad de Actualización Ethernet Remota de Archivos (REFU) está instalado y en ejecución en una computadora con acceso a la red Ethernet de destino.
   - El archivo deseado de "Acceso de Usuario", "Política de IPsec", o "Configuración DNP" está disponible.
2. Iniciar la Utilidad de Actualización Ethernet Remota de Archivo (REFU). Se mostrará la pantalla de REFU (Figura 2-2).
3. Seleccione "Data File". La pantalla de Archivo de Datos REFU se mostrará (Figura 2-5).
4. Seleccione "Choose File" para el archivo(s) a ser actualizados. La utilidad pedirá la ubicación del archivo y el nombre del archivo deseado.
5. Seleccione el archivo deseado. La utilidad rellenar el campo "Configuración DNP" con la ruta/nombre de archivo.
6. Introduzca la dirección IP y el número de serie del control a ser actualizado.
7. Seleccione "Add". La información se añadirá a la lista de controles a actualizarse. Repita el Paso 6 para cualquier otro control a ser actualizado.

   El usuario puede crear una lista de controles que tendrán sus archivos de datos actualizado. Esta lista puede ser guardada si se desea y puede ser recuperada para su uso en una fecha posterior. La lista de los controles y su información asociada (a excepción de la "Update to Version") se almacena en un formato codificado.

8. En el menú desplegable Ajustes seleccione el número de "Reintentos" para ser tratado si hay alguna falla de actualización de los archivos de datos en algún control.

   El número máximo de reintentos es 10. El número predeterminado de reintentos es 3. El rango es de 0 a 10.

9. Seleccione los controles a ser actualizados.
10. Seleccione los tipos de archivos deseados a ser actualizados en cada control individual.
11. Seleccione "Update Selected" o "Update All" para iniciar la secuencia de actualización.

    La Utilidad REFU iniciará la secuencia de actualización para cada control. La secuencia es descrita en detalle en la Secuencia de Actualización de archivos más adelante en este documento.

Resumen de Secuencia de Actualización de Archivos

1. La Utilidad REFU abre una conexión TCP en el puerto 62000.

■NOTA: Puerto 62000 debe estar disponible a través del firewall del usuario para que REFU funcione.

2. La secuencia de autenticación se inicia con el control. La secuencia de autenticación es similar a la autenticación de actualización del firmware.
   - Si la secuencia de autenticación falla, entonces la conexión se cierra automáticamente por el Control.
   - Si la secuencia de autenticación es exitosa, entonces el Control inicia el procedimiento de actualización.
3. La Utilidad REFU Inicia la carga de archivos.
4. La transferencia del archivo es completa.

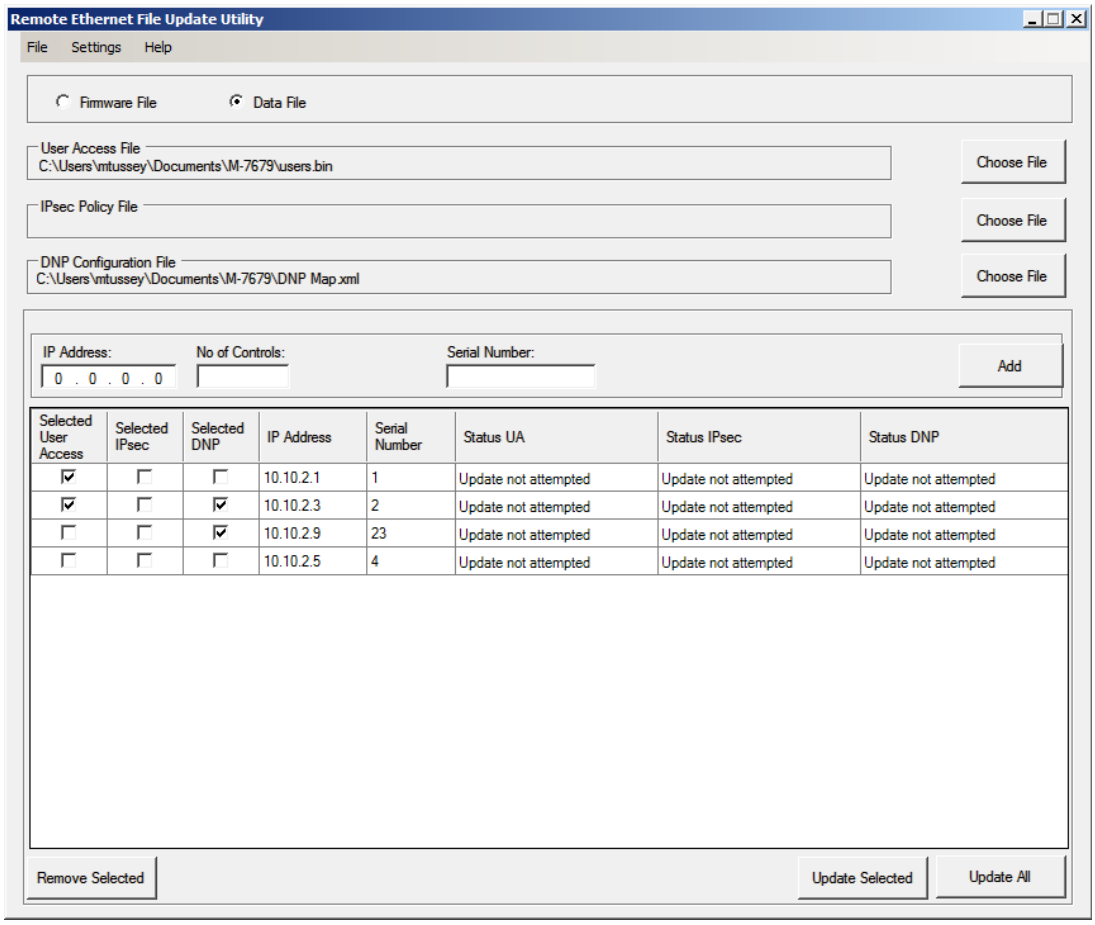


Figura 2-5 Pantalla de Utilidad Ethernet de Actualización Remota de Archivo (archivo de datos)

3.0 Seguridad cibernetica

■ NOTA DE SEGURIDAD CIBERNETICA:
Cuando se habilita la Seguridad cibernética, el acceso a alguna de las funciones descritas en este Sección está sujeta a la política de permisos de acceso designadas por el administrador de la Política de seguridad.

Esta sección describe los elementos de seguridad incorporados en el M-7679 R-PAC, y los ajustes y las opciones de configuración que son necesarios para permitir al unidad comunicarse de forma segura a través de Redes Privadas Virtuales (VPN).

El M-7679 R-PAC es compatible con los requisitos aplicables de la:

- IEEE 1686™-2007 Estándar para Dispositivos Electrónicos Inteligentes de subestación (IED's) Capacidades de seguridad cibernética
- IPsec/IKE
- Radius

IEEE ESTÁNDAR 1686

El M-7679 R-PAC cumple o excede los requisitos establecidos en la norma IEEE Estándar 1686, Estándar para Dispositivos Electrónicos Inteligentes de Subestación Capacidades de Seguridad cibernética (IED's). La Tabla 1 representa la Tabla de cumplimiento (TOC) del M-7679 R-PAC.

Permisos

La Norma IEEE 1686 en su mayor parte define las normas para Nombre de usuario, Contraseñas y los Permisos asociados a cada usuario. Las categorías de permisos específicos se enumeran en la Tabla 2 "Permisos implementados para el Estándar IEEE 1686".

DESCRIPCIÓN GENERAL IPSEC/IKE

IPsec/IKE es directamente compatible con M-7679 R-PAC. El Protocolo de Seguridad de Internet (IPsec) utiliza los servicios de seguridad criptográficos para proteger las comunicaciones a través del protocolo de redes Internet (IP). IPsec es un conjunto de protocolos especificados por la Grupo de Trabajo de Ingeniería de Internet (IETF) que añaden seguridad a la capa IP del tráfico de Internet.

La implementación de IPsec en el M-7679 R-PAC asegura el tráfico de Internet, incluyendo paquetes TCP y UDP. Los elementos importantes que son necesarios para proporcionar una seguridad de datos de red robusta incluyen el cifrado y la autenticación de igual importancia. La seguridad de la comunicación no puede existir sin una combinación tanto de cifrado, para evitar el monitoreo no autorizada de datos confidenciales, como de autenticación que valida la identidad de todas las partes implicadas en el plan de comunicación.

Clausula/ Sub-Clausula	Título de Clausula/ Sub-Clausula	Estado	Comentario
5	Características de Seguridad Cibernética IED	Conocimiento	
5.1	Acceso Electrónico al Control	Cumple	
5.1.1	Derrotar Mecanismos de Contraseña	Cumple	
5.1.2	Número Individual de ID/ Contraseña Soportada	Excede	El producto permite 32 combinaciones de individual ID/ Contraseña
5.1.3	Construcción de excepción en Contraseña letras mayúsculas y minúsculas son intercambiables.	Cumple	
5.1.4	Niveles de autorización por Contraseña	Cumple	
5.1.4.1	Ver Datos	Cumple	
5.1.4.2	Ver ajustes de configuración	Cumple	
5.1.4.3	Forzar Valores	Cumple	
5.1.4.4	Cambios de configuración	Cumple	
5.1.4.5	Cambios de Firmware	Cumple	
5.1.4.6	Administrar ID/Contraseña	Cumple	
5.1.4.7	Registros Auditables	Cumple	
5.1.5	Mostrar Contraseña	Cumple/Excepción	Excepto sobre LCD local
5.1.6	Temporización de Acceso	Cumple	
5.2	Seguimiento de Auditoría	Cumple/Excepción	Sólo puede ver los eventos de seguimiento de auditoría en la computadora
5.2.1	Capacidad de almacenamiento	Cumple	
5.2.2	Guardar registros	Cumple	
5.2.2.1	Número de Registro de evento	Cumple	
5.2.2.2	Fecha y hora	Cumple	
5.2.2.3	ID de usuario	Cumple	
5.2.2.4	Tipo de Evento	Cumple	
5.2.3	Tipos de Eventos de Seguimiento de Auditoría	Cumple	
5.2.3.1	Ingreso a sesión	Cumple	
5.2.3.2	Salir de sesión manual	Cumple	
5.2.3.3	Tiempo transcurrido	Cumple	
5.2.3.4	Forzando valores	Cumple	
5.2.3.5	Configuración de acceso	Cumple	
5.2.3.6	Cambio de configuración	Cumple	
5.2.3.7	Cambio de Firmware	Cumple	

Tabla 1 IEEE Estándar 1686 Tabla de cumplimiento (1 de 2)

Clausula/ Sub-Clausula	Título de Clausula/ Sub-Clausula	Estado	Comentario
5.2.3.8	Cambio de Firmware change	Cumple	
5.2.3.9	Borrar ID/Contraseña	Cumple	
5.2.3.10	Acceder a registros auditables	Cumple	
5.2.3.11	Cambio de Fecha y hora	Cumple/ Excepción	Indicado como un cambio de valor forzado
5.2.3.12	Incidente de alarma		
5.3	Monitoreo y control supervisorio		
5.3.1	Eventos	Excepción	Hecho a través del uso de DNP eventos no solicitados
5.3.2	Alarmas	Excepción	
5.3.2.1	Intento de inicio de sesión no exitoso		
5.3.2.2	Re-iniciar	Excepción	Sin embargo, los usuarios pueden deducir que un reinicio se ha llevado a cabo mediante el examen del bit de inicialización DNP 3.0 se establecen seguidos de una solicitud por tiempo DNP3.0.
5.3.2.3	Intento de uso de software de configuración no autorizado	Cumple	Una clave de cifrado pública deberá ser enviada por el control al software de cliente a petición. Esto se utiliza para autenticar si el software es válida mediante el cifrado de la identificación de usuario y contraseña con el algoritmo y la clave correcta. Esta función se puede activar/desactivar al no elegir "contraseña cifrada" para el nivel de acceso.
5.3.3	Detectar cambio de punto de alarma	Cumple	DNP 3.0
5.3.4	Agrupamiento de eventos y alarmas	Cumple/ Excepción	DNP 3.0 Clase de Poleo
5.3.5	Supervisiorio permisivo del control	Excepción	(TBD)
5.4	Software de configuración	Conocimiento	
5.4.1	Autenticación	Cumple	Ver 5.3.2.3
5.4.2	ID/contraseña del control	Excede	Inicialmente la contraseña es creada por el administrador. Una vez cambiado por el usuario, la contraseña no puede ser leída por cualquier persona.
5.4.3	Características de ID/ contraseña controlada	Cumple	
5.4.3.1	Ver datos de configuración	Cumple	
5.4.3.2	Cambiar datos de configuración	Cumple	
5.4.3.3	Acceso total	Cumple	
5.5	Acceso a puertos de comunicación	Cumple	
5.6	Firmware de aseguramiento de calidad	Cumple	

Tabla 1 IEEE Estándar 1686 Tabla de cumplimiento (2 de 2)

Categorías de Permisos (Acceso permitido)	Permisos por Defecto (X = Categoría de Permisos incluidos en el Grupo de Permisos por Defecto)										
	Ver Datos	Ver Puntos de ajustes	Cambios de puntos de ajustes	Leer archivos	Ver Config	Cambiar Config	Actualizar firmware	Administrar usuarios	Ver registro de auditoría	Control remoto	Cambiar Fecha/ Hora
Datos del monitor	X										
Ver puntos de ajustes		X									
Cambios de puntos de ajustes		X	X								
Ver configuración					X						
Cambiar configuración					X	X					
Configuración de histórico de datos					X	X					
Descarga de histórico de datos				X							
Configurar SOE					X	X					
Descargar SOE				X							
Configurar OSC					X	X					
Descargar OSC				X							
Registro de eventos de seguridad									X		
Administrar usuarios*								X			
Actualizar firmware							X				
Control remoto										X	
Cambiar Fecha/Hora											X
Traer archivo de LED				X							
Escribir al archivo de LED											
Traer archivo de botón				X							
Escribir al archivo de LED											
Escribir pantallas de despertar											
* El usuario puede cambiar la contraseña propia sin administrar los permisos de usuarios											

Tabla 2 Permisos implementados para el Estándar IEEE 1686

REVISIÓN DE RADIUS

Autenticación Remota Dial en Servicio de Usuario (RADIUS) es un protocolo de red que permite la administración de Autenticación centralizada, Autorización y Contabilización (AAA) para las computadoras que se conectan y utilizan un servicio de red. Autentificación y Autorización RADIUS se describen en el RFC 2865, mientras que la Contabilización se describe en el RFC 2866.

RADIUS es un protocolo cliente/servidor que se ejecuta en la capa de aplicación, utilizando UDP como transporte. Se utilizan los siguientes puertos UDP:

- Para Autenticación y Autorización de UDP el puerto 1812 (anteriormente 1645)
- Para Contabilización el puerto UDP 1813 (antes 1646)

RADIUS tiene tres funciones:

1. Autenticar a los usuarios o dispositivos antes de otorgarles acceso a una red
2. Autorizar a los usuarios o dispositivos para determinados servicios de red
3. Cuenta para el uso de dichos servicios

Mecanismo de Autorización de Contraseña

El M-7679 R-PAC incluye la capacidad para utilizar la Autenticación basada en el estándar IEEE 1686. Cuando IEEE 1686 de Seguridad por Contraseña está desactivada, el protocolo RADIUS aunque ajustable no es funcional. Cuando se implementa la Autenticación basado en IEEE 1686, entonces toda la funcionalidad del protocolo RADIUS está disponible. Las siguientes funciones están disponibles si RADIUS está habilitado:

- El M-7679 R-PAC ofrece capacidad de autenticación local SI Y SÓLO SI no hay otro servidor de autenticación remota disponible para el dispositivo. Un ejemplo de un servidor de autenticación remota es el servidor RADIUS.
- El M-7679 R-PAC tiene la capacidad de ser configurado para utilizar dos servidores de autenticación remota. Ejemplos son 2 servidores RADIUS. En caso de que el servidor principal está inactivo y no responda, se utilizará el servidor secundario, y, finalmente, si los dos servidores están inactivos, el dispositivo se regresa de nuevo al servidor local, lo cual es la autenticación de contraseña IEEE 1686.

El dispositivo se suministra con un archivo de contraseña por defecto configurado con un ID y la contraseña de Súper usuario. Corresponde al usuario final cambiar esta contraseña por defecto para garantizar la seguridad de la red. Por lo general, la contraseña local debe coincidir con la política de seguridad del servidor RADIUS.

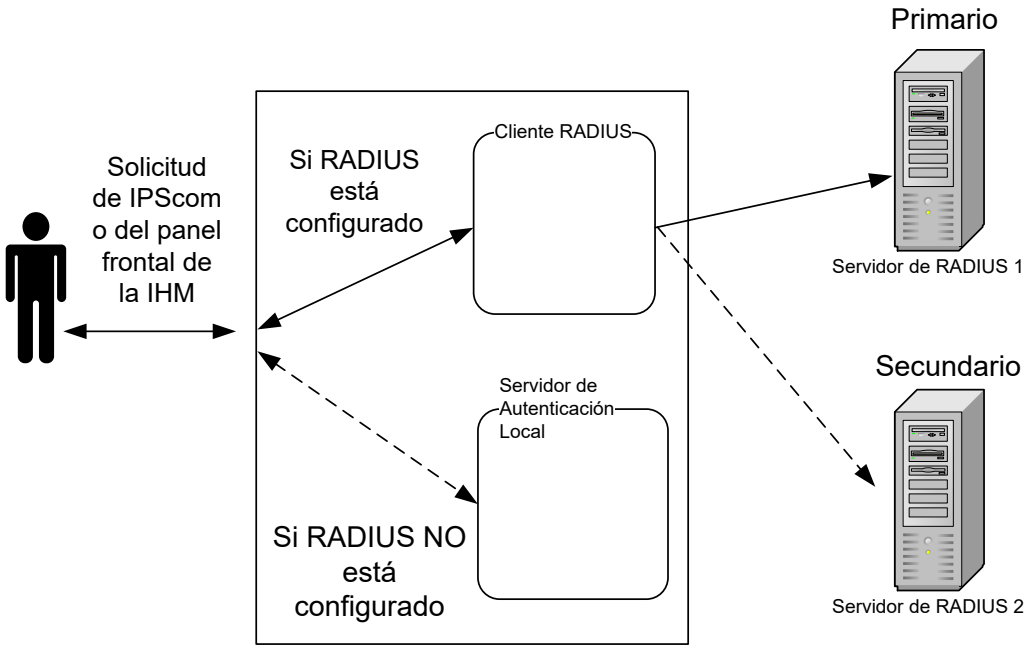


Figura 3-1 Configuración del Servidor RADIUS

Autenticación y Autorización

El firmware del M-7679 R-PAC incluye el cliente y el componente Servidor de Acceso Remoto (RAS) del protocolo RADIUS implementado. El unidad envía una petición a un Servidor RADIUS para obtener acceso a un recurso de red particular, mediante las credenciales de acceso. Las credenciales se pasan internamente a la RAS.

A su vez, el RAS envía un mensaje de Petición de Acceso RADIUS al servidor RADIUS, que solicita autorización para conceder el acceso a través del protocolo RADIUS. Esta solicitud incluye las credenciales de acceso, por lo general en forma de nombre de usuario y la contraseña proporcionada por el usuario. El puerto UDP 1812 se utiliza para comunicar con el servidor RADIUS.

El servidor RADIUS comprueba que la información es correcta mediante los esquemas de autenticación definidos. La identificación del usuario es verificada junto con la dirección de red y los privilegios del usuario.

El servidor RADIUS devuelve uno de tres respuestas al cliente:

- Acceso Rechazado
- Acceso Desafiado
- Acceso Aceptado

Contabilización

La Contabilización de flujo RADIUS se describe en el RFC 2866. El puerto UDP 1813 se utiliza para comunicarse con el servidor RADIUS para propósitos de contabilización.

Cuando el acceso a la red se concede al usuario por el cliente, un Inicio de Contabilización (un paquete de Solicitud de Contabilización RADIUS que contiene un atributo Acct-Status-Type con el valor "start") es enviado por el cliente al servidor RADIUS para señalar el comienzo de acceso a la red del usuario. Los registros "Inicio" suelen contener la identificación del usuario, dirección de red, punto de unión y un identificador de sesión único.

Periódicamente, los registros de actualización provisional (un paquete de Solicitud de contabilización RADIUS que contiene un atributo Acct-Status-Type con el valor "Provisional de actualización") pueden ser enviados por el cliente al servidor RADIUS, para actualizarlo sobre el estado de una sesión activa. Los registros "Provisionales" normalmente transmiten los cambios de puntos de ajustes del usuario.

Normalmente, el cliente envía paquetes de Contabilización-Solicitud hasta que recibe un acuse de recibo de Contabilización-Respuesta, mediante un intervalo de reintento.

En general, el propósito principal de estos datos es registrar la actividad del usuario (Conexión/Desconexión, cambios de puntos de ajustes, transferencia de archivos).

ID de Canal	Descripción
0	Interfase USB
1	Interfase Com sobre UART 0
2	Interfase Serial sobre UART 1
3	Interfase IHM
4	MODBUS Ethernet (se inicia desde el Canal 4 y se puede ejecutar hasta el canal 11 desde es compatible con ocho conexiones MODBUS Ethernet a la vez)

Tabla 3 Contador de RADIUS – Tabla de ID de Canal

AJUSTE DE SEGURIDAD CIBERNÉTICA (ESTÁNDAR IEEE 1686) DESDE IPSCOM

1. Inicie IPScom, establézcala comunicación con el unidad a conectar.
2. Seleccione **Utility/Manage Accounts/Set Access Password Type** desde la barra de herramientas de IPScom. IPScom mostrará la pantalla de "Tipo de contraseña de acceso" (Figura 3-2).

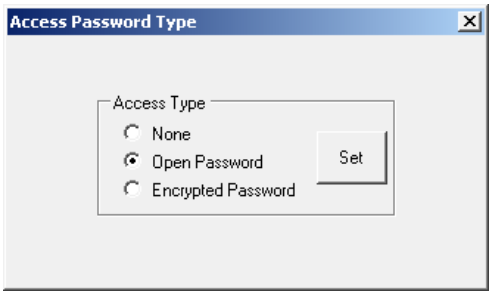


Figura 3-2 Pantalla de tipo de contraseña de acceso

■**NOTA:** El Nombre de usuario predeterminado es "admin1"
La contraseña por defecto es "admin1@M76XX"

3. Seleccione el nivel de acceso deseado y luego seleccione **Set**:
   - **Ninguno –** La Seguridad cibernética no está habilitada. El usuario no se le pedirá que introduzca un Nombre de usuario y contraseña y tendrá acceso a TODAS las características y funciones.
   - **Contraseña abierta –** La contraseña no está encriptada. Esta opción debe ser elegida cuando IPScom no es el único método de comunicación con el unidad.
   - **Contraseña cifrada –** La contraseña es encriptada y autenticada por el unidad para permitir que el usuario inicie sesión en el unidad. Sin embargo, esta selección sólo controla el cifrado de la contraseña de un inicio de sesión de usuario. Los archivos de Puntos de Ajuste y Contraseñas de los archivos contenidos en los Permisos de Cuenta se cifran.

CUENTAS DE USUARIO

■**NOTA:** El Nombre de usuario predeterminado es "admin1"
La contraseña por defecto es "admin1@M76XX"

El unidad contiene por defecto Nombres de usuario, contraseñas, y roles. Un usuario con el permiso **Administrar Usuarios** puede realizar el siguiente:

- Añadir/Eliminar un usuario
- Cambiar los permisos asociados a un usuario
- Asignar un usuario a un Rol específica
- Añadir/Eliminar un Rol
- Abrir/Guardar/Guardar Como, un archivo (.bin)
- Recuperar (Guardar Como) y Ver un Registro Auditable (.bkp)

Aunque el permiso Administrar usuarios le permite al usuario controlar todos los aspectos de un Usuario, el permiso Administrar usuarios no permite cambiar o ver la contraseña de un usuario más allá de establecer inicialmente la contraseña cuando se crea el Usuario. Sin embargo, el permiso Administrar usuarios puede eliminar la cuenta de usuario, cancelando efectivamente la contraseña.

La información de Cuentas de usuario reside en la memoria flash del unidad. Al recuperar (IPScom solamente) los datos se guardan en un archivo con una extensión de archivo (.bin). El archivo contiene toda la información de usuario (s) para la visualización y edición.

Al establecer inicialmente una contraseña o cuando se cambia una contraseña, la sintaxis de la contraseña debe ser conforme a los siguientes criterios:

- La longitud mínima debe ser de 8 caracteres
- La longitud máxima es de 20 caracteres
- Debe incluir al menos una letra mayúscula
- Debe incluir al menos una letra minúscula
- Debe incluir al menos un número
- Debe incluir al menos un carácter no alfanumérico (por ejemplo, @, %, *, etc.)

IPScom presenta los criterios de contraseña en letras rojas en las pantallas de "Cambiar contraseña" (Figura 3-10) y "Agregar usuario" (Figura 3-7). A medida que se cumplen los criterios para la contraseña ingresada, el "tipo" que establece los criterios que se han cumplido los cambios se presentan en negro.

Durante las operaciones "Recuperar permisos de cuentas desde el control" y "Enviar permisos de cuentas al control", se incluye toda la información de cuentas de usuario. Sin embargo, cuando se cambia una Contraseña, sólo la contraseña se escribe en el unidad.

■**NOTA:** Las instrucciones que se presentan en esta sección asumen que el usuario se ha concedido los permisos apropiados (Administrar usuarios) para acceder y realizar cambios en las características y capacidades.

Modificación y Ajuste de cuentas de usuario

El unidad contiene las cuentas de usuario por defecto. Las siguientes instrucciones describen:

- Modificación de permisos de cuentas recuperadas desde el unidad
- Modificación de un permiso de cuenta existente archivo (.bin)
- La creación de una nueva cuenta de usuario en un archivo de permisos de cuentas.

Modificación de permisos de cuentas recuperadas desde el unidad

1. Inicie IPScom, establézcala comunicación con el unidad a conectar.
2. Seleccione **Utility/Manage Accounts/Retrieve Account Permissions from Control** desde la barra de herramientas IPScom. Guarde el archivo de permisos de cuenta como desee.
3. En barra de menú de la pantalla de Administrar Permisos de Cuenta seleccione **File/Open**.
4. Vaya a la ubicación del archivo y seleccione el archivo que contiene los Permisos de cuenta del recuperados para ser modificados.
5. Seleccione **Open**. Siga las indicaciones de IPScom para ingresar el nombre de usuario y la contraseña asociados con el archivo seleccionado. Después de aceptar el inicio de sesión, IPScom mostrará la pantalla Administrar permisos de cuenta.

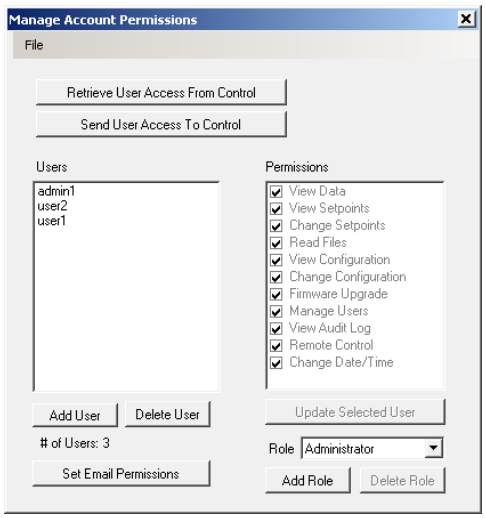


Figura 3-3 Administrar permisos de cuenta recuperados de la pantalla de control

6. Seleccione el **usuario** que se va a modificar.
7. Seleccione los Permisos deseados para el Usuario:
   - La activación o desactivación de los Permisos deseados
   - Selección de "Establecer Permisos de Correo" para agregar automáticamente los permisos necesarios para acceder a la función de Asistencia por Correo Electrónico:
     - Ver Datos
     - Ver Puntos de ajustes
     - Leer Archivos
     - Ver Configuración
     - Administrar Usuarios
     - Ver Registro de Auditoría
   - Selección de un **Rol** con permisos pre-definidos en el menú desplegable Rol (Figura 3-4)

Figura 3-4 Roles Pre-Definidos

8. Cuando se hayan introducido todos los permisos, seleccione **Actualizar Usuario Seleccionado**. El (.bin) original puede ser salvado (Archivo/Guardar) o guardado en un archivo de nombre y/o ubicación diferente (Archivo/Guardar como).
9. Desde la barra de menú de la pantalla de Administración de Permisos de Cuentas seleccione **File/Save** o **Save As**. IPScom mostrarán una pantalla de "Enviar Archivo" para permitir al usuario guardar el archivo en el unidad o en la computadora (Figura 3-5).

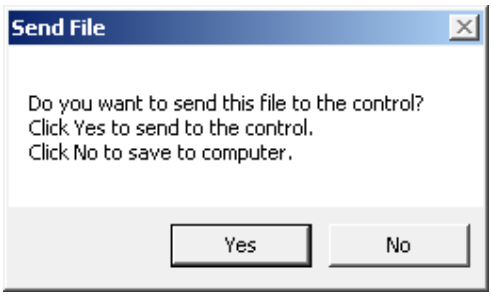


Figura 3-5 Pantalla de enviar archivo de usuario

10. Seleccione **Yes** para enviar el Archivo de Usuario al unidad. IPScom mostrará una pantalla de confirmación. Seleccione **OK**, IPScom cerrará las comunicaciones.
11. Seleccione **No** para guardar el Archivo de Usuario a la computadora. Si se seleccionó **File/Save As**, IPScom mostrar la ventana "User Access File" en la pantalla de Guardar Como.

▲PRECAUCIÓN: Es muy importante registrar el Nombre de Usuario y la Contraseña asociada al archivo guardado. La única manera de acceder al archivo es tener el nombre de usuario y la contraseña correctos. En el caso de escribir el archivo a un unidad, el unidad no podrá tener acceso y requerirá que el usuario se ponga en contacto con la fábrica para restaurar el Nombre de Usuario y la Contraseña predeterminados.

La modificación de Permisos de cuenta en un archivo de acceso de usuario existente (.bin)

1. Inicie IPScom, seleccione **Utility/Manage Accounts/Manage Account Permissions** en la barra de herramientas IPScom. IPScom mostrará la pantalla de "Administrar Permisos de Cuenta" (Figura 3-6).

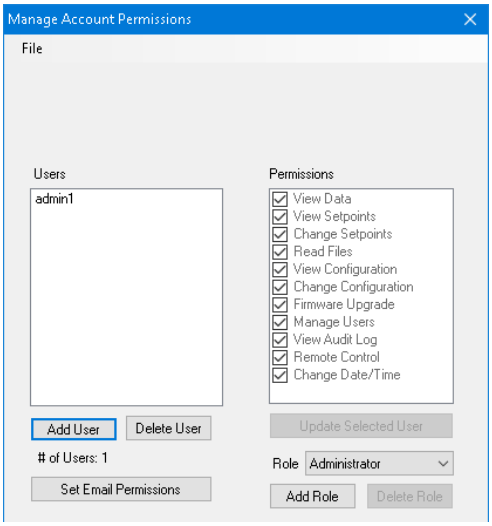


Figura 3-6 Pantalla de administrar permisos de cuenta

2. En barra de menú de la pantalla de Administrar Permisos de Cuenta seleccione **File/Open**. IPScom mostrará la pantalla abierta de archivo binario.
3. Navegue hasta la ubicación del archivo y seleccione el archivo de acceso de usuario (.bin) existente que se modificará.
4. Seleccione **Open**. IPScom mostrará un mensaje para el Nombre de Usuario y la contraseña asociados con el archivo seleccionado. Después de aceptar el inicio de sesión, IPScom mostrará la pantalla Administrar permisos de cuenta.
5. Seleccione el **usuario** que se va a modificar.
6. Seleccione los Permisos deseados para el Usuario:
   - La activación o desactivación de los Permisos deseados
   - Selección de un **Rol** con permisos pre-definidos en el menú desplegable Rol (Figura 3-4)
7. Cuando todos los permisos han sido seleccionados/no seleccionados, seleccione **Update Selected User**. El Archivo Binario original puede ser salvado (Archivo/Guardar) o guardado en un archivo de nombre y/o ubicación diferente (Archivo/Guardar como).

▲PRECAUCIÓN: Es muy importante registrar el Nombre de Usuario y la Contraseña asociada al archivo guardado. La única manera de acceder al archivo es tener el nombre de usuario y la contraseña correctos. En el caso de escribir el archivo a un unidad, el unidad no podrá tener acceso y requerirá que el usuario se ponga en contacto con la fábrica para restaurar el Nombre de Usuario y la Contraseña predeterminados.

El ajuste de una nueva cuenta de usuario en un archivo de acceso de usuario

1. Inicie IPScom, establézcala comunicación con el unidad a conectar.
2. Seleccione **Utility/Manage Accounts/Manage Account Permissions** en la barra de herramientas IPScom. IPScom mostrará la pantalla de "Administrar Permisos de Cuenta" (Figura 3-6).
3. Desda la barra de menú, seleccione **File/Open**. IPScom mostrará la pantalla abierta de archivo binario.
4. Navegue hasta la ubicación del archivo y seleccione el archivo de acceso de usuario (.bin) que se modificará.

5. Seleccione **Open**. IPScom mostrará un mensaje para el Nombre de Usuario y la contraseña asociados con el archivo seleccionado. Después de aceptar el inicio de sesión, IPScom mostrará la pantalla Administrar permisos de cuenta.
6. Seleccione **Add User**. IPScom mostrará la pantalla de "Agregar Usuario" (Figura 3-7).

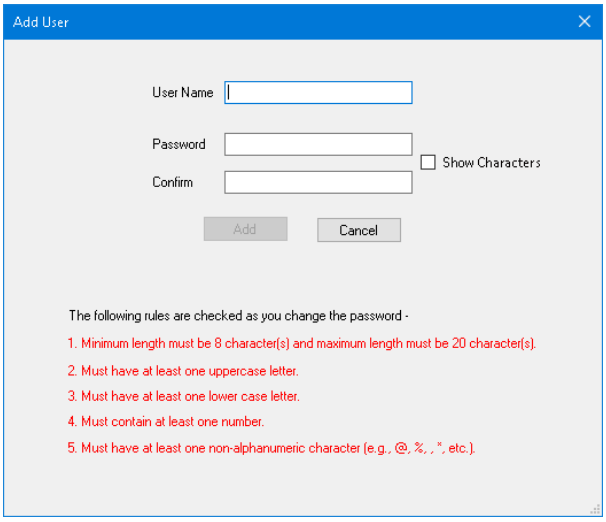


Figura 3-7 Pantalla de agregar usuario

7. Introduzca un Nombre de Usuario y la Contraseña válidos acorde con los criterios presentados en la sección Cuentas de Usuario al principio de este Sección.

   IPScom presenta los criterios de contraseña en caracteres rojos. A medida que se cumplen los criterios para la contraseña ingresada, el "tipo" que establece los criterios que se han cumplido los cambios se presentan en negro.
8. Cuando se han cumplido todos los criterios de Contraseña, a continuación, seleccione **Add**. IPScom volverá a la pantalla de "Administrar Permisos de Cuenta" (Figura 3-3) y mostrará al nuevo Usuario.
9. Seleccione el nuevo Usuario, después seleccione los Permisos:
   - La activación o desactivación de los Permisos deseados
   - Selección de un **Rol** con permisos pre-definidos en el menú desplegable Rol (Figura 3-4)
10. Cuando todos los permisos han sido seleccionados/no seleccionados, a continuación, seleccione **Update Selected User**.

▲PRECAUCIÓN: Es muy importante registrar el Nombre de Usuario y la Contraseña asociada al archivo guardado. La única manera de acceder al archivo es tener el nombre de usuario y la contraseña correctos. En el caso de escribir el archivo a un unidad, el unidad no podrá tener acceso y requerirá que el usuario se ponga en contacto con la fábrica para restaurar el Nombre de Usuario y la Contraseña predeterminados.

Roles

Cuando la S-7600 IPScom está instalado en el PC anfitrión, un archivo de Rol es creado y que contiene los roles predeterminados. Los cambios en los Roles existentes y la creación de nuevos Roles son capturados en este archivo. Sin embargo, Roles creados en otras instalaciones de PC IPScom pueden tener diferentes permisos para el mismo nombre de Rol. Agregar y eliminar "Rols" se lleva a cabo desde la pantalla de "Administrar Permisos de Cuenta" (Figura 3-6).

Recuperación de Permisos de cuenta desde el Control

1. Inicie IPScom, establézcala comunicación con el unidad a conectar.
2. Seleccione **Utility/Manage Accounts/Retrieve Account Permissions from Control** desde la barra de herramientas IPScom. IPScom mostrará una pantalla de diálogo "Archivo Binario" Guardar como.
3. Elija la ubicación de **Guardar como** y escriba el nombre del archivo deseado que contendrá los Permisos de Cuenta recuperados del unidad.
4. Seleccione **Save**. IPScom guardará el archivo (.bin) en la ubicación seleccionada.

Envío de Permisos de Cuenta al Control

1. Inicie IPScom, establézcala comunicación con el unidad a conectar.
2. Seleccione **Utility/Manage Accounts/Send Account Permissions to the Control** en la barra de herramientas IPScom. IPScom mostrará una pantalla abierta de archivo binario.
3. Vaya a la ubicación del archivo y seleccione el nombre del archivo deseado que contiene los Permisos de Cuentas para ser enviado al unidad.
4. Seleccione **Open**. IPScom intentará enviará el archivo seleccionado (.bin) de configuración al unidad de destino.
5. Si IPScom devuelve una pantalla de confirmación "No se pudo enviar el archivo Users.bin al Control" (Figura 3-8), a continuación seleccione **OK** y repita los Pasos 2 a 4.

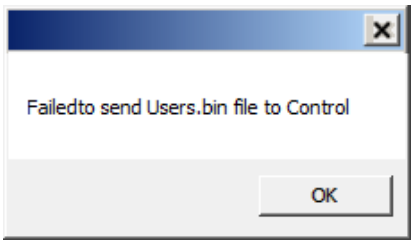


Figura 3-8 Pantalla de confirmación de falla de envío de archivo users.bin al control

6. Si la transferencia de archivos se realiza correctamente, IPScom mostrará una pantalla de confirmación "archivo de Permisos de Usuario enviado al control". Seleccione **OK**, IPScom cerrará las comunicaciones.

   Si se realiza algún cambio en los permisos que fueron enviadas al unidad, los cambios se aplicarán la próxima vez que el usuario inicia sesión en el unidad.

REGISTRO AUDITABLE

El Registro Auditable captura los eventos de seguridad en el orden en que se producen. El Registro Auditable se puede recuperar y visualizar en IPScom. El Registro Auditable se guarda en el PC con una extensión de archivo (.bkp). El Registro Auditable también se puede guardar como archivo de Valores Separados por Comas (.csv).

Cada entrada del Registro Auditable incluye:

- Fecha (mes, día, año)
- Tiempo (hora, minuto, segundo)
- Nombre de Usuario
- La Descripción del Evento considera:
  - Interfase USB
  - Interfase Com sobre UART 0
  - Interfase Serial sobre UART 1
  - Interfase IHM
  - Ethernet MODBUS: Ethernet MODBUS se inicia desde el Canal 4 y puede ejecutarse a través del Canal 11 desde el M-7679 R-PAC es compatible con ocho conexiones Ethernet MODBUS a la vez.

Recuperar, ver y salvar registro auditable

La siguiente secuencia de pasos describe recuperar, ver y guardar el Registro Auditable como un archivo (.bkp).

1. Inicie IPScom, establézcala comunicación con el unidad a conectar.
2. Seleccione **Utility/Manage Accounts/Audit Log/Retrieve** de la barra de herramientas IPScom. IPScom mostrará la pantalla de diálogo de la opción "Guardar Como" con el valor por defecto del archivo con extensión (.bkp).
3. Elija la ubicación de **Guardar Como** y escriba el nombre del archivo deseado que contendrá el Registro Auditable recuperado desde el unidad.
4. Seleccione **Save**. IPScom mostrará una pantalla de confirmación que el archivo se ha guardado.
5. Seleccione **OK**. IPScom mostrará automáticamente la pantalla de Registro Auditable (Figura 3-9).
6. Para ver un Registro Auditable previamente guardado, seleccione **Utility/Manage Accounts/ Audit Log/View**. IPScom mostrará la pantalla de diálogo de la opción "Audit Log file" con el valor por defecto del archivo con extensión (.bkp).
7. Navegue hasta el archivo deseado y seleccione **Open**. IPScom mostrará la pantalla de Registro Auditable (Figura 3-9).

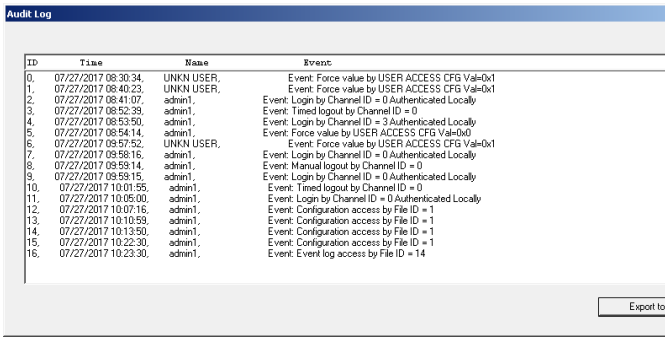


Figura 3-9 Pantalla de registro auditable

8. Para guardar el Registro Auditable que se muestra a un archivo con formato (.csv) seleccionar **Export to CSV**. IPScom mostrará una pantalla de confirmación de archivo guardado.

■**NOTA:** Puede que sea necesario seleccionar **Ver Carpetas Ocultos** en Windows para localizar el archivo CSV.

9. Seleccione **OK**. IPScom regresará a la pantalla de Registro Auditable.

CAMBIO DE CONTRASEÑA

La Contraseña asociada a un Nombre de Usuario específico sólo se puede cambiar mediante la conexión exitosa al unidad destino. Cuando **Change Password** está seleccionado en la pantalla de diálogo (Figura 3-10), sólo la nueva Contraseña se escribe al unidad.

Para cambiar la Contraseña de un usuario particular, haga lo siguiente:

1. Inicie IPScom, establézcala comunicación con el unidad a conectar.
2. Seleccione **Utility/Manage Accounts/Change Password** de la barra de herramientas IPScom. IPScom mostrará la pantalla de estado "Cambiar contraseña" (Figura 3-10).

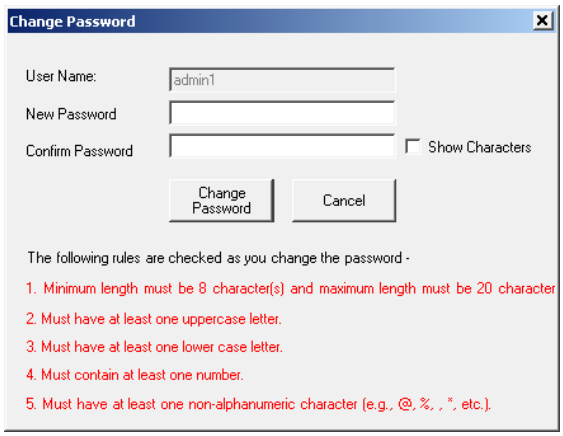


Figura 3-10 Pantalla de cambiar contraseña

3. Introduzca un nueva contraseña consistente con los criterios presentados en la sección Cuentas de Usuario al principio de este Sección.

   IPScom presenta los criterios de Contraseña en caracteres rojos. A medida que se cumplen los criterios para la contraseña ingresada, el "tipo" que establece los criterios que se han cumplido los cambios se presentan en negro.
4. Vuelva a ingresar la nueva Contraseña para confirmar.
5. Cuando se han cumplido todos los criterios de Contraseña, a continuación, seleccione **Change Password**. IPScom mostrará la pantalla de estado "Cambiando contraseña".
6. Cuando la Contraseña se ha cambiado en el unidad IPScom mostrará la pantalla de confirmación "Contraseña modificada Cerrar sesión" (Figura 3-11).

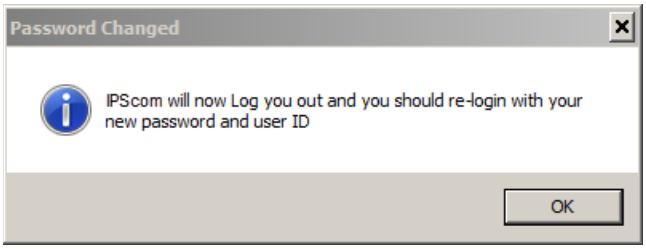


Figura 3-11 Pantalla de confirmación de salir de sesión contraseña guardada

7. Seleccione **OK**. IPScom cerrará la sesión del usuario actual. Para volver a iniciar sesión en el unidad se debe ingresar la nueva Contraseña.

AJUSTE DEL MODO SEGURIDAD

■**NOTA:** Las instrucciones que se presentan en esta sección suponen que el estándar IEEE 1686 ha sido habilitado y el usuario se ha concedido los permisos apropiados para acceder y realizar cambios en las características y capacidades de sujetos.

Configuración de RADIUS desde IPScom

Para configurar los elementos RADIUS del esquema de seguridad cibernética, realice lo siguiente:

1. Obtenga la siguiente información del Administrador de la Red:
   - Dirección IP del servidor primario / Puerto de autenticación / Puerto de contabilidad
   - Dirección IP del servidor secundario / Puerto de autenticación / Puerto de contabilidad
   - Clave Secreta
2. Inicie IPScom, establézcala comunicación con el unidad a conectar.
3. Seleccione **Communication/Setup/Communication Security/Radius Configuration** de la barra de herramientas IPScom. IPScom mostrará la pantalla de "Configuración de Radius" (Figura 3-12).

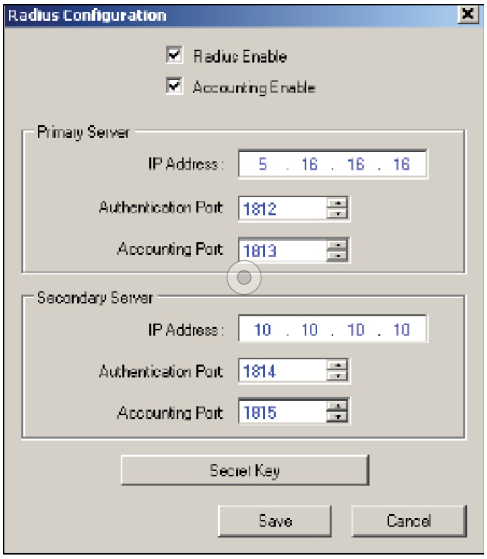


Figura 3-12 Pantalla de Configuración de Radius

4. Introduzca los ajustes necesarios en la pantalla de Configuración de Radius.
5. Desde la pantalla de Radius Configuration seleccione **Secret Key**. IPScom mostrará una pantalla de "Clave de Configuración de Radius" (Figura 3-13).

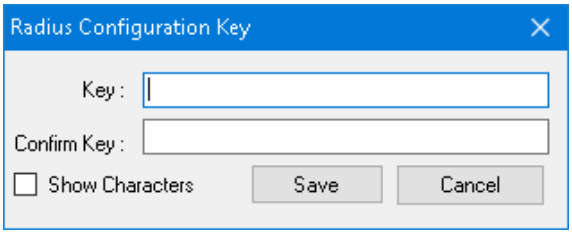


Figura 3-13 Pantalla de Clave de Configuración de Radius

▲**PRECAUCIÓN:** Es muy importante que la Clave de Configuración sea introducida correctamente. En el caso de que no se introduzca correctamente y Radius esté "Habilitado" el servidor Radius denegará el acceso al unidad ya que la Contraseña será encriptada de manera que el servidor Radius no puede descifrar correctamente.

6. Ingrese la Clave de Configuración de Radius.
7. Seleccione **Save**. IPScom escribirá la configuración de configuración de radio en el unidad.

Habilitar y configurar la seguridad de RADIUS desde la IHM

Seguridad RADIUS también se puede habilitar y configurar desde la IHM del panel frontal. La configuración para habilitar la seguridad RADIUS se encuentra en el menú COMMUNICATIONS/Port Settings/Comm Ports Security/Protocol Access. Los ajustes de configuración de RADIUS se encuentran en el menú COMMUNICATIONS/Port Settings/Ethernet/Settings menu.

IPsec Configuración desde IPScom

Para configurar los elementos IPsec del esquema de seguridad cibernética, realice lo siguiente:

1. Inicie IPScom, establézcala comunicación con el unidad a conectar.
2. Para habilitar IPsec desde IPScom, desde el menú desplegable **Communication/Setup/ Communication Security/IPSEC Configuration** seleccione **Enable**. IPScom mostrará la pantalla de confirmación "IPSec Enable" (Figura 3-14).

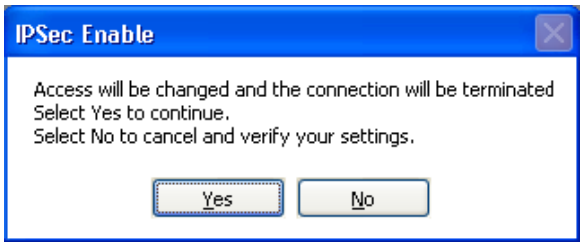


Figura 3-14 Pantalla de confirmación de habilitación IPSec

3. Para configurar IPsec, seleccione **IPSEC Configuration/Configure Endpoint**. IPScom mostrará la pantalla de "Configuración de Punto Final" (Figura 3-15) que permite al usuario añadir, editar, borrar o guardar Puntos Finales IPsec.

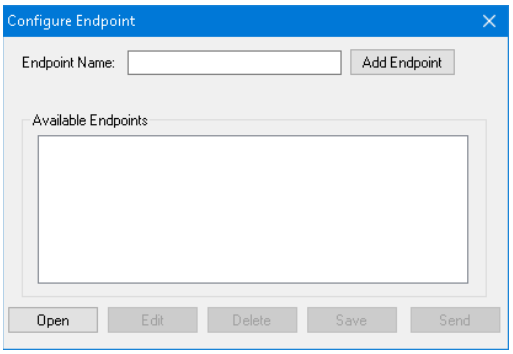


Figura 3-15 Pantalla de configuración de punto final de IPsec

4. Seleccione un Punto Final disponible en la pantalla "Configuración de Punto Final" y luego seleccione **Edit**. IPScom mostrará la pantalla de "Ajustes Generales IPsec" (Figura 3-16), que permite al usuario configurar los ajustes de seguridad IPsec, incluida la política IKE (Intercambio de Clave de Internet), de directivas IPsec, Política de Tiempos de Vida e Identidades.
5. Introduzca los ajustes necesarios en las fichas de la pantalla de Ajustes Generales IPsec (Figura 3-17 a Figura 3-19).

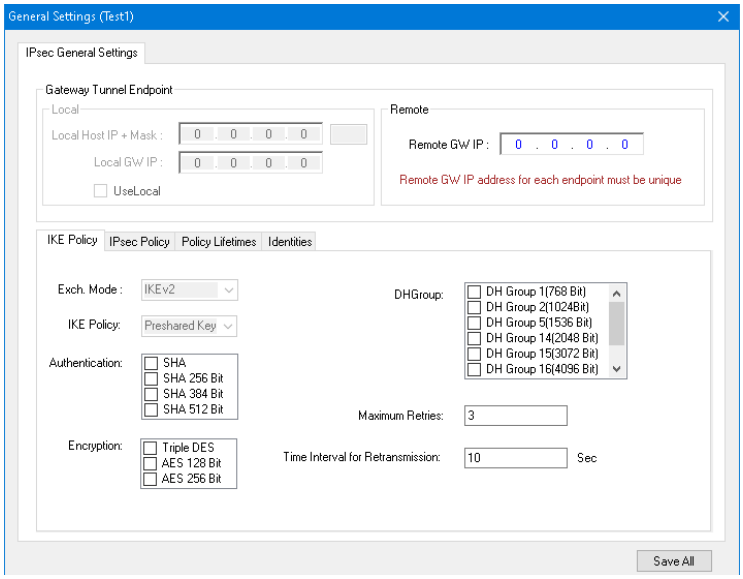


Figura 3-16 Pantalla de ajustes generales de IPsec

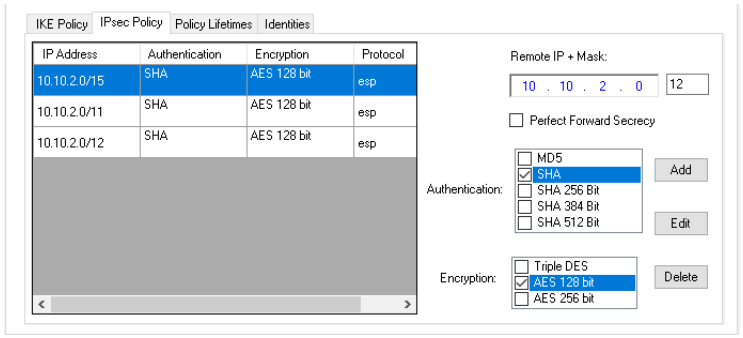


Figura 3-17 Ficha de Ajustes Generales IPsec – IPsec Políticas

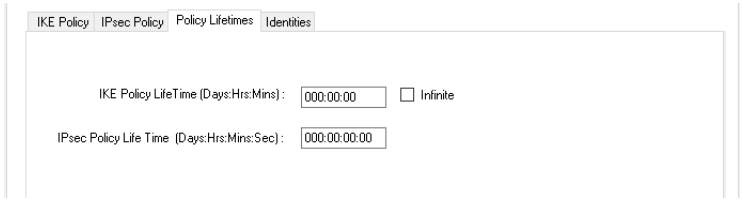


Figura 3-18 Ficha de Ajustes Generales IPsec – Política de Tiempos de Vida

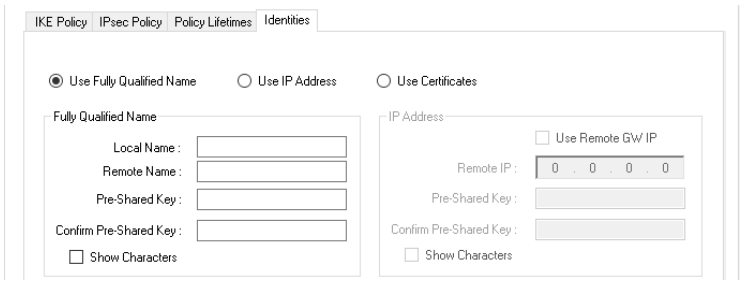


Figura 3-19 Ficha de Ajustes Generales IPsec – Identidades

6. Seleccione **Save All**. IPScom mostrará un Mensaje de Error para alertar al usuario de cualquier configuración necesaria que no ha sido introducida (Figura 3-20).

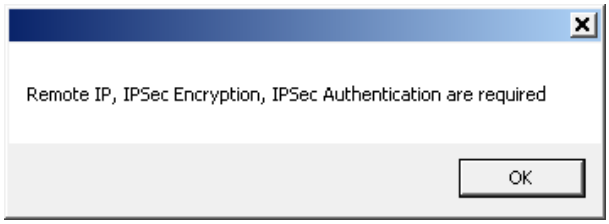


Figura 3-20 Pantalla de error de configuración IPsec

7. Si procede, introduzca todos los ajustes requeridos y seleccione **Save All**.
8. Cierre la pantalla de "Ajustes Generales" y regrese a la pantalla de "Configuración de Punto Final".
9. Añada o edite cualquier Puntos Finales adicionales y seleccione **Save**. IPScom mostrará la pantalla "Guardar como".
10. Introduzca el nombre del archivo de Configuración de IPsec deseado y seleccione **Save**. IPScom mostrará una pantalla de confirmación.
11. Seleccione **OK**. IPScom regresará a la pantalla de "Configuración de Punto Final".

■**NOTA:** Los archivos de configuración de IPsec se pueden ser enviados al control desde la pantalla de Configuración de Punto final.

Enviar el archivo de configuración de IPsec para el unidad

1. Inicie IPScom, establézcala comunicación con el unidad a conectar.
2. Seleccione **Communication/Setup/Communication Security/IPsec Configuration/Send Configuration File** desde la barra de herramientas IPScom. IPScom mostrará una pantalla de diálogo Abrir "Archivo de Configuración de IPSec".
3. Seleccione el nombre de archivo que contiene la configuración IPsec para ser enviado al unidad.
4. Seleccione **Open**. IPScom enviará el archivo seleccionado de configuración al unidad de destino.
5. IPScom mostrará una pantalla de confirmación. Seleccione **OK**, IPScom volverá a la pantalla principal.

Recuperación de un archivo de configuración IPsec desde el unidad

1. Inicie IPScom, establézcala comunicación con el unidad a conectar.
2. Seleccione **Communication/Setup/Communication Security/IPsec Configuration/Retrieve Configuration File** de la barra de herramientas IPScom. IPScom mostrará una pantalla de Guardar Como "archivo de IPsec".
3. Elija la ubicación de **Guardar como** y escriba el nombre del archivo deseado que contendrá la Configuración de IPSec recuperado del unidad.
4. Seleccione **Save**. IPScom guardará el archivo (.ifg) en la ubicación seleccionada y mostrará una pantalla de confirmación.

Habilitación de la Seguridad IPsec desde la IHM

La seguridad de IPsec también se puede habilitar desde el panel frontal IHM. La configuración para habilitar la seguridad IPsec se encuentra en el menú COMMUNICATIONS/Port Settings/Comm Ports Security/ Protocol Access.

Información Legal

Patente

Las unidades descritas en este manual estan cubiertos por patentes de los Estados Unidos, con otras patentes pendientes.

El Comprador se mantendrá inofensivo y sin indemnizar al Vendedor, sus directores, oficiales, agentes, y empleados de cualquiera y todos los costos y gastos, daño o perdida, como resultado de alguna infracción pretendida de las cartas de patente de los Estados Unidos o derechos acumulados de las marcas registradas, si es fedederal, de estado, o Ley comun, surgiendo de la conformidad de los diseños de el Vendedor con el Comprador, especificaciones, o instrucciones.

Garantía

El Vendedor por la presente garantiza que los bienes, los cuales son el tema de este contrato seran fabricados en una manera de buena calidad y todos los materiales usados en el mismo seran nuevos y razonablemente apropiados para el equipo. El Vendedor garantiza que si, durante un periodo de diez años desde la fecha de embarque de el equipo, el equipo debilitado sera detectado por el Comprador en caso de falla o que fallara para trabajar no conforme con las especificaciones de el Vendedor de el producto, el Vendedor correjira los mismos con sus gastos, proporcionado, sin embargo los Compradores embarcaran el equipo prepagado hacia las instalaciones de el Comprador. Luego la Responsabilidad de el Comprador estara limitado al valor de reemplazo de el equipo presentado bajo este contrato.

El Vendedor no da otras garantías expresadas o implicadas que no sean las que se indicarón arriba. El Vendedor especificamente excluye las garantias implicadas de mercantibilidad para un proposito particular. No hay garantías que se extiendan a la descripción aqui contenida. En ningun evento el Vendedor sera responsible por daños consecuenciales, ejemplares, o punitivos de cualquier naturaleza.

Cualquier equipo retornado para reparar deben ser enviados con cargos de transportación prepagados. El equipo debe permanecer como propiedad de el Comprador. Las garantías referidas son evitadas si el valor de la unidad es facturada hacia el Vendedor en el momento de el retorno.

Indemnificación

El Vendedor no sera responsable por cualquier propiedad de daño o lo que sea o por cualquier perdida o daño que surja de esto o resultando de este contrato o de lapresentación o violación del incumplimiento del contrato, o de todos los servicios que seran cubiertos de acuerdo con este contrato.

De ninguna manera el Vendedor sera responsable por las cosas que pasen especialmente accidentales, o los daños consecuentes o referentes pero no limitados, a la pérdida de ganancia o entradas o ingresos, o la pérdida del uso del equipo, costo del capital, costo de poder comprar, costo del reponer el equipo o sistema, y las facilidades o servicios de tiempos de inactividad o reclamos o daños que hagan los clientes o los empleados de el Comprador por tales daños. A pesar de lo que diga el contrato referente al reclamo o daños basados en el contrato, garantía, hasta incluyendo neglijencia o lo contrario.

Sobre ninguna circunstancia el Vendedor sera responsible por cualquier persona que resulte herida o de alguna otra manera.

El acuerdo ha sido que cuando el equipo sea entregado desde ahora en adelante séra usado o utilizado para trabajar en cualquier instalación nuclear, o lugar de actividad. El Vendedor no tendra ninguna liabilidad por cualquier daño de cualquier propiedad, o cualquier daño nuclear, o persona herida, o el daño de cualquier propiedad, or cualquier contaminación nuclear o cualquier propiedad o lugar que este cerca o alrededor de esta facilidad o lugar nuclear. El Comprador esta de acuerdo de no mantener responsable al Vendedor de ninguna parte de problemas o de cualquier cosa referente al contrato. La instalación nuclear significa cualquier reactor nuclear e incluye cualquier lugar o lugares o facilidades donde esta el lugar localizado, y todas las operaciones conducidas sobre ese lugar, y los alrededores, que seran usados para dicha operación.

Nota:

Cualquier ilustración y descripción de parte de Beckwith Electric sera solamentepara el proposito de indentificación solamente.

Los diagramas y las specificaciones de ahora en adelante seran la propiedad de Beckwith Electric y estos materiales, seran usados en estricta confidencia; por lo tanto, no serán usados como base de reproducción de los equipos mencionados sin una autorización escrita de parte Beckwith Electric.

Ninguna ilustración o descripción contenida de ahora en adelante será construida como una garantía de afirmación, promesa, descripción, o ejemplo, y cualquiera de esas garantías expresadas serán excluidas específicamente y esas ilustraciones o descripciones implicarán que la garantía del producto es comerciable o se puede vender o poner o se puede usar para cualquier propósito. No habrá garantía que se extienda mas allá de las garantías de Beckwith Electric en termino de venta.

BECKWITH ELECTRIC
6190 118th Avenue North • Largo, Florida 33773-3724 U.S.A.
TELEFONA (727) 544-2326
beckwithelectricsupport @ hubbell.com
www.beckwithelectric.com
ISO 9001:2015

M-7679-COMS-AG-01 04/19
ESP-0 04/24