Liebert®

Tarjeta IntelliSlot™ Unity™

Guía del instalador/usuario

La información contenida en este documento está sujeta a cambios sin previo aviso y puede no ser adecuada para todas las aplicaciones. Si bien se han tomado todas las precauciones para garantizar la precisión y la integridad de este documento, Vertiv no asume ninguna responsabilidad y renuncia a toda responsabilidad por los daños que resulten del uso de esta información o por cualquier error u omisión. Consulte otras prácticas locales o códigos de construcción, según corresponda, para conocer los métodos, las herramientas y los materiales correctos que se utilizarán para realizar los procedimientos que no se describen específicamente en este documento.

Sitio de soporte técnico

Si encuentra algún problema de instalación o de funcionamiento con su producto, consulte la sección pertinente de este manual para ver si el problema se puede resolver siguiendo los procedimientos descritos.
Visite https://www.VertivCo.com/en-us/support/ para asistencia adicional.

TABLA DE CONTENIDO

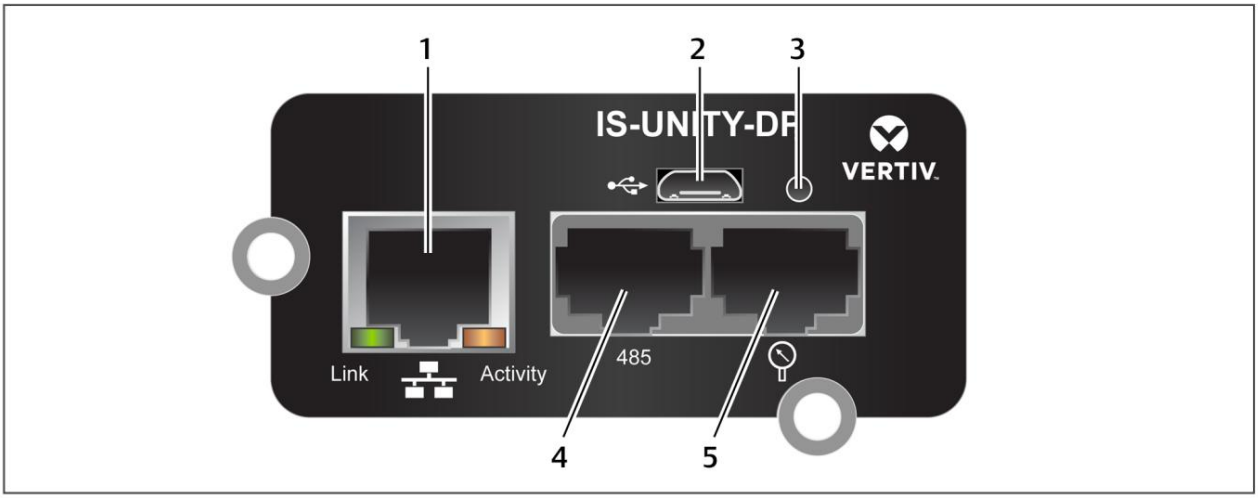
1. INTRODUCCIÓN

Esta plataforma Liebert Unity ofrece comunicación y control mejorados de los productos de alimentación de CA, distribución de energía y gestión térmica. La plataforma se comunica con las herramientas y servicios de software de Vertiv™, incluidos Trellis™, Trellis Power Insight, LIFE™ Services, Liebert SiteScan Web™ y Liebert Nform™.

La plataforma incluye las tarjetas IS-Unity-DP™, IS-Unity-SNMP™ e IS-Unity-LIFE™.

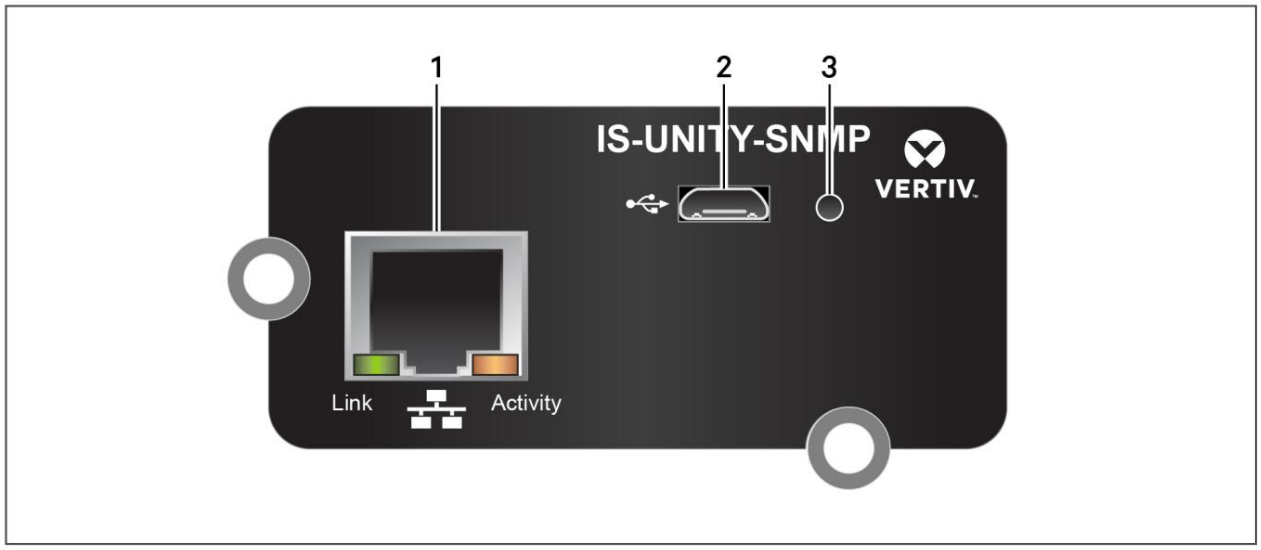
Cada tarjeta emplea el protocolo Velocity para monitorear y administrar una amplia gama de parámetros operativos, alarmas y notificaciones. La tarjeta se comunica con los sistemas de gestión de edificios y los sistemas de gestión de redes a través de los protocolos BACnet, Modbus, SNMP, LIFE/Remote Services y YDN23.

Figura 1.1 Características de la tarjeta IS-Unity-DP



ARTÍCULO	DESCRIPCIÓN
1	Puerto Ethernet RJ-45
2	Puerto micro USB
3	Botón Restablecer, consulte Restablecimiento manual de los valores predeterminados de fábrica en la página 67.
4	Puerto RS-485 (BACnet/MSTP, Modbus RTU o YDN23. Solo se puede usar uno).
5	Puerto de red de sensores Liebert (solo sensores SN)

Figura 1.2 Características de la tarjeta IS-Unity-SNMP



ARTÍCULO	DESCRIPCIÓN
1	Puerto Ethernet RJ-45
2	Puerto micro USB
3	Botón Restablecer, consulte Restablecimiento manual de los valores predeterminados de fábrica en la página 67.

1.1 Compatibilidad con sensores Liebert SN

La tarjeta Unity monitorea hasta 10 sensores integrados y modulares Liebert SN. Los tipos de sensores disponibles incluyen temperatura, humedad, cierre de puertas, cierre de contactos y detección de fugas. Los menús de la pestaña Sensor permiten configurar los sensores y colocarlos en el orden configurado por el usuario para verificar más fácilmente las condiciones de alta prioridad. Los datos del sensor están disponibles a través de SNMP y la interfaz de usuario web. Consulte Menú de la pestaña Sensor en la página 26.

2 INSTALACIÓN

⚠ ¡ADVERTENCIA! Peligro de arco eléctrico y descarga eléctrica. Abra todos los interruptores de desconexión del suministro de energía eléctrica locales y remotos, verifique con un voltímetro que la energía esté apagada y use equipo de protección personal según NFPA 70E antes de trabajar dentro del gabinete de control eléctrico. El incumplimiento puede causar lesiones graves o la muerte.

⚠ ¡ADVERTENCIA! Riesgo de shock eléctrico. Puede causar daños al equipo, lesiones o la muerte.

Abra todos los interruptores de desconexión del suministro de energía eléctrica locales y remotos y verifique con un voltímetro que la energía esté apagada antes de trabajar dentro de cualquier recinto de conexión eléctrica.

El trabajo de servicio y mantenimiento debe ser realizado únicamente por personal debidamente capacitado y calificado y de acuerdo con las regulaciones aplicables y las especificaciones del fabricante.

Abrir o quitar las cubiertas de cualquier equipo puede exponer al personal a voltajes letales dentro de la unidad incluso cuando aparentemente no está funcionando y el cableado de entrada está desconectado de la fuente eléctrica.

AVISO

Riesgo de instalación incorrecta. Puede causar daño al equipo.
Solo un profesional de servicio calificado debe instalar estos productos. Recomendamos que un técnico de Vertiv™ realice la instalación en un sistema UPS grande. Póngase en contacto con Vertiv™ en https://www.vertivco.com/en-us/support/.

AVISO

Riesgo de ID de nodo duplicados si se instalan dos o más tarjetas Liebert IntelliSlot. Puede causar conflictos de red.

Se producirá un conflicto de red interna dentro de un dispositivo cuando se instalen varias tarjetas de comunicación con ID de nodo duplicadas en el dispositivo.

Cada tarjeta IntelliSlot debe tener una ID de nodo única. Esto no será un problema si solo hay una tarjeta instalada en su sistema. Los ID de nodos duplicados se evitan fácilmente con el procedimiento detallado en Instalación de varias tarjetas en un sistema en la página 7.

2.1 Instalación de la tarjeta

La tarjeta Unity se puede instalar en la fábrica o en campo.

Para realizar una instalación de campo:

1. Busque la bahía IntelliSlot en su equipo Liebert. Es posible que tenga una cubierta de plástico.
2. Inserte la tarjeta en la bahía.

NOTA: La tarjeta solo encajará de una manera en el compartimiento porque la placa de circuito no está centrada en la placa frontal. La ranura en la bahía tampoco está centrada.

3. Fije la tarjeta con los tornillos utilizados para la placa de cubierta.

4. Conecte un cable Ethernet al puerto Ethernet RJ-45 de la tarjeta para las interfaces de comunicación IP.
5. Conecte un cable serie al puerto 485 RJ-45 de la tarjeta para las interfaces de comunicación RS-485, consulte Conexión de un cable serie RS-485 en la página 6.

2.1.1 Conexión directa a la computadora para la configuración

Antes de que pueda realizar cambios en la configuración, como configurar los ajustes de IP estática, debe acceder al servidor web de la tarjeta a través de Ethernet.

Para conectarse a la tarjeta:

1. Conecte una computadora que ejecute un sistema operativo Microsoft Windows (Microsoft Windows® XP o posterior) a la tarjeta conectando un extremo de un cable de red en el puerto Ethernet de la computadora y el otro extremo en el puerto Ethernet de la tarjeta Unity. consulte la Figura 1.1 en la página 1.
   El direccionamiento IP privado automatizado (APIPA) normalmente está habilitado de manera predeterminada en las computadoras que ejecutan el sistema operativo Microsoft Windows y asignará una dirección IPv4 de configuración automática cuando no se detecte un servidor DHCP.

NOTA: Este proceso de configuración automática de IP puede demorar de 1 a 3 minutos.

Si es necesario, use el símbolo del sistema de Windows para verificar la configuración de la dirección IP de la computadora:

• Presione la tecla Windows+R, ingrese cmd y haga clic en Aceptar. • Escriba

ipconfig /all y presione Enter, luego verifique lo siguiente, vea la FIGURA:

Configuración automática habilitada = Sí

Dirección IPv4 de configuración automática = 169.254.xx

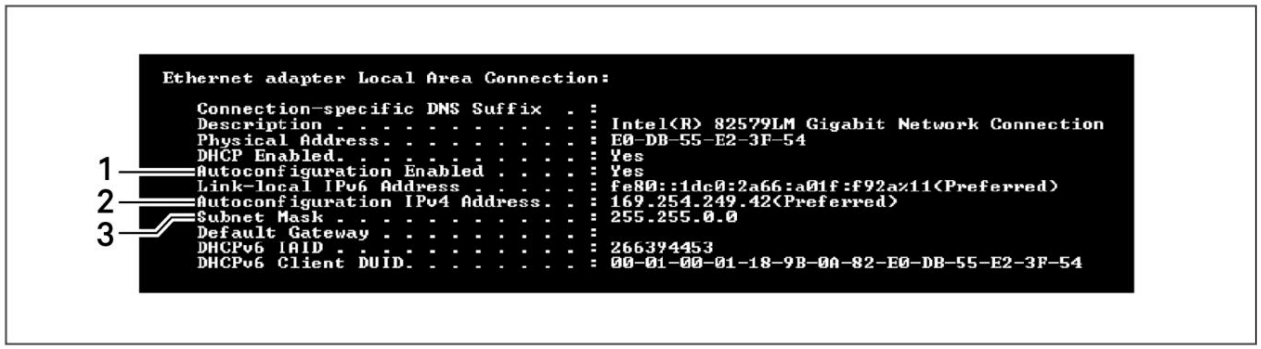
Máscara de subred = 255.255.0.0

NOTA: Ingrese ipconfig /renew para para adquirir una dirección IPv4 de configuración automática si no aparece una.

2. En la computadora, abra una sesión de navegador web e ingrese 169.254.24.7 para conectarse a la tarjeta. Servidor web.

   Se abre la interfaz de usuario de Unity.

Figura 2.1 Líneas de configuración automática en el símbolo del sistema



ARTÍCULO	DESCRIPCIÓN
1	Configuración automática habilitada
2	Dirección IPv4 de configuración automática
3	Máscara de subred

2.1.2 Determinación de la dirección IP DHCP

La tarjeta Unity está configurada de fábrica para DHCP. Si se requiere una configuración de red estática o BootP, cambie el modo de inicio como se describe en Asignación de una dirección IP estática a continuación. Para DHCP, conecte un cable Ethernet activo a la tarjeta y recibirá una dirección IP del servidor DHCP. Comuníquese con el administrador de DHCP para obtener la dirección IP mediante la dirección MAC de la tarjeta Unity. La dirección MAC está impresa en la placa frontal de la tarjeta.

Si el administrador DHCP no está disponible o si no hay una forma conveniente de determinar la dirección IP asignada por el servidor DHCP, use una computadora con una conexión Ethernet directa a la tarjeta y la convención de dirección IPv4 de configuración automática descrita en Conexión directa a la computadora de Configuración en la página anterior, para acceder a la página Web de la tarjeta.

Para ver la última dirección IP asignada por DHCP de la tarjeta:

1. Haga clic en la pestaña Comunicaciones , luego en el menú del lado izquierdo, seleccione Soporte > Redes activas.
2. Verifique el campo Última dirección DHCP/BOOTP, que muestra la última dirección IP asignada por el servidor DHCP. La tarjeta puede retener esa dirección IP cuando se vuelve a conectar a la red DHCP porque la mayoría de los sistemas DHCP reutilizan la misma dirección IP para el mismo dispositivo.

2.1.3 Asignación de una dirección IP estática

Para asignar una dirección IP estática, utilice la conexión Ethernet directa para configurar la tarjeta. Continúe con Conexión directa a la computadora para la configuración en la página anterior y Cambie los nombres de usuario y las contraseñas inmediatamente en la página 7.

2.1.4 Conexión de un cable serie RS-485

Las tarjetas Unity vienen con un bloque de terminales adaptador RJ-45-2POS. El adaptador tiene dos terminales de tornillo para unir los extremos de un cable RS-485 para comunicarse con un sistema de administración de edificios.

1. Busque el cable serie del sistema de gestión del edificio. Si ya tiene un conector RJ-45 en el extremo, determine si usa el mismo pin-out que el conector de la tarjeta Unity.

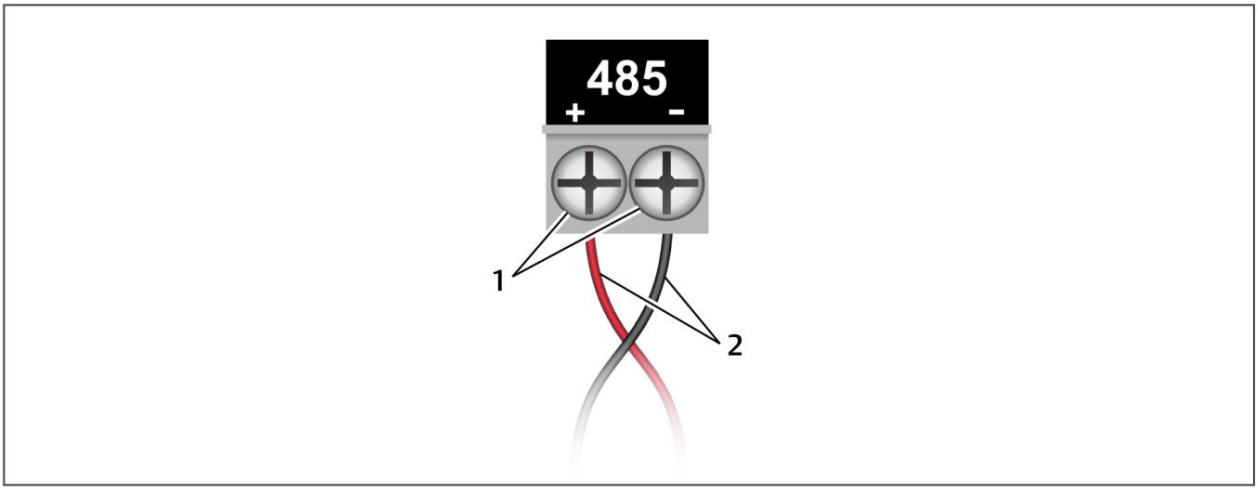
   - Si la disposición de pines es la misma que la del conector de la tarjeta, salte al Paso 6.

2. Pele los extremos de los conductores positivo (normalmente rojo) y negativo (normalmente negro) del cable RS-485 de modo que quede expuesto suficiente cable desnudo para la conexión, aproximadamente 1/4 pulg. (6 mm).

NOTA: No se debe exponer ningún cable pelado cuando se complete la conexión.

3. Coloque el adaptador de modo que el lado con las marcas positiva y negativa quede hacia arriba. El pequeño las marcas están en el mismo lado que las cabezas de los tornillos, como se muestra.

Figura 2.2 Marcas del bloque de terminales del adaptador hacia arriba



ARTÍCULO	DESCRIPCIÓN
1	Tornillos
2	alambres

4. Afloje el tornillo del terminal positivo e inserte el cable rojo lo suficiente en el bloque de terminales para insertar los cables pelados debajo del tornillo, luego apriete el tornillo con cuidado de no romper los cables.

5. Repita el paso 3 con el terminal negativo y el cable negro.
6. Enchufe el cable en el puerto 485 RJ-45 de la tarjeta Unity. Consulte las características de la tarjeta IS-Unity-DP en página 1, para la ubicación del puerto.

2.2 Cambiar nombres de usuario y contraseñas inmediatamente

NOTA: Recomendamos cambiar los nombres de usuario y las contraseñas de los Usuarios locales predeterminados de fábrica con administrador y acceso general de inmediato para salvaguardar la configuración protegida y las áreas de control de la tarjeta Unity.

El usuario administrador predeterminado de fábrica es "Usuarios locales [1]" con el nombre de usuario Liebert y la contraseña predeterminada Liebert (ambos distinguen entre mayúsculas y minúsculas).

El usuario general predeterminado de fábrica es "Usuarios locales [2]" con la contraseña predeterminada Liebert (se distingue entre mayúsculas y minúsculas).

Para cambiar los nombres de usuario y las contraseñas, consulte los pasos en Carpeta de usuarios locales en la página 31.

2.3 Configurar la Tarjeta

La tarjeta Unity requiere una configuración menor para habilitar la conectividad de red básica. El valor predeterminado para la comunicación IP/Web es IPv4, pero se puede cambiar a IPv6 para mayor seguridad. Póngase en contacto con su administrador de red para determinar si es compatible con su red.

1. En el menú de la pestaña Comunicaciones, seleccione Configuración > Red.
2. Habilite el protocolo, IPv4 o IPv6, que se utilizará para comunicarse con la tarjeta Unity y con el equipo Liebert: a. Haga clic en IPv4 o IPv6.

   b. Haga clic en Editar.

   C. Cuando se le solicite, ingrese el nombre de usuario administrativo y la contraseña.
   El nombre y la contraseña predeterminados son "Liebert" (distingue entre mayúsculas y minúsculas).

   d. Haga clic para marcar habilitado.

   mi. Ingrese la dirección IP asignada junto con el resto de la información de red requerida.
   Póngase en contacto con el administrador del sistema si es necesario.
3. Haga clic en Guardar para confirmar los cambios o en Cancelar para descartarlos.
   Los cambios surten efecto después de reiniciar la tarjeta.

2.4 Instalación de varias tarjetas en un sistema

Se puede instalar más de una tarjeta Liebert IntelliSlot en un sistema, pero se deben evitar las rutas circulares y los ID de nodo duplicados durante la instalación. Las siguientes instrucciones se aplican cuando la segunda tarjeta que se instalará es una tarjeta IntelliSlot Unity. Si la segunda tarjeta no es una tarjeta Liebert IntelliSlot Unity, siga las instrucciones del manual del usuario de esa tarjeta.

Antes de comenzar la instalación de una segunda tarjeta Unity, verifique que la primera tarjeta funcione correctamente.

Si la primera tarjeta es una tarjeta IntelliSlot, pero no una tarjeta Unity, y si ambas tarjetas se conectan a la misma red Ethernet, debe desactivar la función de enrutador en la primera tarjeta. Esto evitará rutas circulares. Siga las instrucciones del manual de usuario de la primera tarjeta.

Si la primera y la segunda tarjetas son tarjetas IntelliSlot Unity, se deben tomar medidas para evitar la duplicación de ID de nodo MSTP de Velocity Protocol. De forma predeterminada, las dos tarjetas utilizarían el mismo ID de nodo y una o ambas tarjetas informarían un error de nodo duplicado y no se comunicarían con el sistema.

El ID de nodo predeterminado para una tarjeta Unity es 0, por lo que la segunda tarjeta debe usar 1. Una tercera tarjeta debe usar 2. Una cuarta tarjeta debe usar 100 a 127. Comuníquese con el administrador del sistema acerca del ID de nodo adecuado para la segunda tarjeta, luego realice los siguientes pasos.

1. Abra un navegador web y navegue hasta la segunda tarjeta de Unity.
2. En la pestaña Comunicaciones, haga clic en Configuración > Protocolo de velocidad > MSTP.
3. Haga clic en Editar e ingrese una contraseña y un nombre de usuario si es necesario.
4. Ingrese la nueva ID de nodo.
5. Haga clic en Guardar para confirmar los cambios o en Cancelar para descartarlos.
6. Reinicie la tarjeta:
    a. En la pestaña Comunicaciones, haga clic en Soporte.
    b. Haga clic en Habilitar.
    C. Haga clic en Reiniciar.

2.5 Mejores prácticas de seguridad

La configuración predeterminada en la tarjeta Unity admite una instalación y puesta en marcha rápidas para que los servicios de comunicación básicos estén listos y funcionando rápidamente. La seguridad adecuada de los equipos de infraestructura crítica requiere una configuración adecuada de TODOS los servicios de comunicación. Esta sección resume las configuraciones a examinar para reducir el riesgo de acceso no autorizado a equipos de infraestructura crítica a través de una tarjeta Unity.

La Tabla 2.1 en la página siguiente proporciona una lista de elementos para revisar. Cada uno debe revisarse, configurarse según las necesidades operativas para administrar el equipo y verificar que la configuración admita la funcionalidad operativa deseada sin agregar acceso innecesario o no autorizado al equipo de infraestructura crítica. Se proporciona una referencia a la sección adecuada de este documento para configurar cada elemento.

Tabla 2.1 Configuración para revisar y verificar para reducir el riesgo de acceso no autorizado

ARTÍCULO	DESCRIPCIÓN	REFERENCIA
Cuentas y contraseñas	Cambie los nombres y las contraseñas de las cuentas de administrador y de usuario inmediatamente para eliminar el acceso de credenciales predeterminado.	Cambiar nombres de usuario y contraseñas Inmediatamente en la página anterior
Acceso a la red IP	Habilitar/deshabilitar el acceso de red IPV4 e IPV6 a la UnityCard - deshabilitar la red no utilizada acceso.	Configure la Tarjeta en la página anterior
Acceso Telnet y SSHv2	Habilite/desactive el acceso a telnet y SSHv2 para soporte de diagnóstico y configuración; desactívelo cuando no esté en uso.	Carpeta de red en la página 37
Protocolo de servicio web	Seleccione HTTPS para usar el cifrado SSL al acceder a los datos a través de la interfaz de usuario web.	Carpeta del servidor web en la página 39
Certificados SSL	Cuando use HTTPS, instale su propio SSL Certificados de una autoridad de certificación de confianza o generar certificados autofirmados alternativos	Carpeta de certificados en la página 41
Acceso web protegido con contraseña	Habilite esta opción para solicitar a los usuarios que inicien sesión antes de que se muestre la información del dispositivo al usuario.	Carpeta del servidor web en la página 39

Tabla 2.1 Configuración para revisar y verificar para reducir el riesgo de acceso no autorizado (continuación)

ARTÍCULO	DESCRIPCIÓN	REFERENCIA
Acceso web de escritura remota	Deshabilite para solicitar que todas las actualizaciones del dispositivo y la tarjeta se realicen a través de una interfaz local, a través de una conexión de configuración automática con una PC directamente conectada a la tarjeta Unity o a través de la pantalla de la interfaz de usuario local del dispositivo (si está disponible). ⚠ ¡ADVERTENCIA! Deshabilite esto solo si está absolutamente seguro de que no necesita administrar el dispositivo administrado o la tarjeta Unity a través de una sesión de navegador web remota.	Carpeta del servidor web en la página 39
Protocolos de comunicación	Habilite/desactive los protocolos BACnet, Modbus, SNMP y YDN23; deshabilite cualquiera que no esté en uso.	Activar protocolos de comunicación en la página 11
Configuración de BACnet	Establezca el acceso de escritura del dispositivo administrado en solo lectura para evitar cambios en el dispositivo a través de la interfaz BACnet.	Habilitar el protocolo BACnet en la página 13
Configuración de Modbus	Establezca el acceso de escritura del dispositivo administrado en solo lectura para evitar cambios en el dispositivo a través de la interfaz Modbus; Seleccione la opción adecuada para Limitar el tipo de acceso a la red para restringir qué sistemas pueden solicitar datos Modbus del dispositivo: el acceso puede estar abierto a cualquier sistema, limitado a aquellos en la misma subred que el dispositivo o limitado solo a aquellos de sistemas en una IP confiable Lista de direcciones.	Habilitar el protocolo Modbus en la página 11
Configuración de la versión de SNMP	Habilite/desactive las versiones de SNMP deseadas; Considere usar SNMPv3 con autenticación y encriptación de usuarios.	Configure los ajustes de SNMP en la página 15
Configuración de la tabla de acceso SNMP	Para cada entrada de la tabla Acceso SNMPv1/v2c, establezca el Tipo de acceso SNMP en Solo lectura para evitar cambios en el dispositivo desde los hosts identificados en la entrada de la tabla.	Configure los ajustes de acceso a SNMPv1/v2c en la página 17
Cadenas de comunidad SNMP	Cambie los valores predeterminados de SNMP v1/v2c Trap y Access Community Strings.	Configure los ajustes de captura de SNMPv1 en la página 16 y Configure los ajustes de acceso a SNMPv1/v2c en la página 17
Configuración de SNMPv3	Utilice la configuración de autenticación y privacidad de SNMPv3 para realizar comunicaciones SNMPv3. más seguro.	Configure los ajustes de usuario de SNMPv3 en la página 16
Configuración de YDN23	Establezca el acceso de escritura del dispositivo administrado en solo lectura para evitar cambios en el dispositivo a través de la interfaz YDN23.	Carpeta YDN23 en la página 59
Configuración de protocolo de velocidad	Active/desactive VelocityProtocol que utilizan las aplicaciones de gestión Vertiv™ para acceder a los datos del dispositivo.	Carpeta VelocityProtocol en la página 47

Para mayor seguridad, el firewall y la puerta de enlace de la red local pueden restringirse para permitir solo el tráfico necesario en los puertos de red requeridos. Los puertos utilizados por la tarjeta Unity se enumeran en la siguiente tabla. El administrador puede cambiar algunas configuraciones de puerto.

Tabla 2.2 Puertos utilizados por la tarjeta Unity

RED SERVICIO		PUERTO UTILIZADO	¿POR DEFECTO?	¿SE PUEDE MODIFICAR?
Web	HTTP	TCP 80	Sí	Sí
	HTTPS	TCP 443	Sí	Sí
DNS		TCP y UDP 53	Sí	No
NTP		TCP y UDP 123	Sí	No
SMTP		TCP 25	Sí	Sí
SSHv2		TCP y UDP 22	Sí	No
Telnet		TCP 23	Sí	No
SNMP		UDP 161, 162	Sí	Solo se puede cambiar el puerto de captura 162
ModbusTCP		TCP 502	Sí	Sí
IP de BACnet		UDP 47808	Sí	Sí
Protocolo de velocidad		UDP 47808	Sí	No
VIDA		TCP 80	Sí	Sí

Los detalles para la configuración de todas las opciones se proporcionan en el resto de esta guía.

3 HABILITAR PROTOCOLOS DE COMUNICACIÓN

La tarjeta Unity se comunica con equipos y sistemas de terceros a través de los siguientes protocolos:

- IP BACnet
- MSTP BACnet
- ModbusTCP
- Modbus RTU
- SNMP
- YDN23

NOTA: No se pueden habilitar más de dos protocolos en una tarjeta. Solo se puede seleccionar una versión de BACnet: BACnet IP o BACnet MSTP. Solo se puede seleccionar una versión de Modbus: Modbus TCP o Modbus RTU. Solo uno de los protocolos elegidos puede usar el puerto 485. Elegir dos protocolos 485 causará conflictos.

NOTA: Algunos sistemas de administración de edificios (BMS) se pueden configurar para enviar actualizaciones continuas para los puntos de ajuste del dispositivo, generalmente configurando el mismo valor. El BMS debe configurarse para enviar, en un promedio sostenido, no más de dos escrituras por segundo al dispositivo. Esto permitirá que el dispositivo se ponga al día después de una ráfaga de actualizaciones cuando sea necesario, mientras permite que continúe la comunicación con el dispositivo.

3.1 Habilitar protocolos

Los protocolos se pueden habilitar después de instalar y configurar una tarjeta para conectividad de red básica. Después de habilitar un protocolo, debe configurarse, lo que requiere abrir la carpeta del protocolo deseado (pestaña Comunicaciones > Protocolos > (protocolo a configurar).

Para habilitar dos protocolos de comunicación:

1. En la pestaña Comunicaciones, seleccione Protocolos.
2. Haga clic en Editar e ingrese el nombre de usuario y la contraseña del administrador.
3. Haga clic para marcar la casilla junto a los protocolos a usar.
   - Solo se pueden habilitar dos protocolos. • Solo uno de los dos puede usar el puerto 485.
4. Haga clic en Guardar para confirmar los cambios o en Cancelar para descartarlos.
5. Configurar los protocolos seleccionados. Consulte Edición de la configuración de la tarjeta Unity en la página 29.
6. Reinicie la tarjeta:
   a. En la pestaña Comunicaciones, haga clic en Soporte.
   b. Haga clic en Habilitar.
   C. Haga clic en Reiniciar.

3.1.1 Habilitar protocolo Modbus

Los protocolos se pueden habilitar después de que se haya instalado y configurado una tarjeta.

1. En la pestaña Comunicaciones, seleccione Protocolos > Modbus.
2. Haga clic en Editar e ingrese un nombre de usuario y una contraseña.

3. Seleccione el nivel de acceso (Solo lectura o Lectura/Escritura).
4. Seleccione la interfaz Modbus (Modbus TCP o Modbus RTU).
5. Haga clic en Guardar para confirmar los cambios o en Cancelar para descartarlos.
6. Configure la interfaz Modbus elegida.
   Consulte Configurar Modbus TCP a continuación o Configurar Modbus RTU a continuación.
   Para obtener descripciones de la configuración, consulte Carpeta Modbus en la página 54.

Configurar Modbus TCP

1. En la pestaña Comunicaciones, seleccione Protocolos > Modbus > Modbus TCP.
2. Haga clic en Editar e ingrese un nombre de usuario y contraseña si es necesario.
3. Establezca el tipo de acceso a la red de límite eligiendo de la lista desplegable:
   - Abierto •
   Misma subred
   - Lista de IP de confianza

   Consulte Carpeta Modbus TCP en la página 55 para obtener detalles adicionales.
4. Introduzca el puerto que utilizará el servidor Modbus para escuchar y responder a las solicitudes del protocolo Modbus en función del tipo de acceso de red limitado seleccionado.
5. Ingrese el Recuento máximo de conexiones de clientes.
6. Haga clic en Guardar para confirmar los cambios o en Cancelar para descartarlos.
7. Reinicie la tarjeta:
   a. En la pestaña Comunicaciones, haga clic en Soporte.
   b. Haga clic en Habilitar.
   C. Haga clic en Reiniciar.

Configurar Modbus RTU

1. En la pestaña Comunicaciones, seleccione Protocolos > Modbus > Modbus RTU.
2. Haga clic en Editar e ingrese un nombre de usuario y contraseña si es necesario.
3. Ingrese el ID de nodo y la tasa de baudios.
   - El ID de nodo predeterminado es 1, pero debe tener un valor de 1 a 247 que sea único entre dispositivos conectados a través de la interfaz RS-485.
   - La velocidad de transmisión predeterminada es 9600. 19200 y 38400 también están disponibles.

   Para obtener una descripción adicional de la configuración, consulte Carpeta Modbus RTU en la página 55.

NOTA: Póngase en contacto con el administrador del sistema si no está seguro acerca de la configuración.

4. Haga clic en Guardar para confirmar los cambios o en Cancelar para descartarlos.
5. Reinicie la tarjeta:
   a. En la pestaña Comunicaciones, haga clic en Soporte.
   b. Haga clic en Habilitar.
   C. Haga clic en Reiniciar.

3.1.2 Habilitar el protocolo BACnet

NOTA: Comuníquese con el administrador del sistema o el administrador del sistema de administración del edificio si no está seguro acerca de la configuración.

1. En la pestaña Comunicaciones, seleccione Protocolos > BACnet.
2. Haga clic en Editar e ingrese un nombre de usuario y contraseña si es necesario.
3. Seleccione el nivel de acceso de escritura del dispositivo administrado: solo lectura o lectura/escritura.

   Esto determina la capacidad de un usuario para cambiar la configuración en la tarjeta Unity.
4. Elija la interfaz BACnet: BACnet IP o BACnet MSTP.
5. Establezca el número de instancia del objeto de dispositivo.
6. Establezca el Nombre del objeto del dispositivo.
7. Establezca el tiempo de espera de APDU.
8. Establezca los reintentos de APDU.
9. Haga clic en Guardar para confirmar los cambios o en Cancelar para descartarlos.
10. Configure la interfaz BACnet elegida, consulte Configurar el protocolo IP BACnet a continuación o Configurar Protocolo BACnet MSTP a continuación.

    Para obtener una descripción de la configuración, consulte Carpeta BACnet en la página 53.

Configurar el protocolo IP BACnet

NOTA: Comuníquese con el administrador del sistema o el administrador del sistema de administración del edificio si no está seguro acerca de la configuración.

1. En la pestaña Comunicaciones, seleccione Protocolos > BACnet > IP de BACnet.
2. Haga clic en Editar e ingrese un nombre de usuario y contraseña si es necesario.
3. Ingrese el BACnetIP/Número de puerto.

   Si la tarjeta Unity está en una subred diferente (una posibilidad cuando las unidades monitoreadas son parte de una red Liebert SiteScan u otro servicio de monitoreo de terceros): a. Elija si habilitar o no Registrar como dispositivo externo. b.

   Ingrese la dirección IP del BBMD (dispositivo de administración de transmisión BACnet). C. Ingrese un tiempo, en segundos, para el tiempo de vida del dispositivo externo.

   Para obtener descripciones de la configuración, consulte Carpeta IP de BACnet en la página 54.
4. Haga clic en Guardar para confirmar los cambios o en Cancelar para descartarlos.
5. Reinicie la tarjeta:

   a. En la pestaña Comunicaciones, haga clic en Soporte.

   b. Haga clic en Habilitar.

   C. Haga clic en Reiniciar.

Configurar el protocolo BACnet MSTP

NOTA: Comuníquese con el administrador del sistema o el administrador del sistema de administración del edificio si no está seguro acerca de la configuración.

1. En la pestaña Comunicaciones, seleccione Protocolos > BACnet > BACnet MSTP.

2. Haga clic en Editar e ingrese un nombre de usuario y contraseña si es necesario.
3. Establezca la ID del nodo BACnet MSTP.
   - El ID de nodo predeterminado es 1, pero debe tener un valor de 0 a 127 que sea único entre dispositivos conectados a través de la interfaz RS-485.
4. Establezca la velocidad de datos BACnet MSTP.
5. Establezca la dirección maestra BACnet MSTP Max.
6. Configure los marcos de información BACnet MSTP Max.

   Para obtener descripciones de la configuración, consulte Carpeta BACnet MSTP en la página 54.
7. Haga clic en Guardar para confirmar los cambios o en Cancelar para descartarlos.
8. Reinicie la tarjeta:
   a. En la pestaña Comunicaciones, haga clic en Soporte.
   b. Haga clic en Habilitar.
   C. Haga clic en Reiniciar.

3.1.3 Habilitar SNMP

SNMPv1/v2c y SNMPv3 están habilitados de forma predeterminada. Los protocolos se pueden configurar o se pueden aceptar sus valores por defecto. Las trampas de autenticación no están habilitadas de forma predeterminada. El intervalo predeterminado de Heartbeat Trap es de 24 horas. Esto se puede deshabilitar o se puede cambiar el intervalo.

1. En la pestaña Comunicaciones, seleccione Protocolos > SNMP.
2. Haga clic en Editar e ingrese un nombre de usuario y contraseña si es necesario.
3. Para habilitar Trampas de autenticación, haga clic para marcar la casilla.
4. Para cambiar el Intervalo de captura de latidos, elija un tiempo de la lista desplegable o elija Desactivado para evitar que se envíen trampas de latidos.
   - Los intervalos de tiempo ofrecidos son de 5 minutos, 30 minutos o 1, 4, 8, 12 o 24 horas.
5. Para cada trampa, elija si desea desactivar o establecer el intervalo en uno de los períodos de la pantalla. menú.

   Para obtener descripciones de la configuración, consulte Carpeta SNMP en la página 56.
6. Haga clic en Guardar para confirmar los cambios o en Cancelar para descartarlos.
7. Reinicie la tarjeta:
   a. En la pestaña Comunicaciones, haga clic en Soporte.
   b. Haga clic en Habilitar.
   C. Haga clic en Reiniciar.

MIB de productos globales para la integración SNMP

La tarjeta Liebert IntelliSlot Unity permite la gestión SNMP de equipos Liebert. Para integrar la tarjeta en una implementación SNMP, importe o compile la MIB de Liebert Global Products en la estación de administración de red (NMS).

La MIB de productos globales de Liebert está disponible en https://www.vertivco.com/en-us/support/software download/monitoring/management-information-bases-mibs-for-liebert-products/. Es compatible con los formatos de archivo de Windows® (192436P1) y Unix (192435P1).

Configurar ajustes de SNMP

Los usuarios de SNMPv3 o las configuraciones de captura y acceso de SNMPv1/v2c deben realizarse antes de que se produzca el acceso o las notificaciones de SNMP. La tarjeta Unity permite hasta 20 usuarios SNMPv3, hasta 20 destinos de captura SNMPv1 y hasta 20 direcciones de acceso SNMPv1/v2c.

Los cambios necesarios varían según el tipo de protocolo SNMP utilizado:

• SNMPv1 debe tener configuraciones de captura. •

SNMPv2c debe tener configuración de acceso. • Los

usuarios de SMPv3 deben tener configuraciones configuradas y el método para generar el ID del motor puede ser seleccionado

• la configuración de acceso para SNMPv1/v2c es independiente de la configuración de captura de SNMPv1.

Seleccione el formato de ID del motor SNMPv3

De forma predeterminada, la ID del motor se genera automáticamente utilizando la dirección MAC. Opcionalmente, puede seleccionar una identificación basada en texto en su lugar.

1. En la pestaña Comunicaciones, seleccione Protocolos > SNMP.
2. Haga clic en Editar e ingrese un nombre de usuario y contraseña si es necesario.
3. Edite la configuración:

consulte Carpeta SNMP en la página 56 para obtener descripciones de la configuración y las opciones. • En

Tipo de formato de ID de motor SNMPv3, seleccione Dirección MAC o Texto.

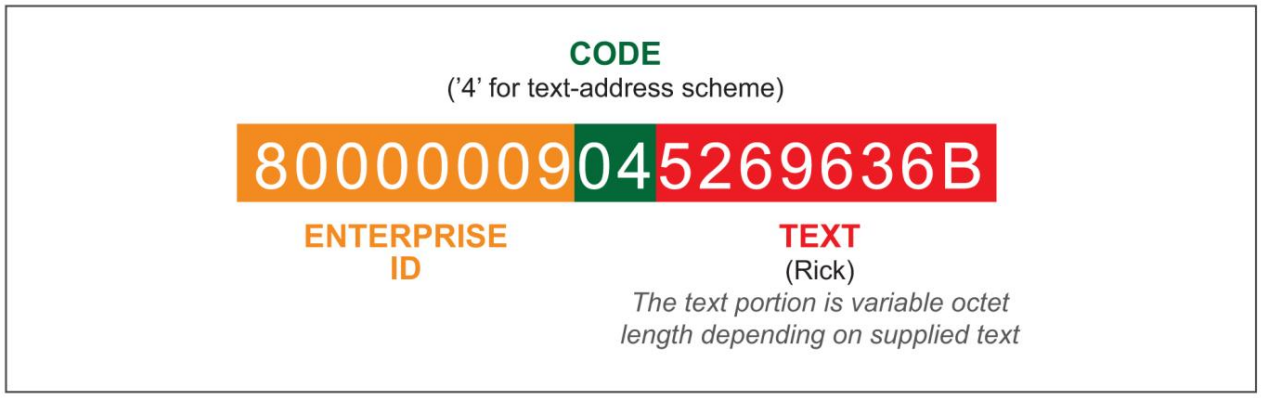
- Si seleccionó Texto, escriba el texto en el que se basará el ID del motor generado. • Haga clic en Guardar para

confirmar los cambios o en Cancelar para descartarlos.

La nueva ID del motor no se muestra hasta después de reiniciar la tarjeta en el Paso 4.

El ID del motor generado por texto es una representación hexadecimal de caracteres ASCII similar a la que se muestra en la Figura 3.1 en la página siguiente.

Figura 3.1 ID del motor SNMP generado usando un esquema de formato de texto



NOTA: Si el tipo de formato o el texto para la ID del motor están incompletos o no son válidos, la ID del motor se genera en función de la dirección MAC.

4. Reinicie la tarjeta para activar los cambios:
   a. En la pestaña Comunicaciones, haga clic en Soporte.
   b. Haga clic en Habilitar.
   C. Haga clic en Reiniciar.

Configurar los ajustes de usuario de SNMPv3

1. En la pestaña Comunicaciones, seleccione Protocolos > SNMP >
   Configuración de usuarios de SNMPv3 20) > Configuración de usuarios de SNMPv3 (1).

NOTA: La configuración debe realizarse para cada usuario que recibirá notificaciones.

2. Haga clic en Editar e ingrese un nombre de usuario y contraseña si es necesario.
3. Ingrese la información y establezca los permisos apropiados para el usuario.
   Para obtener descripciones de la configuración y las opciones, consulte Carpeta de usuario de SNMPv3 en la página 57.
4. Haga clic en Guardar para confirmar los cambios o en Cancelar para descartarlos.
5. Repita los pasos 1 a 4 para usuarios adicionales.
6. Reinicie la tarjeta para activar los cambios:
   a. En la pestaña Comunicaciones, haga clic en Soporte.
   b. Haga clic en Habilitar.
   C. Haga clic en Reiniciar.

Configurar ajustes de trampas SNMPv1

1. En la pestaña Comunicaciones, seleccione Protocolos > SNMP > Trampa SNMPv1 (20).

NOTA: La configuración debe realizarse para cada usuario que recibirá notificaciones.

2. Haga clic en Editar e ingrese un nombre de usuario y contraseña si es necesario.
3. Ingrese la información y establezca los permisos apropiados para el usuario.
   Para obtener descripciones de la configuración, consulte Carpeta de capturas SNMPv1 en la página 58.

4. Haga clic en Guardar para confirmar los cambios o en Cancelar para descartarlos.
5. Repita los pasos del 1 al 4 para cualquier usuario adicional.
6. Reinicie la tarjeta para activar los cambios:
   a. En la pestaña Comunicaciones, haga clic en Soporte.
   b. Haga clic en Habilitar.
   C. Haga clic en Reiniciar.

Configure los ajustes de acceso a SNMPv1/v2c

1. En la pestaña Comunicaciones, seleccione Protocolos > SNMP > Acceso SNMPv1/v2c (20) > Acceso SNMPv1/v2c (1).

NOTA: Al seleccionar la carpeta Acceso SNMPv1/v2c, solo se muestran los ajustes que están disponibles para la configuración.

2. Haga clic en Editar e ingrese un nombre de usuario y contraseña si es necesario.
3. Ingrese la información y establezca los permisos apropiados para el usuario.
   Para obtener una descripción de la configuración y las opciones, consulte Carpeta de acceso SNMPv1/v2c en la página 59.
4. Haga clic en Guardar para confirmar los cambios o en Cancelar para descartarlos.
   La tarjeta debe reiniciarse antes de que se pueda cambiar la configuración de otro usuario.
5. Reinicie la tarjeta para activar los cambios para este usuario: a. En la pestaña Comunicaciones, haga clic en Soporte.
   b. Haga clic en Habilitar.
   C. Haga clic en Reiniciar.

3.2 Descargar asignaciones de protocolos

La Tarjeta Unity permite descargar archivos que enumeran la información disponible desde un dispositivo administrado para cada protocolo habilitado. Los listados identifican los datos disponibles del dispositivo y cómo se representarán o mapearán esos datos en un protocolo particular.

NOTA: Los sensores Liebert SN no son compatibles a través de BACnet o Modbus.

Para descargar una lista de asignación de datos:

Haga clic en la pestaña Dispositivo administrado, luego en Resumen > Descargas.
El encabezado Archivos de asignación de datos muestra archivos de asignación para cada protocolo habilitado:

• BACnetDataMap.txt para BACnet IP y BACnet MSTP • ModbusDataMap.txt para Modbus TCP y Modbus RTU • SNMP_Events.txt, SNMP_Parameters.txt, SNMP_upsMibEvents.txt y SNMP_upsParams.txt para SNMP v1/v2c/v3 • Ydn23DataMap.txt para YDN23

Hay más información disponible sobre la asignación de protocolos BACnet y Modbus en la Guía de referencia de protocolos Liebert IntelliSlot Modbus y BACnet (SL-28170) en www.vertivco.com. Los archivos MIB de SNMP también están disponibles para su descarga desde el sitio.

4 HABILITAR CLIENTE EN LA NUBE PARA LIEBERT® MINI-MATE™

El cliente en la nube es exclusivo para el sistema de gestión térmica Mini-Mate. El menú de configuración para Cloud Client solo se muestra cuando el dispositivo administrado detectado es una unidad Mini-Mate. Para todos los demás dispositivos, NO se mostrará el menú de configuración de Cloud Client.

El cliente en la nube actualiza un servidor en la nube y hace que la información del estado de Mini-Mate esté disponible para una aplicación móvil, lo que proporciona monitoreo de dispositivo remoto para la unidad Mini-Mate.

Para configurar el cliente en la nube, comience con la configuración típica para la compatibilidad con el cliente en la nube (requisitos previos) a continuación.

4.1 Configuración típica para soporte de cliente en la nube (requisitos previos)

La configuración de Cloud Client en una tarjeta Unity sin inicializar requiere lo siguiente:

- La tarjeta Unity debe tener asignada una dirección de red y tener acceso a la URL del Servicio en la Nube. La URL del servicio en la nube suele ser https://icomcms.com.
- El DNS debe estar configurado y funcionando correctamente porque se utiliza para acceder a la nube Servicio.
- La tarjeta Unity debe tener un nombre de sistema que sea único para la organización. La tarjeta de la unidad El "Nombre del sistema" se asigna al "Nombre del administrador" en el Servicio en la nube.
- El dispositivo administrado debe ser un sistema de administración térmica Mini-Mate. De lo contrario, la nube La carpeta del cliente no está disponible en el menú de la interfaz de usuario web de Unity.
- La siguiente información de Cloud Client debe haber sido configurada de fábrica o ser configurada por el cliente utilizando la información proporcionada por la fábrica:
  - Dirección de correo electrónico: la dirección de correo electrónico del cliente asociada con la Organización de servicios en la nube específica para el cliente.
  - Clave de registro: suministrada de fábrica • URL del servicio en la nube: normalmente https://icomcms.com
- El cliente de la nube debe estar habilitado.

Con estos elementos en su lugar o preparados, continúe con Registro en el portal de administración de servicios en la nube para permitir el acceso de usuarios de aplicaciones móviles en la página siguiente.

4.2 Registro en el portal de administración de servicios en la nube para permitir el acceso de usuarios de aplicaciones móviles

Las unidades de gestión térmica deben estar registradas para proporcionar datos a la nube para que los usuarios de aplicaciones móviles reciban las notificaciones de la unidad de refrigeración.

Las unidades se registran según la parte del dominio de la dirección de correo electrónico de la organización. El dominio es la parte que sigue al símbolo “@” y normalmente es el nombre de la organización, por ejemplo: @company.com.

NOTA: Antes de intentar registrarse con el Servicio móvil en la nube, se deben asignar credenciales de red a la tarjeta Unity de la unidad en su red corporativa para acceder a la URL del Servicio en la nube (https://icomcms.com).

NOTA: Al registrar la unidad de refrigeración, asegúrese de utilizar una dirección de correo electrónico con el dominio correcto de la organización. Si se registra utilizando una dirección de correo electrónico con un dominio incorrecto, cancele el registro y comuníquese con el administrador para obtener la dirección correcta.

NOTA: La aplicación móvil está disponible para descargar desde Apple Store o Google Play Store, según su dispositivo móvil. Busque "iCOM CMS".

Para registrarse en el portal de administración:

1. Use un cable Ethernet CAT5 para conectar una computadora/portátil a un puerto Ethernet en Unity tarjeta.
2. En la computadora conectada, abra un navegador web e ingrese la dirección predeterminada de la tarjeta: 169.254.24.7 en la barra de direcciones.

   Se abre la interfaz de usuario web de Unity.
3. Configure el Nombre del sistema antes de intentar registrar la unidad Mini-Mate: • En la interfaz de usuario web de Unity,

   haga clic en la pestaña Comunicaciones . • En el panel Comunicaciones del lado

   izquierdo, seleccione Configuración > Sistema.

   • Haga clic en Editar e ingrese el Nombre de usuario y la Contraseña predeterminados, que es Liebert (caso

   sensible) para ambos. •

   Ingrese un nombre de sistema descriptivo para la unidad Mini-Mate. Esto identificará la unidad para la gestión en el portal de administración del cliente en la nube. • Ingrese las configuraciones restantes del

   sistema si es necesario y haga clic en Guardar.
4. Reinicie la tarjeta para que los cambios surtan efecto: • Panel de

   comunicaciones en el lado izquierdo, seleccione Soporte.

   • En la sección Comandos, haga clic en Habilitar e ingrese el Nombre de usuario y la Contraseña predeterminados, que es Liebert (se

   distingue entre mayúsculas y minúsculas) para ambos.

   • Haga clic en Reiniciar tarjeta.
5. Obtenga una dirección de correo electrónico con un dominio válido del administrador de Unity que administra los dispositivos móviles. acceso a la aplicación para la organización.
6. En la interfaz de usuario web de Unity, haga clic en la pestaña Comunicaciones , consulte Carpeta de cliente en la nube en la página 52.
7. En el panel Comunicaciones del lado izquierdo, seleccione Configuración > Cliente en la nube.
8. Haga clic en Editar e ingrese el Nombre de usuario y la Contraseña predeterminados, que es Liebert (se distingue entre mayúsculas y minúsculas) para ambos.

9. Haga clic para habilitar junto a Cloud Client e ingrese lo siguiente:

- Dirección de correo electrónico = dirección de correo electrónico del cliente asociada con la organización del cliente dentro del servicio en la nube. La organización se basa en la parte del dominio de la dirección de correo electrónico.

- Clave de registro = clave única configurada de fábrica que identifica la tarjeta Mini-Mate/Unity para el servicio en la nube. La clave no se puede compartir entre tarjetas Unity. • URL del servicio en la nube = https://icomcms.com. La dirección del portal de administración de servicios en la nube, a través del cual se administran los usuarios de aplicaciones móviles.

10. Haga clic en Guardar.

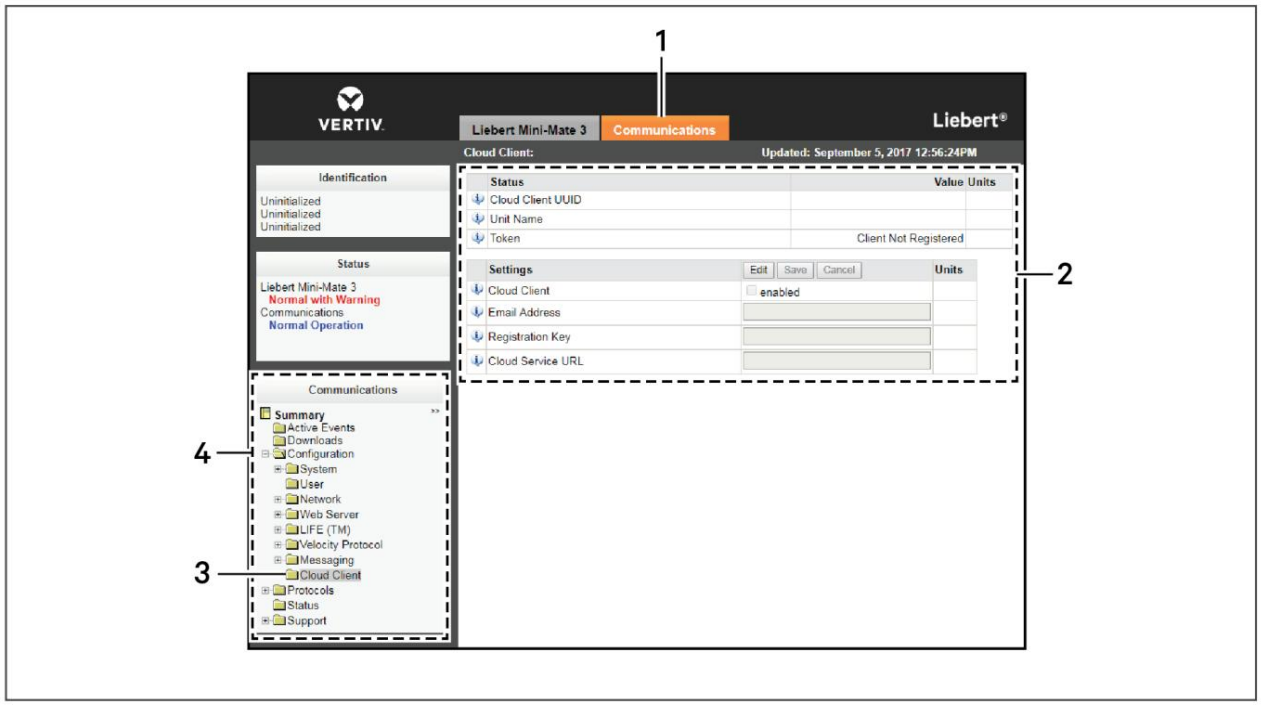
11. Reinicie la tarjeta para que los cambios surtan efecto: • Panel de comunicaciones en el lado izquierdo, seleccione Soporte.

- En la sección Comandos, haga clic en Habilitar e ingrese el Nombre de usuario y la Contraseña predeterminados, que es Liebert (se distingue entre mayúsculas y minúsculas) para ambos.

- Haga clic en Reiniciar tarjeta.

  El dispositivo está registrado en el portal de administración de clientes en la nube.

Figura 3.2 Página del cliente en la nube



DESCRIPCIÓN DEL ARTÍCULO	
1	Pestaña de comunicaciones
2	Configuración y estado del cliente en la nube
3	Carpeta del cliente en la nube
4	Carpetas de comunicaciones

5 DISEÑO DE LA PÁGINA WEB DE LA TARJETA UNITY

La configuración predeterminada de la tarjeta Unity le permite usarla inmediatamente después de la instalación para monitorear el equipo en el que está instalada la tarjeta. La interfaz web personaliza la información para facilitar la supervisión del equipo y la resolución de problemas. Puede nombrar el equipo, ingresar una ubicación, configurar alertas de correo electrónico y de texto y cambiar la configuración del equipo.

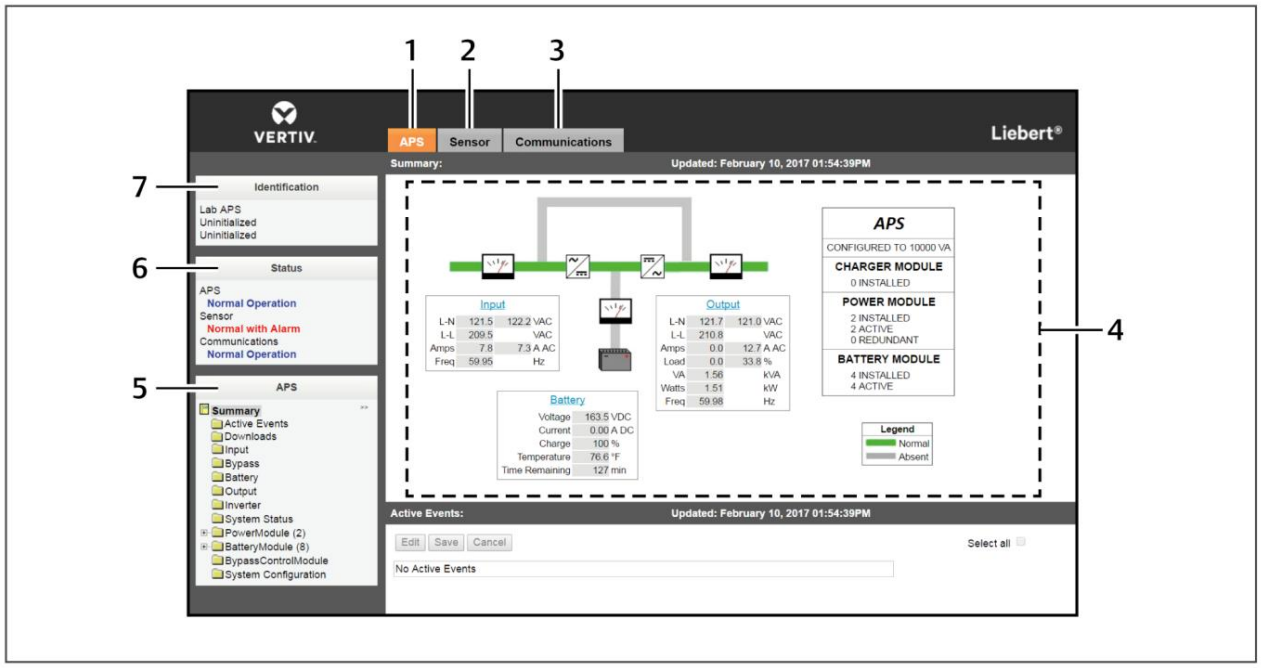
NOTA: El botón Editar aparece atenuado si no se puede cambiar la configuración de un menú.

5.1 Secciones de la página web

Cada tarjeta de unidad tiene una interfaz de usuario de página web (interfaz de usuario web) con las siguientes áreas, consulte la Figura 4.1 a continuación.

• Panel de identificación • Panel
de estado • Panel de
menú de fichas • Área de
detalles

Figura 4.1 Secciones de la página web



ARTÍCULO	DESCRIPCIÓN
1	La pestaña de dispositivos administrados muestra información sobre el equipo monitoreado y controlado. Consulte Menús de la pestaña Dispositivo administrado en la página opuesta para obtener más detalles. La etiqueta de la pestaña nombra el tipo de unidad Liebert en la que está instalada la tarjeta. Por ejemplo, la pestaña Dispositivo administrado para una tarjeta instalada en un UPS Liebert APS tiene la etiqueta "APS" (consulte la Figura 4.1 en la página anterior).
2	La pestaña Sensor muestra información sobre los sensores Liebert SN, si están instalados, incluidos el estado o los datos de cada sensor y los ajustes de configuración del sensor. Cuando los sensores están conectados a la tarjeta, la pestaña Sensor aparece entre la pestaña Dispositivo administrado y la pestaña Comunicaciones. La pestaña no se muestra cuando no hay sensores conectados a la tarjeta. Consulte Menú de la pestaña del sensor en la página 26 para obtener más información.
3	La pestaña Comunicaciones muestra información sobre la tarjeta Unity, como el estado general de eventos del equipo y la interfaz de comunicación, registros de información de terceros, configuraciones de comunicación, configuraciones de protocolos de terceros y estado del sistema. Consulte el menú de la pestaña Comunicaciones en la página opuesta para obtener más detalles.
4	El área de detalles muestra información detallada sobre el dispositivo según la selección de menú realizada en el área de menú de pestañas. Las ediciones del dispositivo y su configuración se realizan en esta sección.
5	Menú de pestañas seleccionadas. De forma predeterminada, la interfaz de usuario web siempre muestra dos pestañas, la pestaña del dispositivo administrado y la pestaña Comunicaciones. Aparece una tercera pestaña, la pestaña Sensor, si se han instalado sensores Liebert SN.
6	El panel de estado muestra el estado del equipo monitoreado, la tarjeta Unity y cualquier sensor Liebert SN conectado a la tarjeta.
7	El panel de identificación muestra el nombre del sistema, la ubicación del sistema y la descripción del sistema.

5.2 Texto de ayuda

Cada página web que muestra la tarjeta Unity tiene texto informativo que se revela al pasar el cursor sobre el icono a la izquierda de la fila Estado, Eventos o Configuración.

La interfaz de usuario web puede mostrar cualquiera de los 6 iconos descritos en la siguiente tabla.

Tabla 4.1 Texto e iconos de ayuda

ICONO	DESCRIPCIÓN
	Evento Normal
	Información del Evento
	Alarma de evento
	Advertencia de evento
	Evento crítico
	información sobre herramientas

5.3 Menús de la pestaña Dispositivo administrado

Los menús en la pestaña Dispositivo administrado enumeran solo los datos que son relevantes para el equipo monitoreado. Por ejemplo, los menús que muestra una tarjeta Unity instalada en un SAI difieren de los menús que muestra una tarjeta instalada en un equipo de gestión térmica. Los elementos de menú seleccionados también muestran información detallada basada en el equipo en el que está instalada la tarjeta. La información de energía se muestra en la pestaña Dispositivo administrado para un UPS, mientras que la información ambiental se muestra para una unidad de administración térmica.

5.4 Menú de la pestaña Comunicaciones

La pestaña Comunicaciones muestra el estado general de los eventos del equipo y la interfaz de comunicación.
Contiene registros de información de terceros, configuraciones de comunicaciones, configuraciones de protocolos de terceros e información de estado del sistema como se detalla en la siguiente tabla.

Tabla 4.2 Menús de la pestaña Comunicación

MENÚ	DESCRIPCIÓN	VER DETALLES:
Eventos activos	Muestra la actividad del evento actual	Eventos activos Carpeta en la página 29
Descargas • Registros del agente (o UnityCard) • Registros de eventos • Registros de datos • Otros archivos	La descarga de archivos a archivos accesibles por texto, delimitados por comas o delimitados por tabuladores facilita la resolución de problemas.	Descargas Carpeta en la página 29
Configuración • Sistema • Usuarios • Autenticación remota • Red • Servidor web • VIDA • Servicios Remotos • Protocolo de velocidad • Mensajería	Muestra información sobre la configuración del sistema, el acceso, las conexiones de red, la configuración de VelocityProtocol y si el correo electrónico y la mensajería SMS están habilitados	Configuración Carpeta en la página 30
Protocolos • Modbus • BACnet • SNMP • YDN23	Muestra información y configuraciones relacionadas con los protocolos de terceros disponibles empleados para monitorear el equipo.	Protocolos Carpeta en la página 53

Tabla 4.2 Menús de la pestaña Comunicación (continuación)

MENÚ	DESCRIPCIÓN	VER DETALLES:
Estado • Estado del sistema • Es necesario reiniciar el sistema • Se cambió la identidad del dispositivo LIFE™ ; es necesario reconfigurar LIFE™ • Conflicto de puerto RS-485 • ID de nodo MSTP VelocityProtocol duplicado • ID de nodo MSTP BACnet duplicado	Muestra el estado general del sistema y si es necesario reiniciar para activar los cambios de configuración; el reinicio se realiza solo desde el Soporte Carpeta	Carpeta de estado en la página 59
Apoyo • Hora y fecha del agente • Modelo del agente • Versión del firmware de la aplicación del agente • Etiqueta del firmware de la aplicación del agente • Versión del firmware de arranque del agente • Etiqueta del firmware de arranque del agente • Número de serie del agente • Fecha de fabricación del agente • Versión del hardware del agente • Versión GDD • Versión FDM • ID de secuencia del producto • Tarjeta de reinicio • Restablecer la tarjeta a los valores predeterminados de fábrica (consulte la NOTA a continuación) • Generar y descargar archivo de diagnóstico • Actualización de firmware • Redes activas	Muestra la información necesaria para el mantenimiento o la resolución de problemas y accesos directos para reiniciar la tarjeta, restablecer la tarjeta Unity a sus valores predeterminados de fábrica y actualizar el firmware de la tarjeta.	Apoyo Carpeta en la página 60 (firmware Actualizar también en)

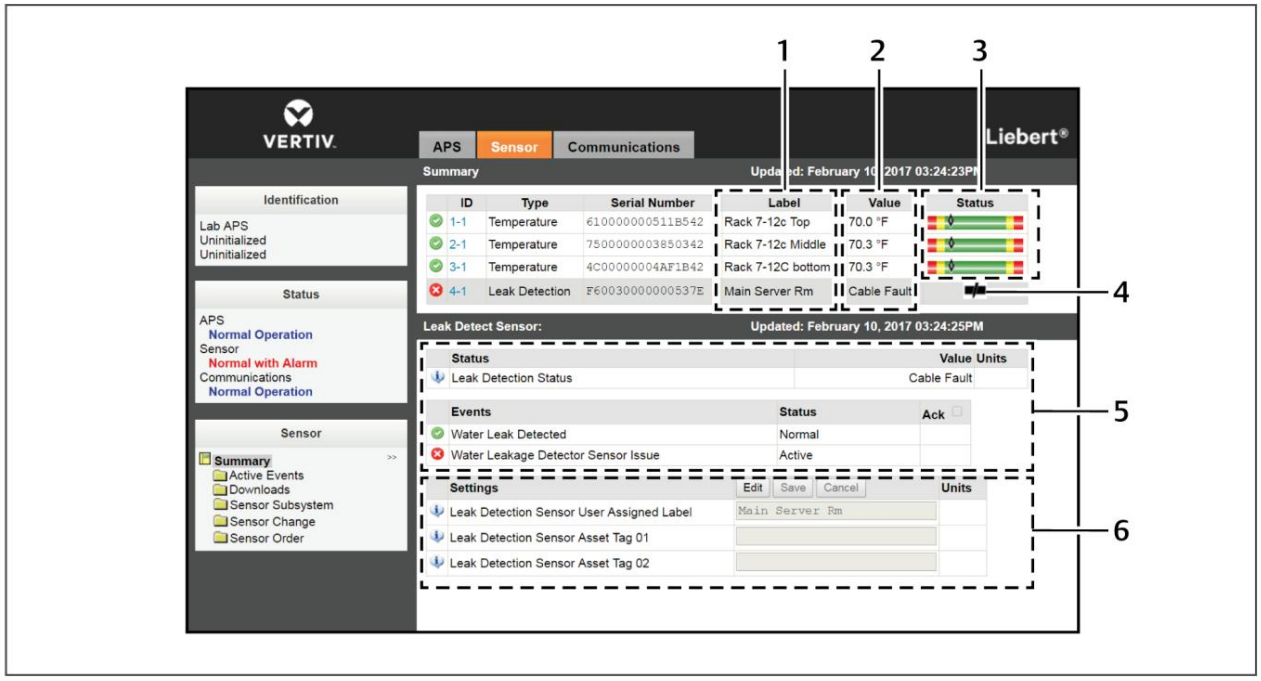
NOTA: La tarjeta se puede restablecer a los valores predeterminados de fábrica manualmente usando el botón de reinicio, consulte Restablecimiento manual a los valores predeterminados de fábrica en la página 67.

5.5 Menú de la pestaña Sensor

NOTA: Solo se muestra si hay un sensor conectado.

Cuando los sensores Liebert SN están instalados y conectados al puerto del sensor en la tarjeta Unity, la pestaña Sensor aparece

Figura 4.2 Página Resumen de la pestaña del sensor



ARTÍCULO	DESCRIPCIÓN
1	Etiquetas asignadas por el usuario para la identificación/ubicación del sensor
2	Valores reales de lectura del sensor
3	Los gráficos indican las lecturas del sensor en relación con los umbrales.
4	Los iconos indican las lecturas del estado del sensor, por ejemplo: falla del cable o puerta abierta/cerrada según la función del sensor.
5	Detalles del sensor: datos del sensor seleccionado en la lista de resumen.
6	Configuración del sensor: configuración/datos editables para el sensor seleccionado en la lista de resumen.

El menú Sensor contiene carpetas que muestran una descripción general de los sensores instalados, el estado de los eventos de los sensores, enlaces de descarga para archivos de registro y ajustes de configuración del sensor que se describen en la siguiente tabla.

Tabla 4.3 Carpetas del menú de la pestaña Sensor

CARPETA	DESCRIPCIÓN
Resumen	Muestra una lista de los sensores detectados actualmente, con su estado y valores. También muestra una sección de detalles sobre el sensor que está seleccionado actualmente
Eventos activos	Muestra una lista de eventos de sensor que están actualmente activos.
Descargas	Muestra una lista de archivos de texto que se pueden descargar. Los archivos disponibles dependen del estado actual de la tarjeta.
Servidor de sensores • Número de modelo del sistema • Estado del sistema • Demasiados sensores • Tragamonedas no disponibles • Sensor de reconocimiento Cambios	Muestra información general sobre los sensores.
Cambio de sensor	Enumera los eventos que muestran los sensores que se agregaron o eliminaron. Si la lista tiene entradas, aparece un botón Confirmar. Al hacer clic en el botón Confirmar se borra la lista. El botón Reconocer de esta página tiene el mismo comportamiento que el botón Reconocer de la página Servidor de sensores.
Orden de sensores	Muestra una lista de sensores y permite configurar el orden en que se muestran los sensores en la página Resumen.

5.5.1 Página de resumen de la pestaña del sensor

La página Resumen de la pestaña Sensor muestra el estado de todos los sensores instalados, detalles sobre el sensor seleccionado y un panel de Configuración que permite cambiar la etiqueta de un sensor, los umbrales, si corresponde, la configuración de alarmas y el reconocimiento de alarmas y eventos. Consulte la Figura 4.2 en la página anterior.

La selección de un sensor permite cambiar su configuración en la parte inferior de la ventana.

Los eventos también pueden reconocerse en esta ventana.

5.5.2 Panel de detalles de resumen de la pestaña Sensor

El panel Detalles de la pestaña Sensor aparece cuando se selecciona la carpeta Resumen. El área muestra el estado de todos los sensores conectados. Consulte la Figura 4.2 en la página anterior.

Los sensores compatibles incluyen:

- Temperatura • Humedad
- Cierre de puerta
- Cierre de contacto
- Detección de fugas

Cuando se selecciona un sensor, los detalles de ese sensor se muestran en este panel. El contenido de la sección de detalles es específico para el tipo de sensor seleccionado. Por ejemplo, un sensor de temperatura muestra las lecturas de temperatura y un sensor de puerta muestra si la puerta está abierta o no.

La Unidad de medida utilizada para los valores de temperatura se define en la configuración Unidades de temperatura de visualización en la pestaña Comunicaciones. Consulte Carpeta del sistema en la página 30.

Los detalles de los sensores incluyen el estado actual o la lectura, el estado del evento y si la lectura está por encima o por debajo del umbral establecido en el panel Configuración.

5.5.3 Cambiar el orden de los sensores

Los sensores se enumeran en el orden en que se instalan. Puede cambiar el orden para colocar los sensores que se consideren más importantes en la parte superior de la lista.

Para cambiar el orden de la lista de sensores:

1. En la pestaña Sensor, haga clic en Orden del sensor.
2. Haga clic en Editar e ingrese el nombre de usuario y la contraseña.
3. Seleccione el botón de radio para que el sensor se mueva.
4. Use las flechas a la derecha de la lista para mover el sensor hacia arriba o hacia abajo.
5. Haga clic en Guardar.

6 EDICIÓN DE LA CONFIGURACIÓN DE LA TARJETA UNITY

La interfaz de usuario web se puede usar para configurar los ajustes de la tarjeta Unity y del equipo monitoreado. Los siguientes pasos se aplican a la realización de cambios en todos los ajustes de configuración.

Para editar la configuración:

1. Abra un navegador web e ingrese la dirección IP de la tarjeta.
2. Haga clic en la pestaña Comunicaciones.
3. En el menú de pestañas, seleccione la carpeta que contiene el ajuste de configuración que desea cambiar.
4. Haga clic en Editar e ingrese un nombre de usuario y contraseña si es necesario.
5. Cambie la configuración.
6. Haga clic en Guardar para aplicar los cambios o en Cancelar para descartarlos.

6.1 Carpetas del menú de la pestaña Comunicaciones

La pestaña Comunicaciones contiene información sobre el estado general de los eventos del equipo y la interfaz de comunicación. Presenta registros de información de terceros, configuraciones de comunicación, configuraciones de protocolos de terceros e información de estado del sistema. Las carpetas de Comunicaciones son:

- Carpeta de eventos activos a continuación
- Carpeta de descargas a continuación
- Carpeta de configuración en la página siguiente • Carpeta de protocolos en la página 53 • Carpeta de estado en la página 59 • Carpeta de soporte en la página 60

6.2 Carpeta de eventos activos

La carpeta Eventos activos no contiene ajustes configurables. La carpeta muestra eventos que afectan la tarjeta Unity.

6.3 Carpeta de Descargas

La carpeta Descargas no contiene ajustes configurables. La carpeta muestra enlaces para descargar registros de protocolos de terceros que están habilitados en la tarjeta Unity. Los registros ayudan a configurar y solucionar problemas de comunicación entre los sistemas de administración de red o de administración de edificios que se utilizan para monitorear el dispositivo administrado.

6.4 Carpeta de configuración

La carpeta de configuración de nivel superior muestra el número de modelo del sistema de la tarjeta Unity. Este nombre está configurado de fábrica y no se puede cambiar. La carpeta Configuración contiene las siguientes subcarpetas:

6.4.1 Carpeta del sistema

La subcarpeta Sistema muestra información general sobre el dispositivo monitoreado y administrado. Puede seleccionar las unidades de temperatura que se muestran, que es "Celsius" de forma predeterminada.

Para editar la información mostrada:

1. Haga clic en Editar e ingrese un nombre de usuario y contraseña si es necesario.
2. Realice los cambios y haga clic en Guardar.

Configuración del servicio horario

La subcarpeta Sistema contiene la carpeta Servicio horario. Cada configuración ofrece un menú de opciones o una casilla de verificación para habilitar/deshabilitar.

Opciones de configuración del servicio horario	
Fuente de tiempo externa	La fuente externa que se usará para la sincronización de tiempo. Predeterminado = Servidor NTP.
Servidor de tiempo NTP primario	URL, nombre de host o dirección IP de la fuente de tiempo NTP principal. Máximo de 64 caracteres.
Servidor de tiempo NTP de copia de seguridad	URL, nombre de host o dirección IP de la fuente de tiempo NTP de respaldo. Máximo de 64 caracteres.
Tasa de sincronización de tiempo NTP	La velocidad a la que se sincronizará la hora con el servidor del protocolo de hora de la red, si NTP es la fuente de hora externa.
Zona horaria	Zona horaria donde se encuentra el dispositivo.

Habilitar la sincronización automática con el dispositivo administrado

Habilite el tiempo de escritura automática en el dispositivo administrado.

Tasa de sincronización automática de dispositivos administrados

Frecuencia a la que se escribirá la hora en el dispositivo gestionado, si se ha seleccionado una fuente de hora externa.

6.4.2 Carpeta de usuarios locales

La subcarpeta Usuarios locales ofrece hasta 10 usuarios y 3 niveles de acceso que se describen en la Tabla 5.1 a continuación.

La contraseña predeterminada para todos los usuarios es Liebert (se distingue entre mayúsculas y minúsculas).

Tabla 5.1 Niveles de acceso de usuarios

NIVEL NOMBRE	ACCESO/ PERMISO TIPO	DESCRIPCIÓN
Sin acceso	Ninguno	El nivel Sin acceso se aplica cuando el "Sitio protegido por contraseña" está habilitado.
Usuario general	Solo lectura	Capaz de ver todas las pestañas, carpetas y subcarpetas de la interfaz de usuario. Un usuario general solo necesitará ingresar la contraseña asignada si el "Sitio protegido por contraseña" está habilitado, consulte Carpeta del servidor web en la página 39. De manera predeterminada, el Usuario local [2] es Usuario con la contraseña predeterminada de Liebert (ambos distinguen entre mayúsculas y minúsculas). La autorización (tipo de acceso) para el usuario local [2] es "Usuario general".
Administrador	Lectura/Escritura	Capaz de editar la configuración usando la contraseña asignada, que siempre se requiere para editar la configuración/ la configuración. De forma predeterminada, el usuario local [1] es Liebert con la contraseña predeterminada Liebert (ambos distinguen entre mayúsculas y minúsculas). La autorización (tipo de acceso) para el usuario local [1] es "Administrador". Asegúrese de tener siempre un usuario administrador, para que pueda acceder y modificar la configuración y otras configuraciones.

¡IMPORTANTE! Registre los nombres de usuario y las contraseñas y guárdelos en un lugar seguro donde se puedan encontrar si se olvidan. Una contraseña perdida no se puede recuperar de la tarjeta IS-UNITY. Si se pierde la contraseña del administrador, la tarjeta debe restablecerse a los valores predeterminados de fábrica y reconfigurarse.

Para cambiar los nombres de usuario y las contraseñas:

NOTA: Máximo de 30 caracteres. Todos los caracteres imprimibles son válidos excepto: \ : ' < > ~ ? " #

1. En la pestaña Comunicaciones, seleccione Configuración > Usuarios locales, luego seleccione la carpeta del usuario a configurar.
2. Haga clic en Editar e ingrese el nombre de usuario y la contraseña del administrador, luego haga clic en Aceptar.
3. Ingrese un nuevo nombre de usuario y contraseña.
4. Vuelva a ingresar la contraseña para confirmarla.
5. En Autorización para Usuario, seleccione el tipo de acceso, ver Tabla 5.1 arriba.
6. Haga clic en Guardar para confirmar los cambios o en Cancelar para descartarlos.

6.4.3 Carpeta de autenticación remota

El nivel superior de la subcarpeta de autenticación remota muestra el tipo de autenticación configurado. La implementación proporciona autenticación y autorización en el servidor remoto.

La carpeta contiene subcarpetas para tipos de autenticación:

Autenticación RADIUS

El servidor RADIUS remoto proporciona la autenticación y la autorización.

Configuración de RADIO

[Habilitar/Deshabilitar selección]

Habilita la autenticación RADIUS en la tarjeta.

Servidor de autenticación principal

Dirección IP del servidor de autenticación principal.

Servidor de autenticación secundario

Dirección IP del servidor de autenticación secundario.

Secreto

El secreto compartido que sirve como contraseña entre el cliente y el servidor.

Se acabó el tiempo

Tiempo en milisegundos entre reintentos de autenticación. Rango: 0 a 65535

reintentos

Número de veces para intentar contactar antes de intentar con un servidor diferente.

Requisitos de configuración del servidor para la autenticación RADIUS

El valor de Filter-Id debe ser

```
unity_group=unityadmin;
```

- o -

```
unity_group=unityuser;
```

- Los atributos están en un archivo de configuración o una interfaz GUI depende del servidor de autenticación implementación.
- Unity_group=unityuser; se puede usar de la misma manera que unity_group=unityadmin; . • Unity_group=unityadmin; y unity_group=unityuser; La cadena debe terminar con un punto y coma.

Autenticación LDAP

El servidor LDAP remoto proporciona la autenticación y la autorización.

NOTA: Si está utilizando una instalación Linux OpenLDAP lista para usar, debe agregar el atributo "Info" para especificar la autorización del grupo Unity, o la autorización LDAP no funcionará. Consulte Adición del atributo "Info" al esquema LDAP para Linux OpenLDAP en la página siguiente.

Configuración de LDAP

[Habilitar/Deshabilitar selección]

Habilita la autenticación LDAP en la tarjeta.

Servidor LDAP

Dirección IP del servidor LDAP.

Base LDAP

Nombre distinguido base, la ruta a las cuentas de usuario de LDAP.

LDAP seguro

Modo SSL.

Nombre de usuario de la base de datos

Bind Distinguished Name, la cuenta de servicio utilizada para acceder al servidor LDAP.

Contraseña de la base de datos

Contraseña de la cuenta de servicio que accede al servidor LDAP.

Atributos de inicio de sesión

Atributo de cuenta que autentica las credenciales del usuario, por ejemplo: CN.

Requisitos de configuración del servidor para la autenticación LDAP

El valor de la información debe ser

```
unity_group=unityadmin;
```

- o -

```
unity_group=unityuser;
```

- Los atributos se ingresan en un archivo de configuración o una interfaz GUI dependiendo de la autenticación implementación del servidor.
- Unity_group=unityuser; se puede usar de la misma manera que unity_group=unityadmin; . • Unity_group=unityadmin; y unity_group=unityuser; La cadena debe terminar con un punto y coma.

Adición del atributo "Info" al esquema LDAP para Linux OpenLDAP

La tarjeta Unity obtiene información de autorización de grupo de un servidor LDAP remoto para un usuario LDAP a través del atributo "Info" en la cuenta de usuario LDAP remoto del usuario. El atributo "Info" especifica la autorización de grupo mediante "unity_group=<x>;" donde <x> es "unityadmin" o "unityuser". Sin embargo, la cuenta de usuario de una instalación Linux OpenLDAP lista para usar no proporciona el atributo "Info", por lo que la compatibilidad con LDAP remoto no funcionará hasta que se agregue la compatibilidad con el atributo "Info" a las cuentas de usuario de LDAP.

El esquema LDAP para una instalación de Linux OpenLDAP está definido y existe en "/etc/ldap/schema". El esquema LDAP para una cuenta de usuario existe en el archivo "nis.ldif" y se especifica en una clase de objeto denominada "posixAccount".

Agregue el atributo "Info" como miembro del atributo "posixAccount" DEBE de modo que siempre se considere para especificar para un usuario. El atributo "Info" ya existe en el esquema LDAP, pero no está asignado a nada en el esquema predeterminado.

Para agregar el atributo "Info" en una nueva instalación de OpenLDAP:

Antes de iniciar OpenLDAP, consulte lo siguiente para editar el archivo “nis.ldif”:

Esquema de objeto original "posixAccount":

- olcObjectClasses: (1.3.6.1.1.1.2.0 NAME 'posixAccount' DESC 'Abstracción de una cuenta con atributos POSIX' SUP top AUXILIAR DEBE (cn $ uid $ uidNumber $ gidNumber $ homeDirectory) MAY (userPassword $ loginShell $ gecos $ description))

Esquema de objeto "posixAccount" actualizado con el atributo "Info" agregado:

- olcObjectClasses: (1.3.6.1.1.1.2.0 NAME 'posixAccount' DESC 'Abstracción de una cuenta con atributos POSIX' SUP top AUXILIAR DEBE (cn $ uid $ uidNumber $ gidNumber $ homeDirectory $ Info) MAY (userPassword $ loginShell $ gecos $ descripción))

Para agregar el atributo "Info" en una instalación OpenLDAP existente:

Use "ldapmodify" u otra herramienta de administrador de LDAP para agregar el atributo "Info" a las cuentas de usuario.

Autenticación TACACS+

El servidor TACACS+ remoto proporciona autenticación y autorización.

Configuración de TACACS+

[Habilitar/Deshabilitar selección]

Habilita la autenticación TACACS+ en la tarjeta.

Servidor de autenticación principal

Dirección IP del servidor TACACS+ primario.

Servidor de autenticación secundario

Dirección IP del servidor TACACS+ secundario.

Secreto

El secreto compartido que sirve como contraseña entre el cliente y el servidor.

Se acabó el tiempo

Tiempo en milisegundos entre reintentos de autenticación. Rango: 0 a 65535

reintentos

Número de veces para intentar contactar antes de intentar con un servidor diferente.

Versión

Versión menor.

Requisitos de configuración del servidor para la autorización TACACS+

El archivo de configuración contiene unity_group=unityadmin; cadena en el campo de acceso.

```
usuario = tacacsAdmin {

servicio = acceso {

unity_group=unityadmin;

}

}
```

- o -

El archivo de configuración contiene unity_group=unityuser; cadena en el campo de acceso.

```
usuario = tacacsAdmin {

servicio = acceso {

unity_group=unityuser;

}

}
```

- Los atributos están en un archivo de configuración o una interfaz GUI depende del servidor de autenticación implementación.
- Unity_group=unityuser; se puede usar de la misma manera que unity_group=unityadmin; . •

Unity_group=unityadmin; y unity_group=unityuser; La cadena debe terminar con un punto y coma.

Autenticación Kerberos

Configuración de Kerberos

[Habilitar/Deshabilitar selección]

Habilita la autenticación Kerberos en la tarjeta.

Servidor (Reino)

Dirección IP del servidor Kerberos.

Nombre de dominio del reino

Nombre del dominio de sistemas que comparten la base de datos de Kerberos.

Nombre de dominio

Dominio donde reside la base de datos de Kerberos en el sistema maestro.

6.4.4 Carpeta de red

El nivel superior de la subcarpeta Red muestra lo siguiente:

Dúplex de velocidad

Selecciona la configuración de velocidad y dúplex del puerto Ethernet de la tarjeta. Está configurado en Automático de forma predeterminada. Si es necesario cambiarlo, comuníquese con el administrador del sistema para obtener la configuración adecuada.

nombre de host

Identifica el nodo de red. Predeterminado = UNITY-serial_number_of_card.

Lista de sufijos de nombres de dominio

Listado de sufijos de nombres de dominio para la resolución de nombres de host. Si es necesario cambiarlo, comuníquese con el administrador del sistema para obtener la configuración adecuada.

Servidor Telnet

Habilita/deshabilita el acceso telnet a la tarjeta para evitar cambios no autorizados. La configuración predeterminada deshabilita el acceso telnet.

Servidor SSHv2

Habilita/deshabilita el acceso SSHv2 (Secure SHell) a la tarjeta para evitar cambios no autorizados. La configuración predeterminada deshabilita el acceso SSHv2.

La carpeta Red también contiene subcarpetas relacionadas con la comunicación:

• Carpetas IPv4 e IPv6 en la página siguiente • Carpeta de prueba del servidor de nombres de dominio (DNS) en la página 39

Carpetas IPv4 e IPv6

La configuración de IPv4 e IPv6 determina qué protocolo de Internet se utilizará para la comunicación a través de la red conectada al puerto Ethernet. Las redes IPv4 e IPv6 se ejecutarán en paralelo (red de doble pila), pero los protocolos son diferentes. Consulte a su administrador de red para determinar qué protocolo debe habilitarse y determinar la configuración correcta.

Configuración de IPv4

Protocolo IPv4

Habilita IPv4 en la tarjeta

Método de dirección IP

Modo en el que se inicia la tarjeta para ser un dispositivo listo para la red (Estático, DHCP, BootP). Predeterminado = DHCP.

Dirección IP estática

Dirección de red para la interfaz

Máscara de subred

Máscara de red para la interfaz que divide una red en segmentos manejables

Puerta de enlace predeterminada

Dirección IP de la puerta de enlace para el tráfico de red destinado a otras redes o subredes

Origen de la dirección del servidor DNS

Origen de la identificación del servidor DNS (Ninguno, Automático, Configurado)

Servidor DNS primario

Dirección de red del servidor DNS principal.

Servidor DNS secundario

Dirección de red del servidor DNS secundario.

Configuración de IPv6

Protocolo IPv6

Habilita IPv6 en la tarjeta.

Método de dirección IP

Modo en el que se inicia la tarjeta para ser un dispositivo listo para la red (estático, automático). Predeterminado = Automático.

Dirección IP estática

Dirección de red para la interfaz.

Longitud del prefijo

Longitud del prefijo de la dirección que divide una red en segmentos manejables.

Puerta de enlace predeterminada

Dirección IP de la puerta de enlace para el tráfico de red destinado a otras redes o subredes. Predeterminado = 64.

Origen de la dirección del servidor DNS

Origen de la identificación del servidor DNS (Ninguno, Automático, Configurado). Predeterminado = Automático.

Servidor DNS primario

Servidor DNS primario

Servidor DNS secundario

Servidor DNS secundario

Carpeta de prueba del servidor de nombres de dominio (DNS)

La prueba del servidor de nombres de dominio verifica los puntos clave de la configuración de un servidor de nombres de dominio (DNS) para un dominio determinado.

Configuración de prueba del servidor de nombres de dominio (DNS)

Respuesta a la última consulta

Respuesta de un servidor de nombres de dominio (DNS) a la última consulta.

Ejemplo: gxtwebdemo.liebert.com resuelto a 126.4.203.251

Tipo de consulta

Tipo de consulta de DNS. (Nombre de host, dirección IP)

Valor de consulta

Valor para que el servidor de nombres de dominio (DNS) lo resuelva. Ejemplo: gxtwebdemo.liebert.com

6.4.5 Carpeta del servidor web

La configuración del servidor web permite realizar algunas configuraciones de seguridad, como HTTP o HTTPS, y habilitar contraseñas.

Configuración del servidor web

Protocolo de servidor web

Seleccione el modo de funcionamiento del Servidor Web (HTTP, HTTPS). Predeterminado = HTTP.

Puerto HTTP

Puerto web estándar no encriptado. Obligatorio si HTTP está habilitado como Protocolo de servidor web. Predeterminado = 80.

Puerto HTTPS

Puerto web seguro estándar; toda la comunicación está encriptada. Obligatorio si HTTPS está habilitado como Protocolo de servidor web. Predeterminado = 443.

Sitio protegido por contraseña

Cuando está habilitado, se requiere una sesión de inicio de sesión antes de que se muestre la información del dispositivo al usuario. Las credenciales de nivel de usuario solo permitirán ver la información del dispositivo. Se requieren credenciales de nivel de administrador para realizar cualquier cambio.

Acceso de escritura remota

Cuando está habilitado, todos los navegadores web tienen acceso de escritura a los datos en todas las páginas web de la tarjeta Unity cuando el usuario inicia sesión con credenciales de administrador. Cuando está deshabilitado, el acceso de escritura está restringido a los navegadores web conectados a través de la dirección de configuración automática de IPv4 en 169.254.24.7. Para obtener información adicional, consulte Conexión directa a la computadora para la configuración en la página 4.

NOTA: Cuando el acceso de escritura remota está deshabilitado, se muestra un indicador en la esquina superior derecha de la página web como recordatorio, como se muestra en la siguiente figura.

NOTA: Solo deshabilite el acceso de escritura remota si está absolutamente seguro de que no necesita administrar el dispositivo administrado o la tarjeta Unity a través de una sesión remota de navegador web. Se requiere una conexión directa local a 169.254.24.7 para habilitar esta configuración.

Tiempo de espera inactivo de la sesión

El intervalo que esperará el software antes de cerrar la sesión de un usuario a menos que haya actividad del usuario (el valor predeterminado es 5 min.)

Figura 5.1 Indicador de acceso de escritura remota deshabilitado

Carpeta de certificados

Cuando el Protocolo de servidor web está configurado para utilizar comunicaciones HTTPS, todas las comunicaciones del servidor web con todos los navegadores se cifran y validan según los algoritmos de seguridad y las comprobaciones de validez especificadas en el certificado SSL que está actualmente instalado en la tarjeta. De manera predeterminada, la tarjeta genera su propio certificado SSL único y autofirmado cuando se enciende por primera vez. Sin embargo, muchas instalaciones desean instalar y utilizar archivos de certificados SSL generados por su propia Autoridad de certificación (CA).

Las selecciones en Certificado proporcionan comandos para Cargar archivos PEM de certificado SSL o Generar certificado SSL autofirmado.

Comandos de certificado

Cargar archivos PEM de certificado SSL

Carga e instala un archivo de clave SSL con codificación PEM y un archivo de certificado que fueron generados por una autoridad de certificación de confianza y que cumplen con las directivas SSL CertificateKeyFile y SSLCertificateFile del módulo mod_ssl de Apache . Consulte Carga de archivos PEM de certificado SSL en la página siguiente.

NOTA: Para obtener más información sobre el uso de certificados SSL por parte de Apache, consulte http://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslcertificatefile.

Generar certificado SSL autofirmado

Genera e instala un nuevo certificado autofirmado basado en el modo seleccionado para Generar modo de certificado SSL autofirmado. Consulte Generación de un certificado SSL autofirmado en la página 43.

Configuración del certificado

Generar modo de certificado SSL autofirmado

Método utilizado para generar un certificado SSL autofirmado. Las opciones son:

- Usar valores predeterminados = los valores usados en lugar de los campos configurables por el usuario son los mismos que los utilizados cuando la tarjeta generó el certificado SSL original en el primer encendido. Los valores predeterminados no se muestran.
- Usar ajustes configurados = los valores ingresados por el usuario en los campos configurables se usan para generar el certificado.

NOTA: Al usar los ajustes configurados, todos los campos configurables, que se describen a continuación, deben tener una entrada para generar correctamente un certificado.

Nombre común

Nombre de dominio totalmente calificado que usarán los clientes del navegador para llegar al servidor web de la tarjeta cuando se ejecuta con el certificado generado con el nombre ingresado aquí.

Organización

Organización o empresa identificada como propietaria del certificado generado.

Unidad organizacional

Unidad organizativa o división de la empresa de la organización identificada como propietaria del certificado generado.

Ciudad o Localidad

Ciudad o localidad de la organización identificada como titular del certificado generado.

Estado o Provincia

Estado o provincia de la organización identificada como propietaria del certificado generado.

Código de país

Código de país (abreviatura de 2 letras) de la organización identificada como propietaria del certificado generado.

Dirección de correo electrónico

Dirección de correo electrónico del contacto dentro de la organización identificado como propietario del certificado generado.

Carga de archivos PEM de certificado SSL

1. En la pestaña Comunicaciones, seleccione Configuración > Servidor web > Certificado.
2. En Comandos, haga clic en Habilitar, luego haga clic en Cargar junto a Cargar archivos PEM de certificado SSL.

   Se abre el cuadro de diálogo de carga. Consulte la figura siguiente.
3. Siga las instrucciones del cuadro de diálogo para seleccionar y cargar los archivos apropiados.

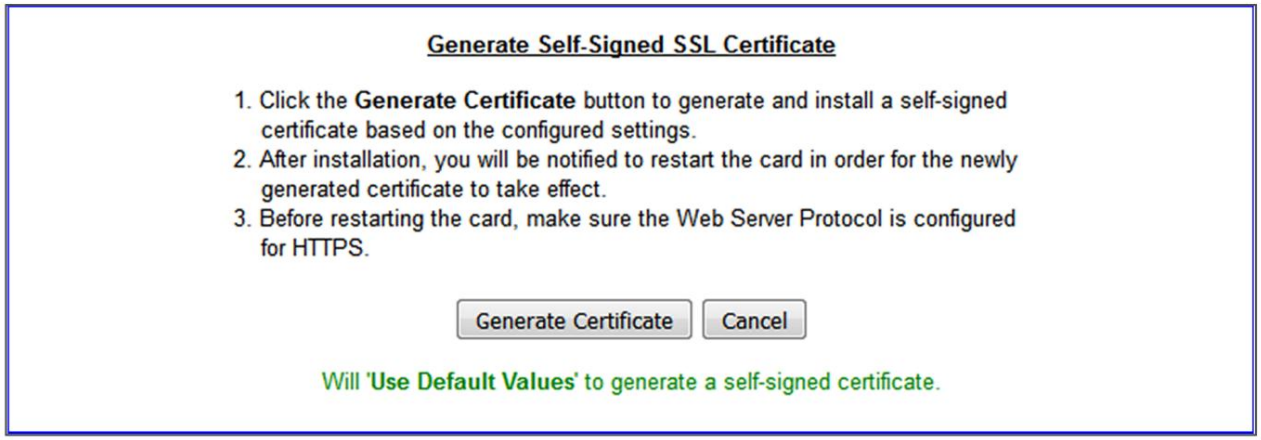
Figura 5.2 Cuadro de diálogo Cargar archivos PEM de clave SSL y certificado

Generación de un certificado SSL autofirmado

1. En la pestaña Comunicaciones, seleccione Configuración > Servidor web > Certificado.
2. En la sección Configuración:
   a. Haga clic en Editar.
   b. En Generar modo de certificado SSL autofirmado, seleccione el modo que desea usar.
   - Si selecciona Ajustes configurados por el usuario, realice entradas en todos los campos de valor configurable (obligatorio) y luego haga clic en Guardar.
3. En la sección Comandos, haga clic en Habilitar, luego haga clic en Generar junto a Generar SSL autofirmado. Certificado.

   Se abre el cuadro de diálogo generar. Consulte la figura siguiente.
4. Siga las instrucciones del cuadro de diálogo para generar e instalar el certificado.

Figura 5.3 Cuadro de diálogo Generar certificado SSL autofirmado



6.4.6 Carpeta LIFE™

La subcarpeta LIFE contiene configuraciones que afectan el uso de la tecnología Vertiv™ LIFE, un servicio de monitoreo y diagnóstico remoto para las unidades Vertiv™. La configuración de LIFE es para uso exclusivo del personal capacitado de Vertiv™ y no requiere cambios por parte del usuario. Las siguientes tablas proporcionan información de referencia sobre la configuración de LIFE.

La configuración de esta carpeta está gestionada por Vertiv™. Se requiere un contrato de servicio.

Para obtener asistencia, comuníquese con el Soporte técnico de Vertiv™ para servicios LIFE al 1-800-435-7250, opción 3.

Tabla 5.2 Configuración de estado de LIFE

ESTADO	DESCRIPCIÓN
Medios de conexión	Los medios de conexión de LIFETechnology
Habilitar fecha y hora	La fecha y hora en que se habilitó el soporte de LIFETechnology.
Ajustes	Descripción
Tecnología LIFE	Habilitar o deshabilitar la tecnología LIFE
Anulación del número de serie del sistema	Cuando está habilitado, un número de serie del sistema configurado por el usuario anulará un número de serie configurado en el dispositivo ,

Tabla 5.2 Configuración de estado de LIFE (continuación)

ESTADO	DESCRIPCIÓN
Número de serie del sistema	Número de serie del sistema, obtenido de la unidad automáticamente
Número de etiqueta del equipo del sitio	Número de etiqueta del equipo del sitio
Identificador del sitio	Identificador del sitio, ingresado por el técnico de servicio
Responder llamada entrante	Habilite la respuesta de llamadas entrantes de LIFEWatch Station
Fecha y hora de la próxima llamada	Fecha y hora de la próxima llamada a realizar al servidor de LIFEWatch Station
Días de intervalo de llamadas	Días entre llamadas de rutina a LIFEWatch Station
Horas de intervalo de llamadas	Número de horas entre llamadas de rutina de LIFEWatch Station
Minutos de intervalo de llamadas	Número de minutos entre llamadas rutinarias de LIFEWatch Station. Este valor se usa junto con val_life_callInterval_hours.
Número de prueba de llamada	El número de intentos de reintentar una llamada después de que falla antes de reprogramar la llamada.

Tabla 5.3 Configuración de mensajería SMS de estado de UPS de LIFE

AJUSTES	DESCRIPCIÓN
SMS de restablecimiento de red principal	Enviar SMS cuando se restablezca la red principal
Red principal restaurada SMSValue	Valor enviado a través de SMS cuando se restaura la red principal
SMS de fallo de red principal	Enviar SMS cuando falla la red principal
Fallo de red principal SMSValue	Valor enviado a través de SMS cuando falla la red principal
Omitir SMS de falla de red	Enviar SMS cuando falla la red eléctrica de derivación
Omitir fallo de red SMSValue	Valor enviado a través de SMS cuando falla Bypass Mains
Cargar al omitir SMS	LIFELoad on Bypass SMS Habilitar
Retraso de SMS de carga en omisión	La cantidad de tiempo para retrasar el envío de un SMS después de que una carga esté en Omisión si la condición aún existe.

6.4.7 Carpeta de servicios remotos

El nivel superior de la subcarpeta Servicios remotos ofrece opciones para conexiones de servicios remotos.

La configuración de esta carpeta está gestionada por Vertiv™. Se requiere un contrato de servicio.

Para obtener asistencia, comuníquese con Vertiv™ LIFE Services al 1-800-435-7250, opción 3.

La carpeta contiene subcarpetas para conectividad y diagnóstico:

• Conectividad de servicios remotos en la página siguiente • Diagnóstico de servicios remotos en la página 47

Opciones y configuraciones de servicio remoto

Número de serie del dispositivo

Número de serie obtenido del dispositivo gestionado. Identifica el dispositivo en el sistema a menos que Dispositivo La anulación del número de serie está habilitada.

Restablecer configuración de servicios remotos

Restablece la configuración del servicio remoto a los valores predeterminados de fábrica.

NOTA: No restablece la configuración de la tarjeta de comunicación.

Servicio remoto

Habilita/deshabilita la conexión de servicio remoto.

Muestreo de datos del dispositivo

Activa/Desactiva el muestreo de datos del dispositivo.

Número de serie del dispositivo

Número de serie utilizado cuando se habilita la anulación del número de serie del dispositivo .

Anulación del número de serie del dispositivo

Habilita/Deshabilita el uso del número de serie obtenido del dispositivo administrado.

Número de etiqueta del equipo del sitio

Número de la etiqueta del equipo del sitio.

Identificador del sitio

Número de identificación del sitio.

ID de instancia de dispositivo

Número de identificación del dispositivo del fabricante.

Centro de servicio País

País en el que se repara el dispositivo.

Conectividad de servicios remotos

Opciones y configuraciones de conectividad de servicio remoto

Resultado de la prueba de conectividad

Resultado de la prueba de conectividad más reciente.

Prueba de conectividad

Inicia la prueba de conectividad.

Evaluar la configuración de servicios remotos

Intente conectarse al servicio remoto para verificar la configuración.

URL de la plataforma de servicio remoto

Dirección URL de la plataforma de servicio remoto. No ingrese el prefijo "http://" o "https://".

Tiempo de reintento de conexión

Período de tiempo para intentar la reconexión en caso de una falla de comunicación. Rango: 30 a 600 segundos.

Habilitar proxy

Habilita el uso de URL de plataforma de servicio remoto para conectarse con un servidor proxy.

Autenticación de proxy

Habilita la autenticación del servidor proxy.

Dirección proxy

Dirección IP o URL del servidor proxy.

Número de puerto IP de proxy

Número de puerto del servidor proxy. Rango: 1 a 65535.

Nombre de usuario delegado

Nombre de usuario del servidor proxy.

Contraseña de usuario proxy

Contraseña del servidor proxy.

URL de la nube de servicio remoto

Dirección URL de la nube de servicio remoto. No ingrese el prefijo "http://" o "https://".

Diagnóstico de servicios remotos

Configuración de diagnóstico de servicio remoto

Estado de comunicación

Resultados de la transacción más reciente.

Recuento de errores de comunicación

Número de errores de comunicación desde el reinicio.

último error de comunicaciones

Mensaje de error de comunicación más reciente desde el reinicio con marca de fecha y hora.

Información del archivo de reglas del dispositivo monitoreado

Detalles sobre el archivo de reglas de servicio remoto vigente para el dispositivo monitoreado.

Estado operativo de los servicios remotos

Estado del servicio remoto.

Estado del dispositivo administrado

Estado de comunicación del dispositivo gestionado con la tarjeta.

6.4.8 Carpeta de protocolo de velocidad

Velocity Protocol contiene cuatro subcarpetas: Managed Device, MSTP, Ethernet e Internal. Velocity es el protocolo de entrada de un sistema gestionado/supervisado.

NOTA: Con la excepción de cambiar la ID de nodo cuando se usan varias tarjetas o cuando se deshabilita el acceso a IP de Velocity-Protocol, la configuración en las subcarpetas de Velocity Protocol no debe modificarse a menos que lo indique un representante de Vertiv™.

NOTA: Liebert® Nform™ requiere que el acceso IP a Velocity esté habilitado.

Opciones del protocolo de velocidad

Acceso IP de protocolo de velocidad

Cuando está deshabilitado, impide el acceso desde un sistema remoto basado en IP mediante el protocolo Velocity. Predeterminado = Deshabilitado.

6.4.9 Carpeta de mensajes

La subcarpeta Mensajería habilita y deshabilita el correo electrónico y la mensajería de texto sobre eventos. La subcarpeta también facilita una prueba para determinar si el correo electrónico y los mensajes de texto se pueden enviar con éxito. La configuración de los dos métodos de mensajería permite especificar quién recibe los mensajes, el formato de los mensajes y otros detalles.

Opciones de mensajería

Correo electrónico

Está habilitado para enviar mensajes de correo electrónico sobre eventos.

SMS

Está habilitado para enviar mensajes de texto sobre eventos.

Correo electrónico

Las selecciones en Correo electrónico determinan cómo la tarjeta envía correos electrónicos sobre eventos.

Ajustes del correo electrónico

Correo electrónico de la dirección

Dirección de correo electrónico del remitente. En la mayoría de los casos, será la dirección de correo electrónico de la persona a quien se deben enviar las respuestas. Ejemplo Soporte@empresa.com

Correo electrónico a la dirección

Dirección de correo electrónico del destinatario. Varias direcciones de correo electrónico están separadas por un punto y coma.

Tipo de asunto del correo electrónico

Asunto del correo electrónico. Este valor será predeterminado para la descripción del evento, a menos que se personalice ingresando Texto de asunto personalizado.

Texto de asunto personalizado

El asunto editable del mensaje. El valor predeterminado es la descripción del evento si no se ingresa nada.

Dirección del servidor SMTP

Nombre de dominio completo o dirección IP del servidor utilizado para retransmitir mensajes de correo electrónico.

NOTA: Si usa un nombre de servidor, es posible que deba configurar un servidor DNS en Configuración de red.

Puerto del servidor SMTP

Puerto del servidor SMTP. Predeterminado = 25.

Conexión SMTP

Tipo de conexión del servidor SMTP. Determina las capacidades del servidor SMTP. Las opciones son:

- Clear = No usar cifrado • SSL/TLS = Cifrado mediante conexión SSL/TLS • STARTTLS = Cifrado SSL/TLS iniciado mediante STARTTLS.

Autenticación SMTP

Habilite o deshabilite la autenticación SMTP de correo electrónico. Se debe proporcionar una cuenta de correo electrónico para que el proveedor de servicios SMTP se autentique.

NOTA: Algunos servidores de correo electrónico pueden requerir cambios en la configuración de la cuenta para permitir la comunicación con la tarjeta Unity. Por ejemplo, Gmail solo reconoce las aplicaciones de Google como seguras. Sin embargo, proporcionan una configuración de cuenta que permite la autenticación con lo que consideran "aplicaciones menos seguras".
Consulte a su administrador de red o proveedor de servicios para obtener detalles de configuración.

Nombre de usuario SMTP

Nombre de usuario de la cuenta de correo electrónico que se usará cuando la autenticación SMTP de correo electrónico esté habilitada.

Contraseña SMTP

Contraseña de la cuenta de correo electrónico que se utilizará cuando la autenticación SMTP de correo electrónico esté habilitada.

Incluir dirección IP en el mensaje

Si está marcada, la dirección IP de la tarjeta del agente se incluirá en los mensajes salientes.

Incluir descripción del evento en el mensaje

Si está marcada, la descripción del evento SNMP se incluirá en los mensajes salientes.

Incluir nombre en el mensaje

Si está marcado, el nombre de la tarjeta del agente se incluirá en los mensajes salientes.

Incluir contacto en el mensaje

Si está marcado, el contacto de la tarjeta del agente se incluirá en los mensajes salientes.

Incluir ubicación en el mensaje

Si está marcada, la ubicación de la tarjeta del agente se incluirá en los mensajes salientes.

Incluir descripción en el mensaje

Si está marcada, la descripción de la tarjeta del agente se incluirá en los mensajes salientes.

Incluir enlace web en el mensaje

Si está marcado, se incluirá un enlace web a la tarjeta del agente y el número de puerto de escucha del servidor web en los mensajes salientes.

Habilitar la consolidación de eventos

Si está marcado, se enviarán múltiples eventos por mensaje saliente.

Límite de tiempo de consolidación

Si la consolidación de eventos está habilitada, se enviará un mensaje cuando haya pasado el 'Límite de tiempo de consolidación' en segundos desde que se recibió el primer evento almacenado en el búfer.

Límite de eventos de consolidación

Si la consolidación de eventos está habilitada, se enviará un mensaje cuando la cantidad de eventos almacenados alcance el 'Límite de eventos de consolidación'.

SMS

Las selecciones en SMS determinan cómo la tarjeta envía mensajes de texto sobre eventos.

Configuración de SMS

SMS desde la dirección

Dirección de SMS del remitente. En la mayoría de los casos, será la dirección de SMS de la persona a la que se deben enviar las respuestas. Por ejemplo: Soporte@empresa.com

SMS a dirección

Dirección SMS del destinatario. Varias direcciones de SMS están separadas por un punto y coma.

Tipo de asunto de SMS

Asunto del SMS. El valor predeterminado es la descripción del evento, a menos que se personalice con Texto de asunto personalizado.

Texto de asunto personalizado

El asunto editable del mensaje. El valor predeterminado es la descripción del evento si no se ingresa nada.

Dirección del servidor SMTP

Nombre de dominio completo o dirección IP del servidor utilizado para retransmitir mensajes SMS.

NOTA: Si usa un nombre de servidor, es posible que deba configurar un servidor DNS en Configuración de red.

Puerto del servidor SMTP

Puerto del servidor SMTP. Predeterminado = 25.

Conexión SMTP

Tipo de conexión del servidor SMTP. Determina las capacidades del servidor SMTP. Las opciones son:

• Clear = No usar cifrado • SSL/TLS = Cifrado
mediante conexión SSL/TLS • STARTTLS = Cifrado SSL/TLS iniciado
mediante STARTTLS.

Autenticación SMTP

Habilite o deshabilite la autenticación SMS SMTP. Se debe proporcionar una cuenta de SMS para que el proveedor de servicios SMTP se autentique.

NOTA: Algunos servidores de mensajería pueden requerir cambios en la configuración de la cuenta para permitir la comunicación con la tarjeta Unity. Por ejemplo, Gmail solo reconoce las aplicaciones de Google como seguras. Sin embargo, proporcionan una configuración de cuenta que permite la autenticación con lo que consideran "aplicaciones menos seguras".
Consulte a su administrador de red o proveedor de servicios para obtener detalles de configuración.

Nombre de usuario SMTP

Nombre de usuario de la cuenta de SMS que se usará cuando la autenticación SMS SMTP esté habilitada.

Contraseña SMTP

Contraseña de la cuenta de SMS que se utilizará cuando la autenticación SMS SMTP esté habilitada.

Incluir dirección IP en el mensaje

Si se marca, la dirección IP de la tarjeta del agente se incluirá en los mensajes salientes.

Incluir descripción del evento en el mensaje

Si se marca, la descripción del evento SNMP se incluirá en los mensajes salientes.

Incluir nombre en el mensaje

Si está marcado, el nombre de la tarjeta del agente se incluirá en los mensajes salientes.

Incluir contacto en el mensaje

Si está marcado, el contacto de la tarjeta del agente se incluirá en los mensajes salientes.

Incluir ubicación en el mensaje

Si está marcada, la ubicación de la tarjeta del agente se incluirá en los mensajes salientes.

Incluir descripción en el mensaje

Si está marcada, la descripción de la tarjeta del agente se incluirá en los mensajes salientes.

Incluir enlace web en el mensaje

Si se marca, se incluirá un enlace web a la tarjeta del agente y el número de puerto de escucha del servidor web en los mensajes salientes.

Habilitar la consolidación de eventos

Si está marcado, se enviarán múltiples eventos por mensaje saliente.

Límite de tiempo de consolidación

Si la consolidación de eventos está habilitada, se enviará un mensaje cuando haya pasado el "límite de tiempo de consolidación" en segundos desde que se recibió el primer evento almacenado en el búfer.

Límite de eventos de consolidación

Si la consolidación de eventos está habilitada, se enviará un mensaje cuando la cantidad de eventos almacenados alcance el "Límite de eventos de consolidación".

Prueba de mensajería

Prueba la configuración para correo electrónico y mensajes SMS. Si la prueba falla, se deben cambiar las configuraciones incorrectas para garantizar que la tarjeta Unity envíe las notificaciones adecuadas si ocurre un evento.

6.4.10 Carpeta del cliente en la nube

NOTA: La configuración del cliente en la nube es utilizada exclusivamente por los sistemas de administración térmica Liebert Mini-Mate. La carpeta Cloud Client se muestra solo cuando el dispositivo administrado por la tarjeta Unity es una unidad Mini Mate.

La subcarpeta Cliente en la nube habilita/deshabilita el monitoreo remoto de dispositivos para una unidad Liebert Mini-Mate al registrar el dispositivo con el cliente en la nube que administra el monitoreo del estado del dispositivo para los usuarios de la aplicación móvil Liebert iCOM CMS.

Opciones de estado del cliente en la nube

UUID de cliente en la nube

Identificador de unidad para la tarjeta Unity que asocia la tarjeta y el servicio en la nube. El identificador se genera internamente, pero se muestra aquí y en el portal de administración del servicio en la nube.

Nombre de la unidad

Nombre descriptivo de la unidad Mini-Mate, completado según el nombre del sistema. Consulte Carpeta del sistema en la página 30 para configurar el Nombre del sistema y otra información específica del dispositivo.

NOTA: El nombre del sistema debe configurarse antes de registrar la unidad con el cliente en la nube.

Simbólico

Identificador único proporcionado por el servicio en la nube que confirma el registro. Si la unidad no está registrada, el campo muestra "Cliente no registrado".

Opciones de configuración del cliente en la nube

Habilitar cliente en la nube

Habilita/Deshabilita el registro de la unidad Mini-Mate con el servicio en la nube.

Dirección de correo electrónico

Dirección de correo electrónico del cliente asociada con la organización del cliente dentro del servicio en la nube. La organización se basa en la parte del dominio de la dirección de correo electrónico.

Clave de registro

Clave única preprogramada de fábrica que identifica la unidad Mini-Mate/tarjeta Unity para el servicio en la nube.

URL del servicio en la nube

La dirección del portal de administración de servicios en la nube, a través del cual se administran los usuarios de aplicaciones móviles. La URL predeterminada es https://icomcms.com.

6.5 Carpeta de Protocolos

La carpeta Protocolos muestra los tipos de protocolos que se pueden habilitar para que una tarjeta Unity se comunique con sistemas de administración como BMS, NOC, etc. No todos los protocolos están disponibles al mismo tiempo, por ejemplo: Modbus RTU y BACnet MSTP no se pueden usar al mismo tiempo porque se usa un puerto RS 485 para el protocolo de salida. La tarjeta permite habilitar dos protocolos de terceros.

NOTA: Para activar y configurar el protocolo Vertiv™ Velocity, consulte Carpeta del protocolo Velocity en la página 47.

Los ajustes en cada una de las subcarpetas configuran los protocolos seleccionados:

BACnet, Ver:

- Carpeta BACnet IP en la página siguiente
- Carpeta BACnet MSTP en la página siguiente

Modbus, consulte:

- Carpeta Modbus TCP en la página 55
- Carpeta Modbus RTU en la página 55

SNMP, consulte:

- Carpeta de usuario SNMPv3 en la página 57
- Carpeta Trap SNMPv1 en la página 58
- Carpeta de acceso SNMPv1/v2c en la página 59

YDN23, consulte Carpeta YDN23 en la página 59.

6.5.1 Carpeta BACnet

Configuración de BACnet

Acceso de escritura del dispositivo administrado

Habilite o deshabilite el servidor BACnet para escribir en el dispositivo administrado.

Interfaz BACnet

Interfaz de servidor BACnet: BACnet IP o BACnet MSTP.

Número de instancia de objeto de dispositivo

El número de instancia (0-4194302) del objeto de dispositivo del servidor BACnet.

Nombre del objeto del dispositivo

El nombre del objeto de dispositivo del servidor BACnet.

Tiempo de espera de APDU

El tiempo de espera en milisegundos entre reintentos de APDU (1-65535).

Reintentos de APDU

El número de veces para retransmitir una APDU después del intento inicial (0-8).

Carpeta IP BACnet

Configuración IP BACnet

Número de puerto IP de BACnet

El puerto para la conexión UDP/IP del servidor BACnet.

Registrarse como Dispositivo Extranjero

Habilite o deshabilite el registro como dispositivo externo.

Dirección IP de BBMD

Dirección IP del dispositivo de administración de transmisión BACnet (BBMD) al que se accederá para el dispositivo externo Registro

Tiempo de vida del dispositivo externo

Tiempo de permanencia en la tabla de Dispositivos Extranjeros de BBMD después del registro.

Carpeta BACnet MSTP

Configuración de BACnet MSTP

ID de nodo

El ID de nodo MS/TP (MAC) del servidor BACnet. Debe ser único para cada nodo en el bus de comunicación.

Velocidad de datos

La tasa de comunicación BACnet MSTP (bits por segundo).

Dirección maestra máxima

El ID de nodo máximo (MAC) en uso en la red MS/TP.

Marcos de información máxima

Número máximo de tramas de información que este nodo puede enviar antes de que deba pasar el token.

6.5.2 Carpeta Modbus

Configuración de Modbus

Acceso de escritura del dispositivo administrado

Habilite o deshabilite el servidor Modbus para escribir en el dispositivo administrado

Interfaz Modbus

Seleccione la interfaz Modbus, ya sea Modbus TCP o Modbus RTU

Carpeta Modbus TCP

El Modbus TCP permite la conexión a la tarjeta mediante:

- Cualquier cliente (Open) permite la comunicación por cualquier dirección IP • Clientes en la misma subred que la tarjeta Unity • Clientes con direcciones IP específicas (Listas de IP confiables); solo se permiten cinco direcciones

Configuración Modbus TCP

Limitar el tipo de acceso a la red

Lista de acceso IP

- Abierto • Misma subred
- Lista de IP de confianza

Puerto

El puerto TCP utilizado por el servidor Modbus para escuchar y responder a las solicitudes del protocolo Modbus.
Predeterminado = 502.

Recuento máximo de conexiones de clientes

Número máximo de conexiones simultáneas permitidas. Rango: 1 a 5.

Carpeta Modbus RTU

Configuración Modbus RTU

ID de nodo

ID del servidor Modbus para la interfaz; obtener del administrador de la red. Debe ser único para cada nodo en el bus de comunicación.

Tasa de baudios

Tasa de comunicación.

- 9600
- 19200
- 38400

Comprobación de paridad

La verificación de paridad de comunicación.

- Ninguno
- Incluso
- Extraño

6.5.3 Carpeta SNMP

Las carpetas y configuraciones en esta carpeta permiten configurar la tarjeta para varios tipos de comunicación SNMP, incluido el acceso, trampas y otras configuraciones de usuario.

Configuración de SNMP

ID del motor SNMPv3

El ID del motor SNMPv3 generado.

NOTA: La ID del motor se basa en la dirección MAC de la tarjeta de forma predeterminada.

Habilitar SNMP v1/v2c

Habilite o deshabilite SNMP v1/v2c.

Habilitar SNMP v3

Habilite o deshabilite SNMPv3.

Trampas de autenticación

Cuando está habilitada, se envía una trampa de autenticación si un host SNMP intenta acceder a la tarjeta a través de SNMP, pero la dirección del host no está en la Configuración de acceso SNMP o está utilizando la Cadena de comunidad incorrecta.

Intervalo de captura de latidos

Habilite o deshabilite y establezca un intervalo de 5 minutos, 30 minutos, 1 hora, 4 horas, 8 horas, 12 horas y 24 horas.

MIB RFC-1628

Habilite o deshabilite la compatibilidad con la recuperación de datos de los objetos MIB RFC-1628.

Trampas MIB RFC-1628

Habilite o deshabilite la compatibilidad con el envío de trampas RFC-1628. La MIB RFC-1628 debe estar habilitada para que funcionen las trampas RFC-1628.

Estas trampas se aplican solo a los sistemas UPS.

MIB de productos globales de Liebert (LGP)

Habilite o deshabilite la compatibilidad para obtener y configurar datos mediante la MIB de Liebert Global Products.

Trampas LGP MIB

Habilite o deshabilite la compatibilidad con las trampas MIB de Liebert Global Products. La MIB de LGP debe estar habilitada para que funcionen las trampas de LGP.

Trampa de notificación del sistema LGP MIB

Habilite o deshabilite la compatibilidad con la trampa de notificación del sistema LGP. Esta es una trampa única que se envía cada vez que se agrega o elimina una alarma o advertencia de la tabla de condiciones. Proporciona una descripción de texto del evento en un varbind del mensaje de captura. La MIB de LGP debe estar habilitada para que funcionen las trampas de notificación de LGP.

Tipo de formato de ID de motor SNMPv3

Selecciona el método para generar el ID del motor. Valores válidos:

• Dirección MAC (predeterminada) = ID de motor creada a partir de la dirección MAC de la tarjeta Unity. • Texto = ID de motor creado a partir del texto ingresado en Texto de ID de motor de SNMPv3. Ver Seleccionar SNMPv3 Formato de ID del motor en la página 15.

Texto de ID del motor SNMPv3

Texto en el que se crea el ID del motor cuando el tipo de formato de ID del motor SNMPv3 es Texto.

NOTA: Si este campo se deja en blanco, la ID del motor se genera a partir de la dirección MAC de la tarjeta Unity.

Carpeta de usuario SNMPv3

La tarjeta Unity admite hasta 20 usuarios SNMPv3 y ofrece seguridad avanzada que incluye autenticación y encriptación. La página de nivel superior es una tabla con configuraciones para los 20. La página muestra un enlace para editar las columnas de la tabla que se muestran para cada usuario de SNMPv3. Se puede acceder a la misma configuración haciendo clic en una carpeta para un usuario, como Usuario SNMPv3 [1].

Para mostrar la configuración, haga clic en cualquiera de los enlaces de usuario de SNMPv3. Después de realizar cualquier cambio, haga clic en Guardar para que los cambios sean efectivos.

Configuración de usuario de SNMPv3

Habilitación de usuario SNMPv3

Seleccione para habilitar la lectura, escritura o envío de notificaciones con las credenciales del usuario.

Nombre de usuario SNMPv3

El nombre de usuario al que se aplican las configuraciones de autenticación y privacidad. Esta cadena puede estar compuesta por caracteres imprimibles excepto dos puntos, tabulador, comillas dobles y signo de interrogación.

Tipo de acceso SNMPv3

Solo lectura, lectura/escritura o solo trampas

Autenticación SNMPv3

Algoritmo criptográfico utilizado para la autenticación: Ninguno, MD5 o SHA-1

Secreto de autenticación SNMPv3

Frase de paso o contraseña utilizada para la solicitud Get de SNMPv3. Esta cadena puede estar compuesta de caracteres imprimibles con la excepción de dos puntos, tabulador, comillas dobles y signo de interrogación. Nota: La entrada debe tener 8 o más caracteres pero no más de 64.

Privacidad SNMPv3

Algoritmo criptográfico utilizado para el cifrado. Las opciones son:

- Ninguno
- DESDE
- AES

Secreto de privacidad de SNMPv3

Frase de paso o contraseña utilizada para la solicitud Get de SNMPv3. Esta cadena puede estar compuesta de caracteres imprimibles con la excepción de dos puntos, tabulador, comillas dobles y signo de interrogación. Nota: La entrada debe tener 8 o más caracteres pero no más de 64.

Direcciones de destino de capturas SNMPv3

Hosts de red que recibirán capturas SNMPv3, identificados con un nombre de red o una dirección IP.
Las direcciones múltiples deben estar separadas por comas.

Puerto de captura SNMPv3

Puerto utilizado por el host de destino para recibir capturas SNMPv3; el valor predeterminado es 162.

Edición de la tabla SNMPv3

Puede configurar la cantidad de información que se muestra en la tabla en la página Configuración de usuario de SNMPv3 [20].

1. Encima de la tabla, haga clic en Haga clic aquí para editar las columnas que se muestran en esta tabla.
2. Marque las casillas junto a la información a incluir en la tabla.

   Las opciones le permiten mostrar la misma información en esta pantalla que la que se muestra cuando se selecciona la carpeta o el enlace para un usuario específico.

Carpeta de capturas SNMPv1

Esta página contiene configuraciones para hosts de red que reciben capturas SNMPv1. Se pueden habilitar y configurar hasta 20 destinatarios de trampas. Al igual que las páginas de SNMPv3, se puede acceder a la configuración de cada destino haciendo clic en los enlaces en la parte de detalles de la página o haciendo clic en las carpetas de los destinos de captura. Además, los datos que se muestran en la tabla se pueden cambiar haciendo clic en el enlace que se encuentra arriba de la tabla.

Configuración de trampas SNMPv1

Direcciones de destino de trampas SNMP

Configure hosts de red que recibirán notificaciones de alerta (es decir, trampas SNMP). El host se puede identificar como una dirección IP o el nombre de red del host.

Puerto de captura SNMP

Puerto utilizado por el host de destino para recibir notificaciones; el valor predeterminado es 162.

Cadena comunitaria de captura SNMP

Cadena que identifica un 'secreto' conocido solo por aquellos hosts que desean recibir una notificación de los cambios de estado del dispositivo. Valor predeterminado: público (distingue entre mayúsculas y minúsculas).

Carpeta de acceso SNMPv1/v2c

Esta página contiene configuraciones para hosts de red que acceden a datos usando SNMPv1/v2c. Se pueden habilitar y configurar hasta 20 hosts de acceso. Se requiere el puerto 161 como puerto de captura SNMP predeterminado para recibir alarmas. Al igual que las páginas de SNMPv3, se puede llegar a la configuración de cada host haciendo clic en los enlaces en la parte de datos de la página o haciendo clic en las carpetas de los hosts de acceso. Además, los datos que se muestran en la tabla se pueden cambiar haciendo clic en el enlace que se encuentra arriba de la tabla.

Configuración de acceso a SNMPv1/v2c

Dirección IP de acceso SNMP

Configurar hosts de red interesados en el acceso a la información del dispositivo. El host se puede identificar como una dirección IP o el nombre de red del host

Tipo de acceso SNMP

Tipo de acceso SNMPv1/v2C: solo lectura o lectura/escritura

Cadena de comunidad de acceso SNMP

Cadena que identifica un 'secreto' para permitir el acceso de solo lectura o solo escritura. El valor predeterminado es acceso de solo lectura: público (distingue entre mayúsculas y minúsculas). Acceso de solo escritura: privado (distingue entre mayúsculas y minúsculas).

6.5.4 Carpeta YDN23

El protocolo YDN23 admitido se basa en la especificación YD-T-1363 mediante una conexión de red RS-485.

Configuración del protocolo YDN23

Acceso de escritura del dispositivo administrado

Habilite o deshabilite el servidor YDN23 para escribir en el dispositivo administrado.

Dirección del dispositivo

Dirección del dispositivo YDN23

Tasa de baudios

La tasa de comunicaciones en bps.

6.6 Carpeta de estado

La carpeta Estado no contiene elementos configurables. Muestra el estado del sistema de la tarjeta Unity y una lista de eventos que afectan el estado de la tarjeta. El estado también se indica mediante los iconos junto a los elementos. Consulte Texto de ayuda en la página 23 para obtener una descripción de los iconos.

6.7 Carpeta de soporte

La carpeta Soporte permite reiniciar la tarjeta Unity, restablecer la tarjeta a sus valores predeterminados de fábrica y actualizar el firmware de la tarjeta. Agente se refiere a la tarjeta Unity.

La carpeta también muestra información sobre la tarjeta para ayudar en la resolución de problemas, como la versión de firmware de la tarjeta, la etiqueta, la dirección MAC e información relacionada.

Configuración de la carpeta de soporte

Fecha y hora del agente

Configuración de fecha y hora para la tarjeta.

Modelo de agente

El modelo de la tarjeta (Unity Platform)

Versión de firmware de la aplicación del agente

La versión de firmware de la tarjeta (2.0 o superior)

Etiqueta de firmware de la aplicación del agente

La etiqueta del firmware de la tarjeta

Versión de firmware de arranque del agente

La versión de firmware de arranque de la tarjeta

Etiqueta de firmware de arranque del agente

La etiqueta del firmware de arranque de la tarjeta

Número de serie del agente

El número de serie de la tarjeta.

Fecha de fabricación del agente

La fecha de fabricación de la tarjeta.

Versión de hardware del agente

La versión de hardware de la tarjeta

Versión GDD

La versión GDD de la tarjeta, actual cuando se instaló el firmware de la tarjeta; el GDD es un documento de referencia patentado para datos de dispositivos.

Versión FDM

La versión FDM de la tarjeta; el FDM es un documento de modelo de datos que define los datos admitidos por los dispositivos que utilizan el protocolo Velocity.

ID de secuencia del producto

El identificador de secuencia del producto de la tarjeta.

Comandos

Habilitar/Cancelar

Tarjeta de reinicio

Reinicie la tarjeta e implemente cambios de configuración

Restablecer la tarjeta a los valores predeterminados de fábrica

Restablecer la configuración de la tarjeta a sus valores predeterminados de fábrica

Generar y descargar archivo de diagnóstico

Genere un archivo que contenga información de diagnóstico y descárguelo con un navegador web.

6.7.1 Carpeta de red activa

Estado de la configuración de red IP actualmente activa para la tarjeta Unity junto con algunos valores anteriores para solucionar problemas de comunicación IP.

Parámetros de redes activas

Dirección MAC Ethernet

Dirección MAC de Ethernet para la tarjeta Liebert IntelliSlot

Dirección IPv4

Dirección de red IPv4 utilizada actualmente

Puerta de enlace predeterminada IPv4

Dirección de red IPv4 utilizada actualmente de la puerta de enlace para el tráfico de red destinado a otras redes o subredes

DNS primario

DNS primario IPv4 utilizado actualmente

DNS secundario

DNS secundario IPv4 utilizado actualmente

Última dirección DHCP/BOOTP

Última dirección IPv4 conocida asignada por DHCP

Última concesión de DHCP

Tiempo de concesión de la última dirección DHCP conocida

Dirección global IPv6

Muestra si DHCPv6 o dirección estática se está utilizando actualmente

Configuración automática de direcciones sin estado

IPv6 SLAAC se asigna automáticamente desde el anuncio del enrutador, si se establece el indicador "A", combinando el prefijo con EUI-64 MAC

Enlace local

Dirección local de enlace IPv6 utilizada actualmente

Puerta de enlace predeterminada IPv6

Dirección de red IPv6 utilizada actualmente de la puerta de enlace para el tráfico de red destinado a otras redes o subredes

Servidor DNS primario

DNS primario IPv6

Servidor DNS secundario

DNS secundario IPv6 utilizado actualmente

Último DHCPv6

Última dirección IPv6 conocida asignada por DHCPv6

Última concesión de DHCPv6

Tiempo de concesión de la última dirección DHCPv6 conocida

6.7.2 Carpeta de actualización de firmware

La tarjeta Unity tiene dos áreas en la memoria flash para el firmware y la configuración. Un área opera actualmente en la tarjeta. La otra área es el firmware anterior en la tarjeta y se considera una imagen alternativa.

La carpeta admite la actualización del firmware de la tarjeta Unity o la reversión a una versión anterior. Si el firmware no se ha actualizado, entonces la versión/configuración anterior no está disponible para revertir.

NOTA: Si se degrada el firmware a una versión anterior, se restablecerán los valores predeterminados de fábrica si hay características en la versión actual que no están presentes en la versión anterior. Sin embargo, si se degrada usando una imagen alternativa, no se reinicia.

Configuración de actualización de firmware

Versión actual del firmware

La versión del firmware que se ejecuta en la tarjeta

Etiqueta de firmware actual

La etiqueta del firmware que se ejecuta en la tarjeta

Fecha de firmware actual

La fecha de compilación del firmware que se ejecuta en la tarjeta

Versión de firmware alternativa

La versión del firmware alternativo (anterior)

Etiqueta de firmware alternativa

La etiqueta del firmware alternativo (anterior)

Fecha de firmware alternativa

La fecha de compilación del firmware alternativo (anterior)

Comandos de firmware

Ejecutar firmware alternativo

Regrese el firmware de la tarjeta a la versión alternativa (anterior).

Actualización de firmware

Actualice el firmware de la tarjeta a una versión nueva/diferente.

Actualización del firmware de la tarjeta

Para obtener una descripción del campo y las carpetas utilizadas al actualizar, consulte Carpeta de actualización de firmware en la página anterior.

Para actualizar el firmware en la tarjeta Unity:

1. En una computadora, descargue el último firmware de la tarjeta Unity desde https://www.vertivco.com/en-us/support/software-download/monitoring/liebert-intellislot-communications-interface-cards/.
   - Si conoce la dirección IP de la tarjeta, escríbala en un navegador web.
   - Si no conoce la dirección IP, conecte la tarjeta a una computadora con un cable Ethernet y abra un navegador web, consulte Conexión directa a la computadora para la configuración en la página 4.

     La tarjeta tiene un conector Ethernet RJ-45 en el frente, vea la Figura 1.1 en la página 1.
     Cuando se conectan directamente, la tarjeta y la computadora negocian automáticamente las comunicaciones, lo que demora aproximadamente 1 minuto. Cuando se establezca la comunicación, abra un navegador web e ingrese la dirección 169.254.24.7, que es la dirección IPv4 de configuración automática predeterminada de la tarjeta.

     Se abrirá la interfaz de usuario web de la tarjeta.
2. En la pestaña Comunicaciones, seleccione Soporte > Actualización de firmware en el menú de pestañas de la izquierda. panel.
3. Haga clic en Editar e ingrese el nombre de usuario y la contraseña del administrador.
4. Haga clic en Internet.

   Se abre la pantalla de actualización de firmware.
5. Busque el archivo de firmware que descargó en el paso 1 para actualizarlo, selecciónelo y haga clic en Actualizar Firmware.

NOTA: No salga de la pantalla Actualización de firmware y no cierre el navegador una vez que comience la actualización. Cualquiera de las dos acciones interrumpirá la descarga.

Volver al firmware alternativo (anterior)

Cuando se actualiza el firmware de una tarjeta, el firmware y la configuración anteriores se mueven al área alternativa. Puede restaurar la versión de firmware y la configuración que se guardan en el área alternativa.

1. En la pestaña Comunicaciones, seleccione Soporte > Actualización de firmware en el menú de pestañas de la izquierda.
   panel.
2. Haga clic en Editar e ingrese el nombre de usuario y la contraseña del administrador.
3. Haga clic en Ejecutar alternativa.
   Se abre un cuadro de diálogo de confirmación.
4. Haga clic en Aceptar.
   La tarjeta se reinicia. Después de reiniciar, la tarjeta ejecuta la versión anterior del firmware y la configuración. El firmware y la configuración reemplazados ahora se almacenan en el área alternativa.

6.7.3 Carpeta de exportación/importación de configuración

Los ajustes de configuración de Unity se pueden guardar en un disco local o una unidad USB importada，y los archivos guardados pueden ser para restaurar la configuración si la tarjeta se restablece/reemplaza y para transferir los ajustes a otra tarjeta.

Opciones de exportación/importación de configuración
Exportar archivo de configuración Guarda la configuración de la tarjeta Unity, que se puede editar y usar para importar configuraciones comunes a otras tarjetas Unity. Consulte Exportación y modificación de un archivo de configuración en la página 66 y Acerca del archivo de configuración exportado a continuación.
Importar archivo de configuración Carga la configuración de la tarjeta Unity contenida en un archivo de exportación modificado o un archivo creado. El archivo de importación generalmente se usa para implementar configuraciones de tarjetas comunes. Consulte Importación de un archivo de configuración en la página 67.

Acerca del archivo de configuración exportado

Un archivo de configuración exportado contiene todos los ajustes de configuración de la pestaña Comunicación de la tarjeta.
La configuración del dispositivo administrado, como UPS o sistema de administración térmica, no está incluida.

Consideraciones de Seguridad

Las contraseñas y otros secretos no se exportan. Los valores protegidos se muestran como asteriscos y las líneas están comentadas. Para usar el archivo como un archivo de respaldo completo e importable, debe reemplazar los asteriscos (*) con su contraseña/valores secretos y descomentar las líneas. También puede hacer referencia al encabezado del archivo de exportación para obtener detalles adicionales.

NOTA: No importe un archivo de exportación no modificado de una tarjeta a otra. Esto podría causar una dirección IP duplicada u otras duplicaciones no deseadas.

NOTA: Si agrega datos confidenciales, como contraseñas, al archivo, le recomendamos que use una conexión HTTPS al importar para asegurarse de que el archivo esté encriptado cuando se transmita.

Formato general

El archivo exportado es autodescriptivo usando líneas comentadas e incluye las siguientes designaciones de formato:

- # precede a los comentarios.
- Los ajustes y sus valores no se comentan. • Dos puntos (:) separan la configuración y el valor. • Las comillas dobles (") encierran todos los valores basados en texto • Los valores numéricos y enumerados no están entre comillas dobles • Los corchetes ([ ]) indican la carpeta que contiene la configuración • La contraseña de usuario y otros secretos están ocultos en el archivo de exportación y la línea se comenta para evitar la importación accidental. Para importar una nueva contraseña u otro secreto, elimine el comentario de la línea e ingrese la nueva contraseña. Debido a que se trata de una cadena de texto, debe estar entre comillas dobles (").

Figura 5.4 Ejemplos de formato de archivo (las líneas de ejemplo están en negrita)

Text

```
[System]
# System Name
# End user assigned name for the
system
# maximum length: 64
System Name: "GXT4"
# Contact Information
# End user assigned contact
information for the system
# maximum length: 50
Contact Information: "IT Manager"
```

Enumerated

```
[Time Service]
# External Time Source
# The external source to use for
time synchronization.
# 0: NTP Server
# 1: Modbus System
# 2: BACnet System
# 3: Velocity Management System
# 4: LIFE (TM) Watch Station
# 5: YDN23 System
# 6: Remote Services System
External Time Source: 0
```

Numeric

```
# Timeout
# The timeout for an
   authentication query to be
   answered.
# range: 0 to 65535 sec
Timeout: 3
# Retries
# The number of times a RADIUS
   server is tried   before another
   is contacted.
# range: 0 to 65535
Retries: 2
```

Secure

```
[Local User.1]
# User Name
# Case sensitive string containing
   printable ASCII characters
   excluding: \:'<>~?#, double
   quote, and space
# maximum length: 30
# minimum length if not blank*: 1
# *This setting can be cleared with
   a blank string.
User Name: "Liebert"
# User Password
# Case sensitive string containing
   printable ASCII characters
   excluding: \:'<>~?#, double
   quote, and space
# maximum length: 30
# minimum length if not blank*: 1
# *This setting can be cleared with
   a blank string.
# ** Protected value not displayed.
   Uncomment following line to
   import new value:
# User Password: "********"
# Authorization for User
# User access privilege level - No
   Access, General User,
   Administrator
```

Exportación y modificación de un archivo de configuración

El archivo exportado tiene formato de texto (.txt) guardado en la carpeta predeterminada creada por el navegador web, que suele ser la carpeta "Descargas" en los dispositivos de Microsoft Windows. El archivo se nombra con el prefijo "config_" seguido de la dirección MAC, el año, el mes, el día y la hora. Esto se incluye para que el archivo sea identificable de forma única. Consulte Acerca del archivo de configuración exportado en la página 64 para obtener detalles de seguridad y formato.

1. En la pestaña Comunicaciones, seleccione Soporte > Exportación/Importación de configuración.
2. Haga clic en Habilitar e ingrese un nombre de usuario y una contraseña.

3. Haga clic en Exportar.

   El archivo .txt se guarda en la carpeta de descarga predeterminada del navegador web.

4. Para preparar el archivo para importarlo: • Guarde el

   archivo en una computadora o carpeta de red. • Abra el archivo en un

   editor de texto y elimine el comentario de la línea que contiene la contraseña o los datos secretos.
   (eliminar #).

   • Elimine los asteriscos (*****) y reemplácelos con la contraseña/valor secreto entre comillas dobles
   (").

   • Un archivo importado solo necesita contener los datos para agregar o actualizar, y no requiere comentarios. Eliminar (eliminar)
   el contenido que no se necesita.

   • Guarde el archivo editado.

Importación de un archivo de configuración

Un archivo de configuración importado generalmente se usa para hacer una copia de seguridad de la configuración de una tarjeta o para configurar muchas tarjetas con una configuración común.

Si el archivo de exportación se utilizará como copia de seguridad, todas las contraseñas y secretos deben restaurarse manualmente.

NOTA: No importe un archivo no modificado. Esto podría causar una dirección IP duplicada u otras duplicaciones no deseadas.

Además, el archivo de importación no requiere comentarios y solo necesita la fecha para actualizarse. Por ejemplo, puede cambiar solo el nombre del sistema o una dirección de red editando el archivo de configuración para que contenga solo esas líneas.

Para importar un archivo de configuración:

1. En la pestaña Comunicaciones, seleccione Soporte > Exportación/Importación de configuración.
2. Haga clic en Habilitar e ingrese un nombre de usuario y una contraseña.
3. Haga clic en Importar y siga las instrucciones del cuadro de diálogo de importación.

6.7.4 Reinicio manual de la tarjeta

1. Localice el pequeño orificio en la parte frontal de la tarjeta que contiene el botón de reinicio, consulte la Figura 1.1 en
   Página 1.
2. Inserte una herramienta recta no conductora en el orificio pequeño y mantenga presionada durante 5 segundos.
   La tarjeta se reinicia sin restablecerla a los valores predeterminados de fábrica. Para restablecer los valores predeterminados de fábrica, consulte
   Restablecimiento manual de los valores predeterminados de fábrica a continuación.

6.7.5 Restablecimiento manual de los valores predeterminados de fábrica

1. Localice el pequeño orificio en la parte frontal de la tarjeta que contiene el botón de reinicio, consulte la Figura 1.1 en
   Página 1.
2. Inserte una herramienta recta no conductora en el orificio pequeño y presione 5 veces. Cada pulsación debe
   ser de 1 a 2 segundos de duración y debe completarse en 10 segundos.
   La tarjeta se restablece a la configuración predeterminada de fábrica.

PRECAUCIÓN: No presione y mantenga presionado el botón durante demasiado tiempo. Si se mantiene presionado durante 5 segundos, se reinicia la tarjeta sin restablecer los valores predeterminados de fábrica.

Esta página se dejó en blanco intencionalmente

VertivCo.com | Sede de Vertiv, 1050 Dearborn Drive, Columbus, OH, 43085, EE. UU.

SL-52645_REV11/590-1305-501E