Control iD

GUÍA DE FORTALECIMIENTO DE SEGURIDAD

Control iD

GUÍA DE FORTALECIMIENTO DE SEGURIDAD

Aviso legal

Este manual se proporciona tal cual, y la información contenida en él está sujeta a cambios sin previo aviso. Las imágenes en este manual son solo para fines ilustrativos.

Revisión	Fecha	Cambios	Autor
1.0	2025-05-27	Revisión inicial	André Curvello

Control iD

GUÍA DE FORTALECIMIENTO DE SEGURIDAD

Introducción

Los iDFace e iDFace Max son controladores de acceso con autenticación facial de última generación desarrollados por Control iD. Cuentan con conectividad Ethernet, lo que permite su integración mediante la REST HTTP API públicamente documentada de Control iD.

Dado que los dispositivos pueden conectarse a una red, se deben tomar varias precauciones para garantizar un funcionamiento óptimo y seguro. Esta guía está destinada a administradores de TI y oficiales de seguridad responsables por la implantación y gestión de dispositivos iDFace en entornos de red seguros.

Este manual proporciona una referencia para el fortalecimiento de la seguridad de iDFace dentro de las infraestructuras organizacionales.

Control iD

GUÍA DE FORTALECIMIENTO DE SEGURIDAD

Resumen

Control iD

GUÍA DE FORTALECIMIENTO DE SEGURIDAD

Actualización de Contraseña y Usuario para Web

Cambiar el nombre de usuario y la contraseña predeterminados para el acceso web es obligatorio al iniciar sesión por primera vez o después de un restablecimiento de fábrica.
Incluso si el administrador decide mantener el nombre de usuario **admin**, debe configurarse una contraseña fuerte.

Requisitos de la contraseña:

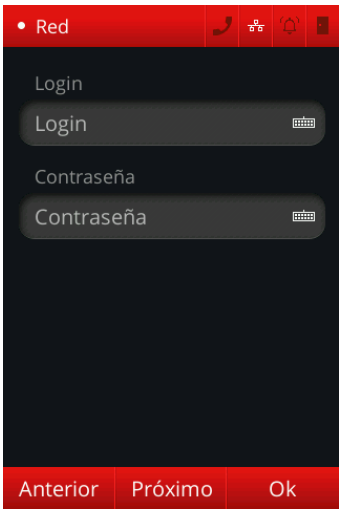
- Mínimo **12 caracteres**.
- Debe incluir números, letras mayúsculas y minúsculas, y símbolos especiales (por ejemplo, !, #, %).
- Evitar palabras del diccionario, información personal, repeticiones o secuencias numéricas.

Procedimiento:

1. Navegar a: Menú > Configuración > Configuración General > Interfaz Web

2. Editar el nombre de usuario y la contraseña según las instrucciones

3. Hacer clic en “Ok” para guardar los cambios y persistir la configuración. Después de esto, la interfaz web y la API solo funcionarán con las nuevas credenciales.



Control iD

GUÍA DE FORTALECIMIENTO DE SEGURIDAD

Preferencia de HTTPS sobre HTTP

Para una comunicación segura entre los dispositivos de control de acceso y los sistemas de gestión de software, se debe utilizar HTTPS en lugar de HTTP.

- Las comunicaciones HTTP pueden ser interceptadas.
- HTTPS garantiza el cifrado mediante SSL/TLS.

Los dispositivos Control iD soportan HTTPS utilizando:

- Un certificado autofirmado generado por la terminal.

- Un certificado proporcionado por el integrador.

Procedimiento:

1. Navegar a: Menú > Configuración > Red > Propiedades de Red > Siguiente (hasta la última pantalla).

2. Activar el interruptor SSL.

3. Seleccionar Certificado Autofirmado o subir un certificado confiable.

4. Hacer clic en “Ok” para guardar los cambios.

El dispositivo ahora funcionará de manera segura a través del puerto 443.

Control iD

GUÍA DE FORTALECIMIENTO DE SEGURIDAD

Habilitar/Deshabilitar Interfaz Web

SSH permite diagnósticos y soporte remoto, pero representa riesgos si las credenciales son comprometidas.

1. SSH está deshabilitado de forma predeterminada.

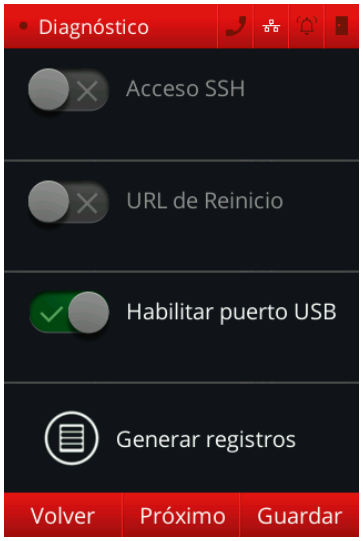
2. Solo habilítelo si es estrictamente necesario.

Procedimiento:

1. Navegar a: Menú > Configuración > Configuración General > Sistema > Diagnóstico.

2. Activar o desactivar el interruptor de Acceso SSH.

3. Guardar los cambios.



Control iD

GUÍA DE FORTALECIMIENTO DE SEGURIDAD

Habilitar/Deshabilitar Interfaz Web

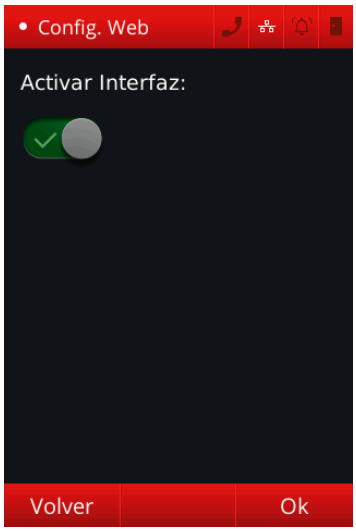
La Interfaz Web ofrece comodidad para gestionar los dispositivos de control de acceso. Control iD proporciona la funcionalidad para habilitarla o deshabilitarla según sea necesario. Cuando se utiliza exclusivamente la API (por ejemplo, integrada con un software OEM, etc.), se recomienda desactivar la interfaz web.

Procedimiento:

1. Navegar a: Menú > Configuración > Configuración General > Interfaz Web > Siguiente.

2. Activar o desactivar el interruptor de la Interfaz Web.

3. Hacer clic en “Ok” para guardar los cambios.



Control iD

GUÍA DE FORTALECIMIENTO DE SEGURIDAD

Registros de Auditoría

Revisar periódicamente los registros de auditoría es fundamental para mantener la seguridad de los dispositivos de control de acceso. Estos registros proporcionan información detallada sobre los cambios de configuración del terminal.

Recomendaciones:

- Habilitar el registro detallado de configuraciones e interacciones del dispositivo.
- Revisar periódicamente los registros en busca de anomalías.
- Exportar los registros a un almacenamiento externo o a un servidor SIEM centralizado.
- Sincronizar la hora del dispositivo con un servidor NTP para garantizar marcas de tiempo precisas en los registros.

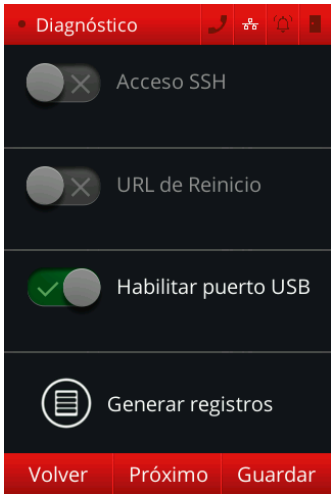
Procedimiento de exportación:

1. Navegue a: **Menú > Configuración > Configuración general > Sistema > Diagnóstico**.

2. Seleccione **Generar registros > Registros de auditoría**.

3. Inserte una memoria USB con formato **FAT32** o configure la exportación remota.

4. Haga clic en **Generar registros** para exportar los registros de auditoría con todas las opciones marcadas (por defecto).



Control iD

GUÍA DE FORTALECIMIENTO DE SEGURIDAD

Gestión de Actualizaciones de Firmware

Mantener el firmware del dispositivo actualizado es vital para abordar posibles vulnerabilidades y garantizar mejorías continuas en la seguridad.

Buenas prácticas:

- Verificar periódicamente la disponibilidad de actualizaciones.
- Aplicar las actualizaciones durante ventanas de mantenimiento para minimizar interrupciones operativas.
- Documentar el historial de actualizaciones con fines de auditoría.

GUÍA DE FORTALECIMIENTO DE SEGURIDAD

Fortalecimiento Adicional de Servicios

Además de deshabilitar el acceso SSH y la Interfaz Web, se recomienda habilitar únicamente los servicios de red necesarios para minimizar la superficie de ataque del dispositivo.

Acciones:

- Identificar y deshabilitar (si están habilitados) los protocolos no utilizados, como RTSP, ONVIF o SIP, según los requisitos de la instalación.

- Revisar regularmente los servicios activos del dispositivo y asegurarse de que solo estén habilitados aquellos esenciales para la operación.

- Utilizar segmentación de red y reglas de firewall para restringir el acceso externo únicamente a los servicios requeridos.

- Monitorear los servicios expuestos en busca de posibles vulnerabilidades o configuraciones incorrectas.

- Tener en cuenta el impacto funcional antes de deshabilitar un protocolo (por ejemplo, ONVIF es necesario para la integración con VMS).

Control iD

GUÍA DE FORTALECIMIENTO DE SEGURIDAD

Puertos de Red Disponibles y sus Funciones

Recurso	Status	Puerto	Descripción	Recomendación
HTTP	Habilitado	80	Interfaz Web (no cifrada)	Deshabilitar, usar solo HTTPS
HTTPS/SSL	Deshabilitado	443	Interfaz Web Segura	Habilitar si se requiere acceso web
RTSP	Deshabilitado	554	Transmisión de audio y video en tiempo real	Habilitar solo si es necesario
ONVIF	Deshabilitado	8000	Interoperabilidad de vigilancia de video	Habilitar solo si es necesario
SIP	Deshabilitado	5060	Señalización VoIP	Habilitar solo si es necesario
SNMP	Deshabilitado	161/162	Monitoreo del dispositivo	Habilitar solo si es necesario
SSH	Deshabilitado	22	Acceso remoto seguro	Habilitar solo si es necesario
OpenVPN	Deshabilitado	1194/UDP (default)	Protocolo de túnel VPN	Habilitar solo si se requiere conectividad VPN

Recurso	Status	Puerto	Descripción	Recomendación
NTP	Deshabilitado	123	Sincronización de tiempo en red	Habilitar para registros precisos
DNS	Deshabilitado	53	Resolución de nombres de dominio	Habilitar si se requiere resolución de nombres de host
DHCP	Deshabilitado	67/68	Configuración automática de IP	Habilitar si se requiere DHCP

Control iD

GUÍA DE FORTALECIMIENTO DE SEGURIDAD

Referencias y Cumplimiento

Esta guía se alinea con estándares y buenas prácticas reconocidas internacionalmente, incluyendo:

- **NIST SP 800-63B** – Directrices de Identidad Digital (autenticación, políticas de contraseñas)

- **ISO/IEC 27001** – Sistemas de Gestión de Seguridad de la Información

- **EN 18031-1 / 18031-2 (RED-DA)** – Marco europeo de cumplimiento de seguridad