Control iD

# SECURITY HARDENING GUIDE

Control iD

# SECURITY HARDENING GUIDE

## Disclaimer

This manual is provided as is, and the information contained herein is subject to change without notice. The images in this manual are for illustrative purposes only.



| Revision | Data | Changes | Author |
|---|---|---|---|
| 1.0 | 2025-05-27 | Initial revision | André Curvello |

Control iD

# SECURITY HARDENING GUIDE

## Introduction

iDFace and iDFace Max are state-of-the-art facial authentication access controllers developed by Control iD. They feature Ethernet connectivity, enabling integration through Control iD's publicly documented HTTP REST API.

As the devices can be connected to a network, several precautions must be taken to ensure optimal and secure operation. This guide is intended for IT administrators and security officers responsible for deploying and managing iDFace devices in secure network environments.

This manual provides a reference for hardening the security of iDFace within organizational infrastructures.

Control iD

# SECURITY HARDENING GUIDE

## Summary

Control iD

# SECURITY HARDENING GUIDE

## Password and User Update for Web Access

Changing the default username and password for web access is mandatory upon first login or after a factory reset.

Even if the administrator decides to keep the username admin, a strong password must be configured.

**Password requirements:**

- Minimum of **12 characters**.

- Must include numbers, uppercase and lowercase letters, and special symbols (e.g., !, #, %).

- Avoid dictionary words, personal information, repetitions, or numeric sequences.

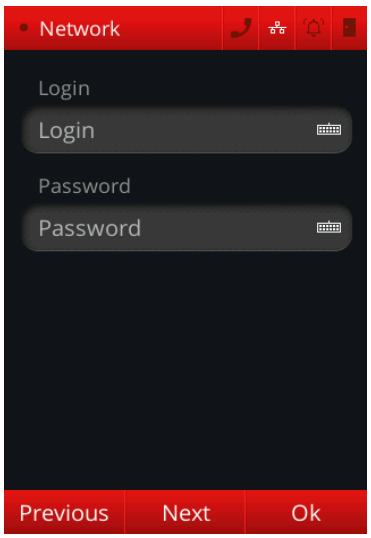
**Procedure:**

1. Navigate to: Menu > Settings > General Settings > Web Interface.

2. Edit the login and password as instructed.

3. Click “Ok” to save changes to persist configuration.

After this, the Web interface and API will only function with the new credentials.



Control iD

# SECURITY HARDENING GUIDE

## Preference for HTTPS over HTTP

For secure communication between access control devices and software head-end systems, HTTPS must be used instead of HTTP.

- **HTTP** communications can be intercepted.
- **HTTPS** ensures encryption via SSL/TLS.

Control iD devices support HTTPS using either:

- A self-signed certificate generated by the terminal.

- A certificate provided by the integrator.

**Procedure:**

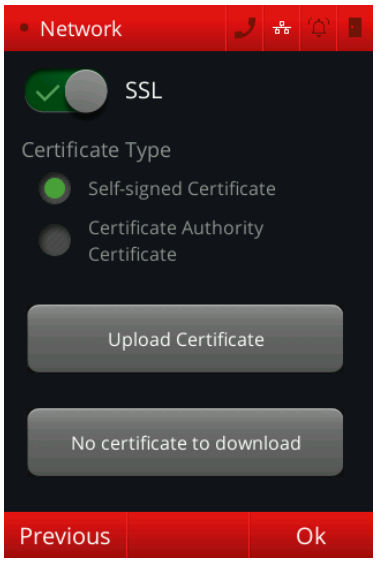
1. Navigate to: Menu > Settings > Network > Network Properties > Next (until last screen).

2. Enable the SSL switch.

3. Select **Self-signed Certificate** or upload a trusted certificate.

4. Click “Ok” to save changes.

The device will now operate securely over port 443.



Control iD

# SECURITY HARDENING GUIDE

## Enabling/Disabling SSH Access

SSH allows remote diagnostics and support, but poses risks if credentials are compromised.

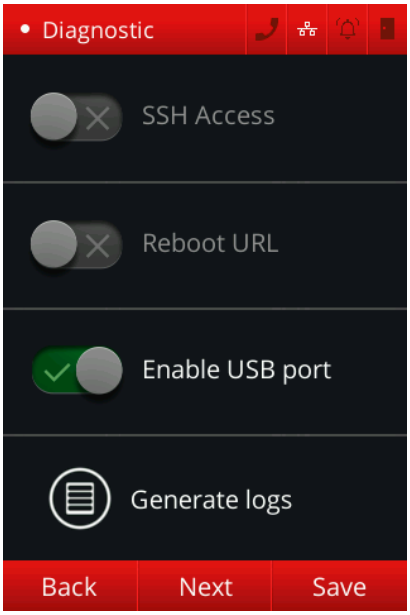
1. SSH is **disabled by default**.
2. Only enable if strictly necessary.

**Procedure:**

1. Navigate to: Menu > Settings > General Settings > System > Diagnostic.

2. Toggle the **SSH Access** switch.

3. Save changes.



Control iD

# SECURITY HARDENING GUIDE

## Enabling/Disabling WEB Interface

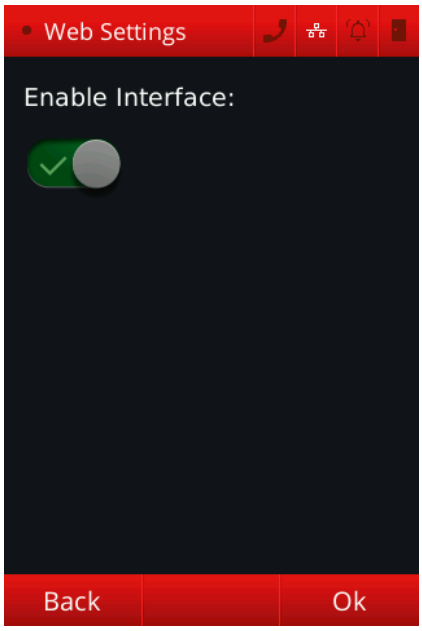
The Web Interface offers convenience for managing access control devices. Control iD provides functionality to enable or disable it as needed. When using the API exclusively (i.e. integrated with a software OEM etc.), we recommend that the web interface be disabled.

**Procedure:**

1. Navigate to: Menu > Settings > General Settings > Web Interface > Next.

2. Toggle the Web Interface switch.

3. Click “Ok” to save changes.



Control iD

# SECURITY HARDENING GUIDE

## Audit Logs

Regularly reviewing audit logs is crucial for maintaining the security of access control devices. These logs provide detailed records of configuration changes of the terminal.

**Recommendations:**

- Enable detailed logging for configuration and device interactions.

- Periodically review logs for anomalies.

- Export logs to external storage or a centralized SIEM server.

- Synchronize device time with NTP to ensure accurate log timestamps.

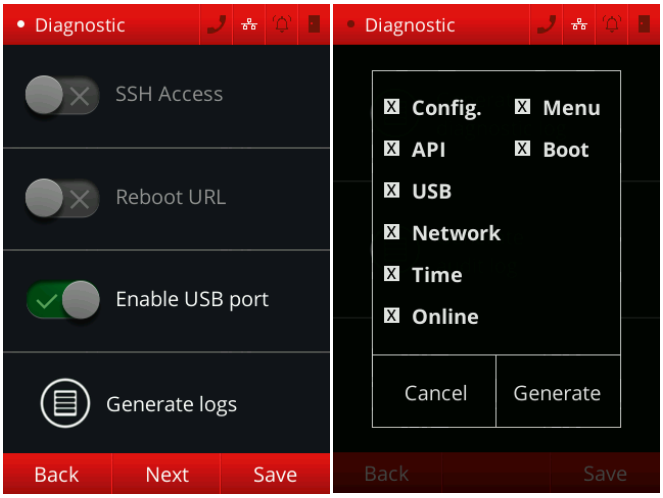
**Export procedure:**

1. Navigate to: Menu > Settings > General Settings > System > Diagnostic.

2. Select **Generate Logs > Audit Logs**.

3. Insert a FAT32 USB stick or configure remote export.

4. Click Generate, to export Audit logs with all options marked (by default).



Control iD

# SECURITY HARDENING GUIDE

## Firmware Updates Management

Keeping device firmware up to date is vital for addressing possible vulnerabilities and ensuring continuous security improvements.

**Best practices:**

- Periodically verify available updates.

- Apply updates during maintenance windows to minimize operational disruptions.

- Document update history for audit purposes.

Control iD

# SECURITY HARDENING GUIDE

## Additional Service Hardening

Other than disabling SSH and Web Interface access, it is advisable to only enable required network services to minimize the device's attack surface.

**Actions:**

- Identify and disable (if they are enabled) any unused protocols such as RTSP, ONVIF, or SIP, depending on deployment requirements.

- Regularly review the device's active services and ensure only those essential for operations are enabled.

- Utilize network segmentation and firewall rules to restrict external access to required services only.

- Monitor exposed services for potential vulnerabilities or misconfigurations.

- Be aware of functional impact before disabling a protocol (e.g., ONVIF required for VMS integration).

Control iD

# SECURITY HARDENING GUIDE

## Available Network Ports and their Features

### Inbound Ports

| Resource | Default Status | Port | Description | Recommendation |
|---|---|---|---|---|
| HTTP | Enabled | 80 | Web Interface (unencrypted) | Disable, use HTTPS only |
| HTTPS/SSL | Disabled | 443 | Secure Web Interface | Enable if web access is required |
| RTSP | Disabled | 554 | Real-time audio and video streaming | Enable only if needed |
| ONVIF | Disabled | 8000 | Video surveillance interoperability | Enable only if needed |
| SIP | Disabled | 5060 | VoIP signaling | Enable only if needed |
| SNMP | Disabled | 161/162 | Device monitoring | Enable only if needed |
| SSH | Disabled | 22 | Secure remote access | Enable only if needed |
| OpenVPN | Disabled | 1194/UDP (default) | VPN tunneling protocol | Enable only if VPN connectivity is required |

### Outbound Ports

| Resource | Default Status | Port | Description | Recommendation |
|---|---|---|---|---|
| NTP | Disabled | 123 | Network time synchronization | Enable for accurate logs |
| DNS | Disabled | 53 | Domain name resolution | Enable if hostname resolution required |
| DHCP | Disabled | 67/68 | Automatic IP configuration | Enable if DHCP required |

Control iD

# SECURITY HARDENING GUIDE

## References and Compliance

This guide aligns with internationally recognized standards and best practices, including:

- **NIST SP 800-63B** – Digital Identity Guidelines (authentication, password policies)

- **ISO/IEC 27001** – Information Security Management Systems

- **EN 18031-1 / 18031-2 (RED-DA)** – European security compliance framework