inception

WEB POWERED SECURITY

Simple & Easy Installation

Integrated Security - Access Control

Inception Cybersecurity Hardening Guide

Overview

This document highlights several ways to help harden your Inception system against todays cyber security threats. No system will be perfectly secure, these suggestions can help to make a system much harder to penetrate. Many aspects of this guide focus on improving the security of user access into the web portal, both locally and via the internet.

The Inception system's security is largely dependent on the security of the network it is connected to. The services of a network professional should be considered to ensure the implementation and maintenance of security within a site's network.

User Options

Users logging in to Inception's web interface for administration and system control is one of the greatest concerns for cybersecurity. Accessing the system locally or remotely via SkyTunnel offers great convenience but care should be taken to ensure the security of the system.

Too many failed login attempts cause the system to automatically lock out for a period of time which helps prevent brute force attacks. But more steps can be taken to help increase the security of the system.

Installer User Account

The Installer user is created by default with default credentials. Changing that user's password and PIN is important, but it is recommended that the username is also changed.

User Access

Access to the web interface should only be given to users who require it. Similarly, users who can access the web interface should have Web Page Profiles that are limited to only what they require access to. This way if someone's account does get compromised, the sections that can be accessed are limited.

Strong passwords and long PINs should be chosen for users. Minimum PIN lengths can be configured in the System Settings.

If an administrator only rarely requires higher level permissions, consider creating a second account so that if their regular day-to-day account is compromised, the higher level sections remain protected.

November 2020

2FA Access

Users who can access the web interface should have 2FA configured. While important for local access, it is even more so if remote access (via SkyTunnel or otherwise) is enabled. This adds an additional layer of protection if a user's username and password or PIN are compromised. 2FA can be enforced for all web users via their Web Page Profile, ensuring users created in future also must use 2FA for web logins.

See the Inception Tech Guide on 2FA available from the Inner Range website for more information.

Local Network Security

A guide that covers securing a site's network is beyond the scope of this document. The services of a network professional should be considered for this purpose.

As Inception's web interface can be accessed via a site's local network, restricting access to the Inception system to only those who require it via networking rules can improve security. Utilizing VPN, Network Segmentation or other similar techniques can ensure the Inception system can only be accessed by specific devices on the customer network.

At the time of writing, Inception supports only HTTP access locally.

Remote Web Interface Access

While disabling remote access over the internet would increase security, being able to access the Inception's web interface from internet connected devices is a great convenience feature.

Manual Configuration

This could be achieved manually via port forwarding, network and router configuration, and care must be taken to ensure this option is configured securely. Utilizing certificates and HTTPS would be considered a minimum for this option. Utilizing dynamic DNS services and other similar services should be avoided.

A network professional should be consulted if using this option.

VPN Connection

A VPN connection to the customer's network can allow remote connection to the Inception's interface but only to authenticated devices.

Inner Range SkyTunnel Sevice

Alternatively, Inner Range's cloud service SkyTunnel provides a secure connection without the additional network configuration. Inception establishes an outbound TCP connection to the SkyTunnel cloud and utilizes AES encryption to ensure secure communications. A browser can then securely access the web interface via a HTTPS connection to SkyTunnel.

If Inception can access the internet, it will attempt to establish this connection by default. If remote access is not required (including use of the SkyCommand App), SkyTunnel Web Access can be disabled in the Network Settings page of the Inception system.

Note: Other Inner Range services like the SkyCommand App require the Inception be connected via SkyTunnel.

When placing Inception behind a firewall (a recommended suggestion), see the SkyTunnel Connectivity Guide for information on which ports and addresses Inception requires to access SkyTunnel.

Firmware Updates

Regular updating of the Inception controller firmware and its supporting modules is recommended. In addition to new and updated features, Inception firmware also contains updates to the operating system and other components that are used internally. This includes any fixes to known vulnerabilities or exploits that may be discovered in those systems.

November 2020