inception

WEB POWERED SECURITY

Simple & Easy Installation

Integrated Security - Access Control

HTTPS Configuration

Overview

This technical note explains how to configure the HTTPS options of the Inner Range Inception controller to allow secure web access.

Introduction

Inception supports local HTTPS access by default when using Inception firmware version 5.0 and higher. Previous versions of Inception allowed secure HTTPS browsing, both remotely and locally via SkyTunnel (https://www.skytunnel.com.au/inception/[InceptionSerialNumber]), but this update supports HTTPS for local network access as well. Using HTTPS instead of plain HTTP to access the Inception web interface ensures that your web traffic is encrypted and sensitive information (e.g. passwords, PINS) cannot be intercepted by third parties monitoring the connection.

By default, Inception comes loaded with an automatically generated self-signed SSL certificate to allow secure browsing, but it is also possible to upload a custom SSL certificate instead, as well as redirecting plain HTTP requests to HTTPS for a higher degree of security.

Accessing the web interface with HTTPS

HTTPS web access is enabled by default with Inception firmware 5.0, no additional configuration is required to turn it on. To access the Inception web interface with an encrypted HTTPS connection, simply navigate to https://[InceptionSerialNumber].local/ in a web browser (where [InceptionSerialNumber] is replaced with your controller's serial number). For example, if your controller's serial number is IN00001234, the URL would be https://in00001234.local/. **NOTE:** If using Windows, you may need to install Bonjour in order for your browser to be able to resolve .local domain names. Alternatively, you can use the Inception's IP address.

Redirecting HTTP requests to HTTPS

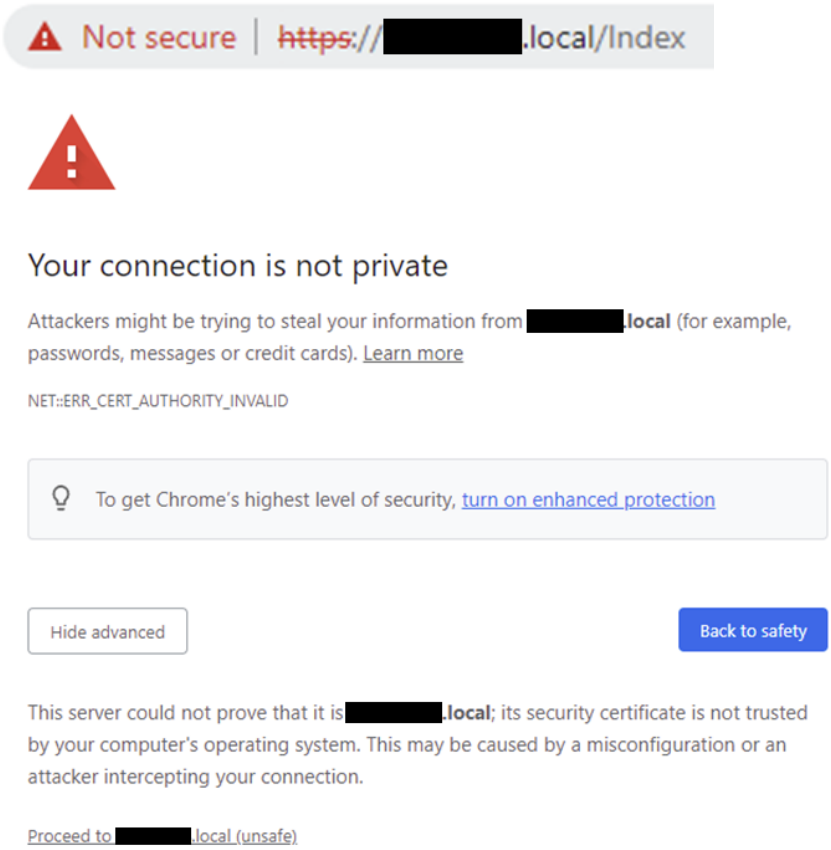
You can also choose to redirect HTTP web access to HTTPS by ticking the "Redirect HTTP to HTTPS" checkbox in the Advanced section on the **[Configuration > General > Network]** page. This option provides a greater degree of security by enforcing HTTPS for all web requests made to the controller. This setting also affects the Inception REST API, so any integrations targeting the API should be configured with the HTTPS URL to ensure they continue to work.

You may see a browser safety warning when accessing the Inception via local HTTPS.

June 2022

Removing the browser safety warning

When accessing the web interface with HTTPS, you may see a safety warning message in your browser, this is due to Inception's self-signed certificate not being trusted by your browser by default. If you choose to proceed anyway, the connection will still be encrypted, however the browser will continue to warn you that the connection is "Not Secure" which can result in a poor user experience.



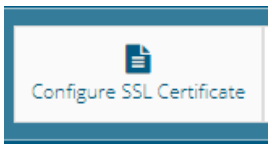
This warning can be removed by either adding the self-signed Inception SSL certificate to your browser's trusted certificate store (method varies depending on browser and operating system) or providing your own trusted certificate to upload to the Inception controller. Importing the self-signed certificate on your local machine is the simplest solution, and requires the use of https://[InceptionSerialNumber].local/ to access your Inception, but for larger networks it is recommended to set the Inception up with a custom SSL certificate signed by a trusted authority.

In order to properly remove this warning, the Inception must be assigned a proper hostname on the domain and a proper SSL certificate signed by a trusted certificate authority (either public or private) must be uploaded to the controller. Network configuration steps will vary depending on your organisation, so contact your IT department or network administrator if you require assistance with this.

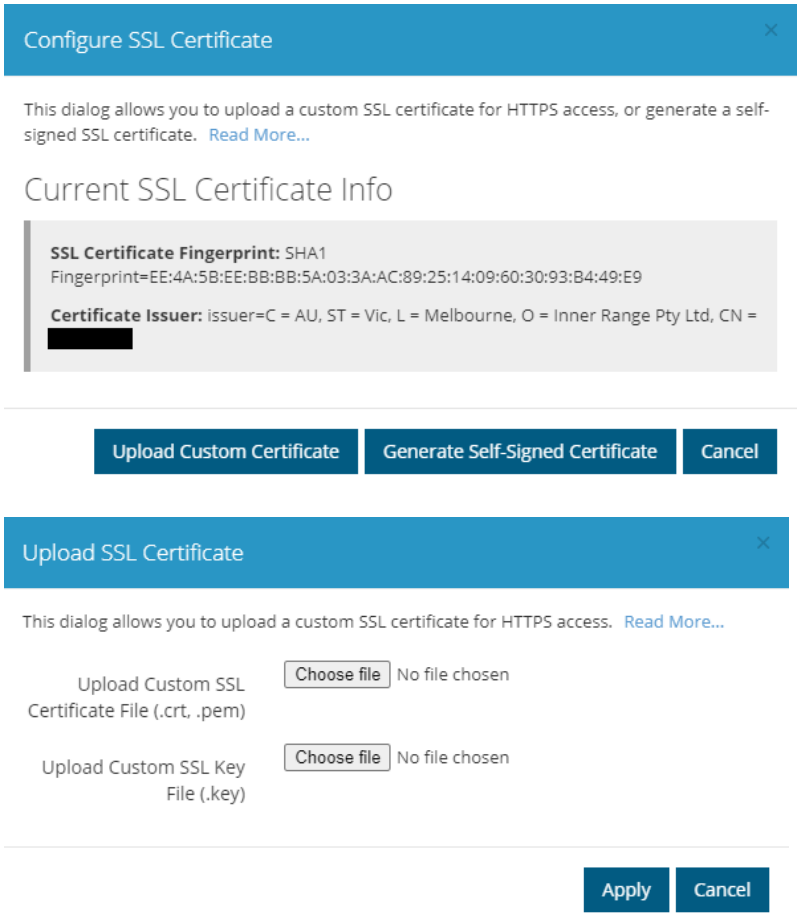
Uploading a custom SSL certificate

To upload a custom SSL certificate to the Inception controller, you will need 2 separate files: the certificate file (which usually has a .crt or .pem extension) and the private key file (usually .key). Both files should be in the PEM format, if your certificate is in a different format, it must be converted to PEM first with an external utility such as OpenSSL.

In the Inception web interface, go to the **[Configuration > General > Network]** page, and click the Configure HTTP/HTTPS button in the top-right toolbar.



A dialog will pop up allowing you to select the certificate and key files to upload. Select the certificate and key files from your filesystem and click Apply to begin uploading the certificate. **NOTE:** In rare cases of HTTPS misconfiguration, users can be locked out from being able to access the web interface, so it is recommended to perform a database backup before making any changes to the HTTPS configuration.



Once the upload completes and the certificate is applied, you will be prompted to refresh your browser after a short period of time. After refreshing the page, the new SSL certificate should be applied to the Inception controller.

Generating a new self-signed certificate

If you want to replace a previously uploaded certificate or one that is due to expire soon, you can choose to generate a new self-signed certificate from the **[Configuration > General > Network]** page. Click the Configure SSL Certificate button in the top-right toolbar to bring up the configuration dialog and click the “Generate Self-Signed Certificate” button. Accept the prompt and the controller will generate a new certificate and prompt you to refresh the page in the browser. The new certificate should now be applied to the controller.