Deep Secure GX integration with iboss Secure Cloud Gateway

April 2020

Table of Contents

1 Introduction

1.1 Scope

This document outlines how to integrate an iboss Secure Cloud Gateway (SCG) with Deep Secure's Gateway extension (GX) appliance.

GX provides a bi-directional guarding capability for ICAP(S) and HTTP(S), as discussed in the *GX Configuration Guide.*

This document details the configuration steps needed for the iboss Secure Cloud Gateway to send data to, and receive data from, GX.

1.2 Background

A typical deployment is as shown below.

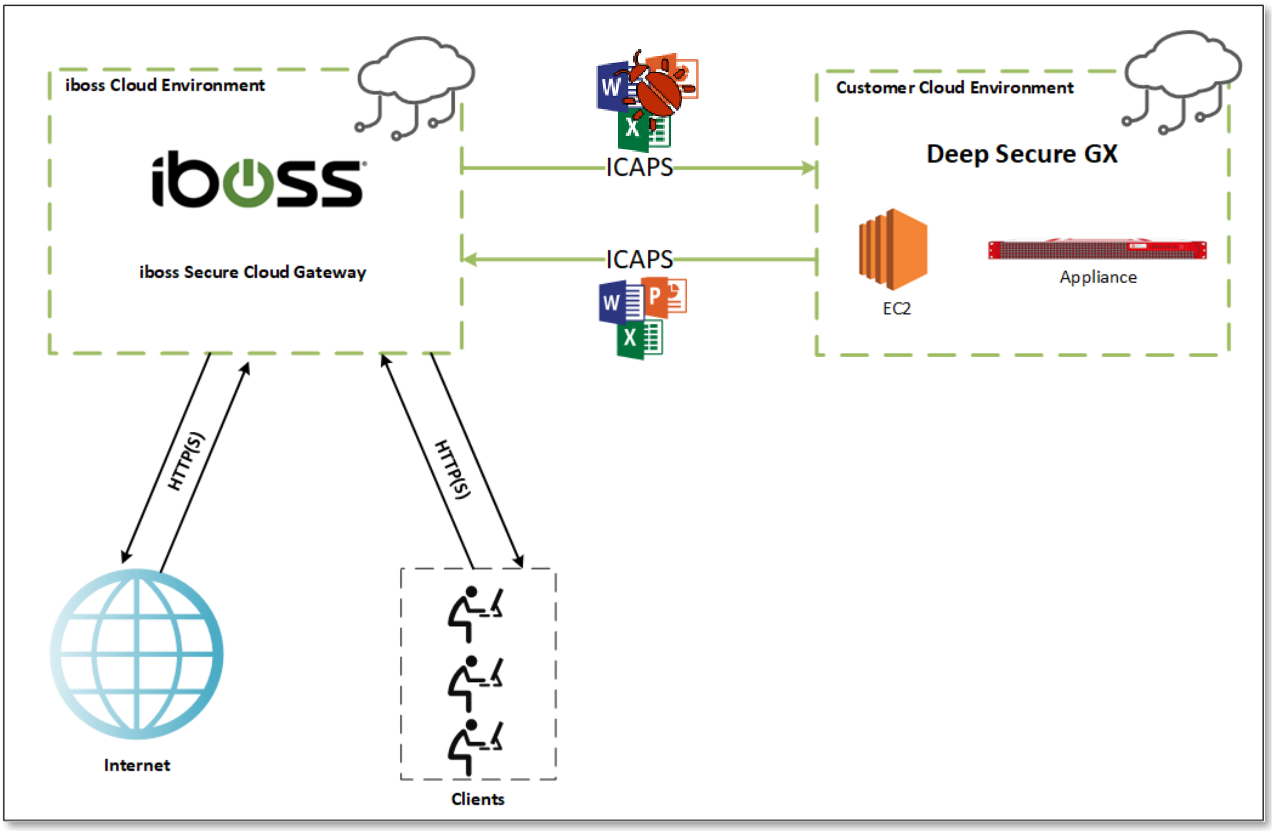


Figure 1.1: GX and iboss deployment

1.3 Audience

This guide is for Deep Secure GX system administrators, who are assumed to have a full understanding of network topology and routing.

1.4 Conventions

This guide uses the conventions shown in Table 1-1:

Convention	Indicates
Emphasis	Terms in a definition list or emphasis for important introductory words in a paragraph.
`Options`	Menu names, options, buttons, keys and other items from the user interface or the keyboard.
Italics	Cross-reference to related information in another document.
<variable>	A value you must supply, for example in a command line.
[<variable>]	An optional value you can supply, for example, in a command line.
✖	**Important information that emphasises or supplements points in the text, or that may apply only in special cases.**
⚠	**A caution that alerts you that failure to take or avoid a specified action could result in the loss of data.**
Tip	**A tip that suggests an alternative method for applying a technique or procedure or helps you to understand the benefits and capability of the product.**

Table 1-1: Conventions in this document

1.5 Purpose

This guide takes you through the steps you need to follow to integrate iboss Secure Cloud Gateway with a GX appliance.

Network traffic should flow, as expected, after performing the steps in this guide. If not, the fault-finding guidance towards the end of this document should be followed.

2 Prerequisites

Before configuring iboss to work with Deep Secure Gateway eXtension there are a number of prerequisites that should be set.

Ensure that you have an activated iboss Secure Cloud Gateway service and the Management interface is reachable.

Ensure the Deep Secure GX has been setup as documented in the *GX Configuration Guide*.

☒ Ensure the #Unidentified content type has been applied to the active profile in the GX. Applying this setting will ensure content that Deep Secure cannot transform is reflected preserving the users web browsing experience.

Ensure the Deep Secure GX Data network can communicate with the iboss SCG Data network. This can be done by using the Diagnostics setting in the GX interface.

Tip This guide has been written with a fresh installation of iboss Secure Cloud Gateway. If this guide is being used to integrate the Deep Secure GX Appliance into an already configured iboss Secure Cloud Gateway, the guidance in this document may not work and you may need to speak to an iboss technical advisor to resolve.

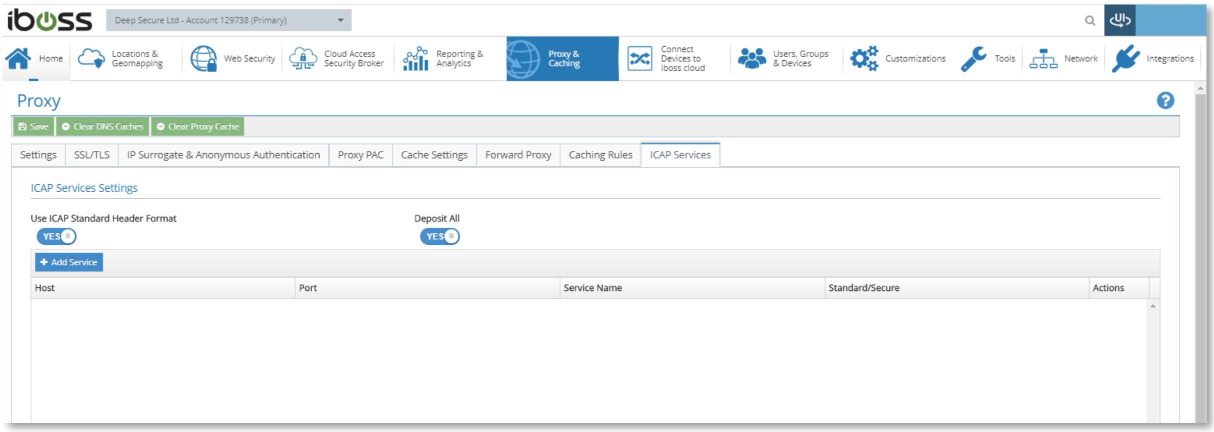
3 Integration Steps

3.1 iboss ICAP Configuration

This section details what is required for non-TLS ICAP connections between the iboss Cloud Secure Gateway and the Deep Secure GX.

Non-TLS ICAP connection should only be used for testing and proving initial data flow. TLS ICAP should be used for all other purposes.

First connect to the iboss management interface and navigate to Proxy Caching → ICAP Services and Click *Add Service.*



ICAP Services Settings

Use ICAP Standard Header Format: YES

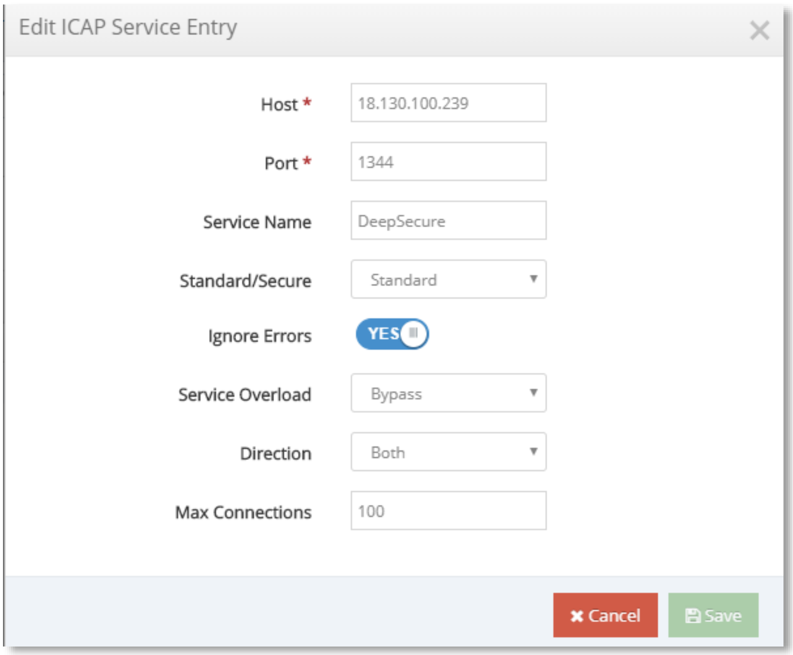
Deposit All: YES

Host	Port	Service Name	Standard/Secure	Actions

Figure 3.1 ICAP Setting Location

Once the ICAP Service settings are open configure them with the following settings, as shown in Figure 3.2:

- Host – IP address of the GX Data Network
- Port – ICAP Port being listened on in GX (default 1344)
- Service Name – A friendly name for the Service
- Standard/Secure – Standard (ICAP)
- Ignore Errors – Whether or not GX error response codes are ignored
- Service Overload:
    - Block – connections to internet are blocked until service is available
    - Bypass – allows internet traffic to still work if GX is busy
    - Wait – Holds the connection open to GX until service is available
- Direction – whether uploads, downloads or both are set to Max Connections – the Maximum number of connections made to GX



Edit ICAP Service Entry

Host * 18.130.100.239

Port * 1344

Service Name DeepSecure

Standard/Secure Standard

Ignore Errors YES

Service Overload Bypass

Direction Both

Max Connections 100

Figure 3.2 Example ICAP settings

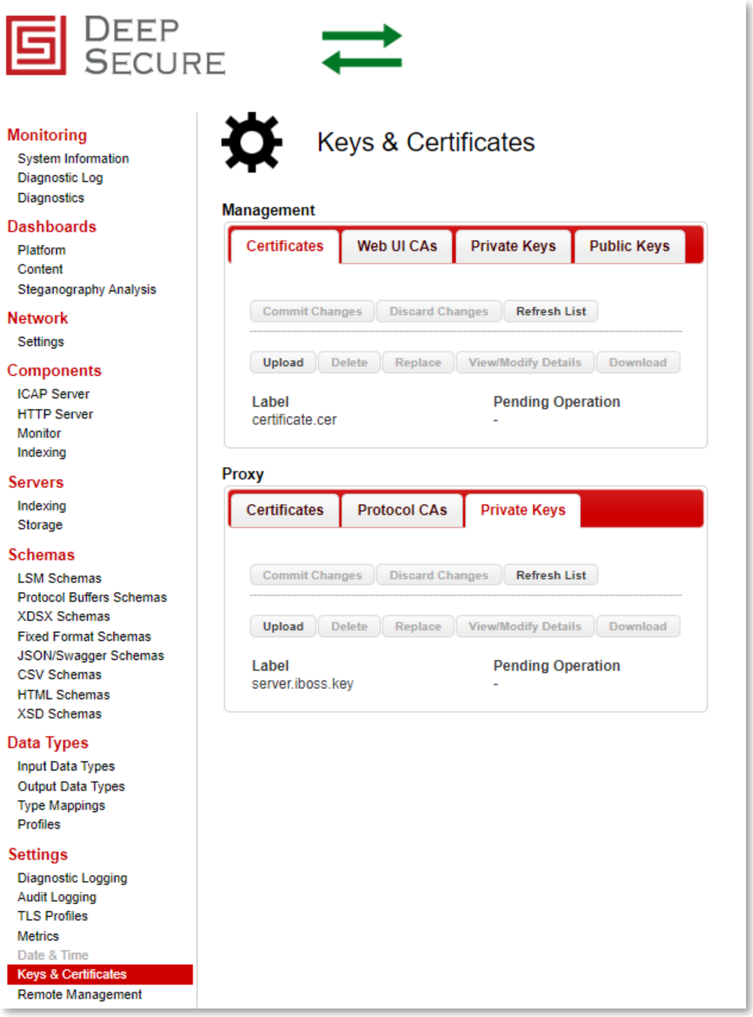
Once the settings have been provided save the settings.

3.2 Deep Secure GX ICAPS Configuration

A GX Server certificate with Private key signed by the CA certificate uploaded to the iboss Secure Cloud Gateway must be created first.

⚠ Do not use the default certificates uploaded onto the GX server – a user should always upload their own key material.

Connect to the management of the GX software and navigate to the *Key and Certificate* location under the Settings heading.



Management

Label	Pending Operation
certificate.cer	-

Proxy

Label	Pending Operation
server.iboss.key	-

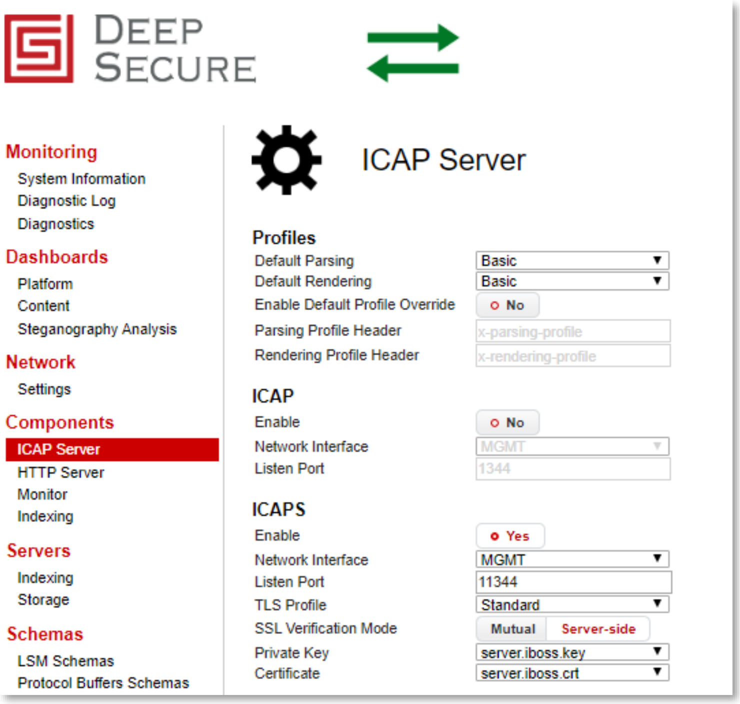
Figure 4.2 Key and Certificate location

Upload the server certificate and private key that match the CA uploaded to the iboss secure cloud gateway. To do this navigate to the *Proxy Certificate* setting and click *Upload*. A file explorer window will appear, select the appropriate server certificate. Once the server certificate has been uploaded the *Pending Operation* will be set to *Add*. To complete the upload process click the *Commit Changes* button, the *Pending Operation* will change to a '-'. Repeat this process for the Server Key and CA certificate.

Tip If a password is protecting the Server Key the *View/Modify Details* button should be used to apply the password protecting the Server Key, before the *Commit Changes* button is clicked.

The final stage is to apply the Server Certificate and Private Key to the ICAPS service on the GX. To do this navigate to Components → ICAP Server applying the following settings:

- Profiles – Leave as the default Basic, unless a custom profile is being applied.
- ICAP – Change Enable to No
- ICAPS – Change Enable to Yes
- Network Interface – Select the interface being used for ICAP Data
- Listen Port – Must match the iboss port configured to send data on
- TLS Profile – Leave as Standard, unless a custom TLS Profile is being used
- SSL Verification Mode – Server-Side
- Private Key – The Private Key previously uploaded
- Certificate – The Server Certificate previously uploaded



ICAP Server

Profiles	
Default Parsing	Basic ▼
Default Rendering	Basic ▼
Enable Default Profile Override	○ No
Parsing Profile Header	x-parsing-profile
Rendering Profile Header	x-rendering-profile
ICAP	
Enable	○ No
Network Interface	MGMT ▼
Listen Port	1344
ICAPS	
Enable	○ Yes
Network Interface	MGMT ▼
Listen Port	11344
TLS Profile	Standard ▼
SSL Verification Mode	Mutual [✓ Server-side]
Private Key	server.iboss.key ▼
Certificate	server.iboss.crt ▼

Figure 4.3 Example ICAPS Configuration

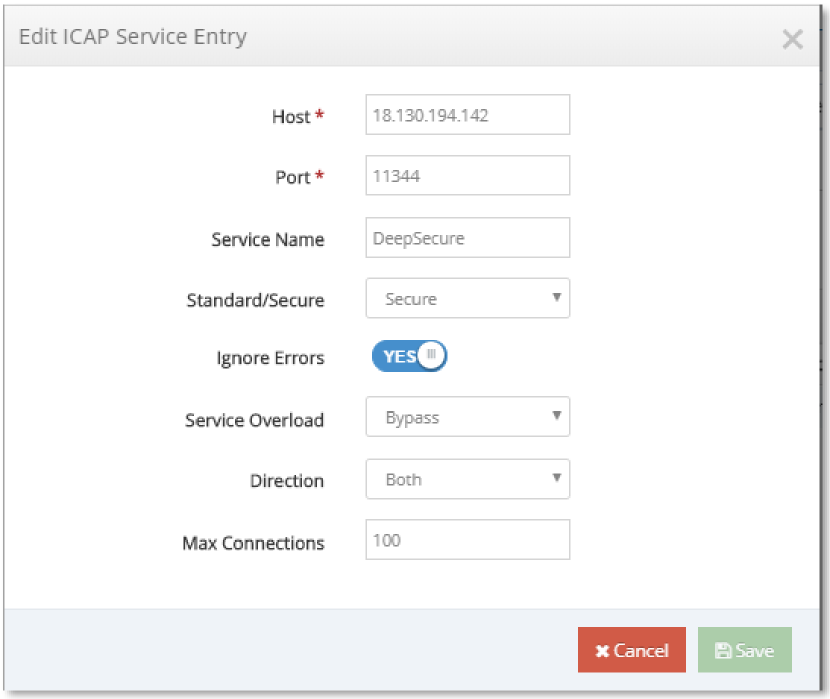
Save the configuration.

3.3 iboss ICAPS Configuration

To make the service suitable for a live deployment TLS should be enabled on the iboss Secure Cloud Gateway and the Deep Secure GX. The following steps detail how to do this.

> ☒ It is assumed that the user has a working Certificate Authority with matching Server certificate and Private Key. If these have not been created, create these before attempting the ICAPS configuration.

First connect to the iboss management interface and create a service in a similar way that an ICAP service is created for the ICAP configuration (Section 3), but choosing Secure instead of Standard for Standard/Secure, as shown below:



Edit ICAP Service Entry

Host *	18.130.194.142
Port *	11344
Service Name	DeepSecure
Standard/Secure	Secure
Ignore Errors	YES
Service Overload	Bypass
Direction	Both
Max Connections	100

Figure 4.1 Example ICAPS settings

Once the settings have been provided save the settings.

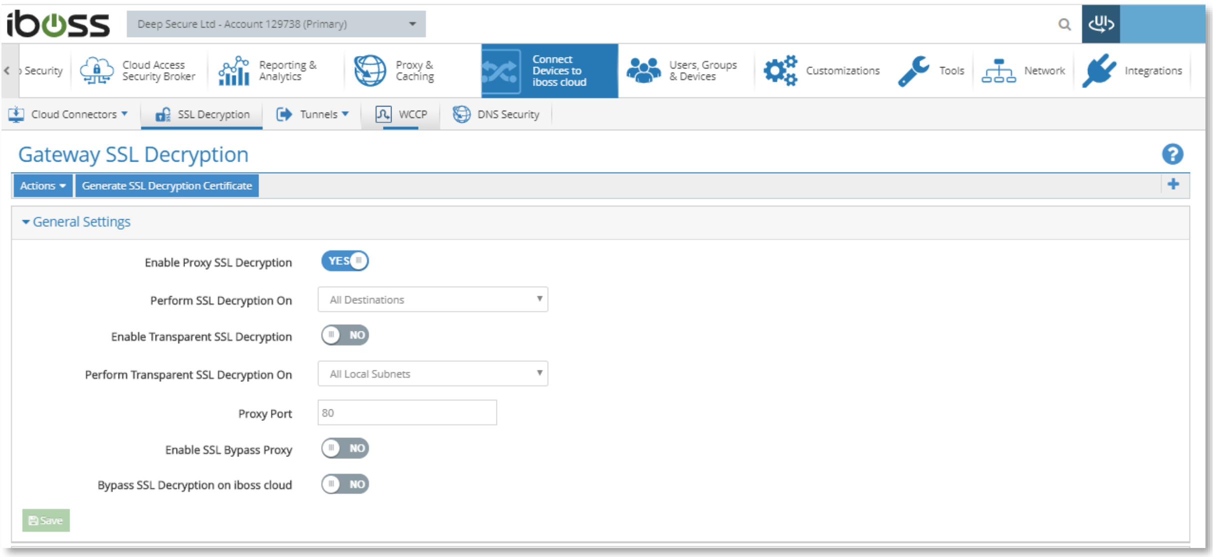
Next within the iboss Secure Cloud management interface navigate to Network → Admin SSL Certificates → Actions → Add Trusted Certificate and Paste the Certificate Authority certificate into the text box. The ICAPS service will now use the imported CA certificate and GX will authenticate itself to iboss – iboss will authenticate GX by validating the GX cert through the certificate chain to the loaded CA cert.

4 Fault Finding

If after following the previous steps data is not being sent to Deep Secure's GX the following may be at fault.

4.1 SSL Decryption

SSL Decryption must be set in the iboss configuration to perform SSL Decryption on all destinations, otherwise not all web traffic will be sent to the Deep Secure GX. To check this setting connect to the iboss Secure Cloud Gateway and navigate to *Connect Devices to iboss cloud* → *SSL Decryption* → *General Settings* and locate '*Perform SSL Decryption On*' setting, which should be set to '*All Destinations*'.



Enable Proxy SSL Decryption: YES

Perform SSL Decryption On: All Destinations

Enable Transparent SSL Decryption: NO

Perform Transparent SSL Decryption On: All Local Subnets

Proxy Port: 80

Enable SSL Bypass Proxy: NO

Bypass SSL Decryption on iboss cloud: NO

Figure 5.1 Example SSL Decryption Setting

5 Supported Data Types

The following data types are currently supported by the Deep Secure GX appliance and all other data types will be returned unchanged which ensures the user experience is unaffected:

Data Type	Content Type
BMP	Image/bmp Image/x-ms-bmp Bmp
CSV	Text/csv Csv
DOCX	Application/vnd.openxmlformats-officedocument.wordprocessingml.document docx
EMF	Application/emf Image/emf Emf
GIF	Image/gif Gif
HTML	Text/html Html Htm
JPEG	Image/jpeg Jpeg Jpg
JPEG2K	Image/jp2 Jp2
JSON	Application/json
MIME	Mime Message/rfc822 Application/x-mimearchive Eml Mht
PDF	Application/pdf Pdf
PNG	Image/png Png
PPTX	Application/vnd.openxmlformats-officedocument.presentationml.presentation pptx
RTF	Text/rtf Rtf Application/msword
TXT	Text/plain Txt
TIFF	Image/tiff Tiff Tif
WMF	Application/wmf Image/wmf Wmf
XML	Embedded/xml
ZIP	Application/zip Application/x-zip-compressed Zip

6 References

GX Configuration Guide