3 - Managing Carriers

The Carriers section is used to create and configure the connections between the Carrier Cloud SBC and other VoIP switching systems. Most commonly, these connections will be with other telephony organisations with which the Platform Operator has a relationship, but connections may also be made to other internal VoIP Platforms within an organisation.

Types of Carriers

Carrier Cloud Manager divides Carriers into three categories:

Carrier Type	Description
Customer	A “Customer” is an ingress only connection to a telecommunications company who will be sending VoIP traffic to the Carrier Cloud Platform to be routed and rated. A Customer will have a “Customer Rating Plan” attached to it, determining how much the Customer will be charged for the calls that are processed through the Platform, and a “Carrier Balance” which will record in real-time the amount that they spend/owe.
Supplier	A “Supplier” is an egress only connection to a telecommunications company to which the Platform will be routing traffic. A Supplier will have a “Supplier Rating Plan” attached to it, specifying how much the calls that are sent to the Supplier cost the Platform Operator, and a “Supplier Balance” which will record the amount of money that has been spent with that Supplier.
Bilateral	A “Bilateral” Carrier is a telecommunications company to which Carrier Cloud sends calls, and from which it receives calls. In this case the Bilateral Carrier is connected to both a “Customer Rating Plan” and a “Supplier Rating Plan”, so both Customer and Supplier costs will be specified for them.

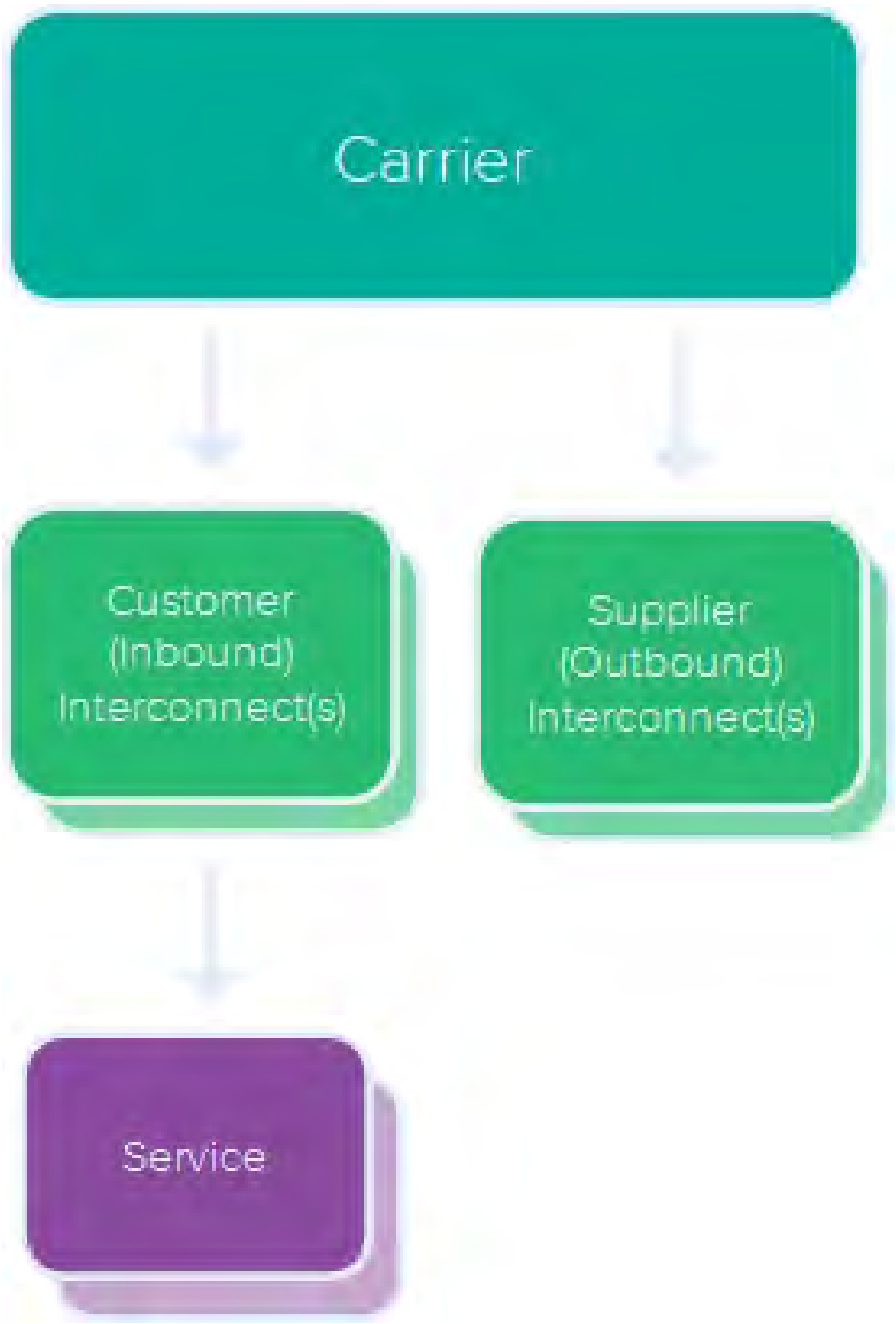
Carrier Components

A Carrier comprises three separate components which must each be configured before the Carrier is ready for use; they are:

Component	Description
Carrier	The "Carrier" itself does not hold any technical information about the connection to the outside world; this is set at the Interconnect level. The Carrier is a management object that determines the type of Carrier connection that is taking place (Customer/Supplier/Bilateral) and with which, one or more Interconnects may be associated. The Carrier also holds the Customer Balance for Customers, the Supplier Balance the Suppliers, or both for Bilateral Carriers. Reference: See the following Section for further information on the difference between Customer and Supplier Balances.
Interconnect	The "Interconnect" is where the technical configuration of the connection between The Carrier Cloud Platform and the external switch that is being connected to is configured. Each (working) Carrier has a minimum of one Interconnect that contains the technical details of the connection; these include: ■ Ingress/Egress IP Addresses ■ Technical Prefixes used ■ Codecs supported ■ DTMF transit method, and ■ Monitoring information.
Service	The "Service" is where the Rating and Routing details for each Interconnect are configured. **Tip:** The Service is only required for Customer Interconnections, never for Supplier Interconnections. While it is common practice to have a single Service per Interconnect, it is possible to have multiple Services where calls are distinguished by different ingress matching settings.

Carrier Components Diagram

The diagram below summarises the relationship between the different components of a Customer and Supplier Carrier.



- Carriers provide top-level financial & partner management
- Interconnects provide technical connectivity
- Services provide commercial decision-making - i.e. (Rating & Routing)

Understanding Customer and Supplier Balances

The Digitalk Carrier Cloud Platform will real-time rate both the cost of the calls to the Customer and using the Supplier Rates that have been provided by the Supplier it will record the price that will be charged to us by the Supplier.

Customer Balance

Carrier Cloud updates the Customer Balance after every call, and it will enforce either prepayment or a postpaid credit limit for the Customer. For Customers the credit control is managed by Carrier Cloud and it will prevent a Customer making any further calls when that limit is reached, even cutting calls off if the limit is reached when calls are in progress.

E-Mail Alerts can be generated and sent to a Customer representative when a defined threshold is reached to warn them of this.

Supplier Balance

The Supplier Balance is different to the Customer Balance. While the Customer Balance relates directly to credit information that is enforced by Carrier Cloud the Supplier Balance records how much money the Platform Operator has spent with a specific Supplier based on the Supplier Rates that they have provided us.

Therefore the pre or postpaid limits are not enforced by Carrier Cloud, in the sense that Carrier Cloud will not stop calls if they are reached. Although of course the Supplier might well refuse additional calls from the Platform.

The limits are used by Carrier Cloud to generate E-Mail Alerts that can notify Account Managers that the credit limit with the particular Supplier is close to being reached.

Note that the Supplier Balance cannot be relied on being 100% accurate, as the credit control for the charges being applied is outside of the Carrier Cloud Platform. It should however provide a close indication of the costs incurred.

Net Exposure

The Net Exposure displays the difference between the Customer and Supplier balance. This figure cannot be directly edited or controlled, instead it is automatically calculated by subtracting the Supplier Balance from the Customer Balance.

Net Exposure Alerts can be used to notify the Platform Manager when the exposure passes a specified threshold. Two types of Net Exposure Alerts can be configured:

- Customer Net Exposure Alerts can alert when the Net Exposure Threshold is breached by the Customer balance dropping below a certain threshold, meaning that the Customer owes enough money to warrant an alert.
- Supplier Net Exposure Alerts alert when the Net Exposure Threshold is breached by the Supplier balance dropping below a certain threshold, meaning that we owe the Supplier enough money to warrant an alert.

Multi Currency Balances

Carrier Cloud Manager supports the ability to assign up to three separate currencies for both Customer and Supplier balances.

Reference: "Multi-Currency Carrier Support" on page 190

What Next?

Follow the links below for information of creating Carrier, Interconnects, and Services:

"Creating a Carrier" on the next page

"Creating an Interconnect" on page 71

"Creating a Service" on page 122

3.1 Creating a Carrier

The first step in the Carrier creation process is to create the Carrier object itself.

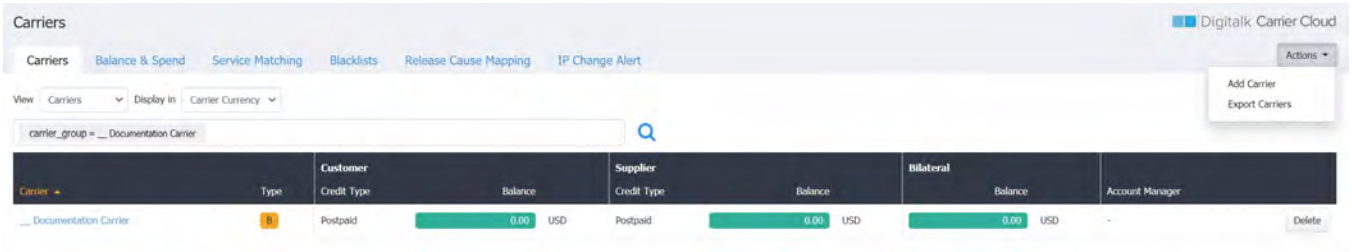
The Carrier acts as the management object for Interconnects and Services and also contains information such as:

- Currency
- Customer Balance
- Supplier Balance
- Net Exposure (The difference between the Customer and Supplier balance)
- Customer Contacts

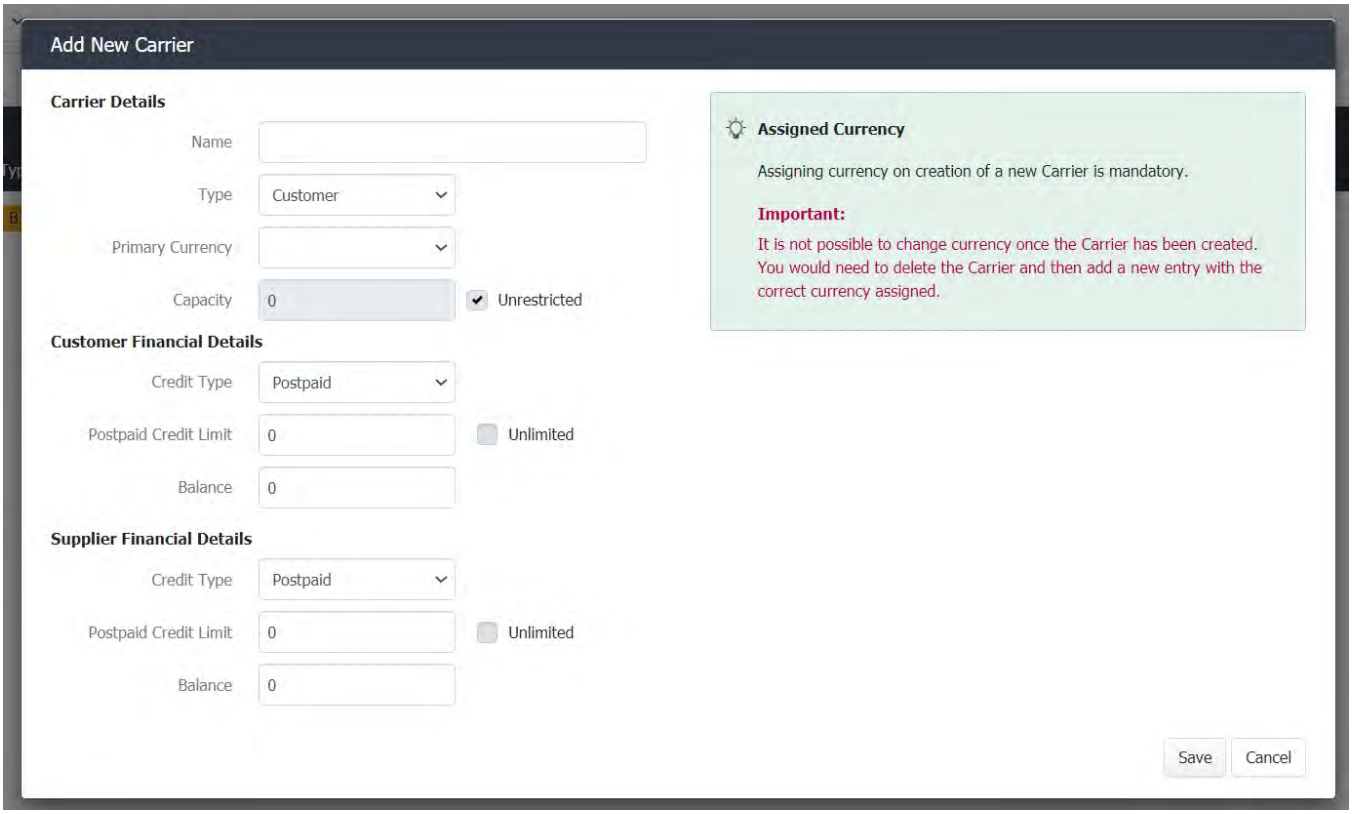
3.1.1 Procedure for Creating and Configuring a Carrier

Follow the steps below to create and configure a Carrier.

1. Select “Carriers” from the navigation bar, or from the Management Links section on the Home screen.
   Result: The Carriers screen is displayed.



2. Select “Add Carrier” from the “Actions” drop-down list box.
   Result: The “Add New Carrier” dialog box is displayed.



3. Use the table below to complete this step.

Note:

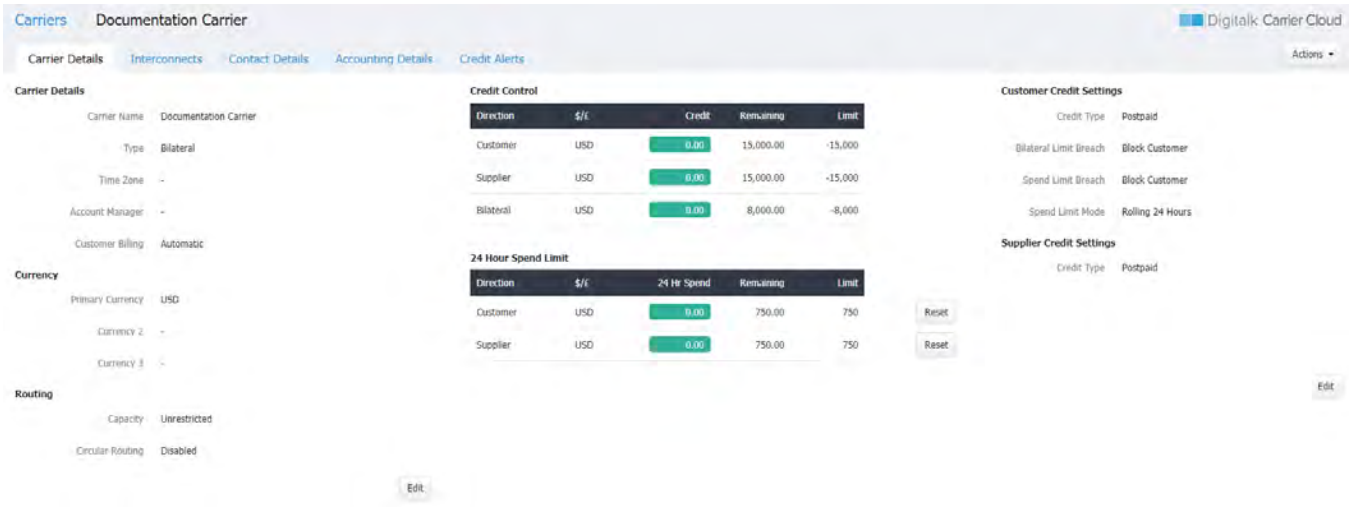
- Carrier Details and Currency must be completed for all Carrier types.
- Customer Financial Details must be completed for Customer and Bilateral Carriers.
- Supplier Financial Details must be completed for Supplier and Bilateral Carriers.

Field	Description	Action
	Carrier Details	
Name	Determines the name by which this Carrier will be known.  **Caution:** Carriers must be named using alphanumeric characters only, avoid using special characters.	Enter the required name in the “Name” field.
Type	Determines the type of Carrier being created. Select from: ■ Customer ■ Supplier, and ■ Bilateral. Reference: See Section "Managing Carriers" on page 51 in this User Guide for further information on Carrier Types.	Select the required Carrier type from the drop-down list box.
Capacity	This optional setting is used to determine how many simultaneous voice sessions this Carrier can support. This option is sometimes used when bandwidth to a particular Carrier is limited.  **Note:** With Bilateral Carriers, this limit applies to the total of inbound and outbound sessions.	If required, set a capacity limit for this Carrier.
	Currency	
Primary Currency	Determines the Primary Currency for the Carrier being created.	Select the required Currency for this Carrier.

	 **Note:** Every Carrier must be configured with at least one Currency. This initial currency is regarded as the "Primary Currency" and is used when displaying overall financial information about the Carrier. If required, additional Currencies can be added to the Carrier (up to a maximum of three in total). When multiple currencies have been configured, it is possible to redefine the Primary Currency is so defined.  **Caution:** However, due to referential data requirements when a currency has been added to the Carrier it is not possible to remove it.	
Customer Financial Details		
Credit Type	Determines if this Customer will be: ■ Prepaid - calls will stop functioning at 0.00 credit. ■ Postpaid - calls will continue below 0.00, and only stop if a postpaid credit limit is reached.	Select the required Credit Type from the drop-down list box.
Postpaid Credit Limit	This setting is only applicable when the Credit Type of Postpaid has been selected. It determines a limit of how far below zero a Customer can go before their calls are stopped, therefore providing some element of liability protection with postpaid calling.	If required, enter the relevant Postpaid Credit Limit.
Balance	This field displays the current balance for a Customer. During initial Carrier creation a balance can be manually entered into this field, however after the Carrier has been created the balance can only be altered using an audited credit/debit process.	If required, set an opening balance for this Customer.
Supplier Financial Details		

Credit Type	Determines if this Supplier is Prepaid or Postpaid **Note:** This limit is provided for reference and for alerting purposes only. The Carrier Cloud Platform will not stop Supplier calls at a pre or postpaid limit as this is not Credit Controlled by this Platform. (Although a Supplier might be enforcing a limit on their Platform.)	Select the required Credit Type from the drop-down list box.
Postpaid Credit Limit	This setting is only applicable when the Credit Type of Postpaid has been selected and records the credit limit that has been agreed with the Supplier.	If required, enter the relevant Postpaid Credit Limit.
Balance	This field displays the Supplier Balance. During initial Carrier creation a balance can be manually entered into this field, however after the Carrier has been created the balance can only be altered using an audited credit/debit process.	If required, set the starting balance for this Supplier.

4. Click “Save”.
   Result: The Carrier is created, and will be displayed on screen.



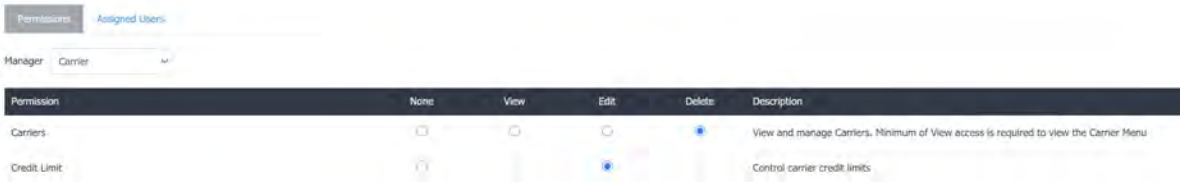
5. If required, click the left-hand "Edit" button to configure the optional carrier settings.
   Result: The optional Carrier Details become configurable.

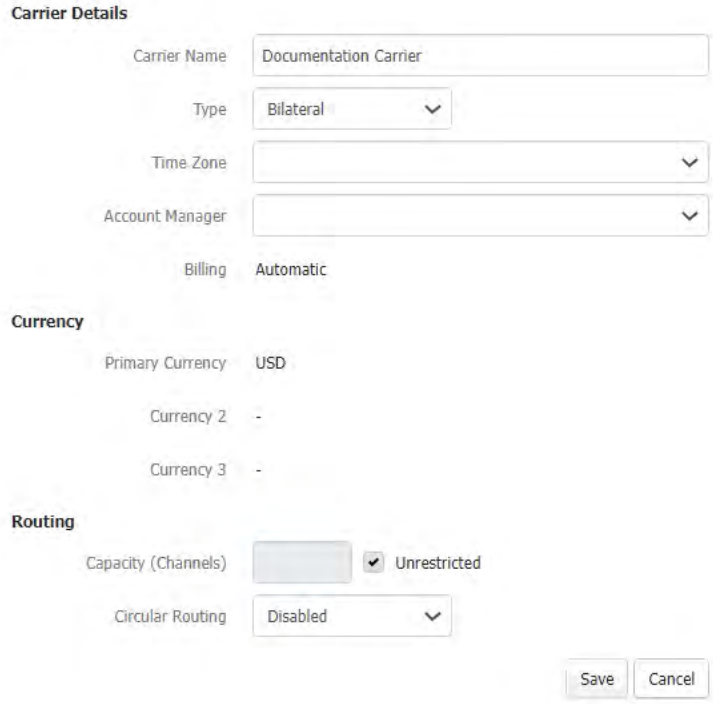
Technical Note:

Regarding Permissions.

Be aware that there are two Edit buttons on the screen. The Edit button on the right-hand side associated with the Credit Control section controls access to the configuration of Credit Setting and is controlled by a specific permission named “Carrier > Credit Limit”.

All of the other Carrier settings are controlled by the “Carrier > Carriers” permission.

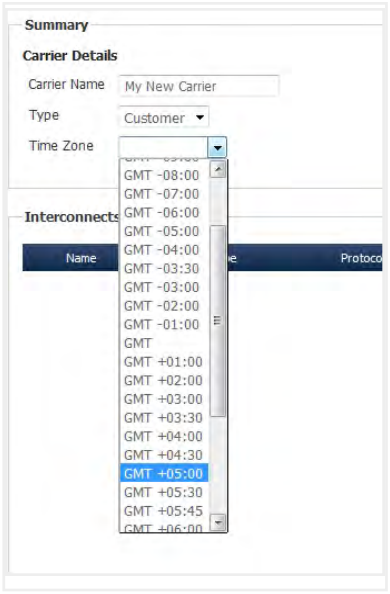




6. Use the table below to complete the Carrier Details and Routing sections.

Field	Description	Action
Carrier Name	This field defines the name of the Carrier. It will be populated with the information configured on the “carrier creation” dialog box that can be edited as and when required.	No action required.

	Caution: Carriers must be named using a combination of alphanumeric characters, avoid using special characters.	
Type	The “Type” drop-down list box displays the type of carrier that was selected on the “carrier creation” dialog box. This Type can be changed at any time, meaning that a carrier that was created as a Customer or Supplier can be converted to a Bilateral Partner.	No action required.
Billing	This is a notification as to whether or not Billing has been scheduled for this Partner.	No action required.
Time Zone	The Carrier Time Zone setting is an optional feature which can be used to "mark" a particular Carrier is operating in a different Time Zone to the Platform default. While this may be configured for purely informational purposes, it also means that "time sensitive" platform features such as Customer Rating, Reporting, and Billing can be managed in the Carrier's Local Time. **Example:** Without using this feature - if a platform is operating in UTC, but a particular Supplier is invoicing in UTC -5 then there will be a mismatch between the Supplier Invoice generated on the Digitalk platform and the "real" Invoice received from the Supplier. This is likely to lead to an extra discrepancy in the build amounts. By configuring the Supplier with a Carrier Time Zone of -5, and setting the "Use Local Carrier Time Zone" option on the Supplier Billing Settings the Supplier Invoice produced on the Digitalk will more closely match the invoice received from the Supplier.	If required, configure the required Time Zone using the drop-down list box.

		
Account Manager	This optional field marks the Account Manager for this Carrier. Account Managers are Carrier Cloud Users. The Account Manager relationship is used for certain reports and access to the Carrier Portal. Reference: See “UG-025-4xx - Carrier Cloud Carrier Portal” for further information on working with Account Managers.	If required, select an Account Manager from the drop-down list box.
Capacity	This defines the maximum number of channels (circuits) available to all Interconnects under this Carrier. This setting can also be configured at the Interconnect level.	If a Carrier level channel restrictions is required, then configure the appropriate number of channels.
Circular Routing	This option will enable/disable the ability to send calls received from a Customer Interconnect to a Supplier Interconnect that is assigned to the same Carrier. The default behaviour is “Disabled” which means that the Supplier WILL NOT be used for Routing, but it may be necessary to “Enable” this function in Test scenarios.	Leave this option at “Disabled” unless Circular Routing is specifically required.
Suspend customer	This feature determines the behaviour of the platform if a Credit Limit is configured on the Net Exposure, and then breached.	If required, enable the “Suspend cus-

traffic on net exposure breach	By default this option is unselected. Which means in the event of a breach calls will still be accepted and routed from the Customer Interconnect(s). When used in this mode Alerts can still be raised for breaches of the Net Exposure, but routing continues. By enabling this option the Platform will suspend ingress traffic if a breach of the Net Exposure Credit Limit occurs. As shown in the example below where the customer is suspended: **Note:** Only the Customer traffic is suspended, and not the Supplier traffic. This means if traffic is sent to the Supplier Interconnect the Customer Interconnect is likely to be re-enabled automatically.	tomer traffic on net exposure breach" feature.

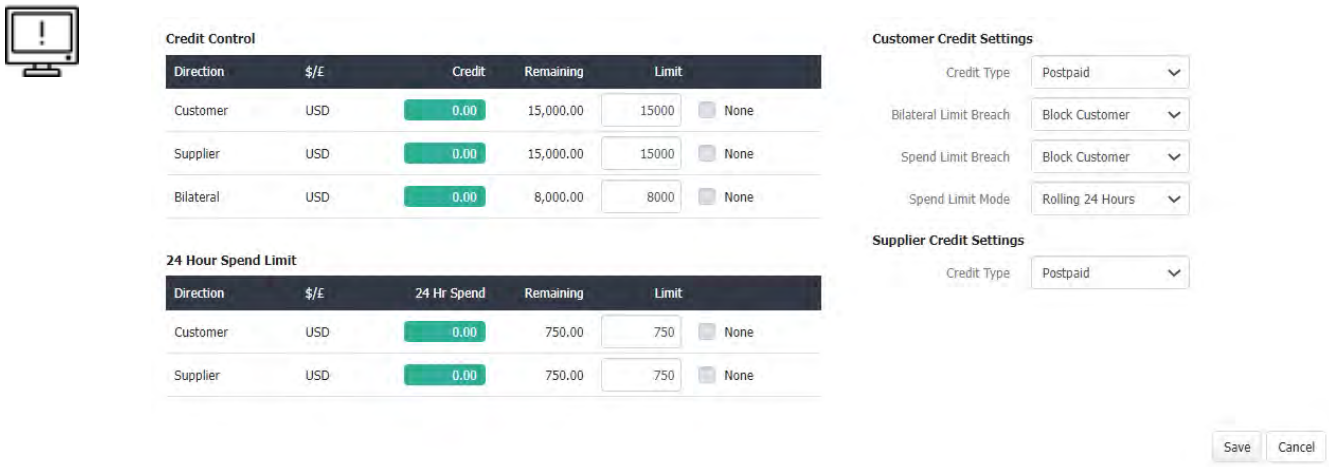
7. If required, click the right-hand "Edit" button to configure Carrier credit settings. (See below for more details.)

Note:
The reason that there are two separate "Edit" buttons for this screen is because there is a separate Permission "Carrier > Credit Limits" that controls whether a CCM User who has access to manage other aspects of the Carrier also has permissions to change financial information such as Credit Limits.

Reference: See "Introducing User and Role Management" on page 1552 for further information.

Technical Note:

Understanding Credit Control



The Credit Control settings allow a Carrier Manager to determine credit behaviour of this Carrier Partner.

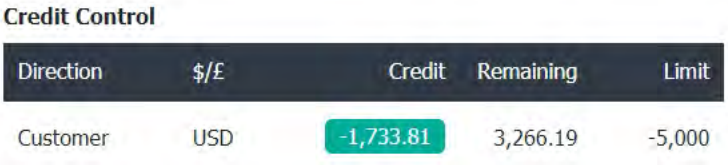
Note: The information below is written in reference to Bilateral Carriers, unilateral Carriers will only display the Customer/Supplier information as appropriate.

Managing Credit Limits

Credit Limits are used to determine the maximum amount of exposure that you, as the Platform Operator, are prepared to accept in relation to the Customer Balance, Supplier Balance, and Bilateral Balance for this Carrier.

Credit Limits are only used with Postpaid Balances, as the credit limit for a prepaid balance is automatically “0”, with no liability extended.

Setting a Customer credit limit of 5,000, means that the customer balance can be reduced to -5000 before the credit limit is reached and calls will be suspended. As money is spent, the “Remaining” figure will show how much credit is left before the credit limit is reached, as shown in the screenshot below.



Setting a Supplier credit limit of 5000, means that the Supplier balance can be reduced to -5000 before this limit is reached. However, with the Supplier credit limit calls will not be suspended by the Platform, (although traffic may be suspended by the Supplier Partner).

Credit Control

Direction	$/£	Credit	Remaining	Limit
Customer	USD	-1,733.81	3,266.19	-5,000
Supplier	USD	-1,250.22	3,749.78	-5,000
Bilateral	USD	-483.59	2,016.41	-2,500

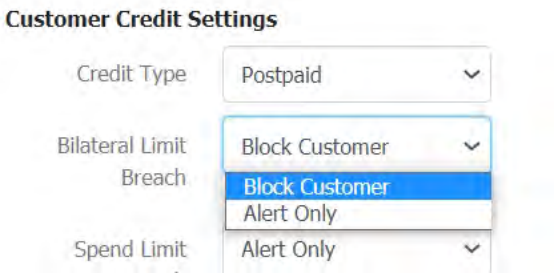
As seen in the screenshot above, the Bilateral balance is a figure derived from the Customer and Supplier Balance, it equals the *(customer balance) – (supplier balance).*

The Bilateral Balance (also known as the Net Exposure) displays your current credit exposure in relation to this Carrier Partner.

A negative balance (as above) means that the customer owes 'you' more than you owe 'them', and a positive balance means that you owe them more than they owe you.

The Bilateral balance credit limit can be used to ensure that the Customer and Supplier balances remain within a particular range of each other. If the bilateral credit limit is reached by Customer balance becoming too low (a negative balance) then an option exists to block customer traffic at that point in time.

This option is set by the “Bilateral Limit Breach” setting which determines if when this limit is reached traffic is blocked, or allowed to continue - with the possibility of alerts being generated if configured.



Tip:

Clarifying Traffic Blocking

The flexibility offered by the CC Platform means that there are many options available for Credit Management that can seem initially daunting.

To try to clarify this the first rule to be aware of is that from a commercial perspective the Carrier Cloud Platform is in control of the rating for the Customer traffic. Customer calls are being rated by the Platform meaning that the responsibility for credit controlling those calls is held by Digitalk. That is why Customer traffic will be suspended, even to the extent of ending calls in progress, if the Customer Credit Limit is reached and why the option exists in relation to Customer traffic to do so if the Bilateral Credit Limit is reached.

The second rule is that Supplier Rating on the Platform is based upon the information we have received from Suppliers, and the platform records Supplier costs to ensure revenue assurance and accurate reconciliation. However, in this case the responsibility for credit control lays with the Supplier Platform. Meaning that while the Supplier Platform may suspend traffic, Digitalk will not suspend on this Platform.

Credit Alerting

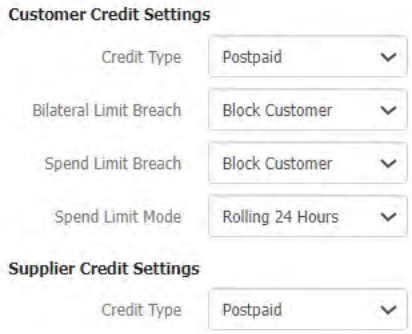
While Traffic Blocking occurs only with Customer traffic when a credit threshold is fully reached, it is possible to send Credit Alert emails. These can be sent in relation to both a low Customer or Supplier balance and in relation to either the Customer or Supplier bilateral net exposure.

If required, it is possible to create multiple alerts for each situation.

Example: For example, if a supplier balance limit was configured to -5000, alerts could be generated at -4000, -4500 and -5000.

Reference: For information on configuring Credit Alerts see here: "Credit Alerts" on page 217

8. Configure the credit settings using the table below.



Field	Description	Action
Customer Credit Type	Determines if the Customer balance is postpaid or prepaid.	Ensure the correct Credit Type is selected.
Bilateral Limit Breach	Determines Platform behaviour when the Customer bilateral balance credit limit is reached. The options available are: ■ Alert Only - Customer traffic will continue but any configured to get Credit Alerts will be sent. ■ Block Customer – Customer traffic will be blocked; any configured alerts will also be sent.	Select the required option.
Spend Limit Breach/ Spend Limit Mode	Determines Platform behaviour when the Customer 24-Hour Spend Limit threshold is reached. See: "Understanding the 24 Hour Spend Limit Feature" on page 188 for more information.	Select the required options.
Supplier Credit Type	Determines if the Supplier balance is postpaid or prepaid.	Ensure the correct Credit Type is selected.

9. If required, configure 24-Hour Spend Limit settings.
See: "Understanding the 24 Hour Spend Limit Feature" on page 188 for more information.

10. Click “Save”.
    The optional settings for the Carrier have been configured.

3.2 Creating an Interconnect

After the Carrier has been created the second step in the Carrier creation process is to create one or more Interconnects “underneath” the Carrier.

It is possible to create as many Interconnects as are necessary, for example for a Bilateral Partner there would be at least two Interconnects one inbound and one outbound.

The Interconnect contains the technical connection details which allows the Platform to validate inbound traffic, apply any number or codec manipulations as needed and then sends the call on to the selected outbound Carrier.

Caution:

While Carriers can, and commonly are, bilateral, serving both ingress and egress (Customer and Supplier) connections.

An individual Interconnect must only be configured as unilateral, or unidirectional, either Customer or Supplier.

Follow the Procedures below to create an interconnect, and then configure it for Customer or Supplier.

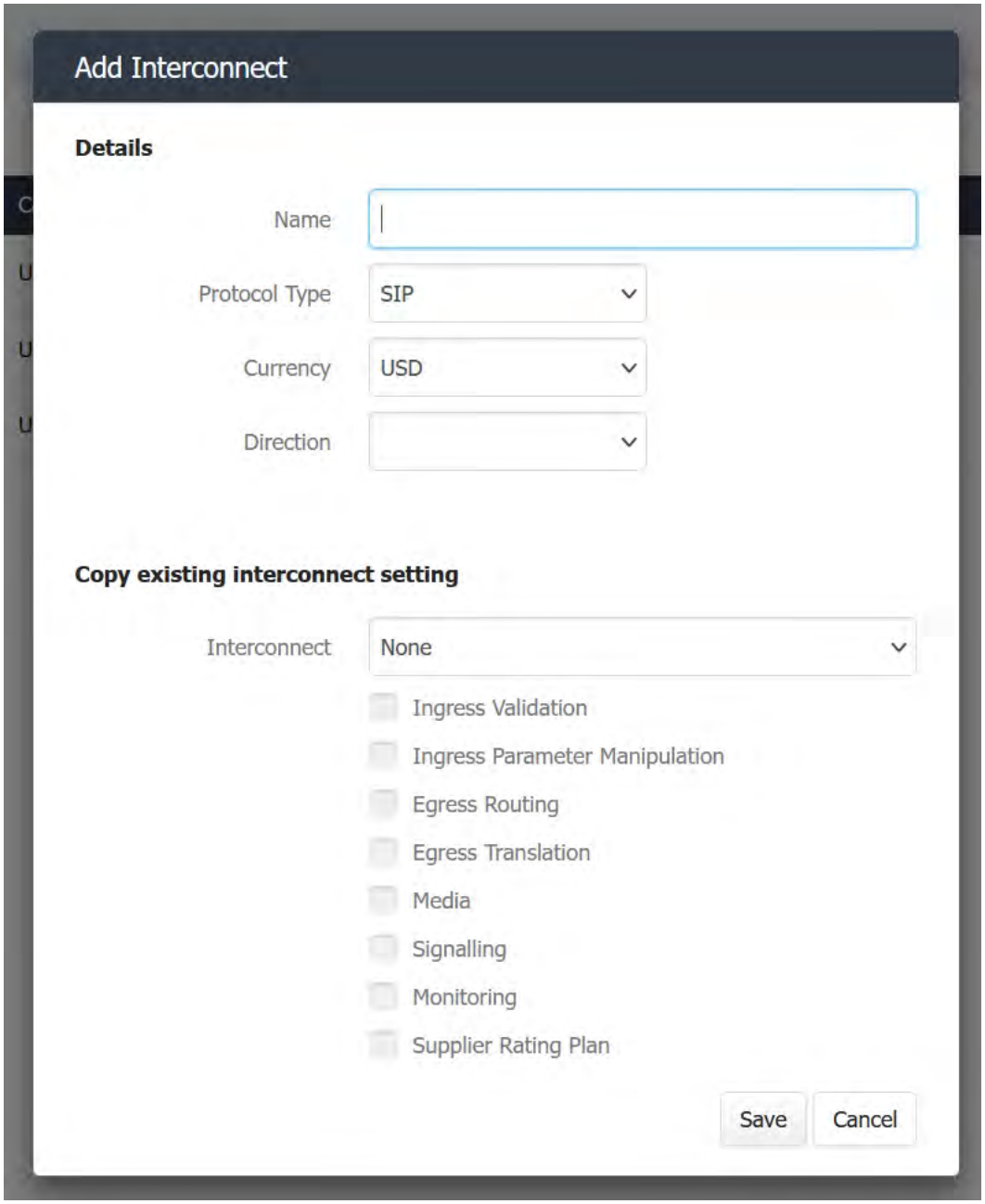
Creating a New Interconnect

Follow the steps below to create an new Interconnect.

1. Navigate to the Interconnects tab.

   Result: The Interconnects page will be displayed, any existing interconnects will be visible here and can be reordered when necessary.

2. Select “Add Interconnect” from the “Actions” menu.
   Result: The “Add Interconnect” dialog box is displayed.



2. Enter the name by which this Interconnect will be known in the “Name” field.
3. Select the required protocol type, SIP or H.323, from the “Protocol Type” drop-down list box.
4. If required, select the Currency that this Interconnect will function in.

Note: The Currency selection available is drawn from the currencies configured for the Carrier,

therefore if the Carrier has been configured with only a single currency that currency will be auto-populated.

Technical Note:

When offering Customer services in **multiple currencies**, different Interconnects will need to be configured for each of the currencies being offered.

This means that only rating plans (customer/supplier as appropriate) in the matching currency will be available for usage with this Interconnect and all traffic passing through this interconnect will be billed in the currency of choice.

Caution: Be aware that it is not possible to re-rate traffic from one currency to another currency.

5. Select the direct of the Interconnect being created, the options are “Customer” for an inbound/egress interconnect, or "Supplier" for an outbound/egress interconnect.

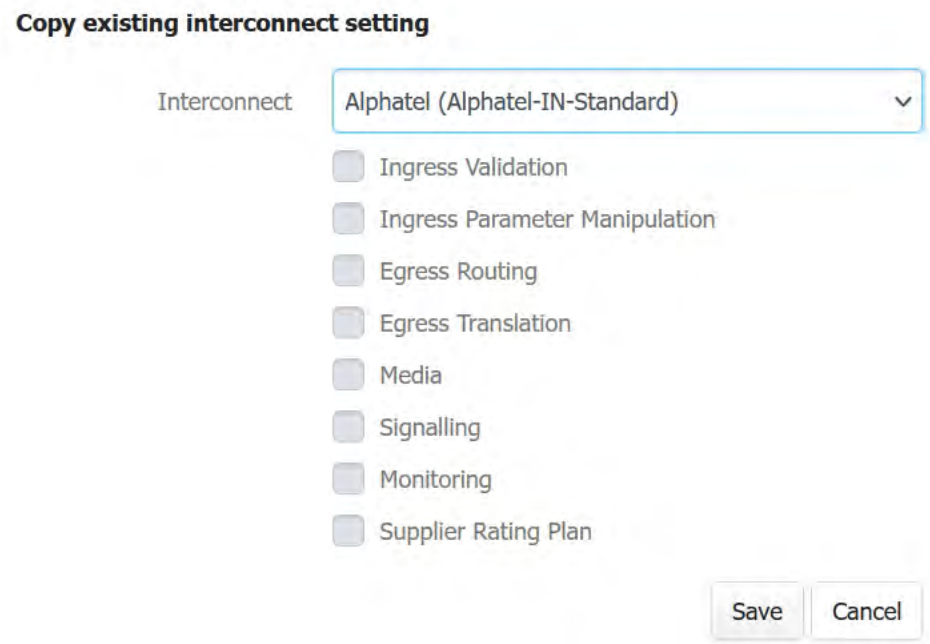
Caution:

Interconnects must always be either Customer or Supplier.

Never use the Bilateral option in a live environment it exists only for legacy support.

6. If this Interconnect is going to copy the settings from an existing Interconnect, select the relevant entry from the “Interconnect” drop-down list box.

Note:
This feature allows a new interconnect to be added this that includes the selected settings from existing interconnect.

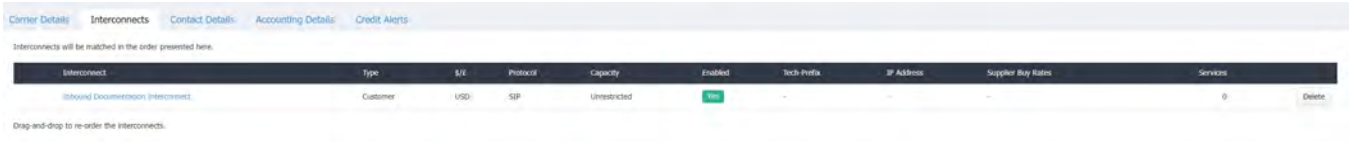


This feature is often useful when creating multiple Interconnects underneath the same Carrier where the majority of the settings are the same, and only a take-prefix may differ.

Technical Note: Note that the SBC IP address is copied by selecting the "Egress Routing" checkbox.

Caution: Be aware that when an Interconnect is created using this copy method it will be created by default as “inactive” to avoid conflicts with the existing entry. It will edits have been made.

7. Click “Save”.
   Result: The Interconnect is created, and is ready to be configured.



Note:

H.323

The screenshot and documented examples in this section all utilise the SIP signalling protocol.

Be aware that the Carrier Cloud does support the legacy H.323 protocol and Interconnects can be created that will use the H.323 terminology instead of SIP usage and terminology.

Next:

"Configuring a Customer Interconnect" on the next page

"Configuring an Supplier Interconnect" on page 98

3.3 Configuring a Customer Interconnect

A Customer Interconnect this provide the technical configuration for the communication between the Carrier Cloud and Customer Partners.

Technical Note:

Renaming Interconnects

Please be aware that after an Interconnect has been created it is not possible for it to be renamed.

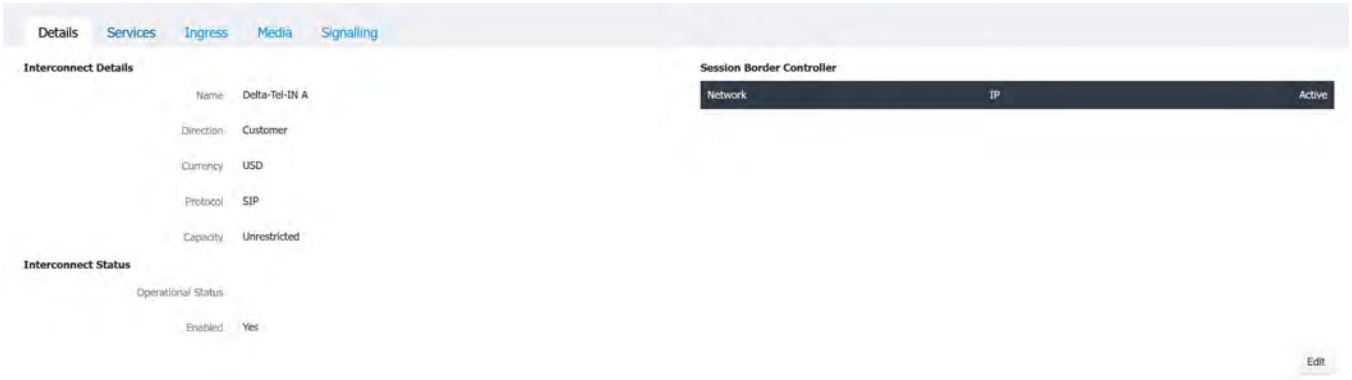
The reason for this is related to ensuring continued data integrity in the CDRs over the long term.

If an interconnect has been named incorrectly, then it can be deleted and recreated; or if it has already been configured then it can be copied with a new name and the original then deleted.

Follow the steps below to configure a SIP Interconnect to validate and route ingress traffic.

1. Click on the name of the Interconnect to be configured.

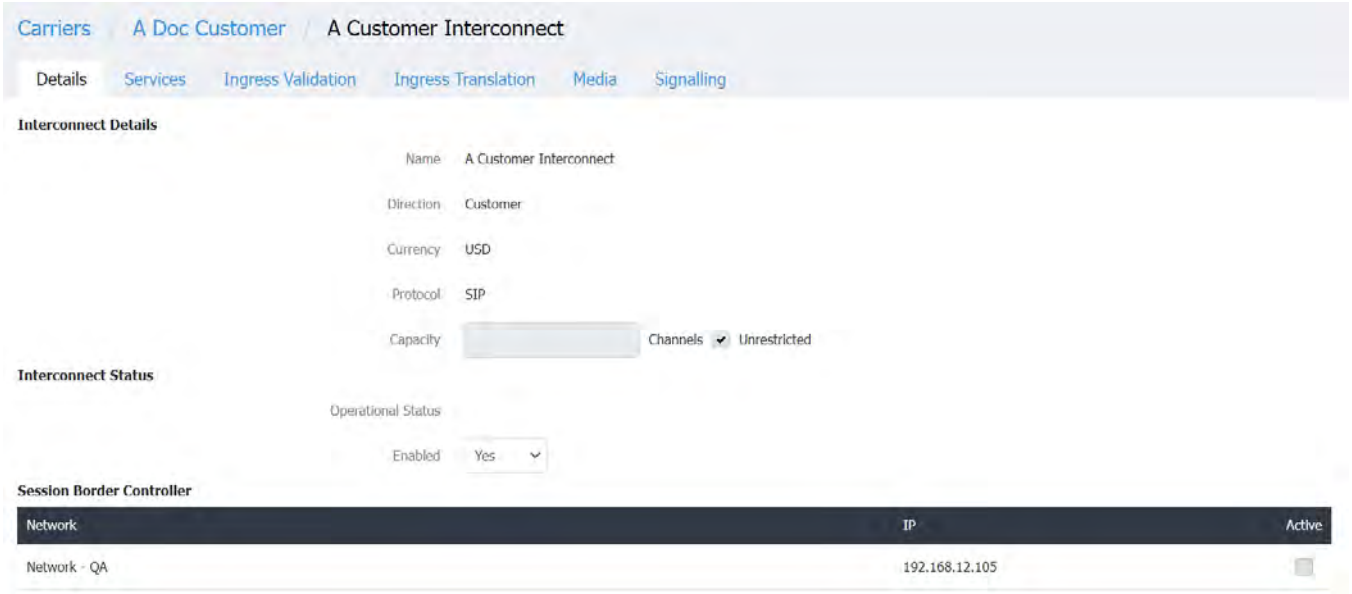
Result: The “Interconnect Management” screen is shown displaying a summary of the information regarding the Carrier Interconnect.



2. Click “Edit”.

Result: The “Details” screen can now be configured.

The Details Tab



3. If required, deselect "unrestricted" and enter a Channel Capacity limit in the “Capacity” field.

Note:
When configured this setting restricts the number of simultaneous calls that will be permitted into the Platform on this Interconnect at any one time.

If this limit is reached, then additional calls will be rejected without a CDR being written.

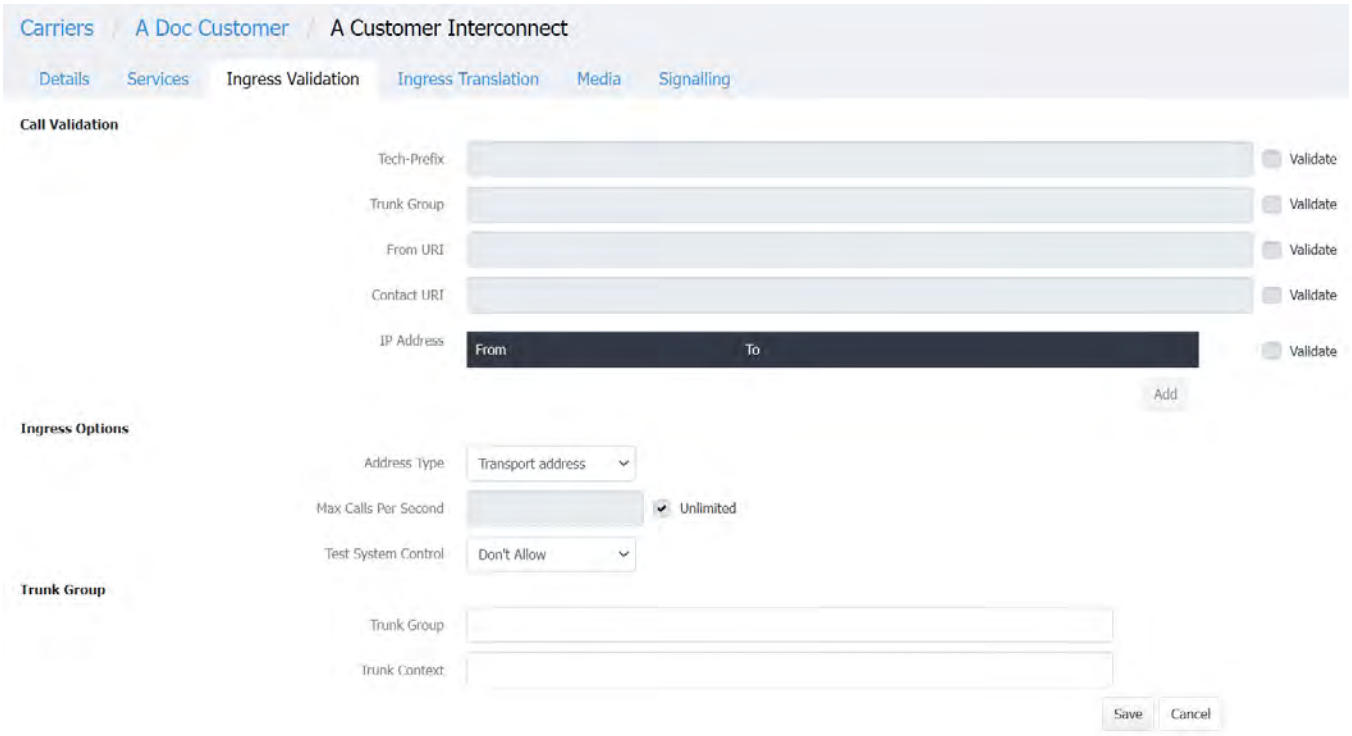
These rejected calls can be viewed on the "Viewing Calls Rejected by the SBC (Failed Inbound Calls)" on page 1539 screen.

5. Ensure the "Status" drop-down list boxes set to Active.
   Setting this field to Disabled will suspend the Interconnect until it is manually changed back to Active.
6. Select the Signalling IP address(es) on which this Interconnect will be receiving or sending traffic.
7. Click “Save”.

Result: The Details screen has now been configured.

The Ingress Validation Tab

1. Click the “Ingress Validation” tab. (Leave the Services Tab until the next step.)
   Result: The “Ingress Configuration” screen is displayed.
2. Click “Edit”.
   Result: The “Ingress Details” settings can now be configured.



3. Click "Add IP" to add an IP Address, and configure the other Ingress validation settings.

Caution:

Important Security Note Concerning Ingress Validation

It is important to understand that these ingress validation settings provide the security to ensure that the Platform only passes traffic from agreed-upon Partner organisations.

This means that ingress validation criteria must be as tightly defined as possible for each inter-connect to prevent exploit opportunities for fraudsters. Additionally, it is good practice to limit the permission to configure Interconnects to a few trusted personnel.

While from a purely technical perspective it is possible on the Carrier Cloud to validate traffic without using an originating IP Address, this method is normally applicable only in some niche routing scenarios when the Platform is working as part of a larger Wide Area Network.

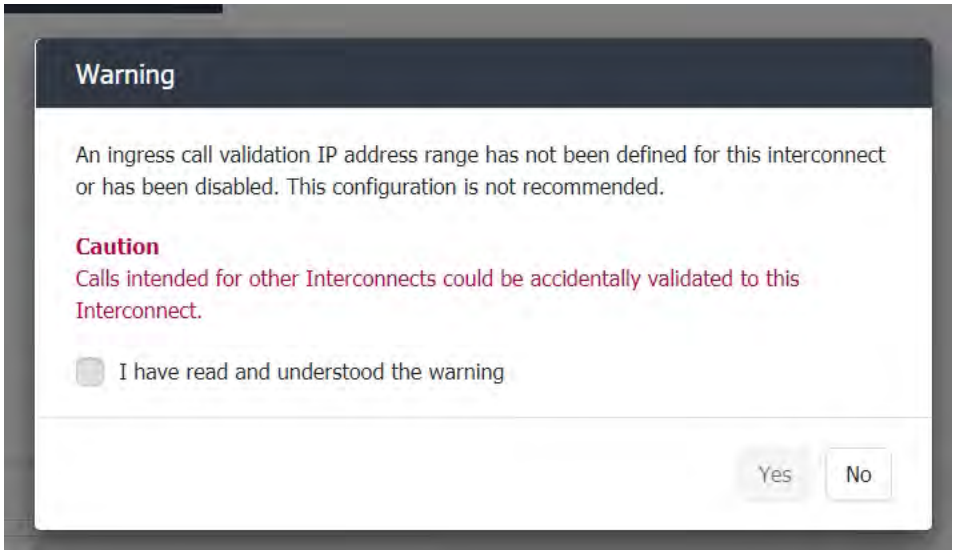
Therefore, to ensure security, the default behaviour of the platform is to require that an IP address is configured as part of ingress validation.

If your organisation needs to support validation **without** using IP addresses, please contact Digitalk Support to specifically enable this functionality on your Platform.

Furthermore. When these settings have been configured, they will provide security on what would otherwise be a public IP address providing transit for signalling and media. They must therefore be considered and managed in a manner similar to password security for network or database access. There is no way to secure an IP Carrier group if these settings become known and are spoofable.

Warning Message

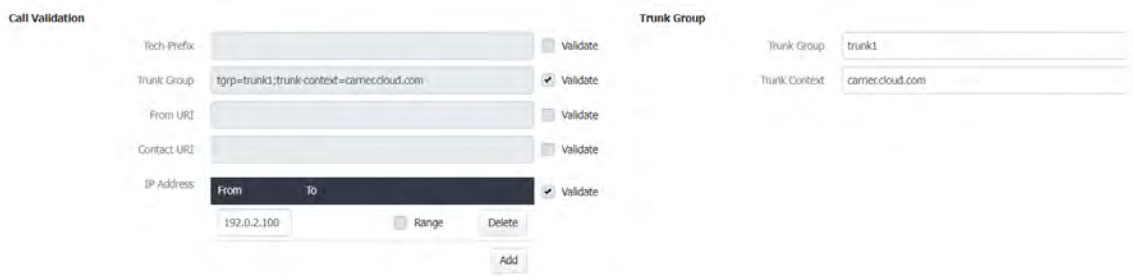
If no IP address range has been defined for this Inbound Interconnect when endeavouring to "Save" this page, the following warning message will be displayed.



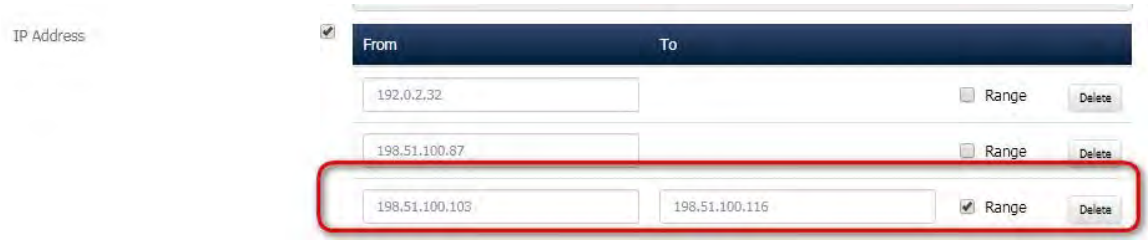
This warning message must be actively acknowledged by selecting the "I have read and understood the warning" message in order to save an Interconnect in this state.

This is to ensure that interconnects are not accidentally configured in this way.

See the table below for further information on validation options.

Method	Description
Tech-Prefix	This validation method checks that the INVITE message begins with a pre-arranged prefix (often referred to as a Tech-Prefix) that has been added as an authentication/identification method by the switch sending the traffic. When the prefix has been matched, it is immediately removed by the Carrier Cloud Platform so as not to confuse routing logic. Example: **1234**4419084250000@address.com In this example the tech-prefix is: 1234 **Tip:** It is strongly recommended to use the Tech-Prefix when validating inbound traffic.
Trunk Group	This validation method supports validation using Trunk Group, in accordance with RFC4904 and is designed for internetworking "Core Routing Engine" environments, rather than direct communication with Customers and Suppliers. Reference: See Section "Understanding Trunk Groups " on page 238 for further information. To validate based upon Trunk Group first select the "Validate" checkbox for the (read-only) Call Validation >Trunk Group field. Then enter the "Trunk Group" and "Trunk Context" in the "Trunk Group" section (as documented below); doing this will automatically populate the read-only "Trunk Group" field in the Call Validation section. 

	Note: It is not possible to type directly in the “Call Validation >Trunk Group”. The only way to populate this information is through the “Trunk Group” section. It is expected that Trunk Group Validation is combined with IP Address validation, as this is mandatory by default on the Digitalk Carrier Cloud. Contact Digitalk support if you need Trunk Group only validation.
From URI	This validation method checks the domain element of the From Address in the SIP header. This field validates on the string entered, and the % symbol can be used as a wild Card if required. Example: 123@sip.mydomain.com - would match calls presented from that address. %sip.mydomain.com - would match any calls presented from that domain.
Contact URI	This validation method checks the domain element of the Contact Address in the SIP header. It uses the same validation logic as “From URI” above.
IP address	This validation method checks the originating IP address in the SIP header. IP validation is the most common validation method and **must be used** in all normal production environments. By default validation is configured to single IP addresses - as shown in the screenshot below:  If, in exceptional circumstances, it is necessary to validate from a range of IP addresses, the "Range" checkbox can be selected. As shown below. **Tip:** As a platform security measure, a single range of IP addresses can contain a maximum of 10 individual IP addresses. If absolutely necessary, additional consecutive ranges can be defined. However, such a configuration can impact on platform security, and Digitalk recommend consulting with Digitalk Support to see if alternative solutions can be configured.



Address Type

When using IP address validation, it is also necessary to set the “Address Type” setting. The setting offers two choices:

- Via Address - validation will use the list of Via IP addresses in the SIP Header, including or omitting the last Via address depending on the setting of the “Include Last Via” checkbox.
- Transport Address - validation will use the Source IP address in the Internet Protocol packet.

Tip:

In normal operation Carrier Cloud will be sending and receiving calls directly from Customers and Suppliers over the public Internet.

Therefore the Transport Address setting must be configured.

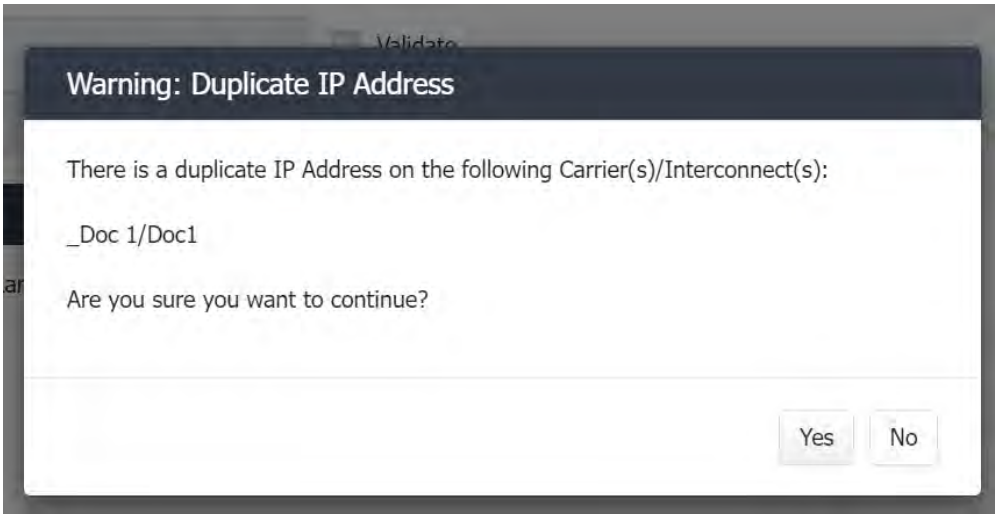
Technical Note:

Duplicate IP Addresses

It is common practice to utilise the same IP address(s) within a single Carrier on multiple interconnects by adding tech-prefixes to the validation to allow the Customer to select a 'service level/product'.

However, it is extremely unusual in normal operations for two separate Customers to share the same originating IP address. (There may be exceptions to this in "internal networking environments" but in normal "business to business" operation this would not be expected to occur.)

Therefore to avoid manual error (accidentally inputting the wrong IP address on the wrong interconnect) a warning is displayed when adding an IP address if it has already been configured on an Interconnect under an alternative Carrier.



4. If an ingress call rate limitation is required; select the “Max Calls Per Second” checkbox, and set the required limit.

Technical Note:
Be aware that this limit applies to an individual SBC cluster.

If the interconnect is assigned to multiple clusters, the same limitation will be set on each.

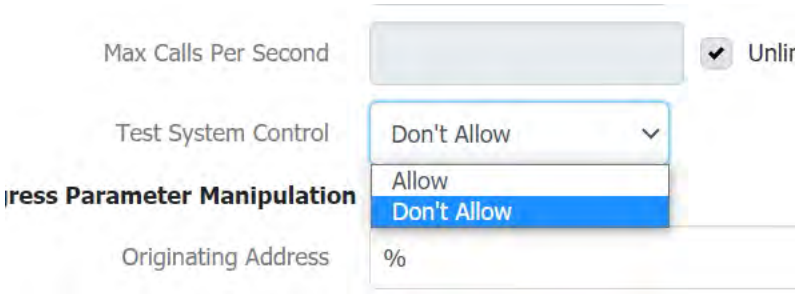
5. Ensure that the "Test System Control" drop-down list box is set to "Don't Allow".

Tip:

Test System Control

The “Test System Control” option must not be selected in normal operation.

This feature is designed for use with automatic or manual testing, and enabling it on a standard Customer Interconnect could result in all traffic being routed without rating or credit control applied.

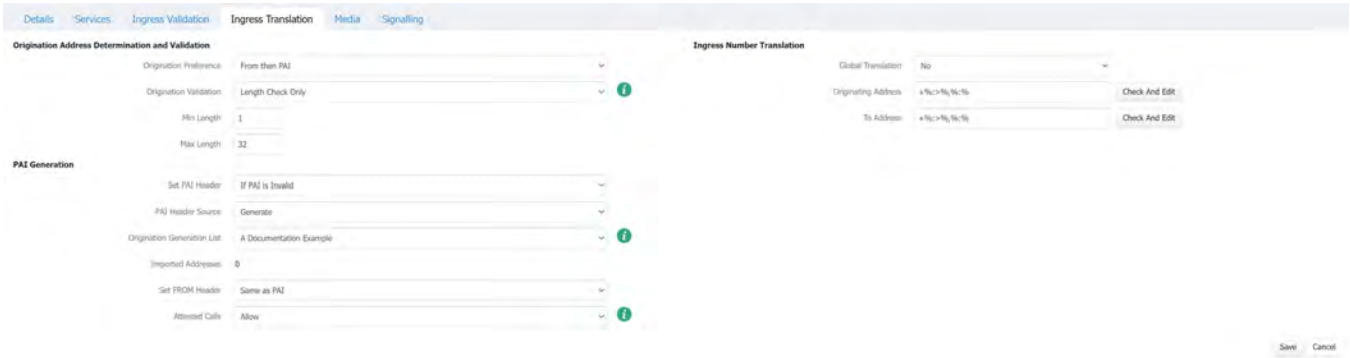


Reference: For further information on Interconnect Testing see the Section "Test Calling Integration" on page 223

6. This section identifies the Trunk Group and Trunk Context headers for this Customer Interconnect.

When used for validation, as described above, these headers will need to be present in the received Invite to successfully validate to this Customer Interconnect.
Alternatively, if the “Trunk Group > Validate” checkbox is not enabled then setting the Trunk Group and Trunk Context fields will set a Trunk Group/Trunk Context for all traffic validating to this Customer Interconnect using an alternative method (such as IP address and tech-prefix). The Trunk Group and Trunk Context headers can then (depending upon configuration) be passed on to a Supplier through the relevant Egress Interconnect.

The Ingress Translation Tab



Technical Note:
The Ingress Translation Tab serves four functions for the Administrator.

- Determines which Origination Header (PAI / From) will be preferred.
- Determines if the presented Origination is considered “valid”.
- Determines if and when the PAI (and From Address) will be generated for calls ingressing on this Interconnect.
- Provides Number Translation options that allow the Administrator to change the presentation of both the Originating Address and Destination Address (remove “+”, leading zeros, etc)

Tip:
There are a number of parameters involved in configuring these options; follow the links below to view dedicated documentation on each subject.

- "Origination Address Identification and PAI Management/Generation" on page 154
- "Supporting Asymmetric Reliable Provisional Responses (100rel)" on page 175
- "Understanding Trunk Groups " on page 238
- "Number Translation Options" on page 1600
- "Global Ingress Number Translation" on page 210
- "Checking and Editing Number Translations Strings" on page 140

1. Ensure that the required Origination Preference is set using the “Origination Preference” drop-down list box. The options available are:

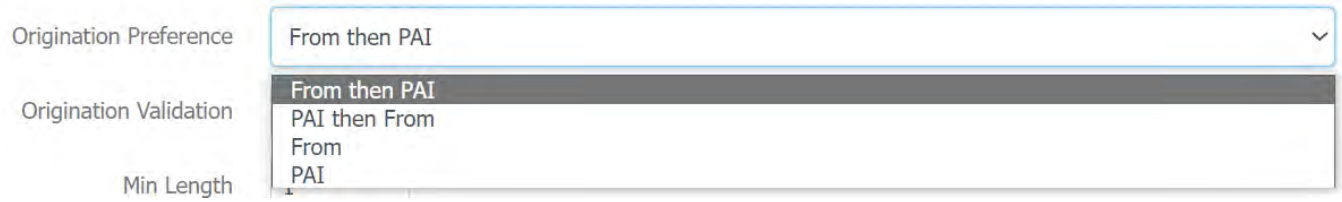
   • From then PAI - When the From Address is of greater or equal validity to the PAI it will be used as the Originating Address within Digitalk Carrier Cloud.

   • PAI then from (Default Option) - When the PAI is of greater or equal validity to the From Address it will be used as the Originating Address within Digitalk Carrier Cloud.

   • From - The From Address will be used as the Originating Address within Digitalk Carrier Cloud regardless of the contents or status of the PAI.

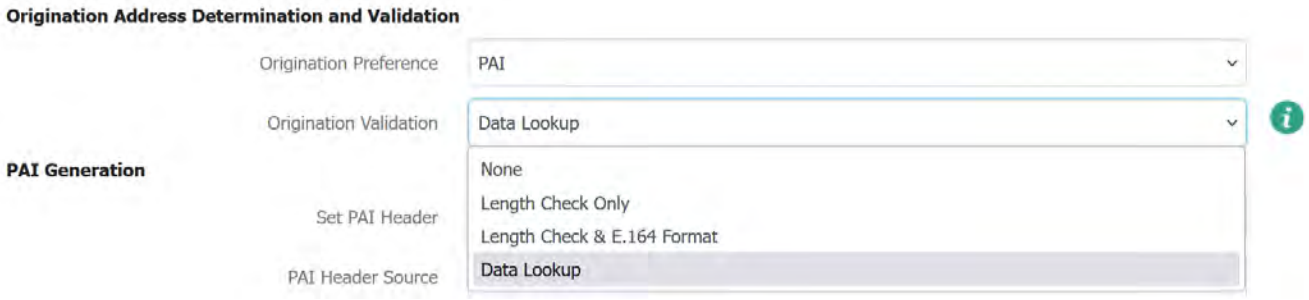
   • PAI - The PAI will be used as the Originating Address within Digitalk Carrier Cloud regardless of the contents or status of the From Address.

   For further information see: "Origination Address Identification and PAI Management/Generation" on page 154



2. If required, determine which form of Origination Validation will be employed by this Customer Interconnect.

   For further information see: "Understanding Invalid/Missing Origins" on page 400 and "Origination Address Identification and PAI Management/Generation" on page 154



Technical Note:

What Can I Do with This Setting?

More information on this setting is provided in the documentation linked above.

However, in summary this setting can be used to determine the validity of the incoming Originating Address.

The result of this check sets a "flag" on the call which is recorded in the CDR and can be reported on using Report Builder. The possible results of the check are as follows:

- CLI validity - not checked
- CLI validity checked – valid
- CLI validity checked – invalid
- CLI validity checked - address missing

Tip:

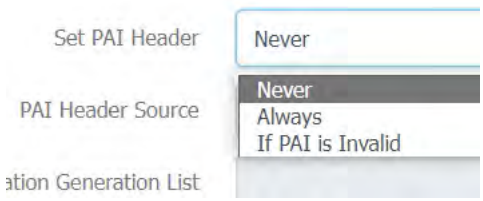
It is important to understand however that the result of the of the validity checked does nothing at this point in the call flow.

Instead the validity status can be used by a number of features within Carrier Cloud to block/allow calls, or to rate and route differently.

For example, an invalid call can be blocked or rated differently on a Customer Rating Plan, blocked or routed differently on a Routing Plan, or blocked from using a particular Supplier Interconnect.

However, a call identified as "invalid" by this check will be routed through the Platform without problem if no further settings relating to this functionality are applied.

3. If the PAI (or From) Header requires generating select the required option from the "Set PAI Header" drop-down box.
   For further information see: "Origination Address Identification and PAI Management/Generation" on page 154

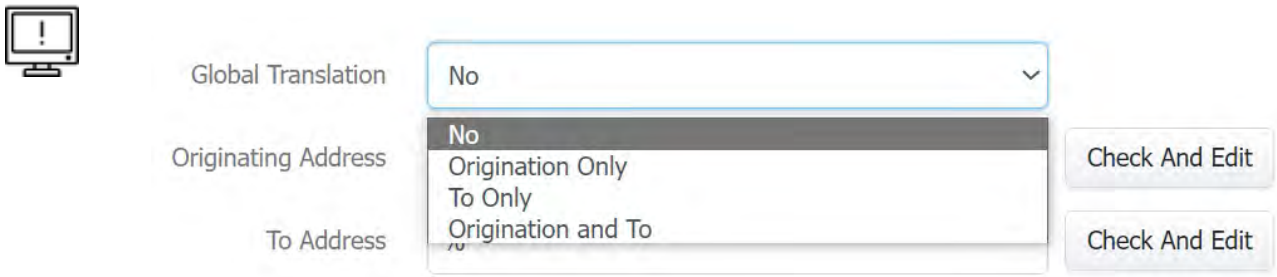


4. If any manipulation of the Originating or Destination Addresses is required at this point configure the “Ingress Parameter Manipulation” settings.

Technical Note:

The number translation options provide a method by which origination and destination (To) addresses can be modified, the most common usage for this is to normalise them to a single format, such as E.164 (without a +).

It is possible to apply a previously configured “global” translation setting using the “Global Translation” drop-down list box, or to enter specific translation string for this interconnect.



Note: Be aware that when using the Global Translation setting it is possible to determine which addresses (origination and/or destination) it applies.

For further information see:

- "Number Translation Options" on page 1600
-
- "Checking and Editing Number Translations Strings" on page 140

Caution:

On Correcting Origin Addresses

It is important to be aware that for all origin-based features on the platform to function correctly (such as Origin Based Rating and Routing) Origination Addresses must be correctly formatted so that they match with both the centralised Origin Codes and Sets for Customer Rating and Routing and the individual Supplier Origin Codes and Sets.

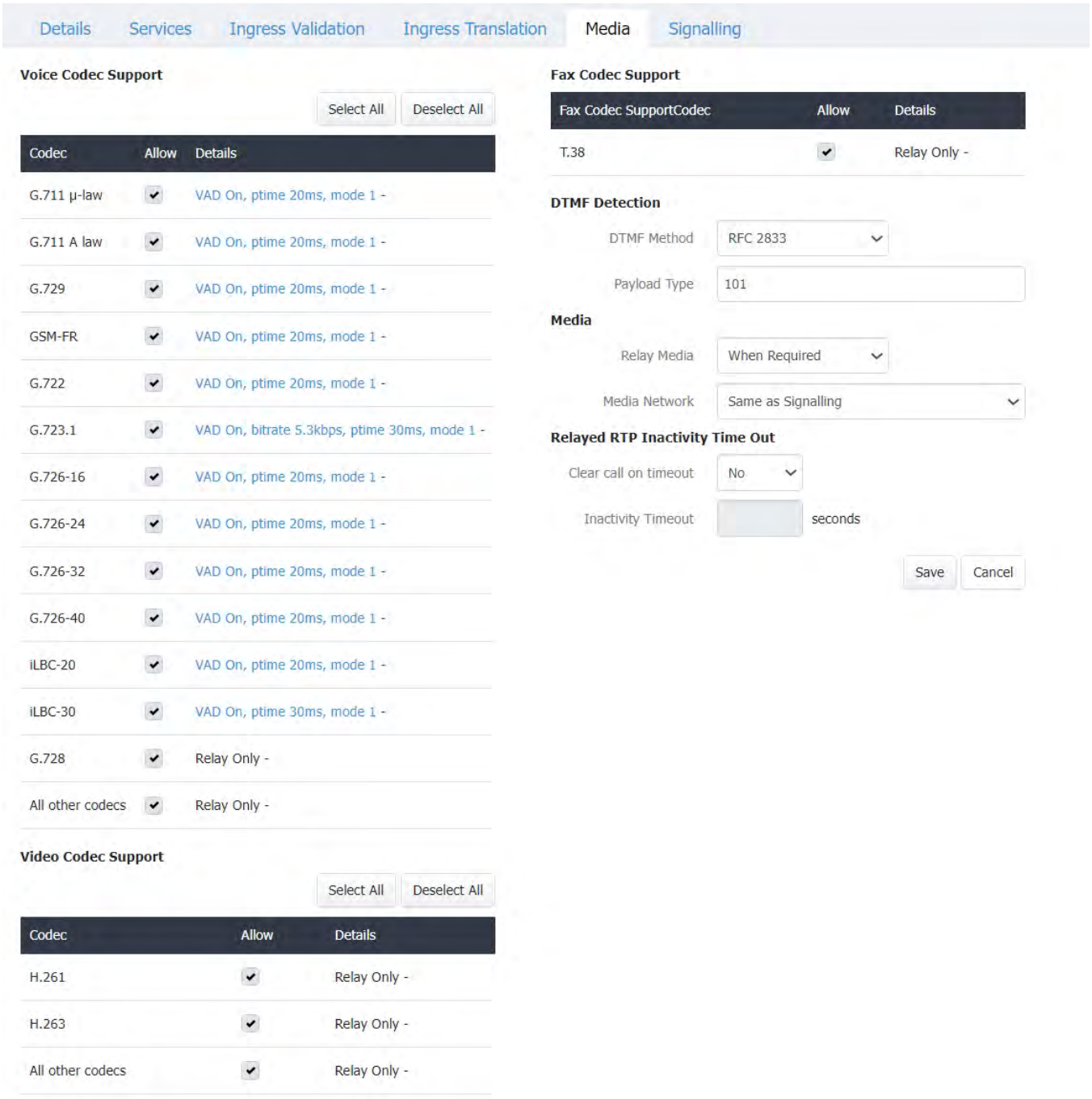
This means, in the same way that Destination Addresses need to be normalised to remove any extraneous prefixes, such as “+” or “00” the same must be done with Originating Addresses to ensure these key functions work correctly.

5. Click “Save”, to save the changes on this screen.

The Media Tab

1. Click the “Media” tab.
   Result: The “Media Configuration” screen is displayed.

2. Click “Edit”.
   Result: The “Media Configuration” settings are available for editing.



3. Configure the Codec support required for this Interconnect.

Technical Note:

Codec Management.

The Codec Management screen provides a list of the most common Codec types that the Carrier Cloud Platform is likely to encounter.

Codecs are divided into two categories “supported” and “relay only”.

With “**relay only**” Codecs (shown on the screen marked with the grey Relay Only text), packets encoded using this Codec can be passed through the Platform, but there is no capacity to manipulate or **transcode** to/from them.this

Supported Codecs can be manipulated and transcoded to/from, (if transcoding is enabled for the call and a transcoding licence is available).

The “Allow” checkbox means that this Codec (or group of Codecs in the case of the “All other Codecs” setting) will be permitted to connect to the Carrier Cloud Platform. To stop a Codec being presented to the Supplier Interconnect as an available option uncheck the “Allow” option.

The order of the Codec list determines the order in which the Codecs are presented to the Supplier Interconnect.

Tip:

Advice on Codec Management

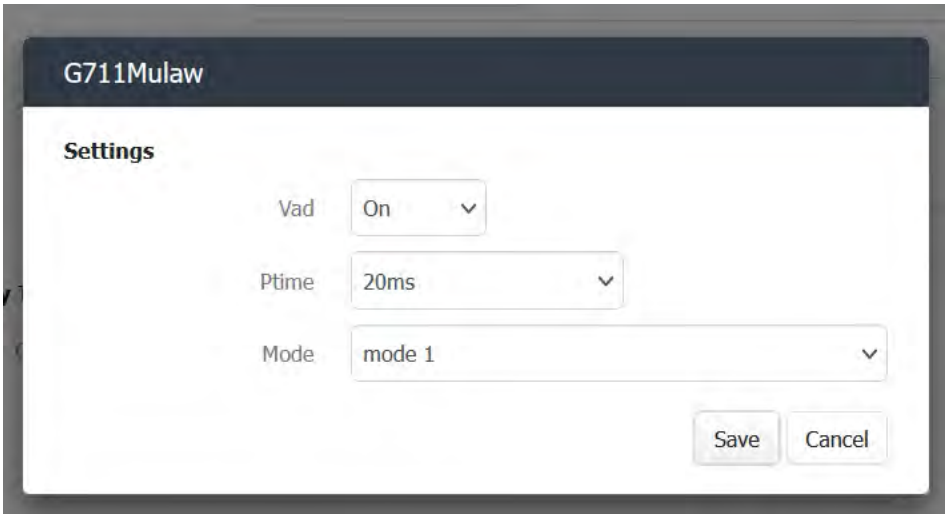
Digitalk advise that in most operational scenarios it is not necessary to restrict Codecs. By not restricting Codecs you allow the Platform to have the best chance of successfully connecting a call and getting the highest possible performance from the Platform.

However, in very specific scenarios where it is required to restrict Codecs the Operator must be aware that removing Codecs from the list will mean that Customers can never route traffic utilising these codecs.

Note:

Manipulating Supported Codecs

Clicking on the details of a supported Codec will present the "Edit Settings" option for that Codec. If required these can then be edited.



Caution:
These settings should be left at their defaults in the vast majority of normal operating scenarios, and must only be altered in consultation with Digitalk Support.

VAD (Voice Activity Detection)

In G.729 and G.723.1 the "VAD" setting in the SDP is directly passed through from the Customer to the Supplier, the setting here is NOT used. However if neither the Customer nor the Supplier has stated a preference for VAD then we will add the preference configured here.

In addition if a Customer's SDP did not include G.729 or G.723.1, and Carrier Cloud is adding these Codecs to the offered list for the Supplier (which will require Transcoding if used) the VAD configuration from Carrier Cloud Manager is used.

In G.711 the "VAD" setting is not set in the SDP, therefore the VoIP Platform will always follow preferences configured on the Customer and Supplier settings.

Packet Duration

The "Package Duration" setting sets the "ptime" (packet time) in the SDP. Interconnects can then support that packet size or choose a different option. Calls on the same Codec but with different packet sizes can be supported by Carrier Cloud without the need for Transcoding.

Modes

Modes have been provided to meet specific interoperability scenarios. The Mode setting must ALWAYS be left at Mode 1, unless specific instructions have been received from Digitalk Support.

4. Take no action with the “DTMF Detection” setting.

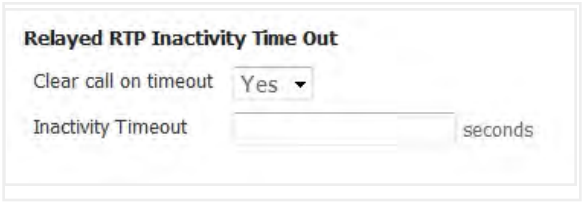
Technical Note:
This setting only has an effect if media is being relayed by the Carrier Cloud Platform and is only used on the Supplier Interconnect.

5. Determine the Media Relay property for this Interconnect.
The default setting is “Always” which provides topology hiding for customers and supplier networks, however other scenarios, such as Open RTP, may require other settings.
See the Technical Note - Relay Media for more information.

6. Ensure that the Media Network drop-down list box remains set to "Same as Signalling".

Note:
This setting must only be changed in consultation with Digitalk Support.

7. Select whether an RTP Inactivity Timeout will be required.



Note:

The Relayed RTP Inactivity Timeout can be used to cancel a call in progress if no RTP packets are received within the designated time period from either the calling or called party.

Note that many devices may not transmit audio during periods of silence on the call, so setting this Inactivity Timeout to a short time period may result in calls in the dropping of calls where no one is speaking.

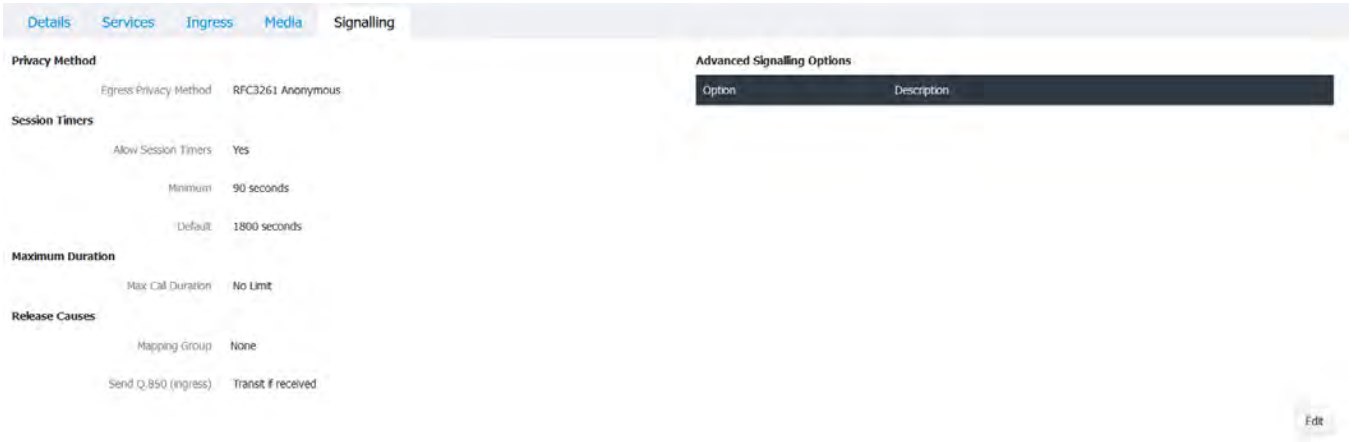
Digitalk recommend in normal operation that this setting is left blank.

8. Click “Save”
   Result: The changes to the screen are saved.

The Signalling Tab

1. Click the “Signalling” heading.
   Result: The “Signalling Configuration” screen is displayed.

2. Click “Edit”.
   Result: The “Signalling Configuration” settings are available for editing.



3. Select the required privacy method for this Interconnect. Choose from:

- RFC3261
- Remote Party ID, and
- RFC3325 P-Asserted Identity.

4. Ensure the Session Timer setting is enabled.

Note:
Session Timers ensure that calls can never be left hanging for extended periods in the event of an exceptional error from the remote Carrier or an SBC failover.

Reference: http://www.ietf.org/rfc/rfc4028.txt

Technical Note:

Session Timers - Further Information

As described in the RFC referenced above, Session Timers are a standard part of the protocol functioning as a "keep alive" mechanism.

Session Timers function by sending occasional UPDATE or additional INVITE (sometimes called a re-INVITE) messages during the call to ensure that both sides remain confident that a signalling path is being maintained.

The responsibility for sending these messages is negotiated during call setup, so this can be the Digitalk SBC or the Carrier's switching device.

Minimum Session Timer

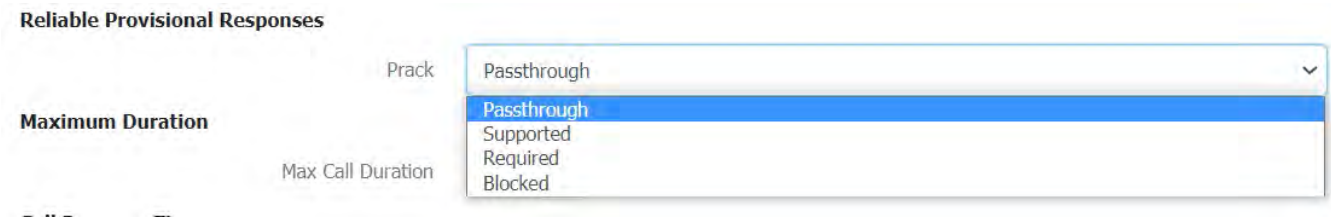
If the Carrier has negotiated responsibility to send the keep alive requests, the Minimum session timer applies. The Digitalk SBC will wait for half of the 90 seconds for a keep alive request. If after 45 seconds (90/2 = 45 seconds) a request has not been received, we will generate a keep alive message and send it to the Carrier. If after another 45 seconds a response has not been received back from the Carrier we will assume that the call is complete and will end it gracefully. 90 seconds is the shortest period of time that can be defined for the Minimum session timer in the SIP specification.

Default Session Timer

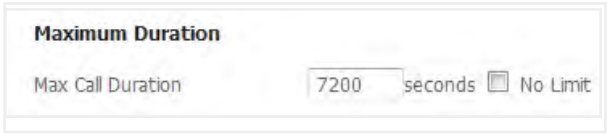
The default session timer applies when the Digitalk SBC has negotiated responsibility for sending keep alive requests. Our default for this setting is 1800 seconds.

This means that we will send a keep alive request every 900 (1800/2) seconds. If the Carrier does not receive a keep alive request after 900 seconds they will send a keep alive request to the Digitalk. If after another 900 seconds they do not receive a response from the Digitalk they will end the call.

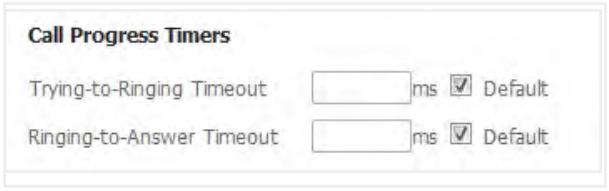
5. If and alternative (asymmetric) Reliable Provisional Response handling is needed for this Interconnect, select the required option.



6. If a “Maximum Call Duration” needs configuring for this Interconnection, unselect the “No Limit” checkbox and set the required call duration.



6. If “Call Progress Timers” are required for this Interconnection, unselect the “Default” checkbox and set the required time outs.



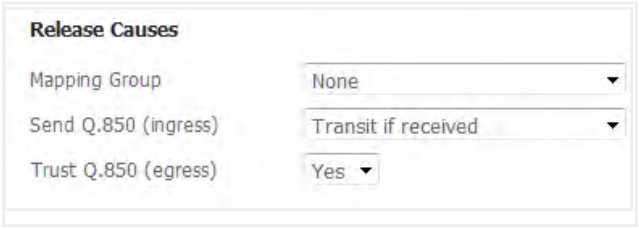
Note:

These timers are designed to deal with a scenario where a Carrier Interconnection sends an initial Trying or Ringing message, but then does not continue by sending a further message to connect or cancel the call.

When this occurs the default SIP timer waits 2 minutes before cancelling the call, and potentially moving onto the next choice in a Routing Plan.

In a live telephony environment a two-minute wait is almost certain to result in the caller hanging up. This setting makes it possible to set a lower timeout, in milliseconds, whereby if the specified message is not received Carrier Cloud will continue to the next routing choice in the Routing Plan and potentially still connect the call.

7. If any Release Cause mapping is required, then configure the required Mapping Group.
Reference: See Section “"Release Cause Mapping" on page 226“ for further information.



8. Click “Save”.
Result: The Interconnect has been configured. this

3.4 Configuring an Supplier Interconnect

A Supplier Interconnect this provide the technical configuration for the communication between the Carrier Cloud and Supplier Partners.

Technical Note:

Renaming Interconnects is not Possible

Please be aware that after an Interconnect has been created it is NOT possible for it to be renamed.

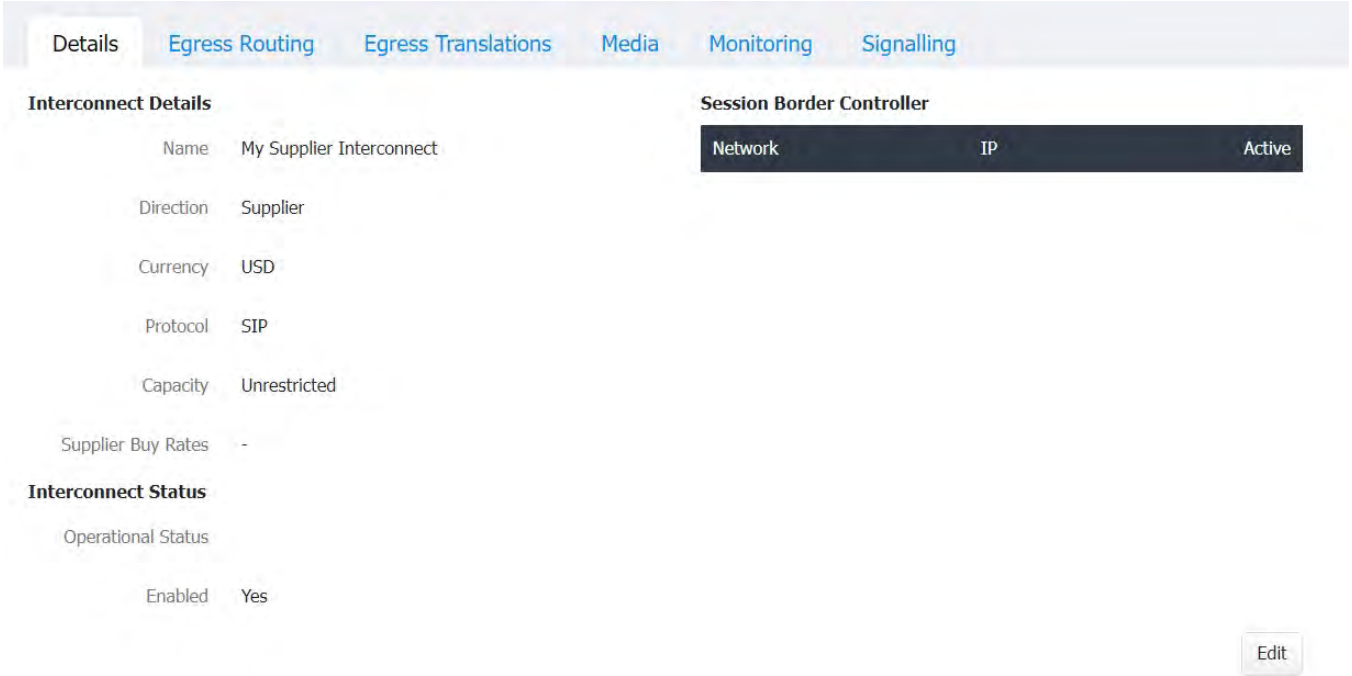
The reason for this is related to ensuring continued data integrity in the CDRs over the long term.

If an interconnect has been named incorrectly, then it can be deleted and recreated; or if it has already been configured then it can be copied with a new name and the original then deleted.

Follow the steps below to configure a SIP Interconnect to route egress traffic to Supplier Partners.

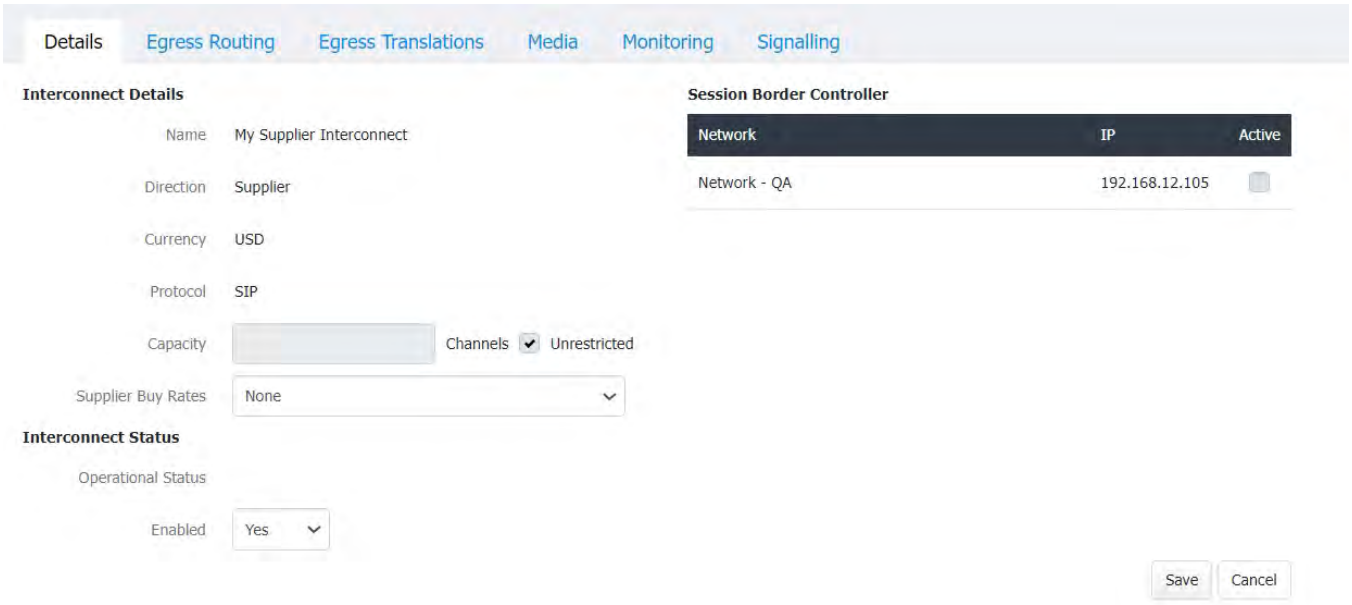
1. Click on the name of the Interconnect to be configured.

Result: The “Interconnect Management” screen is shown displaying a summary of the information regarding the Carrier Interconnect.



2. Click “Edit”.

Result: The “Details” screen can now be configured.



3. If required, deselect "unrestricted" and enter a Channel Capacity limit in the “Capacity” field.

Note:
When configured this setting restricts the number of simultaneous calls that will be sent to this Interconnect at any one time.

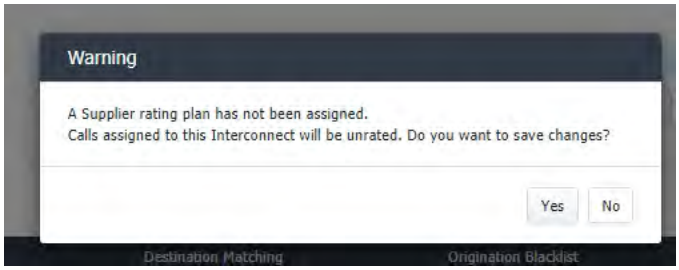
If this limit is reached, then the Interconnect will not be used on a Routing Plan and a subsequent Routing choice will be taken if so available

4. Select the appropriate Supplier Rating Plan for this Interconnect using the “Supplier Buy Rates” drop-down list box.

Note:

While it is not necessary to configure a Supplier Rating Plan for a Supplier Interconnect (it may be desirable in test scenarios) failure to do so will mean that calls that are sent to the Supplier Interconnect will not be rated.

A warning message will be displayed if you try to Save this a Supplier Interconnect without configuring this setting.



Technical Note:

Supplier Interconnects with no Rating Plan Applied

The Platform Operator has a choice determining what occurs in this scenario when a call is routed to a Supplier Interconnect that currently does not have a Supplier Rating Plan enabled when Margin Enforcement has been enabled on Customer Rating.

From Carrier Cloud Release 6.1 Margin Enforcement will block calls being sent to such a Supplier Interconnect where it does not have a Supplier Rating Plan configured. This is a change of behaviour from previous versions of the software.

If your organisation requires the original behaviour whereby calls would be passed in this scenario, a system setting is available to re-enable that.

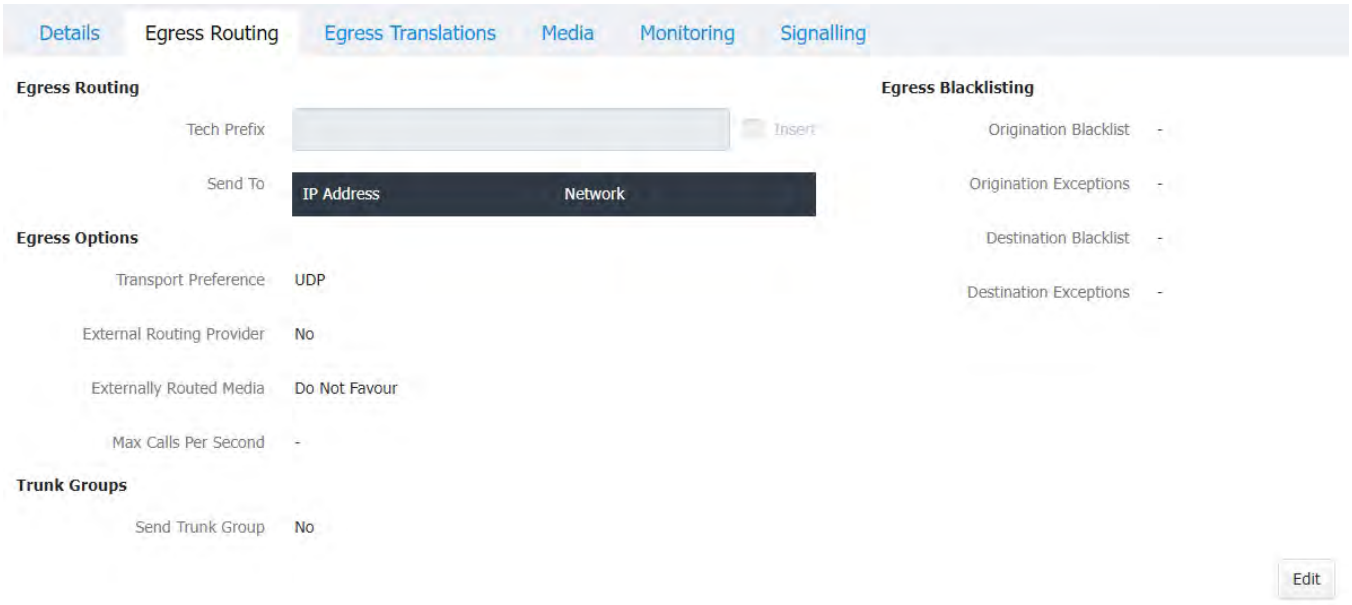
Please contact Digitalk Support to enable that option if required.

5. Select the Signalling IP address from which this Interconnect will be sending traffic.

6. Click “Save”.

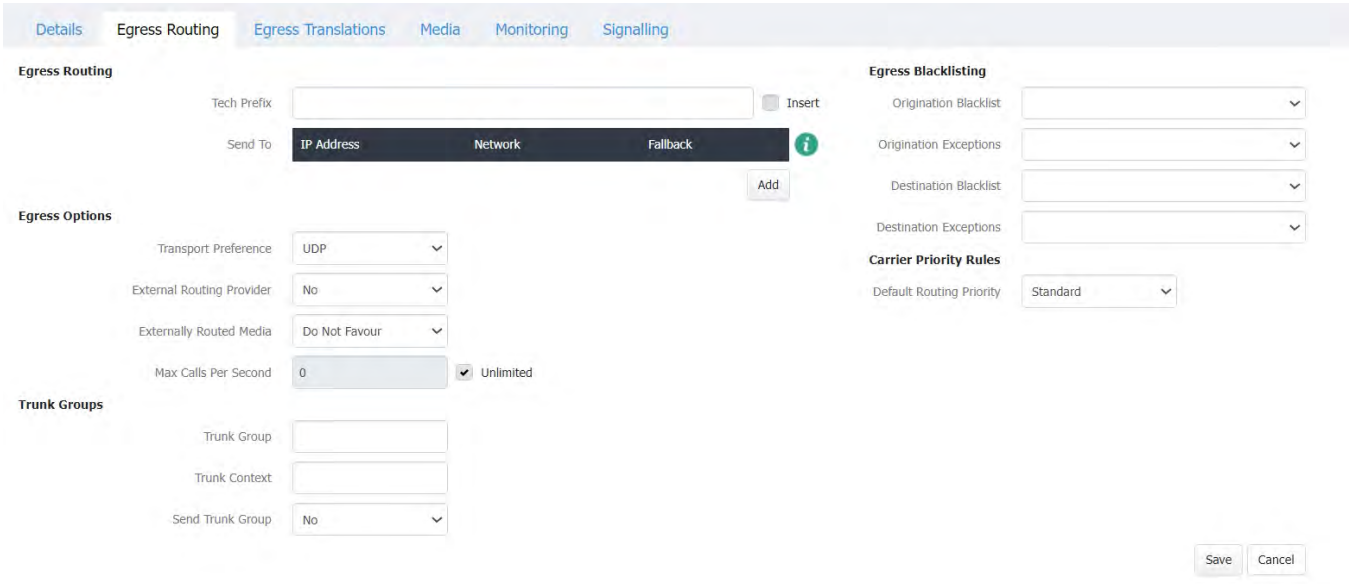
Result: The Details screen has now been configured.

7. Click the “Egress Routing” tab.
   Result: The “Egress Routing” screen is displayed.



Egress Routing

1. Click “Edit”.
   Result: The “Egress Routing” settings are available for editing.



2. Use the table below to complete the Egress Routing configuration.

Field	Tip: Description	Action

<table>
<tr><td>Tech-Pre-fix</td><td>Determines if a tech-prefix will be added to the Destination Address when the call is sent out of the Carrier Cloud Platform.</td><td>If required, select the “Insert Request-URI Prefix” check-box and enter the required prefix.</td></tr>
<tr><td>Send To</td><td>Determines the IP address(es), and where necessary the Network, that the egress traffic using this Supplier Interconnect will be sent.

Technical Note:

Egress IP Technical Notes

Fallback IP(s)

When adding multiple IP addresses, it is possible to mark an IP address as “Fallback”.

IP addresses that are not configured as “Fallback” are referred to as “Primary” IP addresses.

This feature is designed to allow IP Addresses to be added that will only be used “in an emergency”, this meaning when all of the “Primary” IP addresses are unavailable.

Calls will only be sent to Fallback IPs where all Primary IPs have been automatically disabled through the Call Monitoring feature.

Distribution between multiple IP addresses on the same Network

If multiple (non-fallback) IP addresses are assigned for the same network then SBC will automatically divide traffic between them by using each address in turn (sometimes known as a “round-robin” distribution).

If it is necessary to control the distribution between two IP addresses belonging to the same Supplier - then do not add them to a single interconnect instead create two</td><td>Click “Add” and enter the required IP address(es).

  </td></tr>
</table>

(or more) interconnects with the specified IP addresses and the required distribution can be created on the Routing Plan.

Network Selection (Geographic Redundancy Scenarios Only)

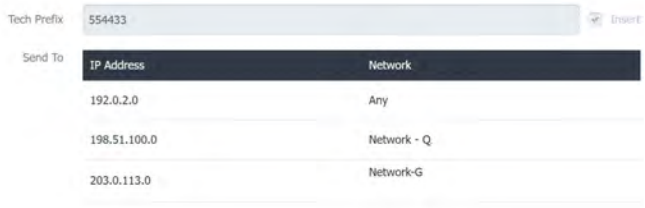
When adding an IP address the “Network” drop-down list box will also become available.

This feature is designed to provide IP control for Customers operating using Geographic Redundancy over multiple networks.

For Platforms operating with only a single Network and on a single Point of Presence no additional selection is possible and the default setting of “Any” cannot be changed.

However, for Platform Operators operating **Geographic Redundancy** where the same Supplier is connected on differing Networks, representing different Points of Presence, this feature allows a Network Administrator to identify if an IP address is present on all networks, or only on a single network.

As shown in the screenshot below:



This means that when the Supplier Interconnect, with multiple IP’s on specific networks, is used to send traffic on a Routing Plan only the appropriate IP address(es) for

	the network being used by the Call will be selected.	
Egress Transport Preference	Determines what transport protocol will be used. Select from: ■ UDP (the default and most commonly used.) ■ TCP, and ■ TLS	Select the required transport protocol.
External Routing Provider	This setting is used when the Digitalk Carrier Cloud Platform is being used in conjunction with a third party routing provider. **Caution:** This setting is only to be used if specifically agreed with your Digitalk Account Management Team.	Leave this setting at "No", unless specifically instructed otherwise because an additional routing Platform is being utilised.
Externally Routed Media	This setting is only relevant in Platforms that have multiple physical points of presence. In such installations selecting this option will minimise the distance travelled over the internal network by the RTP. **Caution:** This setting should only be used if specifically agreed with your Digitalk Account Management Team.	Leave this setting at "Do Not Favour", unless specifically instructed by your Technical Manager/Digitalk Support.
Max Calls Per Second	This setting determines the maximum rate of calls (Calls per Second) that the Carrier Cloud Platform will send through to the Supplier.	If required, select the checkbox and enter the required calls per second limit.
Trunk Group	This Routing method supports validation using Trunk Group, in accordance with RFC4904 and is designed for internetworking "Core Routing Engine" environments, rather than direct communication with Customers and Suppliers.	

	Reference: See Section "Understanding Trunk Groups " on page 238 for further information.	
Send Trunk Group	If enabled, this setting will pass through to the Supplier the “tgrp” and “trunk-context” header from an inbound call (where present). Reference: See “"Understanding Trunk Groups " on page 238” for further information on Trunk Groups	
Blacklists	This setting will apply a Origination and/or Destination Blacklist, and optionally a corresponding Blacklist Exception List, to this Interconnect. When applied calls to numbers/number ranges included on the Blacklist will not be routed to this Interconnect. Unless specifically permitted by the Exception List. Reference: See "Blacklisting" on page 234 for further information.	If required, select an Blacklist/Exception List for this Supplier Interconnect.
Default Carrier Priority Rule	This setting determines the default priority for this Supplier Interconnect via a “Routing Plan Carrier Priority Rule”. Important: Changing this setting for an existing Supplier Interconnect will update the priority for all Routing Plans where a specific Carrier Rule has not already been configured.  **Technical Note:** What does this feature do? "Carrier and Zone Priority Rules" on page 870allow the Administrator to determine if an Interconnect will be included on a particular Routing Plan, and if they are included, to prioritise/de-prioritise the Interconnect in relation to others on the plan when building the routing order. This feature determines the default Carrier priority for a new Interconnect being created on all existing, and future, Routing Plans.  **Caution:** By default, this setting is configured to “Exclude” - meaning that where Carrier Priority Rules are being used the Interconnect will be excluded.	If required, set the "Default Carrier Priority Rule.

Example:

Example Usage: Automatically Exclude until Tested

This feature is sometimes used to automatically exclude a new Interconnect from use on any live Routing Plan until it has completed quality testing.

To do this ensure the Default Carrier Priority Rule is set to “Exclude” (the default setting) until testing has been completed. Then either manually enable the Interconnect on each routing plan required, or edit this setting here to change the global priority for the Interconnect. (See below.)

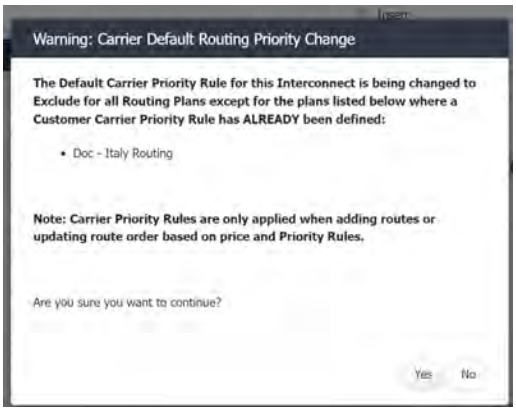
Reference: See "Carrier and Zone Priority Rules" on page 870 for further information on this feature.

Editing this Setting on an Existing Interconnect

If this setting is changed on an existing Interconnect, then the Platform will automatically update the priority setting for this Interconnect on all of the Routing Plans that have been created on the Platform, *unless a specific rule for this Interconnect has already been created* on a Routing Plan.

Example:

The screenshot below shows an example of this:



Here the Default Carrier Priority Rule is being changed to Exclude for all Routing Plans apart from the Routing Plan called "Doc – Italy Routing", because a rule already exists for the Interconnect on that plan.

Scope of Setting

Be aware that changing this setting only updates the Carrier Priority Rule for this Interconnect on the relevant Routing Plans - as with individual rule changes - changing the rule does not immediately have an operational effect on the Routing Plan. To apply the revised priority (priorities) it is necessary to update the plan by running

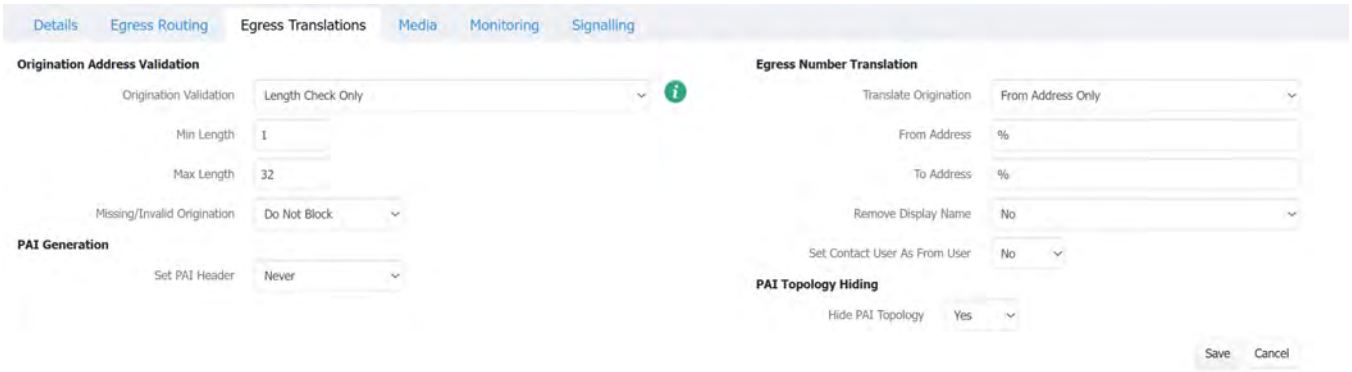
	the “Edit Routing Order Using Priority Rules” wizard.	

3. Click “Save”.

Result: The Egress Routing screen has now been configured.

Egress Translations

4. Click the “Egress Translations” tab.
   Result: The “Egress Translations” screen is displayed.



1. If there is a requirement to manipulate/generate the Originating Address for this call configure the Originating Address Validation and PAI Generation fields as required.

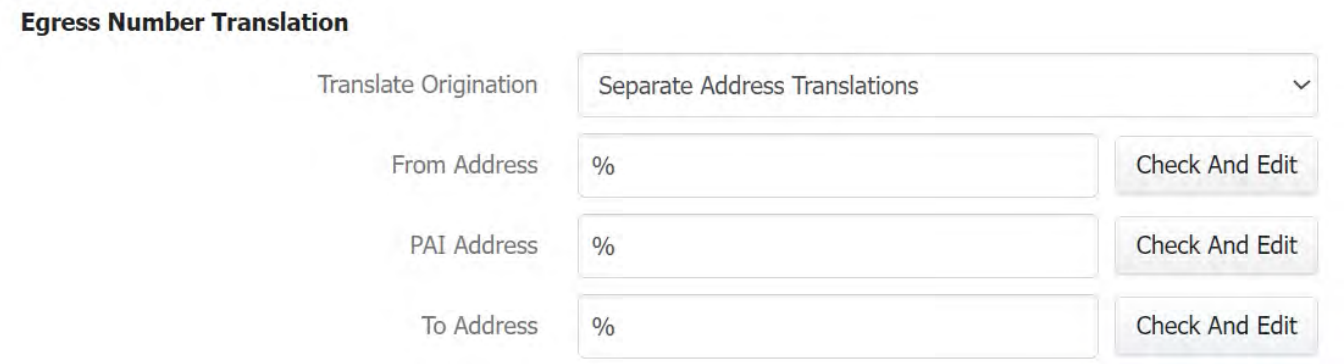
Reference: See "Origination Address Identification and PAI Management/Generation" on page 154for further information.

2. Determine if this Egress Interconnect will permit traffic to be passed through it that has a Missing or Invalid Origination Address.

Note: The drop-down list box provides two options; the default option of "Do Not Block" which will pass missing/invalid traffic, and the alternative option "Block" which when set will not allow missing/invalid traffic to use this Interconnect.

Reference: See "Understanding Invalid/Missing Origins" on page 400 for further information.

3. If any manipulation of the Originating (It is possible to translate either both the From and PAI together using the same setting, or separately) or Destination Addresses is required at this point then configure the “Default Number Translation” settings.



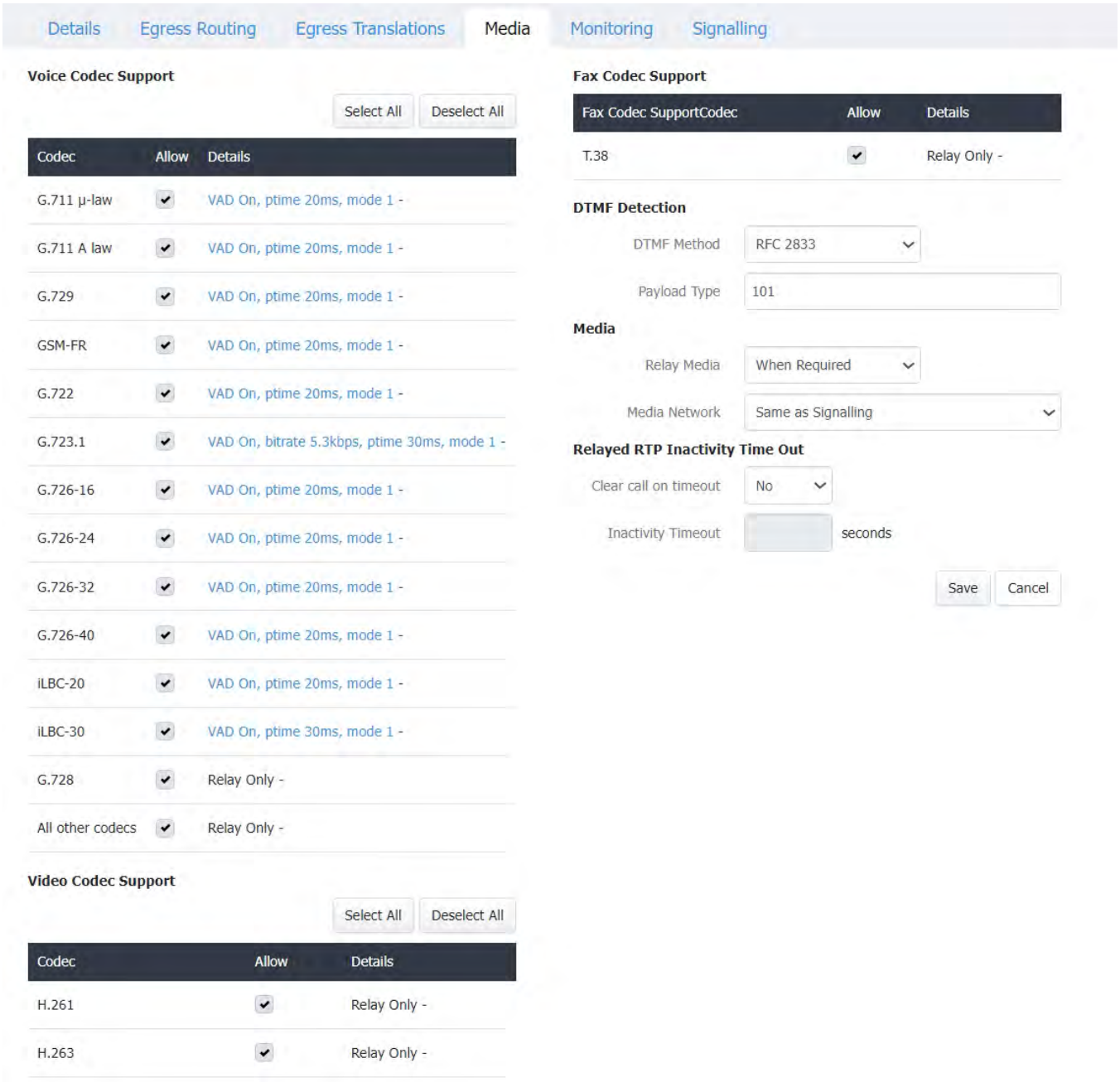
Reference: See "Number Translation Options" on page 1600 and Checking and Editing the Number Translation String for further information.

4. If the traffic being sent to this Supplier Interconnect requires the 'Display Name' to be stripped from the signalling (to/from or both) select the required option from the "Remove Display Name" drop-down list box.
5. If the traffic being sent to this Supplier Interconnect requires the 'Contact User' field in the signalling to be set to the same value as the 'From User' then set the "Set Contact User As from User" drop-down list box to "Yes".
6. Click "Save"
   Result: The changes are saved.

5. Click the "Media" tab.
   Result: The "Media Configuration" screen is displayed.

Media Configuration

1. Click "Edit".
   Result: The "Media Configuration" settings are available for editing.



2. Configure the Codec support required for this Supplier Interconnect.

Technical Note:

Codec Management.

The Codec Management screen provides a list of the most common Codec types that the Carrier Cloud Platform is likely to encounter.

Codecs are divided into two categories “supported” and “relay only”.

With “relay only” Codecs (shown on the screen marked with the grey Relay Only text), packets encoded using this Codec can be passed through the Platform, but there is no capacity to manipulate or transcode to/from them.

Supported Codecs can be manipulated and transcoded to/from, (if transcoding is enabled for the call and a transcoding licence is available).

The “Allow” checkbox means that this Codec (or group of Codecs in the case of the “All other Codecs” setting) will be permitted to pass through the Carrier Cloud Platform. To stop a Codec being presented to the Supplier Interconnect as an available option uncheck the “Allow” option.

The order of the Codec list determines the order in which the Codecs are presented to the Supplier Interconnect.

Tip:

Advice on Codec Management

Digitalk advise that in most operational scenarios it is not necessary to restrict Codecs. By not restricting Codecs you allow the Platform to have the best chance of successfully connecting a call and getting the highest possible performance from the Platform.

However, in a scenario where this it is desirable to send only a specific codec (or to never send a specific codec) to a Supplier the Codec Management features support this flexibility.

Note:

Manipulating Supported Codecs

Clicking on the details of a supported Codec will present the "Edit Settings" option for that Codec. If required these can then be edited.

CAUTION: These settings should be left at their defaults in the vast majority of normal operating scenarios, and must only be altered in consultation with Digitalk Support.

VAD (Voice Activity Detection)

In G.729 and G.723.1 the "VAD" setting in the SDP is directly passed through from the Customer to the Supplier, the setting here is NOT used. However if neither the Customer nor the Supplier has stated a preference for VAD then we will add the preference configured here.

In addition if a Customer's SDP did not include G.729 or G.723.1, and Carrier Cloud is adding these Codecs to the offered list for the Supplier (which will require Transcoding if used) the VAD configuration from Carrier Cloud Manager is used.

In G.711 the "VAD" setting is not set in the SDP, therefore the VoIP Platform will always follow preferences configured on the Customer and Supplier settings.

Packet Duration

The "Package Duration" setting sets the "ptime" (packet time) in the SDP. Interconnects can then support that packet size or choose a different option. Calls on the same Codec but with different packet sizes can be supported by Carrier Cloud without the need for Transcoding.

Modes

Modes have been provided to meet specific interoperability scenarios. The Mode setting must ALWAYS be left at Motthisde 1, unless specific instructions have been received from Digitalk Support.

26. Select the required "DTMF Detection" setting; choose from:

- RFC 2833
- Inband (this setting should only be selected if the G.711 Codec is being used.)
- SIP Info

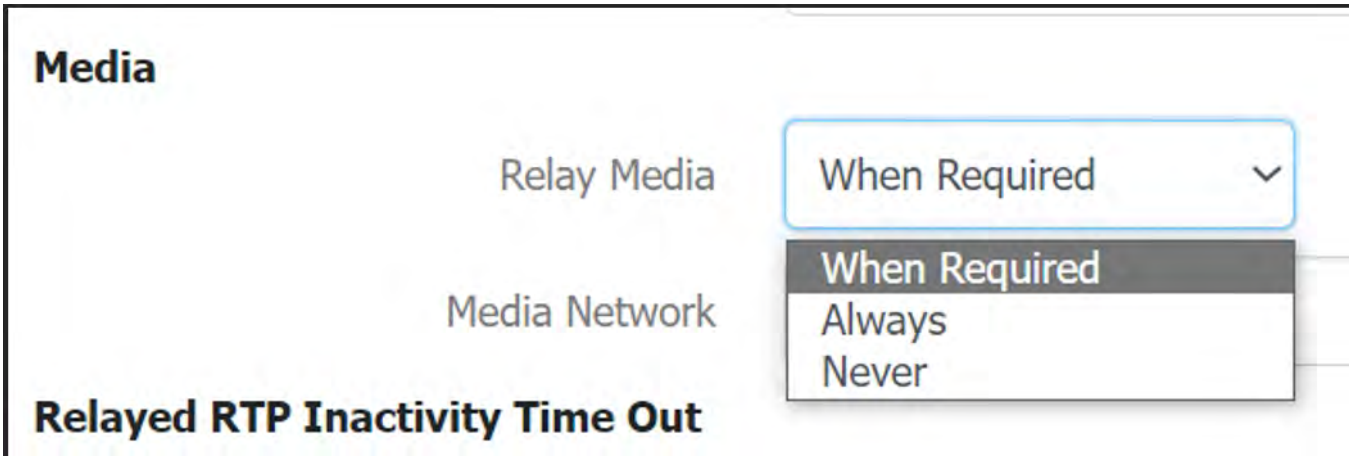
Technical Note:

This setting only has an effect if media is being relayed by the Carrier Cloud Platform.

When this occurs the setting must be configured to the DTMF transit method used by the Supplier, if this is set incorrectly DTMF will not be relayed; or may be relayed incorrectly.

The Inband setting works only with G.7-11 or G.726 (32 or 40 bit variants). If only one Interconnect being used for a call is using Inband then a transcoding licence will be used to convert the DTMF.

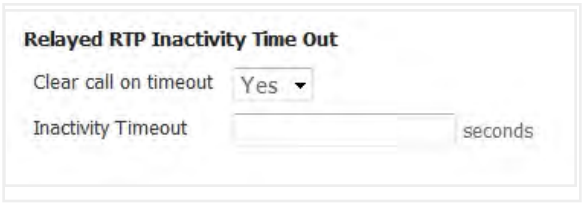
27. Determine the Media Relay property for this Interconnect.
The default setting is “Always” which provides topology hiding for customers and supplier networks, however other scenarios, such as Open RTP, may require other settings.
See the Technical Note - Relay Media for more information.



28. Media Network drop-down list box remains set to "Same as Signalling".

Note:
This setting must only be changed in consultation with Digitalk Support.

29. Select whether an RTP Inactivity Timeout will be required.



Note:
The Relayed RTP Inactivity Timeout can be used to cancel a call in progress if no RTP packets are received within the designated time period from either the calling or called party.

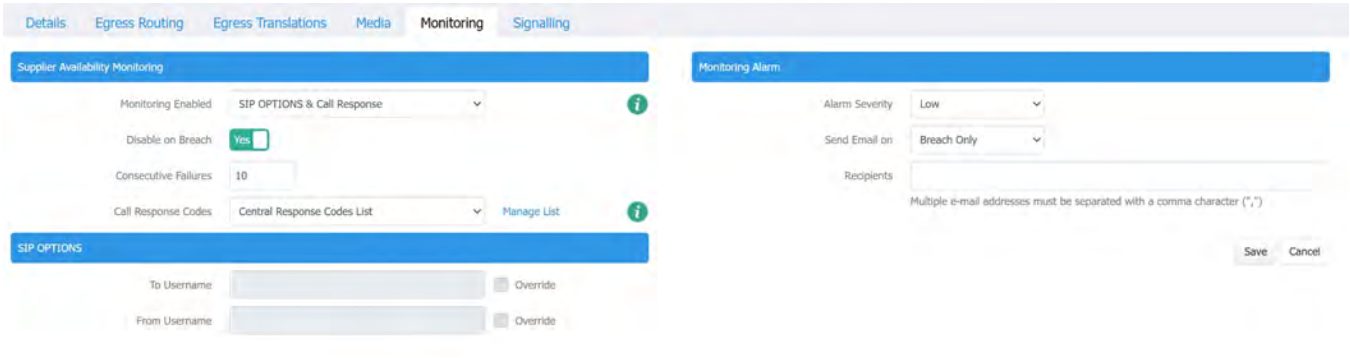
Note that many devices may not transmit audio during periods of silence on the call, so setting this Inactivity Timeout to a short time period may result in calls in the dropping of calls where no one is speaking.

Digitalk recommend in normal operation that this setting is left blank.

7. Click “Save”
Result: The changes to the screen are saved.

Monitoring

1. Click on the “Monitoring” screen.
   Result: The “Monitoring” screen is displayed.



Note:

The Monitoring screen is only relevant to Supplier Carriers, as its role is to monitor the performance of Egress calls made by a Carrier Interconnect.

Therefore the Monitoring heading will only appear when a destination IP address has been saved on the “Egress” configuration page.

This feature differs to Quality of Service Monitoring as this function does not distinguish between different dialling destinations, it is monitoring if the messages being sent to this Supplier Carrier are being acknowledged.

Technical Note:

What Does Monitoring Do and How Does it Work?

The Monitoring settings allow the Platform to automatically disable the Interconnect/IP of non-responsive Suppliers.

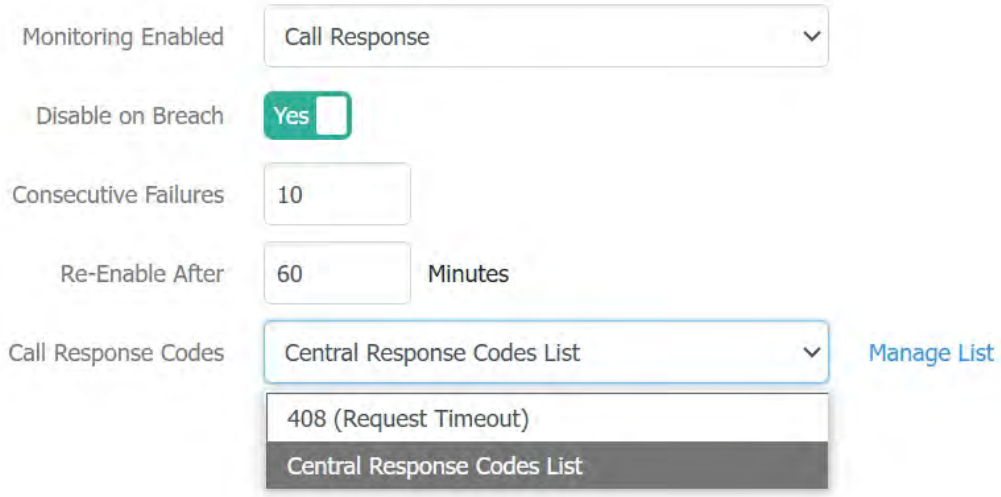
This function works either by monitoring the responses to egress calls and/or by sending a SIP Options message and monitoring the response.

These features can be used independently or together and explained below.

Call Response

The Call Response option works by monitoring the status codes received as a result of an egress call and reacting (either by disabling the interconnect and sending a notification or by only sending a notification) when the “Consecutive Failures” counter is reached.

By default, the only call response code included in this check is '408' – "request timeout". This code is generated when no response is received to an INVITE message sent by the Carrier Cloud to a Supplier Interconnect within 32 seconds of it being sent.



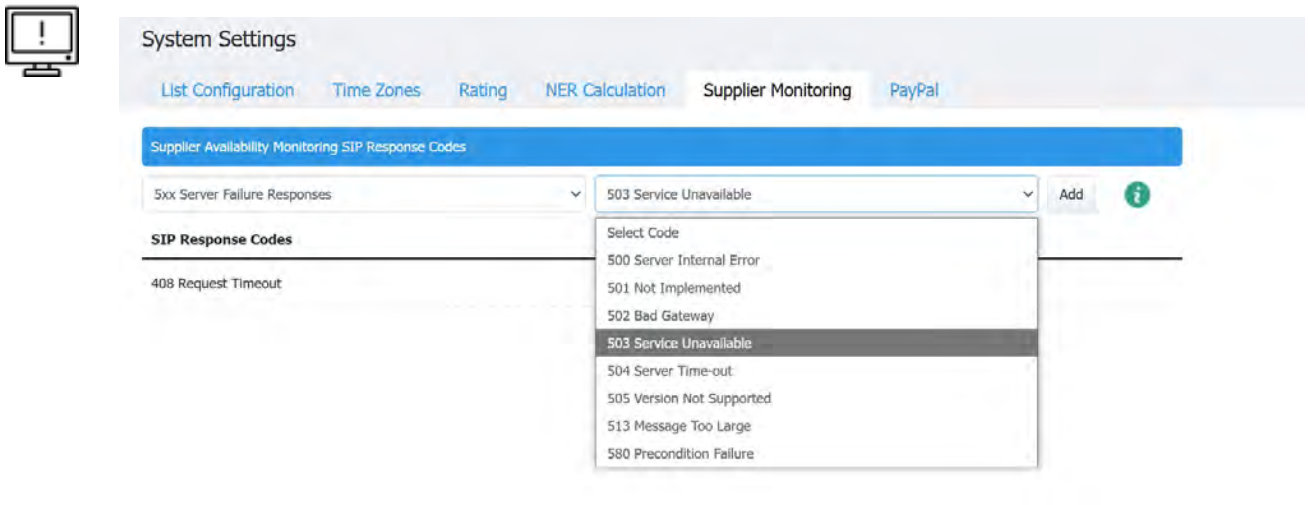
Monitoring Additional Responses - Central Response Codes List

In some circumstances Platform Administrators may wish to include additional call response codes in this Monitoring.

This can be achieved by selecting the "Central Response Codes List" which must have been pre-configured to include the required response codes.

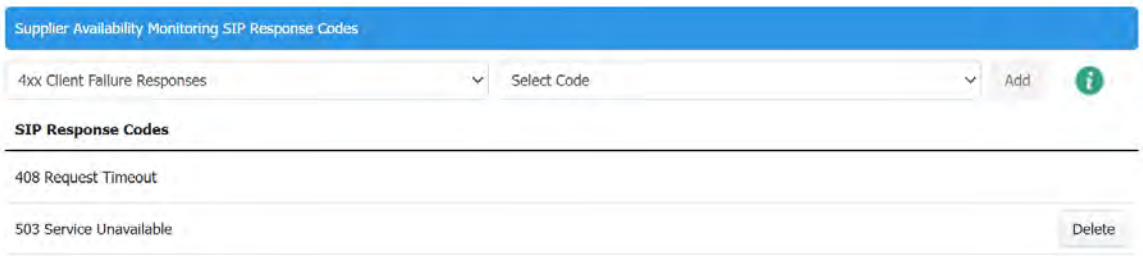
Configuring the Central Response Codes List

The Central Response Code List is accessed through the Admin > System Settings > Supplier Monitoring menu. (Or alternatively, by clicking the "Manage List" link on this screen.)



Screenshot of the “Supplier Monitoring Response Codes” screen.

This screen provides a list of all available SIP Response Codes (408 is ALWAYS monitored). Additional Codes can be monitored by adding them to the list, as shown in the screenshot below where “503 Service Unavailable” has been added.



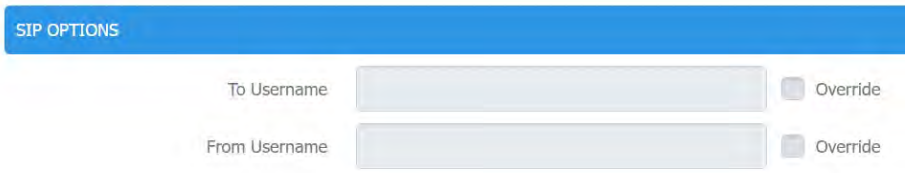
SIP OPTIONS

SIP OPTIONS monitoring does not rely on calls, instead configuring this feature means that the platform will regularly send an OPTIONS message to the Supplier Interconnect to elicit an acknowledgement of “200 OK”.

This acts as a “PING” or “Keep-Alive” message checking if the endpoint is still responding and functioning.

Configuring SIP OPTIONS

In most circumstances it is not necessary to make any configurations changes in order to use SIP OPTIONS as the platform defaults are sufficient. However, the Monitoring screen does allow the Platform Administrator to override the default settings and configure a specific To/From Username where required.



Multiple IP Addresses on a Single Interconnect

If an Interconnect is configured with multiple IP addresses and one of them is found to be non-responsive, then only the individual IP address will be blocked.

This means that as long as the alternative address/es are functioning the Interconnect will remain available for use.

If all IP addresses are non-responsive, then the entire interconnect will be suspended.

Re-enabling

When an Interconnect/IP is disabled by Supplier Monitoring the monitoring methods to determine how it will be re-enabled.

When using SIP OPTIONS, the OPTIONS messages will continue to be sent and the Interconnect re-enabled when a 200 OK is again received.

When just using Call Response this method is not available, and a timer is therefore configured (the default is 60 minutes) at which point the Interconnect will be re-enabled.

Alternatively, it is also possible to manually re-enable an Interconnect/IP disabled by Monitoring by disabling the monitoring feature.

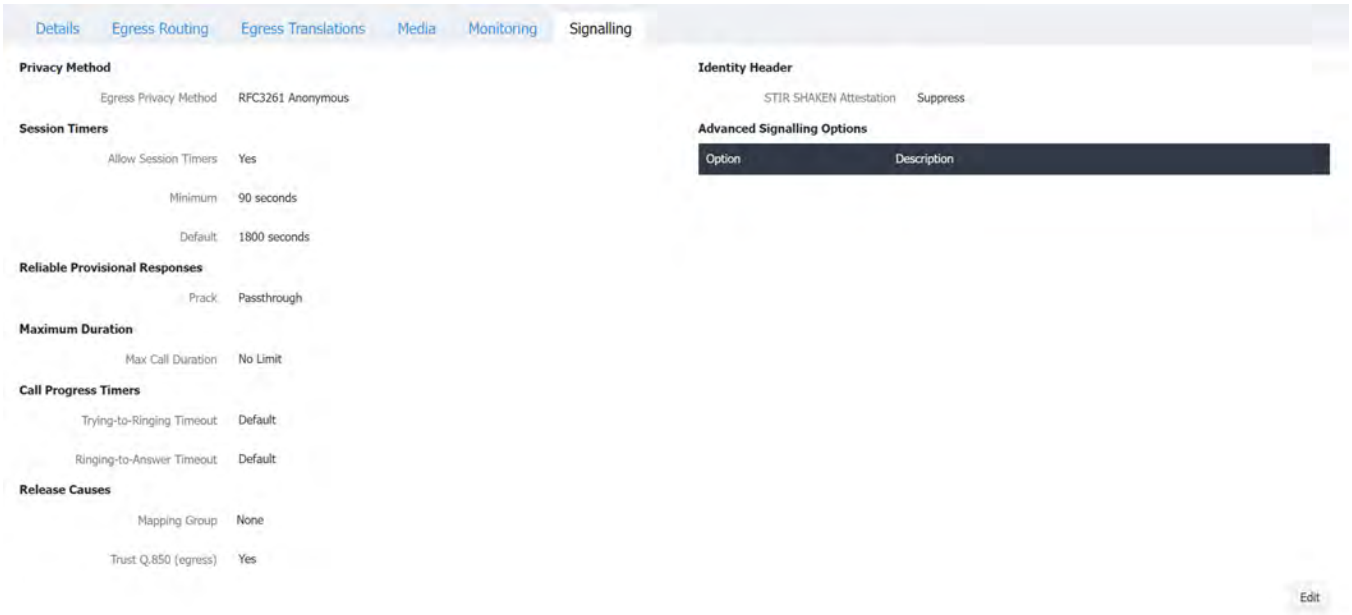
Complete the “Monitoring” section using the table below.

Field	Description	Action
Monitoring Enabled	This option determines if monitoring is enabled. The drop-down list box selects from: ■ None - monitoring is off ■ SIP Options ■ Call Response - monitoring is enabled but SIP Options are not being sent. ■ SIP Options & Call Response - monitoring is enabled and SIP Options will be used.	Select the required option from the drop-down list box.
Alarm Severity	This option determines the level of the alarm that will be generated when there is a monitoring breach. These alarms are monitored in the Alarm Dashboard.	Select the required severity level from the drop-down list box.
Recipients	This option determines the recipients who will receive an email when a monitoring alarm is raised. Leaving this blank means that no email will be sent. Multiple emails can be included by separating them with a comma “,”.	Add the recipient(s) email address(es), as required.
Send Notification on	This option determines if emails will be sent only when a problem is detected, or additionally when the Interconnect is re-enabled and the problem is cleared.	Select the required setting from the drop-down list box.

2. Click the “Signalling” heading.
   Result: The “Signalling Configuration” screen is displayed.

Signalling

1. Click “Edit”.
   Result: The “Signalling Configuration” settings are available for editing.



2. Select the required privacy method for this Interconnect. Choose from:

- RFC3261
- Remote Party ID, and
- RFC3325 P-Asserted Identity.

3. Ensure the Session Timer setting is enabled.

Note:

Session Timers ensure that calls can never be left hanging for extended periods in the event of an exceptional error from the remote Carrier or an SBC failover.

Reference: http://www.ietf.org/rfc/rfc4028.txt

Technical Note:

Session Timers - Further Information

As described in the RFC referenced above, Session Timers are a standard part of the protocol functioning as a "keep alive" mechanism.

Session Timers function by sending occasional UPDATE or additional INVITE (sometimes called a re-INVITE) messages during the call to ensure that both sides remain confident that a signalling path is being maintained.

The responsibility for sending these messages is negotiated during call setup, so this can be the Digitalk SBC or the Carrier's switching device.

Minimum Session Timer

If the Carrier has negotiated responsibility to send the keep alive requests, the Minimum session timer applies. The Digitalk SBC will wait for half of the 90 seconds for a keep alive request. If after 45 seconds (90/2 = 45 seconds) a request has not been received, we will generate a keep alive message and send it to the Carrier. If after another 45 seconds a response has not been received back from the Carrier we will assume that the call is complete and will end it gracefully. 90 seconds is the shortest period of time that can be defined for the Minimum session timer in the SIP specification.

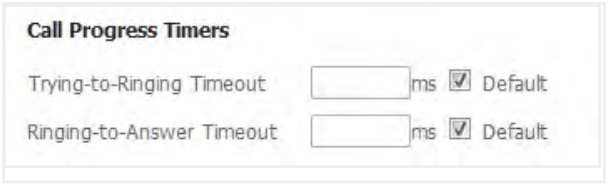
Default Session Timer

The default session timer applies when the Digitalk SBC has negotiated responsibility for sending keep alive requests. Our default for this setting is 1800 seconds.

This means that we will send a keep alive request every 900 (1800/2) seconds. If the Carrier does not receive a keep alive request after 900 seconds they will send a keep alive request to the Digitalk. If after another 900 seconds they do not receive a response from the Digitalk they will end the call.

4. If a "Maximum Call Duration" needs configuring for this Interconnection, unselect the "No Limit" checkbox and set the required call duration.

5. If "Call Progress Timers" are required for this Interconnection, unselect the "Default" checkbox and set the required time outs.



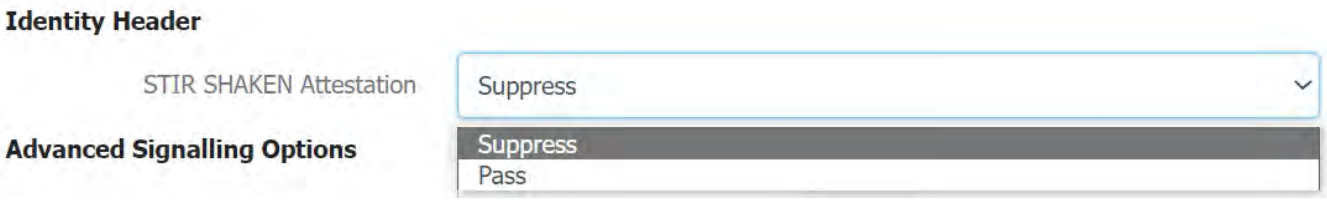
Note:
These timers are designed to deal with a scenario where a Carrier Interconnection sends an initial Trying or Ringing message, but then does not continue by sending a further message to connect or cancel the call.

When this occurs the default SIP timer waits 2 minutes before cancelling the call, and potentially moving onto the next choice in a Routing Plan.

In a live telephony environment a two-minute wait is almost certain to result in the caller hanging up. This setting makes it possible to set a lower timeout, in milliseconds, whereby if the specified message is not received Carrier Cloud will continue to the next routing choice in the Routing Plan and potentially still connect the call.

38. If any Release Cause mapping is required, then configure the required Mapping Group.
Reference: See Section ""Release Cause Mapping" on page 226" for further information.

39. If this Egress Interconnect should pass the STIR/SHAKEN identity header then set the Stir Shaken Attestation drop-down list box to Pass
Reference: See Stir Shaken for further information.



39. Click "Save".
Result: The Interconnect has been configured. this

3.5 Creating a Service

When creating a Customer Carrier the third step in the carrier creation process is to create at least one Service for each Carrier Interconnection.

The purpose of the Service is to determine the Customer Rating Plan and Routing Plan that will be applied to the calls that have been validated to the specified Customer Interconnection.

Services allow the Rating Administrator to:

- Set and change Rating Plans and Routing Plans for the Customer
- Set different Rating and Routing Plans based on time of day, origination number, destination number and digit length.
- Enable Transcoding
- Enable Number Portability

Tip: Supplier Carrier Interconnections do not need a Service.

Technical Note:
For further information on using Centralised Service Matching lists see: "Understanding Service Matching" on page 178

Technical Note:

Maximum Number of Services

Be aware that there is a maximum limit of 3000 Services that can be created under an Interconnect.

However, in normal operation there should be no reason for having extremely high volumes of services such as this. If it is possible that a high number scenario such as this is potentially necessary, please contact Digitalk to discuss operational efficiency and rationalisation.

3.5.1 Procedure for Creating and Configuring a Service

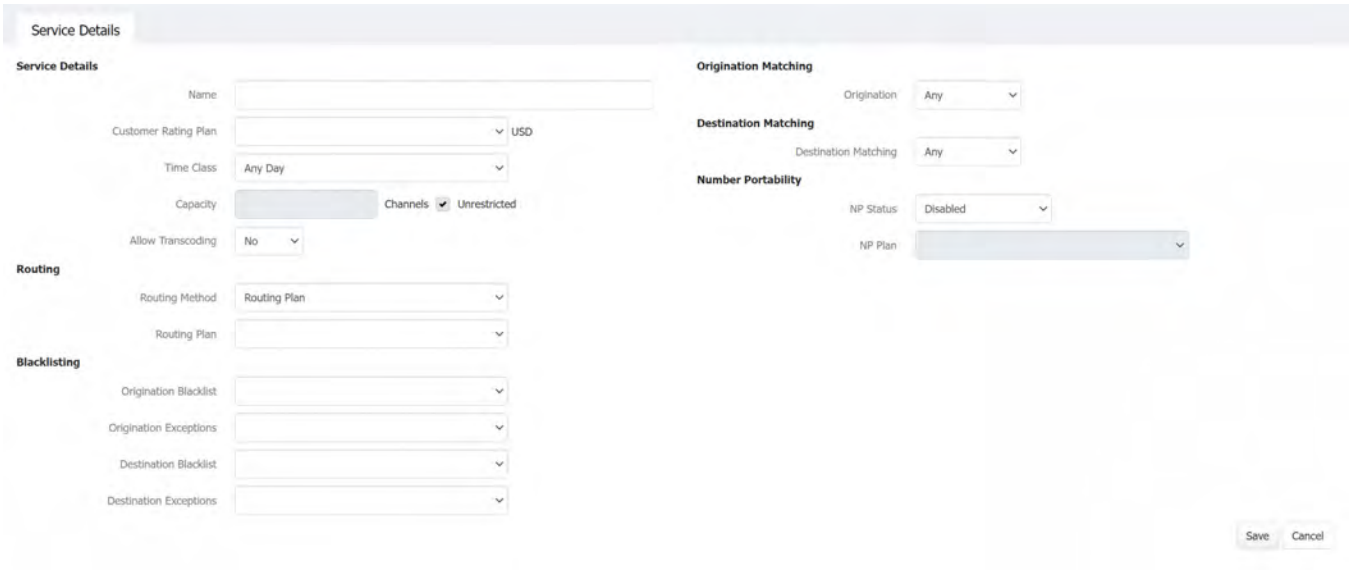
After the Interconnect has been configured, a Service must be added to it to finalise the configuration of the Carrier.

Follow the steps below to configure a Service for an Interconnect.

1. Click on the name of the Interconnect which is to have a Service added to it.

Result: The “Interconnect Management” screen is displayed.

2. Click the "Service" Tab header
3. Select “Add Service” from the “Actions” menu.
   Result: The “Add Service” screen is displayed.

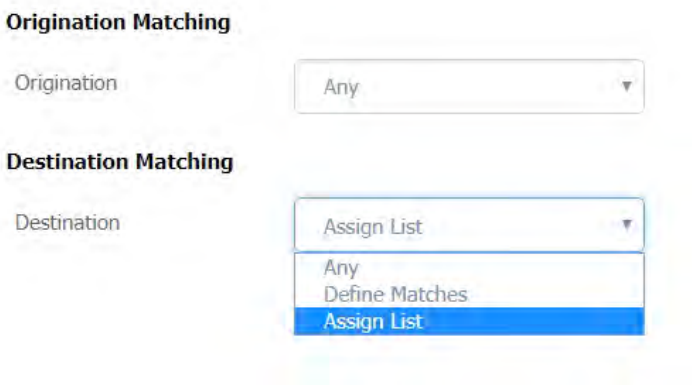


3. Use the table below to complete the settings for the Service.

Field	Description	Action
Name	Determines the name by which this Service will be known.	Enter the required name in the "Name" field.
Customer Rating Plan	Determines the Customer Rating Plan that will be used to charge for calls using this Service. **Note:** Only Rating Plans configured with the same Currency as the Interconnect will be displayed in the drop-down list box. **Caution:** Be aware that while it is possible to leave the Customer Rating Plan field blank this will mean that the rating engine is not engaged for calls passing through this Service. The result of this is that all calls using the service will be routed free. This is by design and can be useful in a test phase, but care should be taken to ensure that this is never set in a live calling environment.	Select the required Customer Rating Plan from the drop-down list box.

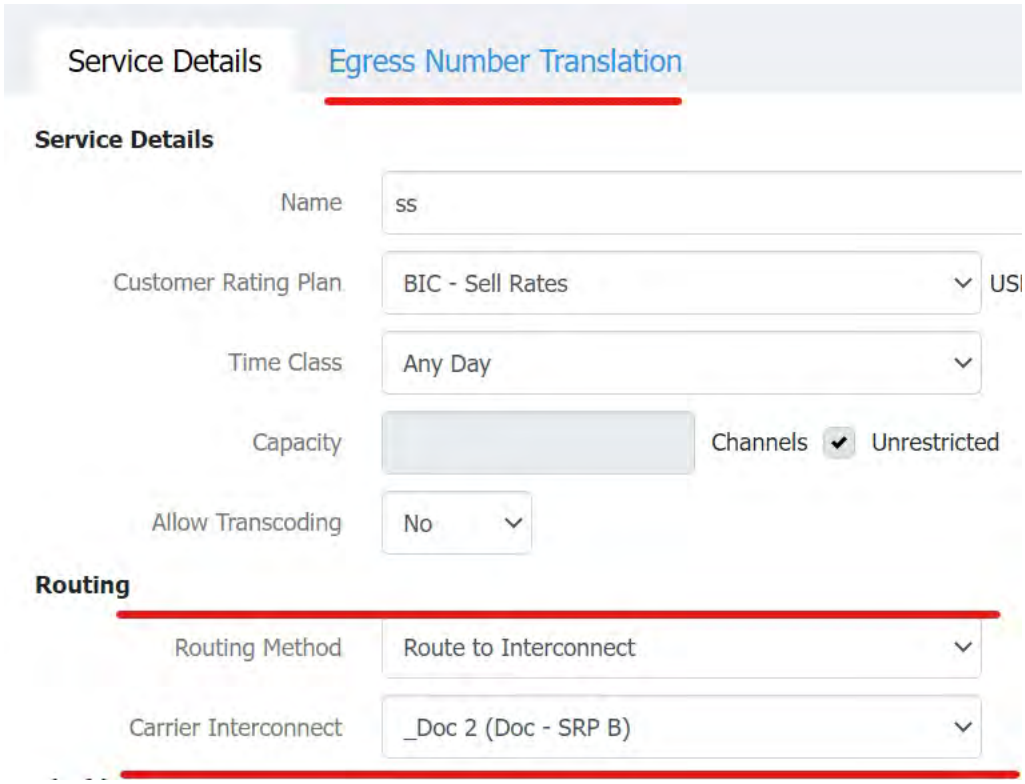
Currency	This is a read only field that records the currency that this service will be working in. The currency will be inherited from the Interconnect, as Services cannot be in a different currency to the Interconnect that they are created under.	No action required.
Time Class	Determines when the Service will be used. To have the Service working all of the time, select the "Anyday" Time Class.  **Note:** Do not leave this entry blank or the Service will not work.	Select the required Time Class from the drop-down list box.
Capacity	This optional setting, determines the capacity of this Service. Enabling this feature provides the option to restrict the total number of calls can use this Service at any one time.  **Note:** If this limit is reached, then additional calls will be rejected without a CDR being written. These rejected calls can be viewed on the "Viewing Calls Rejected by the SBC (Failed Inbound Calls)" on page 1539 screen.	If required, deselected the "unrestricted" checkbox and set the appropriate number of channels.
Allow Transcoding	Determines if transcoding will be allowed when using this Service.	Select "Yes" or "No" from the "Allow Transcoding" drop-down list box as required.
Routing Method	Determines which Routing method will be used. Choose from: ■ Route to Interconnect - which will route calls using this Service to a single Interconnect without using a Routing Plan. This method provides no redundancy. Note: If this option is selected the Egress Number Translation tab (see below) is displayed allowing the option of configuring a specific Translation for this Service .	Select the required Routing Method from the drop-down list box.

	■ Routing Plan - which will route the calls using this Service to a Routing Plan.	
Routing Plan	Determines the specific Routing Plan that the Service will use.	Select the required Routing Plan from the drop-down list box.
Origination Blacklist	This optional setting, applies an Origination Blacklist to this Service. This will prevent calls from a predefined list of Originating Addresses from being routed. Reference: "Blacklisting" on page 234	If required, select a Blacklist.
Origination Exceptions	This optional setting, applies an Origination Exceptions to a Blacklist to this Service.	
Destination Blacklist	This optional setting, applies a Destination Blacklist to this Service. This will prevent calls to a list of predefined Destination Addresses from being routed. Reference: "Blacklisting" on page 234	If required, select a Blacklist.
Destination Exceptions	This optional setting, applies a Destination Exceptions to a Blacklist to this Service.	
NP Status	Determines if the Number Portability look up will be carried out for calls using this service.	Select “Enabled” or “Disabled” from the drop-down list box as required.
NP Plan	If Number Portability has been enabled, and is required, this drop-down list box will determine the Number Portability plan that will be applied to the calls that use this Service.	If required, select the relevant Number Portability plan.
Origination Matching / Destination Matching	Origination/Destination Address Matching is a feature by which a Platform Administrator can restrict the usage of a Service by reference to the origination prefix or address, and/or the destination prefix or address.	If required, configure origination/destination matching as needed.

	A Service can be restricted so that it is only accessible by calls that match a particular Origination and/or Destination address/prefix, or conversely call from a particular Origination and/or Destination address/prefix may be excluded from a specific Service. Two options are available when configuring this feature:  ■ Define Matches - which allows the Administrator to create a specific matching list unique to an individual service, and ■ Assign List - The more powerful and flexible option which allows the creation of a Service Matching List that can be assigned to multiple Services. Reference: See "Understanding Service Matching" on page 178 for more information on creating a Service Matching List.	

Egress Number Translation

If the Routing Method “Route to Interconnect” is selected, then when the Service is saved an additional Tab “Egress Number Translation” will appear. As shown below.



When selected the following screen is displayed:

This Tab allows the Administrator to override the default Origination and Destination Address Translation configured on the Service with a specific Egress Translation that will be applied to the traffic utilising this Service.

Follow the steps below to configure Service Specific Egress Number Translation.

1. Click “Edit”.

Result: The page is ready for configuration.

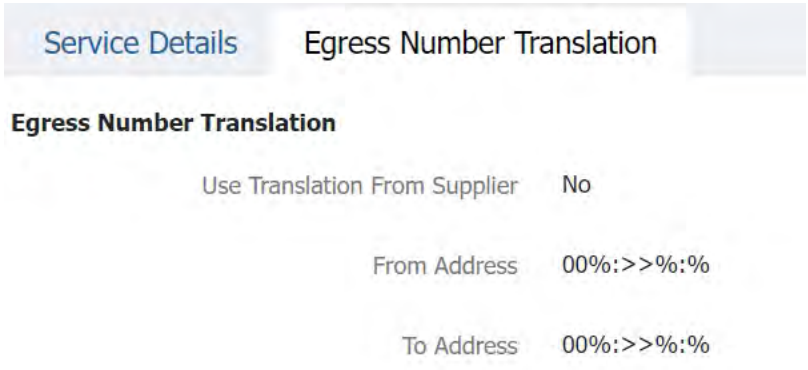
2. Select “No” using the “Use Translation from Supplier” drop-down list box.

3. Configure the required From and To Address Translation.

Reference: "Number Translation Options" on page 1600

4. Click “Save”.

Result: The required translation has been configured.



3.6 Understanding Service Matching

Caution: The total number of code supportable across all Service Matching Lists is 100,000.

Introduction

An important concept in the architectural call flow of the Digitalk Carrier Cloud is to understand that the Service is the point at which the Rating and Routing is determined for the call.

While every Customer Interconnect requires at least one Service, it is possible to create multiple Services under the same Interconnect. This can be done to apply different rating and/or routing for calls based on one of three factors:

- time of day
- origination of the call
- destination of the call

This means that different "choices" can be made for the call flow based on where the call comes from, where the call is going, or the combination of the two.

While it is possible to directly set origination/destination matching on a single Service, this feature is designed for "simple" usage as the settings must be manually configured for each individual Service.

The service matching feature is designed to centralise this functionality by configuring one, or more, Service Matching Lists that can be assigned to one, or more, Services.

This means, for example, an Origination Service Matching List containing all of the prefixes for countries in the European Economic Area could be used to identify European origination traffic across many Services assigned to many different Customer Carriers.

Tip:
While Service Matching Lists always have the capability of being applied to multiple Services, they do not have to be. It is possible to create a Service Matching List and apply it to only a single Customer Interconnect - taking advantage of the ease of number management through the upload of CSVs.

Digitalk recommends a clear naming convention is used in these scenarios to avoid future confusion.

Prefixes/Whole Numbers

It is important to understand that Service Matching Lists can be configured to match either prefixes or whole numbers (or even a combination of the two).

This means that Service Matching Lists can be used to provide whole number "DID" or "Whitelist" matching on destination and/or origination numbers, as long as the total entries in all Service Matching Lists remains below 100,000.

See here for more information here on DID services.

Technical Note:

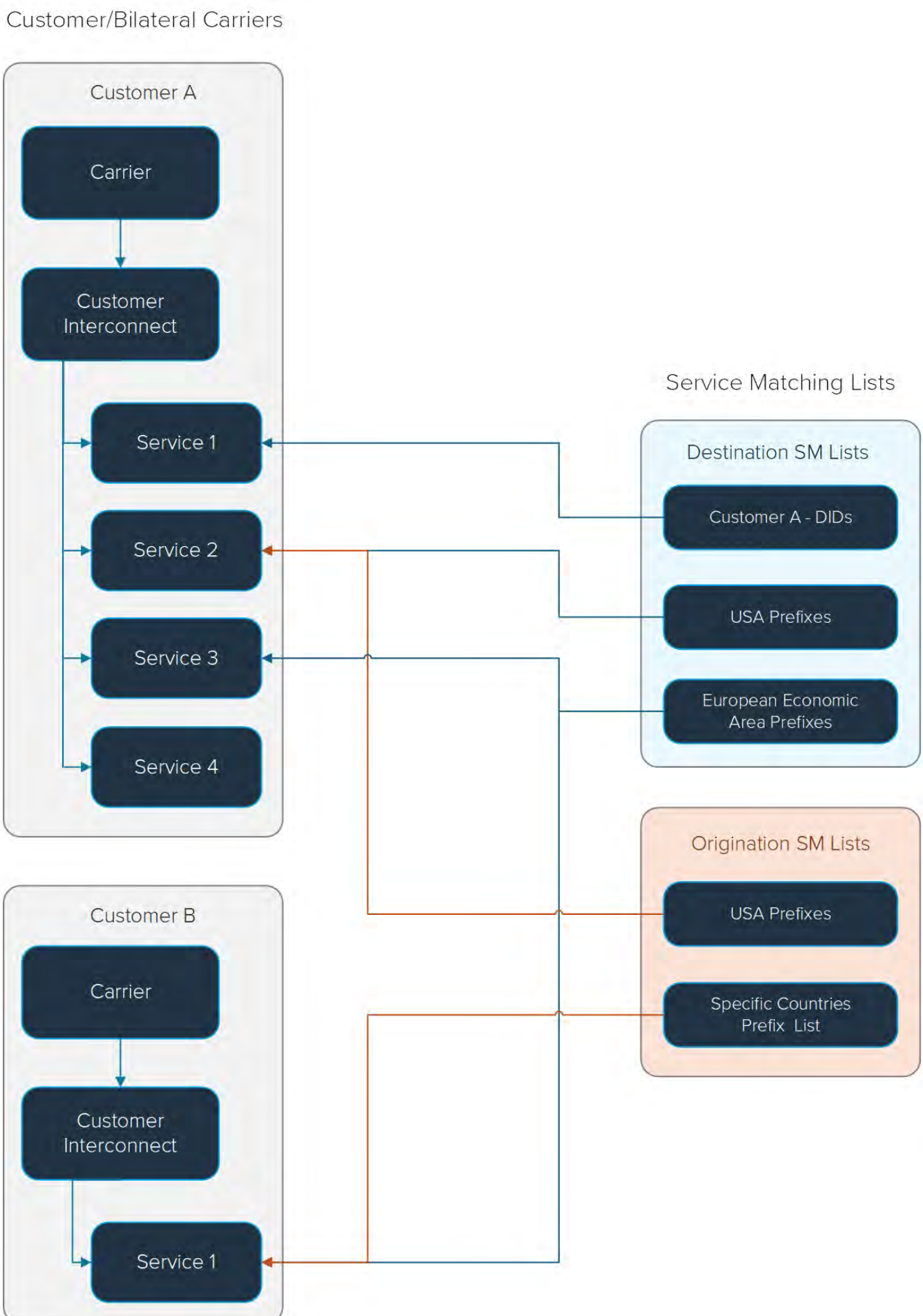
For technical clarity, when we refer to "whole number matching", Service Matching always assumes that the number being matched may be a prefix, even if it is longer than the “standard number length” for the DID in question.

What this means is if a “whole number” such as: 15551234567 is included in a Service Matching List any number longer than this would also be matched. For example, the number 15551234567999 would also match that entry.

It is therefore recommended that service matching for whole numbers is supported by configuring the “Max Digits” setting on the Service Matching List and, where applicable, configuring appropriate Origination Number Validation - preferably the Database Lookup - on the relevant inbound Inter-connect.

Illustration

The screenshot below provides an illustration of how Service Matching Lists can be configured and assigned to single or multiple Services.


Customer/Bilateral Carriers
Customer A
Carrier
Customer Interconnect
Service 1
Service 2
Service 3
Service 4
Service Matching Lists
Destination SM Lists
Customer A - DIDs
USA Prefixes
European Economic Area Prefixes
Origination SM Lists
USA Prefixes
Specific Countries Prefix List
Customer B
Carrier
Customer Interconnect
Service 1

Explanation:

The diagram above shows an extract from a Carrier Cloud Platform.

Two customers are shown, Customer A, whose Customer Interconnect is configured with four Services, and Customer B, whose Customer Interconnect is configured with a single Service.

The Platform has been configured with three destination Service Matching Lists:

- Customer A DDIs - a list of whole number DDIs which have been assigned to the specific Customer.
- USA Prefixes – a list all of the 1xxx prefixes for the USA, excluding the other 1xxx destinations.
- European Economic Area Prefixes - a list of all of the prefixes for the EEA

And, two origination Service Matching Lists.

- USA prefixes - as above but matching call origination
- Specific Countries Prefix List - this is a list of prefixes belonging to a series of specific countries.

The resulting configuration is as follows:

Customer	Service	Destination	Origination	Matches calls...
A	1	Customer A DIDs	-	to only the specific whole number DIDs included on this list, from any origination number. This list is not shared with any other Services.
A	2	USA prefixes	USA prefixes	from and to the USA.
A	3	European Economic Area Prefixes	-	to a country within the European Economic Area, from any origination number.
A	4	-	-	to and from any destination and origination that has not been matched by one of the previous Services.
B	1	European Economic Area Prefixes	Specific Countries Prefix List	to a country within the European Economic Area, from a country on the “specific countries prefix list”. As this is the only service for Customer B, calls will only be routed if they are from a country on the list and going to the EEA.

				All other calls will be rejected (with the status code 503).

Procedures:

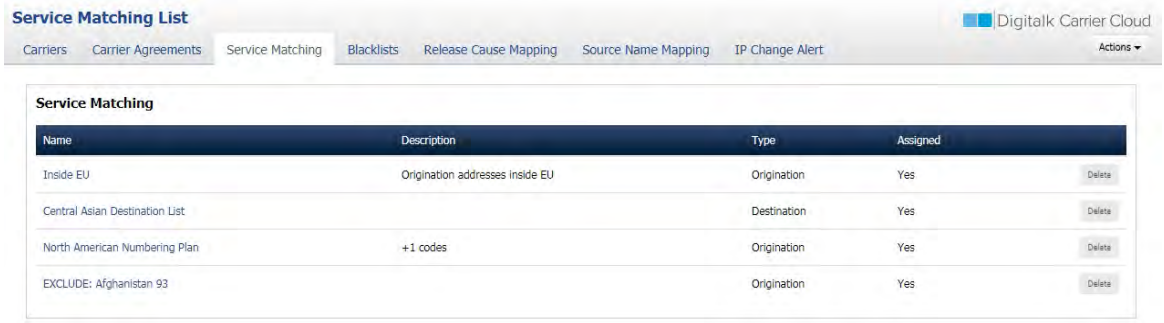
Creating a Service Matching List

Service Matching Lists are configured independently of individual Services, and can then be assigned to multiple Services as required.

Follow the steps below to create a Service Matching List.

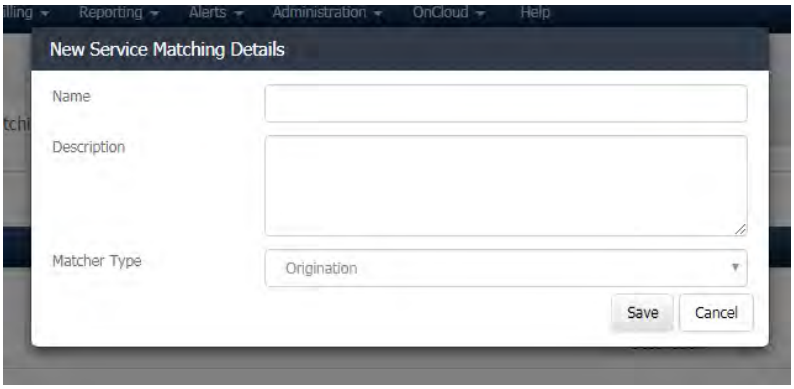
1. Navigate to Carriers > Service Matching.

Result: The "Service Matching" screen is displayed.



2. Select "Add Service Matching" from the "Actions" drop-down list box.

Result: The "New Service Matching Details" dialog box is displayed.



3. Enter the Name by which this Service Matching List will be known.

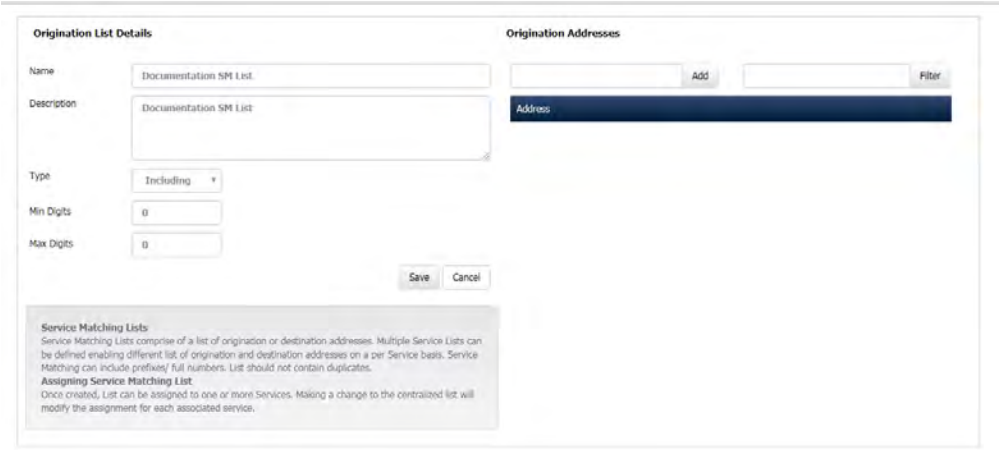
4. If required, add a description of the Service Matching List.

5. Select if the matching list will applied to Origination or Destination addresses, by selecting as appropriate from the "Matcher Type" drop-down list box.

Note: Although Origination and Destination lists are configured separately - as determined by selecting this option - all other aspects of their creation and management are identical.

6. Click “Save”.

Result: The “Origination/Destination List Screen” is displayed.



7. Use the table below to complete this step.

Field	Description	Action
Name	Determines the name by which this Service Matching List is known.	If required, edit the name of the list.
Description	This optional field adds a description of the Service Matching List for reference purposes.	If required, add a description, or edit the existing description.
Type	The “Type” drop-down list box selects from “Including” and “Excluding”. This is used to determine if the Service Matching List will only accept calls from the listed prefixes, or alternatively, reject calls from the listed prefixes. The default setting is “Including”.	Ensure the appropriate Type selection is made.
Min Digits	The Minimum and Maximum digits settings can be used to reject destination or originating addresses, which are under or over a specified number of digits. This can be used to automatically reject incomplete number strings that will lower performance metrics if they are routed onto a Supplier.	If required, configure the appropriate minimum and maximum number of digits that will match this Service Matching List.
Max Digits		

8. Click “Save”.

Result: The Service Matching List is created and ready to have addresses added.

Adding Addresses to a Centralised Service Matching List

After the Service Matching List has been created one or more prefixes, and/or full addresses can be added to it to begin filtering.

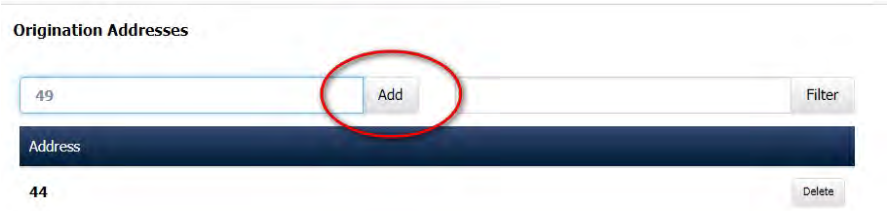
There are 2 methods available to add addresses, described below:

Method 1: Adding a Single Prefix or Address

Follow the steps below to add a single address to a Centralised Service Matching List.

1. Type the prefix or address into the field to the left of the “Add” button.
2. Click the “Add” button.

Result: The entry has been added to the Service Matching List.



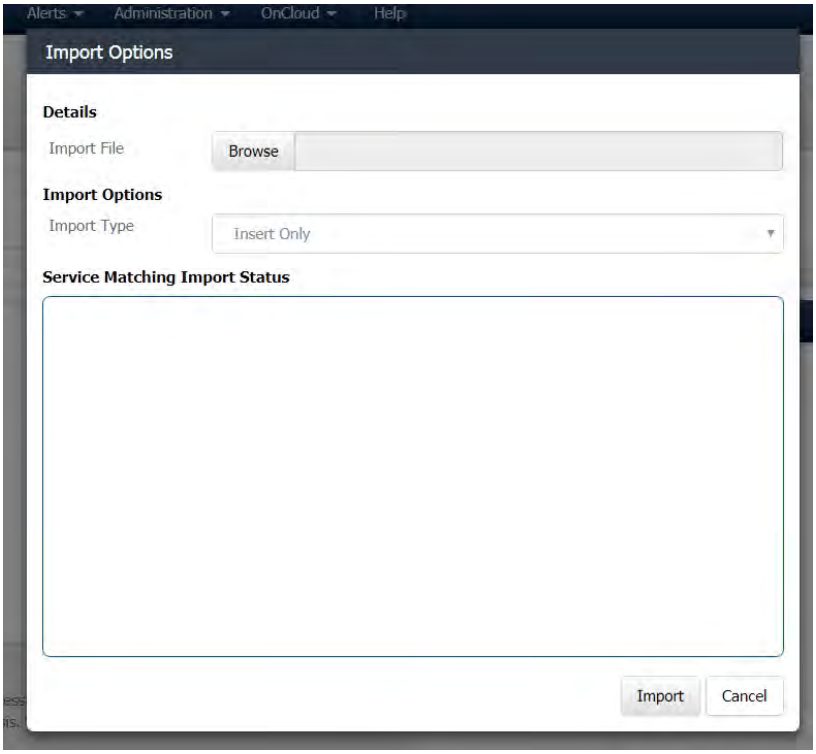
Method 2: Importing a List of Numbers

If a large list of numbers needs to be added to the Service Matching List, this can be imported in a .CSV file.

Follow the steps below to import a list of numbers into a Service Matching List.

1. Select “Import Addresses” from the “Actions” drop-down list box.

Result: The “Import Options” dialog box is displayed.



2. Click “Browse” and select the .CSV file containing the list of addresses of prefixes to be imported.

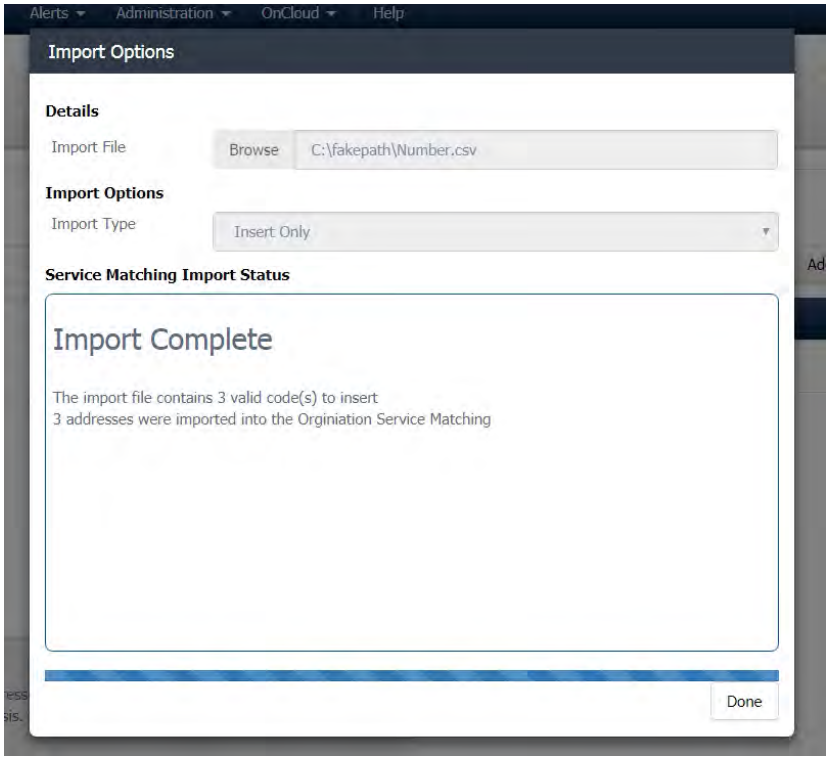
Note:
The file must be in .CSV format, containing a single Column of numbers in the first row.

No header row is required.

3. Select “Insert Only” to add these numbers to the existing list, or “Insert and Update” to replace the existing list with the list being uploaded.

4. Click “Import”.

Result: The file is imported into the Platform, and the dialog updated when the import has completed.



5. Click “Done”.

Result: The Centralised Service Matching List has been updated.

Tip: When the addresses and/or prefixes have been added to the Centralised Service Matching List, the list can be assigned to a Service(s).

3.7 Checking and Editing Number Translations Strings

The “Check and Edit” functionality is available when configuring origination/destination address translation on both the ingress and egress Interconnect.

The syntax for Number Translation is necessarily somewhat complicated, and it is therefore possible for human error to occur when configuring this setting. However, as errors in these fields can prevent calls from being connected, or stop them from being rated correctly, it is important to get these settings correct!

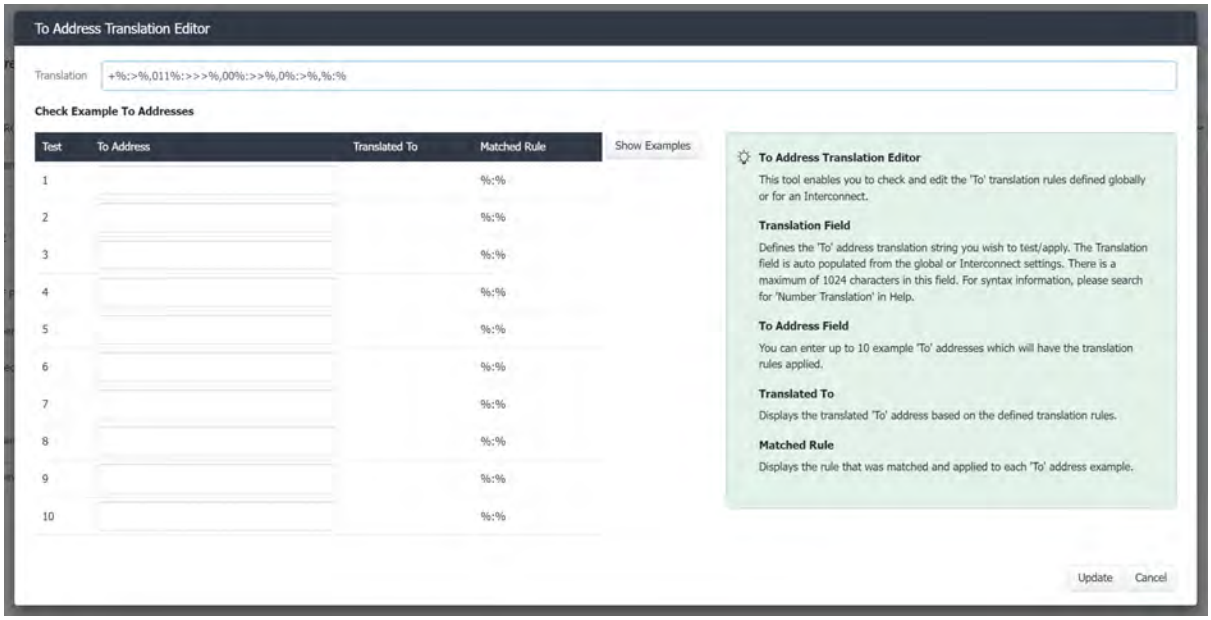
This feature has been provided to enablean Administrator to check how a Number Translation String that they have configured will behave when presented with a series of different numbers, and where necessary edit that string and see the result.

Follow the steps below from the Ingress/Egress Translation page to check and edit a Number Translation String.

Note: Only one string can be parsed at one time (originating or destination).

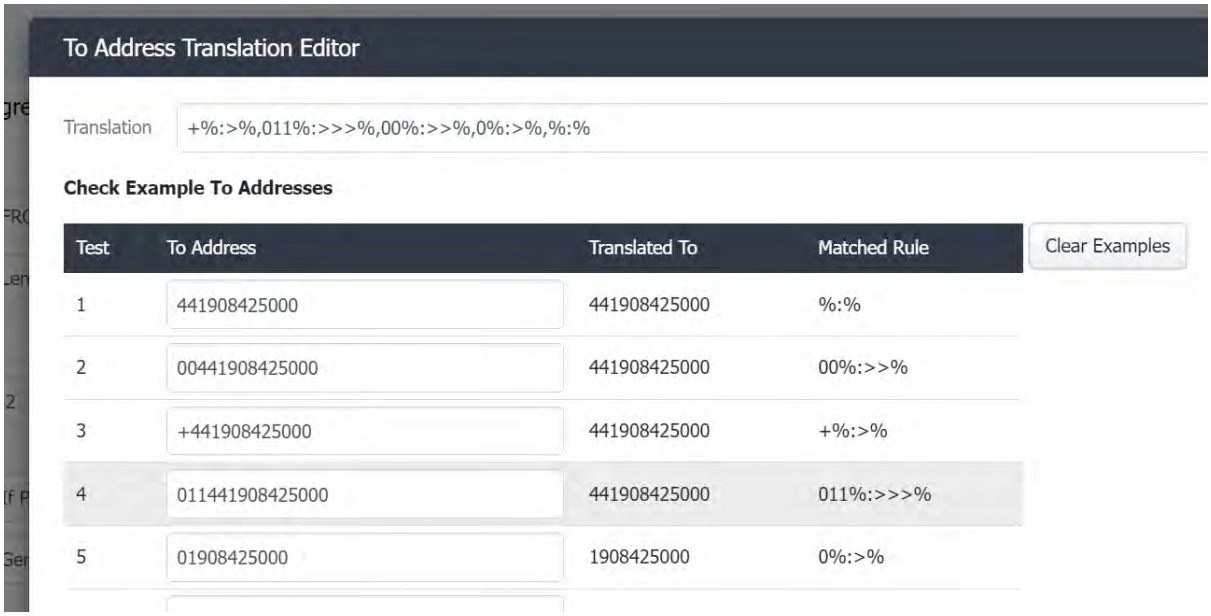
1. Click “Check and Edit” beside the string to be checked.

Result: The “Destination/Origination Address Translation Editor” dialog box is displayed.
Any string that has already been configured will be displayed in the “Translation” field, as shown on the screenshots above and below.



2. Click (if required) “Show Examples”

Clicking “Show Examples” will populate the tests with 5 common number presentations to be tested.This is provided to avoid having to type out common tests repeatedly.



3. If required, enter any additional test numbers in the Destination/Origination Address fields to be tested.

6	anonymous	anonymous	%:%
7	123	123	%:%
8	+++654321	++654321	+%:>%

4. Notice that the “Translated to” column will show the result of the defined Translation on a call with that destination address.

Translation +%:>%,011%:>>>%,00%:>>%,0%:>%,%:%

Check Example To Addresses

Clear Examples

Test	To Address	Translated To	Matched Rule
1	441908425000	441908425000	%:%
2	00441908425000	441908425000	00%:>>%
3	+441908425000	441908425000	+%:>%
4	011441908425000	441908425000	011%:>>>%
5	01908425000	1908425000	0%:>%
6	anonymous	anonymous	%:%
7	123	123	%:%
8	+++654321	++654321	+%:>%

5. If necessary, edit the translation string to see alternative results.

3.8 Enforcement Policies

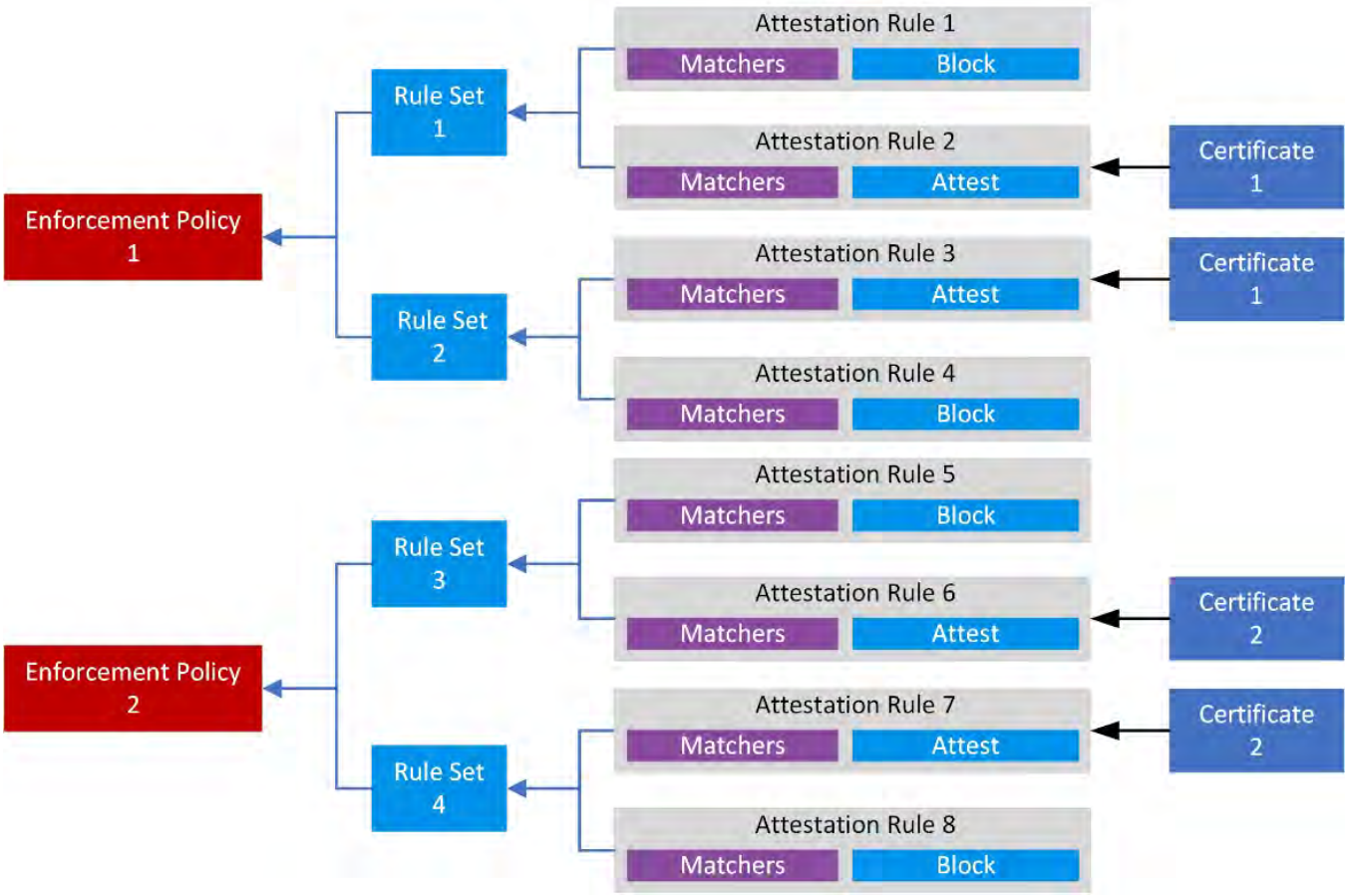
Overview

Enforcement Policies define and hold additional rules that can be applied to Services.

They can be used in relation to features such as Stir/Shaken Attestation, or to block traffic with invalid originations at the level of the Service.

Structure of Enforcement Policies

The diagram below illustrates the structure and relationships of enforcement policies.



In Summary.

- Enforcement Policies can contain any number of Rule Sets. At this point only Attestation Rule Sets are available and so it is likely that the enforcement policy will contain a single Attestation Rule Set.
- Attestation Rule Sets contain at least one, but more where necessary, Attestation Rules. Attestation Rules define the Attestation Action that will be applied to matching calls.

- An Enforcement Policy is enacted by applying it to a Service. A Single Enforcement Policy can be applied to any number of Services.

The following sections describe the creation and configuration of these elements.

Creating an Enforcement Policy

Enforcement Policies function as a “wrapper” for rule sets and rules, it is an enforcement policy that is assigned to a Service to apply the Enforcement Rules to the traffic using that Service.

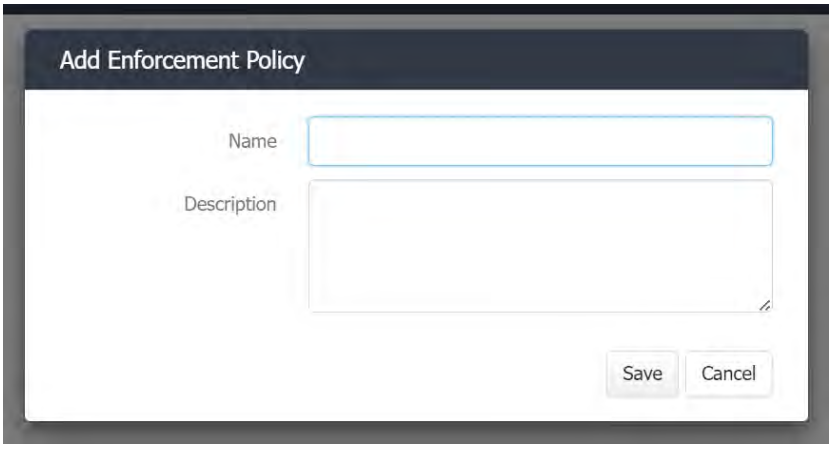
Follow the steps below to create an Enforcement Policy.

1. Navigate to Carriers > Enforcement Policies.

Result: The Enforcement Policies screen is displayed.

2. Select “Add Enforcement Policy” from the “Actions” menu.

Result: The “Add Enforcement Policy” dialog box is displayed.



3. Type the “Name” by which the Enforcement Policy will be known in the “Name” field.
4. If required, add a description for the Enforcement Policy for reference purposes.
5. Click “Save”.

Result: The Enforcement Policy has been created and is ready to have Rule Sets added to it.

Creating an Attestation Rule Set

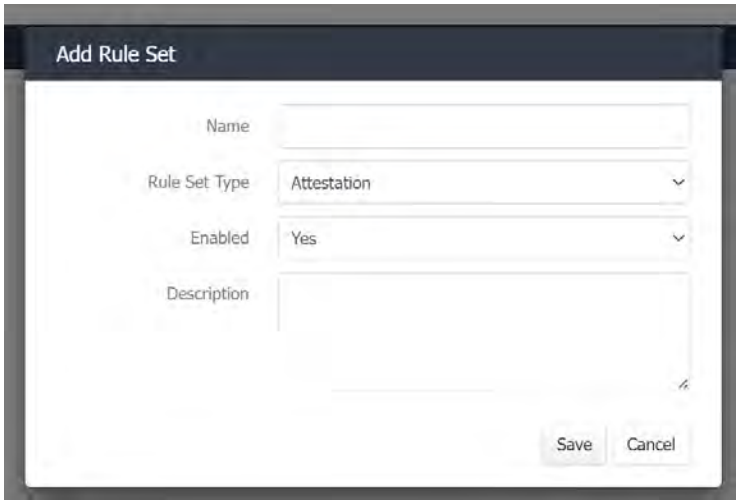
Attestation Rule Sets contain one or more Attestation Rules and are assigned to an Enforcement Policy. the steps below to create an Attestation Rule Set.

1. Navigate to Carriers > Enforcement Policies > Rule Sets Tab

Result: The Rule Sets Tab is displayed.

2. Select "Add Rule Set" from the "Actions" drop-down list box.

Result: The "Add Rule Set" dialog box is displayed.



3. Type the name by which the rule set will be known into the "Name" field.

4. Leave the Rule Set Type set to "Attestation" (no other options are currently available).

5. Leave the Enabled drop-down list box set to Enabled.
   Note: This Rule Set can be disabled in the future if required.

6. If required, add a description to the Rule Set for reference.

7. Click "Save".

Result: The Rule Set has been added and Attestation Rules can now be added to it.

Adding an Attestation Rule to an Attestation Rule Set

After the Attestation Rule Set has been defined one or more Attestation Rules can be added to it.

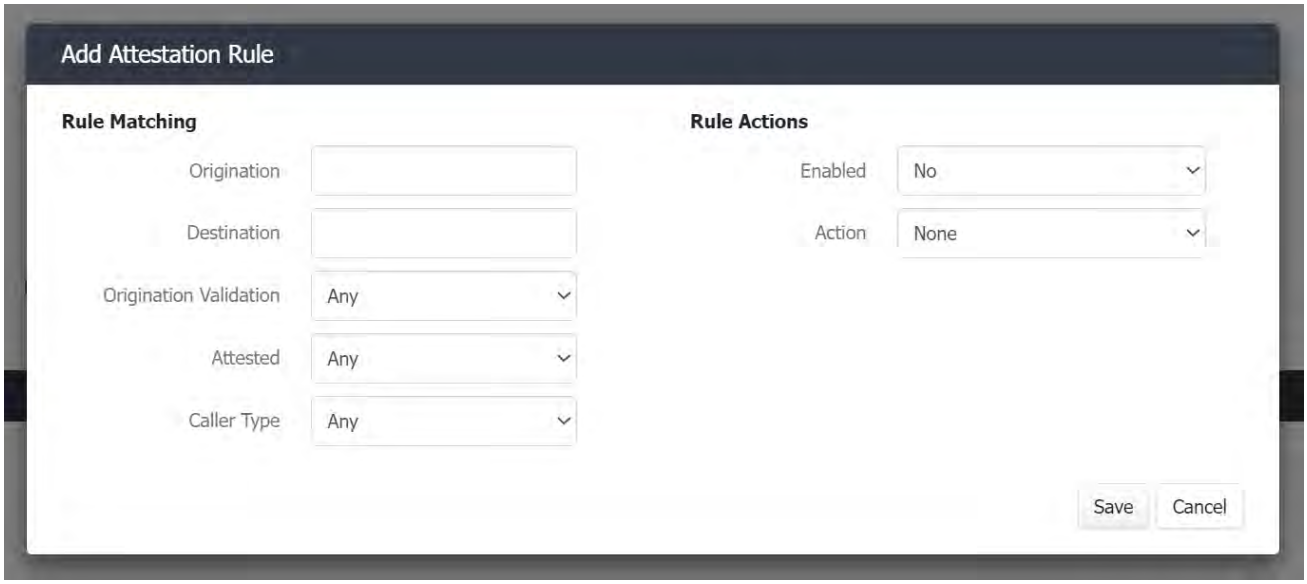
Follow the steps below to add an Attestation Rule to an Attestation Rule Set.

1. Click on the name of the Attestation Rule Set to have a Rule added to it.

Result: The Attestation Rule Set details are displayed.

2. Select "Add Attestation Rule" from the "Actions" drop-down list box.

Result: The "Add Attestation Rule" dialog box is displayed.

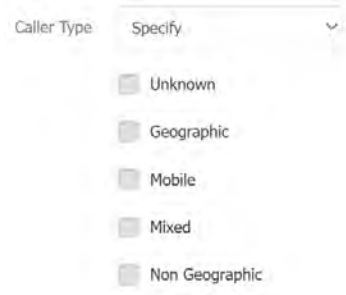


Note: Attestation Rules are made up of two factors, the Matching Rules which define to which telephone calls the Rule will apply and the Action itself.

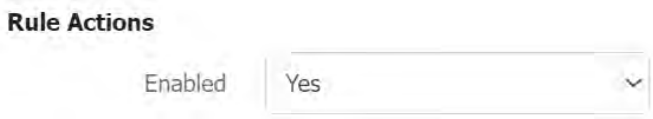
3. Use the table below to define the Rule Matching settings for this Rule.

Field	Description	Action

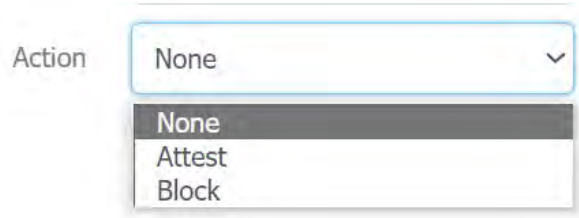
Origination	Matches based upon an Origination prefix or whole number. Leaving this field blank will match all calls. .To specify a prefix, enter the numbers without a percentage symbol. Example: To match only calls originating from the North American Numbering Plan enter “1”.  **Note:** It is only possible to have a single prefix or number in this field.	If required, add origination matching.
Destination	Matches based upon a Destination prefix or whole number. Leaving this field blank will match all calls.  **Technical Note:** To specify a prefix, enter the numbers without a percentage symbol. Example: To match only calls going to the UK enter “44”.  **Note:** It is only possible to have a single prefix or number in this field.	If required, add destination matching.
Origination Validation	This setting provides matching based upon the validity of the Origination. The options available are: • Any - ignores this matching characteristic. • Valid - will only match on valid calls • Missing/Invalid - will only match on calls that have been identified as having invalid Originations. Reference: See "Origination Address Identification and PAI Management/Generation" on page 154 for more information on Origination validity.	If required, configure the origination validation matching.

Attested	This setting provides matching based upon the attestation status of the call. The options available are: • Any - ignores this matching characteristic. • No - will match a call only if it is not attested. • Yes - will match a call only if it is attested.	If required, configure the attestation matching.
Caller Type	This setting provides matching based upon the type of call being received. The options available are: • Any - ignores this matching characteristic. • Specify - will match on one or more of the selected call types, as shown in the screenshot below:  **Note:** This Caller Type Category is determined through a look up in the Digitalk Origination Number Database used for reporting purposes.	If required, configure the caller type validation matching.

4. Ensure Rule Actions > Enabled is set to “Yes” to ensure the rule being created is made active.



5. Select the Action that will be applied to traffic meeting matching criteria from the “Action” drop-down this box.



The actions available are:

- None - No action will be taken.
- Attest - The Attestation Level and Certificate drop-down boxes will be displayed, see below for further information.
- Block – Calls matching the defined rules will be blocked.

6. If “None” or “Block” has been selected, continue with step 9.
   If “Attest” has been selected continue with the next step.

7. Select the required level of Attestation from the “Attestation Level” drop-down list box.

It is expected that the majority of Customers using the Digitalk Platform will be attesting only at Level C. However, consult with your local expert in order to determine the correct Attestation Level for your use case.

8. Select the required Certificate from the “Certificate” drop-down list box.

It is likely that only a single certificate will be available, however Digitalk provides the capability to support multiple Certificates if needed.

9. Click “Save”.

Result: The Attestation Rule has been saved to the Attestation Rule Set.

Repeat the process for additional Attestation Rules as required.

Assigning Attestation Rule Sets to an Enforcement Policy

When all of the required Rules have been applied to the Rule Set, the Rule Set can then be added to the Enforcement Policy.

Follow the steps below from me Enforcement Policy tab to add an Attestation Rule Set to an Enforcement Policy.

1. Click on the Name of the Enforcement Policy to be configured.

Result: The Policy Details page will be displayed.

2. Select the Rule Set to be added to the Enforcement Policy from the drop-down list box, as highlighted on the screenshot below.

3. Click “Assign”.

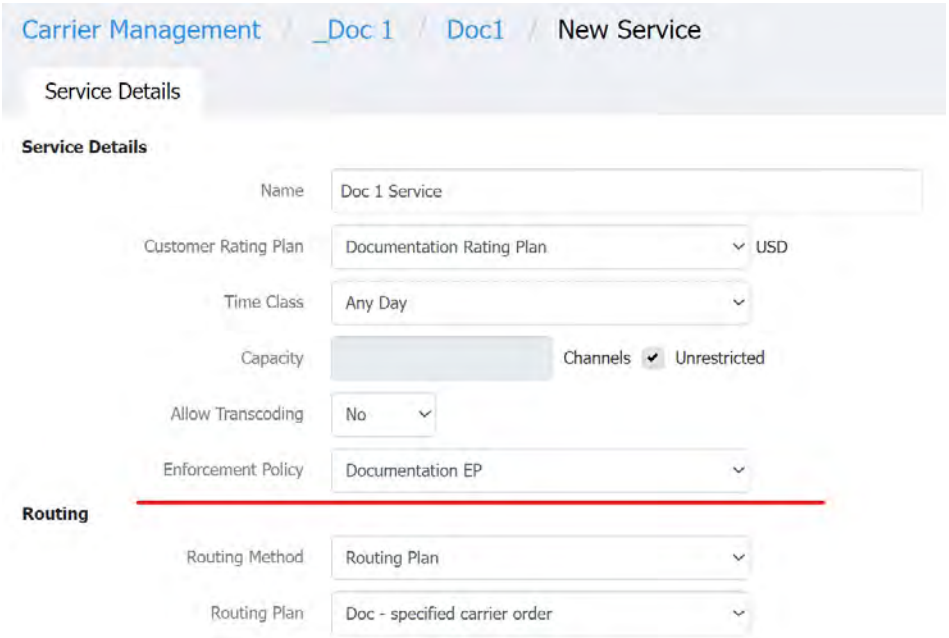
Result: The Rule Set will be added and is immediately active.

Note: The Rule Set can be removed from the Enforcement Policy in the future by selecting the Unassign button.

Assigning an Enforcement Policy to a Service

After the Enforcement Policy has been associated with all of the required Rule Sets, it can be assigned to all relevant Services.

Use the “Enforcement Policy” drop-down list box on a Service to assign an enforcement policy to the Service.



Reference: See "Creating a Service" on page 122 for information on creating and configuring a Service.

3.9 Origination Address Identification and PAI Management/Generation

The Originating Address Identification settings on the Ingress and Egress tabs of the Interconnect determine how the From Address, and the PAI Address, are handled when transiting through the Carrier Cloud.

This sections provide an introduction to these principles and information on what each of the settings do, and an overview of why they might be used.

Introduction to the From/PAI

Understanding the From Address and the PAI

Identities in a SIP call are typically established using the “To” and “From” headers.

The “To” header contains the destination number, and the “From” indicates where the call has originated, most commonly this is a telephone number and is often referred to as the CLI or ANI.

In this situation the SIP Invite headers look as follows:

Example:
INVITE sip:4412345678@example1.com SIP/2.0

Max-Forwards: 70

To: “Taina” <sip: 4412345678@example1.com>

From: “Anuvap” <sip: 441908425000@example2.com>; tag=12345

The “From” address is often known as the “Subscriber Identity” as it is the identity that is presented by the subscriber.

In this example a person, Anuvap, is making a call from 441908425000 to Taina on 4412345678.

However, let us imagine that for some reason, Anuvap wishes to conceal their identity - as can be achieved in the USA on a landline by pressing *67 before dialling or *141 in the UK.

For such a scenario, the Subscriber Identity in the From address, will appear as follows:

Example: From: “Anonymous” <sip: anonymous@anonymous.invalid>; tag=12345

This will withhold the origination information (CLI/ANI) from the end user. However, at a network level this can create a problem. Many SIP network elements may not want to deal with an anonymous caller, as the caller’s identity is required for many network functions. Additionally in accordance with £.164, SIP identities that include non-numeric characters (excluding a leading +) may also be considered “invalid” within a telephony network.

In this situation an additional SIP header, known as P-Asserted-Identity (or PAI) can be used.

PAI is defined in IETF RFC 3325 and is used within the “trusted” realm of a SIP network to retain the identity of calls that are marked as anonymous. (will link to https://tools.ietf.org/html/rfc3325)

This results in a SIP Invite header which would appear as follows, including the P-Asserted-Identity entry:

Example:
INVITE sip:4412345678@example1.com SIP/2.0

Max-Forwards: 70

To: “Taina” <sip: 4412345678@example1.com>

From: “Anonymous” <sip: anonymous@anonymous.invalid>; tag=12345

P-Asserted-Identity: “Anuvap” <sip:441908425000@example2.com>

The PAI is referred to as the “Network Identity” as it is generated at the network level and therefore trusted within the network.

Note:

A Note on RPID

Although this section of the documentation will focus on the PAI Header, the Carrier Cloud Manager can also process and work with the older Remote Party ID or RPID Header in the same way when needed.

Working with PAI in a Global Network

In the scope of global telecommunications many Carriers require a valid Network Identity to be provided either in the Subscriber Identity (not anonymous) or in the PAI Header. Reasons for this include, but are not limited to, meeting regulatory compliance and to apply rating based upon origination as well as destination.

In some circumstances however, calls received by the Carrier Cloud may not present a valid Identity. This is usually because the PAI header is omitted completely, or because the address is invalid or malformed.

The Origination Address Identification management features of the Carrier Cloud allow a Platform Administrator to control Network Identity presentation: to present the received From Address as the PAI, and the ability to modify, or even generate, the PAI where necessary.

Understanding "Origination Preference"

What is the Digitalk “Originating Address”?

As discussed above, in SIP information the Origination of the call can be provided in the From Header and/or the PAI Header. However, on the Digitalk Carrier Cloud Platform there are a number of features that use this Origination information such as Service Matching, Origination-based Rating and Routing, Reporting, and the capability to block traffic with invalid origins.

When the information contained within both of these headers is identical then there is no ambiguity present, however in the common circumstance that the information in these headers differs, Carrier Cloud needs a method for determining which of the two options is going to take precedence.

> Whichever of the two Headers is chosen to be used is referred to within Carrier Cloud as the “Originating Address”. The number (or lack of number) present in this Header (following any Number Translation applied to it) will be used for all origination lookups.

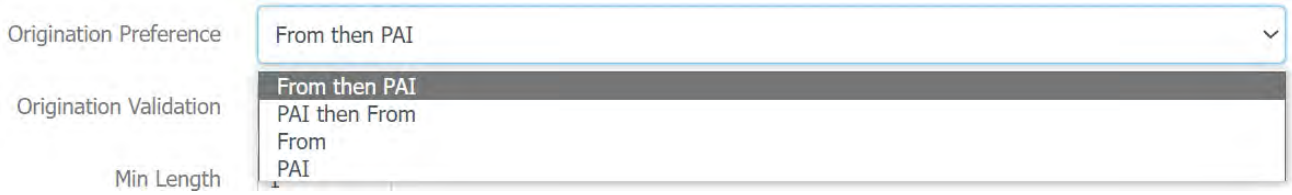
The method for determining which of these two Origination options is preferred, is described in the following section.

Determining Origination Preference

The "Origination Preference" drop-down list box determines the logic by which Carrier Cloud will identify the Originating Address (from the From Address or PAI) which will be used throughout the Platform for origination lookups. (As discussed in the section above.)

There are four options available for selection:

- From then PAI
- PAI then From (default)
- From only
- PAI only



The meaning of the From and PAI only options is hopefully clear. When either of these options is selected only this Header will be used as the Originating Address for traffic received on this inbound interconnect, regardless of whether the information contained is valid, invalid, or missing. The information in the other Header is ignored.

With the PAI then From and From then PAI options there is an important detail to understand. These options set a preference that means that the platform will use the preferred method when the information contained in the two headers is of at "least equal validity".

What this means is as long as the contents of both Headers are equally valid, or the preferred Header is of "greater validity" then the information from that Header will be used. However, if the information in the preferred Header is considered invalid, and the information in the alternative Header is valid then that valid information will be used.

See the examples below for an illustration of these principles:

Example:

Example 1

Origination Preference: PAI then From

Origination Validation: Length Check & E.164 format

Headers Received:

From: anonymous@192.0.2.1:5060

PAI: anonymous@192.0.2.1:5060

In this case, both headers are considered invalid, as they do not match E.164 format. Therefore, the PAI will be used as the Carrier Cloud Originating Address.

Example 2

Origination Preference: PAI then From

Origination Validation: Length Check & E.164 format

Headers Received:

From: 01908425000@192.0.2.1:5060

PAI: 01908425100@192.0.2.1:5060

In this case, both headers are considered valid even though they are presenting different telephone numbers. The Origination Preference setting of PAI then From means that the PAI of 01908425100 will be used as the Carrier Cloud Originating Address.

Example 3

Origination Preference: From then PAI

Origination Validation: Length Check & E.164 format

Headers Received:

From: 441908425000@192.0.2.1:5060

PAI: 441908425000@192.0.2.1:5060

In this case, both headers are considered valid. Therefore, the From Address will be used as the Carrier Cloud Originating Address.

Example 4

Origination Preference: From then PAI

Origination Validation: Length Check & E.164 format

Headers Received:

From: anonymous@192.0.2.1:5060

PAI: 441908425000@192.0.2.1:5060

In this case, the From Address is invalid, but the PAI is valid. The Origination Preference is configured as From then PAI which means therefore the From Address is ignored and the valid PAI will be used as the Carrier Cloud Originating Address.

Example 5

Origination Preference: PAI then From

Origination Validation: Length Check & E.164 format

Headers Received:

From: 441908425000@192.0.2.1:5060

PAI: unknown@192.0.2.1:5060

In this case the situation is reversed. The From Address is valid, but the PAI is invalid. The Origination Preference is configured as PAI then From which means therefore the From Address, not the PAI, will be used as the Carrier Cloud Originating Address.

Example 6

Origination Preference: PAI

Origination Validation: Length Check & E.164 format

Headers Received:

From: 441908425000@192.0.2.1:5060

PAI: unknown@192.0.2.1:5060

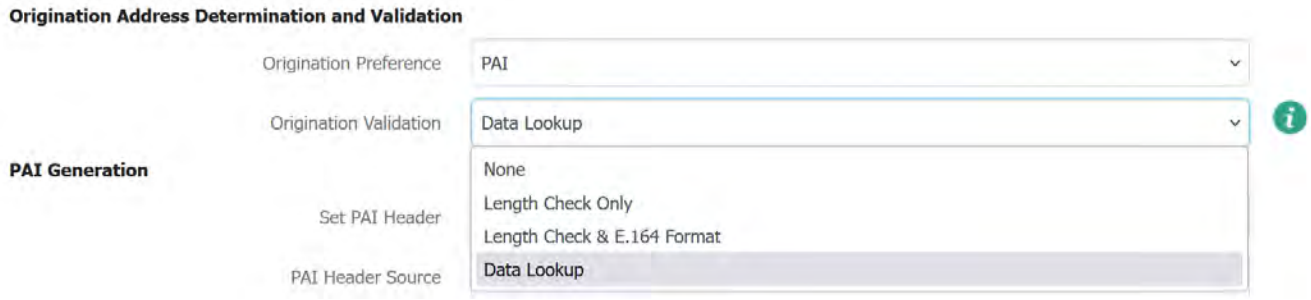
In this case the same headers as above are received, the From Address is valid and the PAI invalid; but the Origination Preference has been set to PAI only.

This means that although the From Address is considered valid it will not be used by the Platform, and the invalid PAI will be used for origination lookups.

Understanding Origination Address Validation Options

Origination Address Validation

Both Ingress and Egress Interconnects offer the same settings for validating an Origination Address.



The table below describes the different options available for validation.

Option	Description
None	No look up will be performed.
Length check only	Validity will be determined only on the length of the Originating Address; the length validity criteria is set below.
Length Check & E.164 format	Validity will be based on both the length (as above) and whether or not the Originating Address received meets the E.164 standard. The E.164 standard states that (while SIP technically supports alpha characters) telephone addresses must consist only of numbers, and an optional '+'.Any call received with an origination that contains other characters, including examples such as "anonymous" or "restricted", is considered invalid.
Data Lookup	With this option calls are not only checked against the E.164 standard (as above) but also against a centralised list of Originating Addresses that Digitalk maintain to assist Customers in ensuring the validity of their calls. A key feature of this look up is the ability to check if the length an Originating Address from a particular country matches the appropriate valid length for that country. This can be required in some business circumstances as different countries support different valid length for Originating Addresses.

	 **Caution:** This option will only appear if this feature has been **specifically** enabled on your Platform. To have this feature enabled please contact your Account Manager for further details.

Tip:

It is important to understand that this feature only provides a "look up" on the Customer Interconnect.

The result of the validity check, whether through Data Lookup or one of the other methods, sets a "flag" on the call in regards to its validity status.

This "validity status" is then used by other platform features to allow/block the call, or rate or route differently.

Contact Digitalk support for further information.

Note:

Although the same settings are used on the Ingress and Egress Interconnects they are independent of each other.

The validation on the Ingress Interconnect determines how the Originating Address will be managed within the Carrier Cloud Platform.

The validation on the Egress Interconnect applies only when the call is leaving the Platform and determines any specific changes that are required for a specific Partner.

What Is the Purpose of Origination Address Validation?

Origination Address Validation is a very powerful feature; however, it is important to understand how and where would applies.

The setting described here on the Interconnect is used to check the validity of the Originating Address.

On an inbound Customer Interconnect, the result of this validity checked does “nothing at this point in the call flow”, other than “making a note of the result of the check”.

What this means is that even if the call is deemed to be “invalid” nothing will occur to that call at the point of validation.

However, the Digitalk Platform provides a number of places where a rating or routing decision can be influenced by the validity status of a call, providing the option to block the call, or rate the call differently.

These places are as follows:

- Enforcement Policies (where available)
- Customer Rating
- Routing, and
- Supplier Rating

Additionally, the validity of the call can be checked by the Supplier Interconnect when egress in the Platform.

Supplier Interconnects then have an option to “block invalid originations”, meaning that no call that is deemed as “invalid” will be sent to that Supplier.

Technical Note:
Note that this ability to rating and route differently, or to block, are available based on the valid/invalid result of the check, no matter which method of checking was used.

While the “Database Look up” is by far the most powerful and accurate method for checking originations, the other simpler methods will still mark the relevant calls as invalid and result in the invalid action being taken elsewhere in the Platform.

CDR Recording

The result of the inbound checked is recorded in the CDR in the column “CLI_validity” - the recorded result will be one of the following options:

- CLI validity - not checked
- CLI validity checked – valid
- CLI validity checked – invalid
- CLI validity checked - address missing

This information can be used as a filter in Report Builder, is visible on the CDR Viewer, and will be included in the FTP of CDRs.

Ingress / Egress PAI Generation Settings

PAI Generation - On the Ingress Interconnect

Note:
A Note on the Order of These Changes in the Call Flow

For Platform Administrators who want to understand exactly when any changes made by these settings will apply.

The PAI modification options on the Ingress side will take place **after** the ingress validation has been passed and any Ingress Translation has occurred. When leaving the Platform, the changes will occur **before** any Egress Translation is made.

Generation Method Description

PAI Generation on the Ingress Interconnect utilises a preloaded list of numbers. The PAI can be assigned to a call received on this Carrier Interconnect from the list based on random or sequential selection.

This method allows the Interconnect Administrator to define one master list that can be used by multiple Customer Interconnects. Alternatively, multiple lists can be defined that are each used for a single Customer, or combinations of the two methods.

See "Origination Generation Lists" on page 170 for further information on defining the Origination Generation lists.

Ingress PAI Generation Settings

The screenshot below shows the Ingress PAI Generation settings.

The table below describes the settings used for Ingress PAI Generation.

Field	Description
Set PAI Header	This field determines if and when the PAI will be generated. The three options available are as follows: Option | Description

<table>
<tr><td></td><td>
<table>
<tr><td>Never -</td><td>The PAI will never be generated for calls using this Interconnect.</td></tr>
<tr><td>Always</td><td>The PAI will always be generated for calls using this Interconnect.</td></tr>
<tr><td>If PAI Is Invalid</td><td>The PAI will be generated for calls using this interconnect only if the PAI that is already presented is deemed to be “invalid”
See above for more information on Origination Address Validation..</td></tr>
</table>
</td></tr>
<tr><td>PAI Header Source</td><td>
This field determines the source of the PAI that will be set for calls using this Interconnect.
The three options available are as follows:
<table>
<tr><td>Option</td><td>Description</td></tr>
<tr><td>Generate</td><td>The PAI will be generated from an “Origination Generation List”.
See below for more information.</td></tr>
<tr><td>Origination Address</td><td>The PAI will be set as equal to the Origination Address source as defined in “Origination Preference” (See above).
This feature is designed to support scenarios where the Administrator wants to set the PAI equal to the From Address either all the time, or in the event of receiving an invalid PAI but a valid From Address.</td></tr>
<tr><td>Origination Address if Valid Else Generate</td><td>The PAI will be set as equal to the Origination Address source as defined in “Origination Preference” (See above) only if the presented address is valid, otherwise the platform will generate a PAI from an “Origination Generation List”.
See below for more information.</td></tr>
</table>
</td></tr>
<tr><td>Origination Gen-eration List</td><td>If the PAI is to be generated from an Origination Generation List this drop-down list box selects the list to be applied for this Interconnect.</td></tr>
<tr><td>Set FROM</td><td>This setting determines how the “From Address” is treated when the PAI is being</td></tr>
</table>

Header	generated. The options available are: • Pass Through - The From address will be passed through unchanged by the generated PAI. This is the default option. • Set as Anonymous - The From address will be marked as anonymous when the PAI has been generated. • Same as PAI - The From address will be set to the same generated identity as the PAI.

Further Platform Implications

It is important that the Platform Administrator is clear that generating an Origination Address on the Ingress Interconnect means that the generated address, not the originally received address, will be used for any further origination lookups elsewhere within Digitalk Carrier Cloud.

This includes:

- Service Matching
- Origin-based Customer Rating and Supplier Rating
- Origin-based Routing
- Blacklisting (both ingress and egress)
- Number Portability

PAI Generation - On the Egress Interconnect

Generation Method Description

PAI Generation on the Egress Interconnect allows the Administrator to determine if and when a PAI will be generated by the platform for calls using this Interconnect.

The method for generating PAIs on the Egress Interconnect differs from the method available on the Ingress side to provide flexibility. The method available on the Egress allows the administrator to generate a random PAI from within a defined range.

See the table below for details.

Egress PAI Generation Settings

The screenshot below shows the Egress PAI Generation settings.

The table below describes the settings used for Egress PAI Generation.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Set PAI Header</td><td>This field determines if and when the PAI will be generated.
The three options available are as follows:
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Never -</td><td>The PAI will never be generated for calls using this Interconnect.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>Always</td><td>The PAI will always be generated for calls using this Interconnect.</td></tr>
<tr><td>If PAI Is Invalid</td><td>The PAI will be generated for calls using this interconnect only if the PAI that is already presented is deemed to be “invalid”
See above for more information on Origination Address Validation.</td></tr>
</table>
</td></tr>
<tr><td>PAI Header Source</td><td>
This field determines the source of the PAI that will be set for calls using this Interconnect.
The three options available are as follows:
<table>
<tr><td>Option</td><td>Description</td></tr>
<tr><td>Generate</td><td>The PAI will be generated using the “Generation Block Start/Size” settings.
See below for more information.</td></tr>
<tr><td>Origination Address</td><td>The PAI will be set as equal to the Origination Address source as defined in “Origination Preference” (See above).
This feature is designed to support scenarios where the Administrator wants to set the PAI equal to the From Address either all the time, or in the event of an invalid PAI but a valid From Address.</td></tr>
<tr><td>Origination Address if Valid Else Generate</td><td>The PAI will be set as equal to the Origination Address source as defined in “Origination Preference” (See above) only if the presented address is valid, otherwise the platform will generate a PAI using the “Generation Block Start/Size” settings.
See below for more information.</td></tr>
</table>
</td></tr>
<tr><td>Block Start</td><td>
This determines the initial number or starting point for the generation of PAI addresses.
Example:

 Example:
Setting “0897900000” is the base for the generation of random numbers (the
</td></tr>
</table>

	range generated by the block size below) starting at this number. **Note:** If the Block Start field is left empty when a PAI requires generating then the PAI will be populated with the contents of the From Address.
Block Size	This determines the range of numbers that will be generated from the starting point. The options available are: 1 (only the single number defined will be used in generation), 100, 1000, 10000, and 100000. This means that by selecting 10000, and using the starting number above, each call will be given a randomly generated PAI between: 0897900000 and 0897999999.
Set FROM Header	This setting determines how the "From Address" is treated when the PAI is being generated. The options available are: • Pass Through - The From address will be passed through unchanged by the generated PAI. This is the default option. • Set as Anonymous - The From address will be marked as anonymous when the PAI has been generated. • Same as PAI - The From address will be set to the same generated identity as the PAI.

3.10 Origination Generation Lists

Origination Generation Lists are used to hold the list(s) of numbers used by the ingress PAI generation feature.

Reference: See "Origination Address Identification and PAI Management/Generation" on page 154 for further information on this feature.

Origination Generation List Features

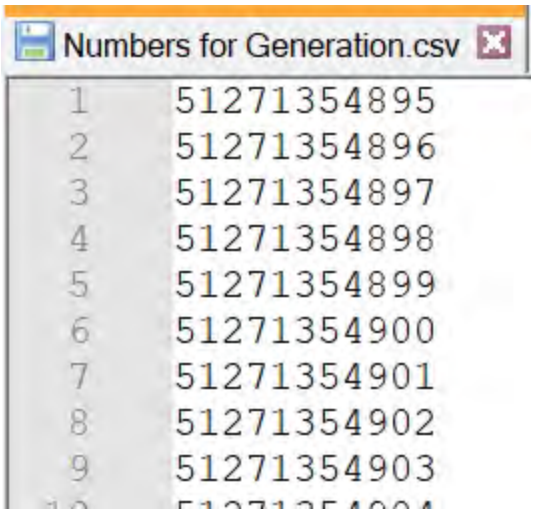
It is possible to create as many Origination Generation Lists as needed on the platform, however the total number of entries held on all lists must not exceed 100,000 entries.

Generation Lists can be defined in one of two modes, Random and Sequential. This determines the way in which the numbers present on the list are presented as the PAI. With Random randomly selecting a number to be presented and Sequential picking entries in order.

The management of Generation Lists includes the ability to import numbers into the list, export the contents of a list, and delete entries from the list through the user interface.

Generation Lists are populated by import from file. The format for the data to be imported is a .CSV file with a single column, without header row, containing the origination numbers to be imported.

As shown in the example below.

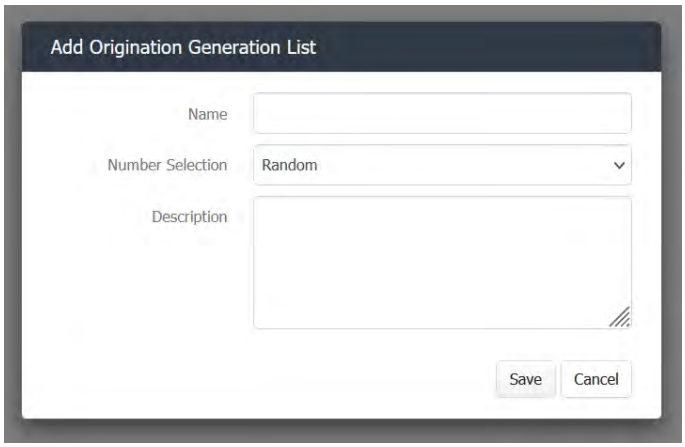


3.10.1 Creating a Generation List

Follow the steps below to create a new Generation List.

1. Navigate to Carriers > Origination Generation.
2. Select "Add Generation List" from the "Actions" menu.

Result: The "Add Origination Generation List" dialog box is displayed.



3. Enter the name by which this Generation List is to be known in the "Name" field.
4. Select whether the number selection method used by this list will be Random or Sequential.
5. If required, add a description to the list for future reference.
6. Click "Save".

Result: The Origination Generation List has been created.

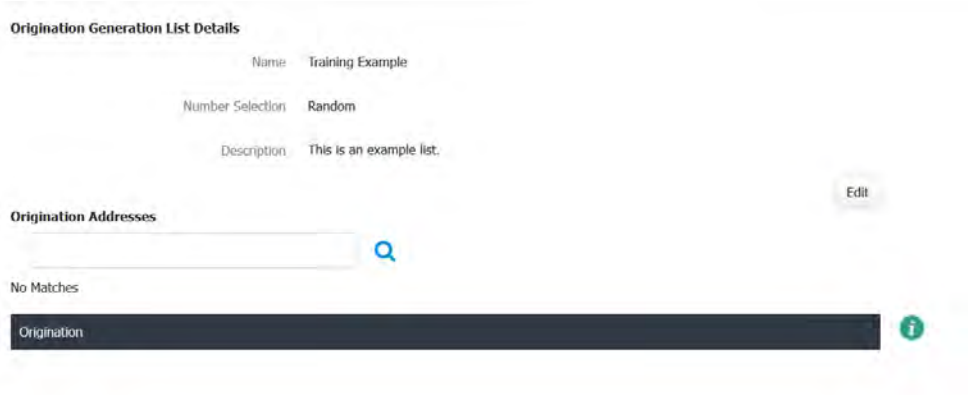
3.10.1.1 Populating an Origination Generation List through Import

The only way to add entries to an Origination Generation List is by import.

Follow the steps in the table below to import Originations into an Origination Generation List.

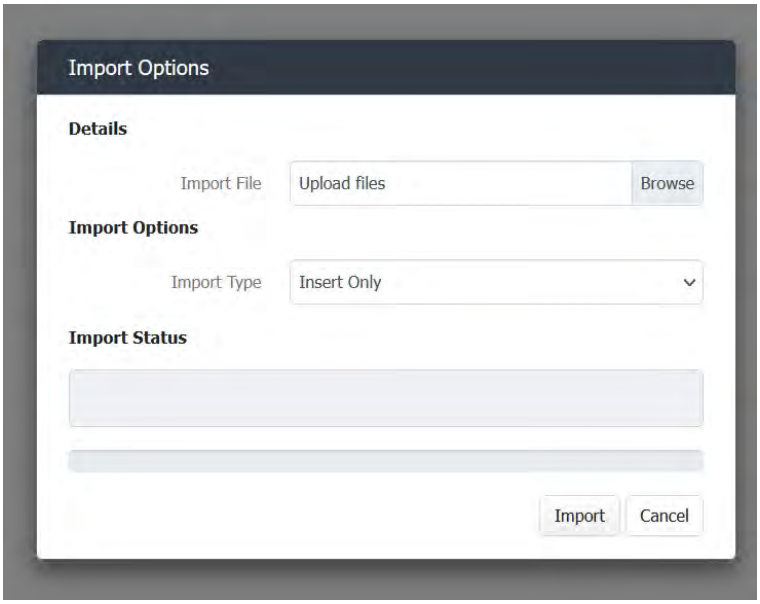
1. Click on the Name of the Origination Generation List to be populated.

Result: The “List Details” screen is displayed.



2. Select “Import Addresses” from the “Actions” menu.

Result: The “Import Options” dialog box is displayed.



3. Browse for the file of origination numbers to be uploaded.

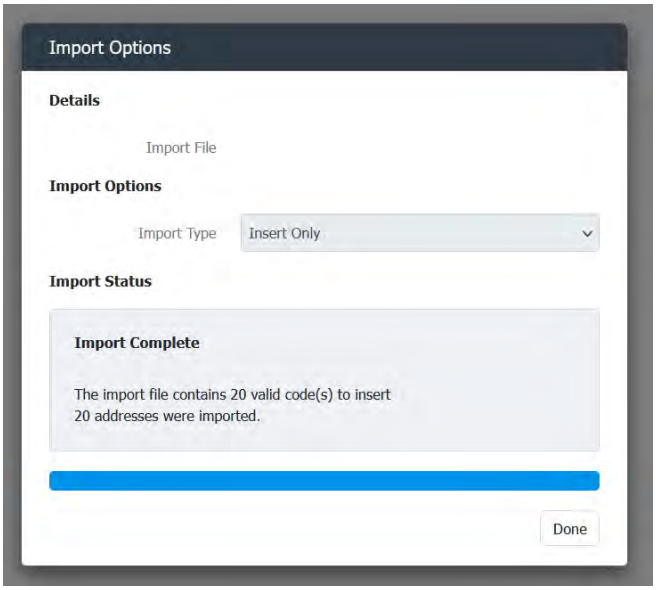
4. Select the Import Type from the following two options:

Insert Only - This option will add to the contents of the new file being uploaded without making any changes to the existing contents of the list.

Insert and Update - This option will replace the existing contents of the list with the contents of the file being uploaded.

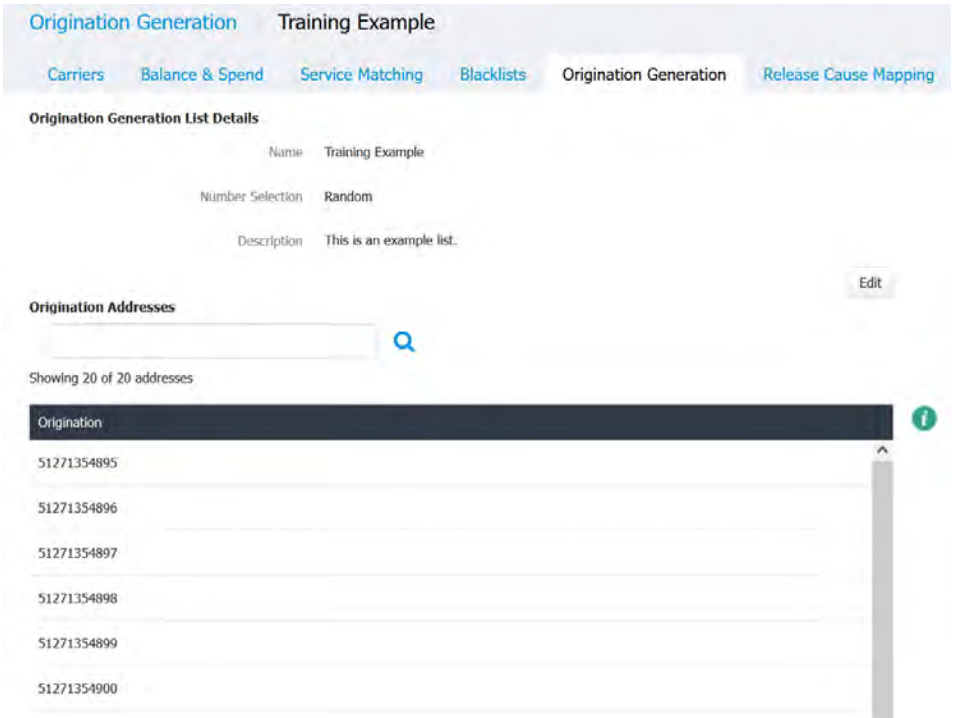
5. Click “Import”.

Result: The selected file will be uploaded.
The Import Status will report upon the details of the upload that has occurred.



6. Click “Done”.

Result: The Origination Generation List has been populated and is ready for use.



Note: Use the search filter to view some/all of the contents of the Origination List.

3.11 Supporting Asymmetric Reliable Provisional Responses (100rel)

Default “Standards-Based” Behaviour

RFC 3262 sets out a specification in regard of providing provisional response method using the 100rel tag and the provisional response acknowledgement (PRACK) method.

This specification provides the standard behaviour for Digitalk Carrier Cloud and is represented in the user interface with the default setting of “Passthrough”.

Selecting Passthrough ensures that Digitalk Carrier Cloud Session Border Controller will forward any 100rel headers that are received - relying on the endpoint being connected to manage the responses. The result of passthrough mode is that 100rel is only enabled when both the Customer and Supplier endpoints request and support 100rel.

Asymmetric Support

There are, however, some specific business cases requiring the generation of a PRACK message where one has not been received from the Customer endpoint, or to discard a provisional message that has been received.

Examples requiring this may include ‘redirections’ to voicemail in a mobile environment, or to allow 'inter-networking' with legacy architecture that does not support provisional acknowledgement (PRACK).

In these cases, the Digitalk Carrier Cloud Session Border Controller can behave asymmetrically, providing different 100rel support to ingress and egress legs if so configured.

To support alternative 100rel behaviours the following three settings have been added and these can be selected by the Platform Administrator for a specific Interconnect.

Technical Note:
These settings are configured on an individual Interconnects using the Signalling tab.

However, be aware that to avoid unnecessary confusion these settings are not available by default, and must be enabled by Digitalk Support.

Option	Description
Supported	Indicates that 100rel is supported on this interconnect. When configured on an Inbound Interconnect, the initial INVITE will never be rejected based on the presence or the absence of 100rel in either the supported or require SIP header. When configured on an Outbound Interconnect, the outgoing initial INVITE will contain 100rel in the supported SIP header.
Required	Indicates that 100rel is required on this interconnect.

	When configured on an Inbound Interconnect, the incoming initial INVITE will be rejected if 100rel does not appear in either the supported or require SIP header. When configured on an Outbound Interconnect, the outgoing initial INVITE will contain 100rel in the require SIP header.
Blocked	Indicates that 100rel is not permitted on this interconnect. When configured on an Inbound Interconnect, the incoming initial INVITE will be rejected if 100rel appears in the require SIP header. When configured on an Outbound Interconnect, the outgoing initial INVITE will not contain 100rel in either the supported or require SIP header.

Further Configuration Details

To support asymmetric 100rel please ensure the following additional configuration is enabled on relevant Interconnects/Services, as failure to do so may prevent this feature working.

- Media Relay. Media Relay must be enabled for Asymmetric 100rel. Media-interworking in an Open-RTP environment is not possible.
- Transcoding. Transcoding must be enabled on the Service being used.
- Ingress and Egress Interconnects. For this feature to be successfully implemented both interconnects being used in routing must have a Reliable Provisional Response setting that is not set 'Passthrough'. An exception to this is that if an ingress interconnect rejects a call because of the Blocked setting then the egress interconnect settings are not considered.

Note:
Asymmetric 100rel support does not ensure reliability of provisional messages. In the situation of one peer not supporting 100rel then messages will not be provided to or from the peer reliably, and therefore should any provisional message become lost then a corresponding provisional message will not be transmitted. Asymmetric 100rel only ensures that PRACK messages are sent and acknowledged even if the opposing party does not support 100rel. Asymmetric 100rel should only be enabled where one party requires 100rel to be supported for successful traffic to be exchanged, potentially at the risk of messages not being transmitted.