



SIP Objects and Transport Endpoints

Configuring SIP routing in the SIP Security
Controller V1.5

Document Version: V1.0
Date: May 2011

1. Introduction

Version 1.5 of the SIP Security Controller introduces *SIP Objects* as a replacement for the SIP Routing feature in V1.4 and in previous versions. SIP Objects were introduced to provide more flexible options for routing SIP Messages and to enable new features to be added.

V1.4 and previous versions of the SIP Security Controller controlled the flow of SIP messages through a series of SIP Routes. Each SIP route was defined by a single target URI and specified a single destination to route all messages for that destination.

In V1.5 SIP Routes are replaced by SIP Objects. A SIP Object is defined by one or more target URIs and may specify one or more destinations for that URI. While SIP Objects are a little more complex than SIP Routes, they offer many additional benefits including the definition of multiple prioritised destinations for each target which enables resilient call routing.

This document describes the main differences between the 1.4 SIP Routing functions and the new SIP Objects implemented in V1.5.

2. SIP Objects and Transport Endpoints

One of the core functions of the SIP Security Controller is to receive SIP messages and to route them to the appropriate destination. The SIP standard defines a *Request URI* which is included the first line of each SIP message starting a new SIP transaction. The SIP Security Controller makes use of these request URIs to route messages. For example a SIP message starting a new call might start with:

```
INVITE sip:info@um-labs.com:5060 SIP/2.0
```

In this case the request URI is *info@um-labs.com*. Request URIs may include a fully qualified domain name, such as *um-labs.com* or may include an IP address.

The SIP Security Controller uses the term *SIP Object* to define the message routing for all messages sharing one or more Request URIs where those request URIs refer to a single logical service. The service may be a group of SIP trunk circuits or a number of PBX systems serving an identified group of users.

SIP Objects allow multiple Request URIs because it is often useful to treat messages with different Request URIs as equivalent. As an example, the primary request URI for SIP calls to UM Labs is *um-labs.com*, but we also allow *sip.um-labs.com*. If both URIs are added to a SIP Object, then those URIs will be treated as equivalent.

The request URI used to define a SIP object may include both the user and host components, for example *info@um-labs.com*, or just the host component, for example *um-labs.com*. In the first case the definition will apply to the specific URI, in the second case the definition will apply to all users in the *um-labs.com* domain.

Each defined SIP Object includes one or more *Transport Endpoints*. A Transport Endpoint defines where messages matching the SIP Object definition should be sent. A Transport Endpoint

Configuring SIP Objects

definition should include the DNS name or IP address of the destination and may also include the network transport (UDP, TCP or TLS) and the transport port number. Note that in some cases, the network transport and port may be determined by a DNS lookup and need not be specified. Multiple Transport Endpoints are allowed to enable resilient configurations. For example if a SIP Object refers to a SIP trunk service, defining multiple Transport Endpoints will enable resilient call routing. If the trunk's primary circuits fail, calls can be routed to via an alternative circuit or even to an alternative trunk provider.

SIP Object processing is applied only to the first messages in a SIP transaction, for example a REGISTER, an INVITE, a BYE or an OPTIONS request. Other messages within the same transaction are automatically routed by the SIP Security Controller using the facilities defined by the various SIP RFCs (Via headers, Record-Route and Route Header).

SIP Objects are used by the SIP Security Controller to manage a number of advanced features including:

- Registration Initiation and authentication
- Proxy Registrar Functions
- Record-Route Separation

2.1. SIP Object Examples

All SIP Object definitions include at least one Target Domain and at least one Transport Endpoint. The Target domain(s) are used to identify message that match the SIP Object definition, the end-point(s) define where those messages should be sent. Some example SIP Object definitions follow.

2.1.1. Simple Object Definition

Primary Domain: um-labs.com
Type: PBX
Transport Resolution: Manual
Transport End Point Type: DNS A
Hostname: pbx.um-labs.com
Port: 5060
Transport: UDP
Priority: 1

This example illustrates a simple SIP Object definition. In this case the Object defines SIP message routing for messages for the UM Labs domain. All messages are sent to the host pbx.um-labs.com. This is a domain name which must be resolved by the SIP Security Controller using a DNS A record (address) lookup. Messages for this SIP Object are routed to a PBX, so the SIP Object type is defined as PBX. Transport resolution is defined as manual which means that Transport Endpoint details must be manually entered.

2.1.2. Object Definition with Multiple Prioritised End-Points

Primary Domain: um-labs.com
Type: PBX
Transport Resolution: Manual
Transport End Point Type: DNS A
Hostname: pbx.um-labs.com
Port: 5060
Transport: UDP
Priority: 1
Hostname: standby.um-labs.com
Port: 5060
Priority: 2

This example includes two Transport Endpoints. The secondary end-point, standby.um-labs.com with a priority rating of 2 will be used only if the primary End-Point is not available.

2.1.3. Object Definition Using IP Addresses

Primary Domain: 10.1.2.3
Type: Trunk
Dest Map: 62.4.5.6
Transport Resolution: Manual
Transport End Point Type: IP
Hostname: 62.4.5.6
Port: 5060
Transport: UDP
Priority: 1

This example illustrates a configuration commonly used to connect corporate PBXs to SIP trunks where IP addresses rather than fully qualified domain names (FQDN) are used in Request URIs and where the PBX forwards a request using the SIP Security Controller's address in the request URI. In this case the definition also includes a destination map. This means that if a request is received with 10.1.2.3 in the request URI (one of the SIP Security Controller's addresses), the domain part of the request URI is mapped to 62.4.5.6 (the trunk's IP) and the request is forwarded to the trunk. The call flow is illustrated in Figure 1.

Configuring SIP Objects

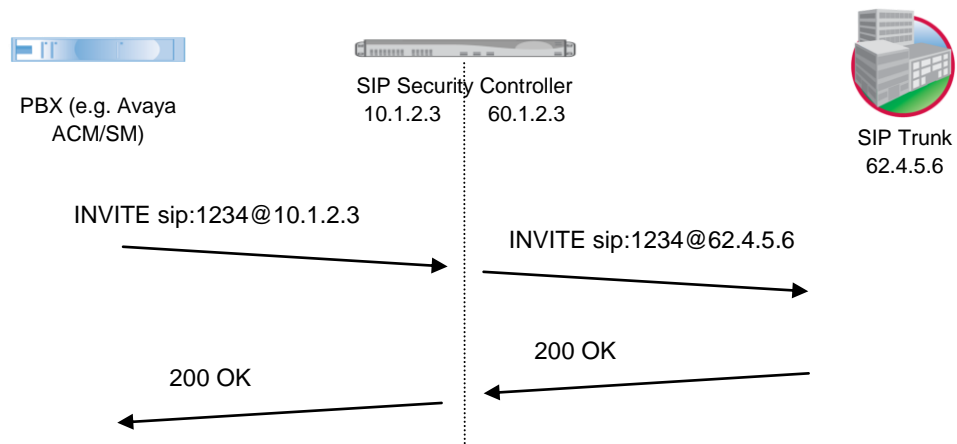


Figure 1 SIP Destination Mapping

2.1.4. Object Definition with Automatic Transport Resolution

Primary Target URI: um-labs.com
Type: PBX
Transport Resolution: Auto

This example defines an Object for a SIP trunk. Transport resolution is defined as Auto which means that the SIP Security Controller should automatically determine the Transport Endpoint by performing a DNS lookup. This will be done by trying DNS lookups in the following order:

1. DNS NAPTR
2. DNS SRV
3. DNS A record

NAPTR (Naming Authority Pointer) is a DNS record type that defines the location and attributes of a service within a domain. When used for SIP, NAPTR records normally define a series of prioritised SVR (service) records which define the name, network transport and port of the domain's SIP server.

For more information on these DNS lookups, refer to a standard DNS reference source, such as the O'Reilly book on DNS and BIND (<http://oreilly.com/catalog/9780596100575/>).

This is the simplest of all SIP Object definitions, but it will work only if the target Domain has the configured their DNS correctly and if NAPTR and/or SRV records are defined for that domain. Unfortunately many SIP trunk providers do not use NAPTR or SRV records. The UM Labs domain does define a set of NAPTR records. If a SIP Object is defined for um-labs.com, and if Transport Resolution is set to Auto, then the SIP Security Controller will use the use the set of Transport Endpoints shown in Figure 2.

Configuring SIP Objects

Transport Endpoints: um-labs.com

	Destination	Port	Type	Order/Pref	Prio/Weight	Available
NAPTR	sip.um-labs.com	5061/TLS	DNS A	5/5	5/5	✘
NAPTR	sip.um-labs.com	5060/TCP	DNS A	10/10	5/5	✘
<input type="checkbox"/>	um-labs.com		NAPTR	10/10		
NAPTR	sip.um-labs.com	5060/UDP	DNS A	15/15	5/5	✘

Figure 2 Auto Transport Endpoints

This set of End-Point direct the SIP Security Controller to send messages to the following locations in decreasing order of priority:

1. sip.um-labs.com via TLS to port 5061
2. sip.um-labs.com via TCP to port 5060
3. sip.um-labs.com via UDP to port 5060

2.2. Authentication and Registration

The SIP Security Controller is able to process SIP authentication and to initiate registration on behalf of a SIP Object. This feature is normally used when the SIP Object refers to a PBX or group of PBXs that are do not support SIP Registration or which cannot be configured to support it. Authentication and Registration can be used to for any combination of:

1. Initiating registration with a second SIP object and maintaining registration status with that object.
2. Responding to authentication challenges on behalf of the SIP object. The SIP Security Controller may be configured to respond to all challenges or to challenges for selected SIP methods (INVITE, BYE, REFER etc).

An example of the use of Registration initiation is the connection of a PBX that does not support outbound SIP registration (for example Avaya ACM with Session Manager) to a SIP trunk that requires registration. This configuration will require that two SIP Objects are defined. The first which for the purposes of this example will be named *pbxobject.com* may be configured to register with a second Object, *trunkobject.com*. This registration will be made on behalf of the Transport Endpoint defined for *pbxobject.com*. After successful registration, inbound calls from the trunk will be relayed to the Transport Endpoint for *pbxobject.com*. The SIP call flow is summarised in Figure 3.

Configuring SIP Objects

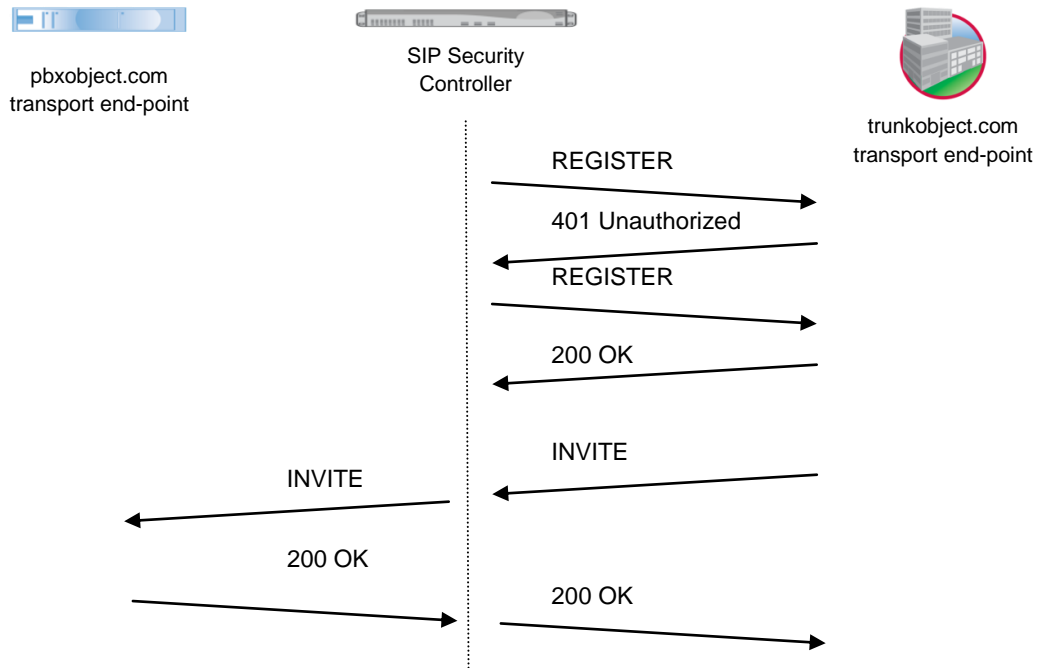


Figure 3 Registration Initiation Message Flow

The SIP Object configuration needed to implement registration initiation and authentication is shown in Figure 4 and Figure 5.

New SIP Object

Domain*: trunkobject.com

Type: PBX Trunk Proxy

Transport Endpoints: Auto Manual

Trusted:

Description: SIP Trunk service

[Advanced Options >](#)

Transport Endpoints

Resolve Method: IP DNS A SRV NAPTR

Destination*: sip.trunkobject.com

Transport: UDP TCP TLS

Port: 5060

Priority: 1

Description:

Figure 4 SIP Object Definition for Trunk

Configuring SIP Objects

New SIP Object

Domain*: ?

Type: PBX Trunk Proxy ?

Transport Endpoints: Auto Manual ?

Trusted: ?

Description: ?

Advanced Options

SIP Domains: ?

B2BUA: ?

Dest Map: ?

Reg Expiry: ?

REFER Mode: Proxy UAS ?

RR Separation: ?

Proxy Registrar: ?

Map Contact URI: ?

Respond Auth Req: ?

Initiate Registration: ?

Target SIP Object: ?

Username: ?

Password: ?

Figure 5 SIP Object definition for PBX

Figure 4 defines the trunk service, while the PBX that will use that trunk is defined in Figure 5. The SIP Object definition for the PBX sets the *Initiate Registration* option. This instructs the SIP Security Controller to send regular registration requests to the Transport Endpoint defined for the target SIP object. If those requests trigger an authentication challenge, then assuming that the *Respond Auth Req* option is selected, the SIP Security Controller will respond to those challenges using the user name and password provided. Any inbound INVITE requests sent to the SIP Security Controller as a result of this registration will be relayed to the Transport Endpoint for the PBX Object.

If the PBX Object sends an outbound INVITE request, this will be forwarded to the trunk. If the trunk responds to that request with an authentication challenge, then the SIP Security Controller will respond to that challenge if the *Respond Auth Req* option is selected.

Note that if *Initiate Registration* is selected, you will almost certainly require the *Respond Auth Req* option to ensure that the SIP Security Controller is able to respond to any authentication challenges. It is however possible to enable *Respond Auth Req* without *Initiate Registration*. In this case the SIP Security Controller will respond to authentication requests on behalf of the PBX object, but will not initiate any SIP requests itself. Note that if *Respond Auth Req* is enabled, then the PBX must be configured to accept all valid SIP requests without requesting authentication. The *Respond Auth Req* option instructs the SIP Security Controller to respond to all authentication requests on behalf of the PBX. It is an error to attempt to have two systems authenticating the same requests.

2.3. Authentication Server Functions

In the authentication examples discussed in section 2.2, the SIP Security Controller is acting as an authentication client, responding to authentication requests with a single user name and

Configuring SIP Objects

password linked to a SIP Object. The SIP Security Controller may also be configured as an authentication server authenticating multiple remote users. In this case a set of user credentials will be defined in a local database or on an external RADIUS server. This function is used when a PBX is unable to authenticate incoming SIP requests or when it is more efficient to have the authentication services provided on a separate system.

Authentication services may be selectively enabled for each SIP Object. This is done by setting authentication policy to local or RADIUS and defining a set of user credentials for that Object.

2.4. Proxy Registrar Functions

V1.5 enhances the authentication services described in section 2.3 by adding a *Proxy Registrar capability*. When the SIP Security Controller receives a SIP Registration Request from a remote user agent (UA), its default behaviour is to relay the registration request to the Transport Endpoint defined by the SIP Object that matches the request. In this configuration if a remote phone sends a SIP REGISTER request then the request will be forwarded to the appropriate Endpoint, normally a PBX, and the PBX will process the registration.

If the Proxy Registrar function is enabled, then the SIP Security Controller will handle all registration processing for the defined SIP Object. This includes authenticating UA registrations. Registration requests are not forwarded to the Transport Endpoint. Subsequent calls and other requests from a registered UA will be forwarded to the Transport Endpoint. Outbound calls to a Registered UA should be sent to the SIP Security Controller using a request URI in the form *sip:username@controllerIP*. The SIP Security Controller will then forward the call with the appropriate Request and Contact URI mappings. An example message flow is shown in Figure 6.

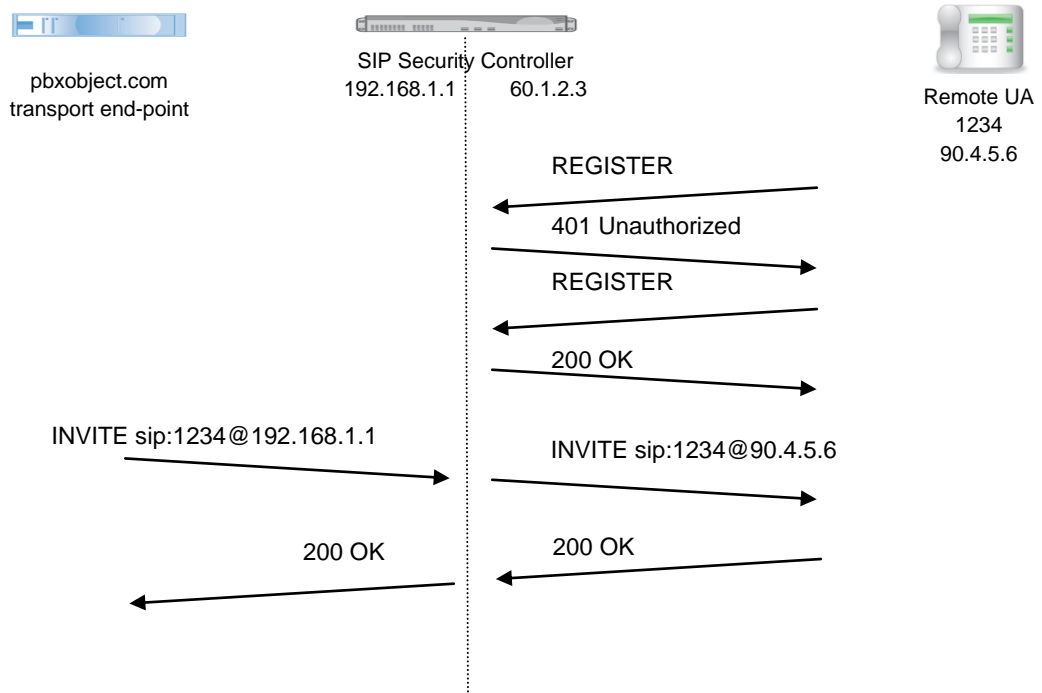


Figure 6 Proxy Registrar Operation

3. Configuring SIP Objects

The SIP Object configuration page is reached via the SIP Objects link on the navigation menu. This page will display any previously configured SIP Objects, or if no SIP Objects exist then a screen to define a new SIP object will be displayed (Figure 7).

New SIP Object

Domain*: ?

Type: PBX Trunk Proxy ?

Transport Endpoints: Auto Manual ?

Trusted: ?

Description: ?

[Advanced Options >>](#)

Figure 7 Defining a SIP Object

As a minimum, the primary domain, the object type and its trust status must be defined. Mark the Object as trusted if it is under local administrative control or it is us a trusted trunk service.

If *Transport Endpoints* are set to auto, then the SIP Security Controller will attempt to automatically determine the Transport Endpoints. This will work only if the domain's DNS entry is correctly defined and if the SIP Security Controller has been configured with a valid DNS. In the case of UM Labs, setting Transport Endpoints to auto generates the following configuration:

If the domain is an IP address or if you wish to specify your own Transport Endpoints, then the manual option should be selected. Transport Endpoint details can then be defined as shown in Figure 8.

New SIP Object

Domain*: ?

Type: PBX Trunk Proxy ?

Transport Endpoints: Auto Manual ?

Trusted: ?

Description: ?

[Advanced Options >>](#)

Transport Endpoints

Resolve Method: IP DNS A SRV NAPTR ?

Destination*: ?

Transport: UDP TCP TLS ?

Port: ?

Priority: ?

Description: ?

Figure 8 Manually defining Transport Endpoints

Configuring SIP Objects

The values that should be entered in each of the fields are summarised in Table 1.

Value	Meaning	Status
Resolve Method	This determines how the SIP Security Controller should interpret the Transport Endpoint. The options are: <ul style="list-style-type: none">• IP Address, treat the destination as a IP address. This Option MUST be used if an IP address is specified.• DNS A, treat the destination as a hostname and perform a DNS A (address) lookup to find the IP address.• SRV, treat the destination as a domain name and perform a DNS SRV (service) lookup to find the IP address, transport protocol and port number.• NAPTR, treat the destination as a domain name and perform a DNS NAPTR (Naming Authority Pointer) lookup. An NAPTR lookup will normally return a number of SRV records which will be used to find the IP address, transport protocol and port number.	Mandatory
Destination	The IP address, domain name or hostname defining this Transport Endpoint	Mandatory
Transport	The transport to use to reach this End-Point	Mandatory if resolve method is IP or DNS A
Port	The port used to reach this End-Point	Mandatory if resolve method is IP or DNS A
Priority	The priority for this End-Point defined as an integer. A SIP Object may have multiple Transport Endpoints, these end-points are used in reverse order of the priority field (low numbers first).	Mandatory if more than one end-point defined.
Description	A short description for this End-Point.	Optional

Table 1 Defining Transport Endpoints

3.1. Advanced Options

Clicking on the advanced options link on the SIP Objects screen, displays an additional set of options (Figure 9).

Configuring SIP Objects

The screenshot shows the 'New SIP Object' configuration window. The 'Domain*' field is set to 'um-labs.com'. The 'Type' is set to 'PBX'. 'Transport Endpoints' are set to 'Manual'. 'Trusted' is unchecked. 'Description' is empty. Under 'Advanced Options', 'SIP Domains' is empty, 'B2BUA' is checked, 'Dest Map' is empty, 'Reg Expiry' is empty, 'REFER Mode' is set to 'Proxy', 'RR Separation' is unchecked, 'Proxy Registrar' is unchecked, 'Map Contact URI' is checked, 'Respond Auth Req' is unchecked, and 'Initiate Registration' is unchecked. Each field has a help icon to its right.

Figure 9 SIP Object, advanced Options

The function and set of allowable values for each of these options is summarised in Table 2. Note that not all of the options defined below will be displayed by default. A number of options are dependent on the settings of other options and will be displayed only when the appropriate settings are selected.

Value	Meaning	Status
SIP Domains	This field allows additional domain names that are equivalent to the primary domain to be defined. The additional domains names should be entered as a comma separated list. The additional names may include a mix of fully qualified domain names or IP addresses. A SIP message where the request URI contains any of the values entered here will be processed in the same way as if it the request URI matched the primary domain.	Optional
B2BUA	Check this box if the Transport Endpoint(s) defined for the SIP object are a back-to-back user agent (most PBXs are). This setting currently has no effect, but it will be used for new features in future versions. It is good practice to select the correct setting now.	Optional
Dest Map	If the request URI of processed SIP transactions should be modified by the SIP Security Controller, enter the mapped value here. See section 2.1.3 for an example of the use of this feature.	Optional
Initiate Registration	If this option is checked, the SIP security controller will send SIP register requests to a second SIP object on behalf of the current SIP object. See section 2.2 for more details of this feature.	Optional, defaults to off

Configuring SIP Objects

Value	Meaning	Status
Reg Expiry	Enter the default registration expiry granted by the Transport Endpoint. This value is used to control registration caching and to control the behaviour or the proxy registrar function.	Optional
Refer Mode	Controls the way that REFER requests are handled. The default setting maps the Refer-To: header of a REFER request to a value that can be understood by external systems such as SIP trunks.	Optional, defaults to Proxy.
RR Separation	<p>Checking this box implements Record-Route separation for messages sent to or received from the Object. When Record-Route Separation is enabled, the SIP Security Controller will ensure that Record-Route headers and Route headers inserted into messages are not forwarded. This feature is implemented by maintaining a record of the Record-Route and Route headers generated and needed by the device communicating with the SIP Object and by the SIP Object. As messages are processed these headers are removed and added as needed to satisfy the requirements of each system.</p> <p>Record-Route separation is useful if a device that make full use of Record-Route headers (for example Avaya ACM or IP Office) needs to communicate with a device that does not support them (for example 3Com NBX). In most cases this option is not needed.</p>	Optional, defaults to off
Proxy Registrar	Enabling this option turns on the Proxy Registrar functions for the SIP Object. The operation of the Proxy Registrar is defined in section 2.4.	Optional, defaults to off.
Map Contact URI	Enabling this option disables Contact URI Mapping. Contact URI mapping is used by the SIP Security Controller to control SIP message routing, particularly if the Security Controller is processing registrations from remoter devices. It is normally required.	Optional, defaults to on.
Respond Auth Req	Enabling the Respond to Authentication Request option will cause the SIP Security Controller to respond to authentication requests on behalf of the defined SIP Object. See section 2.2 for more details on this function.	Optional, defaults to off
Initiate Registration	When this option is enabled, the SIP Security Controller will initiate registrations on behalf of the Transport Endpoint of the current SIP Object to the Transport Endpoint of a second object. See section 2.2 for more details of this function.	Optional, defaults to off

Table 2 SIP Objects, Advanced Settings

4. Converting SIP Routes to SIP Objects

The conversion of a SIP route from a 1.4 system to a SIP object suitable for use in a 1.5 system is relatively simple; just transfer each of the fields of the SIP route to the appropriate field of a new SIP object. The mapping between SIP route and SIP objects is summarised in the following table.

Ref	SIP Route Field	SIP Object Field	Status
1	Target URI	Domain	Required
2	Destination	Transport Endpoint	Required
3	Port	Port	Optional, dependent on Transport Endpoint type
4	Transport Type	Transport	Optional, dependent on Transport Endpoint type
5	Local Domain	Trusted	Optional
6	Destination Map	Dest Map (Advanced Options)	Optional

Table 3 Mapping between SIP Routes and Objects