

# **Configuration Aid To Ingate Firewall/SIParator - RADIUS Accounting Tickets from Ingate Firewall/SIParator**

**Lisa Hallingström**  
Ingate Systems AB



# Table of Contents

<b>How To Use RADIUS Accounting with Ingate Firewall/SIParator .....</b>	<b>3</b>
<b>Ingate RADIUS Accounting.....</b>	<b>5</b>
Accounting attributes used by Ingate Firewall/SIParator .....	6
When Ingate Firewall/SIParator Generates Accounting Data .....	6

## How To Use RADIUS Accounting with Ingate Firewall/SIParator

This is how to configure your firewall/SIParator to use RADIUS Accounting for calls to or from local users.

If you are only interested in accounting for calls to other domains, you only have to turn the RADIUS Accounting on.

If you want to bill for local calls too, you will have to force the users to go via the firewall/SIParator even when they are both on the same side. For this, the firewall/SIParator will have to act as a back-to-back user agent (B2BUA) for all calls.

This feature is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.

First, define the RADIUS server to receive accounting ticks. This is done on the **RADIUS** page. If the RADIUS server should only be used for accounting, you can enter any port number in the table. The firewall/SIParator will use port 1813 for accounting.

If you use the firewall/SIParator as the SIP registrar, and the RADIUS server should be used for SIP authentication as well, you need to enter the port number on which the RADIUS server listens for authentication requests (usually ports 1812 or 1645).

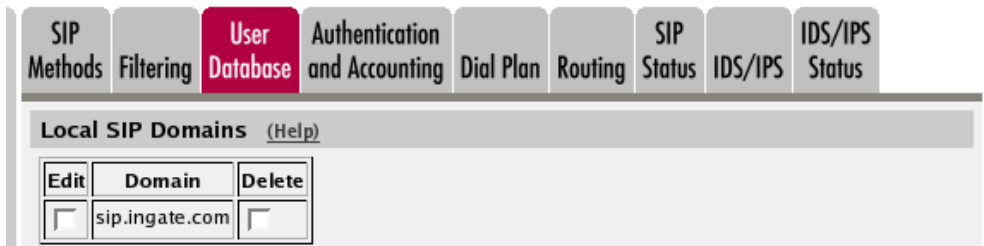
The screenshot shows the RADIUS configuration interface. At the top, there are tabs for 'Basic Configuration', 'Access Control', 'RADIUS', 'SNMP', 'DHCP Server', 'DHCP Server Status', 'Dynamic DNS Update', 'Certificates', and 'Advanced'. The 'RADIUS' tab is active. Below the tabs, there is a section titled 'RADIUS Servers (Help)'. It contains a table with the following data:

Edit Row	RADIUS server		Port	Secret	Delete Row
	DNS name or IP address	IP address			
<input checked="" type="checkbox"/>	193.180.23.77	193.180.23.77	1812	Change Secret	<input type="checkbox"/>

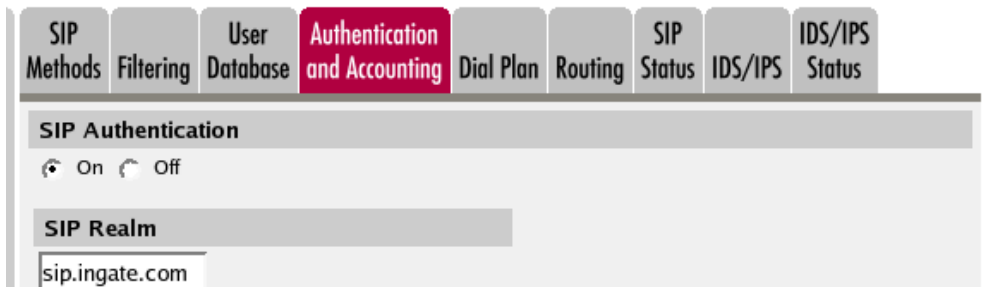
Below the table, there is a field 'Add new rows' with the value '1' and the text 'rows.'. Below that, there are two sections: 'Contact IP Address (Help)' with a dropdown menu showing 'Inside (10.47.2.243)', and 'Identifier (Help)' with a radio button for 'Use NAS-IP-Address' set to 'Yes' and a text field for 'NAS-Identifier'.

Define a local SIP domain. This can be any domain name you like, as long as it isn't an existing domain somewhere else. A good choice is to use your company www domain, but replace the "www" with "sip", like *sip.ingate.com*. The same domain can also be used in pure SIP-to-SIP calls.

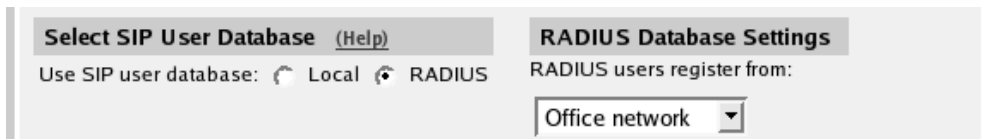
This domain should be entered on the **User Database** page under **SIP Traffic**.



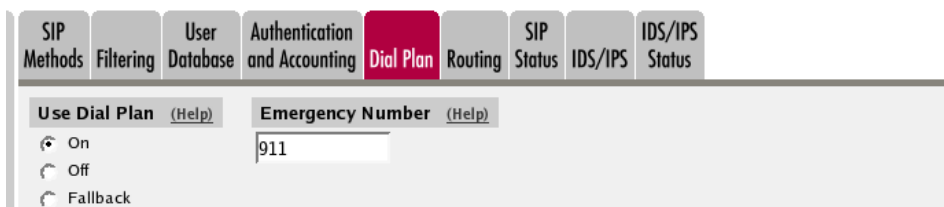
Go to the **Authentication and Accounting** page and turn authentication on. Also enter your SIP domain as the Realm.



If the firewall/SIParator should be used as registrar, you select to use the RADIUS user database for SIP users and also select which network the SIP users can register from.



On the **Dial Plan** page, you define how calls should be routed through the firewall/SIParator. First, turn the Dial Plan on.



In the **Matching From Header** table, you define from which network the calls can come. You can also select what the From header (that tells who is calling) should look like. This is used when matching requests in the **Dial Plan** table below. For this example, you only need one criterion to match on; all calls should be treated the same, regardless of origin.



In the **Matching Request-URI** table, you define call destinations. This is used when matching requests in the **Dial Plan** table below.

In this case, you want to define a **Reg Exp** (regular expression) which matches all Request-URIs. Enter "(.+)"@(.+)" in the Reg Exp field.

Matching Request-URI (Help)									
Edit Row	Name	Use this ...					... or this		Delete Row
		Prefix	Head	Tail	Min. Tail	Domain	Reg Exp		
<input type="checkbox"/>	Any			-			(.+)\@(.+)	<input type="checkbox"/>	

In the **Forward To** table, you define where calls should be forwarded. This is used in the **Dial Plan** table below.

In this case, the calls should be forwarded to their original destination, but the firewall/SIParator should forward them as a B2BUA. Enter "\$0;b2bua" in the Reg Exp field. This will reuse the incoming Request-URI, but make the firewall/SIParator act as a B2BUA instead of a proxy.

Forward To (Help)								
Edit Row	Name	Subno.	Use this ...	... or this			... or this	Delete Row
			Account	Replacement URI	Port	Transport	Reg Exp	
<input type="checkbox"/>	+ Same but b2bua	1	-				\$0;b2bua	<input type="checkbox"/>

At last, you combine these definitions in the **Dial Plan** table. Make a new row in the table and select the definitions from the tables above.

Dial Plan (Help)											
Edit	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete
						Forward	ENUM				
<input type="checkbox"/>	1	Any	Any	Forward	Same but b2bua			-	-	Use the builtin B2BUA	<input type="checkbox"/>

Now, when a SIP user calls another SIP user, the firewall/SIParator will step in and always stay in the path for the call. Both SIP clients will signal to the firewall/SIParator only, and the firewall/SIParator will forward signaling between them. Media will still go directly between the clients.

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

Save/Load Configuration
Show Configuration
User Administration

**Test Run and Apply Conf (Help)**

Duration of limited test mode:

seconds

Apply configuration

## Ingate RADIUS Accounting

Ingate Firewall/SIParator supports RADIUS Accounting as described in RFC 2866.

RADIUS Accounting adds the ability to deliver accounting information about SIP calls from a firewall/SIParator to a RADIUS Accounting server.

RADIUS Accounting is enabled or disabled by a GUI setting. The configuration of RADIUS servers is shared with RADIUS authentication. This means that accounting and authentication uses the same list of servers, and that there is no way to use a specific server for only one or the other of the services. RADIUS Accounting always uses port 1813.

### Accounting attributes used by Ingate Firewall/SIParator

Attribute	No.	Format of value or text	Sample
User-name	1	String of UTF-8 characters	sip:alice@ingate.com
NAS-IP-Address	4	Four octet IP address	193.45.23.245
NAS-Identifier	32	One or more octets	
Acct-Session-Id	44	String of UTF-8 characters	ea1bba66464748908df9f7aa9a439e
Acct-Status-Type	40	Four octets (32 bit unsigned value)	2
Called-Station-Id	30	String of UTF-8 characters	sip:bob@ingate.com 10.17.244.14
Calling-Station-Id	31	String of UTF-8 characters	sip:alice@ingate.com 193.45.23.1
Acct-Session-Time	46	Four octets (32 bit unsigned value)	180
Acct-Terminate-Cause	49	Four octets (32 bit unsigned value)	1

The attributes follow RFC 2865 and RFC 2866, where more information can be found.

The *Acct-Session-Time* and *Acct-Terminate-Cause* are sent when the *Acct-Status-Type* is "Stop".

### When Ingate Firewall/SIParator Generates Accounting Data

The Ingate Firewall/SIParator generates accounting information when accounting is enabled in the configuration and at least one of the following conditions is true:

- Media is handled by the firewall/SIParator, i.e. every case when the media traverses through the firewall/SIParator, or when Remote SIP Connectivity is used for the specific call.

*Configuration Aid To Ingate Firewall/SIParator - RADIUS Accounting Tickets from Ingate Firewall/SIParator*

- The firewall/SIParator acts as a B2BUA. This requires that the SIP Trunking or the Advanced SIP Routing module is installed, and that at least one of the criteria below is met:
  - An XF or B2BUAWM account is used for the specific call.
  - Regular Expressions are used in the **Matching Request-URI** and **Forward To** tables, and the Regular Expression in the **Forward To** table ends with a ";b2bua".
  - **Local REFER Handling** is used for the call.
- **Force Record-Route for All Requests** is used.

To test RADIUS Accounting with Ingate Firewall/SIParator, FreeRADIUS (<http://freeradius.org/>) or any commercial RADIUS server supporting RFC 2866 can be used.