



# RC-2100 SIP Security Controller

---

## User and Administration Guide

Software Release: V1.4

Document Version: V1.0

Date: January 2010

## Table of Contents

1. Introduction .....	4
1.1. Applicability.....	4
2. Getting Started.....	5
3. SIP Security Controller Architecture .....	7
3.1. IP Level Security .....	7
3.2. Application and Protocol Security.....	8
3.3. Content Security .....	9
4. SIP Security Controller Deployment.....	11
4.1. Perimeter Security Gateway .....	11
4.2. Remote Devices .....	12
4.3. DNS Configuration.....	14
5. ZRTP Key Exchange, deployment and operation .....	15
5.1. ZRTP Deployment.....	17
5.2. ZRTP Enrolment .....	17
6. Installing the RC-2100 .....	19
6.1. Unpack and Connect to the Network .....	19
6.2. Establish a web connection to the RC-2100 .....	19
6.3. First Login .....	20
7. RC-2100 Console Interface.....	22
7.1. Connecting to the console .....	22
7.2. Console Menu Functions.....	22
7.2.1. Show Interface IP Addresses.....	23
7.2.2. Change Interface eth0 IP Address.....	23
7.2.3. Emergency Reset Functions .....	23
7.2.4. Reboot the System.....	23
8. Configuration Management.....	24
9. Basic Configuration .....	27
9.1. Network System Settings .....	27
9.2. Network Interfaces .....	29
9.3. VLANs .....	32
9.4. Static Routes .....	32
9.5. SIP Routing .....	33
9.6. Advanced Firewall Control .....	35

10.	SIP Authentication .....	39
10.1.	Registration Caching .....	40
11.	Encryption Management .....	42
11.1.	Certificate Management .....	42
11.2.	Trusting and using the RC-2100's certificate .....	44
11.3.	Media Encryption .....	46
11.4.	Media Encryption with SDES Key Exchange .....	46
11.5.	ZRTP Management .....	47
12.	Logging and Reporting .....	49
13.	User Management .....	51
13.1.	System Administrators .....	51
13.2.	SIP Users .....	51
14.	Product Licensing .....	53
15.	Software Updates .....	54
16.	System Monitoring .....	55
16.1.	Dashboard .....	55
16.2.	Status Graphs .....	56
16.3.	System Status .....	56
16.4.	SNMP Management .....	57
17.	Advanced Topics .....	58
17.1.	SIP Trunks .....	58
17.1.1.	Service Provider Trunks .....	58
17.1.2.	Private Trunks .....	60
17.2.	Deploying the RC-2100 behind a Firewall .....	61
17.3.	Configuring an external syslog server .....	62
18.	Glossary .....	64
19.	Appendix 1, Time zones .....	68

## **1. Introduction**

The RC-2100 SIP Security Controller from UM Labs Ltd is designed to provide security for any VoIP system or network running the Session Initiation Protocol (SIP) or for an application server providing SIP based applications.

This manual is designed to guide you through setting up and configuring the RC-2100. Section 0 of the manual is designed to provide a quick start to enable you to install the system and complete the basic set up. The remaining sections cover other topics in more detail.

Sections 3 and 4 provide details of the product's architecture and offer some advice on product deployment.

Section 6 covers product installation in more detail than section 2 while sections 7 to 16 provide a detailed reference to configuring the RC-2100.

Finally, section 18 provides a glossary, defining some of the terms used in this manual.

### **1.1. Applicability**

This manual is applicable to the RC-2100 SIP Security Controller running software release V1.4.

## 2. Getting Started

This section is designed to highlight the main points of the initial installation and configuration of the RC-2100 SIP Security Gateway, to enable you to get the system running quickly and configured to the extent that in most cases it will be possible to make some basic calls. For more detailed guidance on configuring the system, please refer to the other sections of the User and Administration Guide.

### Quick-start overview

The RC-2100 ships with interface eth0 configured with IP address 192.168.1.1. To configure the system, connect eth0 to a network hub, configure your workstation with an address in the same sub-net (for example 192.168.1.2), connect your workstation to the same hub, launch your browser and connect to <https://192.168.1.1>. Login as *admin* and enter *password* in the password field. After setting a new password for the admin account you will be able to re-configure the system's network settings and proceed with the rest of the installation.

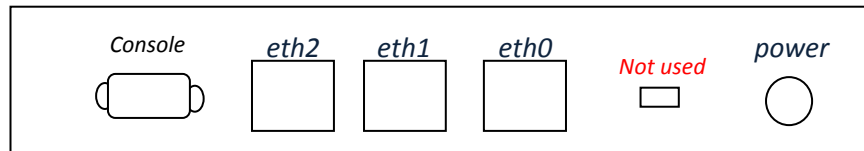
Alternatively, you may change the address of eth0 by connecting to the RC-2100 console interface. Changing the eth0 address avoids the need to reconfigure a workstation solely for configuring the RC-2100. Refer to section 7 of the User and Administration Guide for help with connecting to and using the console.

Ensure that you correctly set the system's time and date before completing the initial configuration. You can this either by defining an NTP server (section 9.1 of the manual) or by manually setting the time. *NOTE: the system will not process calls until the time and date are correctly set.*

Refer to the User and Administration Guide (the manual) for help with the rest of the installation.

### Step 1

Unpack your RC-2100 and connect the system to an Ethernet hub using interface *eth0*. Connect the power supply, the system will boot and be ready for configuration in approximately 3 minutes. Eth0 and the power connector are located on the rear of the system.



### Step2

Interface *eth0* is pre-configured with IP address 192.168.1.1. Configure a system with a browser capable of supporting HTTPS (e.g. IE6, IE7 or Mozilla) with a temporary IP address in the same sub-net (e.g. 192.168.1.2). Then connect that system to the same hub as the RC2100, launch the browser and connect to <https://192.168.1.1>. If you have changed the eth0 IP address via the RC-2100 console menu then point your browser to that address rather than 192.168.1.1.

- Step 3** Ignoring the warnings about the certificate not matching the system name and about the certificate's trust status, login to the RC-2100 as *admin* entering *password* as the password. Generating your own certificate to avoid these warnings in future is discussed in section 11 of the manual.
- Step 4** Assign a new password to the admin account when prompted. Take care not to forget the assigned password as there is no way to recover a lost password.
- Step 5** Visit the *Network System Settings* page of the Admin GUI and set up the network environment. This includes assigning a system name and configuring Domain Name Servers. It is also strongly recommended that at least one Network Time Protocol (NTP) server is defined. You must also configure a *default gateway*, this is normally the IP address of the router that provides your Internet connection. The *Network System Settings* page is more fully described in section 9.1. of the manual
- Step 6** Visit the *Network Interfaces* page of the Admin GUI and assign the network addresses that will be needed in the system's final location. You will normally assign addresses to two of the three interfaces. It does not matter which two interfaces you pick, but a good convention is to use eth0 for your LAN (and connections to your PBX) and eth1 for your Internet connection. Eth2 can be used for any purpose (for example connecting to a different LAN subnet or used as a dedicated management interface). The Network Interfaces page of the Admin GUI is more fully described in section 9.2 of the manual.
- Step 7** Visit the SIP Routing page of the GUI and define the location of your PBX. The RC-2100 will support multiple PBXs. You will need to enter at least the fully qualified domain name (FQDN) or IP address and SIP domain(s) that each PBX serves. The SIP Routing page of the GUI is more fully defined in section 9.5 of the manual
- Step 8** Click on *Save* in the configuration section at the foot of the SIP Routing Page. The browser will switch to the *Configuration Management Page*. Enter a name for the new configuration and set the configuration active.
- Step 9** Reboot the system to activate the new configuration. The system may be rebooted from the *Status and Diagnostics* page (section 16.3).
- Step 10** Visit the *Status and Diagnostics* page again (section 16.3) to check that all required services are running. Note that the SIP Security Engine may not run until the system time is correctly set.

### 3. SIP Security Controller Architecture

Each product in the range of SIP Security Controllers from UM Labs is designed to provide security controls for VoIP and related applications running over the Session Initiation Protocol (SIP) and to provide facilities to support the deployment and operation of SIP networks and applications.

The security threats that face SIP networks can be categorised into 3 main groups:

- Generic IP level security threats. These threats are faced by all IP applications and networks.
- Application and protocol level threats. These threats are specific to the Session Initiation Protocol and the applications that run over the protocol. The threats include call flooding, call hijacking and other call disruption attacks. Left unaddressed, these threats can cause significant disruption to a SIP network, even leading to complete service failure.
- Content level threats. These threats target the content of a voice call, video conference or other SIP session. The threats include unwanted calls, unauthorised call monitoring and for SIP applications capable of transmitting data payloads, malicious content.

The UM Labs SIP Security Controllers are designed to address each of these threat groups.

#### 3.1. IP Level Security

Generic IP level security threats are handled by a robust IP firewall module that is fully integrated in the SIP Security Controller and also customised to process the SIP messages and the RTP media streams that handle voice or video traffic. To ensure a high level of security protection, the firewall module is designed to meet the requirements of the U.S. Government *Firewall Protection Profile for Medium Robustness Environments*. Conformance to this protection profile ensures that the security requirements of all commercial applications and all but the most demanding defence applications are met.

While standard firewalls also provide IP level security, the design of SIP and the nature of the applications it drives means that VoIP applications do not fit well into the firewall security model. All firewalls implement Network Address Translation (NAT). This is done partly for security and partly to provide the necessary translation between private LAN network addresses and public Internet addresses. NAT changes the source and/or destination address of a packet as it passes through the firewall. A problem arises when the protocol packets include embedded network addresses. General purpose firewalls do not examine packet contents and so cannot translate these embedded addresses. In VoIP packets, the embedded addresses define the end-points of a call, without these addresses the call will not work.

This means that not only do general purpose firewalls fall short in protecting a VoIP system from application, protocol and content threats, but the NAT transformations they apply to VoIP messages actually break the protocols. VoIP system designers have to go to great lengths to work around these problems. There is a real risk that these problems force the firewall into a

configuration where the level of security it provides for both voice and data applications is compromised. This risk is magnified whenever a VoIP connection has to pass through more than one firewall or NAT gateway, for example when a home worker makes a call via a DSL router and then through the corporate firewall to the IP-PBX. When a VoIP connection has to pass through a second NAT gateway some of the work-arounds used to address the NAT challenges fail. This problem, the problem of *Far-end NAT traversal*, is well known.

By implementing the IP level security provisions in a purpose-designed product that is capable of processing the higher level protocols, the operation of the firewall module can be tailored to support those protocols and to avoid the limitations of a general purpose device.

### 3.2. Application and Protocol Security

The application and protocol security controls in UM Labs' SIP Security Controller products are provided by a *Stateful SIP Proxy*. The proxy is both *SIP Transaction* and *SIP Dialog* stateful. This means that the proxy retains information about the state of a call or other SIP session for the duration of that call. By maintaining this level of state the Security Controller is able to verify each SIP message that it processes therefore ensure that only fully authorised and validated messages are accepted.

The UM Labs SIP proxy implements the recommendations for stateful SIP Proxies defined in the SIP standard (RFC 3261) ensuring interoperability between other standards conformant SIP products.

The level of state information retained by the SIP proxy in the UM Labs SIP Security Controller products is completely different from the state information stored by a *Stateful Inspection Firewall*. The state information retained by a Stateful Inspection firewall allows the firewall to identify the different packets that are sent on over an IP network and to assign each packet to a session. A session might connect a web browser to a web server or send an email message. Stateful inspection does not provide the firewall with any information on that session, and may not even differentiate between different applications. In contrast, UM Labs' SIP proxy has a complete understanding of the status of all phones or other SIP devices that communicate via the SIP Security controller. This means that the Security Controller knows which phones are active and are able to make or receive calls. It stores information of the status each active call and is able to verify any requests to modify that call, for example to transfer it or to terminate it.

The state information held by the SIP proxy for each active device or call means that it is able to apply a full set of NAT transformations to each SIP message that it processes. This has two benefits, firstly this addresses *all* of the NAT and far-end NAT traversal challenges that standard Firewalls introduce and secondly that the SIP Security Controller can act as an application level proxy in the standard IP network level sense. This means that when installed on the boundary between two networks, the SIP Security controller is able to hide the details of each network from the other. This is the way that proxies for applications such as web and email operate, and makes good security sense on IP networks.

The SIP proxy also controls a second proxy, the RTP proxy. For VoIP applications, the RTP proxy handles the *call media*, the voice or video stream. The end-points for the media stream, defined

as IP address and Ports, are negotiated separately for each call. This negotiation is the responsibility of the SIP protocol using a 3<sup>rd</sup> protocol, Session Description Protocol (SDP) to define these end-points. The UM Labs' SIP proxy mediates in this negotiation providing the necessary address and port mapping to ensure that the media stream can pass through any intermediate NAT gateways. The mediation means that the SIP proxy can record the RTP end-points as part of the state information held for that call. These details are the used to instruct the RTP proxy to accept the media stream for that call. This linkage between the SIP proxy which is responsible for Signalling and the RTP proxy which handles media provides import security controls as it ensures that a media stream is permitted only if the signalling protocol has correctly set up the call. These controls block security threats such as *Call Hijacking* and *RTP Injection* which rely on introducing unauthorised media streams. Such controls are not possible with standard firewall devices.

Additional application and protocol security controls are provided by the validation of all SIP messages. Any malformed or undecipherable messages are rejected. This protects the SIP network from *fuzzing* attacks and also minimises the impact of badly configured or faulty VoIP equipment.

Many of the application and security level threats faced by VoIP systems can be handled by authenticating SIP requests. SIP requests trigger events such as placing a new call, terminating a call, transferring a call and registering a phone with a PBX. Registration is needed so that calls can be routed to the appropriate phone. The SIP standard defines a mechanism for authenticating most SIP requests. Of the 14 different SIP requests currently defined, the standard allows 12 request types to be authenticated. The SIP Security Controller can authenticate all 12 on these requests.

Finally, the SIP Security Controller protects the call setup traffic by providing TLS encryption for signalling. TLS is the standard method of encrypting SIP signalling.

### 3.3. Content Security

The content security controls in UM Labs' SIP Security Controller products protect against threats including unwanted calls and unauthorised eavesdropping. The protection against unwanted calls stems from the SIP authentication and encryption services provided as part of the application and security controls. These controls are supplemented by placing limits on the rate at which calls can be accepted both globally and by call source.

Unauthorised call eavesdropping is prevented by encrypting the media steam. The UM Labs SIP Security Controller uses SRTP to provide media encryption. This is the standard for RTP encryption and is implemented using 128 bit AES, a strong encryption algorithm. The UM Labs SIP Security Controllers provide two alternative key exchange options. Option 1 is SDES (RFC 4568), where the key is agreed as part of the media end-point negotiation (using SDP). The other option is Phil Zimmermann's ZRTP.

SDES provides a basic level of security, as the security of the media encryption key relies on using an encrypted signalling stream (SIP over TLS). Any SIP gateways between the call endpoints must decrypt the signalling stream in order to correctly process the call, so the media encryption

key will be visible to those intervening gateways. The UM Labs SIP Security Controllers provide a gateway implementation of SDES/SRTP which means that the encrypted media stream is always terminated on the gateway. This implementation is suitable for securing the media streams from remote or roaming users and providing a front-end for SIP devices that are unable to support SRTP. Where appropriate, the SIP Security controller will provide back-to-back media encryption establishing two SDES/SRTP sessions between the gateway and the call end-points.

ZRTP establishes a SRTP encryption key over the media stream using a *Diffie-Hellman* key exchange including the Elliptic Curve variant (*ECDH*). By separating key negotiation from the signalling stream, ZRTP avoids many of the weaknesses of other key exchange protocols. For further details on ZRTP see the FAQ at <http://www.zfoneproject.com>. The UM Labs SIP Security Controllers support gateway ZRTP, further details of this option are provided in section 5.

## 4. SIP Security Controller Deployment

UM Labs's SIP Security Controllers are designed to provide security for SIP based applications including VoIP, video calls and other SIP applications including Instant Messaging (IM) and presence based applications. The security controls provided by the UM Labs products include protection against the following security threats:

- Protection for VoIP application servers and gateways enabling external connections to SIP trunks, remote users and other SIP domains
- Protection of other components of the networks from the threats resulting from permitting VoIP traffic to pass through a standard firewall
- Protection for all components of the VoIP network from SIP flooding and call disruption attacks
- Protection against unauthorised call monitoring and eavesdropping.

To ensure the effective implementation of these security controls, the deployment of the SIP Security Controller must be carefully planned.

### 4.1. Perimeter Security Gateway

In most cases the SIP Security Controller will be installed at the network perimeter, providing a dedicated security gateway for all SIP traffic and for any traffic that is generated as the result of a SIP dialog (for example a RTP Media stream). In this configuration, the SIP Security Gateway should be thought of as dedicated Perimeter Security Gateway providing IP level security for VoIP traffic in addition to the SIP application level security controls and protection against content threats. The recommended network layout is shown in Figure 1.

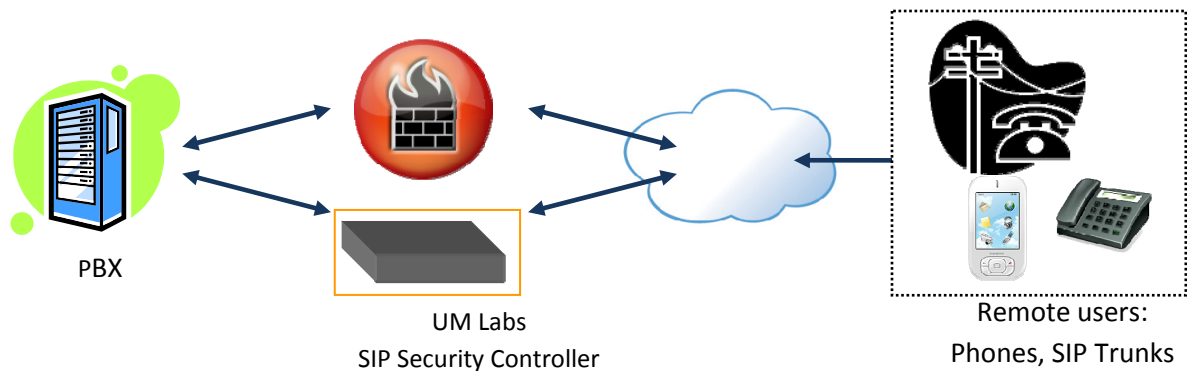


Figure 1 SIP Security Controller Deployment

The PBX should be configured so that its IP route to external networks is via the UM Labs SIP Security Controller. This requirement can be met in one of 3 ways:

1. Define the UM Labs SIP Security Controller as the default gateway for the PBX. This approach is appropriate if the PBX and the SIP Security Controller share a common IP subnet and if the majority of non-local traffic to and from the PBX is to be relayed via the SIP Security Controller.
2. Define one or more static routes on the PBX directing traffic via the SIP Security Controller to a number of defined remote destinations.

3. Set up a static route or use policy based routing (source, destination or protocol based) on a router between the PBX and the SIP Security Controller to direct SIP traffic destined for external locations via the SIP Security Controller.

The recommended deployment has the SIP Security Controller installed in parallel with a general purpose firewall. This configuration is strongly recommended for two reasons. Firstly, the SIP Security Controller is designed to handle SIP and related protocol traffic applying the necessary address mappings to the SIP signalling and allocating the media end-points. This means that RTP streams may be correctly processed without the need for the general purpose firewall to open a large range of ports. Secondly the IP level security module included in the SIP Security Controller provides Firewall grade security for the VoIP and related traffic that it processes. This means that deploying the SIP Security Controller in parallel with a general purpose firewall does not compromise the network's security controls. On the contrary this deployment offers better security than attempting to configure the firewall to relay SIP traffic.

If corporate security policy prevents the recommended parallel deployment, then it is possible to connect the SIP Security Controller to a Firewall DMZ or to an internal network segment. This is very much a second best option because the firewall will need to be configured to allow both SIP and RTP traffic to pass through to the SIP Security Controller. These necessary configuration changes could reduce the level of security that the firewall provides to the rest of the network. In addition the Network Address Translation (NAT) functions on the Firewall will require additional configuration on the SIP Security Controller. This additional configuration needed on both the firewall and the SIP Security Controller is discussed in section 17.2 of this manual. Finally the SIP Security Controller is designed to ensure that RTP media packets are processed without introducing delay or *jitter* that could reduce the voice quality on VoIP calls. This benefit is lost if the RTP media also has to pass through a general purpose firewall.

### 4.2. Remote Devices

The configuration required to enable a remote device, such as a SIP software phone or a hardware phone to connect and make calls via the SIP Security Controller depends on whether or not the device is in a local domain.

SIP uses domains in much the same way as email and web applications. A SIP address, or more correctly a SIP *URI* looks a lot like an email address or web URI. SIP URIs include a user component and a domain component. For example the following SIP URIs are both within the um-labs.com domain:

```
sip:info@um-labs.com  
sip:400@um-labs.com
```

The user component of a SIP URI can be a name or a number. While the domain component is normally a domain name it may be any IP address, so the URI `sip:400@80.1.2.3` is a syntactically valid SIP URI.

The SIP Security Controller defines a domain as local if the SIP application server that routes calls for that domain is under the same administrative control as the SIP Security Controller. There is

no limit on the number of local domains that the SIP Security Controller can handle, but each should be defined as local with an entry in the SIP Routing table. The routing table entry will define the name or address of the SIP application server that controls that domain.

If a remote device is in a local domain then that device should be configured so that its SIP Registration requests are sent via the SIP Security Controller. The Security Controller will then forward those requests to the application server for this domain. For most SIP devices this means entering the SIP security controller's domain name as a SIP Proxy or Outbound Proxy. As an example, on a CounterPath eyebeam phone the SIP Security Controller's domain name should be entered in the Proxy box (see Figure 2 where sip.um-labs.com is the domain name of the security controller for the UM Labs domain).

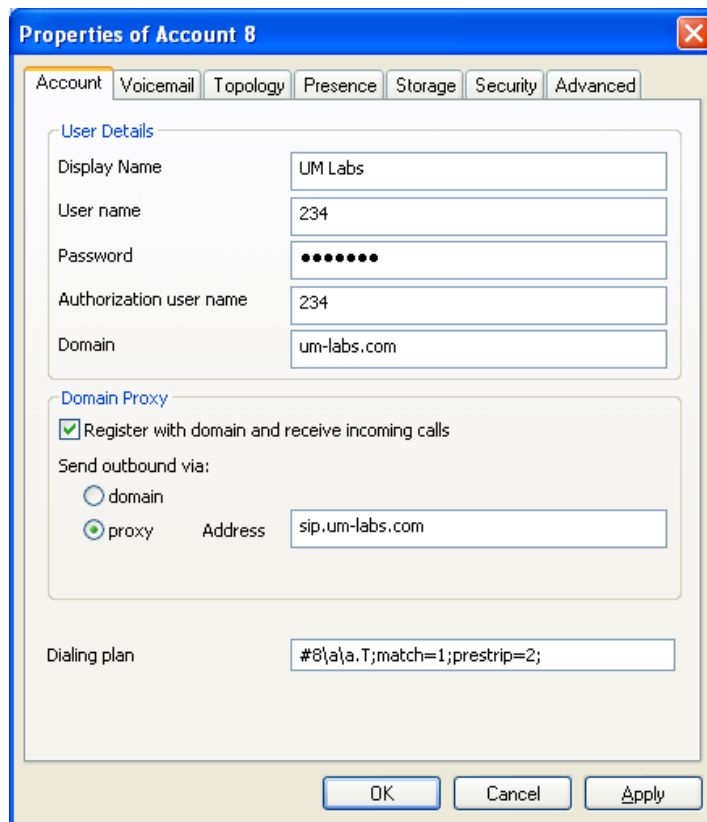


Figure 2 CounterPath Soft--phone Configuration

Devices in local domains have special privileges, they are able to place calls to other devices in local domains and to non local domains.

If a remote device is not in a local domain then no special configuration is needed. Assuming the device is configured to make calls to other SIP domains, and assuming that the SIP Security Controller and the required supporting services are configured to allow calls from non-local domains the remote device can place calls to any of the local domains protected by the SIP Security Controller simply by calling the SIP URI. The SIP Security Controller places restrictions on non-local domains; devices in those domains are allowed to call URIs within a local domain, but not URIs in non-local domains. This restriction prevents unauthorised call relay and toll fraud.

### 4.3. DNS Configuration

To enable devices in local domains to send their registration requests and subsequent calls via the SIP Security Controller and to enable devices in other domains to call users in a local domain, the SIP Security Controller's domain name and IP address need to be added to the Domain Name Server that handles the local domain or domains.

There are two options for configuring DNS entries for SIP devices. The first is to add a simple A (address) record, mapping the devices fully qualified domain name to an IP address. The second and better option is to make use of SRV records. An SRV record allows devices to find the location and other details about an application server for a domain. In the case of SIP, correctly setup SRV records define the location of the SIP server for the domain and define the preferred transport. The DNS data for the UM Labs domain includes the following entries:

```
; SRV records
; Offer TLS/UDP TLS higher priority (lower value)
;
;      pri wt port
_sip._udp.um-labs.com.  IN      SRV      15  5 5060      sip.um-labs.com.
_sip._tls.um-labs.com.  IN      SRV      5   5 5061      sip.um-labs.com.
;
; A records
sip                IN      A        217.154.219.173
;
```

Figure 3 Example DNS Entries

The first two entries define the two available SIP transports for this domain (UDP and TLS). TLS has a lower priority value (higher priority) than UDP so connecting devices should use secure TLS in preference to unsecured UDP. In both cases the server is sip.um-labs.com and the default ports and UDP and TLS transports (5060 and 5061) should be used. The third entry is a standard A record defining the IP address for that server. Refer to the documentation for your local DNS for more information on this topic.

You will of course need to ensure that the appropriate SIP transports are enabled on your Security Controller (see section 9.2).

## **5. ZRTP Key Exchange, deployment and operation**

Version 1.2 of the UM Labs SIP Security Controller, includes support for ZRTP protocol version 1.0 and is compatible with other devices running the same version. Protocol version 1.0 is the version described in the latest ZRTP Internet Draft which has been submitted to the IETF. The draft may be viewed at:

<http://tools.ietf.org/html/draft-zimmermann-avt-zrtp>

ZRTP support is provided as an additional cost optional.

ZRTP is a key exchange protocol designed to securely negotiate media encryption keys for use by the Secure Realtime Transport Protocol (SRTP). SRTP in-turn protects a media stream (voice or video) from wiretapping and unauthorised eavesdropping by encrypting the media stream and thus enabling a VoIP user to make encrypted calls.

The encryption keys used by SRTP must meet some specific requirements. SRTP uses the Advanced Encryption Standard (AES) which is a symmetric cipher. SRTP therefore requires that communicating devices establish shared secret keys, as the same key is used to encrypt and to decrypt a media stream. Each VoIP call needs a minimum of two keys as separate key is used for each media stream. A simple voice call has two media streams (one in each direction) while a video call will need at least 4 keys (two for voice, two for video). The lifetime of the keys is limited to the duration of the call; keys are discarded when the call ends. SRTP does not define how the encryption keys are set up, this task is left to other protocols.

There are a number of key exchange protocols designed for use with SRTP. The two most widely implemented are SDES (defined in RFC 4568) and ZRTP. The UM Labs SIP Security Controller supports both of these protocols.

SDES is a simple protocol; it exchanges SRTP keys along with other media parameters as part of the call setup. Call setup messages are transported by a signalling protocol such as the Session Initiation Protocol (SIP). To maintain SRTP key security and integrity the signalling protocol must be encrypted, with SIP this is achieved by using TLS, the same protocol that is used to secure access to web sites. The problem with this approach is that it is difficult and sometimes impossible to ensure end-to-end security of the TLS connection. Intermediate devices that are responsible for call routing must be able to process the signalling stream in order to correctly handle the call. This inevitably means that those same devices will be able to monitor the SDES key exchange. This limitation means that SDES is suitable only for use where the end-to-end integrity of the signalling stream can be assured. In practice this limits the use of SDES to securing calls over trusted network links.

ZRTP has been designed to address these limitations. ZRTP is a key exchange protocol that runs over the media stream. This means that its security and integrity are not dependent on the signalling stream. ZRTP also includes some specific defences against Man-in-the-Middle (MitM) attacks and can therefore detect any attempt by a network operator, a service provider or a malicious attacker to intercept or modify the key exchange.

This design means that ZRTP is suitable for use on all VoIP calls including those that cross network boundaries or are made in geographical regions where the security and integrity of regular calls cannot be assured. This has prompted the development of ZTRP for a range of devices; it is now possible to make ZRTP protected VoIP calls from soft-phones running on Windows, Mac and Linux desktops and from many Symbian or Windows Mobile based cell-phones.

One of ZRTP's design goals is to provide end-to-end call encryption and to ensure that no



intermediate device is able to monitor or intercept the key exchange.

To assist in reaching this goal, ZRTP generates a Short Authentication String (SAS) which is normally displayed to each caller. Callers may verbally compare the SAS to provide confirmation that that the key exchange has completed successfully without interference from a MitM and that the call is fully protected.

To aid this comparison, the SAS is normally displayed as a pair of easily pronounceable and distinctive words, for example *prowler concurrent*.

In some circumstances there may not be a human caller at each end of the ZRTP protected call. As an example the call may be routed via a gateway or a PBX to a phone that is not capable of handling encrypted media or of displaying the SAS. In these cases, the ZRTP key exchange takes place between the phone and the gateway or PBX.

The gateway device will not normally have a human user on hand to read the SAS. To handle these cases ZRTP provides some additional features that enable a ZRTP capable phone to enrol with a trusted device such as a gateway. This enrolment process establishes some additional shared secrets between the device and the phone. These additional secrets together with the protocol design ensure that once the enrolment procedure is correctly completed, any future attempts at a MitM attack during key exchange are immediately detected.

The UM Labs SIP Security controller provides a gateway implementation of ZRTP and supports device enrolment as defined in the protocol definition. With this implementation, the UM Labs SIP Security Controller enables ZRTP capable phones to make encrypted calls via the SIP Security controller to any commercial PBX. At the time of writing, no commercial PBXs have direct support for ZRTP and only a minority of systems support any other media encryption protocols.

## 5.1. ZRTP Deployment

The UM Labs SIP Security controller is normally deployed a network perimeter protecting the PBX (Figure 4).

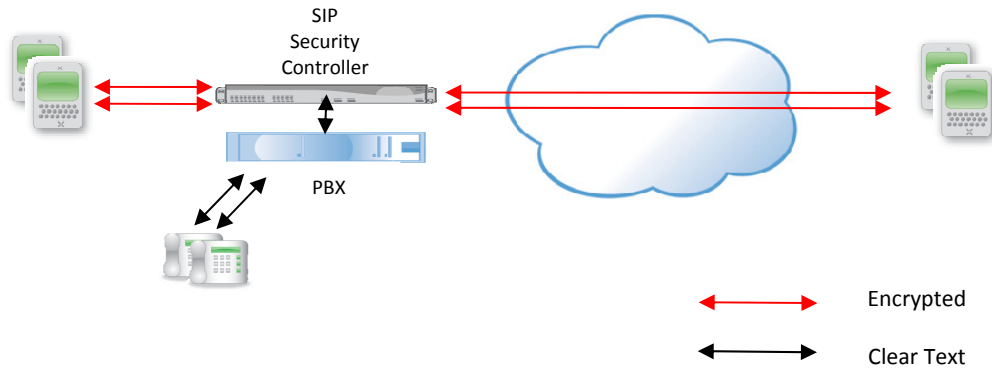


Figure 4 ZRTP Deployment

This deployment means that encrypted calls may be made from any local or remote ZRTP capable phone. The SIP Security Controller will decrypt all calls forwarding them over a trusted network link where they may be routed to their destination. Calls routed to other local or remote phones capable of supporting encryption will be re-encrypted by the SIP Security Controller. Calls routed to local phone without cryptography support will remain in clear-text. This approach means that service can be extended to a wide range of devices and clear-text call legs may be limited to trusted networks.

In the special case where two ZRTP capable phones participate in a call, each phone will negotiate a separate ZRTP session with the Security Controller.

## 5.2. ZRTP Enrolment

As the secure ZRTP key exchange operates between the phone and the security controller which means that for most calls there is no opportunity to manually compare the SAS with another human user, it is strongly recommended that all devices enrol the security controller prior to deployment. This enrolment process will establish the additional secrets needed to ensure that all subsequent calls are protected against MitM attacks.

The enrolment process is simple, the user just calls a pre-defined number. For additional validation the SAS displayed on the user's phone may be manually checked with the SIP Security Controller's system administrator. The SAS is displayed to the administrator on the Security Controller's GUI (Figure 5).

Enrolled Users



URI	Date Enrolled	SAS	Is Active	Verified By	
602@voipcode.co.uk	20 Dec 2008	prowler concurrent		admin	Delete
603@voipcode.co.uk	21 Dec 2008			admin	Delete

Figure 5 ZRTP Enrolled Users

The SIP Security Controller will process enrolment calls when those calls arrive on a previously defined network interface. If most ZRTP users will be using soft-phones running on laptops or network connected PDAs then it is recommended that dedicated enrolment network is set up. Devices can be connected to that network and enrolled as they are issued to users. Limiting enrolment to a single network guarantees physical proximity of the devices during enrolment so that the SAS displayed by the device and by the SIP Security Controller may easily be checked.

The same approach may be used for registering mobile phones if those phones are able to establish a WiFi connection to the enrolment network, otherwise the enrolment interface should be configured so that enrolment calls may be made from a remote network.

In all cases, an enrolment URI must be defined. The URI should be handled by a trusted local PBX and can either direct the caller to a pre-recorded message or could ring a phone that can be answered by the SIP Security Controller administrator.

Assuming that the SAS displayed on the callers phones matches the SAS displayed on the SIP Security Controller GUI, then the SIP Security Controller administrator must mark the SAS as verified by clicking on the verify button displayed adjacent to the enrolled user. The phone use must also mark the SAS as verified. The mechanism for doing this will depend in the phone. If Zfone is in use the *Register with this PBX* option from the Edit menu should be checked while the enrolment call is still active.

## 6. Installing the RC-2100

Installation and initial configuration of the RC-2100 is completed in 3 easy steps:

- Unpack the RC-2100 and connect it to the network
- Establish a Web connection to the RC-2100 using a default IP address
- Login and complete the basic configuration

### 6.1. Unpack and Connect to the Network

The RC-2100 is equipped with 3 10/100 Mbit/sec Ethernet port, a power connector and a serial console port. The network ports and named eth0, eth1 and eth2 and correspond to the connections shown in Figure 6.

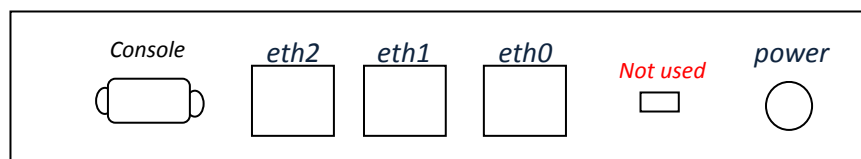


Figure 6 RC-2100 Back Panel Connections

For the initial configuration, connect the system to an Ethernet network port using *eth0*, the connector closest to the power connector. Connect the supplied power supply to the system which will start to boot. The green LEDs on each Ethernet port will light up as will a green LED on the front of the system. The complete boot process takes approximately 60 seconds.

On first boot, port eth0 is pre-configured with a fixed IP address 192.168.1.1, netmask 255.255.255.255. To continue with the configuration, manually configure a workstation to have a different address on the same IP subnet (for example 192.168.1.2, netmask 255.255.255.0) and connect that workstation to the same Ethernet network as the RC-2100. You may find it convenient to use an Ethernet cross-over cable to establish this connection. The use of a cross over rather than connecting to a hub may be necessary if your network happens to use 192.168.1.0 as its local network number.

Alternatively you may change this default address to one that corresponds to you local network. This can be done via the console menu. Connection to the RC-2100 console menu requires a serial cable (not supplied) and a suitable terminal emulator. See section 7 for details.

### 6.2. Establish a web connection to the RC-2100

Using your preferred browser on the workstation configured and connected in the previous section, establish a connection to:

<https://192.168.1.1/>

or to the address assigned to eth0 via the console menu. Note that for security reasons, you must establish an HTTPS (encrypted) connection. To protect the confidentiality of your password, plain text connections are not allowed. HTTPS connections are controlled by a *server*

*certificate*. The browser will compare the certificate presented by the server with the URI used to make the connection and will issue a warning if the identity in the certificate does not match the URI. As all RC-2100s ship with a standard certificate, your browser will issue a warning. The format depends on the browser used. This warning can be avoided in the future by generating and/or installing a new self-signed or CA signed certificate. This process is discussed in section 11 of this manual.

If you wish to check the validity of the certificate presented by the RC-2100, the standard certificate shipped with all new systems is as follows:

<b>Issued To:</b>	default.um-labs.com
<b>Organisation:</b>	UM Labs Ltd
<b>Serial Number:</b>	A0:4E:AD:2B:DB:8B:AB:6E
<b>Issued By:</b>	default.um-labs.com
<b>Issued On:</b>	Apr 27 06:39:22 2008 GMT
<b>Expires On:</b>	May 17 06:39:22 2010 GMT
<b>MD5 Fingerprint:</b>	64:42:73:BD:6E:08:C6:18:B9:1B:60:66:FA:58:BD:B7

### 6.3. First Login

Once you have accepted the certificate presented by the RC-2100's web server, you will be presented with a login screen similar to that shown in Figure 7. Login as *admin* using the default password. The login credentials needed for this initial login are:

<b>User name:</b>	admin
<b>Password:</b>	password

Note that both username and password are case sensitive.

Once you have logged in you will be asked to read and accept the standard license agreement and to change your password. Chose a strong password but take care not to forget the password as there is no mechanism to recover a lost password.

## RC-2100 SIP Security Controller

The text of the license agreement may be read at:

[http://www.um-labs.com/license\\_agreements.html](http://www.um-labs.com/license_agreements.html)



The image shows a login prompt for the RC-2100 SIP Security Controller. The header features the UM Labs Ltd logo on the left with the website sip.voipcode.co.uk below it. To the right, the text reads 'RC-2100 SIP Security Controller for Trunks and Remote Connections'. The main area contains a 'login:' label followed by a text input field, a 'password:' label followed by a text input field, and a 'Login' button below them. At the bottom, there is a copyright notice: 'Copyright © 2008 UM Labs Ltd'.

**Figure 7 RC-2100 Login Prompt**

At this point you are ready to begin the basic configuration (see section 9 of this manual).

## 7. RC-2100 Console Interface

The RC-2100 SIP Security Controller offers a console menu that provides a number of low level system configuration functions. These functions include:

- Viewing the currently configured IP addresses
- Changing the IP address of interface eth0
- Changing the system's default IP gateway
- Emergency reset functions
- Rebooting the system

### 7.1. Connecting to the console

The RC-2100 provides a DB9 serial port for console connections (see Figure 6). The console connection requires a null modem serial cable (DB9 to DB9 or DB9 to DB25). This cable is *not* supplied with the system.

To use the console interface, connect one end of a suitable cable to the RC-2100 console port and the other end to the serial port of a system running a terminal emulator capable of using the system's serial port, for example Windows HyperTerminal. Configure the terminal emulator as follows:

Speed:           38400 baud  
Parity:           None  
Stop bits:        1

Start the terminal emulator and hit enter once or twice to activate the console menu.

### 7.2. Console Menu Functions

The console menu offers a series of numbered options. To select one of the displayed options, enter the option number when prompted (see Figure 8).

```
-----  
|                               UM Labs RC-2100 Console                               |  
|  
|      1) Show Interface IP addresses      |  
|      2) Change Interface eth0 IP address |  
|      3) Emergency Reset functions       |  
|      4) Reboot the system               |  
|      5) Exit                             |  
|  
|      Option:                             |  
|  
-----
```

Figure 8 RC-2100 Console

### 7.2.1. Show Interface IP Addresses

This option displays the currently configured IP address and subnet mask of each active network interface.

### 7.2.2. Change Interface eth0 IP Address

This option changes the IP address of the eth0 network interface. This enables the factory default address of 192.168.1.1 to be changed to an address that matches the range used on your local network, simplifying the task of connecting to the Web GUI. Note that as the console interface does not allow changes to the default IP gateway, both the RC-2100 and the system running the web browser must be connected to the same IP subnet.

IP address changes will take effect at the next system reboot.

### 7.2.3. Emergency Reset Functions

These functions are provided to recover a system when access to the Web Interface is no longer available because of previous configuration errors.

1. Reset Admin GUI Password. This option re-sets the password for the *admin* login to its default value (see section 6.3). This option takes effect immediately.
2. Reset to Factory Defaults. This option resets the system to the factory default configuration by deleting the existing configuration. **This option should be used with caution as deleting the configuration is not reversible.** The change will take effect on the next system reboot. Note that if the IP address of eth0 was previously changed using the console menu, then that change will be retained.

### 7.2.4. Reboot the System

Selecting this option triggers an immediate system reboot.

## 8. Configuration Management

In common with the other SIP Security Products from UM Labs, the RC-2100 provides sophisticated Configuration Management. This means that a system can store multiple configurations any one of which may be activated. This feature makes it easy to experiment with new configurations and to roll-back to a known working configuration if things go wrong.

The RC-2100's configuration management is based on three simple principles:

1. The system runs using an active configuration. This configuration is locked and cannot be directly changed.
2. Any configuration item on any of the web GUI pages can be changed; these changes are "remembered" by the configuration management system and held in a temporary area. These changes do not affect the system's operation.
3. When you have finished making changes you have the option of discarding all changes or saving the changes as a new named configuration.

The configuration management page (see Figure 9) lists the currently active configurations and shows which configuration is active.

	Description	Date Created	Active
<input type="checkbox"/>	Default Configuration	16 Dec 2008, 17:40	
<input checked="" type="checkbox"/>	UM Labs Active Config	16 Dec 2008, 17:43	<input checked="" type="checkbox"/>

Figure 9 Configuration Management

The majority of the Web GUI pages provide two sets of buttons that provide an interface to configuration management. Figure 10, which shows the static routes page, illustrates these buttons.

**New Route**

**Destination:**

**Network Mask:**

**Gateway:**

**Description:**

---

**Configuration Management**

Figure 10 Configuration Control

The first set of buttons, apply and cancel, save or discard any changes made to the current page. These buttons are disabled until at least one change has been made to the current page. Clicking on Apply saves the changes made on the current page to the temporary area and allows further changes to be made on other pages. Clicking on Cancel discards all changes on the current page.

The second set of buttons applies to the complete configuration. These buttons remain inactive until changes have been applied to at least one individual page. The configuration management buttons provide a short cut to the configuration management page. Clicking on *Abandon Config* will discard all the changes held in the temporary area, while clicking on *Save Config* will navigate to the Configuration Management page where the pending changes can be viewed or saved as a new named configuration. Clicking on *See Changes* will display a summary of the differences between the active configuration and the current temporary configuration.

Some pages do not have the configuration management buttons. This is because the configuration items on these pages apply to the system as a whole and are not specific to individual configurations. These pages are Encryption Management (section 11), License Management (section 14) and Software Updates (section 15).

Figure 11 shows the dialog displayed when a new configuration is saved. Enter a short descriptive comment in the Description box and click on save. The configuration will then be displayed with other saved configurations.

The RC-2100 imposes a limit of five saved configurations, including the active configuration. Once the limit has been reached, older unwanted configurations must be deleted before any new configurations can be saved. Note that in some cases configurations may be dated 1<sup>st</sup> January 2000. This is because those configurations were saved before the system's configuration had been completed and NTP servers were defined. NTP servers are essential to ensure that the system clock is set accurately. Configuring NTP servers is discussed in section 9.1. These older configurations, including the system's default configuration may be deleted once an operational configuration has been saved and set active.

To activate a saved configuration, click on the *Set Active* button next to the required configuration. Note that in software version V1.0 you must then reboot the system to ensure that all system components are re-started with the new configuration. The system is rebooted from the System Status page (section 16.3).

	Description	Date Created	Active
<input type="checkbox"/>	Default Configuration	16 Dec 2008, 17:40	
<input checked="" type="checkbox"/>	UM Labs Active Config	16 Dec 2008, 17:43	<input checked="" type="checkbox"/>

**New Configuration**

Date: 24 Dec 2008, 18:26

Description:

Figure 11 Saving a new Configuration

Prior to saving a new configuration, it is often useful to view a summary of the changes made. Clicking on the *Changes* button will display a summary of the changes made. An example is

shown in Figure 12. In this case an additional network interface (eth1) has been activated and a new SIP route has been added.

Network Interfaces			
Object	Property	Original	New
eth2	Enabled	✗	✓
	IP Address		172.1.2.3
	Network Mask		255.255.0.0

SIP Routes			
Object	Property	Original	New
um-labs.com	Destination		securepbx.um-labs.com
	Port		5061
	Transport type		TLS
	Local Domain		✓

Figure 12 Configuration Change Summary

## 9. Basic Configuration

This section describes how to complete the basic configuration of the RC-2100. There are two main stages; to configure the IP Network settings for your system and to configure the SIP routing rules.

IP Network settings are split over 3 pages. The first page defines the system wide settings, host name, domain, Domain Name Server and other settings. The second page configures each of the network interfaces that will be used on your system. The third page allows the definition of static IP routes. Network system settings and Network Interfaces are mandatory, at least one network interface must be defined. Static IP routes are optional and are normally required only if your internal network has included a number of routed sub-networks.

### 9.1. Network System Settings

The GUI page for network system settings is shown in Figure 13. The first part of the screen is used to define key system-wide settings. Many of the input fields are required. Positioning your cursor over the ? symbol next to each input field will display some help text describing that field.

Host Name:	<input type="text" value="sip"/>	?
Domain Name:	<input type="text" value="voipcode.co.uk"/>	?
Default Gateway:	<input type="text" value="192.168.19.1"/>	?
Web Proxy:	<input type="text"/>	?
Primary DNS:	<input type="text" value="192.168.19.1"/>	?
Secondary DNS:	<input type="text"/>	?
Tertiary DNS:	<input type="text"/>	?
Primary NTP:	<input type="text" value="192.168.19.1"/>	?
Secondary NTP:	<input type="text"/>	?
Time Zone:	<input type="text" value="London"/> ▼	?
SysLog Server:	<input type="text"/>	?
SNMP Community String:	<input type="text" value="public"/>	?
RTP Port Range:	<input type="text" value="16000"/> - <input type="text" value="16200"/>	?

**Network Interfaces**

Name	IP	Mask	UDP	TCP	TLS	Link Status	Status
eth0	192.168.19.30	255.255.255.0	✓	✓	✓	✓	✓
eth1	192.168.190.30	255.255.255.0	✓	✓	✓	✓	✓
eth2			✓	✓	✓	✗	✗

**Static Routes**

Destination	Network Mask	Gateway	Description
192.168.251.0	255.255.255.0	192.168.19.5	Test Route

Figure 13 Network System Settings

The lower part of the screen summarises the configured network interfaces on the system and any configured static routes. If this is your first login only one interface with the default IP address of 192.168.1.1 or an alternative value set via the console interface will be displayed. (Figure 13 is taken from a system that has been partly configured, so an additional network interface is shown).

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

Value	Meaning	Status
<b>Host name</b>	This is the name of the system. The hostname must be unique within your IP domain. It should be assigned by your local network administrator.	Mandatory
<b>Domain Name</b>	This is your local IP domain name which is usually based on your organisation's domain name. The IP domain is usually the same as the domain name used by your SIP applications, although it does not have to be.	Mandatory
<b>Default Gateway</b>	This is the IP address of the default gateway for your network. If the RC-2100 is connected between your private network and the Internet this is the IP address of your Internet router or DSL gateway. This address must be on the same IP sub-net as one the RC-2100's local network interfaces.	Mandatory, must be an IP address
<b>Web Proxy</b>	The name or IP address of web proxy that the RC-2100 must use to connect to the UM Labs update server.	Optional (not used in V1.0)
<b>Primary DNS</b>	The IP address of the system's primary name server. The name server may be reachable via any of the RC-2100's active network interfaces. You can use either a name server on your own network or an ISP's Name Server.	Mandatory, must be an IP address
<b>Secondary DNS</b>	A backup name server	Recommended, must be an IP address
<b>Tertiary DNS</b>	A second backup name server	Optional, must be an IP address
<b>Primary NTP</b>	A domain name or IP address of a reliable time source. A reliable time source is necessary to enable the RC-2100 to accurately log and time calls. Most ISPs provide an NTP server.	Mandatory, may be an IP address or a hostname
<b>Secondary NTP</b>	A backup NTP server	Optional
<b>Time Zone</b>	Select the appropriate time zone for your location. Time zones are ordered by geographic region and by capital city within regions	Mandatory

Value	Meaning	Status
<b>Syslog Server</b>	The name or IP address of an external syslog server. If defined, a copy of all log records will be sent to this server. As this may generate a lot of traffic the server should be on a local network.	Optional, may be an IP address or a hostname
<b>SNMP Community String</b>	Define a value for an SNMP community string to be used if SNNP is enabled. SNMP is enabled on the network interfaces page.	Optional
<b>RTP Port Range</b>	Define the local ports that the RC-2100 will use as RTP source ports for outbound media streams and destination ports for inbound media streams. The range should be large enough to handle the expected number of simultaneous calls. Each call needs 4 consecutive ports. Avoid making the range too large as this will consume memory and reduce system performance. A good guide line to allocate sufficient ports to handle twice the expected maximum number of simultaneous calls.	Mandatory

Table 1 Network System Settings

## 9.2. Network Interfaces

The Network Interfaces page defines which of the available network interface are active and sets the IP address and other parameters for that interface. When first displayed, the page lists the available interfaces on the system showing the interface’s MAC address, its current IP address is set and a check box that enables or disables this interface.

**eth0**

IP Address: 192.168.19.30  
 MAC Address: 00:0D:B9:14:73:C0  
 Interface Type: Physical Network Interface

Enabled:

MTU:  ?

Media:  ?

IP Address:  ?

Network Mask:  ?

SIP UDP Port:   ?

SIP TCP Port:   ?

SIP TLS Port:   ?

Transparent Proxy:  ?

External Firewall IP:  ?

Web GUI Enabled:   ?

ICMP echo:  ?

SNMP:  ?

[SNMP Client List](#)

Figure 14 Network Interface Configuration

By clicking in on the triangular arrow next to the interface name, the display can be expanded which allows additional parameters to be viewed and set. Figure 14 shows an example network interfaces page with the display for eth0 expanded.

To enable a new interface check the enabled box, expand the display for that interface and provide the details needed to configure that interface. To modify an existing interface, simply update the configuration details. The values that should be entered in each of the fields on this page are summarised in Table 2.

Value	Meaning	Status
<b>MTU</b>	MTU stands for <i>Maximum Transmission Unit</i> and represents the largest packet that may be transmitted over that interface. In almost all cases this should be left as the default value for an Ethernet network, 1,500 bytes. Lower values may be needed if routers between the RC-2100 and any destination are incorrectly configured and do not provide the appropriate feedback if the default value is too high.	Optional
<b>Media</b>	This value sets the media type used by the network interface. In almost all cases this should be left as the default value of <i>auto-sense</i> which instructs the network interfaces to detect the media type provided by the hub or switch to which it is connected and automatically adopt the appropriate configuration. This value should be changed only if a problem with the hub or switch causes the auto-sense setting to fail	Optional
<b>IP Address</b>	Set or change the IP address for this interface. The IP address will be allocated by your network administrator.	Mandatory
<b>Network Mask</b>	Set or change the subnet mask for this interface. The network mask will be allocated by your network administrator.	Mandatory
<b>SIP UDP Port</b>	Check the checkbox if the SIP proxy should accept SIP messages over a UDP transport on this interface. The SIP proxy can be forced to use a different port than the default for this transport (5060) by changing the port setting.	Mandatory if SIP over UDP is required on this interface
<b>SIP TCP Port</b>	Check the checkbox if the SIP proxy should accept SIP messages over a TCP transport on this interface. The SIP proxy can be forced to use a different port than the default for this transport (5060) by changing the port setting.	Mandatory if SIP over TCP is required on this interface

Value	Meaning	Status
<b>SIP TLS Port</b>	Check the checkbox if the SIP proxy should accept SIP messages over a TLS encrypted transport on this interface. The SIP proxy can be forced to use a different port than the default for this transport (5061) by changing the port setting.	Mandatory if SIP over TLS is required on this interface
<b>Transparent Proxy</b>	Check this box if the RC-2100 should operate as a transparent proxy on this interface. Transparent proxy operation means that the RC-2100 will accept and process SIP messages even if the IP destination of those messages is for some other system. The most common use of this setting is to ensure that the RC-2100 processes SIP messages sent by a PBX to an external service such as a SIP trunk. If the PBX is configured so that its default IP gateway is the RC-2100 then messages sent directly to the SIP trunk's IP address will be processed by the RC-2100. If you are in doubt, enable this feature	Optional but recommended
<b>External Firewall IP</b>	If SIP messages sent via this interface reach their destination via a Firewall or other gateway that provides Network Address Translation (NAT), enter the external IP address of that Firewall here. This enables the RC-2100 to apply the necessary address mappings that are needed to enable SIP messages to traverse the Firewall. Refer to sections 4 and 17.2 for more information on this topic.	Optional
<b>Web GUI Port</b>	Check this box if you wish to allow connections to the RC-2100 Web Management interface on this network interface. Web management connection use encrypted connections (HTTPS), the default port for this service is 443. The port can be changed from the default by changing the port setting.	At least one network interface must have Web GUI connections enabled
<b>ICMP Echo</b>	Check this box if the RC-2100 should respond to ICMP echo requests (ping) on this interface. If the check box is clear, then the RC-2100 will silently ignore any ICMP echo requests received.	Optional

Value	Meaning	Status
<b>SNMP</b>	Check this box if the RC-2100 should respond to SNMP queries on this interface. Note that the RC-2100 allows only monitoring via SNMP (SNMP get). For security reasons, using SNMP to change the RC-2100's configuration is not permitted. If SNMP is enabled, SNMP queries are permitted only from clients whose IP addresses are explicitly listed in the SNMP client list for this interface. To view and manage this list, click on the triangular arrow next to <i>SNMP Client List</i> . New clients may be added as a <i>FQDN</i> , or an IP address. IP addresses can be entered as host IP addresses or subnets in CIDR format (for example 192.168.1.0/24).	Optional

Table 2 Network Interface Settings

### 9.3. VLANs

The VLANs page enables one or more VLAN network interfaces to be configured for any of the system's physical network interfaces. VLANs may be configured only for inactive physical interfaces, it is not possible to configure a VLAN on an active interface with an assigned IP address. Each physical interface may host multiple VLAN interfaces.

VLAN interfaces are created by selecting a host interface and entering a VLAN tag, see Figure 15). Note that the choice of host interfaces will be limited to currently inactive physical interfaces. Once created, the VLAN interface will be named *hostif.tag*, for example a VLAN interface with a tag value of 40 created on eth2 will be named eth2.40. This new interface will be displayed on the Network Interfaces page (see section 9.2) where it may be configured in the normal way.

Once a VLAN has been created on a host interface that host interface will no longer be available for normal (non VLAN) use. If you wish to assign an IP address to the host interface and use it as a non VLAN interface you will first need to delete all defined VLANs from that interface.

Interface Name	Host Interface	VLAN Tag	
eth2.20	eth2	20	<input type="button" value="delete"/>

**New VLAN**

Host Interface:

VLAN Tag:

Figure 15 Defining a VLAN interface

### 9.4. Static Routes

The static routes page displays any existing static IP routes, allows any displayed route to be deleted and allows the addition of new static routes, see Figure 16.

To add a new static route enter the destination IP address, which may be a host or network, the next hop gateway and a short description of this route.

Destination	Network Mask	Gateway	Description	
192.168.251.0	255.255.255.0	192.168.19.5	Test Route	Delete

**New Route**

Destination:  ?

Network Mask:  ?

Gateway:  ?

Description:  ?

Figure 16 Static IP Routes

The destination and network mask must be entered separately (CIDR notation is not allowed). If the destination is a host then the mask should be 255.255.255.255, if the destination is an IP subnet then the mask should be appropriate to define that subnet. The next hop gateway must be an IP address on the same IP subnet as one of the RC-2100's configured and active network interfaces. The description is purely to remind the system administrator of the purpose of this route, it plays no part in setting the route up.

### 9.5. SIP Routing

The SIP routing table is the main control point for determining how the RC-2100 processes SIP messages. The RC-2100 examines the *Request URI* and if necessary, the *To URI* of each message that marks a new *SIP Transaction*. The RC-2100 first checks the full request URI and then the domain component of the Request URI. If a matching entry is found in the SIP routing table, then the message and all subsequent inbound messages for the same SIP transaction are routed to the defined destination.

SIP routes are most commonly used to direct incoming traffic for the local SIP domain to the PBX that handles calls for that domain. For example if the PBX handling calls for the domain *voipcode.org* is at 192.168.55.10, then the route shown in Figure 17 would direct all calls to that PBX.

There is no limit to the number of SIP domains that the RC-2100 can support and therefore no limit to the number of PBXs or other SIP destinations that can be supported. There are also no restrictions on the location of a SIP destination; destinations can be on a local subnet reached via any of the RC-2100s interface or at geographically remote locations reached via the RC-2100's default gateway or a static route. However, most locations will need only a single route, directing calls for the local SIP domain to the PBX that handles those calls.

URI	Destination	Trans	Local	Status	Auth
<input type="checkbox"/> voipcode.co.uk	sw19voip.voipcode.co.uk	UDP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Auth</a>
<input type="button" value="Delete"/>					

**New Route**

Target URI:  ?

Destination:  ?

Port:  ?

Transport type:  UDP  TCP  TLS ?

Local Domain:  ?

Destination Map:  ?

Figure 17 SIP Routing Table

New SIP routes are added by providing the appropriate values on the *New Route* form. The values that should be entered in each of the fields on this form are summarised in Table 3.

Value	Meaning	Status
<b>Target URI</b>	The Target URI is a SIP URI (without the SIP or SIPS prefix) or a SIP domain name that defines the target for this route. The domain name or domain part of a SIP URI can be a name or an IP address. Examples of valid targets include: <ul style="list-style-type: none"> <li>• um-labs.com</li> <li>• info@um-labs.com</li> <li>• 82.3.4.5</li> <li>• +442030213200@um-labs.com</li> <li>• <a href="#">+442030213200@82.3.4.5</a></li> </ul>	Mandatory
<b>Destination</b>	The destination for SIP messages received for the target. The destination can be expressed as full qualified domain name or an IP address	Mandatory
<b>Port</b>	The port that the RC-2100 should use to establish a transport link to the destination.	Mandatory
<b>Transport Type</b>	Chose the transport type that the RC-2100 should use to send SIP messages to the destination. If the destination is a another UM Labs SIP Security controller or other device that supports Signalling encryption then TLS is the best option. If in doubt then UDP is supported by virtually all SIP systems.  If TLS transport is selected, then the RC-2100 will also offer SRTP media encryption to that destination.	Mandatory
<b>Local Domain</b>	Check this box is the target domain (or URI) is local. A local domain has special privileges. Only calls originating from local domains may be routed to non-local domains (this prevents unauthorised call relay and toll fraud) and SIP requests from local domains may be subjected to additional authentication checks. SIP authentication is discussed in section 10.	Optional

Value	Meaning	Status
<b>Destination Map</b>	The destination map defines an optional URI (name or IP address) that is used to map SIP request URIs routed by this routing table. Destination mapping is normally needed only for handling incoming requests from some SIP trunk services. The use of destination maps is discussed in section 17.1.1.	Optional

Table 3 SIP Routing

The displayed list of SIP routes includes an *Auth* link. Clicking on this link allows authentication services to be configured for local domains. SIP Authentication is an advanced topic which is discussed in section 10.

## 9.6. Advanced Firewall Control

The RC-2100 includes an IP Firewall module that is designed to protect the device itself and other components of the VoIP network from IP level attacks. The firewall is preconfigured to allow only authorised SIP message streams (configured on the network interfaces page, section 9.2) and RTP media streams permitted by the SIP signalling. The Firewall module is also responsible for preventing flooding attacks and for logging any unauthorised connection attempts.

**Warning:** the settings on this page control the operation of the Firewall rules which provide IP Level security. Changing the default values may lead to service disruption. Refer to the manual before proceeding.














TCP Probe Log Limit (per minute):	<input type="text" value="5"/>	
UDP Probe Log Limit (per minute):	<input type="text" value="5"/>	
Ignored Ports (UDP):	<input type="text" value="67,68,137,138,139"/>	
Ignored Ports (TCP):	<input type="text"/>	
TCP Spoof Log Limit (per minute):	<input type="text" value="5"/>	
UDP Spoof Log Limit (per minute):	<input type="text" value="5"/>	
Max Web Admin Logins:	<input type="text" value="3"/>	
UA SIP/TLS Connection Limit:	<input type="text" value="3"/>	
UA SIP/TCP Connection Limit:	<input type="text" value="3"/>	
UA SIP/UDP Rate Limit (per minute):	<input type="text" value="1500"/>	
Interface SIP/TLS Connection Limit:	<input type="text" value="50"/>	
Interface SIP/TCP Connection Limit:	<input type="text" value="50"/>	
Interface SIP/UDP Rate Limit (per minute):	<input type="text" value="3000"/>	

Figure 18 Advanced Firewall Control

The advanced firewall control page (Figure 18) allows changes to be made to the some of the IP firewall module's operational parameters. The parameters are pre-set to the optimal values for

most installations. Review the following discussion carefully before making any changes as inappropriate changes can lead to operational failures.

Parameter	Purpose	Notes
<b>TCP Probe Log Limit</b>	Limits the rate at which unauthorised TCP connection attempts are logged. Limit applies to each unique source IP and port combination.	If the system is subjected to a flood attack, logging every single connection request will quickly fill the logs and slow the system down. This parameter limits the number of log entries created without losing important information.
<b>UDP Probe Log Limit</b>	Limits the rate at which unauthorised UDP datagrams are logged. Limit applies to each unique source IP and port combination.	If the system is subjected to a flood attack, logging every single connection request will quickly fill the logs and slow the system down. This parameter limits the number of log entries created without losing important information.
<b>Ignored UDP Ports</b>	Lists the destination UDP ports that are excluded from logging.	Most networks carry traffic on a number of UDP ports that if logged will simply fill the logs with unnecessary information. Examples include ports used by Microsoft (137 to 139) and DHCP ports (67, 68). The ignore list is specified as a comma separated list of ports.
<b>Ignored TCP ports</b>	Lists the destination UDP ports that are excluded from logging	In most cases all unauthorised TCP connection requests should be logged so this list is empty.
<b>TCP Spoof Log Limit</b>	Limits the rate at which TCP connection requests with spoofed source IP addresses are logged. Limit applies to each unique source IP and port combination.	A spoofed request is defined as one where the request arrives on one network interface, but the source of the request is a network connected to another interface.
<b>UDP Spoof Log Limit</b>	Limits the rate at which UDP datagrams with spoofed source IP addresses are logged. Limit applies to each unique source IP and port combination.	A spoofed request is defined as one where the request arrives on one network interface, but the source of the request is a network connected to another interface.

Parameter	Purpose	Notes
<b>Max Web Admin Logins</b>	Limits the number of concurrent web admin logins.	This limit applies at the TCP level, if the login limit is reached all further attempts to connect to the web admin GUI will be blocked. This limits the impact of TCP connection floods.
<b>UA SIP/TLS Connection Limit</b>	This limits the number of SIP/TLS connections permitted from a single User Agent.	A UA is identified by its source IP address. A source IP address may represent a NAT gateway. This gateway may be used by a number of different SIP phones, so this parameter should be set high enough to allow all such phones to connect.
<b>UA SIP/TCP Connection Limit</b>	This limits the number of simultaneous SIP/TCP connections permitted from a single User Agent.	A UA is identified by its source IP address. A source IP address may represent a NAT gateway. This gateway may be used by a number of different SIP phones, so this parameter should be set high enough to allow all such phones to connect.
<b>UA SIP/UDP Rate Limit</b>	This limits the rate at which SIP/UDP datagrams will be accepted from a single UA. A SIP registration may take 3 or 4 datagrams and an INVITE about the same number.	A UA is identified by its source IP address. A source IP address may represent a NAT gateway. This gateway may be used by a number of different SIP phones, so this parameter should be set high enough to allow all such phones to send regular REGISTER, INVITE and other requests
<b>Interface SIP/TLS Connection Limit</b>	This limits the number of simultaneous SIP/TLS connections permitted via any one of the the RC-2100's network interface (from any source).	This parameter is designed to limit the impact of connection flooding, but should be set high enough to allow all legitimate traffic.
<b>Interface SIP/TCP Connection Limit</b>	This limits the number of simultaneous SIP/TCP connections permitted via any one of the the RC-2100's network interface (from any source).	This parameter is designed to limit the impact of connection flooding, but should be set high enough to allow all legitimate traffic.

Parameter	Purpose	Notes
<b>Interface SIP/UDP Rate Limit</b>	This limits the rate at which SIP/UDP datagrams will be accepted on any one of the RC-2100's network interface (from any source).	This parameter is designed to limit the impact of connection flooding, but should be set high enough to allow all legitimate traffic.

**Table 4 Advanced Firewall Controls**

## 10. SIP Authentication

The SIP standard defines a number of different *SIP Methods*. The standard also states that each of these methods (with the exception of ACK and CANCEL) may be authenticated. The SIP standard defines the use of Digest Authentication to provide this authentication service. Digest Authentication (defined in RFC 2617) is a challenge-response authentication mechanism. If a request submitted by a *UAC* is to be authenticated, the receiving *UAS* will reject that request with a response that indicates that authentication is required. That response will include an authentication challenge. The *UAC* must then re-submit the request with the correct response.

SIP Authentication is an important component of a well designed set of security controls. By requesting authentication for SIP methods that establish new calls, terminate existing calls or transfer calls, many of the security threats that can disrupt both individual calls and complete VoIP systems can be addressed. Equally, the SIP methods that provide information about a system (for example OPTIONS, SUBSCRIBE and NOTIFY) divulge details that an attacker may find useful and so should be authenticated where possible and blocked when not possible.

Unfortunately many PBXs and other SIP applications cannot be configured to authenticate all SIP methods. While virtually all PBX systems will authenticate REGISTER requests and most will authenticate INVITE, fewer systems will authenticate BYE and other requests leaving the network open to a range of call disruption attacks.

The RC-2100 is designed to supplement or replace the authentication service offered by the PBX. The RC-2100 will authenticate those methods not authenticated by the PBX. For example if the PBX authenticates only REGISTER and INVITE then the RC-2100 could be configured to authenticate all other SIP methods (see Figure 19).

**IMPORTANT:** it is an error to configure the RC-2100 to authenticate methods that are authenticated by the PBX (or the destination for the SIP Routing Table entry). The authentication mechanism defined by the SIP standard does not allow for a single request to be authenticated twice.

The screenshot shows a configuration window for SIP Authentication Policy. It has the following fields and options:

- Domain:** voipcode.co.uk
- Authentication Source:** LOCAL
- Authentication Realm:** voipcode.co.uk
- Authentication Policy:**
  - INVITE
  - REGISTER
  - BYE
  - OPTIONS
  - INFO
  - REFER
  - NOTIFY
  - SUBSCRIBE
  - MESSAGE
  - PRACK
  - UPDATE
  - PUBLISH
- Buttons:** Apply, Cancel

Figure 19 SIP Authentication Policy

Figure 19 shows the information needed to configure the authentication service for a domain defined in the SIP routing table. The values that should be entered in each of the fields on this form are summarised in Table 5.

Value	Meaning	Status
<b>Authentication Source</b>	This defines source of authentication (usernames and passwords) that the RC-2100 will use to authenticate requests originating from the defined domain. V1.0 provides only local database. Usernames and passwords must be entered on the SIP users page (section 13.2). Selecting <i>NONE</i> disables all authentication for this domain.	Mandatory
<b>Authentication Realm</b>	The value for the realm string to be used in authentication challenges. This is normally set to the same value as the domain name.	Mandatory
<b>Registration Expiry</b>	Enter the default expiry value that the destination for this SIP route will assign to REGISTER requests. Most PBX will use 3600 seconds but the value may be shorter. This field is informational and is used by the RC-2100's registration caching (see section 10.1).	Optional
<b>Authentication Policy</b>	Check the checkboxes for each SIP method that the RC-2100 should authenticate. The RC-2100 will not attempt to authenticate any SIP methods whose check box is cleared.	Mandatory

Table 5 SIP Authentication

There are a number of restrictions to the use of SIP authentication.

1. As already mentioned, it is an error to attempt to authenticate any methods authenticated by the PBX (or other server at this domain's destination).
2. Authentication can be applied only to local domains. This is a reasonable restriction as no authentication credentials will be available for users in remote domains.
3. Authentication is based on the From URI. The From URI represents the originator of a request. This means that a request from a non-local domain to a local domain cannot be authenticated while a request from a local domain to a non-local domain may be authenticated. For this reason, the RC-2100 does not permit calls or other SIP requests from non-local domains to other non-local domains. Non-local domains may send requests only to local domains. The single exception to this policy is that devices defined as destinations in the SIP routing table may send requests to any domain, even if the from URI used in that request indicates that the request's origin is a non-local domain. This policy is necessary to ensure the correct operation of SIP trunks and is reasonable because the route destination of a local domain is by definition a trusted device.

### 10.1. Registration Caching

The RC-2100 provides a Registration Caching service. Registration caching is a process where the RC-2100 keeps a record of the state of any device registrations that pass through. The registration cache is part of the state information maintained by the RC-2100 (see section 3.2). Registration caching has two functions; it enables calls to be routed to remote users whose

phone is registered in a local domain and it reduces the number of registration requests that the PBX must process.

When a remote phone is located behind a firewall or other NAT gateway that phone must generate regular SIP traffic to maintain the address and port mappings on that firewall. If these mappings are not maintained, then the remote phone will be unable to receive inbound calls. Many phones have a SIP keep-alive option which sends regular short messages designed to maintain their local firewall's address and port mapping. Phones that lack this facility are often configured to re-register at regular intervals (30 or 60 seconds), these registration requests have the same effect as the SIP keep-alives. Unfortunately, this places an additional load on the PBX and may become a problem if there a large number of remote phones. As an example the Asterisk PBX has a built-in limit for processing registrations; if remote devices register every 60 seconds then Asterisk can support only 360 remote devices.

The RC-2100 addresses this problem by recording the registration expiry granted by the PBX. Additional registration requests received within that expiry time are answered by the RC-2100 and are not forwarded to the PBX.

Registration caching requires no specific configuration.

## 11. Encryption Management

The RC-2100 uses encryption for 3 different purposes.

1. To provide HTTPS (TLS) encrypted connections to the Web GUI
2. To provide TLS encryption for SIP signalling
3. To provide SRTP media encryption.

The set of encryption management pages control all aspects of encryption.

### 11.1. Certificate Management

The TLS modules used for Web GUI connections and for SIP signalling share the same public/private keys and certificates. The Encryption Management page controls the generation of public/private key pairs and the creation of self-signed certificates or certificates signed by an external trusted Certificate Authority (CA).

All newly installed RC-2100s use a single common certificate. This certificate will generate web browser warnings as the certificate will not match the name or address that the browser uses to connect to the RC-2100 (see section 6.2). This same certificate will by default be used to control SIP connections over TLS. The results will depend on the device making or accepting the connections. Some phones, for example the hardware phones manufactured by *snom AG* (<https://www.snom.com>) will happily accept any certificate, while others, for example the CounterPath eyebeam software phone will check the certificate and reject the connection if the details in the certificate do not match name or IP address used to establish the connection.

Even if you do not plan to use SIP over TLS or those SIP devices that use TLS do not enforce certificate checks, it is good practice to always generate a self-signed or better still a CA signed certificate that includes both your organisation name and your RC-2100's official host name. The Encryption Management page offers both of these options.

The Encryption Management page is split into two regions. The top region displays the currently installed certificate. The important fields in this display are the Subject, the Not After field and the certificate fingerprint. The Subject field includes a Common Name (CN) parameter which must match the IP domain name of your RC-2100. This domain name should be used by TLS capable SIP devices and web browsers to connect to the RC-2100. The Not After field shows the expiry date of the current certificate. The Fingerprint is used by browsers to provide a manual method for checking the authenticity of the presented certificate. See Figure 20 for an example.

**Certificate Management**

```

Version: 3 (0x2)
Signature Algorithm: sha1WithRSAEncryption
Validity
Not Before: Dec 20 17:31:54 2008 GMT
Not After : Dec 20 17:31:54 2010 GMT
Subject: C=UK, L=London, O=UM Labs Ltd, CN=sip.voipcode.co.uk
X509v3 extensions:
X509v3 Subject Key Identifier:
2F:71:9A:3F:4D:15:FF:DB:52:E5:23:91:90:CB:19:FD:28:95:56:98
X509v3 Authority Key Identifier:

```

**New Certificate Details**

Country:  (\*) ?

State/Province:  ?

City:  (\*) ?

Organisation Name:  (\*) ?

Organisational Unit:  ?

Host name:  (\*) ?

Email Address:  (\*) ?

Lifetime (years):  ?

**Generate Certificate**

?
  ?
  ?

Figure 20 Certificate Management

The lower region of the page presents a form that collects the information needed to generate a new self-signed certificate or a certificate request. The values that should be entered in each of the fields on this form are summarised in Table 6. Mandatory fields are marked with a (\*).

NOTE: correct certificate generation depends on the correct setting of the RC-2100's clock, for this reason it is strongly recommended that certificate generation is carried out after the basic network configuration has been complete and after at least one NTP server has been defined (see section 9.1).

Value	Meaning	Status
<b>Country</b>	Select your country from the drop-down list.	Mandatory
<b>State/Province</b>	Enter your state/province if appropriate.	Optional
<b>City</b>	Enter your town or city.	Mandatory
<b>Organisation Name</b>	Enter your company name.	Mandatory
<b>Organisational Unit</b>	Enter your department.	Optional

Value	Meaning	Status
<b>Host Name</b>	<p>Enter the fully qualified domain name of your RC-2100. This name must be registered with a domain name server and must resolve to the IP address that connecting devices use to establish TLS connections to the RC-2100.</p> <p>This name is almost always a combination of the hostname and domain name entered on the Network System Settings page (section 9.1). The only time where the certificate hostname might differ from the values on the network setting page is when remote devices establish TLS connections via a proxy device that relays TLS traffic to the RC-2100.</p> <p>It is permissible to use an IP address in place of a fully qualified domain name, but this practice is not recommended.</p>	Mandatory
<b>Email Address</b>	<p>Enter the email address of a contact responsible for certificate management. You can use either a personal address or a generic address such as <a href="mailto:ca@um-labs.com">ca@um-labs.com</a></p>	Mandatory
<b>Lifetime</b>	<p>Enter the required certificate lifetime in years. Note that certificate generation process assumes that all years are 365 days long.</p>	Mandatory

Table 6 Certificate Generation

The buttons at the end of the page are activated when all of the mandatory fields are complete. The function of each button is:

**Self-Signed:** This generates a self-signed certificate using the details entered. A self signed certificate is installed immediately, replacing the existing certificate.

**Cert-Request:** This generates a certificate request (in PEM format). The certificate request must be saved locally and then submitted to a trusted Certificate Authority for signing. The mechanism for signing a certificate request is dependent on the CA used. Refer to the documentation for that CA.

**Import-Cert:** This prompts for the pathname of a local file containing a certificate signed by a trusted CA. The certificate must be in PEM format. Once imported and checked for validity this certificate is installed immediately, replacing the existing certificate.

## 11.2. Trusting and using the RC-2100's certificate

Many software phones, including the CounterPath eyebeam require that the certificate of the SIP proxy that they use is confirmed as trusted before a TLS connection for SIP signalling can be made. If you have installed a certificate signed by a trusted CA which in turn has a certificated signed by a well known Certificate Authority (for example VeriSign) then it is likely that your system will already have an appropriate root certificate installed and that no further action need be taken. If you are using a self-signed certificate then you will need to manually verify and trust the certificate.

## RC-2100 SIP Security Controller

For installations where the CounterPath phone is running on Windows, the certificate must be installed in the Windows Trusted Root Certificate store. The simplest way to do achieve this is to run Internet Explorer (not Mozilla or any other browser) and connect to the RC-2100's Web GUI. If the RC-2100's certificate is not already trusted or signed by a trusted CA you will see a message similar to Figure 21.



Figure 21 Internet Explorer Certificate Warning

Click on the view certificate button, then select the details tab and compare the certificate details displayed with those shown on the RC-2100's encryption management page. Pay particular attention to the SHA1 fingerprint, described as the *thumbprint* by Internet Explorer (see Figure 22).

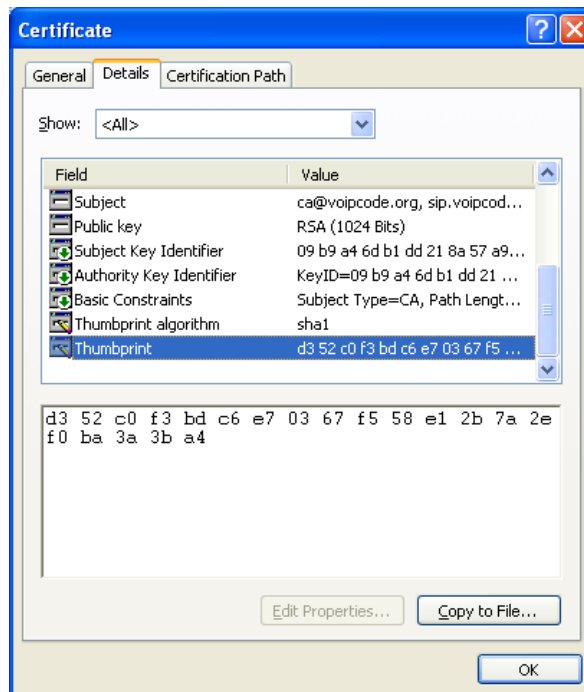


Figure 22 Verifying a Certificate with Internet Explorer

If the details match the certificate summary displayed on the RC-2100's encryption management page, click on the General tab and then click on the Install Certificate button. The certificate will

be installed the Windows Trusted Root Certificate cache and can be used by any application running on that system.

Note: there is no need for the user to login to the GUI to complete this process.

### 11.3. Media Encryption

The RC-2100 can optionally confirm the encryption status of a media stream by playing a short audio tone at the start of a call. The tone is played only on those legs of a call where the media is encrypted. For example if a remote SIP user places a call via an IP-PBX to a number on the standard phone network and if the media stream between that remote user and the RC-2100 is encrypted then the remote SIP user will hear the tone, but the call recipient on the PSTN will not.

Encryption alerts are enabled by checking the *Enable Audio Notification* box on the Media Encryption Management page.

### 11.4. Media Encryption with SDES Key Exchange

The RC-2100 supports the use of SRTP media encryption. SRTP is defined in RFC 3711. SRTP requires that encryption keys for each media stream are established using some external mechanism. Each voice call needs two encryption keys, one for each media stream. Keys are discarded at the end of a call.

The RC-2100 includes support for SDES key exchange (RFC 4568). SDES makes use of the SIP signalling stream to exchange media encryption keys. No configuration is required to enable this feature; the RC-2100 will automatically set up encryption keys and secure the media streams with SRTP when possible. The rules that determine when SDES are used are as follows:

1. If a User Agent Client sends SIP requests to the RC-2100 using TLS transport and if a SIP INVITE request includes a valid SDES crypto offer in the SDP payload then the RC-2100 will add a matching crypto answer to the response and will then secure the media streams to and from that UAC with SRTP.
2. If the RC-2100 forwards an INVITE request to a UAS over a TLS transport connection then the RC-2100 will add a SDES crypto offer to the SDP payload. If the UAS includes a valid crypto answer in the SDP reply then the RC-2100 will secure the media streams to and from that UAC with SRTP.

If both the UAC and UAS are capable of supporting SDES then the RC-2100 will negotiate different sets encryption keys with the UAC and UAS and will set-up SRTP streams using these keys. Media received from the UAC will be decrypted, re-encrypted using a different key and forwarded to the UAS.

Note that if a SDES crypto offer is received over a UDP or TCP transport then the RC-2100 will ignore it and the media streams will not be encrypted. The use of TLS to secure SIP signalling is mandatory when SDES is used.

### 11.5. ZRTP Management

The RC-2100 supports ZRTP as an alternative key exchange mechanism to SDES. ZRTP was designed by Phil Zimmermann, who also developed PGP email encryption (see [www.zfoneproject.com](http://www.zfoneproject.com) and section 5 of this manual). ZRTP is an additional cost option which requires a separate license.

Like SDES, ZRTP is a key exchange protocol which enables to SIP devices to agree encryption keys to use with SRTP to encrypt a media stream. ZRTP has many advantages over SDES. It uses the media stream itself to establish the encryption keys which means that it can work with any SIP transport. This approach also means that encryption keys are not visible to intermediate SIP routing devices. The RC-2100 operates as a ZRTP end-point negotiating keys with a ZRTP capable UAC or UAS. Where both SDES and ZRTP are available, ZRTP will be used in preference to SDES.

ZRTP includes features to detect and prevent Man-in-the-Middle (MiTM) attacks. These include the ability to “enrol” a User Agent and establish secrets that are shared between the UA and the RC-2100 that prevent MiTM attacks. This prior enrolment is optional but is recommended particularly for organisations that are providing ZRTP capable phones to roaming users to enable those users to make encrypted calls back to the office.

ZRTP enrolment is controlled on the ZRTP Management GUI page (see Figure 23).

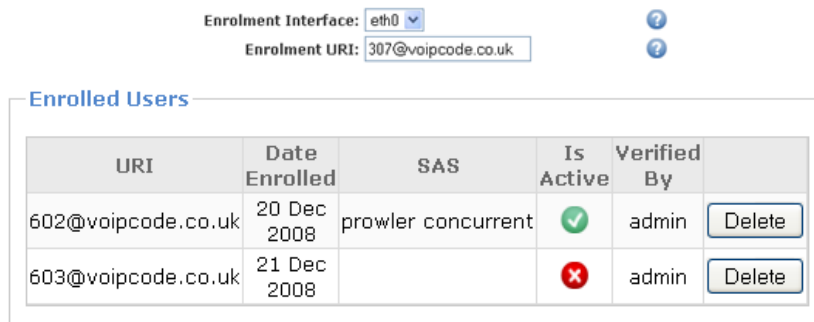


Figure 23 ZRTP Enrolment

The ZRTP enrolment implemented on the RC-2100 is designed to allow trust to be established between a phone and the RC-2100. As part of this process the RC-2100 and the phone will exchange secrets that confirm this trust relationship and prevent any subsequent MitM attack.

As the enrolment process is designed to establish this trust relationship, enrolment should be completed only when other methods exist to check the authenticity of the enrolling phone (for example physical proximity). The recommended process for enrolling a ZRTP phone is as follows:

1. Set up a physically protected network in close proximity to the RC-2100. One option is to dedicate one of the RC-2100's network interfaces for this purpose and connect that interface to a small hub or even an ethernet cross-over cable.
2. Define the enrolment interface on the ZRTP configuration GUI and define an enrolment URI. The enrolment URI should be a number recognised by your PBX. The number can play back a

## RC-2100 SIP Security Controller

simple message or be routed to an identified extension, such as the SIP Security Controller's system administrator.

3. Connect the ZRTP phone that you wish to enrol to the enrolment network, make sure that it registers via the RC-2100 to the local PBX (if appropriate).
4. Call the enrolment URI (depending on your phone's configuration is usually enough to dial the portion of the URI to the left of the @).
5. Ensure that ZRTP correctly secures the call and note the Short Authentication String (SAS) that is displayed by the phone (see Figure 24).
6. Refresh the ZRTP management page and check that the newly enrolled phone is correctly displayed and that the SAS matches that displayed by the phone.



Figure 24 Zfone Control Panel

7. If the displayed short authentication strings match then click the verify button on the web GUI and mark the gateway as trusted on the phone. The mechanism for this is dependent on the phone used. In Zfone click on the *Register with this PBX option* on the edit menu.

Note that once enrolled, the phones entry in the enrolment list will indicate is that that phone is currently associated with an active ZRTP call. If the phone is active then the SAS for the current call is displayed.

An enrolled phone's enrolment status may be cancelled by deleting its entry from the list of enrolled phones displayed on the ZRTP management page.

## 12. Logging and Reporting

**NOTE: the logging and reporting page builds a summary of available logs before content is displayed. On a busy system this may take a minute or more.**

Event logging on the RC-2100 is controlled by the settings on the Logging and Reporting page. The RC-2100 logs all important events including:





- SIP Message Processing
- IP Firewall Security alerts
- Web GUI Authentication events
- Generic system events
- Operating system events
- Web GUI access events

To keep each of these logs to a manageable size, the RC-2100 closes the log when it reaches a predetermined size and starts a new log file. The old log file is renamed and a preset number of old log files are retained. The logging and reporting page allows viewing and searching of the current version of each of the above log files and all retained versions of each file. Searching capabilities are provided by the web browser.

The Logging and Reporting page can also enable additional details to be logged (Debug Logging) and enable a complete trace of all SIP messages processed (SIP Packet Trace). SIP Packet tracing is extremely useful for problem diagnosis, but it should be enabled only when needed. SIP packet tracing will generate some very large files. If left running on a live system it will reduce performance, affect call quality and in extreme cases could cause system failure by filling up all available log space.

As the RC-2100 is a diskless system, there is no long term storage for log files. If the system is rebooted all log files are discarded. If you need to retain log files for audit purposes then define a syslog server on the Network System Settings page (section 9.1 and 17.3). A copy of all log file entries (with the exception of the SIP packet trace) will be sent in real-time to this server.

The Logging and reporting page is split into two sections (see Figure 25). The upper section controls logging parameters while the lower section allows log files to be viewed. The values that should be entered in each of the fields in the control section are summarised in Table 7.

Retained Log Versions: 4   
 Max Log File Size (Kb): 1024   
 Enable Debug Logging:    
 Enable SIP Packet Trace:  

**Log Viewing**

Log type	Current	Historical Index
System Messages	<a href="#">View</a>	<a href="#">View</a>
Kernel Log	<a href="#">View</a>	<a href="#">View</a>
IP Firewall	<a href="#">View</a>	<a href="#">View</a>
Config Management	<a href="#">View</a>	<a href="#">View</a>
SIP Proxy Log	<a href="#">View</a>	<a href="#">View</a>
SIP Packet Trace	<a href="#">View</a>	<a href="#">View</a>
Security	<a href="#">View</a>	<a href="#">View</a>
Authentication	<a href="#">View</a>	<a href="#">View</a>
Web Access Log	<a href="#">View</a>	<a href="#">View</a>

Figure 25 Logging and Reporting

Value	Meaning	Status
<b>Retained Log Version</b>	The number of log file versions to retain, excluding the current version (range 1-4)	Mandatory
<b>Max Log File Size</b>	The maximum size a log file may grow to before it is closed and a new version started. Size is measured in Kilobytes	Mandatory
<b>Enable Debug Logging</b>	Increase the verbosity of the logs	Optional
<b>Enable SIP Packet trace</b>	Save a copy of all processed SIP messages for diagnostic purposes	Optional (do not leave running on a live system)

Table 7 Logging Control Settings

Logs may be viewed by clicking on the appropriate link in either the current or historical index column. Clicking on a link in the current column will show the most recent log file. Clicking on a link in the historical index column will show a list of available log files each with their start and end times and dates. This list includes the current log file.

## 13. User Management

The RC-2100 makes use of two separate user databases. The first controls access to the Web Management GUI, the second is used for SIP authentication (if enabled). The user management pages provide control over both user authentication databases.

### 13.1. System Administrators

The RC-2100 ships with a single pre-defined GUI login, admin (see section 6.3). The system administrators page enables additional administrative users to be added and details, including full name, email address and password of existing users to be changed. The page also allows admin users to be deleted, but note that it is not possible to delete original *admin* user. Figure 26 shows the System Administrators page.

Login	Full Name	Email	Last IP	Role
admin	System Admin			Top Level

**Add a new System Administrator**

Administrator's Type:

Login:

Full Name:

Mail Address:

Figure 26 System Administrators

To add a new administrator, enter a login name, full name and email address and click on *Save*. The new admin login will be created and a random password will be assigned. The password will be displayed on the screen and should be communicated to the new admin user via a secure communication channel. The new user will be forced to change this password on first login. To change the details of an existing user (including the password) click on the login name and fill in the form.

The administrator type defines the rights granted to the new administrator, the available rights levels are:

- Top Level: Can carry out all administrative functions including creating other administrators. The default admin login is a top level administrator.
- Security: Can carry out most functions, but has no access to the Encryption Management pages and cannot create other administrator accounts.
- Cryptographic: Access is limited to the Encryption Management functions only.
- Audit: May view logs but is not permitted to make any configuration changes.

### 13.2. SIP Users

The SIP users page is used to manage the local database that the RC-2100 uses to authenticate SIP requests (see section 10). The RC-2100 will authenticate selected SIP requests that originate

## RC-2100 SIP Security Controller

from devices (for example hardware and software phones) within a local domain. This authentication service requires that the RC-2100's authentication database holds a user name and a password for each device. User names must be specified as full URIs including a domain name. The SIP or SIPs prefix is not needed and should not be entered. Note that passwords are displayed in clear text because this authentication database will be managed by the VoIP administrator and can potentially contain a large number of device URIs and passwords.

Each authenticated device must be configured with the same authentication data that is held for that device by the RC-2100. The format used will depend on the individual device, but it is likely that the user and domain part of the URI will be entered separately (see Figure 2 on page 13 for an example).

The SIP Users Page is split into two sections (Figure 27). The upper section lists all defined URIs with the corresponding passwords.

SIP URI	Password	
234@um-labs.com	testpass	Delete
800@voipcode.org	8ahdsg6	Delete

**New User**

SIP URI:	<input type="text"/>	?
Password:	<input type="text"/>	?

Figure 27 SIP Users

Note that passwords are deliberately displayed in clear text as this page will be used to manage the registration passwords for a number of different devices. This page provides a permanent record of those passwords.

The lower section enables new SIP URIs and passwords to be added to the list.

## 14. Product Licensing

The RC-2100 will operate for a period of 30 days from its initial installation on an evaluation. After that time the system will stop processing calls, although it will still be possible to use web GUI.

The product licensing page lists installed licenses and enables new licenses to be applied. A system running with an evaluation license will always display a license with a license ID consisting of zeros (see Figure 28).

System ID:  
ED0F76

License ID	Description	License Metric	
0000-0000-0000-0000	Evaluation License - Expires 2009-01-15	0	Delete

**New License**

License ID:  ?

Activation key:  ?

Figure 28 License Management

To enable the RC-2100 to continue operation after the evaluation period, the product must be licensed. To license the product visit <http://www.um-labs.com/activate.html> and enter the License ID supplied with the product, the system ID (displayed on the license management page) and the full contact details of the end-user. When all the necessary details are complete click on submit. Assuming that the license ID is valid and that it has not been activated on another system, then an activation key is displayed. This key and the original license ID must be entered in the New License section of the license management page.

Valid formats for the License ID and Activation key are:

**License ID:** AAAA-AAAA-AAAA-AAAA

**Activation Key:** AAAA-AAAA

## 15. Software Updates

**NOTE: the software updates page checks and summarises all available updates before content is displayed. This may take several seconds.**

The software updates page lists available updates that have been loaded on to the RC-2100, identifies which update is currently active and allows new updates to be loaded and activated (see Figure 29).

Current Version: V1.2

Available Images

Version	Date	Description	Active	
V1.2	24 December 2008	Rev 1256	✓	
V1.2	19 December 2008	Factory Default Image		Activate

Figure 29 Software Updates

All systems are shipped with a factory default image. This is always shown at the top of the list of available software images. New images are shipped as software updates which are made available from time to time by UM Labs. When a new update is available, all users with a current support contract will be notified by email. It is therefore important that accurate contact details are entered when the product is registered. The email notification will contain a link to download the new update.

When a notification email is received, the update should be downloaded and saved. All RC-2100 updates are approximately the same size, around 9 Mbytes. A saved image can be uploaded to the RC-2100 by clicking on *Browse* and selecting the saved file. The update will be uploaded and subjected to a number of checks. These checks include verification of cryptographic checksums to ensure that image is a valid and that it has not been tampered with. If the image passes these checks it will be added to the list of available images.

To activate a new image, simply click on the activate button and answer “Yes” when asked to confirm the system reboot. Upgrades, replacing an active image with a new image with a higher version number, will retain your system’s configuration. Downgrading, replacing an active image with a new image with a lower version number is not recommended and may damage your system’s configuration.

Activating the factory default image will discard all configuration information and return your system to its default settings. This includes setting the IP address of eth0 to the default value of 192.168.1.1 or an alternative default set via the console interface.

## 16. System Monitoring

The RC-2100 offers four methods for monitoring system activity and status. The first is the logging and reporting system (section 12), the other three methods are covered in this section.

### 16.1. Dashboard

The dashboard is the default home page for the web GUI and is displayed after logging in. The main dashboard display shows a summary of the number of current active calls and the number of User Agents with an active SIP registration made via the RC-2100. Details of the current active calls and of the currently registered User Agents can be viewed by clicking on the relevant tabs.

The main display also displays a number of key operational parameters. These parameters are displayed in 3 groups; Statistics, Encryption and Failures. The meaning of each displayed parameter is as follows:

#### Statistics:

- **Peak Active Calls:** The maximum number of active calls established through the RC-2100 in the last hour, day or month. Note that an active call is defined as SIP INVITE transaction identified by a call-ID, a To URI and a From URI. If a User Agent makes a call through the RC-2100 to a PBX and as a result the PBX forwards that call to an end-point via the RC-2100 then this will count as two calls.
- **Total Calls:** A cumulative count of initiated calls over the last hour, day or month.
- **Peak Registrations:** The maximum number of active UA registrations made through the RC-2100 in the last hour, day or month.

#### Encryption:

- **TLS:** The number of TLS encrypted calls (SIP INVITE transactions) made in the last, minute, hour day or month.
- **SRTP:** The number of calls (SIP INVITE transactions) where the media stream was encrypted using SRTP with the encryption keys exchanged in the SIP signalling stream using SDES (RFC 4568). Note that the RC-2100 will not permit an SDES key exchange unless the SIP signalling uses TLS.
- **ZRTP:** The number of calls (SIP INVITE transactions) where the media stream was encrypted using SRTP with the encryption keys exchanged in the media stream. If ZRTP is used to establish SRTP encryption keys, SIP signalling may use UDP as a transport protocol. See section 11.5 for more information on ZRTP.

#### Statistics:

- **Calls:** The number of failed calls in the last minute, hour, day or month.
- **SIP Messages:** The number of SIP messages that have failed processing in the last minute, hour, day or month.

- Authentication: The number of SIP authentication failures in the last minute, hour, day or month. This counter records only authentication failures where authentication is processed by the RC-2100.

## 16.2. Status Graphs

The Dashboard also provides a *Graphs* tab. Clicking on this tab displays a menu where parameters can be selected for status graphs.

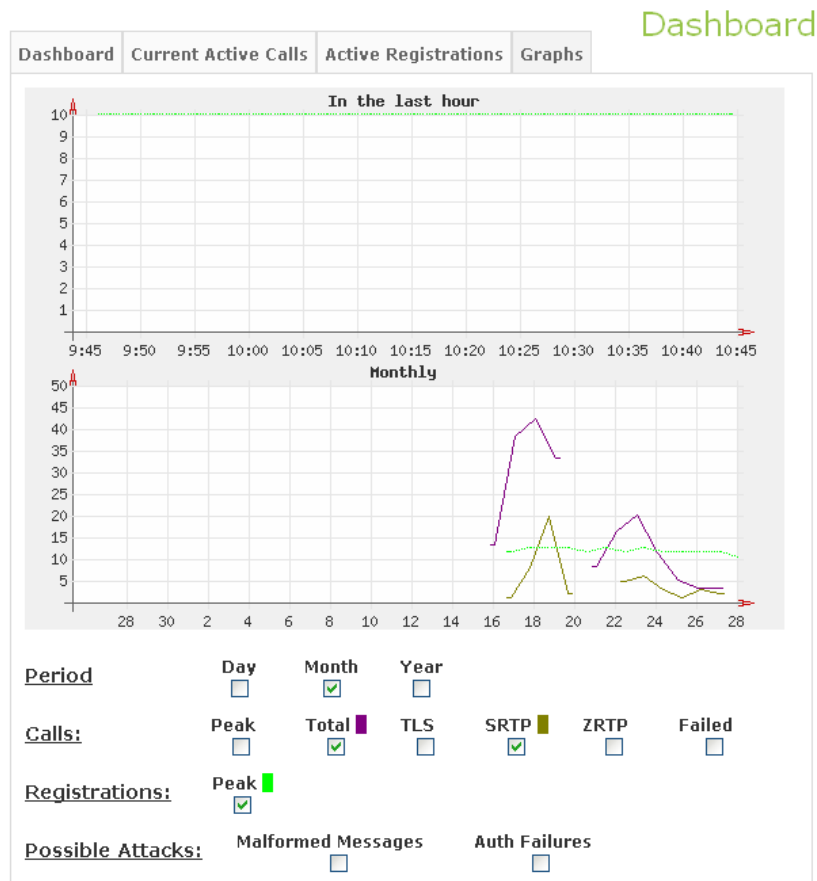


Figure 30 Registration and Active Call Graphs

An example graph is shown in Figure 30. This shows the total calls, the number of calls made where the SIP messages were transported over a TLS channel and the number of active registrations for the last month and the last hour.

In the last hour there were no active calls, but 10 active User Agent Registrations. In the last month, call activity peaked at approximately 42 calls on the 18<sup>th</sup> with 20 of those calls using TLS.

## 16.3. System Status

**NOTE:** the system status page runs real-time checks on critical external servers before content is displayed, this process will take several seconds. The delay will be longer if one or more servers fail to respond.

The system status page checks and reports on the status of critical local services and external servers and in some cases provides control over those services. The status page also lists active GUI logins.

The services monitored by this page are:

**System Services:**

SIP Security Engine	The local service responsible for handling all SIP messages and RTP media streams. Stopping this service will stop all new calls and immediately terminate any active calls.
NTP	The local time synchronisation server. This server should be running at all times to ensure that the system's clock remains accurate.

**Remote Services:**

DNS	The status of each Domain Name Server defined on the System Settings page (section 9.1). At least one DNS must be running. The system may fail to forward calls if no name servers are available.
Syslog	The status of the external syslog server (if defined). The use of an external syslog server is recommended to enable the long-term storage of logs.
NTP	The status of each NTP server defined in the System Settings page. At least one NTP server must be running to ensure accuracy of the RC-2100's clock. Accurate time keeping is important for many of the security controls.

The system status page also offers a range of network diagnostic tools.

Ping is used to check that a system (defined by name or IP address) is reachable. Note that ICMP Echo must be enabled on the local network interface that will be used to reach the destination for this diagnostic to work.

NSlookup is used to check that the RC-2100 can correctly resolve a domain name to an IP address. This utility is particularly useful for diagnosing routing problems, as the result returned will reflect the DNS lookups used by the SIP routing subsystem.

## **16.4. SNMP Management**

The RC-2100 supports SNMP Network monitoring. For security reasons, SNMP must be enabled on each network interface where it is required and a list of permitted SNMP clients must be defined. Entries in the permitted client list may include IP subnets using CIDR notation (for example 192.168.1.0/24). SNMP access is read-only.

## 17. Advanced Topics

### 17.1. SIP Trunks

The term SIP trunk describes a method for using SIP as an alternative to a standard phone line (trunk connection). In most cases a SIP trunk describes a service offer by a SIP service provider to allow a VoIP system to make SIP calls via the service provider to other networks, including the standard phone network.

The term SIP trunk may also be used to describe the link between two locations within the same company.

#### 17.1.1. Service Provider Trunks

The majority of SIP trunk services require that the PBX register with the trunk service. Normally one registration is needed for each number or line provided by the trunk. This registration process enables the trunk to correctly route inbound calls. The trunk operator will provide the necessary registration details. These details should include a domain name (or IP address) of the Registration Server plus one or more usernames and passwords. The PBX should be configured to register with each of the supplied usernames and passwords (refer to your PBX documentation for information on configuring these registrations).

If the PBX is able to register successfully with the trunk service then no special configuration is needed on the SIP Security Controller, assuming that the following conditions are met:

1. The PBX, or a router between the PBX and the SIP Security Controller, is configured so that traffic sent from the PBX to the Trunk provider is routed via the SIP security controller (see section 4.1).
2. The network interface on the SIP Security Controller that receives traffic from the PBX is configured to run a transparent proxy (see section 9.2).
3. The SIP Security Controller is able to send traffic to the trunk provider.
4. If the registration server is defined by a domain name, the at least one Domain Name Server has been configured on the RC-2100.

In some cases it is not possible for the PBX to register with a trunk service. In this case the trunk provider may configure the trunk service so that all incoming calls on the provided number are routed to a pre-configured domain name or IP address. If this configuration option is used, then the trunk service should be configured to route all calls to the SIP Security Controller and an additional SIP route should be configured (see section 9.5).

The required SIP route is shown in Figure 31. The target URI must be either the IP address of one of the SIP Security Controller's interfaces or a hostname which resolved to that address (use whichever value was given to the SIP Service provider). If you would prefer to use a name rather than an IP address, it is important to ensure that this name is different from the target URI of any other defined SIP routes. If necessary create a DNS alias for the SIP Security controller (for example trunkin.yourdomain.com) and use that.

## RC-2100 SIP Security Controller

The destination defined in the SIP route must be the name or IP address of the target PBX. As this route will handle calls from external users, it should be defined as a non-local domain (leave the local domain checkbox blank).

The route will forward any inbound requests from the SIP trunk to the defined PBX. By default the request URI will not change. This means that if the Trunk provider is forwarding calls to 80.1.2.3 and that one of your assigned phone numbers is 020 8123 4567 then the PBX will receive SIP INVITE requests starting with:

```
INVITE sip:02081234567@80.1.2.3
```

If the PBX is unable to handle this request, then a destination map added to the route will convert the request URI to a format that can be understood by the PBX.

**New Route**

Target URI:	<input type="text" value="80.1.2.3"/>	?
Destination:	<input type="text" value="192.168.19.16"/>	?
Port:	<input type="text" value="5060"/>	?
Transport type:	<input checked="" type="radio"/> UDP <input type="radio"/> TCP <input type="radio"/> TLS	?
Local Domain:	<input type="checkbox"/>	?
Destination Map:	<input type="text" value="voipcode.co.uk"/>	?

**Figure 31 Routing Calls from a SIP Trunk**

If for example the destination map value is voipcode.co.uk, then the INVITE in the previous example will be mapped to:

```
INVITE sip:02081234567@voipcode.co.uk
```

The domain name (or IP address) used in the Destination Map may be the same as the target URI used in another routing entry.

### 17.1.2. Private Trunks

The RC-2100 provides an ideal solution to the problem of providing a secure VoIP link between two locations within the same organisation. For example two RC-2100s could secure the link between a branch office and a head office encrypting all SIP signalling with TLS and securing all media traffic with SRTP. Larger organisations with multiple branch locations may chose to install an EC-4200 at the head office which could handle links from multiple branches (see Figure 32).

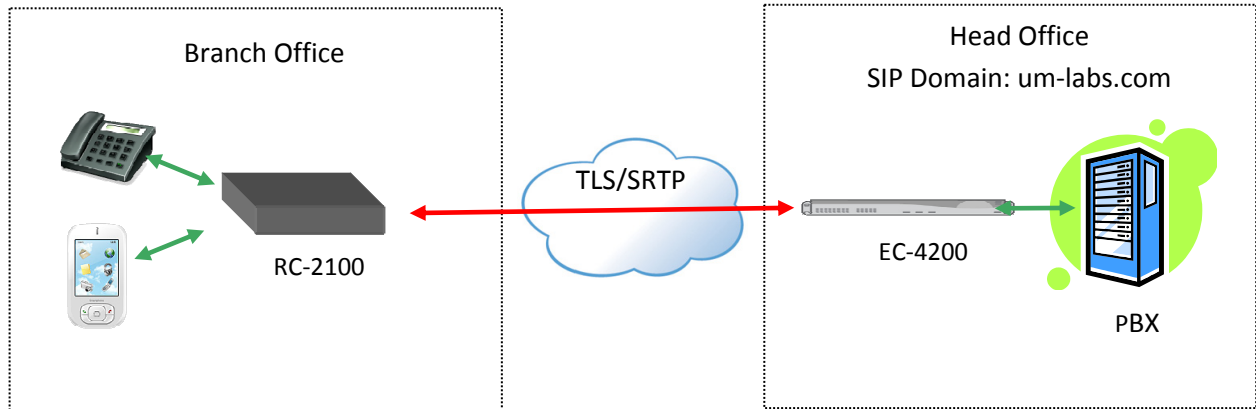


Figure 32 Securing Remote Office Connections

To configure this link, a SIP route should be defined on the branch office RC-2100. SIP routes are configured on the SIP Routes page (section 9.5.) Assuming the SIP domain in use at the head office PBX is um-labs.com and that the domain name for the EC-4200 is sip.um-labs.com, the required route is:

URI	Destination	Trans	Local	Status	Auth
<input type="checkbox"/> um-labs.com	sip.um-labs.com	TLS	<input checked="" type="checkbox"/>		<a href="#">Auth</a>
Delete					

Figure 33 Branch Office SIP Route

Setting the SIP transport to TLS will force the branch office RC-2100 to use an encrypted channel for all SIP signalling sent to the head office and to negotiate SRTP encrypted media streams. The phones in the branch office should be configured to register with the um-labs.com SIP domain at sip.um-labs.com (the SIP Security Controller at the head office). To achieve this, the phones should either have their default IP gateway set to their local RC-2100 or should be configured to use the RC-2100 as their outbound proxy. In the former case the RC-2100 must be configured to run a transparent proxy (see Network interfaces, section 9.2)

The head office SIP Security will need a SIP route to direct traffic to the PBX:

URI	Destination	Trans	Local	Status	Auth
<input type="checkbox"/> um-labs.com	pbx.um-labs.com	UDP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Auth</a>
Delete					

Figure 34 Head Office SIP Route

Note that in both cases the route is defined as local.

If SIP authentication services are required they should be enabled at the head office, not at the branch office.

## 17.2. Deploying the RC-2100 behind a Firewall

While the preferred deployment for an RC-2100 is in parallel with an existing firewall, there are occasions when this deployment is not possible, either because of local security policy or because of a lack of available IP addresses. In either of these cases, the RC-2100 may be installed behind a firewall.

There are many possible options to deploy a RC-2100 behind a Firewall, one of the simplest is to use two interfaces on the RC-2100 and to connect the system between the Firewall's DMZ and the internal network, see Figure 35.

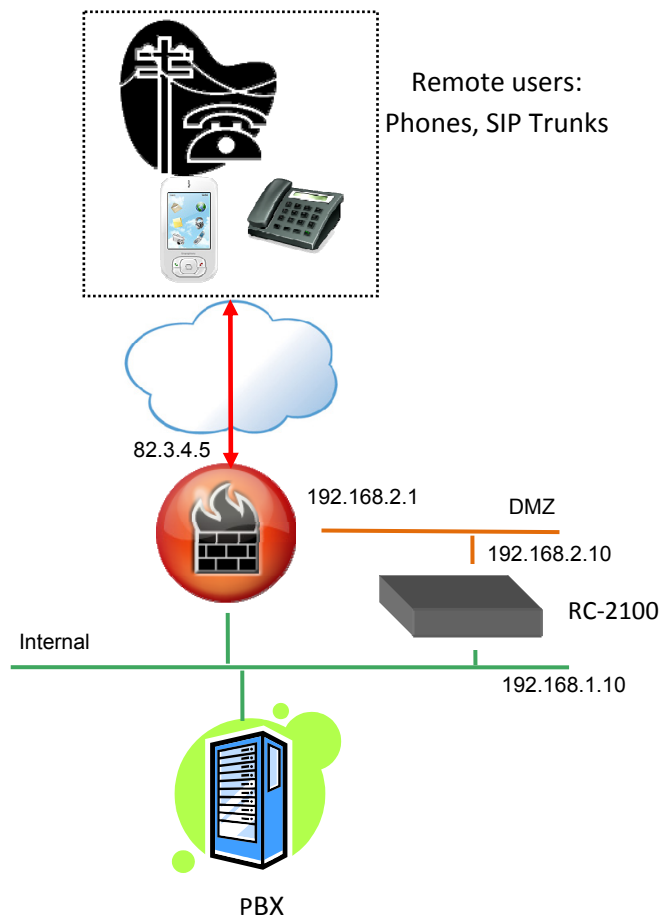


Figure 35 RC-2100 Firewall Connections

In this configuration, the Firewall must be configured to allow bidirectional SIP and RTP traffic between its external interface (82.3.4.5) and the RC-2100 on the DMZ. The details of the Firewall's configuration will depend on the SIP transports used and on the RTP port range defined on the RC-2100's Network System Settings page (section 9.1). Assuming that the RC-2100 is configured to use all 3 SIP transports on the default ports and that the default RTP port range of 16000-16200 is used then the following firewall rules will be required to enable SIP and

RTP traffic. These rules also assume that all external SIP destinations, for example SIP Trunks are using the standard ports.

- Enable inbound UDP, destination port 5060 source port any, apply destination IP mapping from 82.3.4.5 to 192.168.2.10
- Enable outbound UDP, source port any destination port 5060, apply source IP mapping from 192.168.2.10 to 82.3.4.5
- Enable inbound TCP connections, destination port 5060 source port any, apply destination IP mapping from 82.3.4.5 to 192.168.2.10
- Enable outbound TCP connections, source port any destination port 5060, apply source IP mapping from 192.168.2.10 to 82.3.4.5
- Enable inbound TCP connections, destination port 5061 source port any, apply destination IP mapping from 82.3.4.5 to 192.168.2.10
- Enable outbound TCP connections, source port any destination port 5061, apply source IP mapping from 192.168.2.10 to 82.3.4.5
- Enable inbound UDP, destination port range 16000 to 16200 source port any, apply destination IP mapping from 82.3.4.5 to 192.168.2.10
- Enable outbound UDP, source port range 16000 to 16200 destination port any, apply source IP mapping from 192.16.2.10 to 82.3.4.5

Additional firewall rules will be needed if one or more of the Domain Name Server or NTP servers are reached via the firewall, or if there is a requirement to allow access to the admin GUI via the Firewall. The option rules are as follows:

- Enable outbound UDP, source port any destination port 53, apply source IP mapping from 192.168.2.10 to 82.3.4.5. This enables DNS lookups via the Firewall.
- Enable outbound UDP, source port any destination port 123, apply source IP mapping from 192.168.2.10 to 82.3.4.5. This enables access to a NTP server via the Firewall.
- Enable inbound TCP connections, destination port 443 source port any, apply destination IP mapping from 82.3.4.5 to 192.168.2.10. This enables web GUI connections via the Firewall.

The RC-2100 should be configured to use the Firewall's DMZ IP address (192.168.2.1) as a default gateway. In addition the Firewall's external IP address (82.3.4.5) must be entered as the *External Firewall IP* on the set up for the RC -2100s network interface.

Finally, the PBX should be configured to use the RC-2100's IP address (192.168.1.10) as its default gateway.

### **17.3. Configuring an external syslog server**

If a remote syslog server is defined on the network system settings page (section 9.1) then that remote server must be configured to accept log messages from the RC-2100 and to handle those messages appropriately. The details of the necessary configuration settings will depend on syslog server used and its host system. The following examples are based on a Unix system.

The first step is to ensure that your syslog server will accept log entries from a remote system. In most cases the default behaviour is to reject log entries from non local IP addresses. Unix syslog servers require a startup flag to enable acceptance of syslog messages from remote systems. Assuming that the address of the interface that the RC-2100 uses to send messages to the remote syslog server is 192.168.1.1 then add the following argument to your systems startup script for syslog:

```
-a 192.168.1.1:*
```

The trailing \* indicates that the syslog server will accept messages from any UDP source port.

The second step is to define how received syslog messages should be processed. The RC-2100 users a number of syslog facilities and levels to tag its messages. Most system and kernel messages use standard Unix levels and facilities. SIP proxy messages are sent with the local1 facility while Web Access log messages are sent with daemon.info. To enable all SIP proxy messages to be sent to /var/log/sipproxy.log and all Web Access log messages to be sent to /var/log/rc2100gui.log add the following lines to your system's syslog.conf file and re-start the syslog server.

```
local1.*          /var/log/sipproxy.log
daemon.info       /var/log/rc2100gui.log
```

Many systems will require that these logfiles are manually created before the syslog server is re-started. You should also ensure that these entries do not conflict with any existing log policy.

## 18. Glossary

<b>Address of Record</b>	The formal name a SIP device's permanent identity. This is defined as a SIP URI, for example <a href="mailto:sip:+442030213200@um-labs.com">sip:+442030213200@um-labs.com</a> or <a href="mailto:sip:info@umlabs.com">sip:info@umlabs.com</a>
<b>CA</b>	See Certificate Authority.
<b>Call Hijacking</b>	A VoIP security threat that allows a malicious attacker to take control of an established call.
<b>Certificate Authority</b>	A Certificate Authority (CA) is a trusted system that can sign certificates by producing a cryptographic hash of a server certificate. If a device such as browser has an authenticated copy of the CA's own certificate then any certificate signed by that CA or by an intermediate CA whose certificate is signed by the trusted CA can in turn be trusted. Trust means that identify of the system presenting a signed certificate can be established. Web browsers are shipped with a number of known root certificates of well-known CAs for this purpose.
<b>CIDR</b>	Classless Inter-Domain Routing. CIDR IP addresses provide a convenient way of representing an IP network address and a subnet mask. CIDR addresses are not limited to Class A, B and C addresses. For example while 192.168.1.0/24 is a standard class C network, 192.168.1.16/28 represents a set of 16 IP addresses starting at the network address of 192.168.1.16.
<b>Device Registration</b>	See Registration
<b>Diffie-Hellman</b>	Diffie-Hellman (D-H) key exchange is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.
<b>ECDH</b>	Elliptic Curve Diffie-Hellman (ECDH) is a key agreement protocol that allows two parties to establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. It is a variant of the Diffie-Hellman protocol using elliptic curve cryptography.
<b>Far End NAT-Traversal</b>	Far End NAT-Traversal refers to the challenge of making a VoIP call when that call must pass through a remote firewall or other NAT Gateway that may not be under the direct control of the organisation running the VoIP service.
<b>FQDN</b>	Fully qualified domain name. An internet domain name including both host and domain parts. For example <a href="http://www.um-labs.com">www.um-labs.com</a>

<b>IP Address</b>	A unique address that identifies a device on an IP network. IPV4 addresses are expressed in the familiar dotted notation, for example 10.11.22.33.
<b>Jitter</b>	The term jitter is used to describe unwanted variations in one or more characteristics of a periodic signal. In the context of VoIP processing, jitter is most commonly introduced by variable intervals in the delivery of RTP packets. This variation can be caused by network delays or processing delays at network gateways. Jitter results in a degradation in the quality of an audio (or video) signal as perceived by the caller or recipient.
<b>Media</b>	The voice and/or video stream of a VoIP or Video call
<b>MiTM</b>	Man-in-the-Middle. A method of attacking an encrypted data stream where the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker.
<b>NAT</b>	Network Address Translation. The process where a Firewall or other gateway maps IP addresses between private addresses used on a protected IP subnet and public addresses used on the Internet.
<b>Port</b>	On IP devices, a port is a service identifier. Standard services <i>listen on well known ports</i> . For example email servers listen on port 25 and most web servers listen on port 80. Ports used in VoIP applications are not fixed in the same way. While SIP servers normally listen on port 5060 or 5061, other ports may be used, and the ports used by RTP media streams are dynamic and have to be negotiated for each call.
<b>Registration</b>	The process where a VoIP end-point, for example a hardware or software phone, registers with a PBX to link its permanent identify with its local network identity and to indicate its willingness to accept calls. Its permanent identity, or Address of Record (AOR) is equivalent to a phone number and on SIP networks is defined as a SIP URI
<b>Request URI</b>	<p>The URI in the first line of a SIP message. The Request URI indicates the target of the request. For example a SIP message starting with:</p> <pre>REGISTER sip:um-labs.com SIP/2.0</pre> <p>is request to register at the destination indicated by the Request URI (sip@um-labs.com), while the message starting with:</p> <pre>INVITE sip:+442030213200@trunk.net SIP/2.0</pre> <p>Is a request to place a call to the destination indicated by the Request URI (<a href="mailto:sip:+442030213200@trunk.net">sip:+442030213200@trunk.net</a>).</p>
<b>RTP</b>	Realtime Transport Protocol, the protocol that delivers media for SIP based application and other VoIP protocols

<b>RTP Injection</b>	A VoIP security threat that allows a malicious attacker to feed an alternative media (voice or video) stream into an established call.
<b>RTP Media</b>	See Media
<b>SDES</b>	A protocol for establishing SRTP encryption keys via SIP signalling.
<b>SDP</b>	Session Description Protocol. The protocol used by SIP and carried as a SIP message payload to negotiate media (RTP) end-points for a call.
<b>Self-Signed</b>	A certificate signed by the certificate issuer rather than a trusted CA. Generating a self-signed certificate offers a quick way to get a web server or other device using TLS encryption up and running, but the certificate cannot be automatically verified.
<b>Server Certificate</b>	A signed public key presented in a special format by a web server when an encrypted (HTTPS) connection is established. Ideally the certificate should be signed by a trusted <i>certificate authority</i> , but certificates may also be <i>self-signed</i> .
<b>Signalling</b>	The component of a VoIP protocol suite responsible for call control, including call setup, call termination, call transfer and device registration.
<b>SIP</b>	Session Initiation Protocol. The signalling protocol for SIP based VoIP applications.
<b>SIP Methods</b>	<p>Each SIP transaction starts with a SIP request such as INVITE (to start a new call) or BYE (to terminate an existing call). The formal name of these requests is SIP Methods. There are a total of 14 different SIP methods, these are:</p> <ul style="list-style-type: none"><li>• INVITE , start a new call</li><li>• ACK, acknowledge a final response to a previous request.</li><li>• REGISTER, register a User Agent (phone)</li><li>• BYE, terminate a call</li><li>• OPTIONS, request status information from a SIP device</li><li>• INFO, carries signalling information for an established call</li><li>• CANCEL, cancel a pending request</li><li>• REFER, a request to a UA to connect to a resource identified by a URI</li><li>• SUBSCRIBE, a request to be notified about certain events (e.g. available for calls)</li><li>• NOTIFY, carries event information following a previous subscribe</li><li>• MESSAGE, transports SIP Instant Messages</li><li>• PRACK, Acknowledge provisional SIP responses</li><li>• UPDATE, changes parameters in an established call</li><li>• PUBLISH,</li></ul>
<b>SIP Transaction</b>	A series of SIP messages that define a logical transaction, for example registering a phone, placing a call or terminating a call.

<b>SRTP</b>	Secure RTP, a variant of the RTP protocol where the media payload (the voice of video) is encrypted.
<b>TLS</b>	Transport Layer Security, the official name for the SSL protocol used to encrypt web access. SIP uses TLS to encrypt Signalling Messages.
<b>UA</b>	See User Agent
<b>UAC</b>	See User Agent Client
<b>UAS</b>	See User Agent Server. A UAS processes requests from a UAC.
<b>URI</b>	Uniform Resource Identifier. A standardised way of locating resources on IP networks. A URI consists of a <i>scheme name</i> which identifies the resource type (for example a web page or a callable SIP address) followed by a scheme specific identifier. Examples include <a href="http://www.um-labs.com">http://www.um-labs.com</a> and <a href="sip:info@um-labs.com">sip:info@um-labs.com</a>
<b>User Agent</b>	A SIP User Agent (UA) is an end-device (for example a hardware or software phone or a PBX). User Agents include both client and server applications.
<b>User Agent Client</b>	The collection of client applications in a User Agent. A UAC normally register with a UAS using the REGISTER method, initiate or receive calls using the INVITE method and terminate calls using the BYE method. A UAC may also use any of the other SIP methods.
<b>User Agent Server</b>	The collection of server applications in a User Agent
<b>ZRTP</b>	Phil Zimmerman's protocol for key exchange which establishes encryption keys for SRTP sessions via the media stream.

## 19. Appendix 1, Time zones

The system's time zone must be set as described in section 9.1. The Web GUI provides a choice of over 450 time zones arranged in 15 Regions. Each region is highlighted, and the time zones within that region are arranged alphabetically. The regions are:

- Africa
- America
- Antarctica
- Arctic
- Asia
- Atlantic
- Australia
- Brazil
- Canada
- Chile
- Europe
- Indian
- Mexico
- Pacific
- US

For reference a complete list of time zones follows:

Region	Time zone
Africa	Abidjan
Africa	Accra
Africa	Addis Ababa
Africa	Algiers
Africa	Asmera
Africa	Bamako
Africa	Bangui
Africa	Banjul
Africa	Bissau
Africa	Blantyre
Africa	Brazzaville
Africa	Bujumbura
Africa	Cairo
Africa	Casablanca
Africa	Ceuta
Africa	Conakry
Africa	Dakar

Region	Time zone
Africa	Dar es Salaam
Africa	Djibouti
Africa	Douala
Africa	El Aaiun
Africa	Freetown
Africa	Gaborone
Africa	Harare
Africa	Johannesburg
Africa	Kampala
Africa	Khartoum
Africa	Kigali
Africa	Kinshasa
Africa	Lagos
Africa	Libreville
Africa	Lome
Africa	Luanda
Africa	Lubumbashi

*RC-2100 SIP Security Controller*

Region	Time zone
Africa	Lusaka
Africa	Malabo
Africa	Maputo
Africa	Maseru
Africa	Mbabane
Africa	Mogadishu
Africa	Monrovia
Africa	Nairobi
Africa	Ndjamena
Africa	Niamey
Africa	Nouakchott
Africa	Ouagadougou
Africa	Porto-Novo
Africa	Sao Tome
Africa	Timbuktu
Africa	Tripoli
Africa	Tunis
Africa	Windhoek
America	Adak
America	Anchorage
America	Anguilla
America	Antigua
America	Araguaina
America	Buenos Aires, Argentina
America	Catamarca, Argentina
America	ComodRivadavia, Argentina
America	Cordoba, Argentina
America	Jujuy, Argentina
America	La Rioja, Argentina
America	Mendoza, Argentina
America	Rio Gallegos, Argentina
America	San Juan, Argentina
America	Tucuman, Argentina
America	Ushuaia, Argentina
America	Aruba
America	Asuncion
America	Atikokan
America	Atka
America	Bahia
America	Barbados
America	Belem
America	Belize
America	Blanc-Sablon

Region	Time zone
America	Boa Vista
America	Bogota
America	Boise
America	Buenos Aires
America	Cambridge Bay
America	Campo Grande
America	Cancun
America	Caracas
America	Catamarca
America	Cayenne
America	Cayman
America	Chicago
America	Chihuahua
America	Coral Harbour
America	Cordoba
America	Costa Rica
America	Cuiaba
America	Curacao
America	Danmarkshavn
America	Dawson
America	Dawson Creek
America	Denver
America	Detroit
America	Dominica
America	Edmonton
America	Eirunepe
America	El Salvador
America	Ensenada
America	Fort Wayne
America	Fortaleza
America	Glace Bay
America	Godthab
America	Goose Bay
America	Grand Turk
America	Grenada
America	Guadeloupe
America	Guatemala
America	Guayaquil
America	Guyana
America	Halifax
America	Havana
America	Hermosillo
America	Indianapolis, Indiana

*RC-2100 SIP Security Controller*

Region	Time zone
America	Knox, Indiana
America	Marengo, Indiana
America	Petersburg, Indiana
America	Vevay, Indiana
America	Vincennes, Indiana
America	Indianapolis
America	Inuvik
America	Iqaluit
America	Jamaica
America	Jujuy
America	Juneau
America	Louisville, Kentucky
America	Monticello, Kentucky
America	Knox IN
America	La Paz
America	Lima
America	Los Angeles
America	Louisville
America	Maceio
America	Managua
America	Manaus
America	Martinique
America	Mazatlan
America	Mendoza
America	Menominee
America	Merida
America	Mexico City
America	Miquelon
America	Moncton
America	Monterrey
America	Montevideo
America	Montreal
America	Montserrat
America	Nassau
America	New York
America	Nipigon
America	Nome
America	Noronha
America	Center, North Dakota
America	New Salem, North Dakota
America	Panama
America	Pangnirtung
America	Paramaribo

Region	Time zone
America	Phoenix
America	Port-au-Prince
America	Port of Spain
America	Porto Acre
America	Porto Velho
America	Puerto Rico
America	Rainy River
America	Rankin Inlet
America	Recife
America	Regina
America	Rio Branco
America	Rosario
America	Santiago
America	Santo Domingo
America	Sao Paulo
America	Scoresbysund
America	Shiprock
America	St Johns
America	St Kitts
America	St Lucia
America	St Thomas
America	St Vincent
America	Swift Current
America	Tegucigalpa
America	Thule
America	Thunder Bay
America	Tijuana
America	Toronto
America	Tortola
America	Vancouver
America	Virgin
America	Whitehorse
America	Winnipeg
America	Yakutat
America	Yellowknife
Antarctica	Casey
Antarctica	Davis
Antarctica	DumontDURville
Antarctica	Mawson
Antarctica	McMurdo
Antarctica	Palmer
Antarctica	Rothera
Antarctica	South Pole

RC-2100 SIP Security Controller

Region	Time zone
Antarctica	Syowa
Antarctica	Vostok
Arctic	Longyearbyen
Asia	Aden
Asia	Almaty
Asia	Amman
Asia	Anadyr
Asia	Aqtau
Asia	Aqtobe
Asia	Ashgabat
Asia	Ashkhabad
Asia	Baghdad
Asia	Bahrain
Asia	Baku
Asia	Bangkok
Asia	Beirut
Asia	Bishkek
Asia	Brunei
Asia	Calcutta
Asia	Choibalsan
Asia	Chongqing
Asia	Chungking
Asia	Colombo
Asia	Dacca
Asia	Damascus
Asia	Dhaka
Asia	Dili
Asia	Dubai
Asia	Dushanbe
Asia	Gaza
Asia	Harbin
Asia	Hong Kong
Asia	Hovd
Asia	Irkutsk
Asia	Istanbul
Asia	Jakarta
Asia	Jayapura
Asia	Jerusalem
Asia	Kabul
Asia	Kamchatka
Asia	Karachi
Asia	Kashgar
Asia	Katmandu

Region	Time zone
Asia	Krasnoyarsk
Asia	Kuala Lumpur
Asia	Kuching
Asia	Kuwait
Asia	Macao
Asia	Macau
Asia	Magadan
Asia	Makassar
Asia	Manila
Asia	Muscat
Asia	Nicosia
Asia	Novosibirsk
Asia	Omsk
Asia	Oral
Asia	Phnom Penh
Asia	Pontianak
Asia	Pyongyang
Asia	Qatar
Asia	Qyzylorda
Asia	Rangoon
Asia	Riyadh
Asia	Saigon
Asia	Sakhalin
Asia	Samarkand
Asia	Seoul
Asia	Shanghai
Asia	Singapore
Asia	Taipei
Asia	Tashkent
Asia	Tbilisi
Asia	Tehran
Asia	Tel Aviv
Asia	Thimbu
Asia	Thimphu
Asia	Tokyo
Asia	Ujung Pandang
Asia	Ulaanbaatar
Asia	Ulan Bator
Asia	Urumqi
Asia	Vientiane
Asia	Vladivostok
Asia	Yakutsk
Asia	Yekaterinburg

*RC-2100 SIP Security Controller*

Region	Time zone
Asia	Yerevan
Atlantic	Azores
Atlantic	Bermuda
Atlantic	Canary
Atlantic	Cape Verde
Atlantic	Faeroe
Atlantic	Jan Mayen
Atlantic	Madeira
Atlantic	Reykjavik
Atlantic	South Georgia
Atlantic	St Helena
Atlantic	Stanley
Australia	ACT
Australia	Adelaide
Australia	Brisbane
Australia	Broken Hill
Australia	Canberra
Australia	Currie
Australia	Darwin
Australia	Hobart
Australia	LHI
Australia	Lindeman
Australia	Lord Howe
Australia	Melbourne
Australia	NSW
Australia	North
Australia	Perth
Australia	Queensland
Australia	South
Australia	Sydney
Australia	Tasmania
Australia	Victoria
Australia	West
Australia	Yancowinna
Brazil	Acre
Brazil	DeNoronha
Brazil	East
Brazil	West
Canada	Atlantic
Canada	Central
Canada	East-Saskatchewan
Canada	Eastern
Canada	Mountain

Region	Time zone
Canada	Newfoundland
Canada	Pacific
Canada	Saskatchewan
Canada	Yukon
Chile	Continental
Chile	Easter Island
Europe	Amsterdam
Europe	Andorra
Europe	Athens
Europe	Belfast
Europe	Belgrade
Europe	Berlin
Europe	Bratislava
Europe	Brussels
Europe	Bucharest
Europe	Budapest
Europe	Chisinau
Europe	Copenhagen
Europe	Dublin
Europe	Gibraltar
Europe	Guernsey
Europe	Helsinki
Europe	Isle of Man
Europe	Istanbul
Europe	Jersey
Europe	Kaliningrad
Europe	Kiev
Europe	Lisbon
Europe	Ljubljana
Europe	London
Europe	Luxembourg
Europe	Madrid
Europe	Malta
Europe	Mariehamn
Europe	Minsk
Europe	Monaco
Europe	Moscow
Europe	Nicosia
Europe	Oslo
Europe	Paris
Europe	Podgorica
Europe	Prague
Europe	Riga

RC-2100 SIP Security Controller

Region	Time zone
Europe	Rome
Europe	Samara
Europe	San Marino
Europe	Sarajevo
Europe	Simferopol
Europe	Skopje
Europe	Sofia
Europe	Stockholm
Europe	Tallinn
Europe	Tirane
Europe	Tiraspol
Europe	Uzhgorod
Europe	Vaduz
Europe	Vatican
Europe	Vienna
Europe	Vilnius
Europe	Volgograd
Europe	Warsaw
Europe	Zagreb
Europe	Zaporozhye
Europe	Zurich
Indian	Antananarivo
Indian	Chagos
Indian	Christmas
Indian	Cocos
Indian	Comoro
Indian	Kerguelen
Indian	Mahe
Indian	Maldives
Indian	Mauritius
Indian	Mayotte
Indian	Reunion
Mexico	Baja Norte
Mexico	Baja Sur
Mexico	General
Pacific	Apia
Pacific	Auckland
Pacific	Chatham
Pacific	Easter
Pacific	Efate
Pacific	Enderbury
Pacific	Fakaofu
Pacific	Fiji

Region	Time zone
Pacific	Funafuti
Pacific	Galapagos
Pacific	Gambier
Pacific	Guadalcanal
Pacific	Guam
Pacific	Honolulu
Pacific	Johnston
Pacific	Kiritimati
Pacific	Kosrae
Pacific	Kwajalein
Pacific	Majuro
Pacific	Marquesas
Pacific	Midway
Pacific	Nauru
Pacific	Niue
Pacific	Norfolk
Pacific	Noumea
Pacific	Pago Pago
Pacific	Palau
Pacific	Pitcairn
Pacific	Ponape
Pacific	Port Moresby
Pacific	Rarotonga
Pacific	Saipan
Pacific	Samoa
Pacific	Tahiti
Pacific	Tarawa
Pacific	Tongatapu
Pacific	Truk
Pacific	Wake
Pacific	Wallis
Pacific	Yap
US	Alaska
US	Aleutian
US	Arizona
US	Central
US	East-Indiana
US	Eastern
US	Hawaii
US	Indiana-Starke
US	Michigan
US	Mountain
US	Pacific

*RC-2100 SIP Security Controller*

Region	Time zone
US	Pacific-New
US	Samoa