Resolution1 Locksmith Install Guide

Resolution1 Locksmith Install Guide

This guide focuses on the more critical aspects of the installation and is not intended to cover every step or address all installation possibilities. Please contact support if you need additional assistance.

Important: Resolution1 SecurityLocksmith runs on Ubuntu 12.10 LTS 64-bit PC (AMD64) server. Please do not upgrade your appliance to the latest version of the Ubuntu OS (i.e. DO NOT run 'do-release-upgrade' to upgrade it).

Preparing for Installation

Before installing the appliance, you should determine the networking addresses that will be used while configuring Resolution1 Locksmith. This will insure that your network outage will be minimal while installing AD Locksmith. Locate and record these items:

- Bridge IP Address ______________________________
  This IP address should be one that is routable on the network that the bridge is on.
- Subnet Mask for the Bridge: ____________________________________
  An example of a subnet mask is 255.255.255.0
- Management IP Address:____

Note: The Management IP address MUST be in a different subnet from the one that the bridge is on.

Installing the Appliance

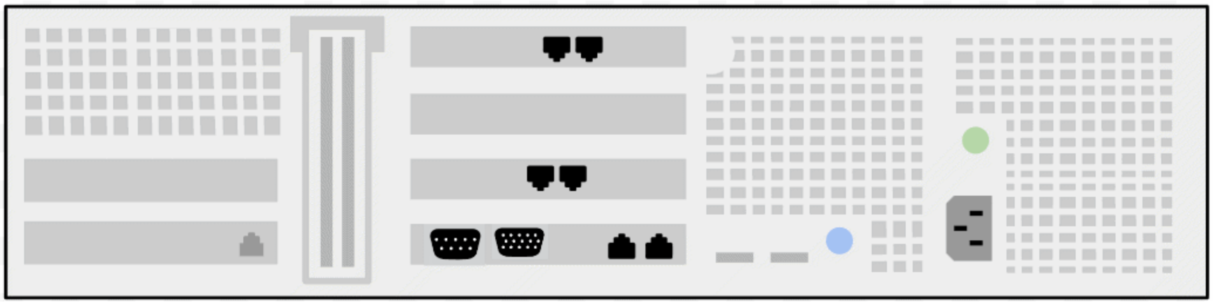
Resolution1 Locksmith uses four Ethernet ports for communication: the IN port, the OUT port, the port to the collector (We recommend Resolution1 Network Security Monitoring for best performance), and the port to the management user interface.

The appliance should be mounted in a server rack and Ethernet cables attached to the four ports.

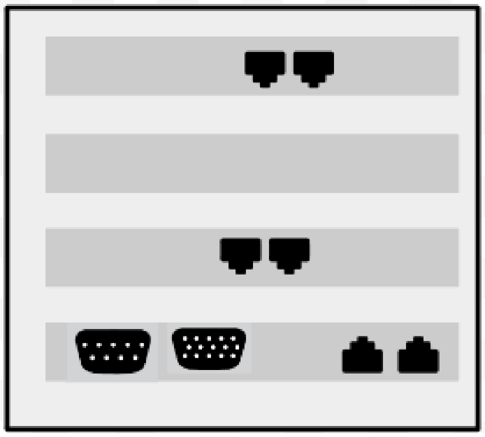
To install the appliance

1. Mount the appliance to the server rack.
2. Plug in the power supply.

Resolution1 Locksmith Installation Diagram



Closeup of Ethernet Ports



There are three sets of Ethernet ports located in the middle of the server: an upper set, a middle set, and a lower set of ports. Attach your Ethernet cables to the following ports, as displayed in the above diagram:

- The Ethernet IN cable from your server to one of the Ethernet ports located in the upper set of ports. The dual Ethernet ports are a bridged interface. You can choose either port for the Ethernet IN cable.
- The Ethernet OUT cable from your server to the Ethernet port in the bridged interface. Select the port that is not already used by the Ethernet IN cable.
- The Manage Ethernet cable from your server to the left port located in the middle set of Ethernet ports.
- The Ethernet cable from your collector server, such as Resolution1 Network Security Monitoring, to the right (sniff) port located in the middle set of Ethernet ports.
- You can access the web interface via the DHCP ports from the lower set of Ethernet ports to configure Resolution1 Locksmith. See Configuring Resolution1 Locksmith By Web Interface on page 12.

Logging into the Console

Before configuring Resolution1 Locksmith, you should log in to the appliance and configure it for your network.

To change the user’s default password

1. Log in as user **locksmith**
2. Enter the password. The default password is **lock_123**
3. You should change this password immediately by entering the command **passwd** and providing a new password for user **locksmith**

Configuring Resolution1 Locksmith for Your Network

Prerequisites for Configuration

After changing the default password, you will need to configure the Resolution1 Locksmith appliance. This should be run upon first boot up of the appliance. Before configuring the appliance, you should make sure that the following prerequisites are met.

First, you should obtain three certificates:

- A management certificate
- A trusted CA resigning certificate
- An untrusted CA resigning certificate

Resolution1 Locksmith ships with self-signed certificates, and can generate self-signed certificates for proof of concept.

However, it is suggested that you acquire your own Certificate Authority and create certificates for this purpose.

The second prerequisite for Resolution1 Locksmith is that you need to insure that there is enough allocated space on the network. The Resolution1 Locksmith appliance is placed between the firewall and the core switch or another appropriate location in the egress path. It is assigned some dedicated IP addresses. Because of this, make sure to allocate a large enough subnet in order to have available IP addresses for assignment to the appliance in the egress network.

You can configure Resolution1 Locksmith in one of two ways: by running a Python script on the Resolution1 Locksmith console, or by accessing the configuration page through the web interface.

See Configuring Resolution1 Locksmith By Console on page 10.

See Configuring Resolution1 Locksmith By Web Interface on page 12.

Configuring Resolution1 Locksmith By Console

To configure Resolution1 Locksmith by using the console, you will need to run a Python script that is provided. After running the script, a series of questions appears. You will need to provide the information asked.

To configure the appliance by using the console

1. Make sure that the appliance is connected to the network and powered on.
2. Run the Python script with root privileges by typing sudo ./configure-locksmith. py .
3. At the first prompt, **enter the IP address used for the bridge interface**. Use dotted quad notation. This address needs to be routable on the network that it’s been on.
4. At the second prompt, **enter the subnet mask for the bridged interface**. The default address is 255.255.255.0 .
5. At the third prompt, enter the IP and subnet info for the sniff interface. This interface will send out all traffic decrypted that goes through the bridged interface. Use dotted quad with CIDR notation. The default is 169.254.6.16/16 .
6. At the fourth prompt, enter the address for the ARP IP, accept the default for this address, which is 169.254.6.18, and hit Enter. This is the destination address for all mirrored traffic that goes through the

fake MAC interface, and should only be changed if there is a conflict with another address on the network.

7. At the fifth prompt, enter the hardware address where ARP will send all traffic, accept the default for this address, which is 000000010203, and hit Enter. This is commonly referred to as the MAC address. These are hard coded into the network and should only be changed if there is a conflict.
8. At the sixth prompt, enter the IP for the management interface. This address is used for remote access and the web interface. This address needs to be on a different subnet than the bridged interface, or Locksmith cannot function. It is also highly recommended for security reasons that this IP address not be accessible by clients.
9. At the seventh prompt, enter the default route (default gateway). This is the default gateway address for the network.
10. At the eighth prompt, enter the DNS server. If you want to use more than one DNS server, it should be added in the config file.

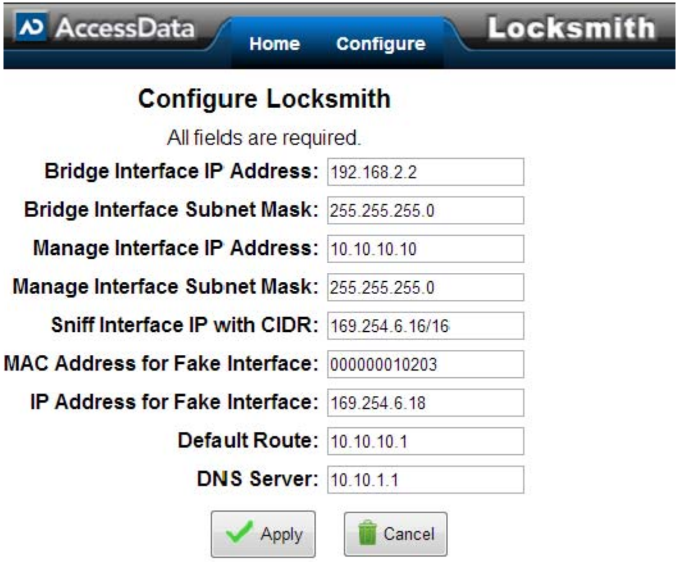
Configuring Resolution1 Locksmith By Web Interface

You can configure the Resolution1 Locksmith appliance through the website and by entering information in the fields provided.

To configure the appliance by using the web interface

1. Connect the Locksmith appliance to your network from one of the bottom two DHCP Ethernet ports in the appliance. See Installing the Appliance on page 7.
2. Turn on the server.
3. Once the server is running, open a web browser window. Internet Explorer is the recommended browser.
4. Go to https://<IP_Address>:4443/configure.html.
5. Enter the information in the fields. See Web Interface Configuration Screen Options on page 13.
6. Click Apply.

Resolution1 Locksmith Configuration Screen



Configure Locksmith

All fields are required.

Bridge Interface IP Address: 192.168.2.2

Bridge Interface Subnet Mask: 255.255.255.0

Manage Interface IP Address: 10.10.10.10

Manage Interface Subnet Mask: 255.255.255.0

Sniff Interface IP with CIDR: 169.254.6.16/16

MAC Address for Fake Interface: 000000010203

IP Address for Fake Interface: 169.254.6.18

Default Route: 10.10.10.1

DNS Server: 10.10.1.1

Web Interface Configuration Screen Options

The following are the options that you can enter in the web interface configuration screen.

Web Console Configuration Screen Options

Field	Description
Bridge Interface IP Address	Field where you enter the IP address for the bridged interface. Use dotted quad notation (For example, 1.1.1.1). This address needs to be routable on the network that the bridge is on and will be used as the source IP address for all proxied SSL connections.
Bridge Interface Subnet Mask	Field where you enter the subnet mask for the bridged interface.
Manage Interface IP Address	Field where you enter the IP address for remote access and the web management page. This address can be used to access the console with SSH, or access the web management page on port 4443. This address should not be on the same subnet as the Bridge Interface Subnet Mask. For security reasons, you should not allow clients to access this address.
Manage Interface Subnet Mask	Field where you enter the subnet for the manage interface. This subnet should be a different subnet mask than the Bridge Interface Subnet Mask.
Sniff Interface with CIDR	Field where you enter the IP and subnet information for the sniff interface. THis interface will send out all traffic decrypted that goes through the bridged interface. The default address is 169.254.6.16/16 . **Note: Make sure to use dotted quad with CIDR notation.**
MAC Address for Fake Interface	Field that lists the hardware address where ARP (Address Resolution Protocol) will send all traffic. The default is 000000010203. THis address will only need to be changed if there is a conflict.
IP Address For Fake Interface	Field that lists the IP address for the ARP. This is the destination address for all traffic that goes through the bridged interface. The default address is 169.254.6.18. You will only need to change this address if it conflicts with the sniff address or another address on the network.
Default Route	Field where you enter the default gateway address for the network.
DNS Server	Field where you enter the address for the DNS server.

Configuring Resolution1 Locksmith to Work with Your PKI

Resolution1 Locksmith relies upon a Public Key Infrastructure (PKI) for decrypting SSL. You need to configure AD

Locksmith to work with your existing PKI. Before restarting the appliance, you need to have three certificates:

- A management certificate
- A trusted CA resigning certificate
- An untrusted CA resigned certificate

The management certificate needs to be a web server certificate that is a base64 encoded X.509 certificate with the RSA private key unencrypted in the same file (password protection is not supported). The trusted and untrusted certificates need to be CA signing certificates that are also base64 encoded X.509 with an unencrypted RSA private key. The suggested key size for the signing certificates is 1024 bits. Higher bit keys will cause exponential CPU usage when resigning traffic.

Resolution1 Locksmith ships with self-signed certificates, and can generate self-signed certificates for proof of concept.

However, it is recommended that you acquire your own Certificate Authority and create certificates for this purpose. If you decide to use the certificate shipped with Resolution1 Locksmith, you will need to copy the following file to each client:

```
/opt/Resolution1Security/Locksmith/server.pem
```

Configuring Certificates

There are two ways to configure the certificates for Resolution1 Locksmith. The first way is to use the management web site. After the certificates have been uploaded, restart the Resolution1 Locksmith service. This will start resigning SSL traffic.

The second way to configure the certificates is in the command line of the appliance.

To configure the resigning certificates

1. Copy the trusted and untrusted certificate and key to the appliance.
2. Move the files to /opt/Resolution1Security/Locksmith .
3. Type **sudo vi /opt/Resolution1Security/Locksmith/config.json** .
4. On line 20 at the **ca-cert-key**, change **server.key** to the name private key file of the trusted root signing certificate.
5. On line 21 at the **untrusted-ca-cert-file**, change **untrusted.pem** to the name of the untrusted root signing certificate.
6. On line 27 at the **ca-cert-file**, change **server.pem** to the name of the trusted root signing certificate.
7. On line 29 at the **untrusted-ca-cert-key**, change **untrusted.key** to the name of the private key file of the untrusted root signing certificate.
8. Save the file.

Once Resolution1 Locksmith, restart the Resolution1 Locksmith service using `/etc/init.d/locksmith.restart` .

Important: Once Resolution1 Locksmith is started, SSL traffic will be decrypted and users will receive certificate errors on their browsers if the certificates have not been distributed. You may want to perform this test in a controlled (test) environment.