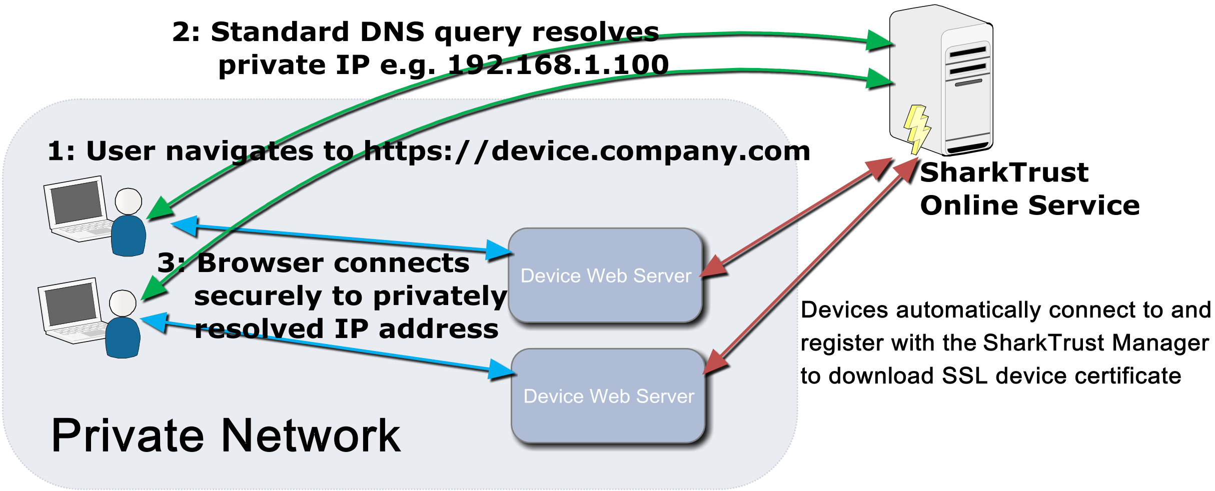
SharkTrust™ User Manual

This document uses the domain names *.realtimelogic.com for illustration purposes. The names must be changed to the domain name and name server names configured for your SharkTrust instance. See the SharkTrust Service Installation and Management document for details.

Introduction

In short, a device with an embedded web server is connected to a private network with Internet access. The device connects to the online SharkTrust service and downloads an SSL certificate for use with its internal web server. The SSL certificate downloaded by the device is signed for a domain name. To make sure the browser trusts the device, the online SharkTrust service also provides DNS services for the connected devices. As an example, a device may have the name "device" and the domain name may be "product.company.com". The fully qualified name for the device will then be **device.product.company.com** and a browser may navigate to the device's internal web server by navigating to **https://device.product.company.com**


2: Standard DNS query resolves
private IP e.g. 192.168.1.100
1: User navigates to https://device.company.com
SharkTrust
Online Service
3: Browser connects
securely to privately
resolved IP address
Device Web Server
Device Web Server
Devices automatically connect to and
register with the SharkTrust Manager
to download SSL device certificate
Private Network

The SharkTrust service groups a set of devices into a group called a zone. Each zone registered with the SharkTrust service is a domain name and each domain name may be used by multiple end customers.

A zone used by multiple end customers must be managed by the device manufacturer. A device manufacturer may also let the end customers register and manage their own zones. This feature is particularly useful for larger end customers that may have many devices running on their Intranet(s).

Adding a New Zone

In the following examples, we use the domain name defibrillator.tk, a domain name we registered for the purpose of showing how a product may use a product specific domain name.

A new zone is created by first setting the zone's (sub) domain name's nameservers to the two following addresses:

- NS1.REALTIMELOGIC.COM
- NS2.REALTIMELOGIC.COM

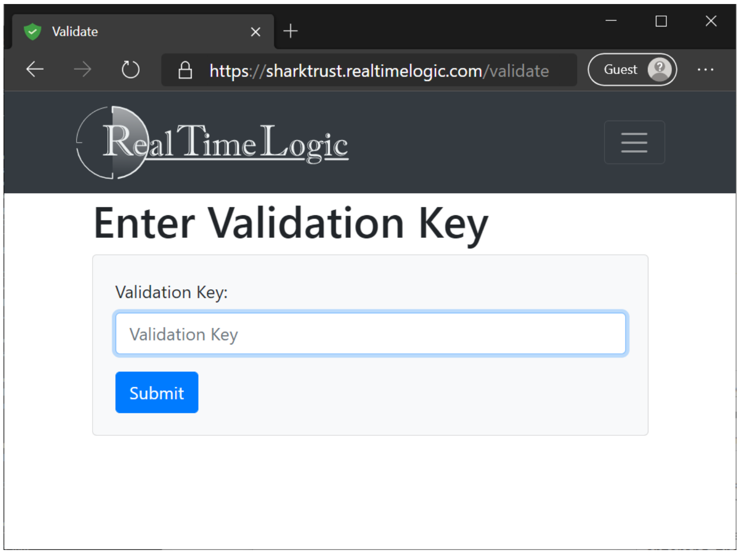
You may proceed to the second step when running a whois command for the zone's (sub) domain name returns the new nameserver names.

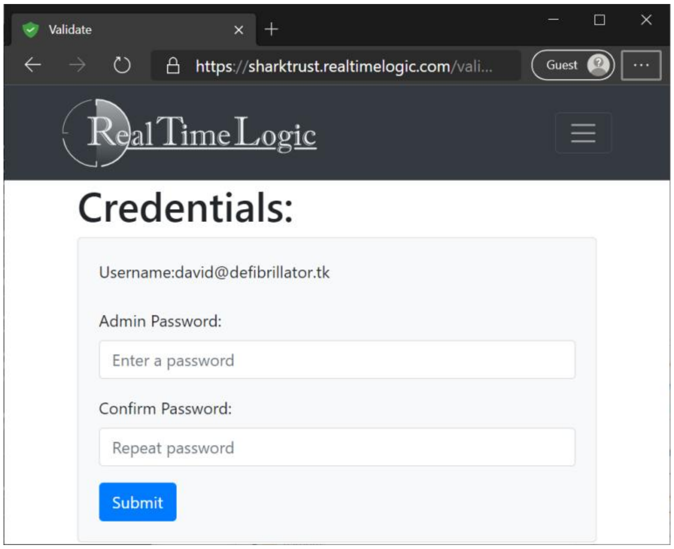
The following example shows how to run whois on the command line and the result produced by the command. You may also use any online whois service.

```
$ whois defibrillator.tk

   Domain name:
      DEFIBRILLATOR.TK

   Domain Nameservers:
      NS1.REALTIMELOGIC.COM
      NS2.REALTIMELOGIC.COM
```

Navigate to https://sharktrust.realtimelogic.com when the whois command is able to resolve the new name servers. Enter the domain name and your email address. Click the submit button and wait for the SharkTrust registration email.

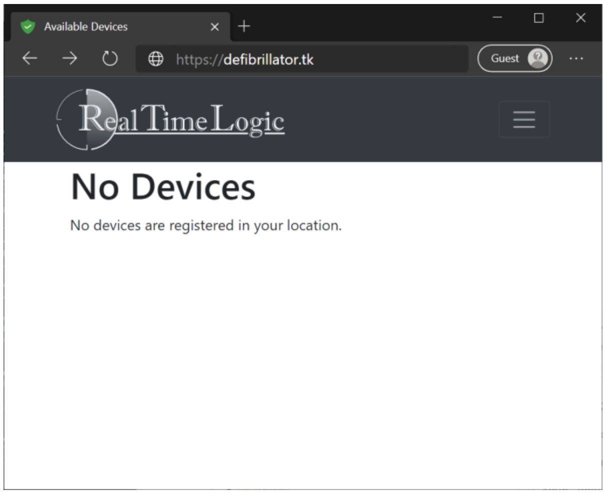
When you receive the registration email, click on the registration link, copy, and paste the registration key from the email into the online form as shown in the left screenshot below. Click the submit button and proceed to creating the zone's administrator account as shown in the right screenshot below.





Username:david@defibrillator.tk

After registering and setting the zone password, the zone administrator will receive an email when the new zone is ready -- in other words, when the DNS has been configured for the (sub) domain name and an SSL certificate has been installed for the new online zone service. Clicking the link in the email takes the zone administrator to the public DNS information page.



No Devices

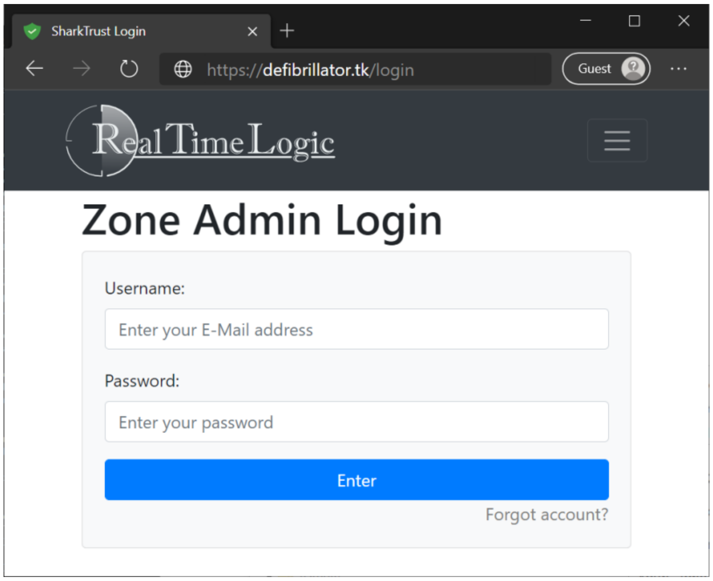
No devices are registered in your location.

In the left screenshot, notice that the new domain name defibrillator.tk is now managed by the same online SharkTrust service.

The public DNS information page shows devices registered for the users local network. The administrator can also login and navigate back to the DNS information page to view all registered devices for all network locations. The list is initially empty since no devices have been registered.

Registering Devices

Each zone registered with the SharkTrust service has its own secret zone key. This zone key can either be embedded in the device software or be user configurable. The zone key must be user configurable for device products that let the end customer create his own zone. We recommend that you initially test connecting a device to Real Time Logic's SharkTrust test server https://sharktrust.realtimelogic.com/ as explained in the C Source Code Example. You may use the same C Source Code Example for connecting to your own SharkTrust instance.



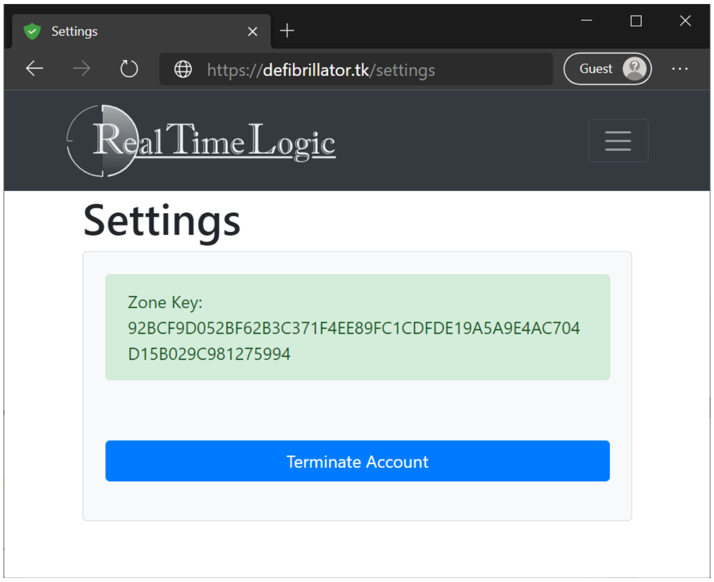
Zone Admin Login

Username:

Enter your E-Mail address

Password:

Enter your password

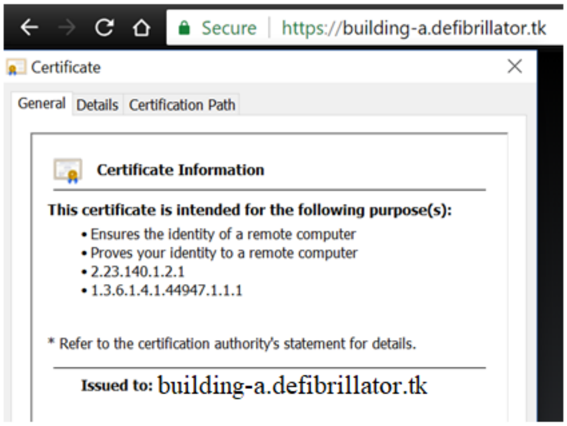


Settings

Zone Key:
92BCF9D052BF62B3C371F4EE89FC1CDFDE19A5A9E4AC704D15B029C981275994

See the C Source Code Example and the SharkTrust Protocol Specification for information on how to use the zone key in a device and for information on how to name devices -- i.e set sub-domain name for devices. The following screenshot shows a user navigating to a device running on a private network.

SharkTrust™ User Manual



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 2.23.140.1.2.1
- 1.3.6.1.4.1.44947.1.1.1

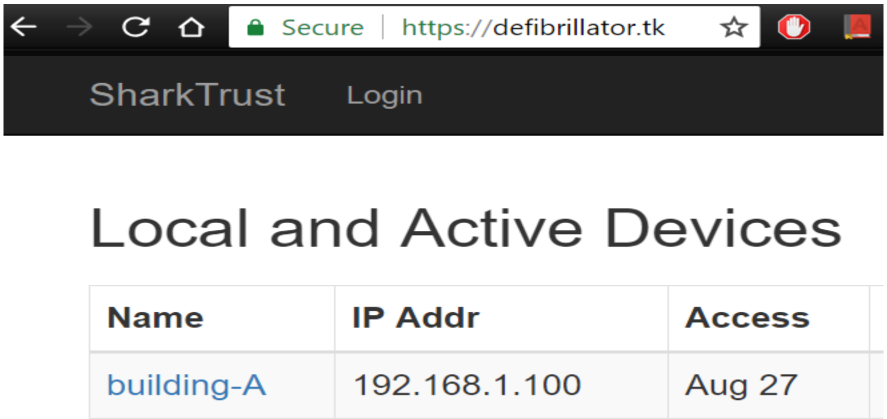
* Refer to the certification authority's statement for details.

Issued to: building-a.defibrillator.tk

In the screenshot to the left, the device is named "building-a" and the Fully Qualified Domain Name (FQDN), which is the device name + zone name, is building-a.defibrillator.tk.

The device's FQDN resolves to the device's private IP address -- the Intranet IP address. The zone domain name defibrillator.tk resolves to the online SharkTrust server's IP address.

Any (non authenticated) person may navigate to the domain name https://defibrillator.tk to get a list of local devices. The person must be within the same network as the devices. Only devices on the same network are listed unless the user is authenticated as the administrator.

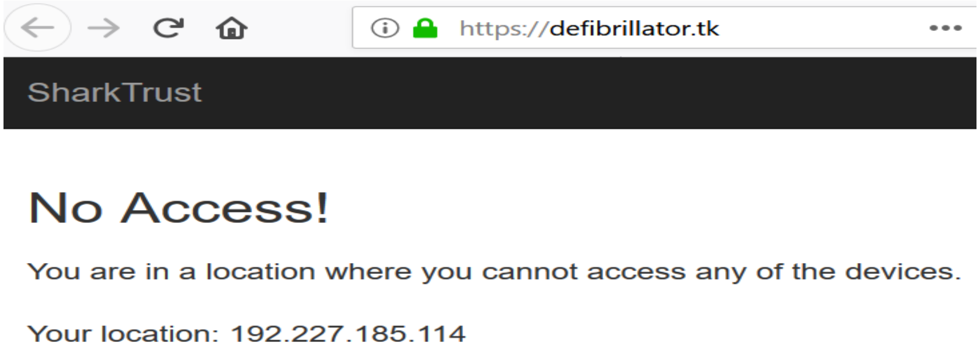


Local and Active Devices

Name	IP Addr	Access
building-A	192.168.1.100	Aug 27

Showing devices that only belong to the network prevents other customers that are using the same domain name from viewing devices not part of their realm. It also prevents users from attempting to navigate to a device that will not respond. Although the DNS name is global and public, the resolved IP address belongs to a private network and can only be accessed from within the same network.

The following figure shows a person visiting from outside the network:



No Access!

You are in a location where you cannot access any of the devices.

Your location: 192.227.185.114