



## **System Administration Manual**

Secure Connection as a Service



August 2019

© Copyright 2019 Blacksands, Inc. All rights reserved. Contents and terms are subject to change by Blacksands without prior notice. Reproduction or transmission of this publication is encouraged.

### **Trademarks**

Copyright© 2019 Blacksands, Inc. All rights reserved. Blacksands® and certain other marks are registered trademarks of Blacksands, Inc., in the U.S. and other jurisdictions, and other Blacksands names herein may also be registered and/ or common law trademarks of Blacksands. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Blacksands, and Blacksands disclaims all warranties, whether express or implied, except to the extent Blacksands enters a binding written contract, signed by Blacksands General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Blacksands. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Blacksands internal lab tests. In no event does Blacksands make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Blacksands disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Blacksands reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

You can report errors or omissions in this or any Blacksands technical document to [techdoc@blacksandsinc.com](mailto:techdoc@blacksandsinc.com).



1. Introduction	5
1.1. Basic Architecture	5
1.2. Introduction of Roles	7
1.3. Introduction to the Blacksands Virtual Receiver	9
2. User Access	10
2.1. User Certificate Management	10
2.2. New User Registration	11
2.2.1. Windows Certificate Installation	12
2.2.2. OSX Certificate Installation	15
2.3. Authentication, Authorization, and Routing	16
2.3.1. User / Device Authentication	18
2.3.2. User / Device Authorization	19
2.3.3. User / Device Routing	20
2.3.4. User / Device Heartbeat	20
3. Blacksands Manager	21
3.1. Accessing the Blacksands Manager	21
3.2. Managing Services	22
3.2.1. Creating a New Service	22
3.2.1.1. Creating a New KVM (Remote Desktop) Service	25
3.2.1.2. Setting up the Target PC for Blacksands Remote Connection	26
3.2.2. Managing Services	31
3.2.2.1. Enabling / Disabling a Service	31
3.2.2.2. Modifying a Service	32
3.2.2.3. Deleting a Service	33
3.3. Managing Users	34
3.3.1. Creating a New User	34
3.3.2. Modifying a User	36
3.3.3. Deleting a User / Device	37
3.3.4. Adding a User / Device to a Service	38
3.3.5. Adding a Stakeholder to Service	39
4. Deploying Blacksands Virtual Receiver	42



4.1.Virtual Receiver Requirements	42
4.2.Downloading Virtual Receiver	44
4.3.VMWare ESXi 6.5.0 Example	45
4.4.Registering the Blacksands Virtual Receiver	46
4.4.1.Accessing bsuser Tools	48
4.4.2.Setting up Networking	48
4.4.3.Restarting Virtual Receiver	49
4.4.4.Viewing Network Adapters	49
4.4.5.Registering a Virtual Receiver	49
4.4.5.1. Starting the Registration Process	49
4.4.5.2. Setting Emails for the Registration Process	50
5. Event Logs	52
5.1.Overview	52
5.2.Definitions	52
5.3.Explanation	52



## 1. Introduction

Blacksands is a revolutionary connectivity solution, providing unparalleled security and flexibility for today's dynamic organizational requirements without the massive overhead of traditional ad-hoc systems. Blacksands Secure Connection as a Service (SCaaS) provides unparalleled security and flexibility in an incredibly user friendly interface.

This introduction will describe the simple installation, deployment, and management of Blacksands Secure Connection as a Service (SCaaS). Blacksands solution offers an Invisible Edge, Unique User/Device Certificates, a Simple Management Interface, and Dynamic Point-to-Point Connections.

Blacksands is OS and device agnostic, meaning it can run on most operating systems and devices.

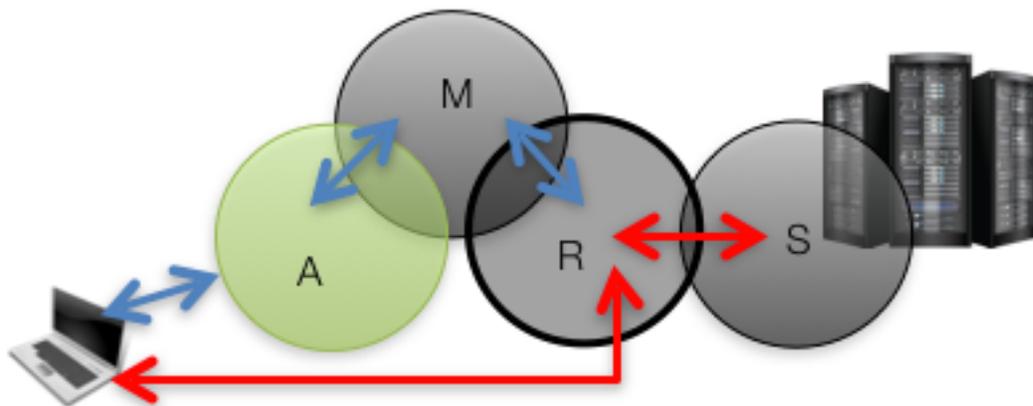
Blacksands is compatible with Google's Chrome browser, Microsoft Explorer and Firefox.

### 1.1. Basic Architecture

Blacksands proprietary 'Separation of Powers Architecture' provides unparalleled security, scalability, flexibility, and is simple to use.

1. **Authorizer** - forward facing identification system
2. **Manager** - invisible, external cloud management system
3. **Receiver** - invisible, software edge device and gateway (Virtual Receiver)
4. **Certificates** - unique industry standard certificates for every user device

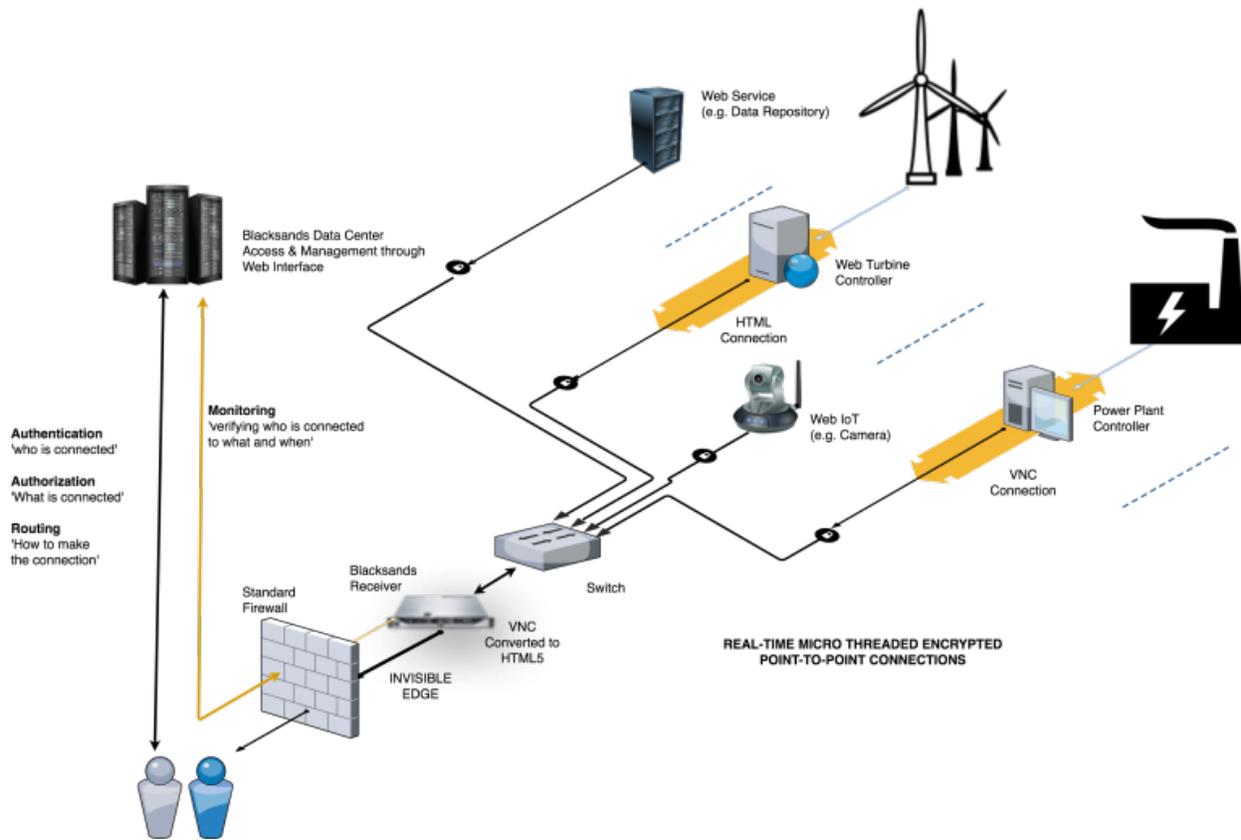
Blacksands proprietary, 'Separation of Powers' architecture is designed to invert the typical internet connectivity process. Instead of the standard Trust but Verify process where one connects to the entire internet and then attempts to filter out malicious or illegitimate traffic, Blacksands, prior to making any network connection at the edge, dynamically authenticates, authorizes, and provides point-to-point routing through its external management architecture to pre-defined services (PCs, Applications, IoT Devices).



**STEP 1** A secure connection begins when a user establishes an encrypted session to a Blacksands Authorizer (A). The Authorizer's job is to identify the users, maintain a connection heart-beat, provide routing information for selected services from the Manager (M). The user is identified using two-factor authentication (unique certificate and password). Neither the password nor a hash of the password is ever passed over the internet. Once a user is identified, the user is provided a list of authorized services.

**STEP 2** When the user selects a particular service through the Authorizer (A), the Manager (M) sets up the point-to-point connection. The Blacksands Virtual Receiver (R) is dynamically set to receive a new session from a particular user, with a specific certificate, at a specific IP address and route the session to a particular service on the back end. Simultaneously, the user is provided the route to the particular Virtual Receiver, providing an encrypted, point-to-point connection.

**STEP 3** The user's new point-to-point connection is made to the Virtual Receiver (R). The user again passes their unique certificate to the Virtual Receiver (R) front end. The Virtual Receiver proxies the new connection to a particular Service (S) at a specific IP address and port.



## 1.2. Introduction of Roles

**Blacksands has three basic roles:**

- **Administrators** – global visibility and control of the organization’s Blacksands system
- **Stakeholders** – local management of pre-determined services and user access to those services
- **Users** – simple, secure access to authorized services

Both Administrators and Stakeholders have access to the Blacksands Manager. Administrators have global visibility and control over all Users, Virtual Receivers, and Services within their organizational unit. Stakeholders have local management over User access to particular Services where they have been granted Stakeholder rights.



Administrators can create new Users by providing a few pieces of information including the User's email address. Once created, the new User will receive an email with instructions to create his/her Blacksands Certificate. (above)

Administrators can create new Services by providing basic networking information and a Blacksands provided FQDN. Each Service is provided its own, unique, obfuscated FQDN (automated Blacksands process) and requires a routable IP and Port.

Administrators can add and remove Stakeholders to specific Services on an individual basis. The Stakeholder will only be able to see and modify attributes of that particular Service, primarily User access.

Administrators and Stakeholders can add and remove Users to a Service. While Administrators can manage all Services, the Stakeholder can only see/manage his/her particular assigned Service/s.



### 1.3. Introduction to the Blacksands Virtual Receiver

The Blacksands Virtual Receiver provides unparalleled security, control, and flexibility.

#### **TOTAL CONTROL OF THE EDGE:**

- Blacksands creates invisible private networks providing a drastically reduced threat vector for critical infrastructure
- Blacksands dynamic Authentication, Authorization, and Routing allow real-time session control and network architecture
- Blacksands dynamically creates and manages unique, point-to-point, encrypted connections without exposing anything else on the host network, controlling the traffic from OSI layers 3-7
- Blacksands can be combined with existing tools to form a cohesive and comprehensive tactical network defense plan

Blacksands focuses on networks, endpoints, applications, and data. It can be deployed to provide secure connection for web based applications and devices, as well as PCs (view only or full control). Typical endpoints include - robotics controllers, file repositories, web cameras, and productivity management systems.

#### **TYPICAL DEPLOYMENT**

- Virtual Receiver (Virtual Machine) deployed behind standard firewall
- Blacksands SCaaS (Secure Connection as a Service) includes external Management, including dynamic authentication, authorization, and routing
- Integration into existing internally TCP/IP networked architecture using internal IP or internal DNS
- Human connection through user friendly web based interface
- Application connection control through simple API
- Optional Internal Authorizer for LAN SCaaS



## 2. User Access

### 2.1. User Certificate Management

Blacksands uses Certificates for a number of critical operations, first and foremost, for identification of the person or application initiating the connection. Blacksands uses high-end industry standard certificates which are managed in Blacksands own certificate authority.

#### USAGE

The initial connection process with the Authorizer at <https://client.blacksandsecurity.com> utilizes a dual certificate based authentication process where both the site and the user must share and accept one another's Certificates.

The same User Certificate that is passed in the initial authentication process is used for every new Service connection. This means that each time a new service is opened the Virtual Receiver requests the User to pass their Certificate again.

Blacksands issues unique Certificates for each User device that will be connecting to a given Service. That means that a specific User may have multiple devices (i.e. laptop, work desktop, tablet device...) each with a unique Blacksands Certificate. This provides the company with the ability to efficiently and securely manage multiple User devices including BYOD.

The Blacksands User Certificate lives within a Blacksands Certificate chain. Industry best practices require the three public certificates :

- [blacksands\\_inc\\_ca\\_root.crt](#)
- [blacksands\\_inc\\_ca.crt](#)
- [blacksands\\_ca\\_l3.crt](#)

Each of the above certificates must be installed prior to the User Certificate.

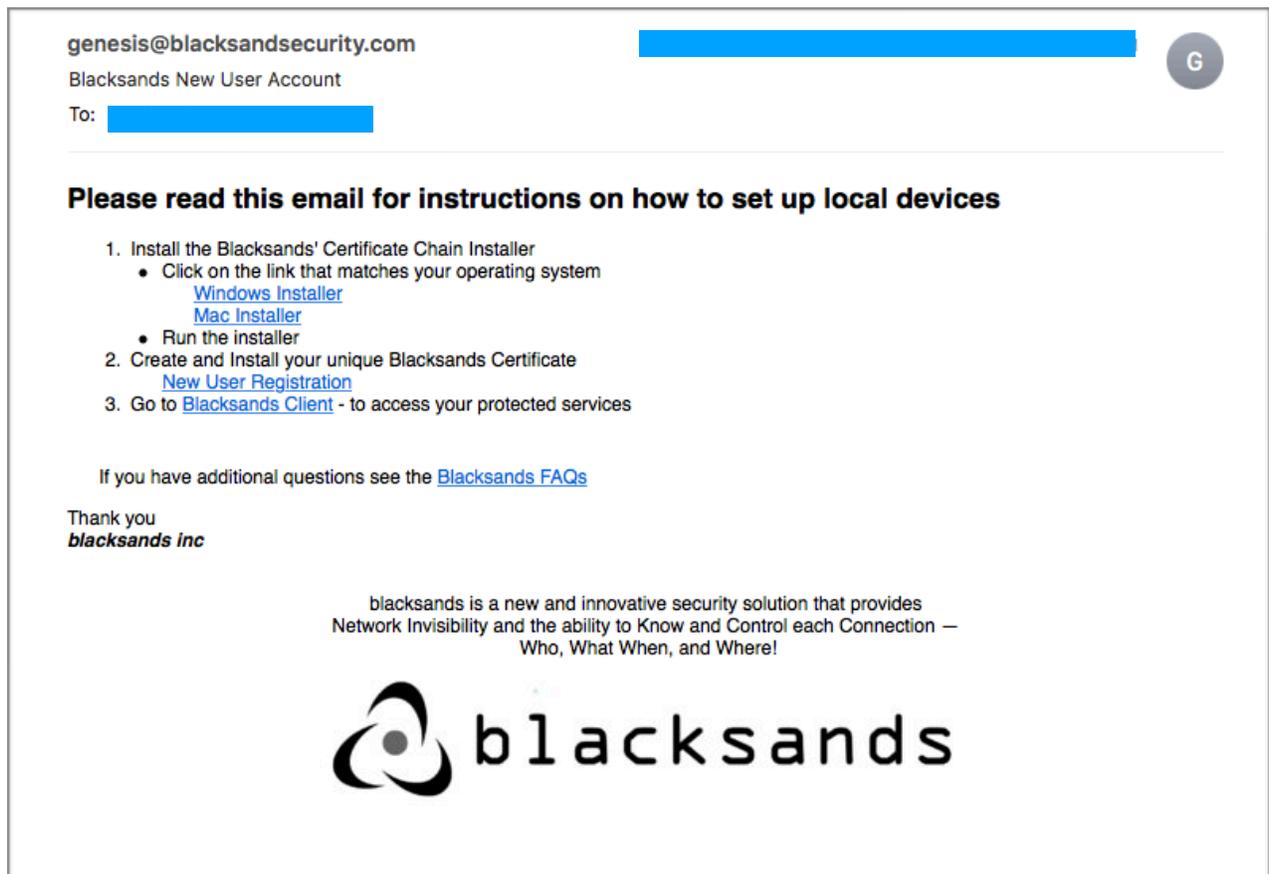


## 2.2. New User Registration

A new Blacksands User will receive an email invitation. This email has basic instructions and links to the required Blacksands Certificate Creation and Installation functions.

### IMPORTANT:

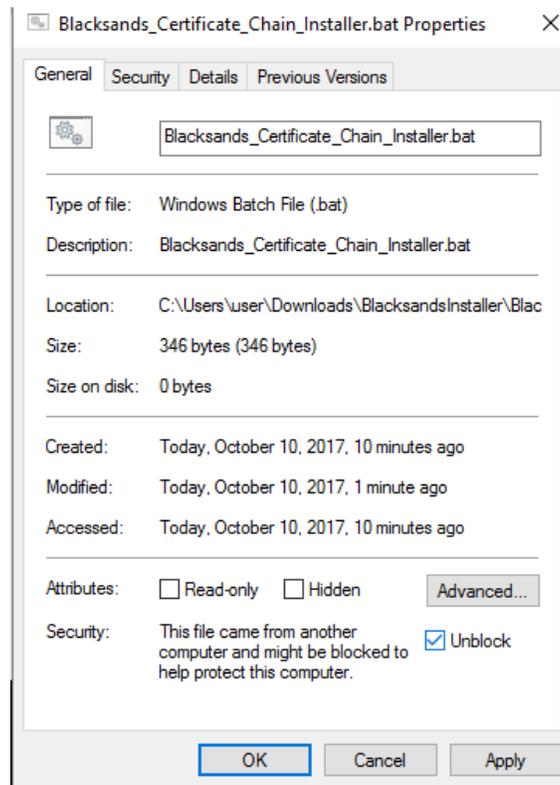
It is important to note that the 'New User Registration' link is a one time use only link and is available for 72 hours. Therefore, the email must be opened on the appropriate device that will be used to access the Blacksands protected service/s.



Blacksands New User Account Email

## 2.2.1. Windows Certificate Installation

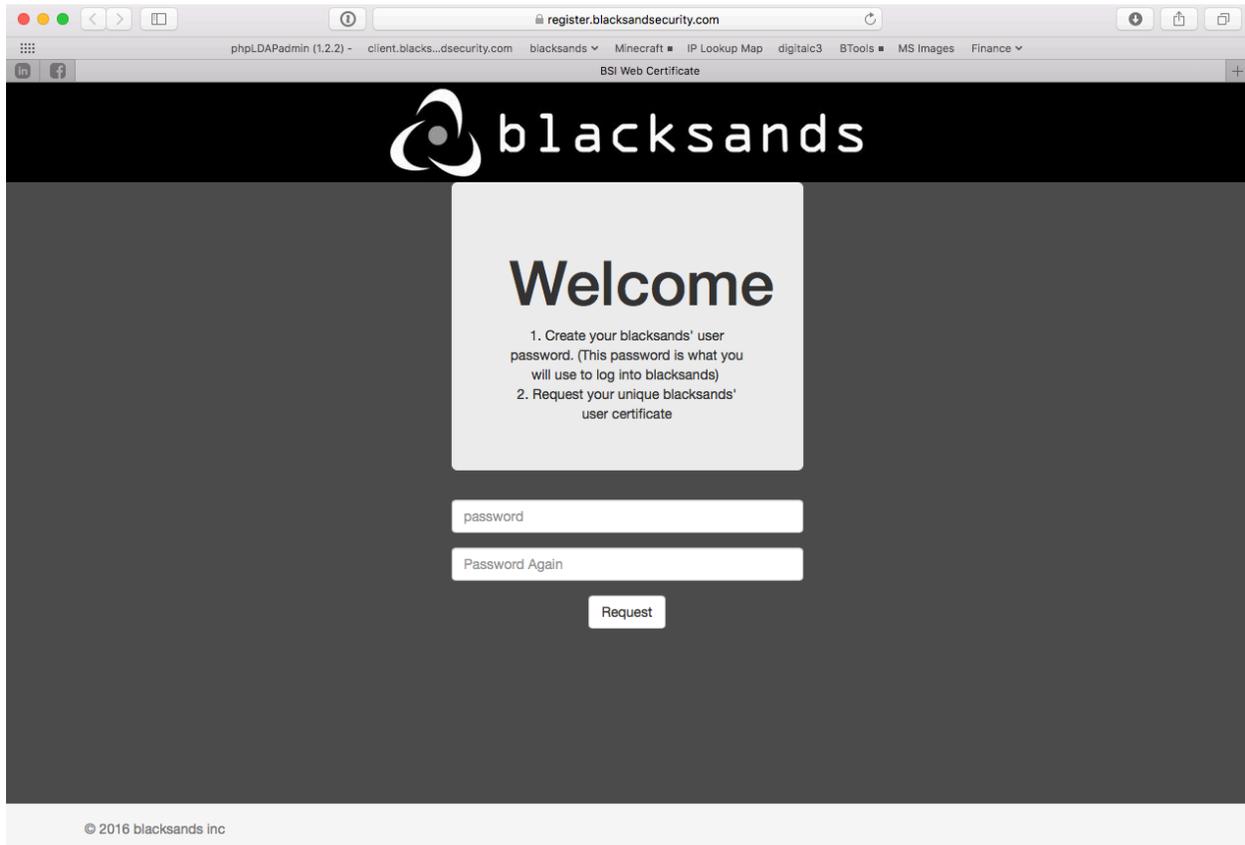
- I. The User downloads the appropriate Installer (Windows) and installs the Blacksands Certificate Chain. (Blacksands New User Account Email)
  - I.A. Often the User will need to 'Unblock' the Blacksands Certificate Chain Installer.exe file in order to run it. (This is because the Blacksands Certificates are not yet installed on their device)
  - I.B. Right Click on the file
  - I.C. Click 'Unblock'



- I.D. Click 'OK'
- II. Run the Installer
- III. The User clicks on the "New User Registration" link (Blacksands New User Account Email) and generates their unique Certificate.



III.A.The default browser will go to <https://register.blacksandsecurity.com>

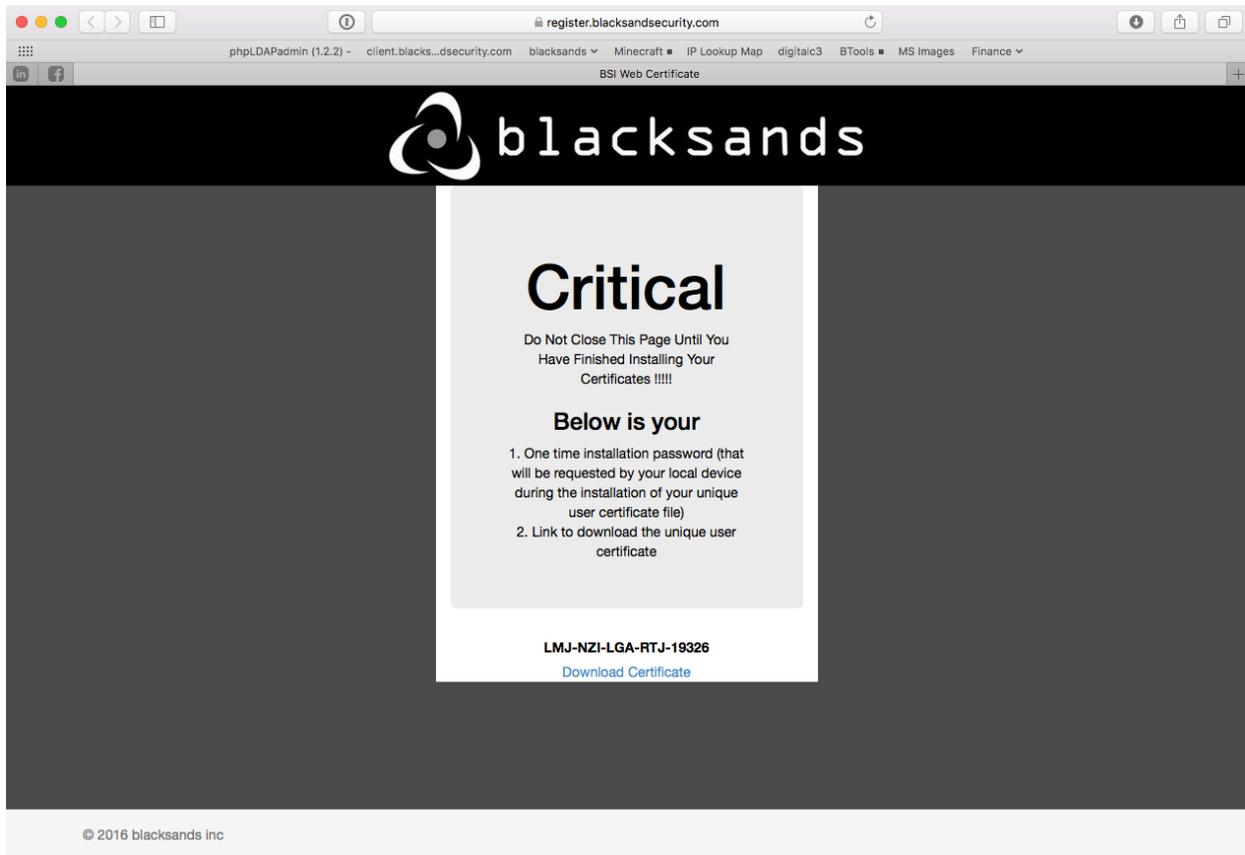


III.B.The User inputs their new Blacksands Password (twice)

III.C.Blacksands generates their unique User Certificate

III.D.The User downloads the Certificate

III.E.DO NOT CLOSE THE WINDOW – as it has the **Installation Key**



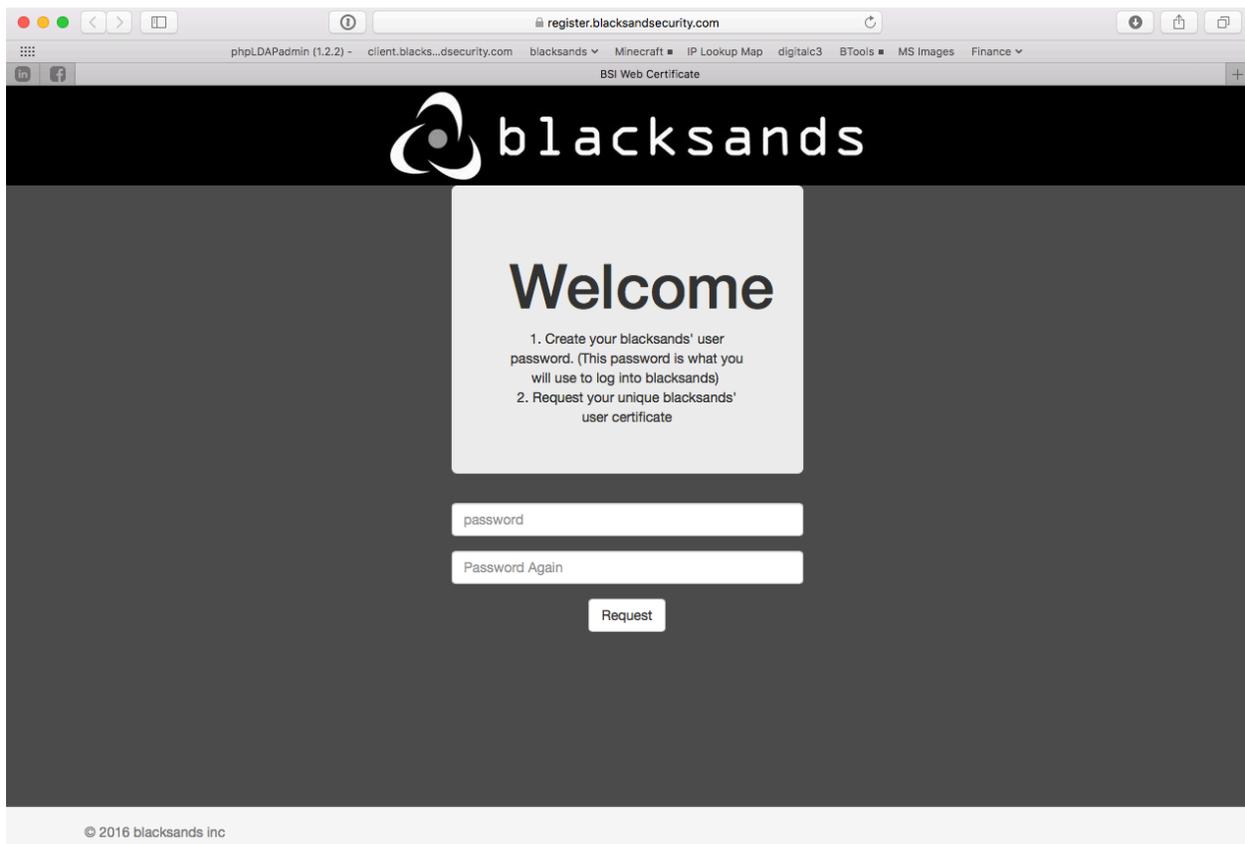
- IV. The User double clicks the downloaded Certificate.
- V. The OS will ask for the Password. This is the Installation Key in the above window. This is the only time the Installation Key is used.
  - V.A.The User inputs the Installation Key and installs their unique Certificate on their device.



## 2.2.2. OSX Certificate Installation

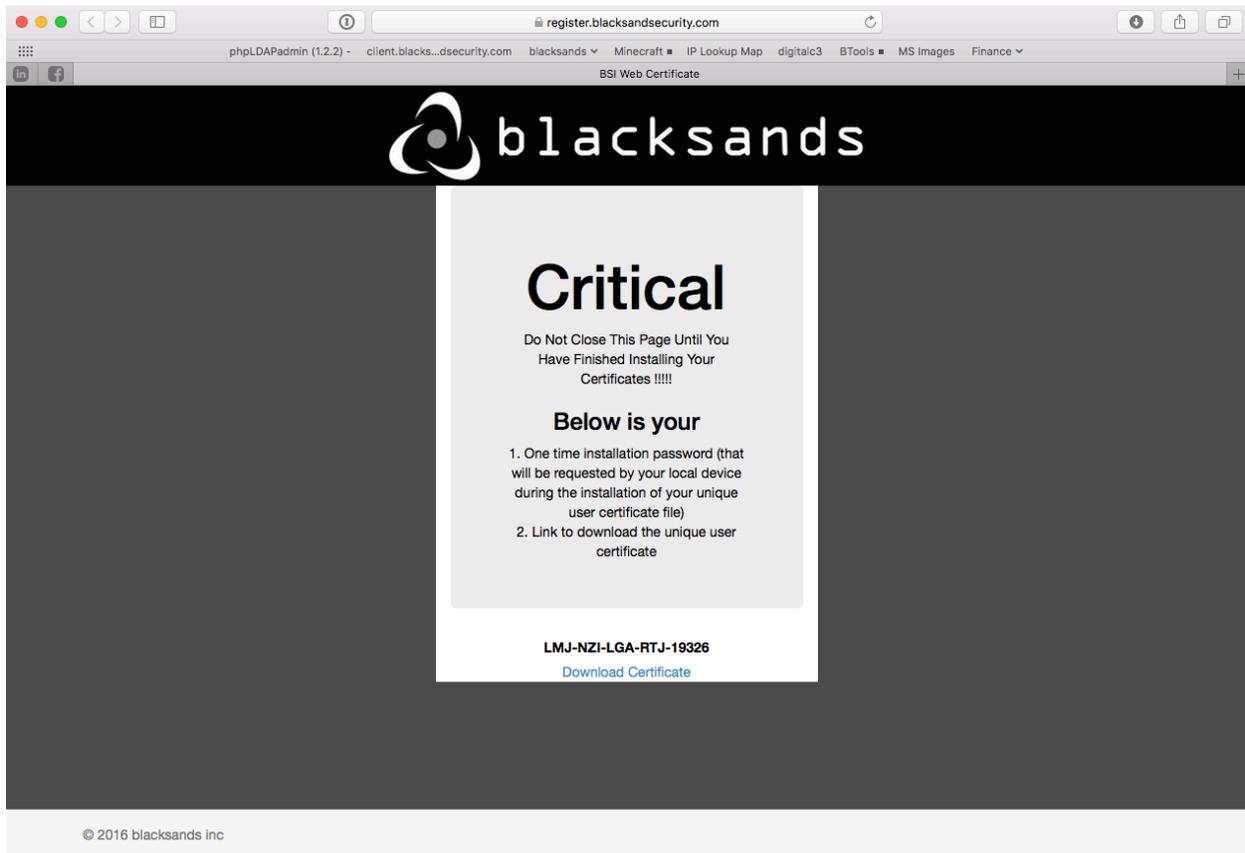
Installing Blacksands Certificate chain and unique Certificate:

- I. Download the Mac Installer from the email or <https://github.com/blacksandsinc/osx/blob/master/Blacksands.dmg>
- II. Double click the Blacksands.dmg file. (you may have to allow this in the Mac security settings)
- III. The User clicks on the "New User Registration" link (Blacksands New User Account Email) and generates their unique Certificate.
- IV. The default browser will go to <https://register.blacksandsecurity.com>

A screenshot of a web browser showing the registration page for Blacksands. The browser's address bar displays "register.blacksandsecurity.com". The page has a dark header with the Blacksands logo and name. The main content area is dark gray with a white box containing the text "Welcome" and two numbered instructions: "1. Create your blacksands' user password. (This password is what you will use to log into blacksands)" and "2. Request your unique blacksands' user certificate". Below the instructions are two input fields labeled "password" and "Password Again", and a "Request" button. The footer of the page shows "© 2016 blacksands inc".

- IV.A. The User inputs their new Blacksands Password (twice)
- IV.B. Blacksands generates their unique User Certificate
- IV.C. The User downloads the Certificate

IV.D. DO NOT CLOSE THE WINDOW – as it has the **Installation Key**



- V. The User double clicks the downloaded Certificate.
- VI. The OS will ask for the Password. This is the Installation Key in the above window. This is the only time the Installation Key is used.
  - VI.A. The User inputs the Installation Key and installs their unique Certificate on their device.

## 2.3. Authentication, Authorization, and Routing

To access any Blacksands protected Service a User must first be Authenticated, Authorized, and then Routed. This process is unique to Blacksands and attempting to access a Blacksands protected Service in any other way is not possible.

The process is quite simple. A legitimate User with an installed Blacksands Certificate on the device they are using, proceeds to a Blacksands Authorizer (<https://client.blacksandsecurity.com>), provides his/her Certificate, Password, and then selects the protected Service desired. A new window will be opened in the User's browser,



and a point-to-point encrypted connection is established from the User's device to the protected Service.

**Three Requirements:**

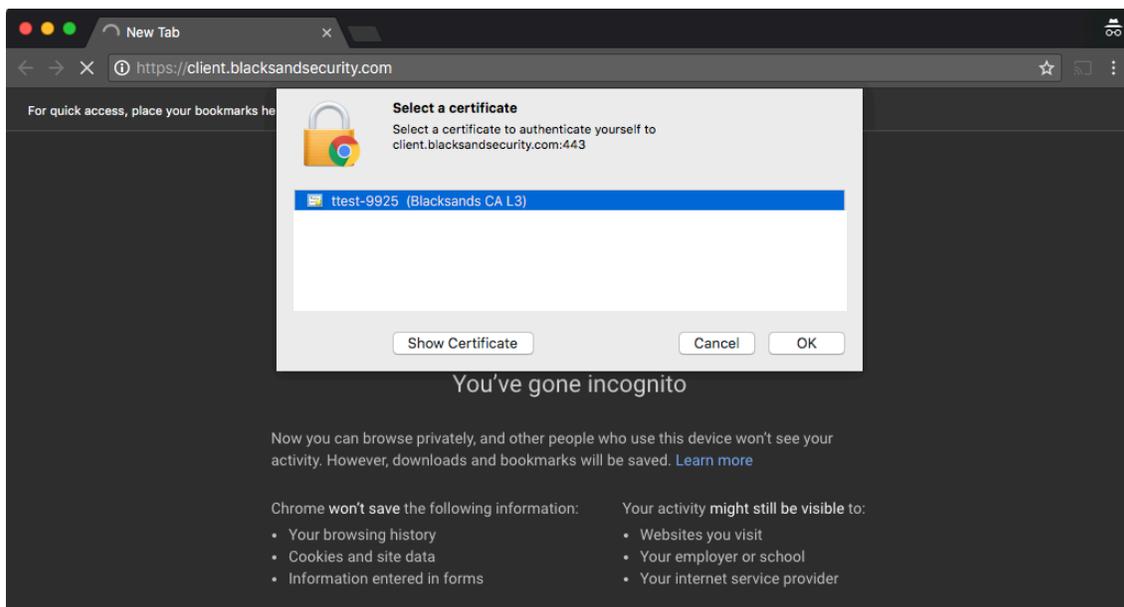
- The User must have a legitimate Blacksands Certificate already installed on the connecting device.
- The User must use a supported Blacksands OS and browser.
- The User device must have an internet connection that is able to access the Blacksands Authorizer and Virtual Receivers.



### 2.3.1. User / Device Authentication

Blacksands authenticates Users utilizing multi-factor authentication. The two-factors used are - something you have (Certificate) and something you know (Password).

The User proceeds to <https://client.blacksandsecurity.com>. Before any information is returned to the User's browser, Blacksands will request the unique User Certificate.



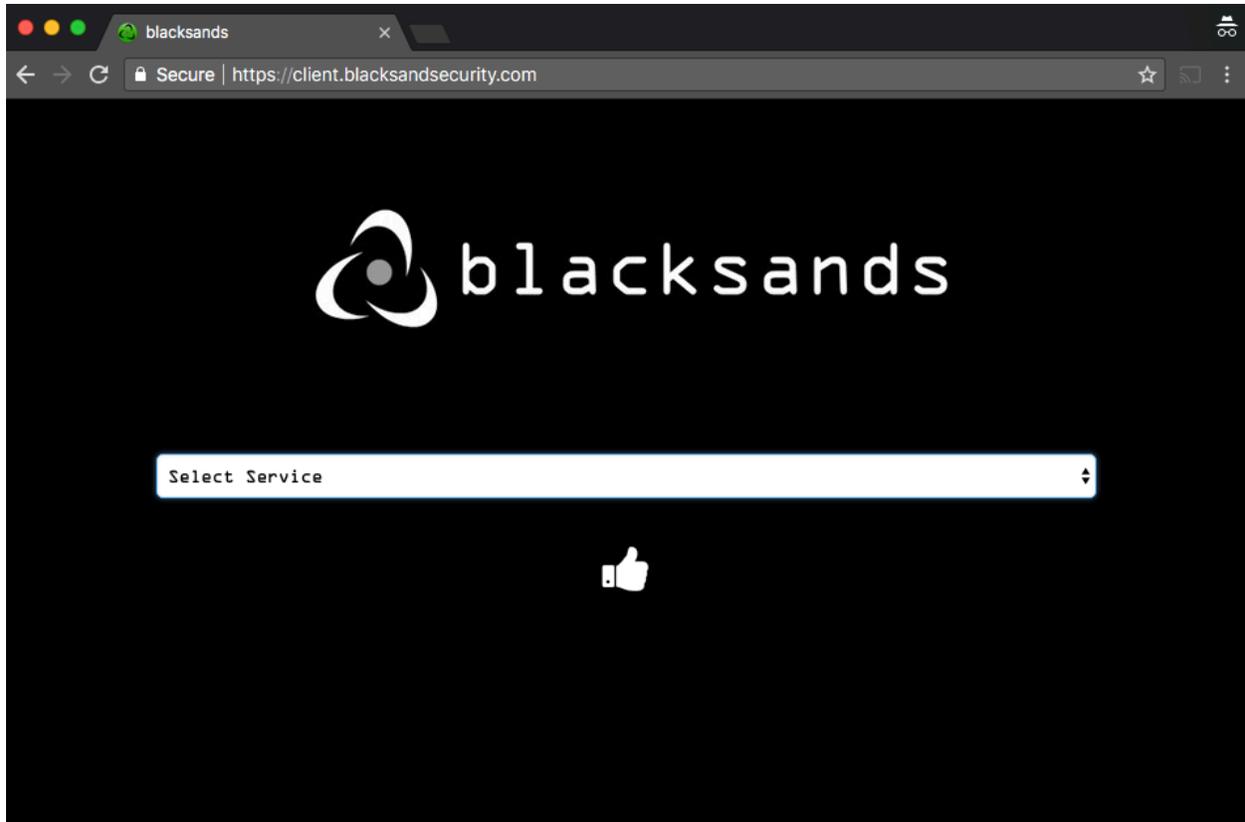
When the User provides a legitimate Blacksands Certificate, Blacksands verifies the User's identity by requesting the User's Password.





The Blacksands Authorizer provides 120 seconds for password verification. If the legitimate password is not provided in that window the session ends and the browser must be refreshed to begin again.

When a legitimate password is provided Blacksands populates the browser with the User's specific available Services in a drop-down menu. The User is able to highlight a Service and select the Thumbs Up to proceed to that service.



### 2.3.2. User / Device Authorization

Users are never provided an option for any Service that he/she has not been given permission to access. Therefore, only legitimate Services are listed in the drop-down list. When a pre-Authorized Service is selected and the Thumbs Up button activated, the Blacksands system Authorizes the User to access the protected Service through its particular Virtual Receiver.

Because each User device has a unique Blacksands Certificate, administrators and stakeholders can vary the Service Authorization based on device specific Certificates.



For instance, policy and governance can be upheld by administrators / stakeholders, in that they may only allow work PCs to access particular sensitive work applications, but home PCs can be permitted to access less sensitive applications.

### 2.3.3. User / Device Routing

After the Service is selected, a new window or tab opens in the Users' browser. It is automatically populated with the specific, obfuscated, Blacksands DNS entry associated with the given Service.

When the browser reaches the Virtual Receiver, behind which the service resides, the Virtual Receiver verifies the identity of the User, once again, by requesting the User's Certificate.

After the Certificate is provided, the Virtual Receiver routes the User to the protected Service and sandboxes the User into that specific, single session.

### 2.3.4. User / Device Heartbeat

The User must leave the original browser window / tab open while accessing the Blacksands protected Service/s. As a security measure, in the backgrounds, Blacksands maintains a 'heartbeat'. This 'heartbeat' continually verifies the User's identity and sessions. If, for any reason (hacker, loss of internet connection, computer problems), the heartbeat is interrupted, all of the User's connections to Blacksands protected Services are instantly severed.

In order to reestablish, a connection, the User must restart the process over from the beginning.



### 3. Blacksands Manager

#### 3.1. Accessing the Blacksands Manager

To Access the Blacksands Manager, a User must be either an Administrator or a Stakeholder (See Section 1.2). If the User has either of these Roles, then after the User is Authorized by the Blacksands System (See Section 2.3.2 ), the User will find the service 'Blacksands Admin Panel' in his/her drop down list. The User selects this



Service and the Thumbs Up Button.

A new window will open and request the User Certificate again. (Certificate Verification occurs for every new Service Connection)

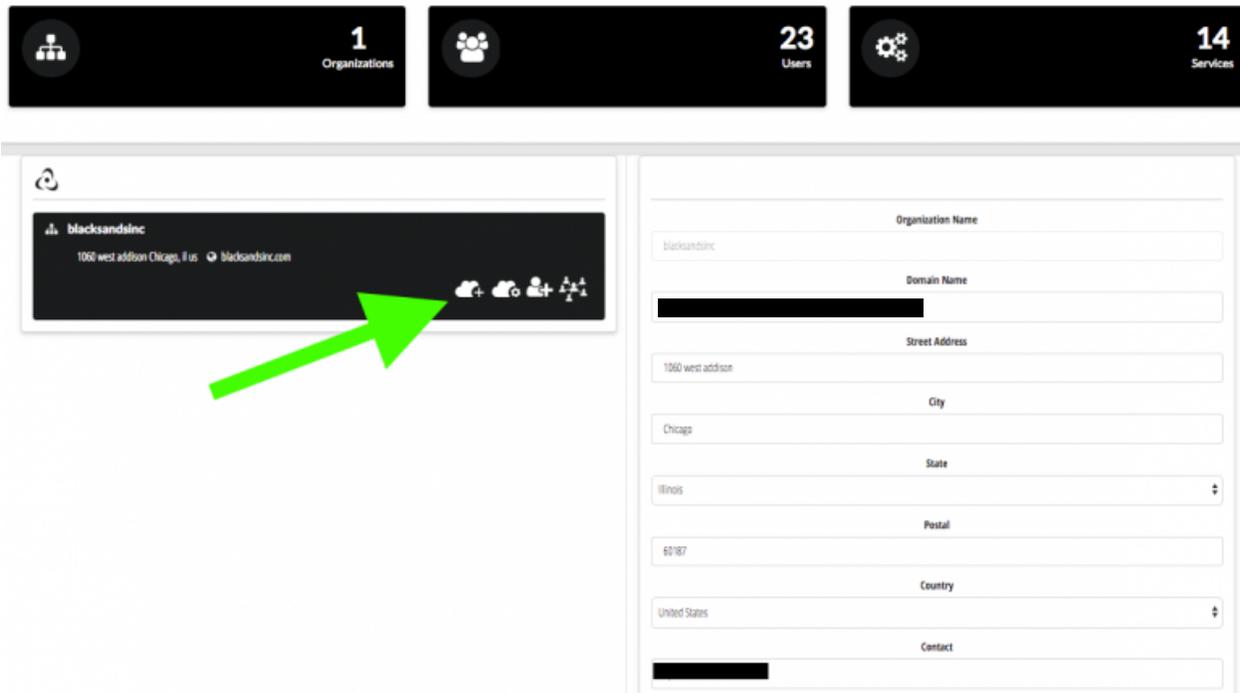
A screenshot of the organization details form. The form fields are: Organization Name (blacksandsinc), Domain Name (redacted), Street Address (1000 west addition), City (Chicago), State (Illinois), Postal (60187), Country (United States), and Contact (redacted).

## 3.2. Managing Services

### 3.2.1. Creating a New Service

A Service can be an HTML Application, PC, or HTML IoT device.

The Service is set up by selecting the Create New Service Icon. (Cloud with the + )



The screenshot displays the Blacksands management interface. At the top, there are three navigation cards: 'Organizations' with a count of 1, 'Users' with a count of 23, and 'Services' with a count of 14. Below these cards is a list of organizations. The first organization, 'blacksandsinc', is highlighted. A green arrow points to the 'Create New Service' icon (a cloud with a plus sign) located in the bottom right corner of the organization card. To the right of the organization list is a form for creating a new service, with fields for Organization Name, Domain Name, Street Address, City, State, Postal, Country, and Contact.

Field	Value
Organization Name	blacksandsinc
Domain Name	[Redacted]
Street Address	1000 west addison
City	Chicago
State	Illinois
Postal	60187
Country	United States
Contact	[Redacted]



In the right panel are four (4) fields that are used to establish the Service connection.

- **Service Name** - is the common name for the service (e.g. CRM, Robot 4, PC1 in Lab1) This is the name that will appear in the drop down list for the User after authentication.
- **Description** - is an added field for management to add additional information about the Service.
- **Up Stream Server** - is the IP or internal FQDN and Port of the Service. (e.g. 10.10.20.100:21 or abcd.mydomain.com:21)
- **Virtual Receiver Address** - is the external IP address that is routed to the Blacksands Virtual Receiver. Most enterprise environments will have the Virtual Receiver behind a firewall with an internal IP address and will forward the external IP to the internal IP address. This field is NOT the internal IP, but rather the external IP address that the FQDN will use in conjunction with DNS.
- **Thumbs Up** - After all fields are completed... click thumbs up to initialize/establish the Service

**Service Name**

**Description**

**Up Stream Server**

**Receiver Address**



Once the Service is created the right hand window adds a few fields.

**FQDN** - Blacksands creates, through an automated process, and registers an obfuscated DNS entry for each Service that is created.

**URI** - a URI is sometimes required for certain applications. This is application specific and not always required.

**Service Status** - is a field that appears after initialization which allows an Administrator to Enable or Disable a Service from one place. Disabling a Service from here, will prevent all access to that Service globally, rendering it unavailable to any and all Users, with one click.

<b>Service Name</b>	
Demo CRM	
<b>FQDN</b>	
https://	ghew1232.blacksandsecurity.com
<b>Organization</b>	
blacksandsinc	
<b>Description</b>	
Demo CRM	
<b>Up Stream Server</b>	
192.168.1.21:6066	
<b>Uri</b>	
Uri	
<b>Receiver Address</b>	
108.203.128.66	
<b>Service Status</b>	
Enabled	
<b>Service Validation</b>	
	blacksandsincg2sN1Glxh5datmpSEFzwQZFihKVS0k77tLlBjtXlPByUSfn



### 3.2.1.1. Creating a New KVM (Remote Desktop) Service

Blacksands utilizes a proprietary client for connection from the back of the Virtual Receiver to the target PC. There are two basic PC connection modes:

- **Read Only** - provides the User with near real-time screen visualization. This does NOT allow the User the ability to upload, download, or modify the PC environment, in any way.
- **Full Access** - provides the User with simultaneous control and visualization of the PC. Control is limited to KVM (keyboard, video, and mouse). The User is not able to upload or download anything into the PC environment directly.

Each mode is a unique Service. This means that a single PC will likely have two (2) Services with unique setups in the Blacksands Manager (a Read Only and a Full Access), allowing for individual devices to be given different access control

#### **Requirements:**

- A PC, like any Service, must be routable from the Blacksands Virtual Receiver with port 5900 accessible.
- A PC must have the BsIRDS server installed.

#### **Set Up:**

In the Blacksands Manager, select 'Create a New Service' icon and fill out the fields as you would to establish any Service. (for more information on creating a Service - see Create a Service 3.2.1) To delineate between 'Read Only' and 'Full Access', the Administrator will input the appropriate URI code in the appropriate field for the Service once the Service has been created.

#### **To create a Read Only PC Service :**

/readviewer

(requires the slash '/' before readviewer)

#### **To create a Full Access PC Service:**

/fullviewer

(requires the slash '/' before fullviewer)



### 3.2.1.2. Setting up the Target PC for Blacksands Remote Connection

To enable Blacksands to make a connection to a particular PC the following is required:

- Blacksands Virtual Receiver must have routable network access to the PC
- PC's internal security must allow access from the Blacksands Virtual Receiver
- The PC must have the Blacksands BsIRDS server installed and running
- Installation requires Admin privileges on the PC

BsIRDS or "Blacksands Inc Remote Desktop Services".

BsIRDS allows a secure, remote, point to point, encrypted connection to single desktop. BsIRDS installs the application KeyExchange, this application will pair tokens with a given Blacksands Virtual Receiver. KeyExchange will only communicate to Blacksands Virtual Receiver's backend private networks 10.0.0.0/8 (255.0.0.0), 172.16.0.0/12 (255.240.0.0), 192.168.0.0/16 (255.255.0.0) using IPv4 addressing. Installing BsIRDS and running the Key Exchange will require Windows local administrator permissions. BsIRDS can only be paired with a single Blacksands Virtual Receiver.

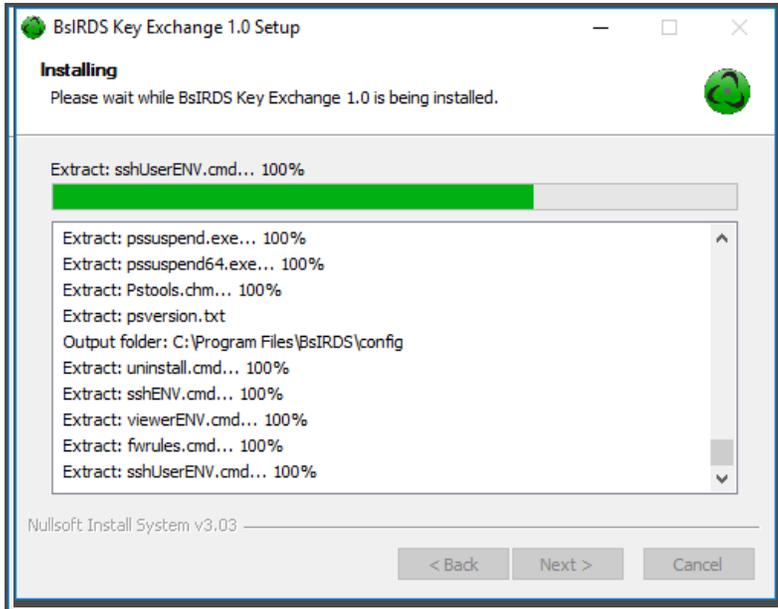
#### 1. Installing Blacksands BsIRDS Application

Start the setup by following the link at the following URL:  
<https://s3.amazonaws.com/bsi-release/www/index.html>

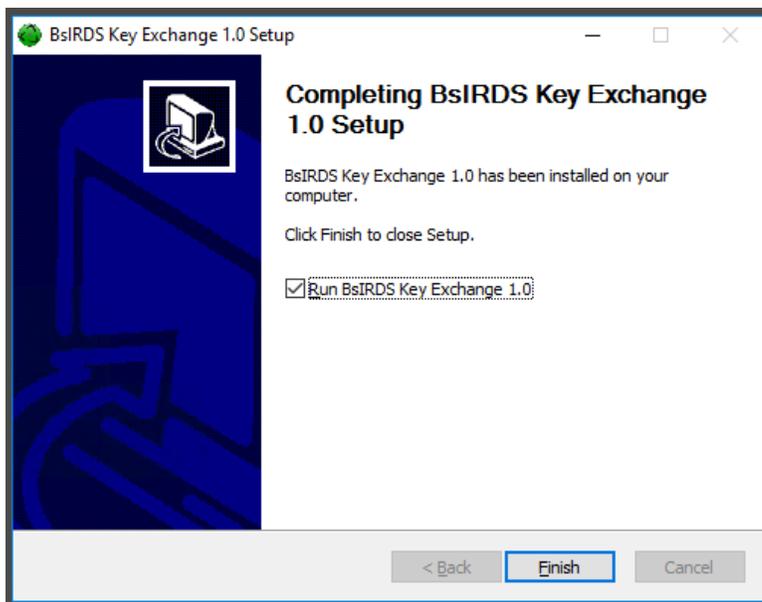




SetupBsIRDS.exe, this will require Windows Administrator Permissions  
Please read the License Agreement then Select I Agree or Cancel. The installer will start extracting the required files.

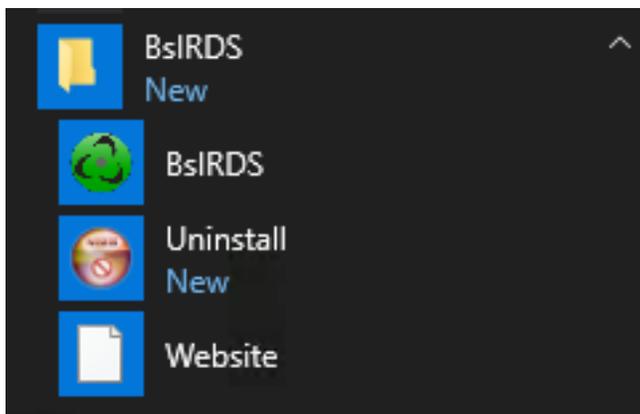


Select Finish



2. KeyExchange can be initiated the following ways:

Desktop Shortcut BsIRDS



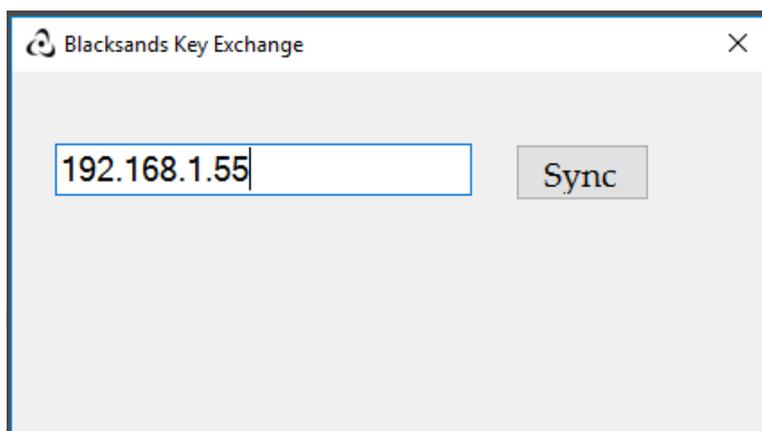
#### Windows Start Menu

### 3. BsIRDS Configuration

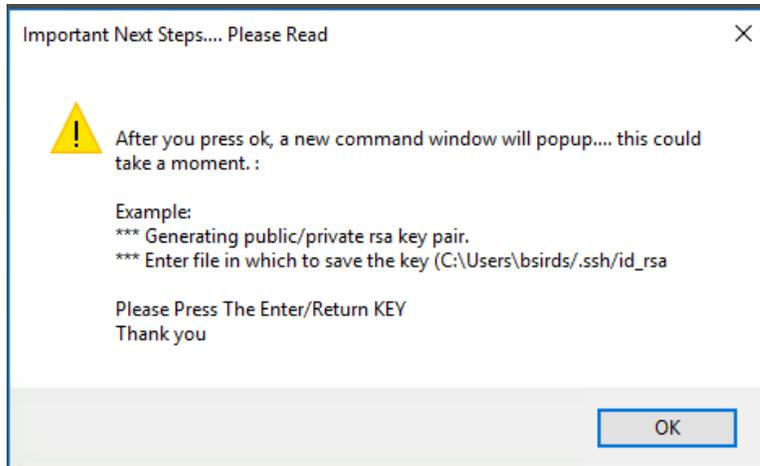
Every time the BsIRDS application is able to successfully connect to a Blacksands Virtual Receiver the following system checks are performed:

- (a) A new local service account will be created called BsIRDS.
- (b) Windows firewall rules will be set to only allow the Blacksands Virtual Receiver to talk to the BsIRDS application.
- (c) The Blacksands Virtual Receiver's token will be added to the BsIRDS configuration

Initiate the BsIRDS Application with Administrator permissions, input the Blacksands Virtual Receiver private IPv4 address and press the Sync button.

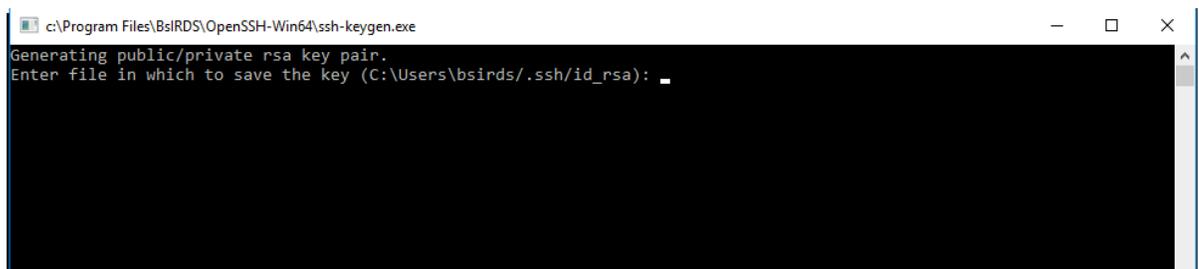


The first time Key Exchange is run, you will be presented with a prompt that will require you to perform an action of pressing the Enter or Return key (depending on your keyboard layout)



Click OK

New screen will open requiring you to press Enter or Return



Once you see the Thank you popup, you can select OK and close the Key Exchange application.





Blacksands BslRDS application configuration is now complete

4. If client computer is using a different firewall than the local Windows Firewall, those rules will have to be configured manually.

Direction	Remote IPv4	Local Port	Action	Application
Ingress	Receivers Private IP	22	Allow	NA
Ingress	127.0.0.1/32	5900	Allow	NA
Egress	NA	NA	Allow	c:\Program Files\BslRDS\KeyExchange.exe

## 3.2.2. Managing Services

### 3.2.2.1. Enabling / Disabling a Service

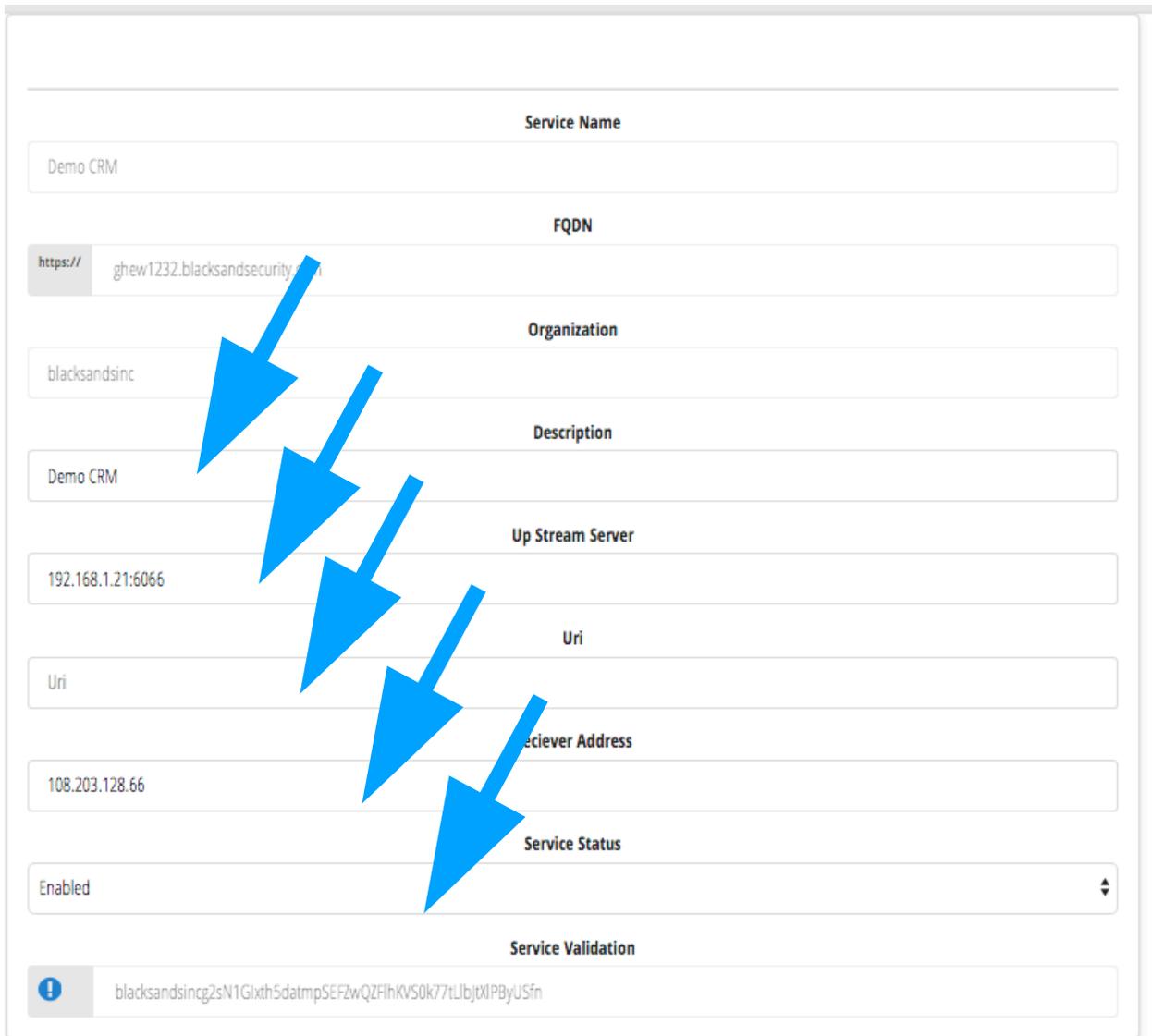
Each Service can be Enabled or Disabled globally, by simply toggling the 'Service Status' tab.

<b>Service Name</b>	
Demo CRM	
<b>FQDN</b>	
https://	ghew1232.blacksandsecurity.com
<b>Organization</b>	
blacksandsinc	
<b>Description</b>	
Demo CRM	
<b>Up Stream Server</b>	
192.168.1.21:6066	
<b>Uri</b>	
Uri	
<b>Receiver Address</b>	
108.203.128.66	
<b>Service Status</b>	
Enabled 	
<b>Service Validation</b>	
	blacksandsincg2sN1Glxh5datmpSEFzWQZFihKVS0k77tLlBjtXlPByUSfn

### 3.2.2.2. Modifying a Service

A Service can be modified by simply changing the values in the associated fields. The modifications available are Description, Up Stream Server, URI, Virtual Receiver Address, Service Status.

NOTE : Modifying a Service can have adverse effects on its availability.

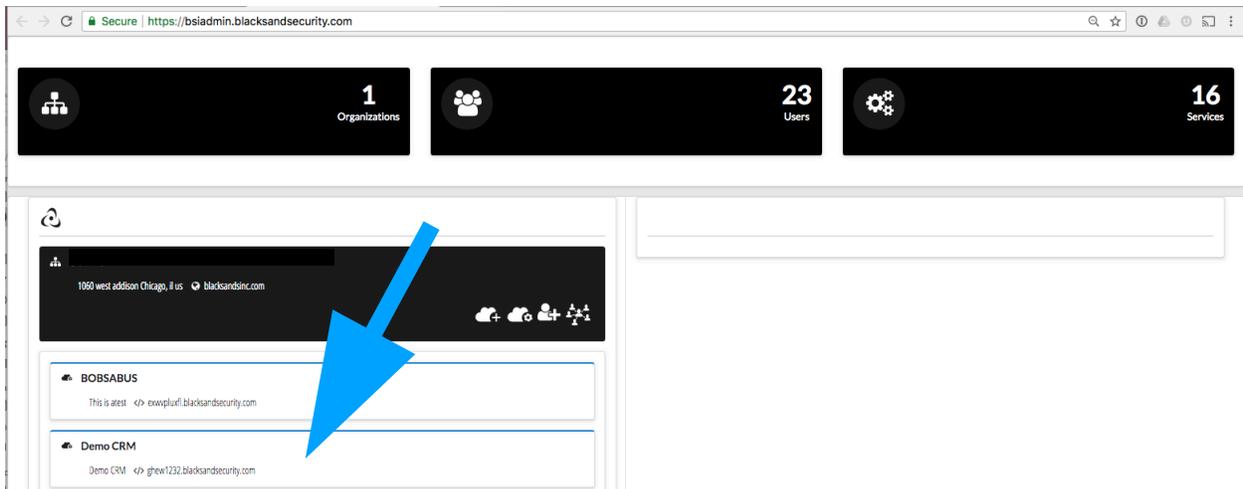


<b>Service Name</b>	
Demo CRM	
<b>FQDN</b>	
https://	ghew1232.blacksandsecurity.com
<b>Organization</b>	
blacksandsinc	
<b>Description</b>	
Demo CRM	
<b>Up Stream Server</b>	
192.168.1.21:6066	
<b>Uri</b>	
Uri	
<b>Receiver Address</b>	
108.203.128.66	
<b>Service Status</b>	
Enabled	
<b>Service Validation</b>	
blacksandsincg2sN1Glxth5datmpSEFZwQZFihKVS0k77tLlbtXlPByUSfn	

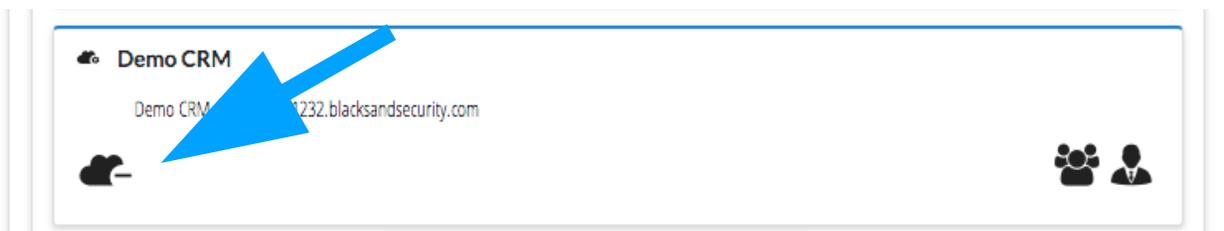
### 3.2.2.3. Deleting a Service

To Delete a Service:

First select the desired Service on the left side of the 'Blacksands Manager' under the Organization.



Then, select the Delete icon below the Service Name and Description. This will permanently delete the service, rendering it inaccessible indefinitely to all users. Be sure you desire to make this action permanent as it is not reversible once selected. If this is done and not desired, the Service will need to be reestablished, and all connections to that service reestablished.

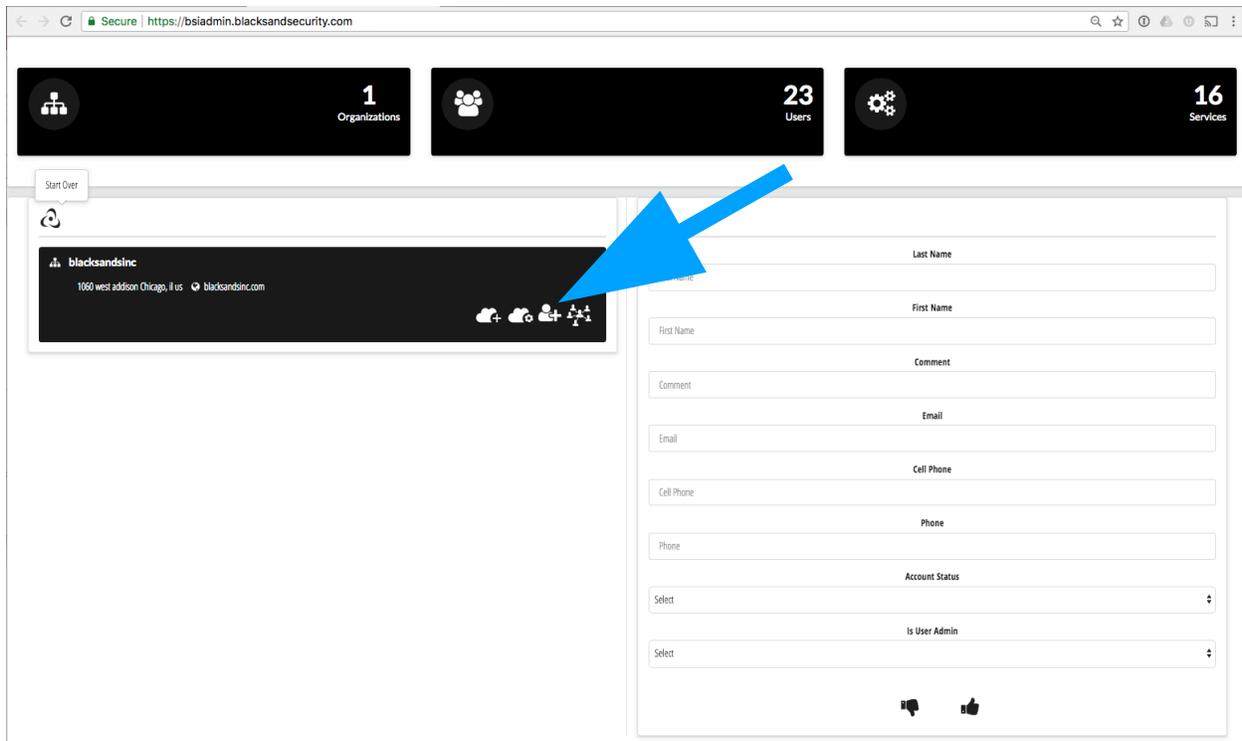




## 3.3. Managing Users

### 3.3.1. Creating a New User

To create a new User select the Add User Icon on the left window of the Manager. This will open a window to the right with (8) fields to fill.





## ACCOUNT STATUS

The 'Account Status' field provides a single point to manage an individual's device and their global access. If an Administrator Disables a User / Device account, the Certificate associated with that User and Device will not be able to access any Blacksands protected Service. By changing this status back to Enabled, the User's Device will be reinstated along with the authorized Services associated with that Device.

## IS USER ADMIN

The 'Is User Admin' field identifies the particular User and Device associated by its unique Blacksands Certificate as an Administrator. When set to 'True' the User and the associated Device with its associated Certificate can access the Blacksands Manager as an Administrator with full Administrator rights.

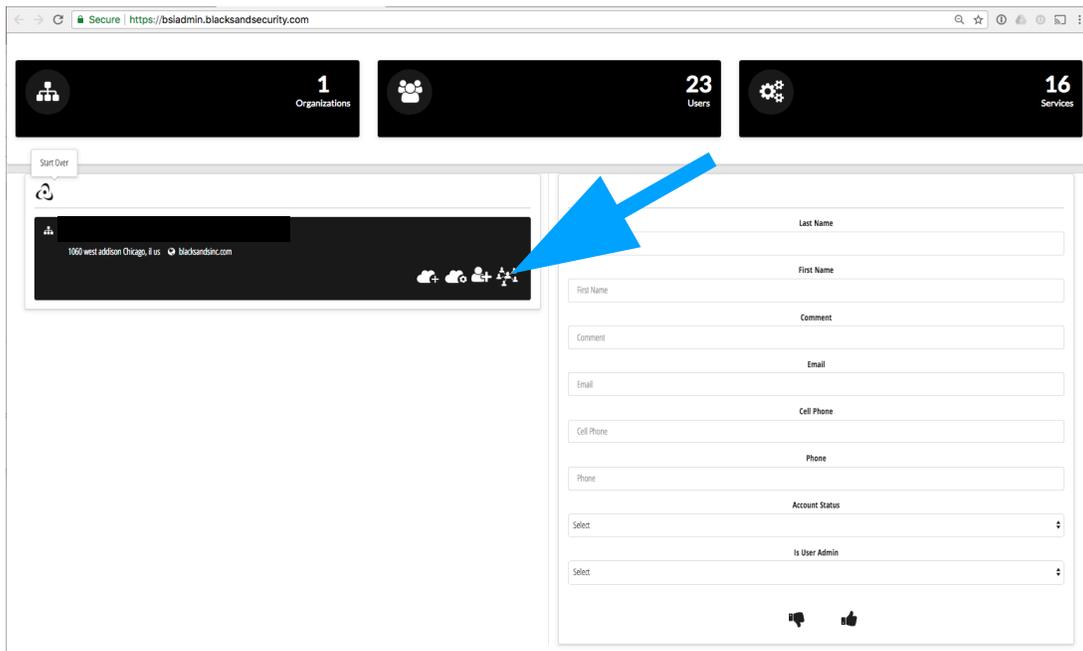
Last Name	
<input type="text" value="Last Name"/>	
First Name	
<input type="text" value="First Name"/>	
Comment	
<input type="text" value="Comment"/>	
Email	
<input type="text" value="Email"/>	
Cell Phone	
<input type="text" value="Cell Phone"/>	
Phone	
<input type="text" value="Phone"/>	
Account Status	
<input type="text" value="Select"/>	
Is User Admin	
<input type="text" value="Select"/>	
 	



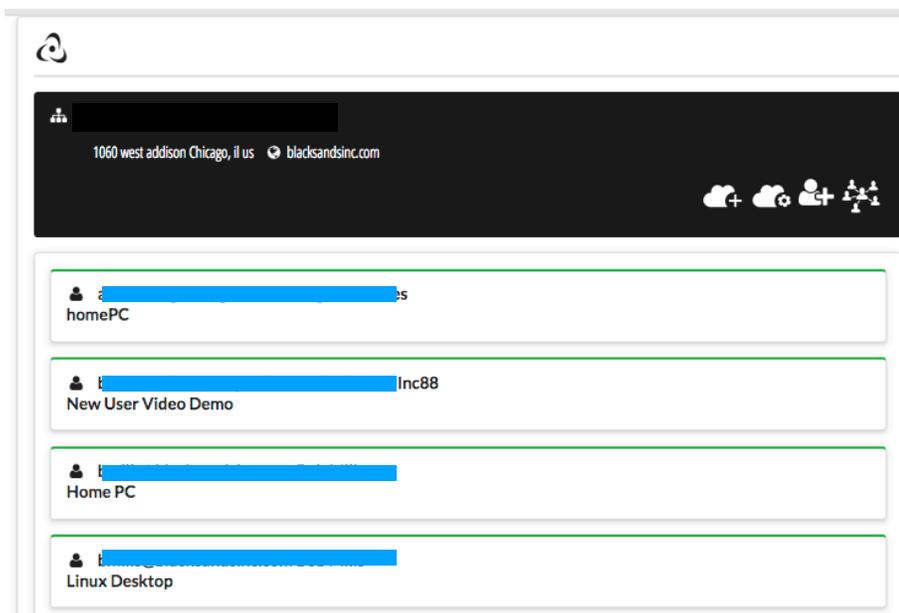
Once all the fields are appropriately filled, select the Thumbs Up icon. The new User will receive an email, at the address provided, to begin the registration process.

### 3.3.2. Modifying a User

Select the Show Users Icon in the left window.



This will produce a list of all Users and their associated Devices.

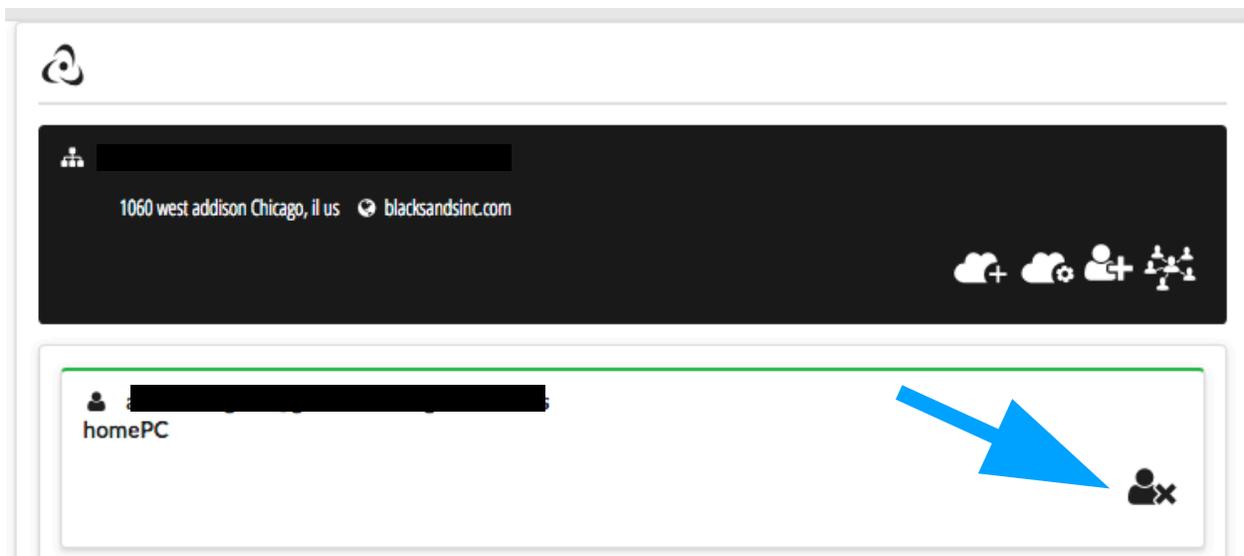




When a particular User / Device is selected, the right window shows the specific information associated with that User / Device. An Administrator can modify any of the fields at any time.

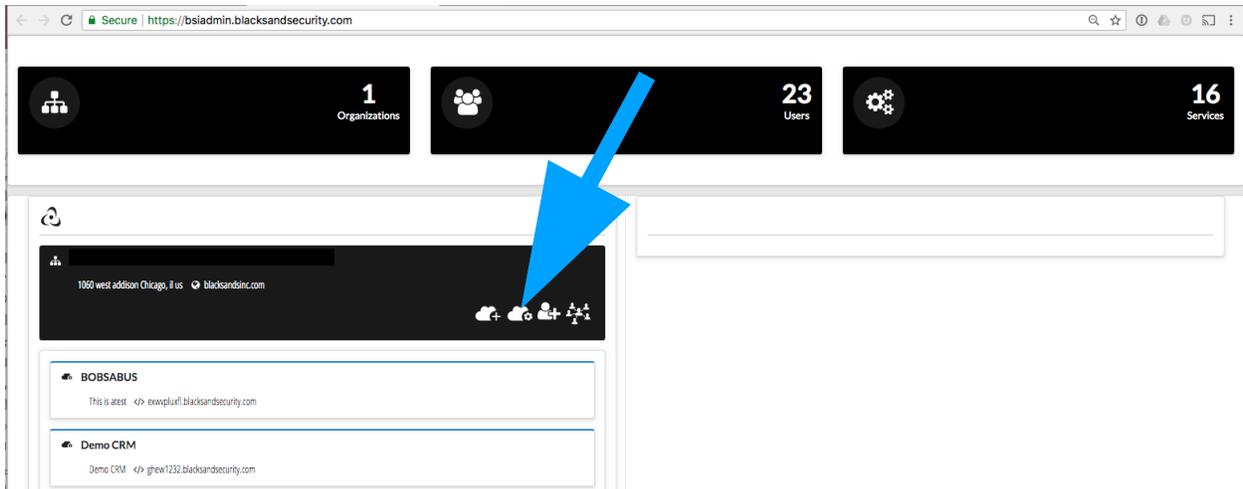
### 3.3.3. Deleting a User / Device

When particular User / Device is selected the delete icon is available in the right side panel. An Administrator can permanently delete the associated User / Device by selecting the Delete icon. This action is not reversible. If this is selected and not desired, a new invitation will need to be generated (new user registration redone) and access to all services will be required to be setup again.

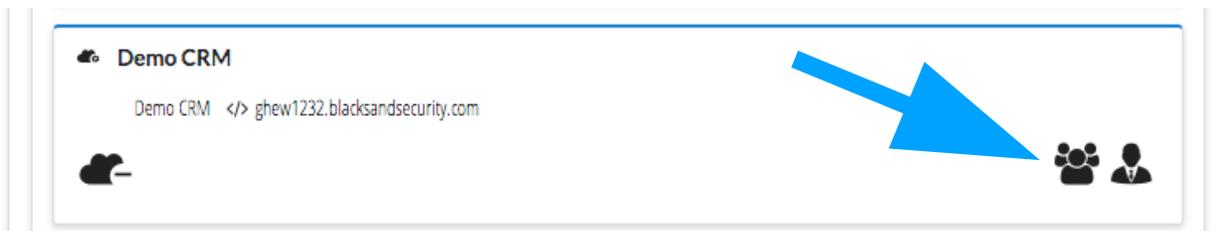


### 3.3.4. Adding a User / Device to a Service

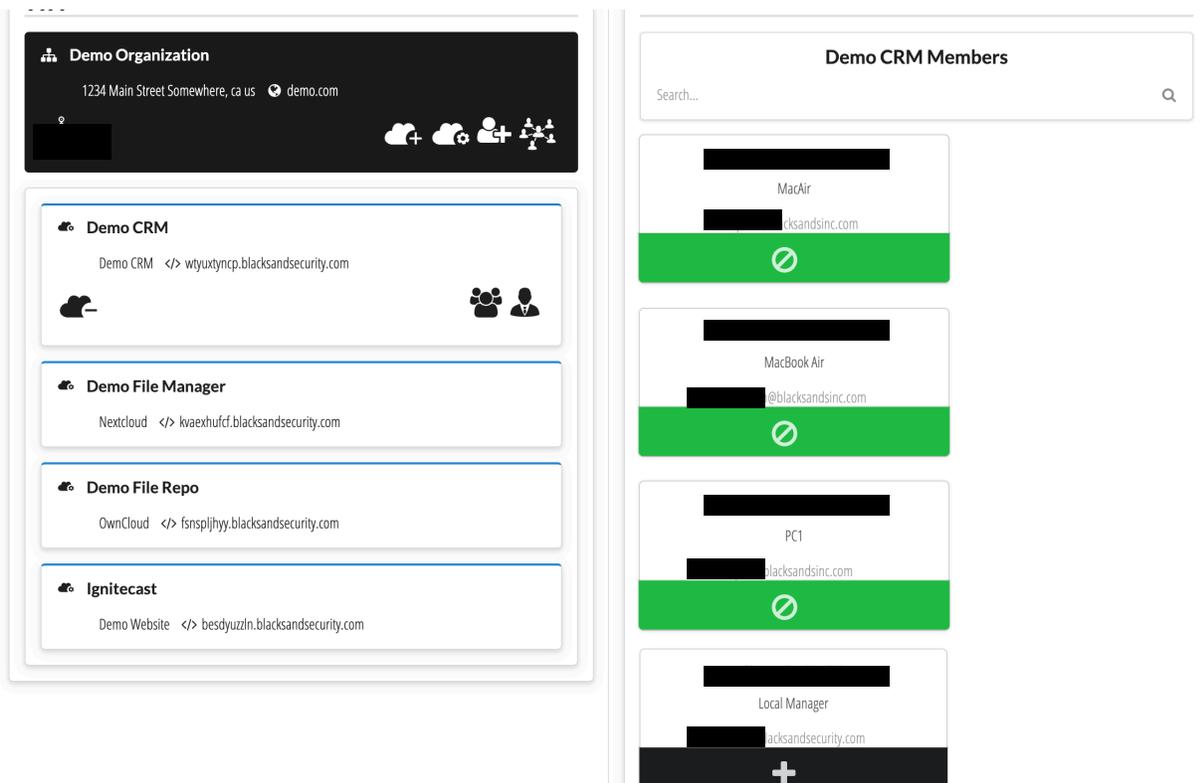
An Administrator or a Stakeholder can add a User to a Service. First the Administrator or Stakeholder selects the 'Show Services' icon and then selects the specific Service to which he/she would like to add a specific User/Device.



Then Administrator or Stakeholder selects the 'Show Service Members' icon.



A new window opens with the User list in the right panel. Green Means that the User / Device is authorized to access the particular Service. Black means it is not authorized for the particular service. To enable or revoke access for a specific User / Device to / from a specific Service, the User / Device button either Green or Black is selected. Once the User / Device button changes color the change is complete.



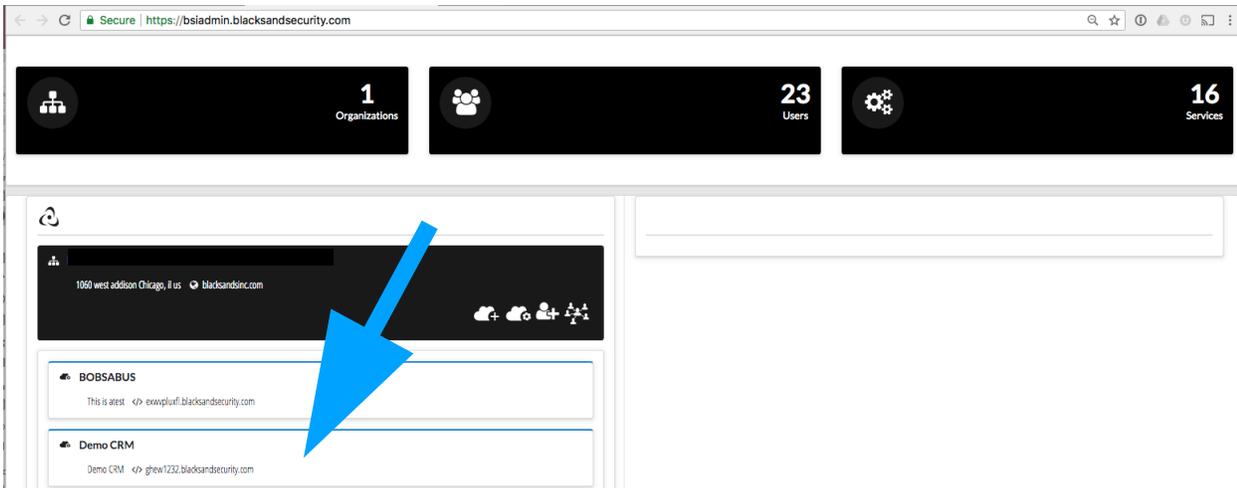
### 3.3.5. Adding a Stakeholder to Service

Stakeholders are similar to Administrators as they have access to the BlackSands Manager. However, a Stakeholder is limited in his/her functionality. Stakeholder access to any Service can only be granted by an Administrator.

When a User / Device is designated a Stakeholder for a specific Service, then that User / Device will be able to manage other User's access to that particular Service. The Stakeholder is also provided the ability to Modify the Service fields. The Stakeholder cannot Add, Delete, or Modify Users. Nor can the Stakeholder Add or Delete Services.

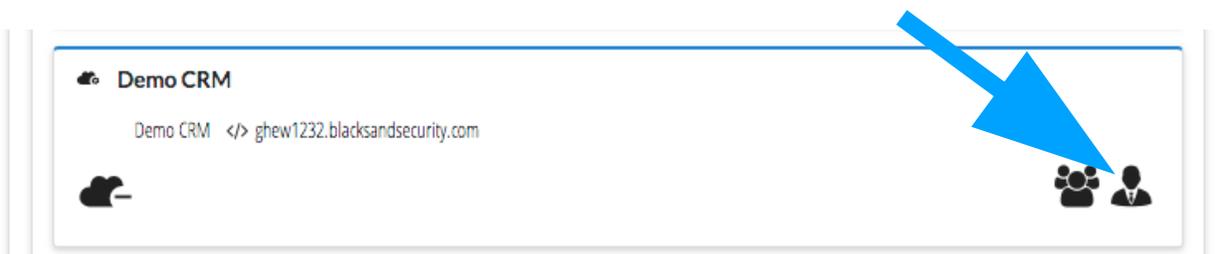


A Stakeholder is restricted to only managing User access to the specific Service/s they are Stakeholders for. A Stakeholder can be a member of other Services as well.



To Add a Stakeholder to an existing Service, a Blacksands Administrator selects the particular Service.

Then the Administrator selects the 'Show Stakeholder Management' icon.



A new window similar to the 'Add Users to Service Window' opens. The Administrator selects the particular User / Device selects the right arrow and adds that User / Device to the 'In Service' list. Once the User / Device turns green the Stakeholder access is granted. Similarly, an Administrator can remove a Stakeholder by selecting the User/ Device from the 'In Service' list and selecting the left arrow. The User / Device is moved to the 'Not In Service' list and when it turns green the Stakeholder access is revoked.



When the User and associated Device (now Stakeholder) accesses the Blacksands Authorizer a new Service appears in the drop down list of Services: 'BlackSands Manager'. The Stakeholder will only see Services that he/she has the ability to manage within the Blacksands Manager Service.

---

**Add and Remove Members**

← →

**Not In Service**



A vertical list of six member cards. The top card has a green background and a white person icon. The other five cards have white backgrounds and black person icons. All names are redacted with black bars.

**In Service**



A vertical list of three member cards, all with white backgrounds and black person icons. All names are redacted with black bars.



## 4. Deploying Blacksands Virtual Receiver

### 4.1. Virtual Receiver Requirements

In order for the rapid and effective installation of the Blacksands Virtual Receiver the following requirements must be met:

**(Company Provides)Company network accessible**

- 1 Static IP address per Virtual Receiver
- HTML application/s
- Web Accessible IoT Device/s
- Windows Test Equipment PC/s with accessible port: 5900
- VMWare ESXi 6.5+ VMWare Virtual Center 6.5+

#### Hardware

Processor should be one of the following combinations:

- Four(4) Sockets
- Two(2) Sockets Two(2) Cores
- Four(4) Cores

Ram:

- Four(4) GB (4096 MB) Ram
- Storage:80 GB Virtual Hard Drive

#### Network Rules: Inbound

External IP should be able to initiate request to VM: from Blacksands - 67.225.220.203 to Virtual Receiver External IP(xxx.xxx.xxx.xxx):Port 22 & Port 443

#### Network Rules: Outbound

VM should be able to initiate requests to IPv4 IP:

- Address 91.189.91.23 Port 80 and 443 TCP (software/security updates)
- Address 91.189.91.26 Port 80 and 443 TCP (software/security updates)
- Address 91.189.88.162 Port 80 and 443 TCP (software/security updates)
- Address 91.189.88.161 Port 80 and 443 TCP (software/security updates)
- Address 91.189.88.149 Port 80 and 443 TCP (software/security updates)
- Address 91.189.88.152 Port 80 and 443 TCP (updates) Port 123 UDP (NTP)
- Address 74.125.69.108 Port 587 TCP (Device Registration)



Address 74.125.69.109 Port 587 TCP (Device Registration)

Address 67.225.220.110 Port 443 TCP (Device Registration)

Address [DNS Server (i.e. Google 8.8.8.8)] Port 53 TCP/UDP (DNS)

Address 67.225.220.131 Port 5680 (Blacksands bus)



## 4.2. Downloading Virtual Receiver

Download VM From given URL:

<https://s3.amazonaws.com/bsi-release/www/index.html>

Log into your VMWare Web Console, this demonstration will be using VMWare ESXi 6.5.0

Unzip the file BlacksandsInc\_Receiver\_v2.4.zip and a new directory will be created:

- BlacksandsInc\_Receiver\_v2.4
  - BlacksandsInc\_Receiver\_v2.4.ova
  - sha256sum.exe
  - sha256.sha

### Verifying Download

To check the file hash please do the following:

#### **OSX:**

in command window cd into BlacksandsInc\_Receiver\_v2.4 execute the following command

```
shasum -c sha256.sha
```

#### **Windows:**

In command window cd into BlacksandsInc\_Receiver\_v2.4 execute the following command

```
sha256sum.exe -c sha256.sha
```

### 4.3. VMWare ESXi 6.5.0 Example

Select **Create / Register VM**, select **Deploy a virtual machine from OVF or OVA files** then click **Next** (see Diagram 1.)

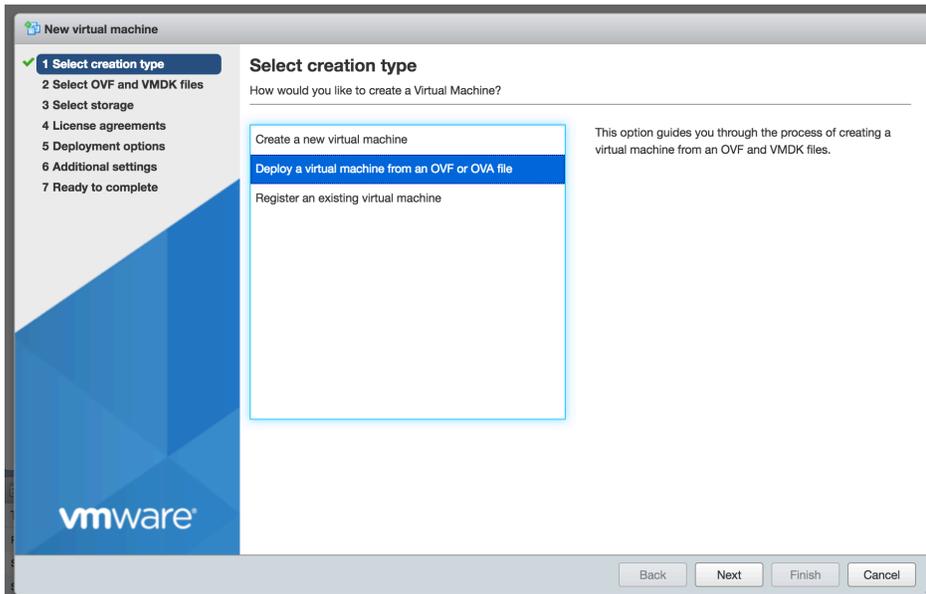


Diagram 1

Add **Name** and **drag** the **BlacksandsInc\_Receiver\_vXX.ova** into the **blue box** and click **Next** (see Diagram 2.)

Select **Storage** and click **Next**

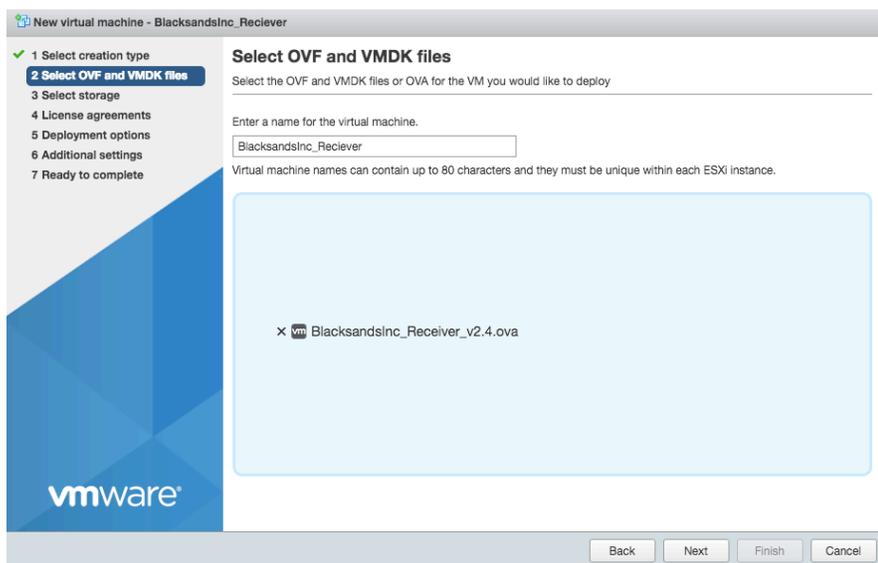


Diagram 2



Select **Deployment Options** and click **Next**

Review the settings and click **Next** at **Ready to complete** (see Diagram 3.)

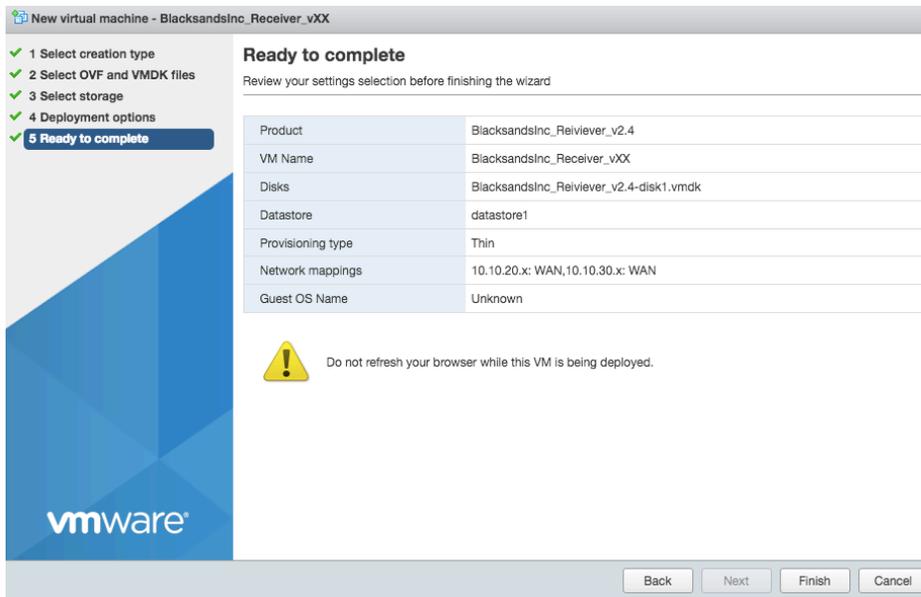


Diagram 3

## 4.4. Registering the Blacksands Virtual Receiver

**Power On** the newly created VM.

Start a **console** to the VM.

If you experience the following Error:

'SSE 4.2 Instruction Set Not found'

Please see Appendix A for instructions and Blacksands Non-SSE4\_2 Receiver Download process.





#### 4.4.1. Accessing bsiuser Tools

Hit 'TAB' a couple of times to see a list of available tools. (adapters, arp, registration, restart, set, shutdown, speedtest)

```
bsiuser@config:~#  
adapters      registration  set           speedtest  
arp           restart      shutdown  
bsiuser@config:~#
```

#### 4.4.2. Setting up Networking

The initial settings are WAN0 - DHCP and LAN0-3 DISABLED

The first change will be to setup networking for WAN0

Type 'set' and then hit 'TAB'. This will provide you with the the different 'set' functions available.

```
bsiuser@config:~# set  
lan0 lan1 lan2 wan0
```

Type 'set wan0'

```
bsiuser@config:~# set wan0  
Please select dhcp or static or off  
[dhcp/static/off/back]: static  
IPv4 Address: [REDACTED]  
IPv4 Subnet Mask: 255.255.255.248  
IPv4 Gateway: [REDACTED]  
Please enter DNS seperated by spaces  
IPv4 DNS: 8.8.8.8
```

Then input the appropriate networking information including; Address, Subnet, Gateway, and DNS.

You can also set one of the LAN interfaces for the internal network in the same way.



Anytime you adjust networking on the Virtual Receiver, the device will need to be restarted for the changes to take effect.

### 4.4.3. Restarting Virtual Receiver

Type 'restart' in order to force the rebooting of the Virtual Receiver. You will be required to confirm this request.

### 4.4.4. Viewing Network Adapters

In order to view WAN0, LAN0-3 you can view the current adapter settings. Type 'adapters show' and it will list the current settings.

```
bsiuser@config:~# adapters show
```

Name	Setting	IP	NetMask	Gateway	Speed	Duplex	Link
lan0	dhcp	192.168.1.15	255.255.255.0	proto	10000Mb/s	Full	yes
lan1	manual	Not Set	Not Set	Not Set	10000Mb/s	Full	yes
lan2	manual	Not Set	Not Set	Not Set	10000Mb/s	Full	yes
wan0	static	108.203.128.68	255.255.255.248	108.203.128.70	10000Mb/s	Full	yes

### 4.4.5. Registering a Virtual Receiver

In order for a Blacksands Virtual Receiver to connect to the Blacksands infrastructure and be available for an organization to use, an automated Registration and Provisioning Process must occur.

The 'registration' option has three sub-functions: 'complete', 'reset', and 'start',

```
bsiuser@config:~# registration
complete reset start
```

#### 4.4.5.1. Starting the Registration Process

Type 'registration start'. You will be prompted to confirm the registration of this Virtual Receiver. Note, that this resets the Virtual Receiver in the system. This also REQUIRES proper networking. We suggest utilizing some of the other networking tools prior to Registering the Virtual Receiver (i.e. 'arp', 'speedtest', 'adapters')

```
bsiuser@config:~# registration
complete reset start
bsiuser@config:~# registration start
Do you want to register this instance? [yes/no]: yes
```



#### 4.4.5.2. Setting Emails for the Registration Process

You will be asked for two emails:

The first is an 'Admin Email'. This is a member of your organization that is already a valid Blacksands Administrator. He/she will receive an email requesting approval of this Registration process for your organization.

The second email is your email (the person installing the Virtual Receiver). This email address will be used to report on any changes to the Blacksands Virtual Receiver. These 2 email addresses may be the same for a given organization.

```
bsiuser@config:~# registration start
Do you want to register this instance? [yes/no]: yes

Please Read .....

This device can only be registered by a valid blacksands member that has admin privileges.
You will be prompted for an admin email address.
Continue ? [yes/no]: yes
Enter Admin Email or quit: [redacted]
Enter Admin Email or quit: [redacted]

Please Read .....

You will be prompted for your email address.
This email address will be used for any updates
Continue ? [yes/no]: yes
Use: [redacted] [yes/no]: yes
One moment please.....
One moment please.....
One moment please.....
One moment please.....
bsiuser@config:~#
```

The Registration process may take a few minutes. If you receive a 'Could not retrieve the package, exiting' error. Wait a few minutes and try again.

```
bsiuser@config:~# registration complete
One moment please.....
One moment please.....
Could not retrieve the package, exiting
bsiuser@config:~#
```



Once the Registration Process is complete, the following message will be displayed and the Blacksands Virtual Receiver is ready for use.

```
bsiuser@config:~# registration complete
```



## 5. Event Logs

### 5.1. Overview

Blacksands Virtual Receiver provides two types of logs, network logs and Virtual Receiver local application logs. Virtual Receiver local application logs consists of Action and Request logs.

### 5.2. Definitions

**Kernel syslog facility** - a standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, indicating the software type generating the message, and assigned a severity label.

**Blacksands log Facility** - JSON string using the ISO 8601 date time format

**Action logs** - events that occur between Virtual Receiver and Manager

**Request logs** - events that occur between User and Virtual Receiver

### 5.3. Explanation

Network logs come from the Kernel syslog facility and follow two rules, allowed or blocked (see diagram 1)

```
May 11 14:17:32, ALLOWED IN=wan0 OUT= SRC=x.x.x.x DST=x.x.x.x LEN=191 TOS=0x00
PREC=0x00 TTL=53 ID=0 DF PROTO=TCP SPT=51158 DPT=443 WINDOW=7987 RES=0x00 ACK PSH
URGP=0

May 11 10:33:58, BLOCKED IN=wan0 OUT= SRC=x.x.x.x DST=x.x.x.x LEN=40 TOS=0x00
PREC=0x00 TTL=240 ID=46520 PROTO=TCP SPT=6666 DPT=443 WINDOW=1024 RES=0x00 SYN URGP=0
```

**EXAMPLE OF NETWORK KERNEL LOG ENTRY  
DIAGRAM 1**

Blacksands Action and Request logs are processed by the Blacksands Log Facility.



Diagram 2 shows the events to be processed by the Virtual Receiver from the Manager.

```
2018-03-28 10:51:40,013, TYPE:INFO, MSG:{"hash": "/UID=1111-2222-3333-4444-5555/CN=tjones-1234:SERIAL", "upstream": "x.x.x.x:1234", "request": "add", "fqdn": "abcdefg.blacksandsecurity.com", "ip": "x.x.x.x"}  
2018-03-28 11:03:43,103, TYPE:INFO, MSG:{"hash": "/UID=1111-2222-3333-4444-5555/CN=tjones-1234:SERIAL", "request": "rm-all", "ip": "x.x.x.x"}
```

### ACTION EVENTS DIAGRAM 2

Diagram 3 shows the events being processed between the User and Virtual Receiver.

```
2018-03-28 11:03:43,103, MSG:{"host": "x.x.x.x", "status": "101", "request": "GET /websocketify HTTP/1.1", "size": "14858031", "subject": "/UID=1111-2222-3333-4444-5555/CN=tjones-1234", "serial": "1234", "server": "abcdefg.blacksandsecurity.com", "be": "x.x.x.x", "b": "585.397", "ber": "585.397"}
```

### REQUEST EVENT DIAGRAM 3

Blacksands can work with a customer in setting up Blacksands Parsers within the customer SIEM or log collector.



## Record of Changes

Revision Level	Section	Change Description	Date	Comments
1.2.2	4.1	Change	14 June 2018	Changed VM version requirements to ESX 6.5
1.2.3	4.2	Add	21 June 2018	Add error message for missing SSE 4_2 in VM Download and fix - Appendix A
1.26	3.34 Appendix A	Modify	23 August 2019	Modified the User / Service interaction
1.26	Appendix A	Remove Appendix	23 August 2019	Remove Section
1.27	Document	Update	18 September 2019	Minor Revisions