



SUREedge[®] Migrator 5.7.0

Installation Guide for Azure



Contents

1.	Introduction	3
1.1	Deployment Scenarios	3
1.2	Installation Overview	4
2	Deploying SUREedge Migrator	5
2.1	Getting Azure Parameters.....	5
2.2	Communication between Source Server and SUREedge® Migrator.....	7
2.3	Obtaining SUREedge Installers.....	9
2.3.1	Getting Installers.....	9
2.3.2	Getting Disk.....	10
2.4	Preparing SUREedge Store	10
2.4.1	Creating a VM	10
2.4.2	Uploading Packages	11
2.4.3	Installing Store	11
2.5	Creating Proxy Image	12
2.5.1	CentOS Proxy Image.....	12
2.5.2	Windows proxy image	14
2.6	Preparing SUREedge MC	16
2.6.1	Creating a VM	16
2.6.2	Uploading Packages	16
2.6.3	Installing SUREedge Migrator	17
3	Configurations	27
3.1	Configuring Hypervisor.....	27
3.2	Configuring Proxy	29
3.2.1	Linux Proxy Image configuration	29
3.2.2	Windows Proxy Image configuration.....	30
3.3	License Configuration.....	31
4	Contacting Support.....	33



1. Introduction

SUREedge® Migrator is a proven enterprise-class software appliance for Application Mobility, significantly simplifying and improving the process of moving enterprise applications and systems across disparate environments. With a multi-tier application migration planner, agentless architecture, WAN throttling, application awareness and world class encryption and deduplication capabilities, SUREedge Migrator is easy to deploy, highly scalable and hardware- and hypervisor-agnostic. With the ability to capture and migrate applications, data and servers between disparate virtualization environments, data centers and public, private and hybrid clouds, SUREedge® Migrator is the most complete and easy-to-use solution available in the market.

1.1 Deployment Scenarios

SUREedge® Migrator can be deployed in various configurations to meet the needs of the situation:

- a. A single instance of SUREedge Migrator can be deployed to move systems, applications and data of physical systems into virtualization environments, between different virtualization environments or onto new storage devices. This process is referred to as *on-boarding*.
- b. A pair of SUREedge Migrator instances can be used to move systems, applications and data between compute environments - from one data center to another, from physical systems into private or public clouds, across compute clouds and other virtualization environments, or any computationally "distant" environments. This process is referred to as *migration*.

The main difference between migration and on-boarding scenarios is the number of SUREedge Instances that are needed: on-boarding requires installing one SUREedge Migrator instance in the target virtualization environment, whereas migration requires two - one at the source site where the systems to be migrated reside, and one at the target site where they will live after the migration.

Note that the same SUREedge Migrator software is installed and same installation procedures are followed for both the source and target instances; the role of a given instance (target or source) is determined solely by its configuration. Therefore, these installation instructions apply to both source and target site installs.



1.2 Installation Overview

To set up an environment for on-boarding or migration you should first determine the location(s) where SUREedge Migrator should be installed. You can then:

- ❖ Obtain the required documentation and software for the environment(s) you have identified. You should have ***SUREedge Migrator 5.7.0 Installation Guide for Azure*** (this document) and the software packages for installing SUREedge Migrator.
- ❖ Perform the installation of SUREedge Migrator software as instructed.
- ❖ License and configure SUREedge Migrator as appropriate for each environment, as described in the Installation Guide and the User Guide.

This Installation Guide covers the steps necessary for installing SUREedge Migrator in Azure environment. The following sections will take you through the steps to obtain installation materials and to install, license and configure SUREedge Migrator to run in Azure environment. You can then use the ***SUREedge Migrator 5.7.0 User Guide*** to configure and start using SUREedge Migrator for on-boarding or migration.



2 Deploying SUREedge Migrator

2.1 Getting Azure Parameters

Before starting SUREedge deployment on Azure, user need to create and register an application in Azure. User need to note some of the parameters from Azure which will need while [configuring SUREedge hypervisor](#).

At the end of this section, you will get following parameters:

- ✓ Subscription ID
- ✓ Application ID
- ✓ Secret Key
- ✓ Directory ID
- ✓ Resource Group
- ✓ Storage Account
- ✓ Location

Following are the steps to get the parameters:

Step 1: Create an Azure Active Directory application

1. Sign in to your Azure Account through the [Azure portal](#).
2. Select **Azure Active Directory**.
3. Select **App registrations**.
4. Select **New registration**.
5. Provide a name and keep the default **Supported account types**. Select **Web** for Redirect URL for the type of application you want to create. Provide URL in the provided textbox. Click **Register**.

You've created your Azure AD application and service principal.

Step 2: Assign the application to a role

1. Sign in to your Azure Account through the [Azure portal](#).
2. Navigate to **All Services > Subscriptions**.
3. Select the *subscription* to assign the application to.
4. Select **Access Control (IAM)**.
5. Select **Add > Add role assignment**.
6. Select the role you wish to assign to the application. To allow the application to execute actions like reboot, start and stop instances, select the **Contributor** role. By default,



Azure AD applications aren't displayed in the available options. To find your application, search for the name and select it.

7. Select **Save** to finish assigning the role.

Step 3: Get Directory ID


- Sign in to your Azure Account through the [Azure portal](#).
- Select **Azure Active Directory**.
- Select **Properties**.
- Copy the **Directory ID**.

Step 4: Get application ID and authentication key

- Sign in to your Azure Account through the [Azure portal](#).
- Select **Azure Active Directory**.
- Select **App registrations**.
- From **App registrations** in Azure AD, select your application.
- Copy the **Application ID** and store it in your application code.
- Select **Certificates & secrets**.
- Select **New client secret**.
- For *Add a client secret*, provide a description of the key and duration for the key and click **Add**.
- After saving the key (**Secret Key**), the value of the key is displayed. ***Copy and store this value because you can't retrieve the same key later.***

Client secrets
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE
Password uploaded on Fri May 10 2019	5/10/2020	Ybuyex5AQmbuF[-.x0pjYx]vafa9eVm6 

Step 5: Get subscription ID

1. Sign in to your Azure Account through the [Azure portal](#).



2. In the left navigation panel, click **Subscriptions**. The list of your subscriptions is displayed along with the **subscription ID**. Get the subscription ID for the subscription assigned to the application.

Step 6: Get Resource Group & Region

1. Sign in to your Azure Account through the [Azure portal](#).
2. In the left navigation panel, click **Resource groups** and select **Add**.
3. Provide **Resource group** name and select Region (**Location**) from drop down list.
You need to choose same resource group and same region wherever required in further steps.

Step 7: Get Storage Account

1. Sign in to your Azure Account through the [Azure portal](#).
2. In the left navigation panel, click **Storage accounts** and select **Add**.
3. Select the **Resource group** which was created earlier from drop down list.
4. Provide **Storage account name** and select **Location** from drop down list. Make sure location is same as Region selected in earlier steps. Keep the rest parameters default and click **Create**.

Once created, **Storage account** will be listed.

2.2 Communication between Source Server and SUREedge® Migrator

Open the following ports to ensure that the SUREedge Migrator can communicate with the source servers to be migrated to Azure.

Protocol	Ports	Purpose	Comments
TCP	3389	RDP Port	Needed for remote troubleshooting
TCP	22	SSH Port on SUREedge Migrator (Store)	Needed to handle the capture data and metadata
TCP	22 OR *	SSH Port on Linux Source server (22 is default)	Needed to stream capture data from Linux client
TCP	3306	DB port on SUREedge Migrator (MC)	Needed to communicate with DB



Protocol	Ports	Purpose	Comments
TCP	80	HTTP Port on SUREedge Migrator (MC)	Needed to host Web-GUI
TCP	1024-65535	Dynamic Ports required for Capture	Needed to stream capture data from Windows client
TCP	139	Required on SUREedge Migrator (MC) and Source server to establish communication for Capture	Needed for agentless capture
TCP	445	Required on SUREedge Migrator (MC) and Source server to establish communication for Capture	Needed for agentless capture
TCP	21	Default FTP port, to enable SUREedge Migrator (MC) and Source server to be able to FTP SUREedge Migrator (Store VM)	Needed to upload catalog
ICMP	-	Enable ICMP to ping the source server	Needed to check connectivity to the source server to MC, Store VMs



2.3 Obtaining SUREedge Installers

2.3.1 Getting Installers

This section contains the instructions for downloading SUREedge Migrator installer and some accompanying tools that may be of use. SUREedge Migrator software can be obtained via secure FTP (SFTP). Please use an SFTP client (such as **WinSCP** - <https://winscp.net/eng/download.php>) to download the SUREedge Migrator software installer and tools from the SFTP site. The examples in this section show the download process using WinSCP.

- Please use the following information to connect to the SFTP host:
Host name: <HostName>
Port number: 995
User name: sure01
Password: *Please write to support@surelinesystems.com for the password*
- Click "Yes" to accept the server fingerprint and continue to log in.
- Open the folder named "Download."
- The **Download** folder contains the following subfolders:
 - 1) **Tools** contains SUREedge Pre-Requisite tools, some useful Third Part Apps and Cloud deployment scripts.
 - 2) **SUREedge Installation Package** contains SUREedge Installer binaries.
- Navigate to **SUREedge Installation Package** folder: The folder "SUREedge Installation Package" is divided into subfolders for all available versions of SUREedge Migrator. You can navigate to the latest version ("Current Release") to obtain the package for installing in the environment.
- The **Current Release** folder contains installer packages for various platforms.
- Please download and unzip the "**SUREedge_Software_Appliance_Basic_Installer.zip**". It consist of following files:
 - surestor-prereq-installer.tar.gz
 - surestor-installer.tar.gz
 - surestor-installer-scripts.tar.gz
 - sureedge-centos-proxy-prereq-installer.tar.gz
 - SUREedge_Software_Setup.exe
 - SSDiscoverUtilitySetup.exe
 - Version



2.3.2 Getting Disk

Obtain **SUREdge_Storage_engine_system.vdi** disk from provided source. Make sure for basic installer this file must be present along with installer binaries.

2.4 Preparing SUREdge Store

2.4.1 Creating a VM

1. Sign in to your Azure Account through the [Azure portal](#).
2. Select **Virtual machines** and click **Add**.
3. For **Create a virtual machine**,
 - a. Select a **Resource group** (which was created in [Getting Azure Parameters](#) section) from drop down list.
 - b. Provide **Virtual machine name**.
 - c. Select **Region** (which was created in [Getting Azure Parameters](#) section) from drop down list.
 - d. Select **Image** as *Ubuntu Server 16.04 LTS*.
 - e. For **Size**, select *Standard D3_v2 (4 core and 14GB ram)*.
 - f. For “ADMINISTRATOR ACCOUNT”, choose **Authentication type** as *password*. Provide desired **Username**, **Password** and **Confirm password**.
 - g. For “INBOUND PORT RULES”, choose *Allow selected ports* for **Public inbound ports**. Select *SSH, HTTPS and HTTP* from drop down list from **Select inbound ports**.
 - h. Click “**Next : Disks >**” and select **OS disk type** as *Standard HDD*.
 - i. Add One Extra data disk of size more than 100 GB (Data Disk will vary depending on the size and number of systems to be captured).
Select **Create and attach a new disk**.
For **Create a new disk**:
 - a. Provide **Disk type** as *Standard HDD*.
 - b. Provide **Name** for disk to be created.
 - c. Provide **Size (GiB)** for the disk. Recommended size is >100 GB.
 - d. Keep the default **Source type**.
 - j. From “ADVANCED”, choose *No* for **Use managed disks**. Select the [Storage account](#) which was created earlier.



- k. Select **Review + create** to validate parameters. Once validation is passed, select **Create**.

2.4.2 Uploading Packages

1. SSH to the store using public IP of store (Go to **Virtual Machines** and select store VM which is created above).
2. Upload following packages to `/home/sureline` directory of store VM which is created above.
 - a. `surestor-prereq-installer.tar.gz`
 - b. `surestor-installer-scripts.tar.gz`
 - c. `surestor-installer.tar.gz`

2.4.3 Installing Store

1. Connect to the deployed vm using SSH and run following commands:

```
sudo tar -xzvf surestor-prereq-installer.tar.gz -C /
sudo tar -xzvf surestor-installer-scripts.tar.gz -C /home/sureline
sudo tar -xzvf surestor-installer.tar.gz -C /
cd /opt/sureline/proxy-installer
sudo bash install_store_prereq.sh Azure
cd /home/sureline
sudo bash store_prepare_sure.sh Azure
sudo bash store_installer.sh
```
2. Edit `sshd_config` file with following command:

```
Sudo vi /etc/ssh/sshd_config
```
3. Add following content in `sshd_config` file and save it.

```
KexAlgorithms curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1
```
4. Reboot the store

```
sudo reboot
```
5. Verify store installation by running

```
sudo systemctl status surestor
```



2.5 Creating Proxy Image

SUREedge Migrator consists of two components: A Management Console (“MC”) and a SUREedge Storage Engine (“Store”) that should be created on the Azure Cloud.

Create two instances (SUREedge MC and SUREedge store) on Azure Cloud using Azure images of 2k16 and CentOS respectively.

Note: Make sure MC/store/storage account should be created in same resource group / location / subnet and proxy VHDs should be uploaded in same storage account which is present in same Resource group where both instances (SUREedge MC and SUREedge store) are created.

2.5.1 CentOS Proxy Image

2.5.1.1 Creating a VM

1. Sign in to your Azure Account through the [Azure portal](#).
2. Select **Virtual machines** and click **Add**.
3. For **Create a virtual machine**,
 - a. Select a **Resource group** (which was created in [Getting Azure Parameters](#) section) from drop down list.
 - b. Provide **Virtual machine name**.
 - c. Select **Region** (which was created in [Getting Azure Parameters](#) section) from drop down list.
 - d. Select **Image** as *CentOS-based 7.5*.
 - e. For **Size**, select *Standard D3_v2 (4 core and 14GB ram)*.
 - f. For “ADMINISTRATOR ACCOUNT”, provide desired **Username**, **Password** and **Confirm password**.
 - g. For “INBOUND PORT RULES”, choose *Allow selected ports* for **Public inbound ports**. Select *SSH, HTTP and HTTPS* from drop down list from **Select inbound ports**.
 - h. Click “**Next : Disks >**” and select **OS disk type** as *Standard HDD*.
 - i. From “ADVANCED”, choose *No* for **Use managed disks**. Select the [Storage account](#) which was created earlier.
 - j. Select **Review + create** to validate parameters. Once validation is passed, select **Create**.



2.5.1.2 Uploading Packages

1. SSH to the store using public IP of Centos Proxy VM (Go to **Virtual Machines** and select store VM which is created above).
2. Upload ***sureedge-centos-proxy-prereq-installer.tar.gz*** package to `/home/sureline` directory of CentOS VM created above.

2.5.1.3 Installing Package

1. Connect to deployed vm using SSH and run following commands:

```
sudo tar -xzvf sureedge-centos-proxy-prereq-installer.tar.gz -C /  
cd /opt/sureline/proxy-installer/  
sudo bash prepare_centos_proxy.sh Azure
```
2. Turn off Linux server from Azure portal.
3. Note VHD file name.
Go to azure portal and select **Home** > **StorageAccount** > <Storage Account Name Of Linux Server> > **blob** > **vhds** > <Name of Vm+Timestamp>.vhd
4. Turn Off Linux server from Azure portal and never start again.
Go to azure portal and select **Home** > **Virtual Machines** > <Linux Server Name> > **Delete**
5. Use VHD file name without .vhd as proxy image name.
E.g. From URL =
<https://sureedge550jbsa.blob.core.windows.net/vhds/sureedge550centos720190513151340.vhd>
Use proxy image name = **sureedge550centos720190513151340**



2.5.2 Windows proxy image

2.5.2.1 Creating a VM

1. Sign in to your Azure Account through the [Azure portal](#).
2. Select **Virtual machines** and click **Add**.
3. For **Create a virtual machine**,
 - a. Select a **Resource group** (which was created in [Getting Azure Parameters](#) section) from drop down list.
 - b. Provide **Virtual machine name**.
 - c. Select **Region** (which was created in [Getting Azure Parameters](#) section) from drop down list.
 - d. Select **Image** as *Windows Server 2016 Datacenter*.
 - e. For **Size**, select *Standard D3_v2 (4 core and 14GB ram)*.
 - f. For “ADMINISTRATOR ACCOUNT”, provide desired **Username**, **Password** and **Confirm password**.
 - g. For “INBOUND PORT RULES”, choose *Allow selected ports* for **Public inbound ports**. Select *RDP* from drop down list from **Select inbound ports**.
 - h. Click “**Next : Disks >**” and select **OS disk type** as *Standard HDD*.
 - i. From “ADVANCED”, choose *No* for **Use managed disks**. Select the [Storage account](#) which was created earlier.
 - j. Select **Review + create** to validate parameters. Once validation is passed, select **Create**.

2.5.2.2 Installing Package

1. Update the following settings:
 - a. Disable firewall:
Go to **Control Panel > System and Security > Windows Firewall > Turn Windows Firewall Off or On** (Customize Settings) and **Turn Off Windows Firewall** for public and private networks.
 - b. Open the Command Prompt window as an administrator. Change the directory to `%windir%\system32\sysprep`, and then run `sysprep.exe`.
 - c. In the System Preparation Tool dialog box, select **Enter System Out-of-Box Experience (OOBE)**, and make sure that the **Generalize** check box is selected.
 - d. In **Shutdown Options**, select **Shutdown** and Click **OK**.
2. Turn off Windows server:



- a. Go to azure portal and select **Home** > **Virtual Machines** > <Windows Server Name> > **Stop**
Note: This VM should not be started again after sysprep & shutdown.
3. Note VHD file name:
 - a. Go to azure portal and select **Home** > **StorageAccount** > <Storage Account Name of Windows Server> > **blob** > **vhds** > <Name of Vm+Timestamp>.vhd
4. Delete Windows server:
 - b. Go to azure portal and select **Home** > **Virtual Machines** > <Windows Server Name> > **Delete**
5. Copy Image name
 - a. Use VHD file name without “.vhd” as proxy image name
E.g. From URL =
<https://sureedge550jbsa.blob.core.windows.net/vhds/sureedge5502k1620190513152601.vhd>
Use proxy image name = **sureedge5502k1620190513152601**



2.6 Preparing SUREedge MC

2.6.1 Creating a VM

1. Sign in to your Azure Account through the [Azure portal](#).
2. Select **Virtual machines** and click **Add**.
3. For **Create a virtual machine**,
 - a. Select a **Resource group** (which was created in [Getting Azure Parameters](#) section) from drop down list.
 - b. Provide **Virtual machine name**.
 - c. Select **Region** (which was created in [Getting Azure Parameters](#) section) from drop down list.
 - d. Select **Image** as *Windows Server 2016 Datacenter*.
 - e. For **Size**, select *Standard D3_v2 (4 core and 14GB ram)*.
 - f. For “ADMINISTRATOR ACCOUNT”, provide desired **Username**, **Password** and **Confirm password**.
 - g. For “INBOUND PORT RULES”, choose *Allow selected ports* for **Public inbound ports**. Select *RDP* from drop down list from **Select inbound ports**.
 - h. Click “**Next : Disks >**” and select **OS disk type** as *Standard HDD*.
 - i. From “ADVANCED”, choose *No* for **Use managed disks**. Select the [Storage account](#) which was created earlier.
 - j. Select **Review + create** to validate parameters. Once validation is passed, select **Create**.

2.6.2 Uploading Packages






1. RDP to the MC VM. (Go to **Virtual Machines** and select MC VM which is created above > **Connect > Download RDP file**).
2. Enter username and password as mentioned while creating VM for MC.
3. Upload following packages to any folder on MC.
 - a. SUREedge_Software_Setup.exe
 - b. SSDDiscoverUtilitySetup.exe
 - c. SUREedge_Storage_engine_system.vdi
 - d. Version



2.6.3 Installing SUREedge Migrator

Once you have identified the Windows system where the SUREedge Migrator MC will run and found the resources required to install an instance of SUREedge Migrator.

1. Login to SUREedge MC with rdp file. (Go to **Virtual Machines** > <MC VM> **Connect** to download .rdp file)
2. Once login to SUREedge MC, locate to the installer files.

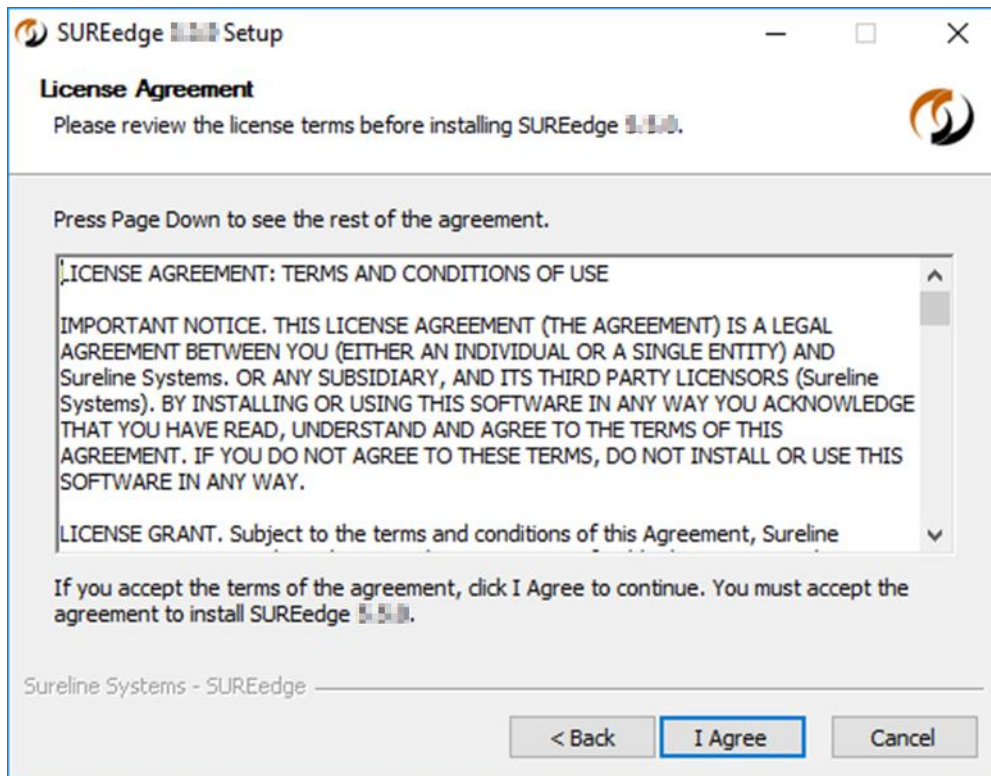
 Licence.bin	4/9/2019 12:17 PM	BIN File	1 KB
 SSDDiscoverUtilitySetup	5/9/2019 6:23 AM	Application	73,803 KB
 SUREedge_Software_Setup	5/9/2019 6:24 AM	Application	947,239 KB
 SUREedge_Storage_engine_system.vdi	5/2/2019 8:03 PM	Text Document	0 KB
 version	4/30/2019 7:17 AM	File	1 KB

3. Run "SUREedge_Software_Setup" file as an administrator. This shows "Validating installer pre-checks..." screen. Wait for some time to display a first screen as "Welcome to SUREedge 5.7.0 Setup".





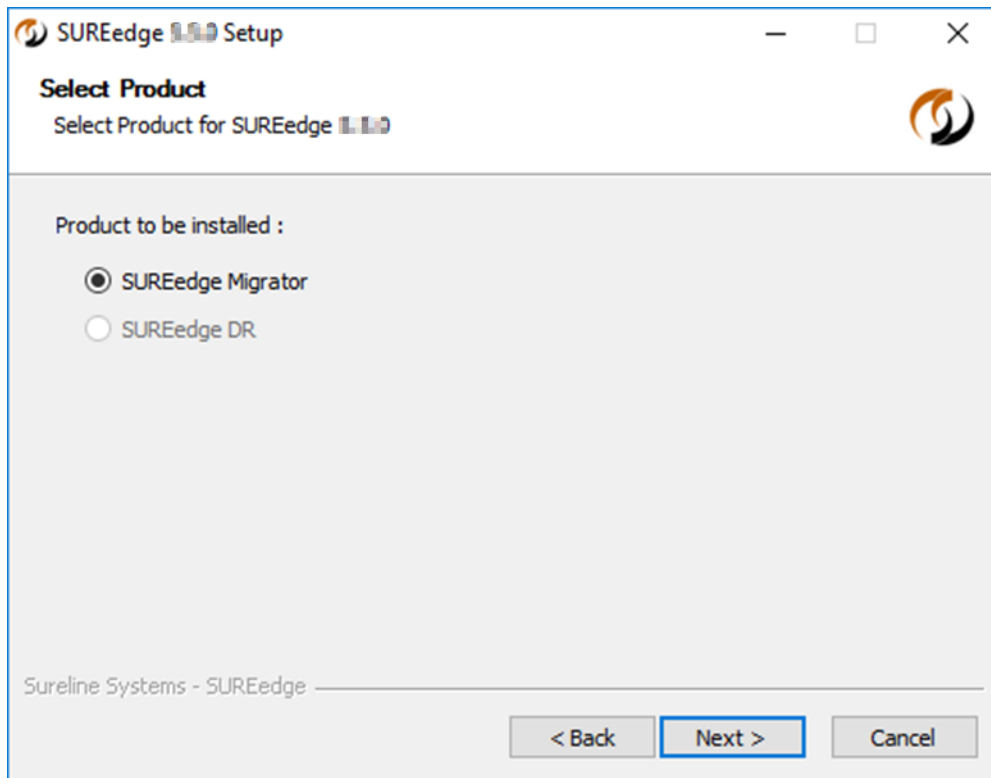
4. Click **Next** to display your *License Agreement*.



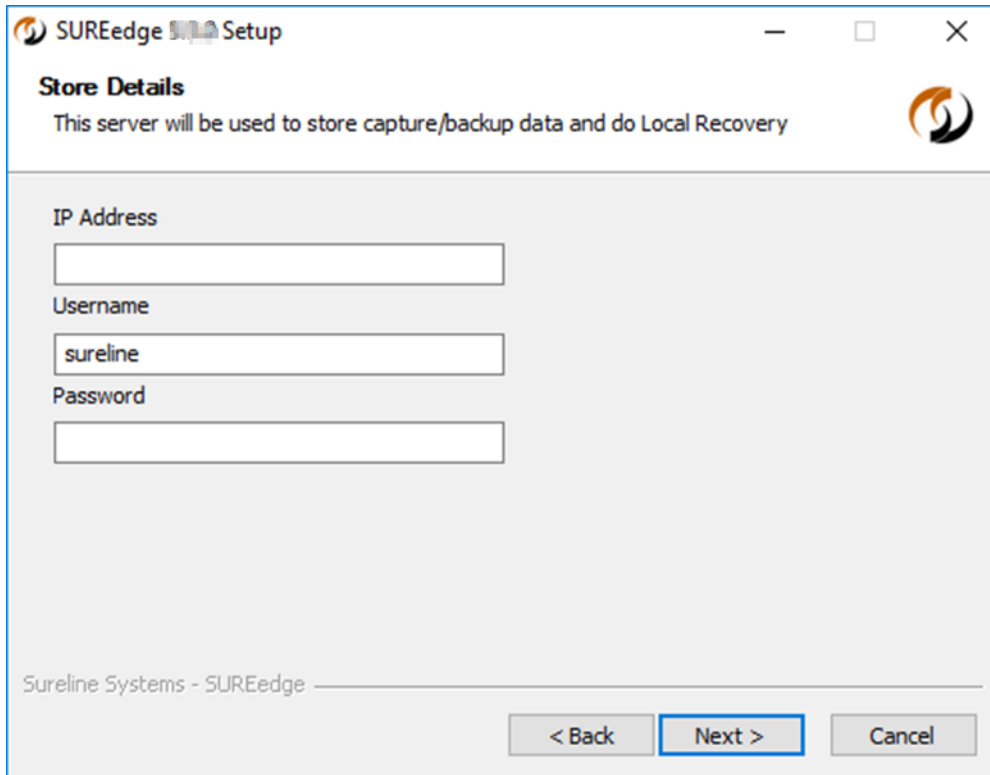
5. Please read the license agreement and click **I Agree** to continue.



6. By default, the “SUREedge Migrator” is selected.

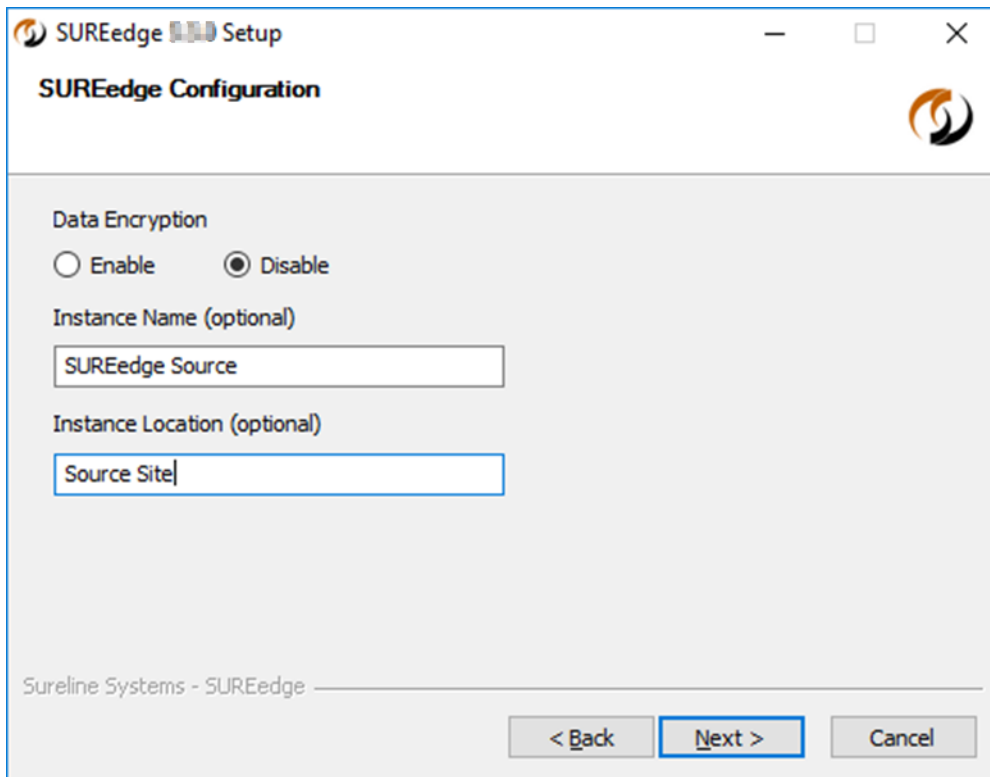


7. Click **Next** to display *Store details*.



The screenshot shows a Windows-style application window titled "SUREedge Setup". Inside the window, the "Store Details" section is active, with a subtitle stating "This server will be used to store capture/backup data and do Local Recovery". The form contains three input fields: "IP Address" (empty), "Username" (containing "sureline"), and "Password" (empty). At the bottom of the window, there is a taskbar area with the text "Sureline Systems - SUREedge" and three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

8. Provide internal IP address for store with credentials. Click **Next**. This validated the store parameters and shows screen for *SUREedge Configuration*.

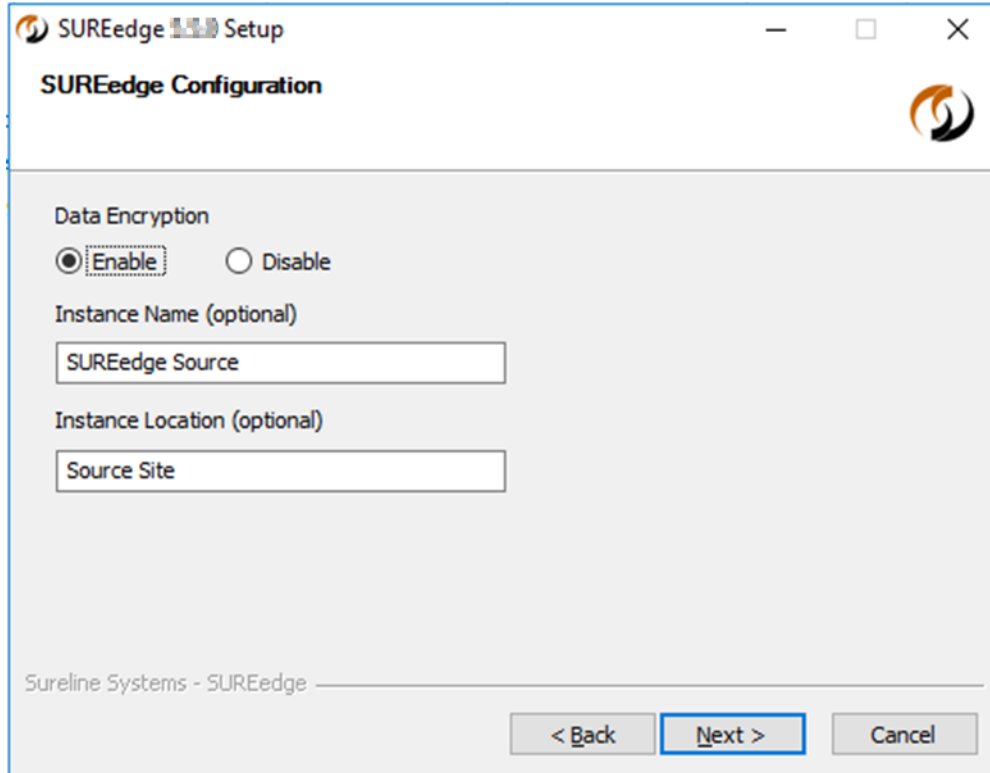


9. By default, “Data Encryption” is disabled. SUREedge Migrator can be configured to encrypt the image data that is stored and transferred across the network. Choosing “Enable” here will enable data encryption, and “Disable” will turn it off. Note that if this feature is not enabled all captured data will be stored and transferred un-encrypted. Provide **Instance Name** and **Instance Location** if needed. Click **Next** to display *Install* screen.

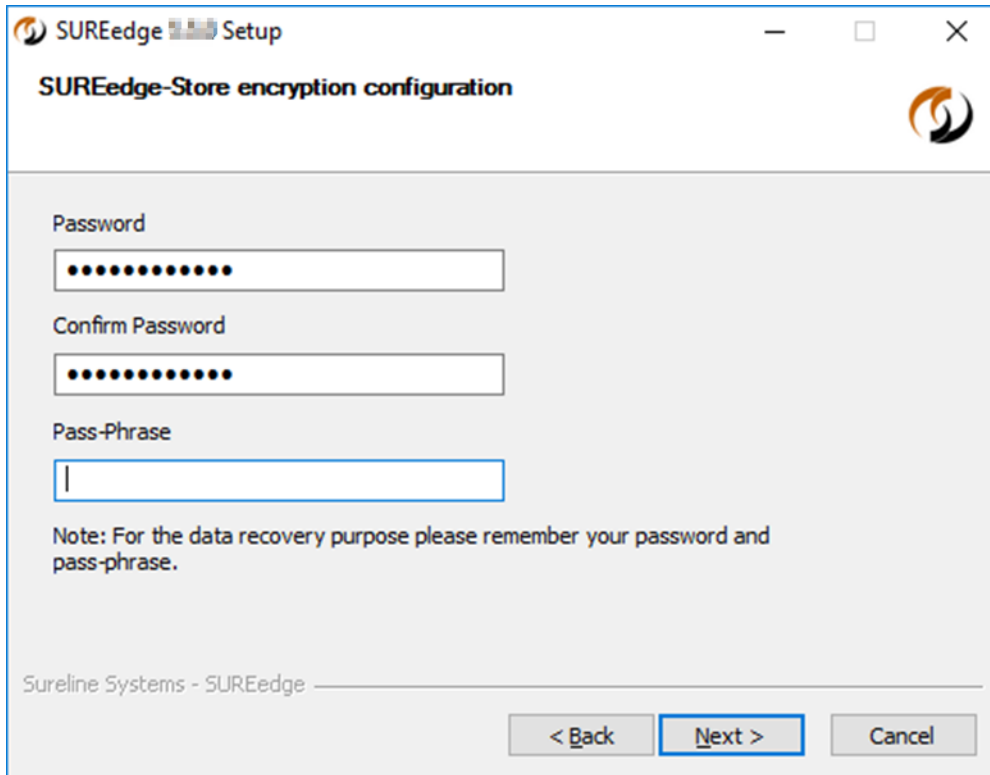


10. Select “Data Encryption” as *Enable*.

Note: Make sure to enable encryption on target site as well if you are enabling it on client side.

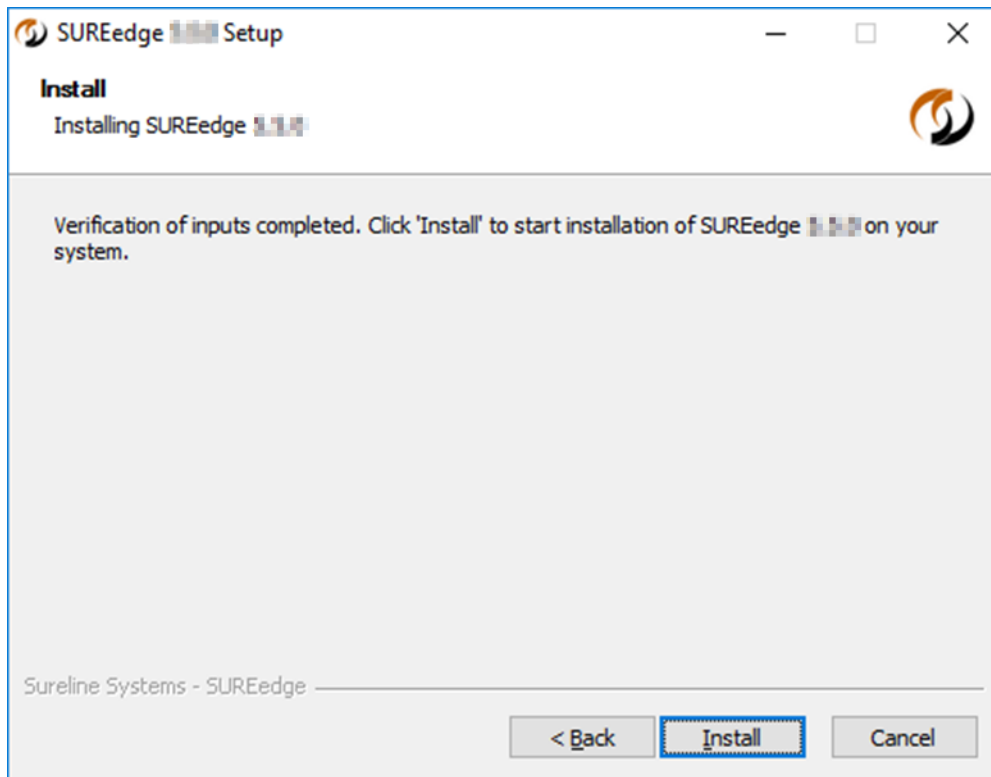


11. Provide **Instance Name** and **Instance Location** if needed. Click **Next** to display *SUREedge-store Encryption Configuration* screen.

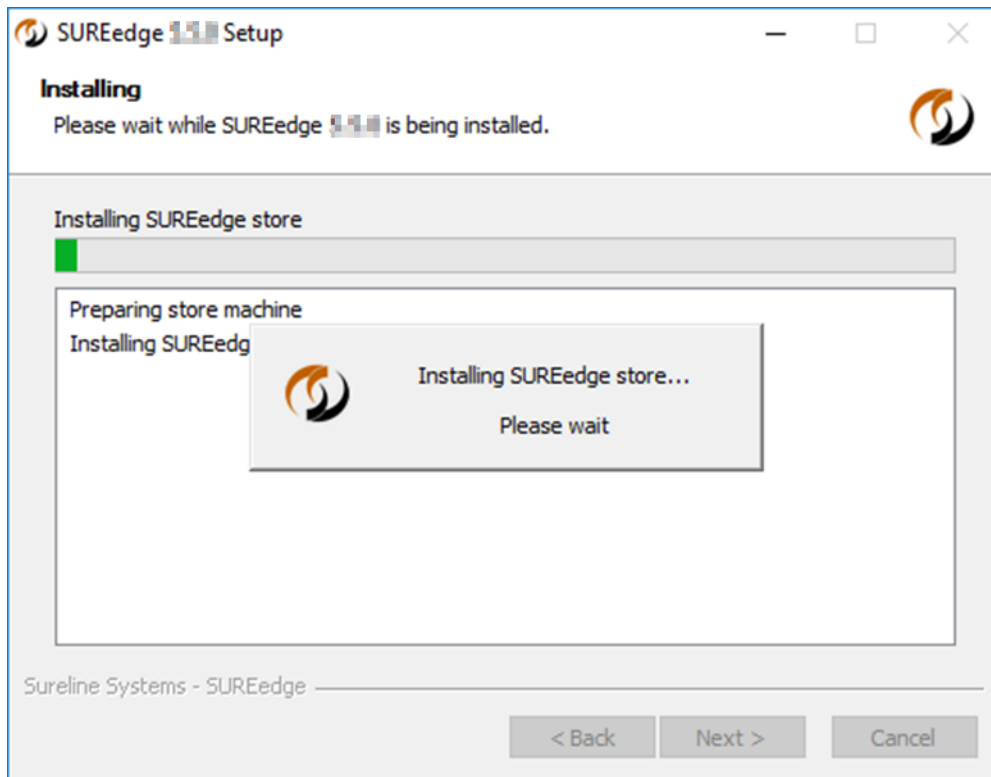


The screenshot shows a Windows-style window titled "SUREedge Setup". Inside the window, the title "SUREedge-Store encryption configuration" is displayed at the top. Below this, there are three input fields: "Password" (filled with 12 dots), "Confirm Password" (filled with 12 dots), and "Pass-Phrase" (empty). A note below the fields reads: "Note: For the data recovery purpose please remember your password and pass-phrase." At the bottom of the window, there is a status bar that says "Sureline Systems - SUREedge" and three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

12. Provide **Password**, **Confirm Password** and **Pass-Phrase** for data encryption. Remember password and pass-phrase which is required while de-crypting data.
13. Click **Next** to display Install screen.

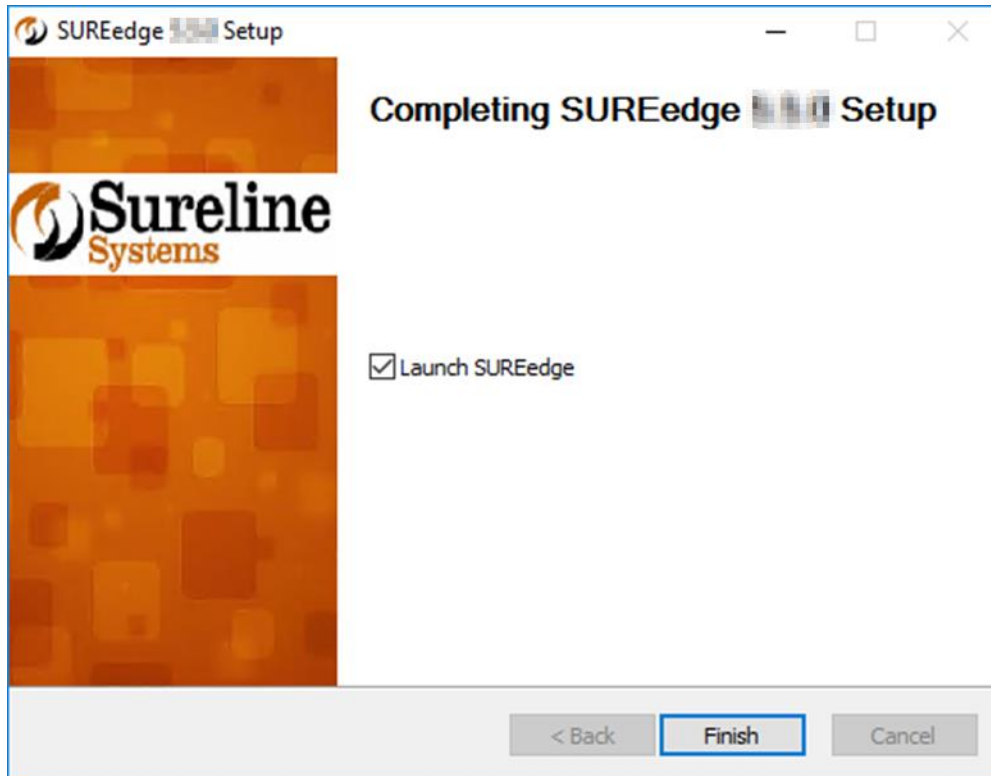


14. Click **Install** to proceed with the installation or **Cancel** to exit without installing. The time required to complete the installation will vary depending on the performance and load of the systems involved, the storage size(s) involved, etc.
15. The progress of the installation will be displayed while the install is ongoing:





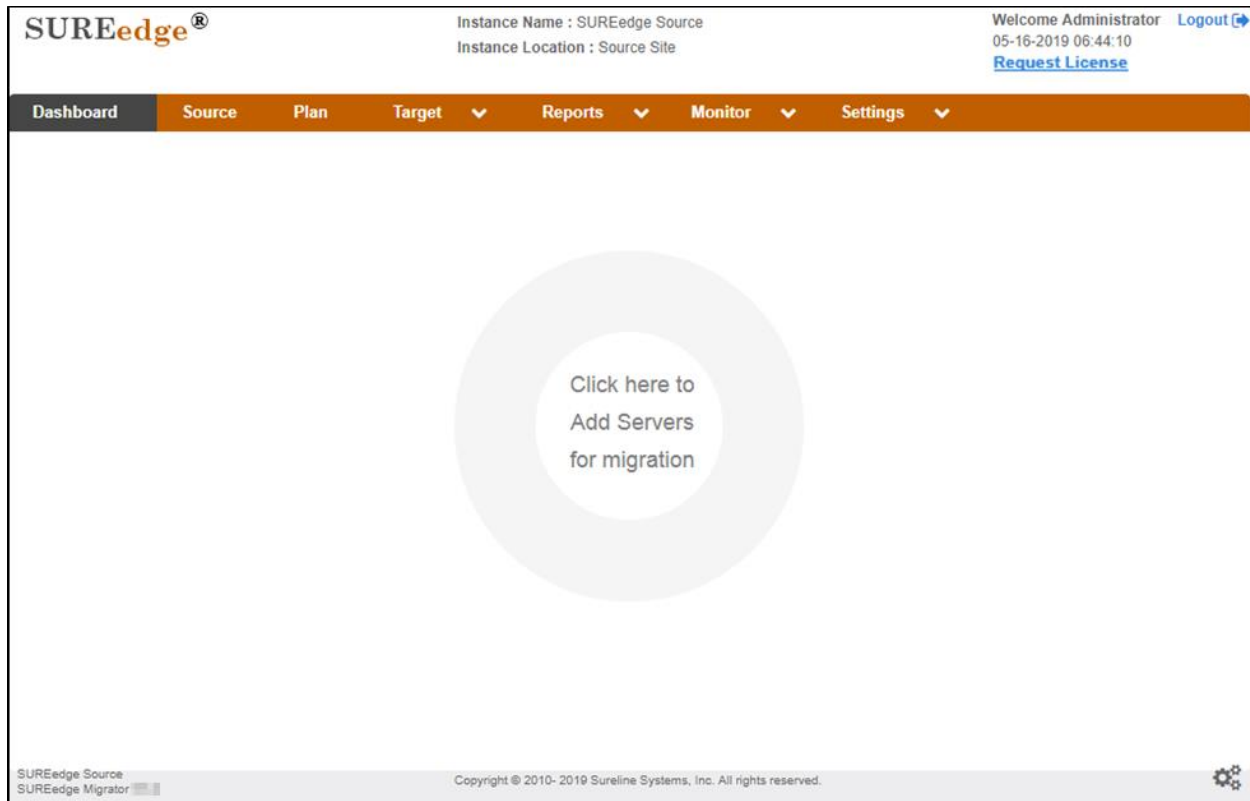
16. Once the installation is completed, click on the **Finish** button.





3 Configurations

Once installation is completed, you can launch SUREedge Migrator (<https://localhost/sureedge/index.php/>) and do various configurations as mentioned in the subsequent sections. Default home page after login displays like below:



3.1 Configuring Hypervisor

1. Login to SUREedge Migrator.
2. Go to **Settings** > **Instance**.
3. Click on **Edit** link in front of "Hypervisor configuration"
4. Select **Type** as *Windows Azure* for Hypervisor configuration popup.



Hypervisor configuration

Type : *

Windows Azure

Subscription ID : *

17a-a94d-c5af84277256

Application ID : *

373-8255-4ecb48958533

Secret Key : *

.....

Directory ID : *

3b9-bf80-8d8dc62cb3ad

Resource Group : *

sureedge550jbrg

Storage Account : *

sureline

Location : *

Central US

Account Type : *

AzureGlobalCloud

Submit

Cancel

5. Populate the data in the above screen. Refer [Getting Azure Parameters](#) section to get the parameters. For **Account Type**, select *AzureGlobalCloud*.

6. Click **Submit** to save the hypervisor configuration.



Note: After submitting the above form if hypervisor configurations are not saved, fill the form again and re-submit it. This is known issue in 5.7.0



3.2 Configuring Proxy

3.2.1 Linux Proxy Image configuration

1. Login to SUREedge Migrator Management Console (MC).
2. Go to **Settings > Instance > Proxy Image Configuration**.

Proxy Image Details			
OS Type	Image Name	User Name	Actions
windows	sureedge-windows-proxy-550	sureline	
linux	sureedge-linux-proxy-550	sureline	

3. For **OS Type linux**, from **Actions** column, click **Edit Proxy Image** icon.

Edit Proxy Image

Proxy Image Details

OS Type : *
Linux

Image Name : *
sureedge550centos7201

Username : *
sureline

Password : *
••••••••••

Submit Cancel

4. Provide Image Name as [VHD file name](#) for Linux Proxy (name without .vhd extension) and enter the credentials for Linux Proxy VM.
5. Click **Submit**.



3.2.2 Windows Proxy Image configuration

1. Login to SUREedge Migrator Management Console (MC).
2. Go to **Settings > Instance > Proxy Image Configuration**.

Proxy Image Details			
OS Type	Image Name	User Name	Actions
windows	sureedge-windows-proxy-550	sureline	
linux	sureedge-linux-proxy-550	sureline	

3. For **OS Type windows**, from **Actions** column, click **Edit Proxy Image** icon.

Edit Proxy Image

Proxy Image Details

OS Type : *

Image Name : *

Username : *

Password : *

4. Provide **Image Name** as [VHD file name](#) for Windows Proxy (name without .vhd extension) and enter the credentials for Windows Proxy VM.
5. Click **Submit**.



3.3 License Configuration

As mentioned earlier a license is not required to install SUREedge Migrator, though it will operate with reduced functionality until a license is supplied. To start the actual Migrator of systems you will need to supply a permanent license.

For a permanent license, click on “Request License” in the upper right corner of the screen. A popup will appear with instructions and all the information required to request a license.

Request License

To obtain a license please contact Sureline Customer Support at support@surelinesystems.com and provide this :

Appliance
Serial Number : A3038BFD-306A-4A55-9EC6-66F8D2142818


along with your contact information to obtain your license. Thank you!

Close

Please send the **Appliance Serial Number** to support@surelinesystems.com or please call sales (408–331-7940) to request a license. A member from our team will provide a license key via email. For detailed instructions on how to activate your license key, please see the **SUREedge Migrator User Guide**.

1. Login to SUREedge Migrator.
2. Go to **Settings > Instance**.
3. Click on **Edit** link in front of “SUREedge license configuration”





Instance Name : SUREedge

Welcome Administrator
02-27-2019 04:57:00
Licenses Used : 7 of 20

Dashboard
Source
Plan
Target
Reports
Monitor
Settings

Configuration	Action
SUREedge license configuration	Edit
SUREedge-Store network configuration	Edit
SUREedge-MC network configuration	Edit
SUREedge-Store encryption configuration	View
Recovery Host network configuration	Edit
Enable/Disable Upload to Cloud	Edit
Image Caching configuration	Edit
Number Of Parallel Capture Jobs	Edit
Number Of Parallel Recovery / Image Caching Jobs	Edit
Hypervisor configuration	Edit
Hypervisor Share Configuration	Edit
Cloud Transfer Bandwidth Throttling	Edit
SUREedge Instance Name	Edit
SUREedge Instance Location	Edit

- Click on **Choose File** button to browse the license file location. Select the license file.

SUREedge License

Click the choose file button below to select a license to upload.

File path : *
[Choose File](#)

No file selected.

Click on **Submit**.



4 Contacting Support

The Sureline Systems website (<http://www.surelinesystems.com>) provides a support page where you can submit your issues. A ticket will be generated automatically and the support team will contact you.

Email us:

Alternatively, you can write an email to support@surelinesystems.com with a detailed description of the issue. This will automatically create a support ticket, and a member of our customer support team will reach out to you soon after.

Telephone Support:

You can also contact us directly on this number **408-331-8750**, if you wish to speak with a Sureline Systems Engineer directly.