Persistent

SUREedge® DR 6.6.1

Manual Installation Guide for GCP

Legal Notices

Warranty

The only warranties for products and services are set forth in the express license or service agreements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty of any kind, implied, statutory, or in any communication between them, including without limitation, the implied warranties of merchantability, non-infringement, title, and fitness for a particular purpose. Accelerite shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from Accelerite or its licensors required for possession, use or copying. No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Accelerite.

Copyright Notices

Trademark Notices

Accelerite and Persistent are trademarks or trade name or service mark or logo of Accelerite/Persistent. All other brands or products are trademarks, trade name, service mark, logo or registered trademarks of their respective holders/owners thereof.

Disclaimer

The SUREedge products are available and support only the English language.

Table of Contents

Introduction

Welcome to SUREedge DR! Data migration can be a lengthy and difficult, although a necessary, process. SUREedge®DR is a proven enterprise-class Disaster Recovery solution that simplifies DR Testing and DR, taking advantage of the Cloud as a ready-to-use DR infrastructure. SUREedge DR enables enterprises to implement a Disaster Recovery solution locally, at a remote site, in the Cloud, or even all three. Customers can start with local DR and seamlessly expand to a remote site or the Cloud by deploying a SUREedge instance at the target site. With SUREedge-DR's Any-to-Any Recovery capability, you can recover physical and virtual systems (any hypervisor) to an alternate hypervisor or your preferred Cloud. This flexibility allows you to avoid hardware, hypervisor, and Cloud lock-ins.

Deployment Scenarios

SUREedge® DR supports many different deployment configurations to meet the needs of various situations:

- **Cloud-targeted DR**: The cloud is leveraged as a failover site for on-premise workloads or workloads in another cloud.
- **Site-to-site DR**: The source and target environments are non-cloud based.
- **Intra-cloud DR**: The goal is to protect against unavailability due to loss of resources in or connectivity to a region or zone within a public or private cloud.
- **Cloud-to-site DR:** Reverses the cloud-targeted scenario and uses a non-cloud, on-premises virtualization environment to protect cloud-based workloads.

In all these scenarios an instance of SUREedge DR is deployed in each of the source and target environments. The source SUREedge DR instance is responsible for capturing images of the protected systems and efficiently transferring them to the target instance. The target SUREedge DR instance receives and manages the system images and orchestrates the transformation and instantiation process when recoveries are performed.

Installation Overview

To set up an environment for Backup and Disaster recovery you first determine the location(s) where SUREedge DR should be installed according to the scenarios described above. You can then:

- Obtain the required documentation and software for the environment(s) you have identified. You should have an **Install Guide** (this document) for each environment and, if required, the software packages for installing SUREedge DR in those environment(s).
- Perform the installation of SUREedge DR software as instructed using the **Installation Guide**.
- License and configure SUREedge DR as appropriate for each environment as described in the **Installation Guide** and **User Guide**.

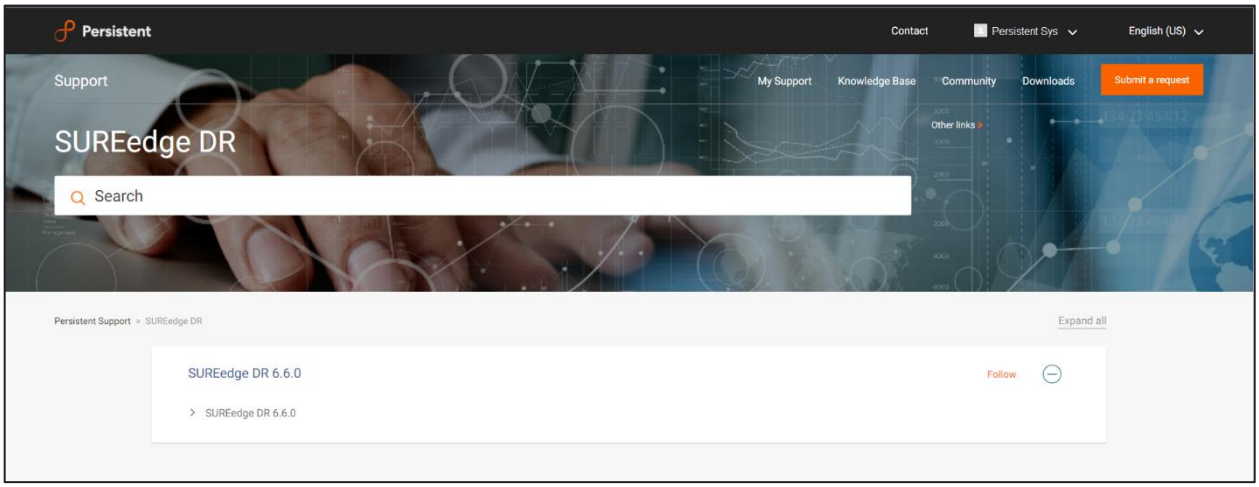
This Installation Guide covers the steps necessary for installing an instance SUREedge DR in a GCP environment. The following sections will take you through the steps to obtain installation materials and to install, license and configure SUREedge DR to run in a GCP environment. You can then use the **User Guide** to configure and start using SUREedge DR for Backup and Recovery.

Installing SUREedge DR

SUREedge DR installers, tools and documentation are all available online for download or deployment. The next sections will detail you to obtain the documentation and software binaries you will need to get started with SUREedge DR.

Downloading SUREedge DR Installer

You can download the installation media from the Accelerite portal using the following URL:
https://support.accelerite.com/hc/en-us/categories/4411552394381
You will need an Accelerite account to access the SUREedge DR Installer. If you do not have an Accelerite account, please click on **Submit a request**. After request is approved, you will have access to the download area:

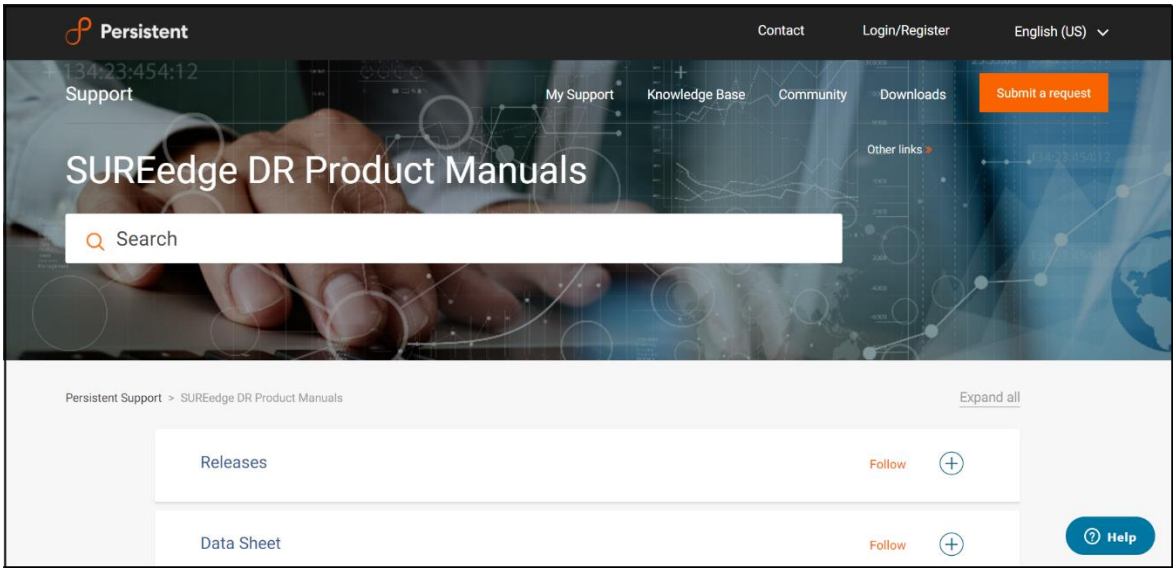


Select the **software version** you wish to install from the list, then click **Download** to start your download.

Obtaining Documentation

SUREedge DR documentation is available for download as PDF files from the Accelerite. To get access to SUREedge DR documentation, navigate to this URL in your browser:
https://support.accelerite.com/hc/en-us/categories/4410194460941-SUREedge-DR-Product-Manuals
You will need an account to log in and access the SUREedge DR documentation. If you are a new user, please click on **Login/Register**. After the request is approved, you can access the

documents:



Select the **Releases** section and then click the software version; then locate document you wish to download and click the **PDF** button.

Prerequisites

To create virtual machines in the target project(s) where recovered servers will be relocated SUREedge DR needs to perform operations using a service account with sufficient permissions and have network access to the new virtual machines. This requires that the necessary APIs be enabled for the project(s) where VMs will be recovered and the availability of a service account with the appropriate roles and permissions enabled. You must also make sure that the virtual networking for the project(s) is configured such that for the duration of the recovery operation the recovered VMs can be reached by the SUREedge DR instance that you deploy.

The following sections describe the specifics of these prerequisites and how to meet them.

Accounts and Privileges

To be able to make the cloud API calls required to create the cloud-side virtual machines and transform them to run in the cloud SUREedge DR needs the project to have the necessary APIs enabled and a service account with the appropriate permissions. Persistent provides a script that you can use to make the process of creating the roles and enabling the APIs easier. The details of required APIs, roles and permissions are outlined in Section 4, “Required APIs, Roles and Permissions”.

Networking Configurations

SUREedge DR uses Google Cloud Virtual Private Cloud (VPC) networks and requires specific networking firewall rules to be configured for deployment and recovery of workloads. This section describes networking requirement and firewall rules needed for deployment.

All projects where VMs will be recovered must be reachable by the SUREedge DR instance; if multiple projects are involved, then this will require a Shared VPC. (Note: Legacy networks are not supported.) Any project can host the Shared VPC with the remaining projects attached. In the case where all recovered systems are going into a single project then the SUREedge DR instance should be deployed there and the default VPC for the project can be used.

Configuring Firewall rules

To create and transform servers being recovered in GCP the SUREedge DR instance must be able to communicate with the VMs being created in the cloud. To allow this any firewalls between the SUREedge DR instance and the projects that will contain the recovered VMs must allow the following network communications:

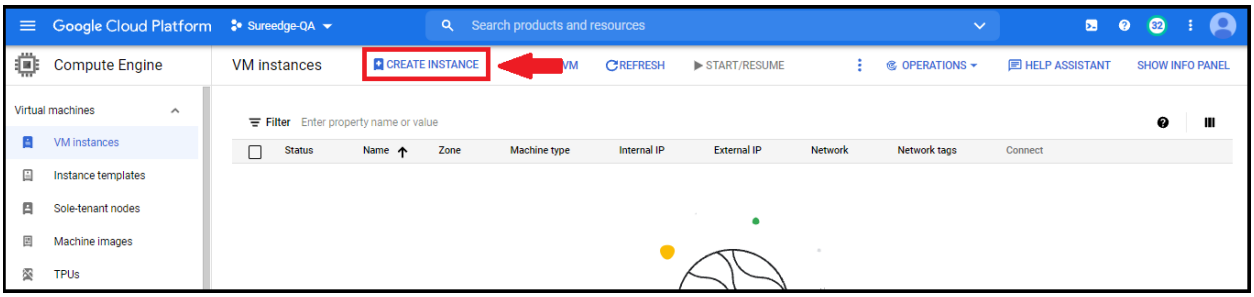
- **ICMP**: Firewalls must allow ICMP packets to be passed between the SUREedge DR instance and the target projects and networks.
- **TCP**: Ports 22, 25025, 25026, 25027, and 25028 must be open between the SUREedge DR instance and the target project networks.
- **TCP**: Ports 80 and 443 are used to access the SUREedge DR UI and must be open between the SUREedge DR MC VM and any systems where a browser will be used to access the DR UI.

Deploying SUREedge DR

This section contains the instructions for deploying SUREedge DR on the Google Cloud Platform. The below steps help you to create Store and MC on GCP.

Create Store VM

1. Login to GCP and navigate to the **Compute Engine** (https://console.cloud.google.com/) and click the **VM Instances.**
2. Select **Create Instance** on the top pane. The VM manual deployment setting page opens:



3. Enter **Name** of VM in the format as **“**sureedge-dr-linux-vm- followed by the string of user choice”.
   For Example: sureedge-dr-linux-vm-test
4. Choose **Region** and **Zone** from the drop-down list.

5. In machine configuration setting Choose **Machine Type** as a **e2-standard-4 (4 vCPU, 16 GB memory)** from the drop-down list.
6. In Boot Disk Section, select the **Operating system** as an **Ubuntu, Version** as an **Ubuntu 20.04 LTS, Boot disk type** as a **Standard Persistent disk**, and add disk **Size** according to the requirement.
7. In the Identity and API access section, choose **Service account** from the drop-down list.
8. In Networking Section, add the **Network tags** if required. choose **Network Service Tier** as a **Standard (us-central1**) from the selection.
9. In the Disks section select, **ADD NEW DISK** fill in the below details:

- Enter disk **Name** as per format for example: sureedge-dr-linux-(Name for your understanding).
- Select **Disk source type** as a **Blank disk** from the drop-down list.
- Select **Disk setting** as **Standard persistent disk** from the drop-down list.
- Enter the disk **Size** in GB as per requirement.

  Note: The minimum disk size is 1024 GB.
- Click **SAVE** to make changes permanent.

10. Select **CREATE** to create store VM.

Create User

1. Connect to deployed VM using SSH and run the following commands to create a user:
   `sudo adduser sureline`
2. Enter a **New Password** for the user.
   Note: remember or note down this password to configure into the Sureedge management console (MC).
3. Run the following commands to complete the setup:
   `/etc/sudoers`
   `sureline ALL=NOPASSWD: ALL`
   `Defaults:sureline !requiretty`

   Password authentication
   `$sudo vi/etc/ssh/sshd_config`
   Change `passwordauthentication= yes`”

   Restart SSH
   `$sudo /etc/init.d/ssh restart`

Upload Packages

1. SSH to the store using public IP of VM store VM (Go to VM instances and select store VM which is created above).
2. Upload the following Package to `/home/sureline` directory of the store VM:

- surestor-prereq-installer.tar.gz
- surestor-installer-scripts.tar.gz
- surestor-installer.tar.gz

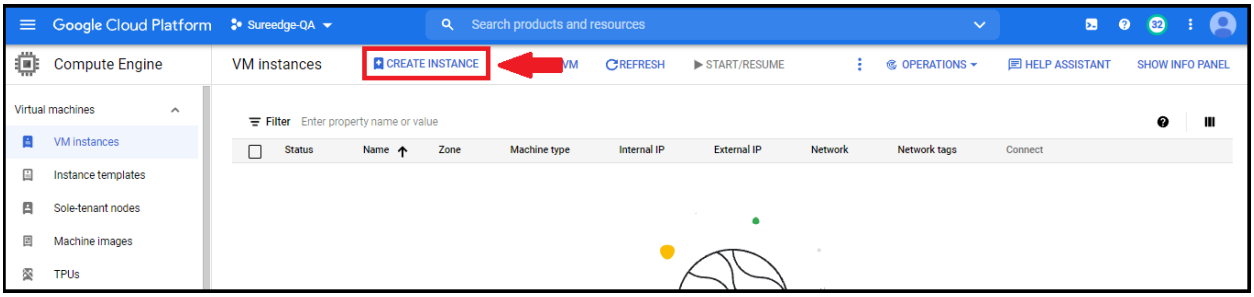
  Note: Refer the Downloading SUREedge DR Installer section to download the installer files.

Installation

1. Connect to deployed vm using SSH and run following commands:
   ```
   tar -xzvf surestor-prereq-installer.tar.gz -C/

   sudo 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 GCP
   ```
2. The installation progresses and once the installation is completed run the following commands:
   ```
   cd ~
   sudo bash store_prepare_sure.sh GCP


   sudo bash store_installer.sh
   ```
3. Make sure `/sure and /sure/db` partitions are mounted.
4. Verify store installation by running below command:
   ```
   sudo systemctl status surestor
   ```

Create Management Console (MC)

1. Login to GCP and navigate to the **Compute Engine** (https://console.cloud.google.com/) and Click the **VM Instances.**
2. Select **Create Instance** on the top pane. The VM manual deployment setting page opens:

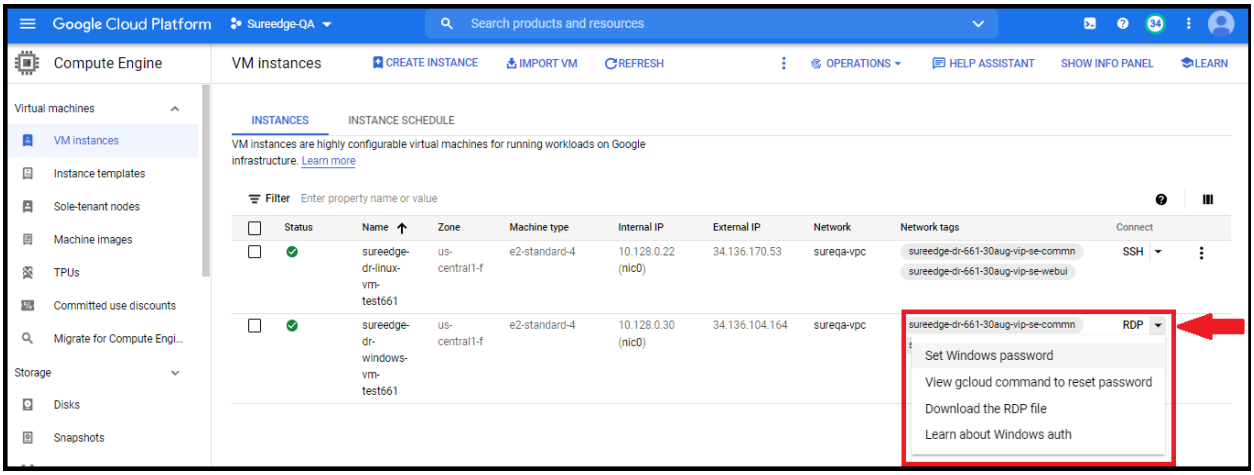


3. Enter **Name** of VM in the format as “sureedge-dr-windows-vm- followed by the string of user choice”.
   For Example: sureedge-dr-windows-vm-test
4. Choose **Region** and **Zone** from the drop-down list.
5. In the machine configuration setting choose **Machine Type** as a **e2-standard-4 (4 vCPU, 16 GB memory)** from the drop-down list.
6. In the Boot Disk Section, select the **Operating system** as a **Windows, Version** as a **Windows Server 2019 Datacenter, Boot disk type** as a **Standard Persistent disk**, and add disk **Size** according to the requirement.
7. In the Identity and API access section, choose **Service account** from the drop-down list.
8. In the Networking Section, add the **Network tags** if required. Choose **Network Service Tier** as a **Standard (us-central1**) from the selection.
9. Select **CREATE** to create a management console VM.
10. Select **EDIT** on the top pane and find the Custom metadata option.
    Enter the following values and click **Save**.

Parameter (key)	**Value**
storeVMName	Enter the linux store name For Example: sureedge-dr-linux-vm-test
mcVMName	Enter windows mc name For Example: sureedge-dr-windows-vm-test

Create User

1. Select the Management Console VM and click **RDP** choose **Set Windows password** from drop-down list. Set new Windows password window opens.



2. Enter **Username** for the windows VM. Select **Set**. The new windows password window shows the **Password** for the windows VM.

   Note The password will appear once save and secure properly.

Upload Package

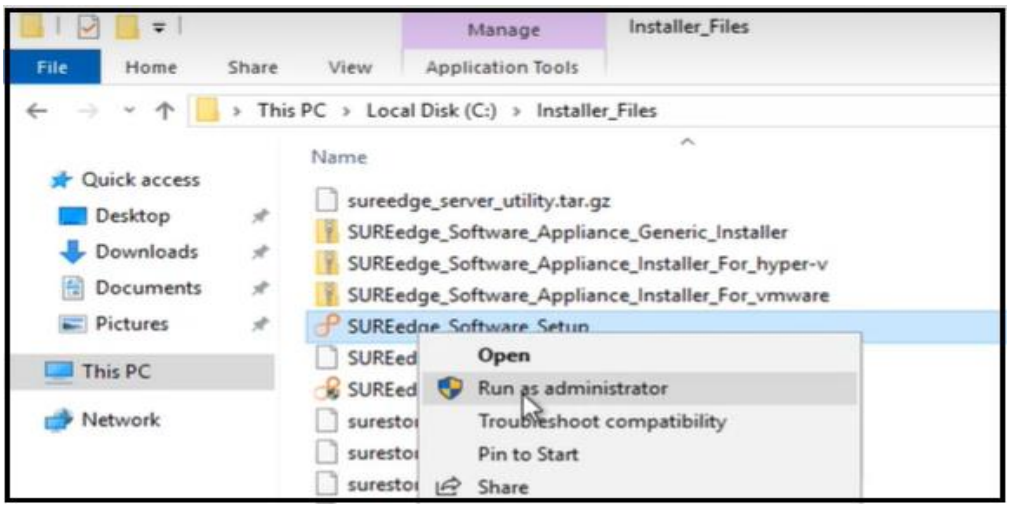
Connect to deployed VM using RDP and copy the below packages that are available with installer zip.

Note: Refer the Downloading SUREedge DR Installer section to download the installer files.

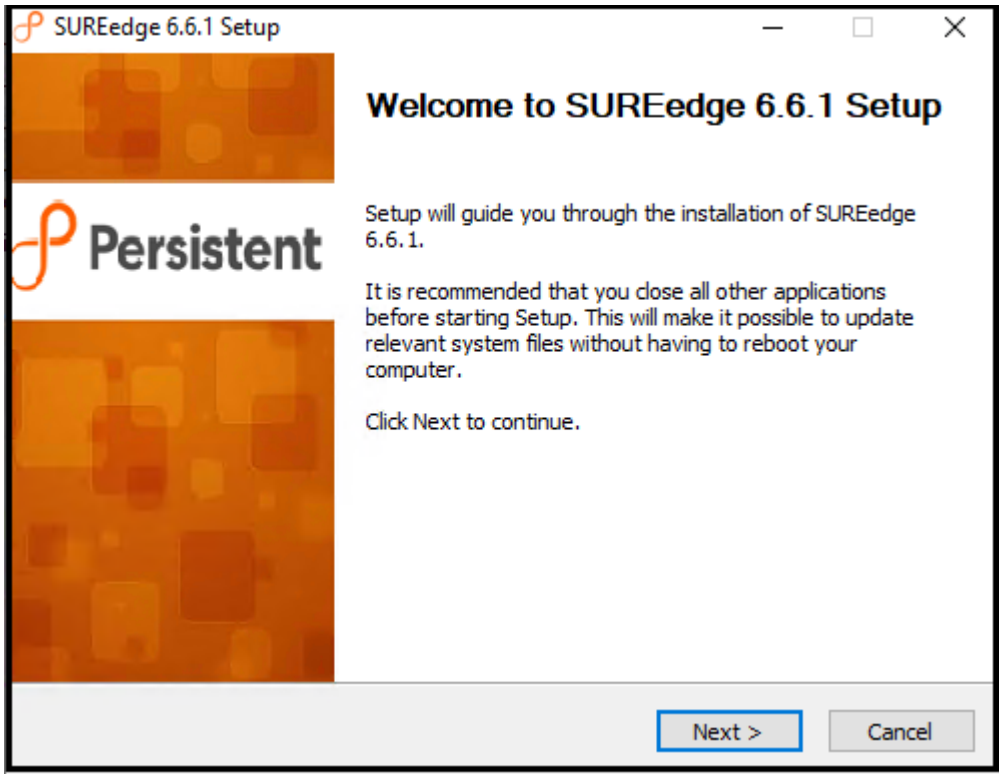
- SUREedgeServerUtility.exe
- SUREedge_Software_Setup.exe
- SUREedge_Storage_engine_system. image
- Version
- SUREedge_Software_Appliance_Generic_Installer.zip
- SUREedge_Software_Appliance_Installer_For_vmware.zip
- SUREedge_Software_Appliance_Installer_For_hyper-v.zip

Installing SUREedgde DR

Once the GCP installer is downloaded and extracted, your GCP server is ready and has the required pre-requisites installed/allocated the SUREedge DR software can be installed. Copy or download the SUREedge DR installer package for GCP and your license key to the GCP server where it is to be installed and right click on the installer and select **Run as Administrator** for Installation:

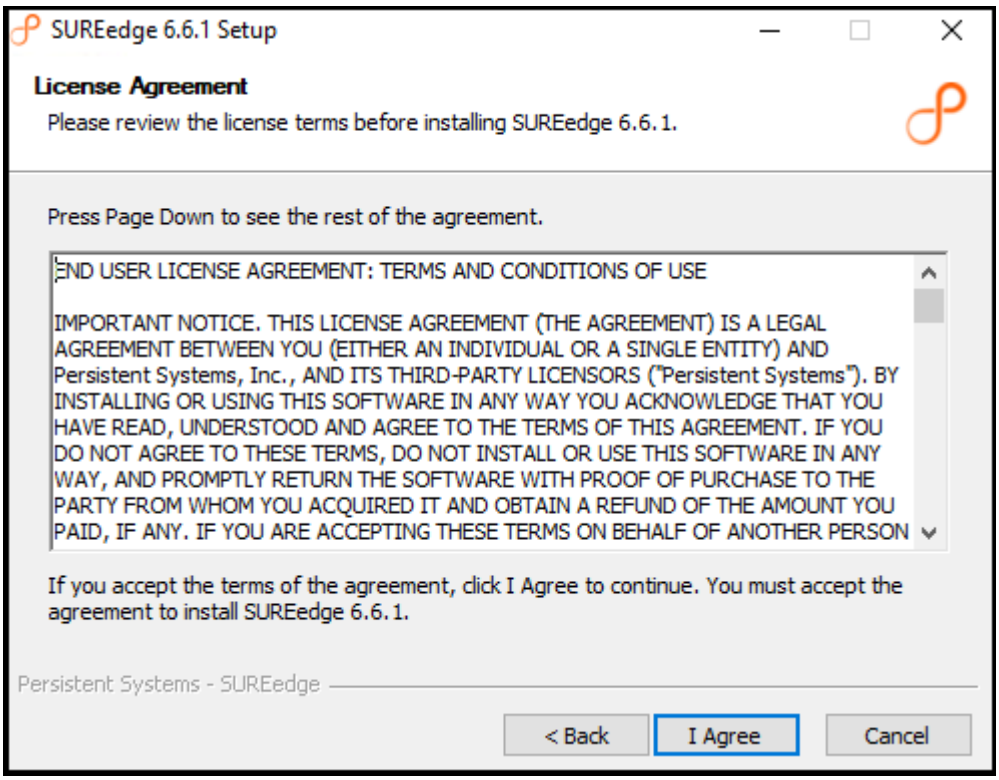


1. The first screen you'll see is a welcome screen:



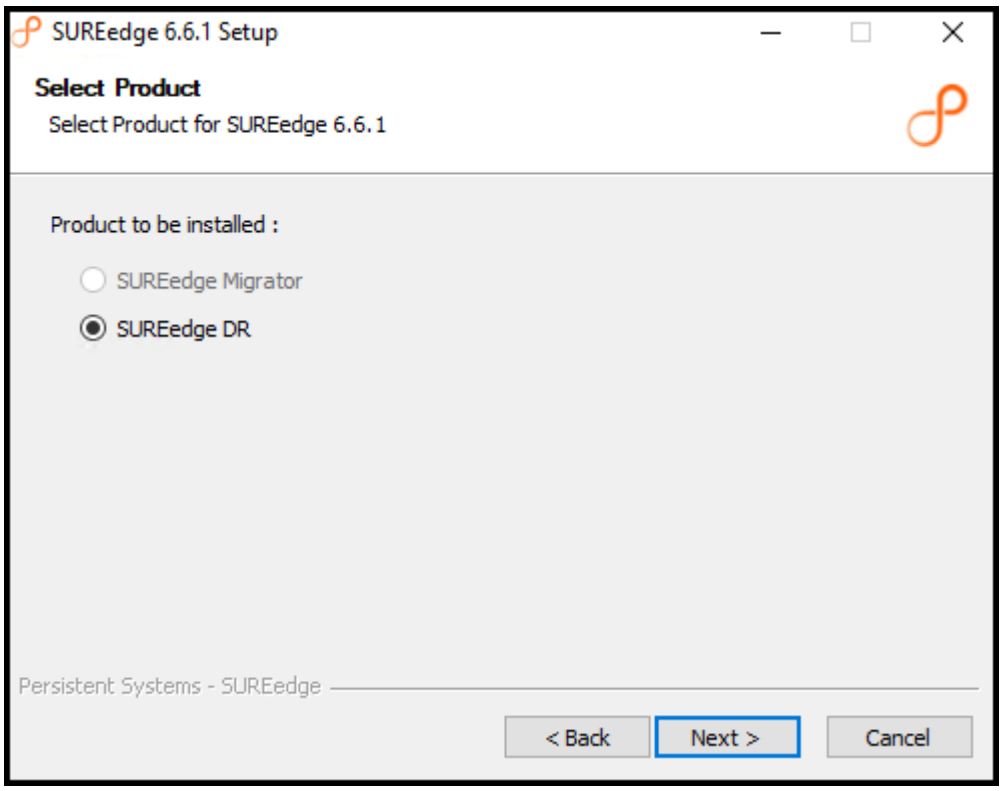
Click **Next** to continue.

2. Read the license agreement and click **I Agree** to continue.

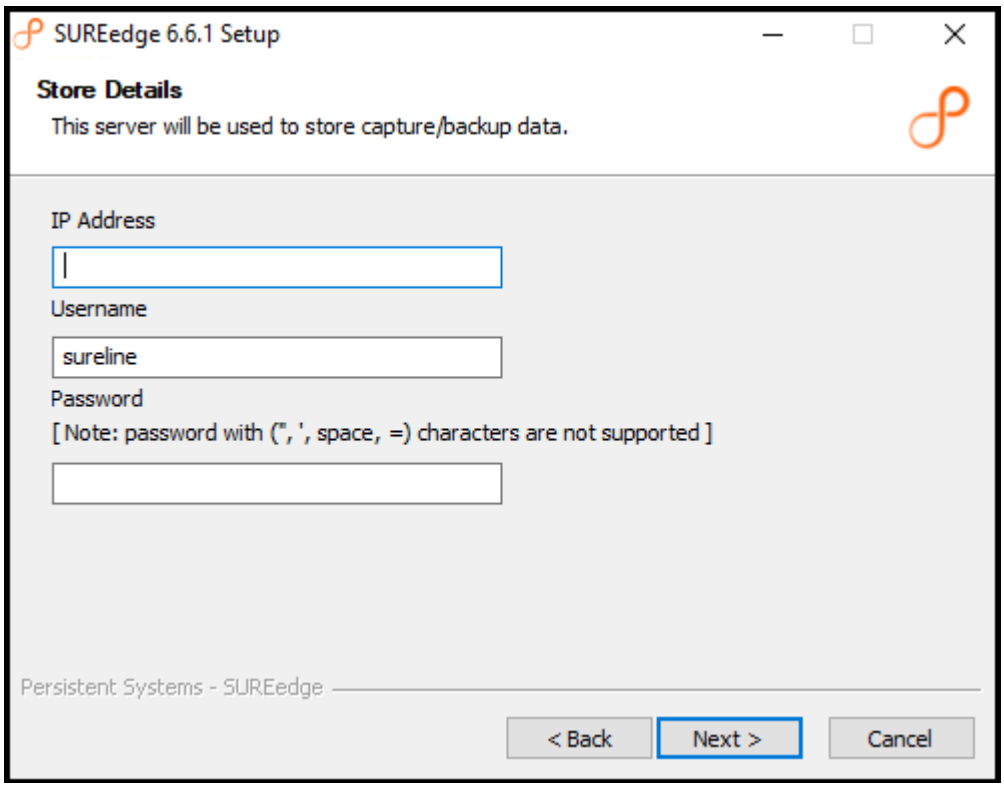


3. On the next screen, select the product to be installed and click **Next** to continue:

   By default, the “SUREedgeDR” is selected.



4. Specify details about Store Details and click **Next**:



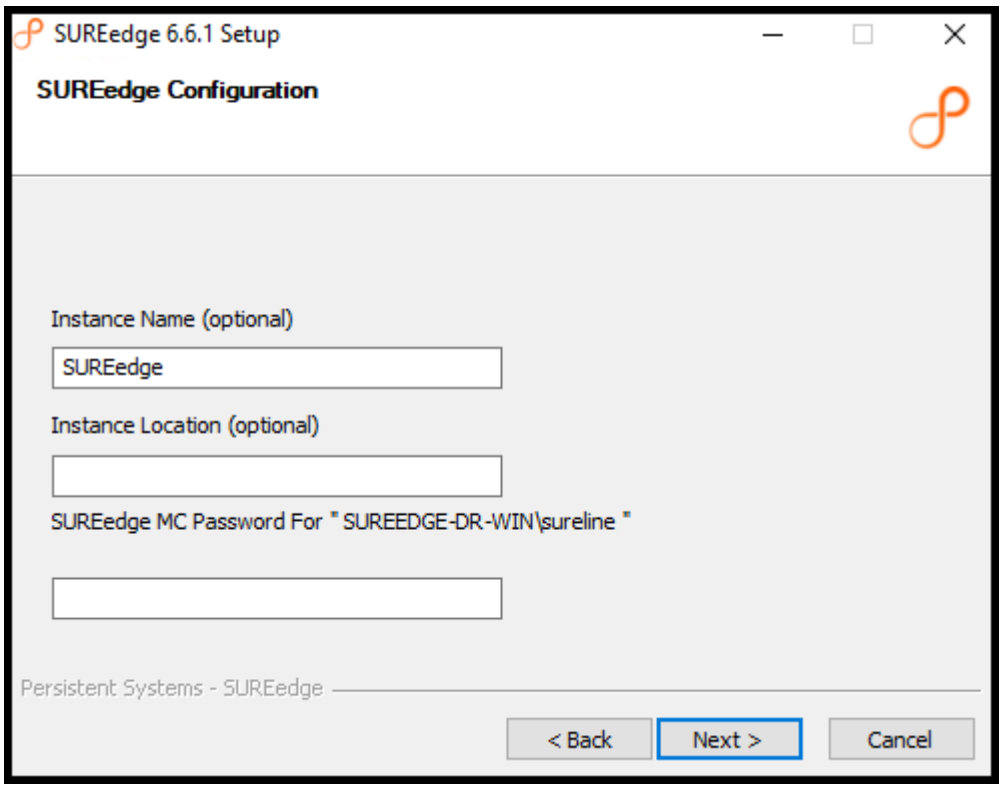
The fields should be filled in as follows:

\ **IP Address**: The IP address of the linux store VM will be filled in (10.128.0.44 in this example) and normally does not need to be changed.

Note: Enter store internal IP address.

\ **Username and Password**: Specify the credentials for the Store account under which SUREedge DR will perform operations.

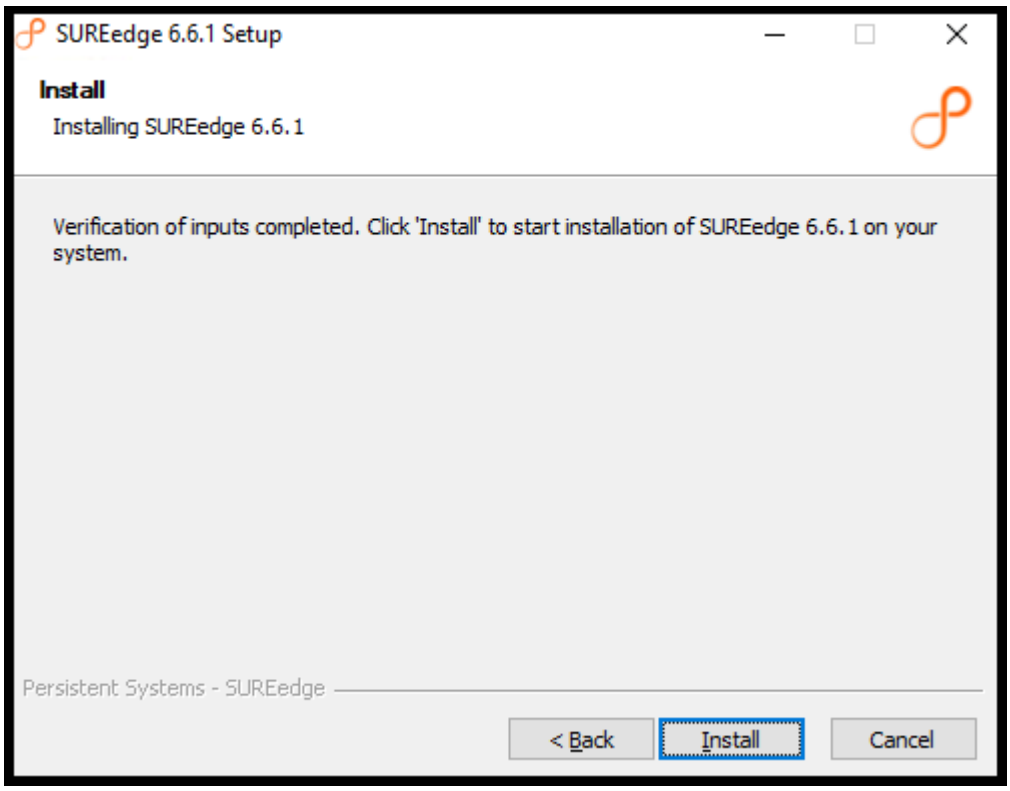
5. Enter SUREedge configuration details and click **Next**:



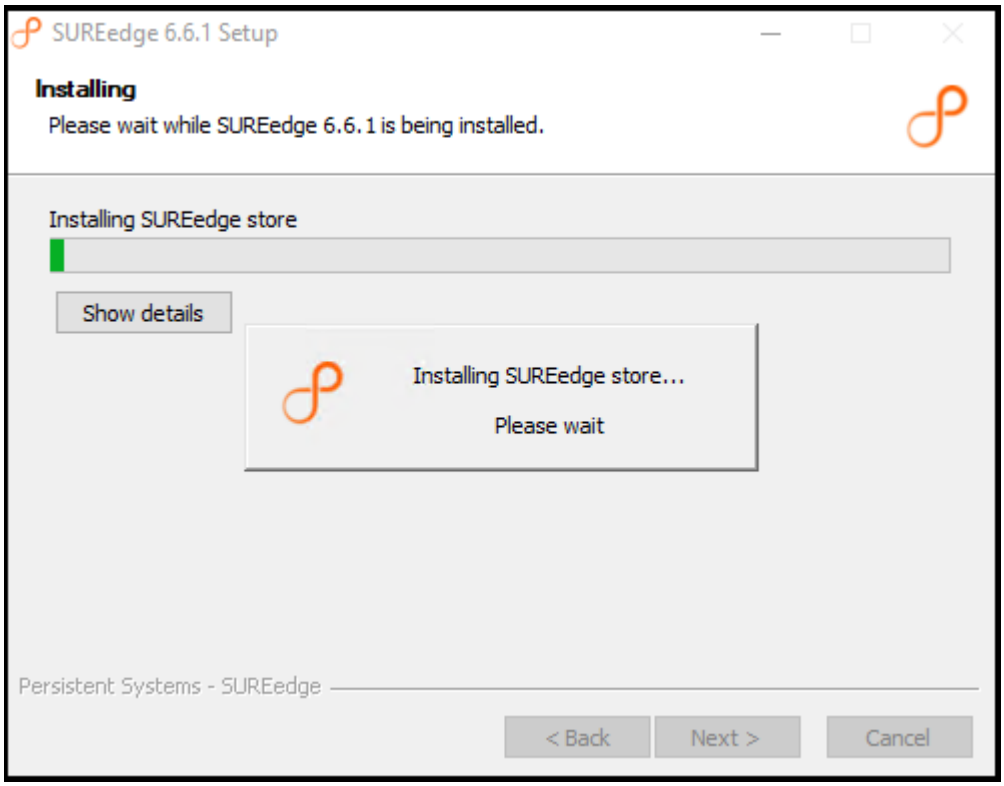
The fields should be filled in as follows:

- **Instance Name**: Enter the Instance name and Its optional field (For Example: SUREedge as shown in example)
- **Instance Location**: Enter the Instance location and its option field.
- **SUREedge MC Password**: Enter the windows MC password.

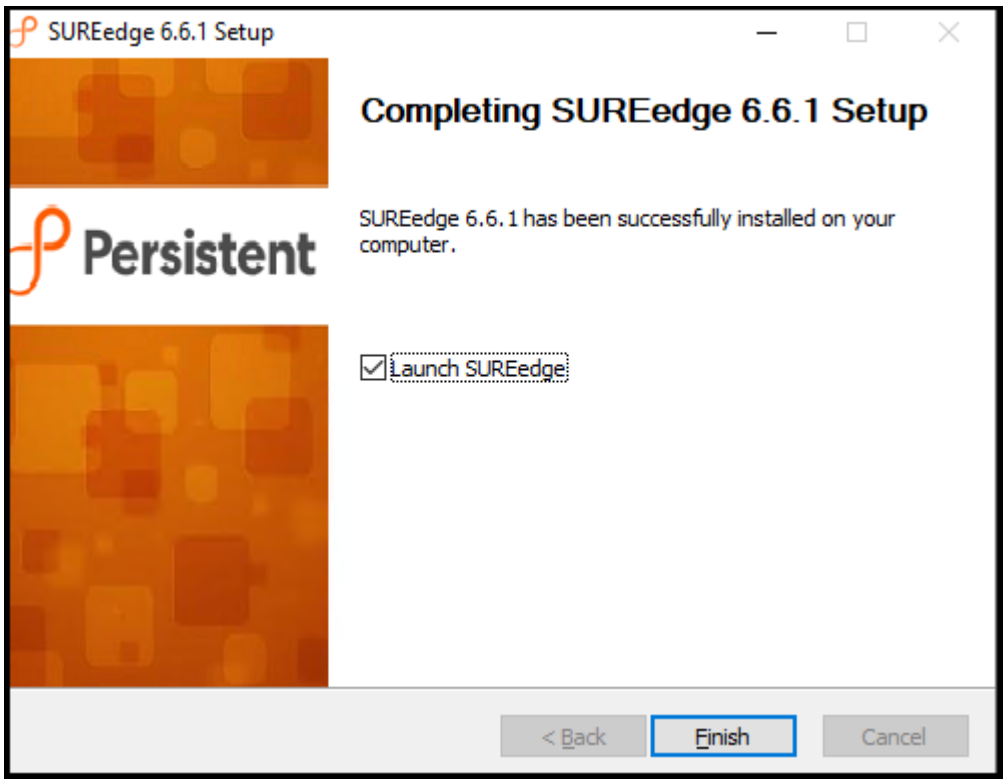
6. The next screen is the final confirmation that you wish to continue with the installation process:



Click **Install** to proceed with the installation or **Cancel** to exit without installing.
The time required to complete the installation is depend on the performance, load of the system and storage size(s) involved.



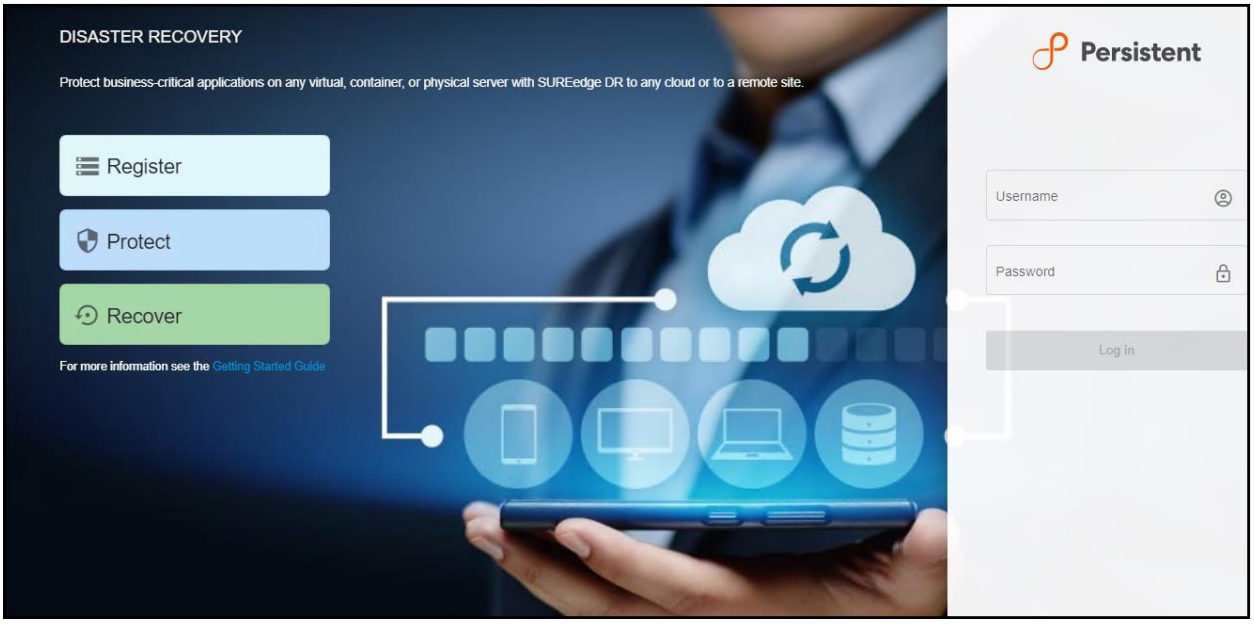
Once the installation is finished, you can see the completion screen:



7. Click on **Finish** to complete the installation.

SUREedge DR is now installed on the system. To connect to the SUREedge DR user interface, open a Google Chrome web-browser window and type the name or IP address of the Windows SUREedge Management Console (MC) component have been just installed.

You can now log into the DR user interface using the credentials that you specified during the installation. It displays a login screen:



You are now all set to start backing up your servers and applications using **SUREedge DR**. Refer to the **SUREedge DR User Guide** for the next step to **Backup** and **Restore** your servers.

Required APIs, Roles and Permissions

SUREedge DR requires that certain APIs can be used within the project(s) where VMs will be recovered and needs a service account with the appropriate roles and permissions enabled. The APIs, roles and required permissions are listed in the table below:

Required Project APIs		
iam.googleapis.com	cloudresourcemanager.googleapis.com	logging.googleapis.com
compute.googleapis.com	storage-component.googleapis.com	monitoring.googleapis.com
Required Roles		
iam.serviceAccountUser	logging.logWriter	roles/monitoring.metricWriter
roles/monitoring.viewer		
Required Permissions		
compute.addresses.create	compute.addresses.createInternal	compute.addresses.delete
compute.addresses.deleteInternal	compute.addresses.get	compute.addresses.list
compute.addresses.setLabels	compute.addresses.use	compute.addresses.useInternal
compute.diskTypes.get	compute.diskTypes.list	compute.disks.create
compute.disks.delete	compute.disks.get	compute.disks.list
compute.disks.setLabels	compute.disks.update	compute.disks.use
compute.disks.useReadOnly	compute.disks.createSnapshot	compute.images.get
compute.images.list	compute.images.useReadOnly	compute.snapshots.create
compute.snapshots.delete	compute.snapshots.useReadOnly	compute.instances.attachDisk
compute.instances.create	compute.instances.delete	compute.instances.detachDisk
compute.instances.get	compute.instances.getSerialPortOutput	compute.instances.list
compute.instances.reset	compute.instances.setDiskAutoDelete	compute.instances.setLabels
compute.instances.setMachineType	compute.instances.setMetadata	compute.instances.setMinCpuPlatform
compute.instances.setScheduling	compute.instances.setServiceAccount	compute.instances.setTags
compute.instances.start	compute.instances.startWithEncryptionKey	compute.instances.stop
compute.instances.update	compute.instances.updateNetworkInterface	compute.instances.updateShieldedInstanceConfig
compute.instances.use	compute.licenseCodes.get	compute.licenseCodes.list
compute.licenseCodes.update	compute.licenseCodes.use	compute.licenses.get
compute.licenses.list	compute.machineTypes.get	compute.machineTypes.list
compute.networks.get	compute.networks.list	compute.networks.use
compute.networks.useExternalIp	compute.nodeGroups.get	compute.nodeGroups.list
compute.nodeTemplates.list	compute.projects.get	compute.regionOperations.get
compute.regions.get	compute.regions.list	compute.subnetworks.get

compute.subnetworks.list	compute.subnetworks.use	compute.subnetworks.useExternalIp
compute.zoneOperations.get	compute.zones.get	compute.zones.list
iam.serviceAccounts.get	iam.serviceAccounts.list	resourcemanager.projects.get
storage.buckets.create	storage.buckets.delete	storage.buckets.get
storage.buckets.list	storage.buckets.update	storage.objects.create
storage.objects.delete	storage.objects.get	storage.objects.list
storage.objects.update	compute.disks.resize	runtimeconfig.variables.create
runtimeconfig.variables.delete	runtimeconfig.variables.get	runtimeconfig.variables.list
runtimeconfig.variables.update	runtimeconfig.variables.watch	

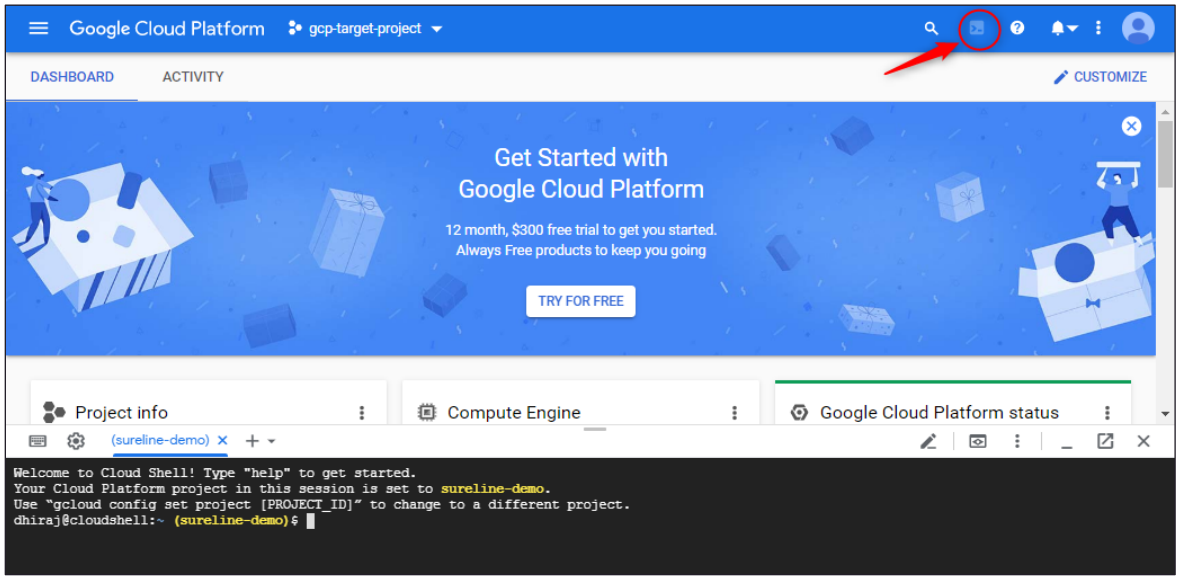
To ease the process of setting up these permissions, Persistent provides a script that can be run in a cloud shell in your account. Create a service account and grant it the required roles and permissions. Run the script under a user account with the following roles:

- **Owner:** Privileges for the project(s) into which systems can be recovered
- **Organization Role Administrator:** Privileges for the account
- **Organization Administrator**: Privileges for the cloud account

Note: If the systems being recovered is brought up within a single project, then the recovery can be achieved with permissions strictly enabled for that project. In this case, the script can be run with only the project's **Owner** role.

Running the Setup Script

To run the permissions setup script, click **Activate Cloud Shell** at the top of the Google Cloud Platform Console:



A Cloud Shell session opens inside a new frame at the bottom of the console and displays a command-line prompt. It may take a few seconds for the session to be initialized.
At the prompt, run the command below to download a configuration script to create Google Cloud roles and service accounts:

```
gsutil cp gs://sureline-release/DR/6.6.1/SUREedgePreDeployment/* .
```

This command copies the following files into the Cloud Shell environment:

```
SUREedgeDRPreDeployment.py
sureedge_deployment.json
```

Run the script `SUREedgePreDeployment.py` to create the required role and service account for SUREedge DR. The script's usage is as follows:

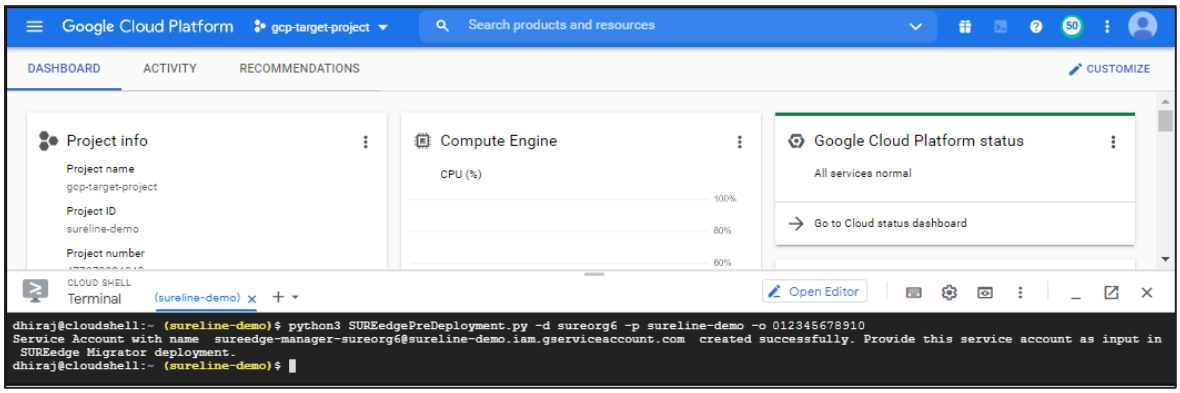
```
python3 SUREedgePreDeployment.py [-h] -d <DEPLOYMENT_NAME> -p <PROJECT_ID>
[-o <ORG_ID>]
```

where the arguments are:

Argument	Description	Required
-h, --help	Show this help message and exit	No
-d *<DEPLOYMENT_NAME>* --deployment-name *<DEPLOYMENT_NAME>*	A suffix that is appended to the Service Account and Role names created by the script. Must be less than 8 characters and contains lowercase letters and numbers.	Yes
-p *<PROJECT_ID>* --project-id *<PROJECT_ID>*	The ID of the GCP project that hosts your DR instance.	Yes
-o *<ORG_ID>* --org-id *<ORG_ID>*	The numeric GCP organization ID in which the role is created, and that administers the project(s) where recovered systems exist.	No

For example, run the following command to create roles and permissions using the suffix sureorg2 for deployment of a SUREedge DR instance into the project **sureline-demo** within the organization whose ID is *012345678910*:

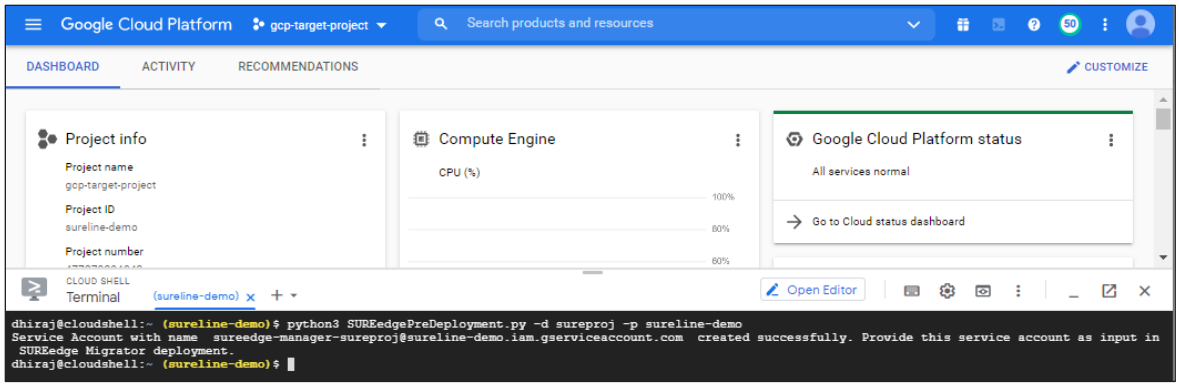
```
python3 SUREedgePreDeployment.py -d sureorg6 -p sureline-demo -o 012345678910
```



This creates the role **SUREedge Manager sureorg6** within the organization with ID *012345678910*, within the project **sureline-demo,** and creates the service account: `sureedge-manager-sureorg6@sureline-demo.iam.gserviceaccount.com`.

If all recovery operations occur within a single project then run the script without the organization ID option (`-o <ORG_ID>`):

```
python3 SUREedgePreDeployment.py -d sureproj -p sureline-demo
```



This command creates SUREedge Manager sureproj role and the service account: `sureedge-manager-sureproj@sureline-demo.iam.gserviceaccount.com` in the `sureline-demo` project.

Obtaining Licenses

Each instance of SUREedge DR must be licensed to perform recovery. If you have not received your license(s) you can obtain it (them) through your designated contact at Accelerite Systems or by contacting the Accelerite Support Team at support@accelerite.com.
Once you purchase the SUREedge DR, you will get a permanent GUID license. These licenses are tied to a specific SUREedge DR instance. To obtain your GUID licenses you will need to supply the Appliance Serial Number to Persistent Systems for all your SUREedge DR instances after they have been installed. Detailed instructions on getting your Appliance Serial Number(s), obtaining your permanent licenses and applying them to your SUREedge DR instance(s) can be found in your SUREedge DR User Guide(s).
Once you have license(s) for your SUREedge DR instance(s) they will need to be installed before you can perform recovery operations. Instructions for installing licenses on the SUREedge DR instances can be found in the **Settings** section of the SUREedge DR User Guide.

Contacting Support

Accelerite Software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by being able to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Submit enhancement requests online
- Download software patches
- Look up Accelerite support contacts
- Enter into discussions with other software customers
- Research and register for software training

To access the Self-serve knowledge base, visit the Accelerite Support home page at https://support.accelerite.com/hc/en-us

Most of the support areas require that you register on the Accelerite Support Portal. Many also require a support contract.

To register an account at the Accelerite Support Portal, visit https://support.accelerite.com/hc/en-us

To know more about registration process at Accelerite support portal, visit https://support.accelerite.com/hc/en-us/articles/202042570-New-user-registration-process

About Persistent

With over 13,500 employees around the world, Persistent Systems (BSE & NSE: PERSISTENT) is a global services and solutions company delivering Digital Engineering and Enterprise Modernization.

www.persistent.com

India

Persistent Systems Limited
Bhageerath, 402,
Senapati Bapat Road
Pune 411016.
Tel: +91 (20) 6703 0000
Fax: +91 (20) 6703 0008

USA

Persistent Systems, Inc.
2055 Laurelwood Road, Suite 210
Santa Clara, CA 95054
Tel: +1 (408) 216 7010
Fax: +1 (408) 451 9177
Email: info@persistent.com