Persistent

SUREedge® DR 6.6.1

Installation Guide for Azure

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 by taking advantage of the Cloud as a ready-to-use DR infrastructure. SUREedge DR enables enterprises to implement a Disaster Recovery solution at three level- locally, at a remote site, in the Cloud. You can start with local DR and seamlessly expand to a remote site or the Cloud simply 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-premise 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 on-boarding or migration, you must first determine the location(s) where SUREedge DR should be installed.

You can then:

- Obtain the required documentation and software for the environment(s) you have identified. You should have the **SUREedge DR Installation Guide 6.6.1 for Azure** (this document) and the software packages for installing SUREedge DR.
- Perform the installation of SUREedge DR software as instructed.
- License and configure SUREedge DR 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 DR in Azure environment. The following sections takes you through the steps to obtain installation materials and to install, license and configure SUREedge DR to run in Azure environment. You can then use the **SUREedge 6.6.1 DR User Guide** to configure and start using SUREedge DR for on-boarding or migration.

Deploying SUREedge DR

Getting Azure Parameters

Before starting SUREedge deployment on Azure, you must create and register an application in Azure. You must make note of some of the parameters from Azure which are required while configuring the Hypervisor Configuration setting later in this process.

At the end of this section, you 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 into 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.

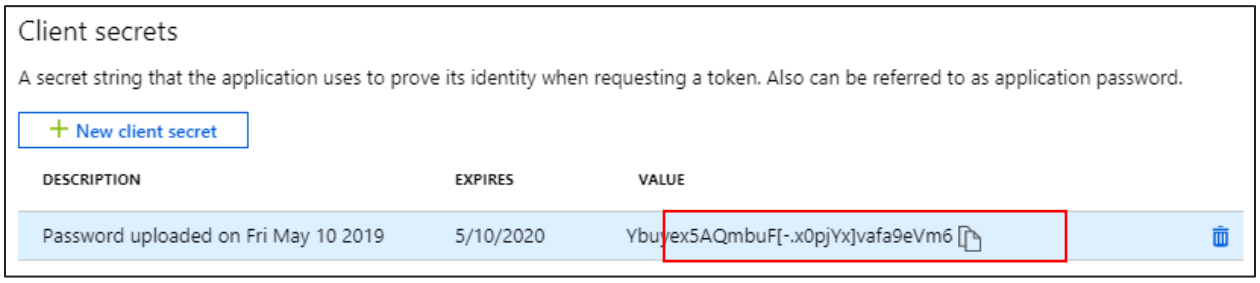
Step 2: Get Directory ID

1. Sign into your Azure Account through the Azure portal.
2. Select **Azure Active Directory**.
3. Select **Properties**.
4. Copy the **Directory ID.**

Step 3: Get application ID and authentication key

1. Sign into your Azure Account through the Azure portal.
2. Select **Azure Active Directory**.
3. Select **App registrations**.
4. From **App registrations** in Azure AD, select your application.
5. Copy the **Application ID** and store it in your application code.
6. Select **Certificates & secrets**.
7. Select **New client secret**.

8. For *Add a client secret*, provide a description of the key and duration for the key and click **Add**.
9. 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***.



Step 4: Get subscription ID

1. Sign into 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 5: Get Resource Group & Region

a) Create an Azure Active Directory application:

1. Sign into 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.

b) Get Resource Group & Region

1. Sign into 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.
3. You need to choose the same resource group and same region wherever required in further steps.

c) To provide resource group level permissions

1. Follow the above step 1 and 2 to create the application and resource group
2. Create the enterprise application
3. Create the resource group
4. Follow the below steps to Provide the resource group level permissions
   - Sign into your Azure Account through the Azure portal.
   - Go to home and navigate to resource groups
   - select the resource group

5. select the Access Control (IAM) on the left navigation pane.
6. Select Add > Add role assignment.
7. Select the Contributor role to assign to the application.
8. select the enterprise application and save the application.

d) Creating separate resource Group for network objects

1. Follow the above step 1 and 2 to create the application and resource group
2. Create resource group for SUREedge installation
3. Create separate resource group for network resources
4. Create virtual network under network resource group
5. Create enterprise application
6. Follow the below steps to Provide the resource group level permissions
   - Sign into your Azure Account through the Azure portal.
   - Go to home and navigate to resource groups
   - Select the resource group
   - Select the Access Control (IAM) on the left navigation pane.
   - Select Add > Add role assignment.
   - Select the Contributor role to assign to the application.
   - Select the enterprise application and save the application.
   - Create virtual network under network resource group
   - Assign the network to MC and store machines.

Step 7: Get Storage Account

1. Sign into 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** get listed.

Communication between Source Server and SUREedge® DR

To capture and transform servers being recovered in Azure 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.

Obtaining SUREedge Installers

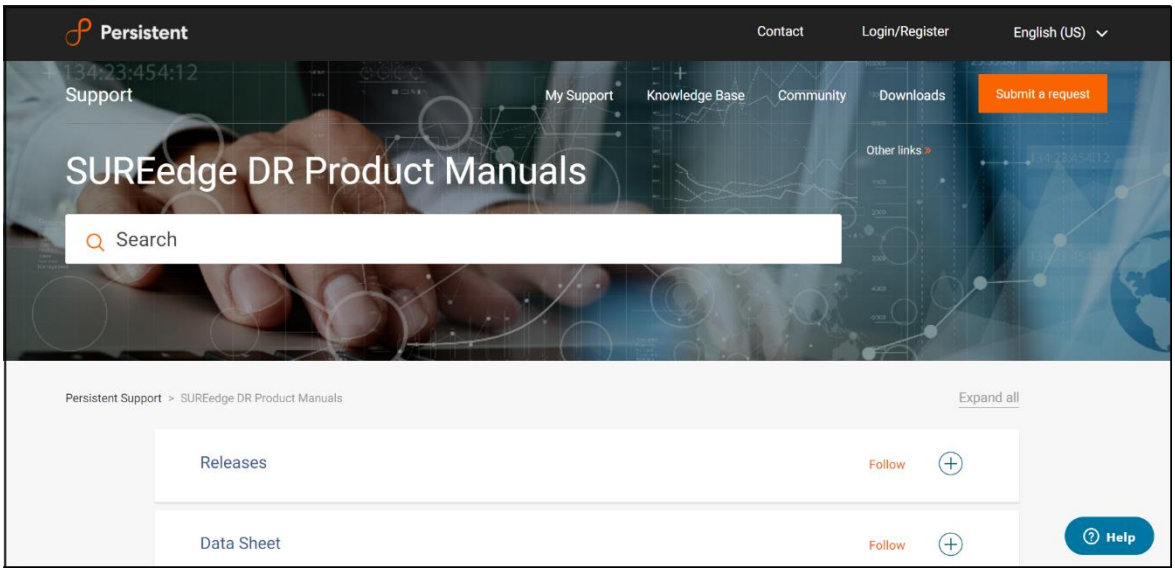
SUREedge DR installers, tools and documentation are all available online for download or deployment. The next sections details you to obtain the documentation and software binaries that you need to get started with SUREedge DR.

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:



In the **Releases** section, select the software version for which you want documentation, then find the desired document and click the **PDF** button to download it.

Preparing the SUREedge Store

Creating your SUREedge DR Store is done by deploying a linux-based VM in your Azure environment and installing the SUREedge DR Store software components on it.

Creating a VM

1. Sign into your Azure Account through the Azure portal.

2. Select **Virtual machines** and click **Add**.
3. To ***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 20.04 LTS*.
    e. For **Size**, select *Standard B4ms (4 core and 14GB ram)**.***
    f. For “ADMINISTRATOR ACCOUNT”, choose **Authentication type** as *password*. Provide **Username** as “sureline”, **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 1024 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 >1024 GB.
        d. Keep the default **Source type**.
    j. Select next and Add network details.
    Make sure following ports are open in network security group.
        - 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
    k. Select **Review + create** to validate parameters. Once validation is passed, select **Create**.

Getting Installers

The SUREedge DR Installer is available to download using the following wget command:

```
wget https://sure-builds.s3.us-west-1.amazonaws.com/dr/661/GA/SUREedgeLinuxAzurePackage.tar.gz
```

Uploading Packages

1. SSH to the store using public IP of store with sureline user (Go to **Virtual Machines** and select store VM which is created above).

2. Upload or untar following packages to `/home/sureline` directory of store VM which is created above.
   - `tar -xvzf SUREedgeLinuxAzurePackage.tar.gz`
   - `sudo chmod 755 install_sureedge_store.sh`

Installing Store

1. Connect to the deployed vm using SSH and run following commands:
   - Find the attached data disk device path, eg `/dev/sdb`
2. Install the store software by running the following command, substituting the data disk's device path where appropriate:
   ```
   sudo bash install_sureedge_store.sh Azure
   <data_disk_device_name>
   ```
3. Verify the store software installation is running using the following command on store VM:
   ```
   sudo systemctl status surestor.service
   ```
   Note: At store, execute following command:
   ```
   touch /etc/rc.local
   ```

Creating Proxy Images

SUREedge DR consists of two components: a Management Console ("MC") and a SUREedge Storage Engine ("Store") that must both be created on the Azure Cloud.

Create two instances (SUREedge MC and SUREedge store) on Azure Cloud using Azure images of Windows 2019 and CentOS respectively.

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

CentOS Proxy Image

Creating your SUREedge DR linux proxy is done by deploying a linux-based VM in your Azure environment and installing the SUREedge DR Store software components on it.

Creating a VM

1. Sign into 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 availability option as "**No infrastructure option required**"
   d. Select **Region** (which was created in Getting Azure Parameters section) from drop down list.
   e. Select **Image** as *CentOS-based 7.5*.
   f. For **Size**, select *Standard D3_v2 (4 core and 14GB ram)***.**

g. For “ADMINISTRATOR ACCOUNT”, provide **Username** as “sureline”, **Password** and **Confirm password**.
h. 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**.
i. Click “**Next: Disks >**” and select **OS disk type** as *Standard HDD*.
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**.

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.

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. Run this command to assume proxy is ready:
```
touch /home/sureline/proxy_ready
chown sureline:sureline /home/sureline/proxy_ready
```
3. Turn off Linux server from Azure portal.
4. 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**
5. Turn Off Linux server from Azure portal and never start again.
   Go to azure portal and select ***Home*** > ***Virtual Machines*** > **<Linux Server Name>** > **Delete**
6. Use VHD file name without .vhd as proxy image name.
   For example:
   From URL = https://sureedge550jbsa.blob.core.windows.net/vhds/sureedge-centos720190513151340.vhd
   Use proxy image name = **sureedge-centos720190513151340**

Windows proxy image

Creating your SUREedge DR windows proxy is done by deploying a windows-based VM in your Azure environment and installing the SUREedge DR Store software components on it.

Creating a VM

1. Sign into 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 2019 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**.
    k. Connect this VM using given **username** and **password**.
    l. copy **SUREedgeServerUtility.zip** to this VM from MC by downloading it from the register UI of MC.

    create the file `C:\\sureedge.config` on the VM and edit it to contain the following lines:

    ```
    mcip= <MC-ip-address>
    mcport= 25028
    version= <SUREedge-version>
    ```

    For example

    ```
    mcip= 10.1.0.4
    mcport= 25028
    version= 6.6.1.28928
    ```

    a. Get **token** from MC (from register server UI)
    b. Run this command in cmd from path where SUREedgeServerUtility.zip is extracted, SUREedgeServerUtility.exe /NOADD /token=<token of sureedge>
    c. Open the Command Prompt window as an administrator. Change the directory to %windir%\system32\sysprep, and then run **sysprep.exe**
    Note: Firewall must be turned off.

d. In the System Preparation Tool dialog box, select Enter System Out-of-Box Experience (OOBE), and make sure that the Generalize checkbox is selected.
e. In Shutdown Options, select **Shutdown** and click OK.

Installing Package

1. 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.
2. 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
3. Delete Windows server:
   b. Go to azure portal and select ***Home*** > ***Virtual Machines*** > <Windows Server Name> > **Delete**
4. 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/sureedge20190513152601.vhd

   Use proxy image name = **sureedge20190513152601**

Preparing the SUREedge MC

Creating your SUREedge Management Console (MC) is done by deploying a Windows-based VM in your Azure environment and installing the SUREedge DR MC software components on it.

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 2019 Datacenter.*
    e. For **Size**, select *Standard D4s_v3 (4 core and 16GB 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. Click “Next” and provide networking details.

Make sure following ports are open in network security group

- **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
  Make sure ports are opened in a configured network. Else open ports by adding into the inbound port rule using Azure console.
    j. Select Review + create to validate parameters. Once validation is passed, select Create.
    k. After creating MC server, Click on MC server -> go to networking -> Check inbound rules.

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. Download packages for MC installation.

```
Curl – o c:/ SUREedgeWindowsAzurePackage.zip
  https://sure-builds.s3.us-west-
  1.amazonaws.com/dr/661/GA/SUREedgeWindowsAzurePackage.zip
```

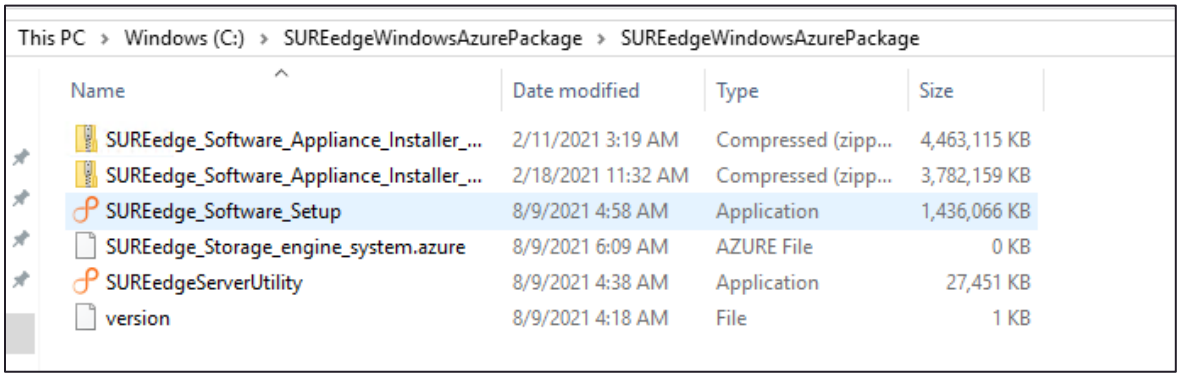
Upload the following packages to any folder on the MC:

a. SUREedge_Software_Setup.exe
b. SSDiscoverUtilitySetup.exe
c. SUREedge_Storage_engine_system.azure
d. Version

Installing SUREedge DR

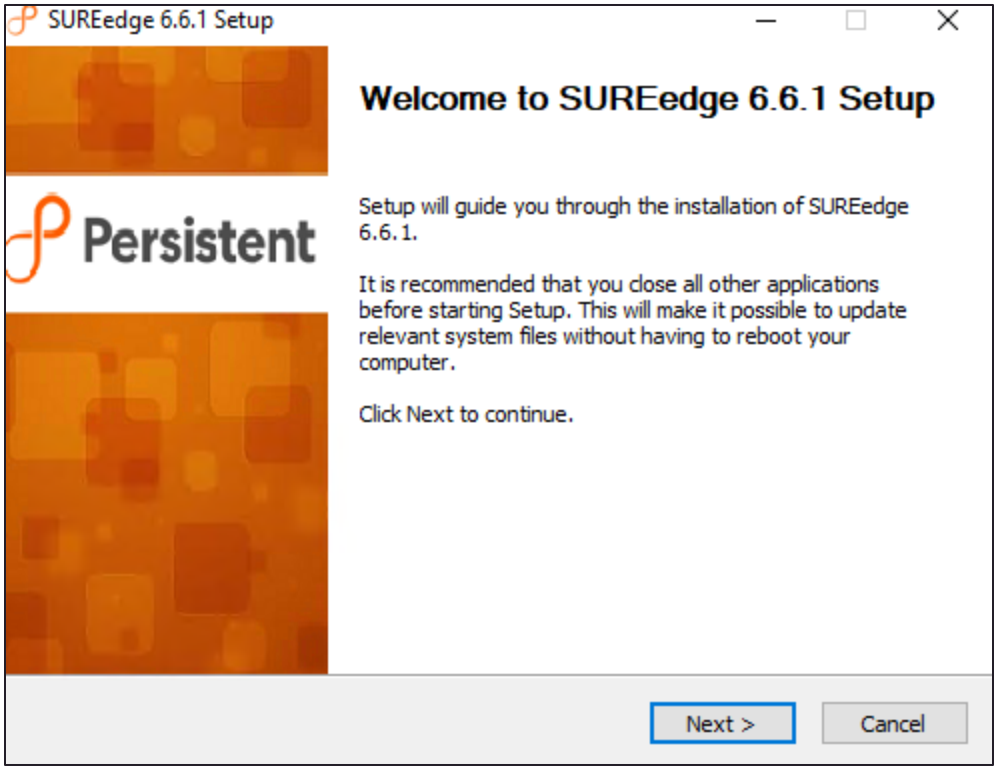
Once you have identified the Windows system where the SUREedge DR MC will run and found the resources required to install an instance of SUREedge DR:

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 the installer files.

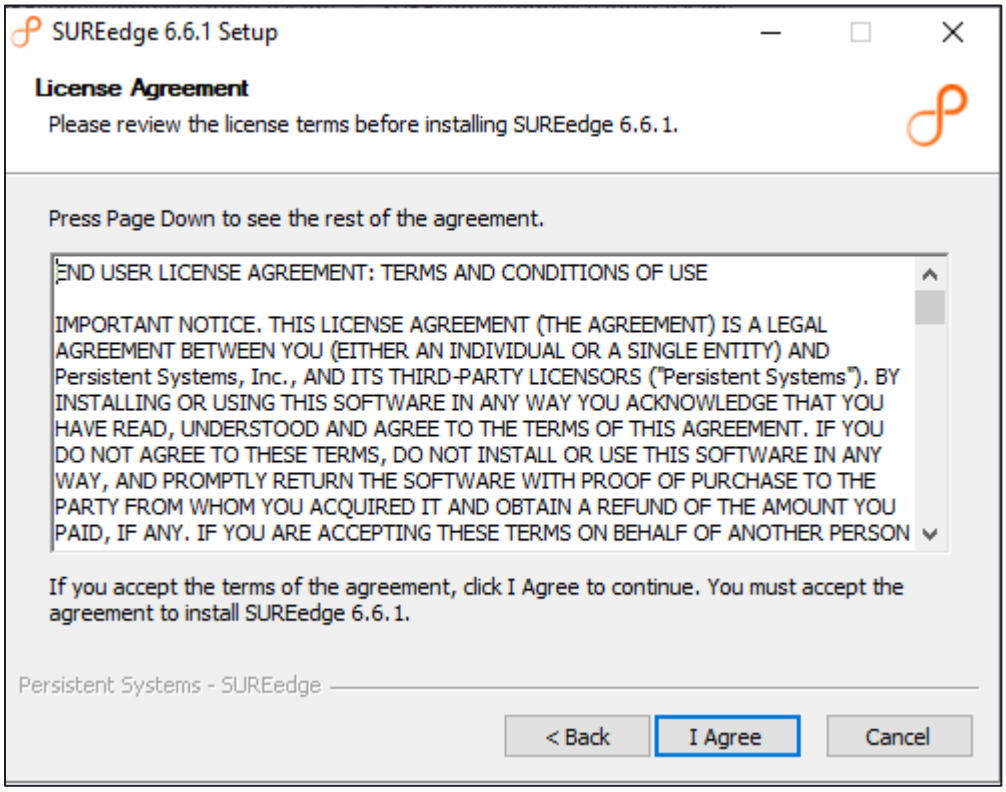


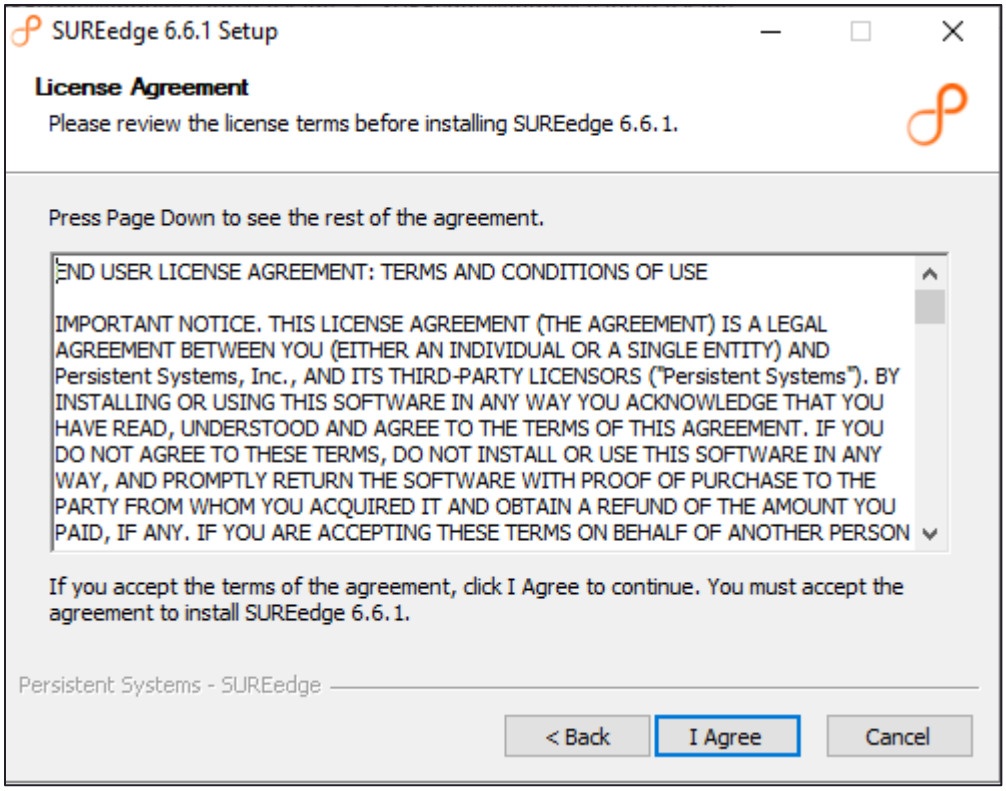
Run “SUREedge_Software_Setup” file as an administrator. This shows “Validating installer pre-checks…” screen. Wait for some time to display a first screen as “Welcome to SUREedge 6.6.1 Setup”.

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

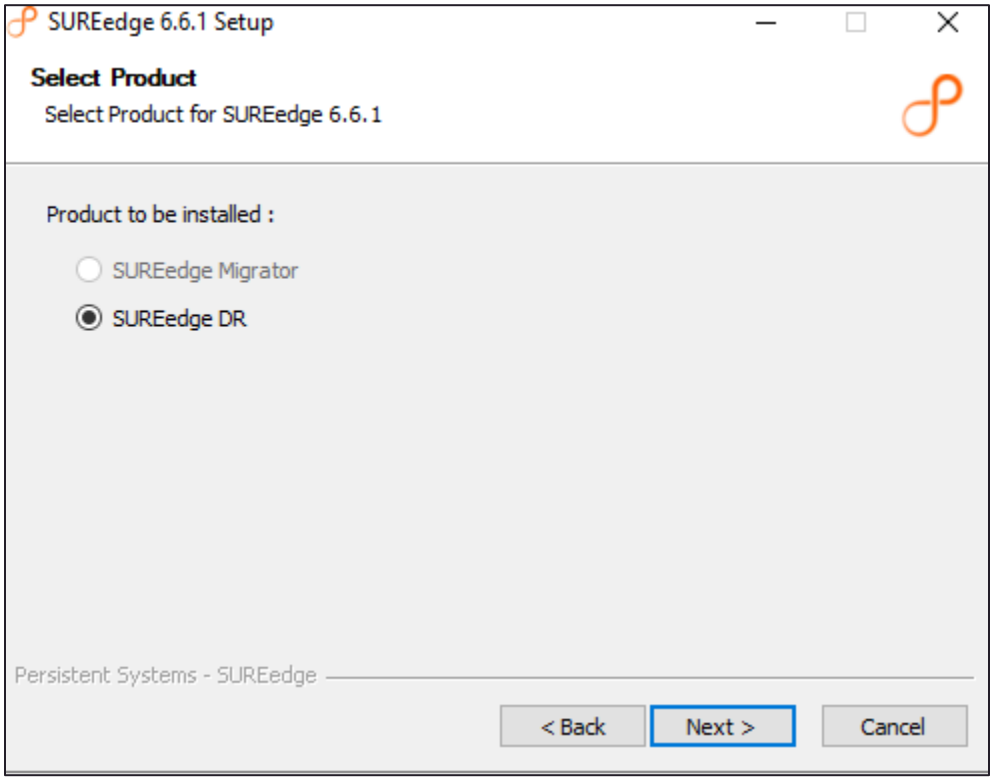


4. Please read the license agreement and click **I Agree** to continue.



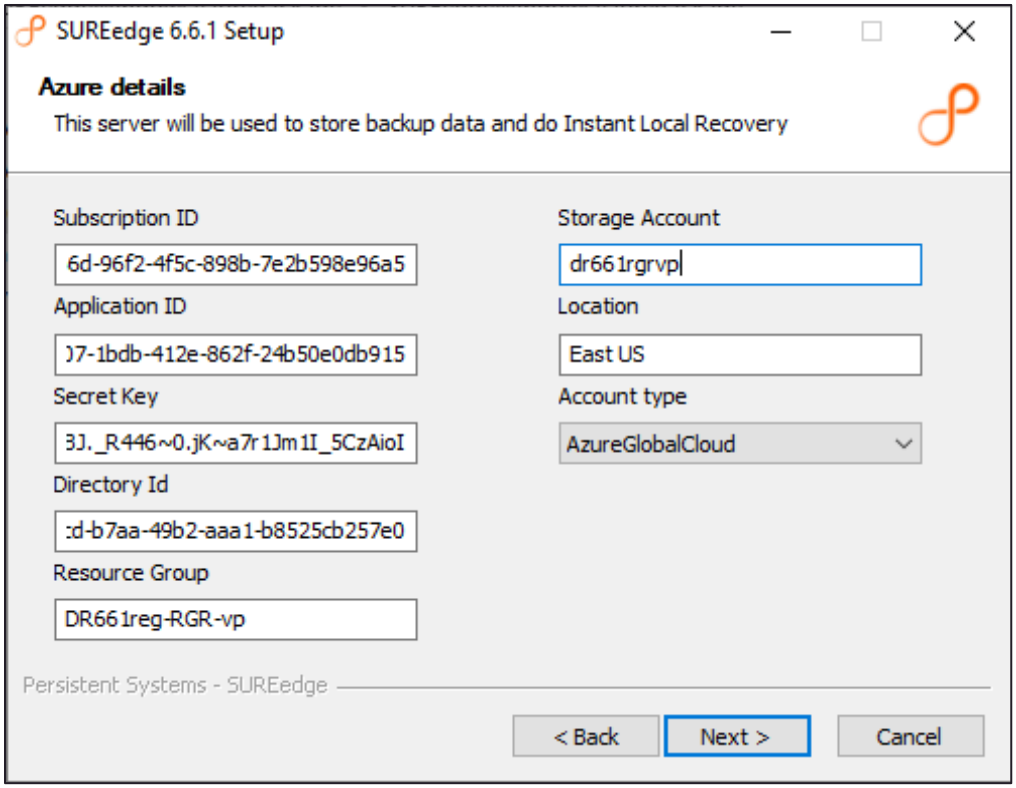


5. Click **Next** to display *Azure details*:

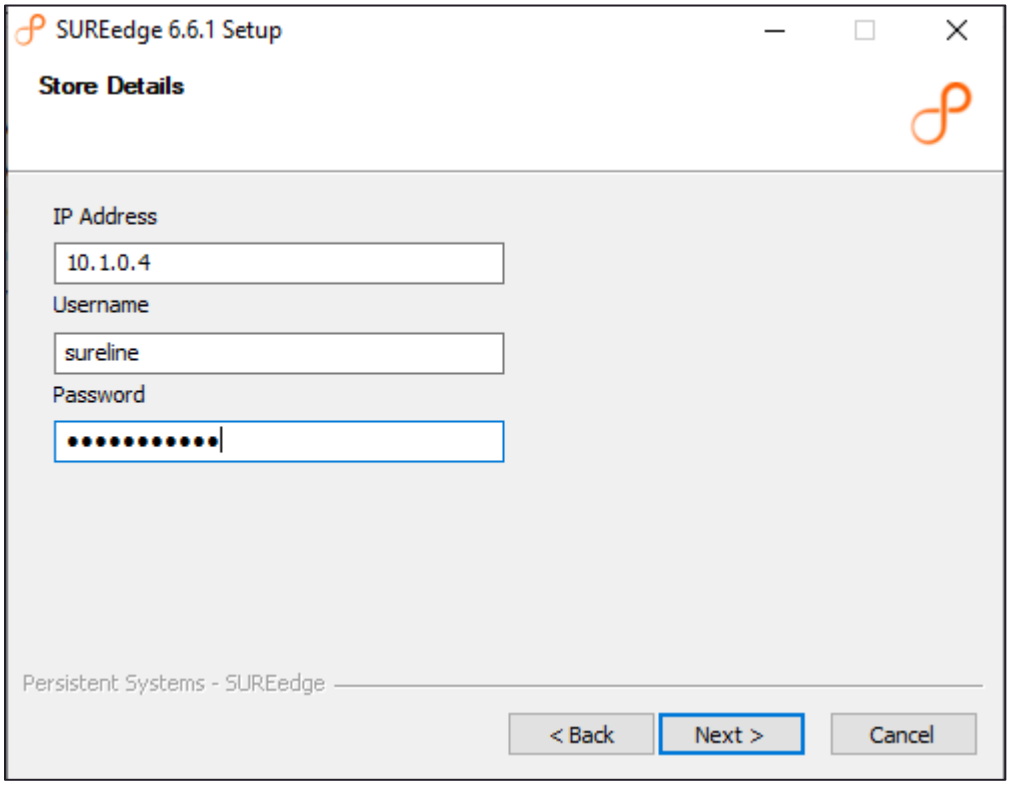


By default, the “SUREedge DR” is selected.

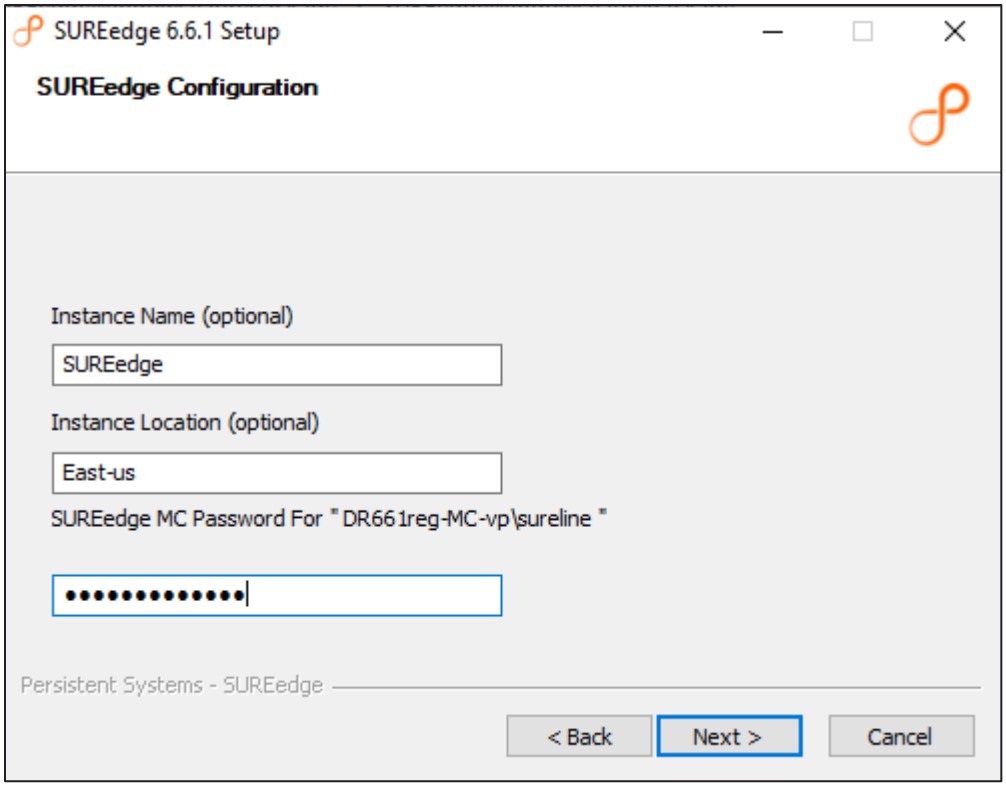
6. Provide internal IP address for store with credentials and click **Next**:



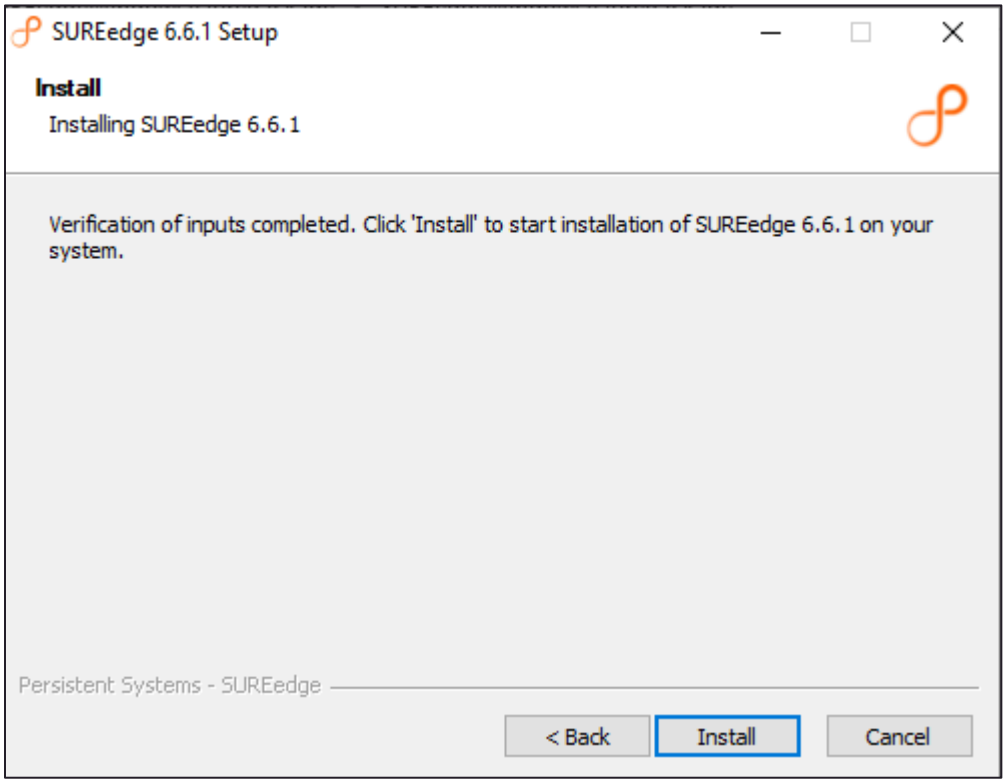
This validated the store parameters and shows screen for *SUREedge Configuration*.



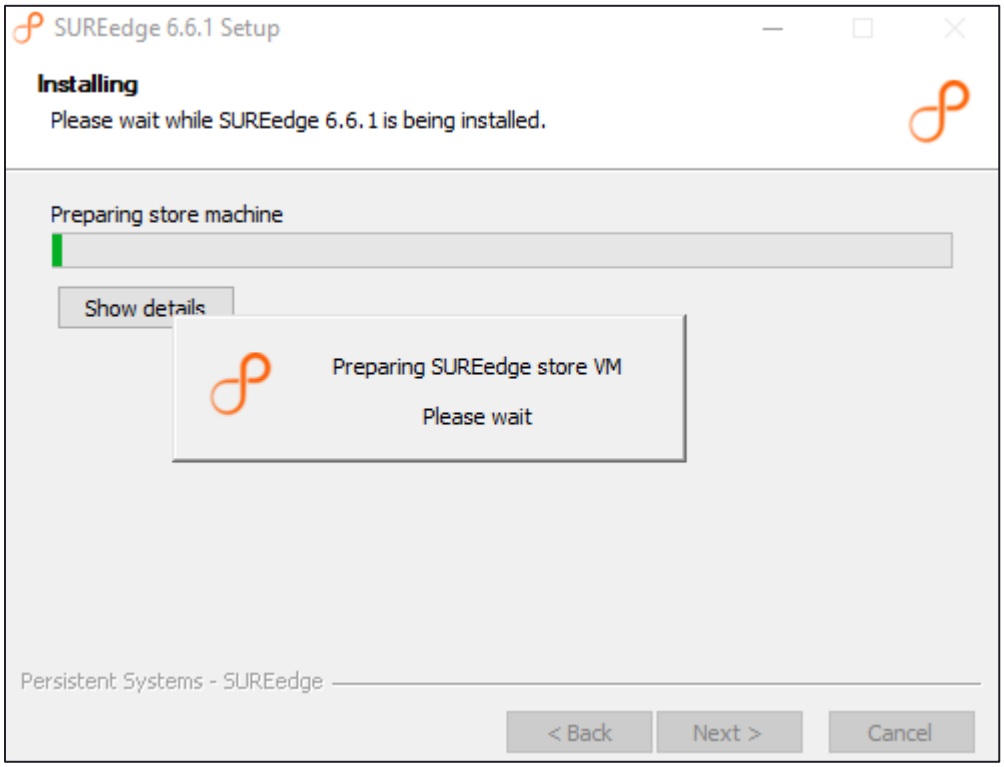
7. Enter SureEdge Configuration Details and click **Next**:



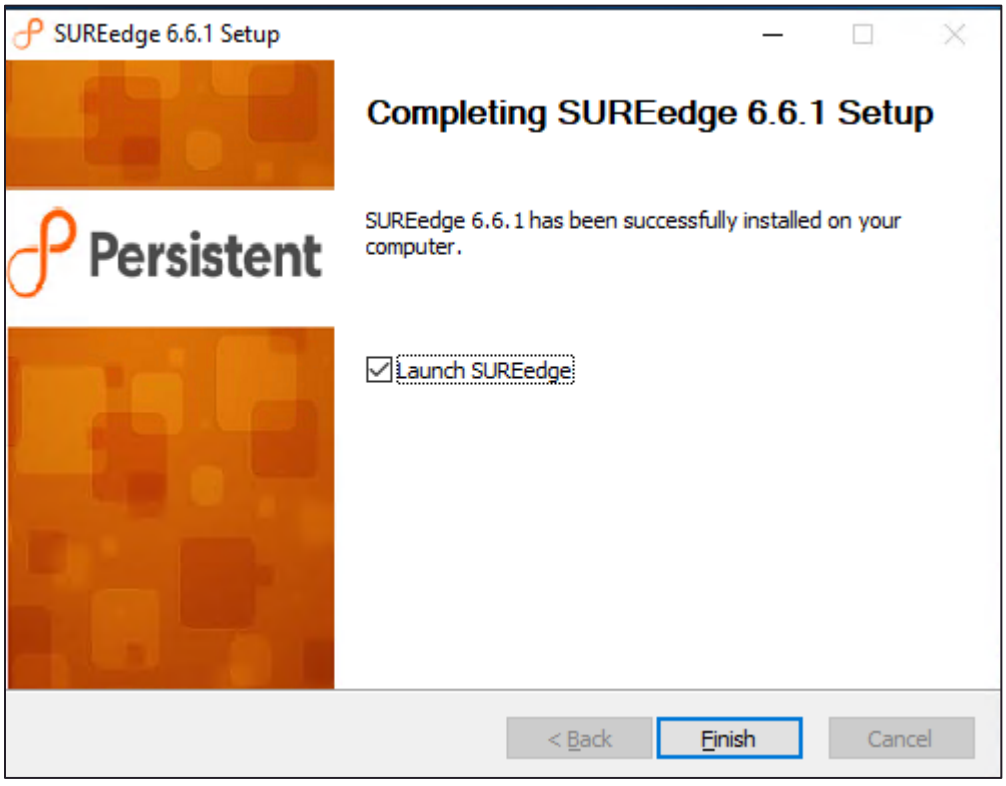
8. Click **Install** to proceed with the installation or Cancel to exit without installing.
   The time required to complete the installation may vary depending on the performance and load of the systems involved, the storage size(s) involved, and so on.



The progress of the installation will be displayed while the install is ongoing:

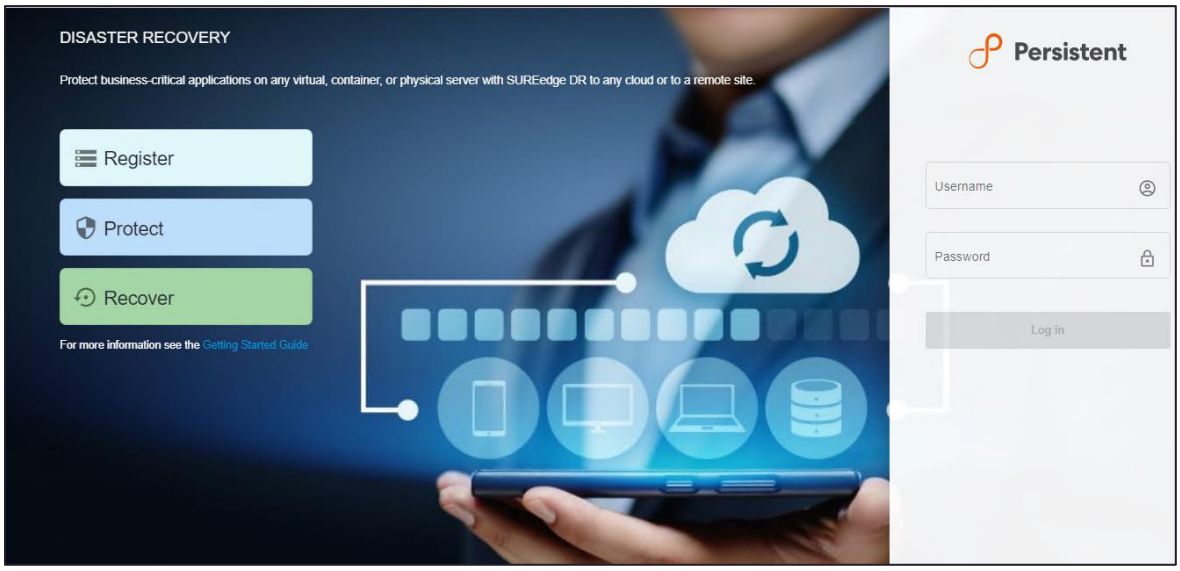


9. Once the installation is completed, click on the **Finish** button.

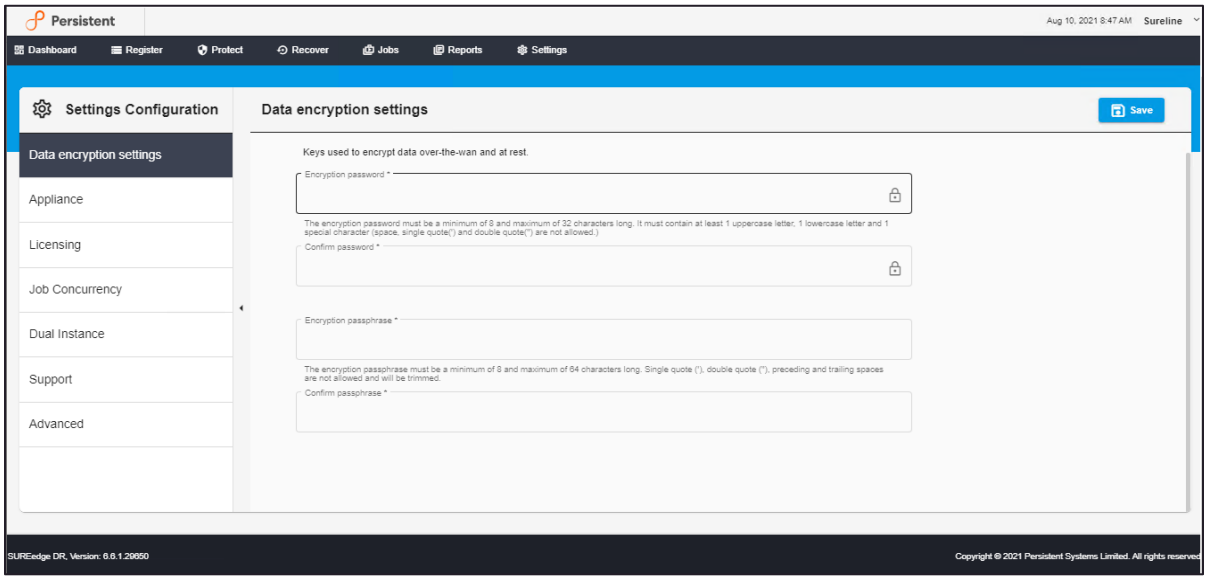


Configurations

Once installation is completed, you can launch SUREedge web UI using Firefox/Chrome browser using https://localhost or https://<MC VM IP>. Use SUREedge MC VM credentials to login to SUREedge WEB UI. (https://localhost/sureedge/index.php/) and do various configurations as mentioned in the subsequent sections. Default home page after login displays like below:

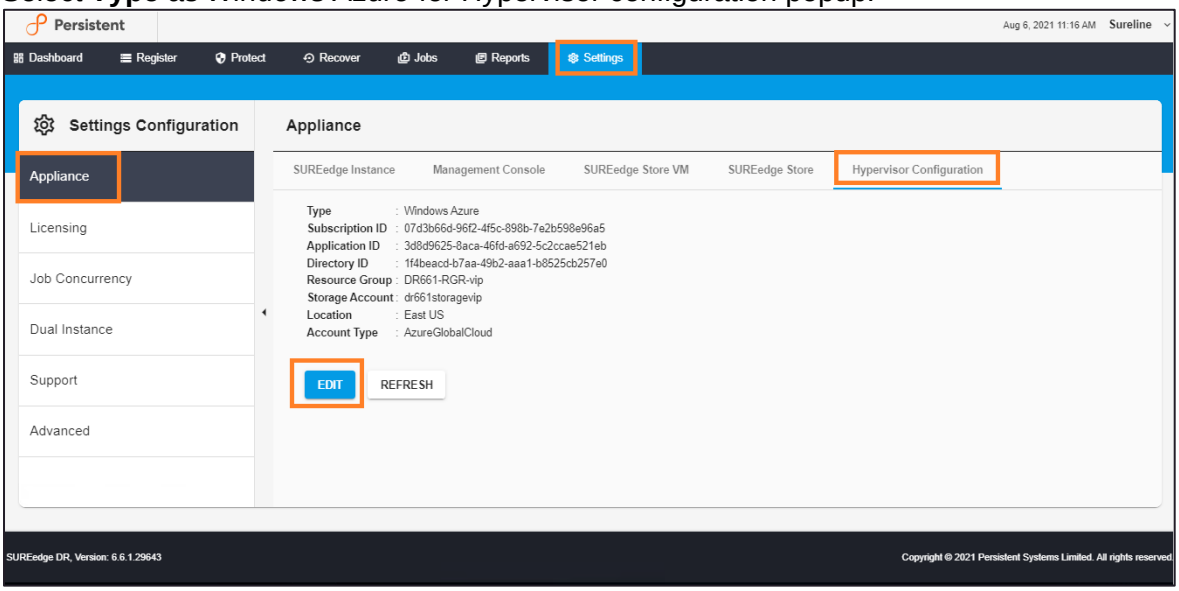


Log into the SUREedge DR instance, using the login password for the MC instance that you saved in Step f, section, “Creating a VM”. You will be presented with the **Data Encryption Settings** page:

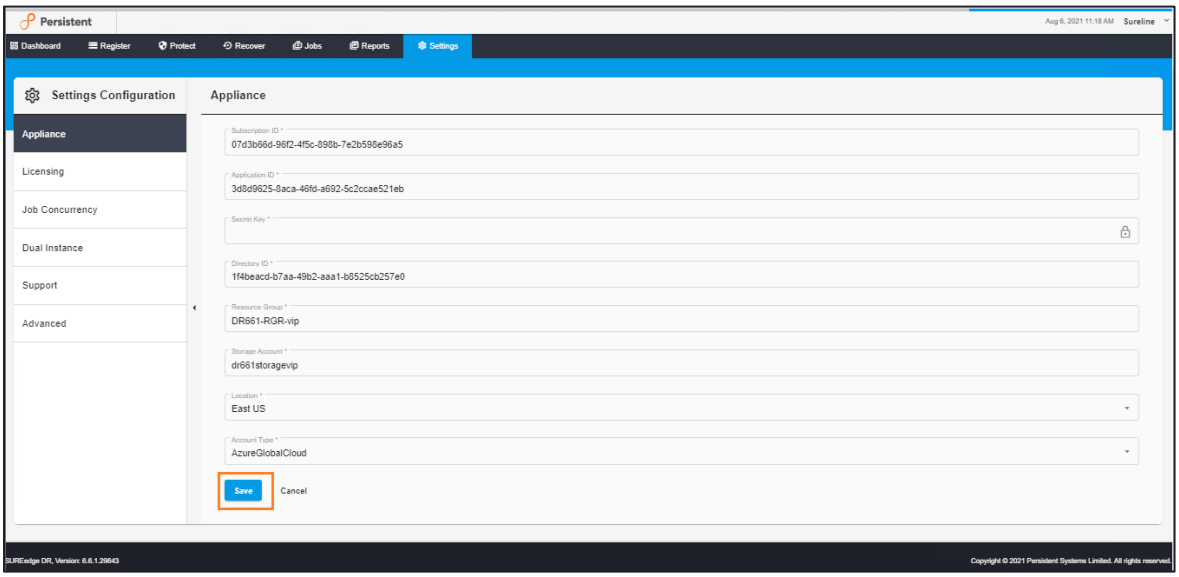


Verify and or Modify Hypervisor Configuration

1. Login to SUREedge DR.
2. Go to **Settings** > **Appliance>Hypervisor Configuration**.
3. Click **Edit** in “Hypervisor configuration”
4. Select **Type** as *Windows Azure* for Hypervisor configuration popup.



5. To modify populate the data in the above screen. Refer Getting Azure Parameters section to get the parameters. For **Account Type**, select *AzureGlobalCloud*.



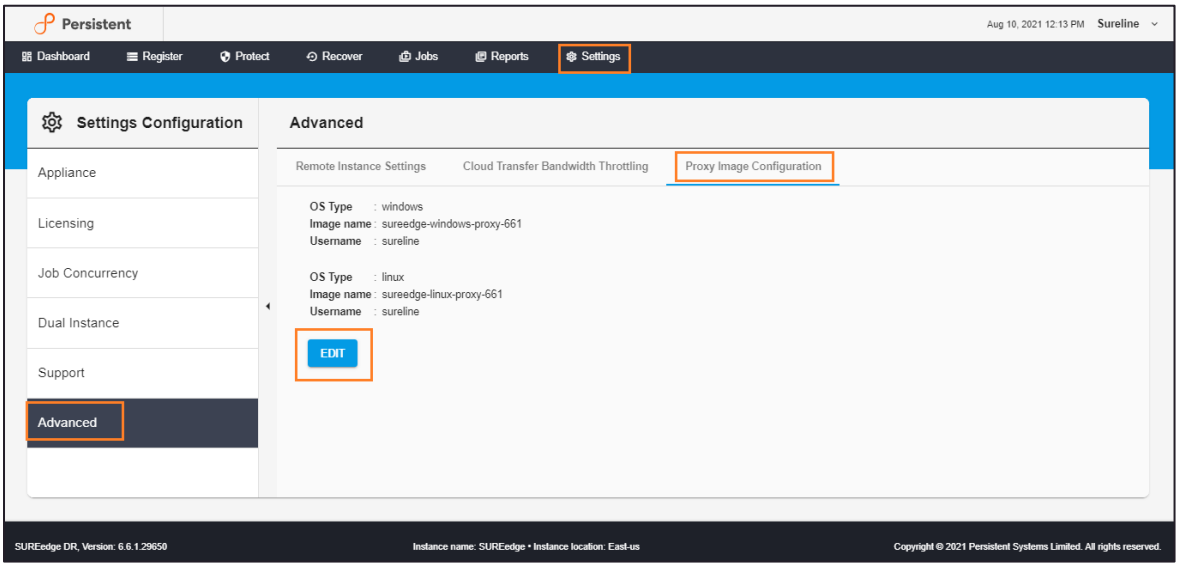
6. Click **Save** to save the hypervisor configuration.

Configuring Proxy

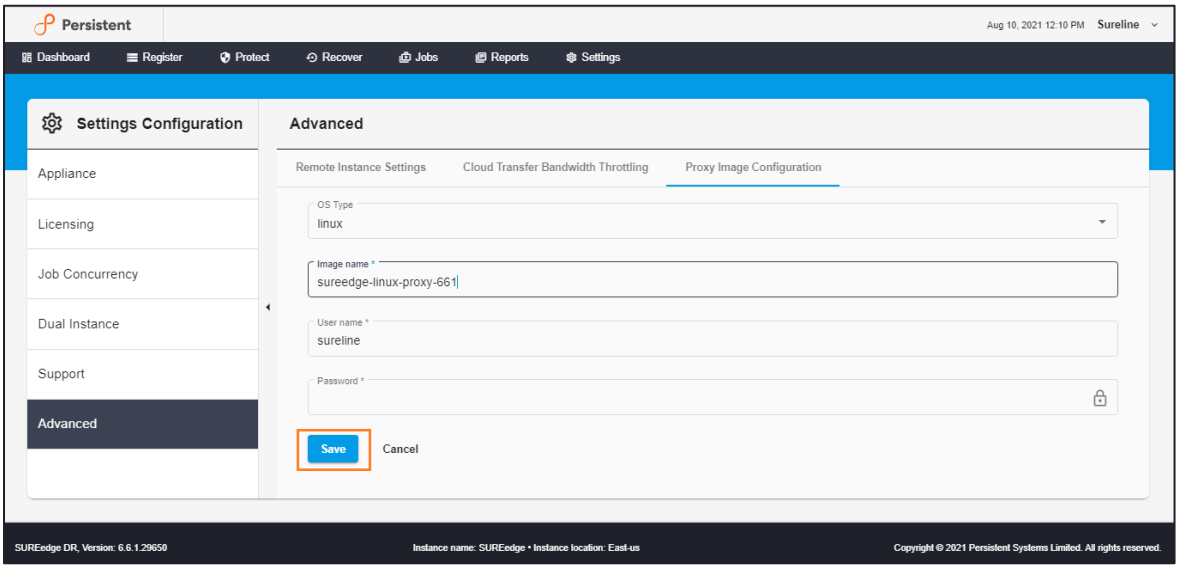
You need to configure your SUREedge DR with details of proxy images to be used during recovery

Linux Proxy Image configuration

1. Login to SUREedge DR Management Console (MC).
2. Go to **Settings** > **Advanced**> **Proxy Image Configuration,** click **Edit** icon.



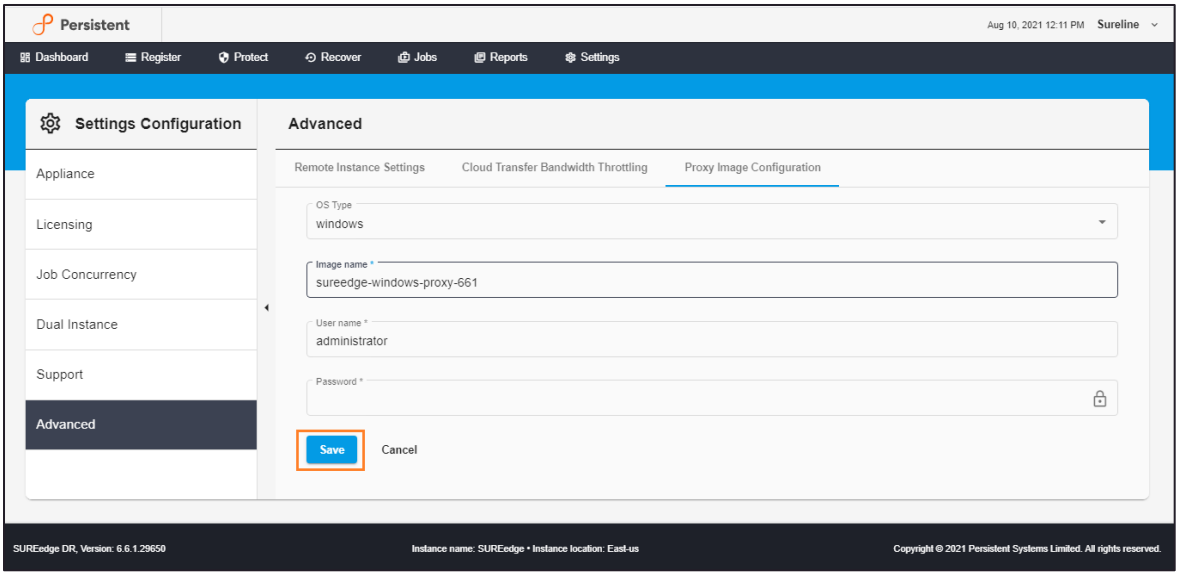
3. For **OS Type** select *linux* from dropdown list.



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 **Save**.

Windows Proxy Image configuration

1. Login to SUREedge DR Management Console (MC).
2. Go to **Settings** > **Advanced**> **Proxy Image Configuration,** click **Edit** icon
3. Select **OS Type** as a *windows*from dropdown list.



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 **Save**.
6. Verify Proxy Image creation.

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 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 *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