FORTRA

Clearswift Secure Email Gateway

Version 6.0.0

Installation Guide

(on Microsoft Azure)

Copyright Terms and Conditions

202503071227

Contents

Copyright Terms and Conditions ii
Contents iii
1. About this guide 1
Who is this guide for? 1
Alternative installation types and migration 1
2. Before installing 2
Types of installation 2
Prerequisites 2
3. Configure a virtual machine using Microsoft Azure 3
3.1 Create the VM 3
3.2 Configure the basic settings 3
Project Details 3
Instance details 3
Administrator account 4
Inbound port rules 4
3.3 Configure the disk settings 5
VM disk encryption 5
OS disk 5
Data disks 5
3.4 Configure the networking settings 5
Network interface 5
Load balancing 6
3.5 Configure the additional settings 6
3.6 Review and create the VM 7
Check the VM configuration 7
Generate new key pair 7
3.7 Configure public IP address and DNS name 7
3.8 Increase the disk size 7
3.9 Expand the OS partition 8
Required partition size 8
Increase the size of the partitions 8
4. Install Secure Email Gateway 13

Install from the Clearswift online repositories 13
5. Configure Secure Email Gateway **15**
Post-installation actions 15
Set a password for Azure user 15
Configure update repositories 16
Create administrator accounts 16
Complete the Initial Setup Wizard 17
Post-wizard actions 18
SSH access 18
Contact Fortra **19**
Fortra Support Portal 19

1. About this guide

This guide provides information for administrators installing Clearswift Secure Email Gateway onto a virtual machine using Microsoft Azure. It covers the requirements and procedures necessary for a full installation.

Who is this guide for?

This guide is intended for use by:

- New and existing customers installing Secure Email Gateway version 6.0.0 on the Microsoft Azure platform.

Alternative installation types and migration

This guide focuses on the installation of a new instance of Secure Email Gateway on Microsoft Azure.

If you require information on the following, refer to the Installation Guide.

- Alternative installation types: see the "**Before installing**" chapter.
- Migrating from version 5.7.0 to 6.0.0: see the "**Migrate**" chapter.

You can access all installation guides from the Online Help.

2. Before installing

This chapter outlines prerequisites and considerations you need to make before installing the cloud-hosted Secure Email Gateway. Secure Email Gateway runs on 64 bit Red Hat Enterprise Linux (RHEL) 9.4.

Types of installation

You can install Secure Email Gateway onto a virtual machine using Microsoft Azure.

Note that for the **Personal Message Management (PMM)** feature, you must install a separate network interface controller.

Prerequisites

Before installing, ensure that you have the following:

- A valid Microsoft Azure account
- Your subscription details

3. Configure a virtual machine using Microsoft Azure

This chapter outlines how to create the Azure virtual machine (VM) required to host Secure Email Gateway, using the Azure portal.

> For detailed instructions on using external resources, such as the Azure portal, refer to the appropriate documentation by the providers. Fortra is not responsible for changes to any of the procedure steps described.

3.1 Create the VM

1. Sign in to the Azure portal.
2. Select **Create a resource**.
3. Select **Virtual machine** > **Create**.

3.2 Configure the basic settings

Use the **Basics** tab to configure the details of your virtual machine.

Project Details

- Enter your **Subscription** and **Resource group**.

Instance details

- Enter **Virtual machine name**.
- For **Region**, select the nearest data center for your location. You will need this information in order to log in to the machine later.

> Some regions might have limitations on available disk types and disk sizes. For more information, see https://azure.microsoft.com/en-us/regions/.

- For the **Availability**, **Zone** and **Security** settings, select appropriate options as per the current policy of your organization.
- Under **Image**, click **See all images**. In the Marketplace, search for Red Hat. Select a **Red Hat Enterprise Linux (RHEL) 9.4** option.

- Select an appropriate **VM architecture**.
- Set **Run with Azure Spot discount** as per the current policy of your organization.
- Under **Size**, click **See all sizes** and select a suitable VM size. We recommend a VM with 16 GB of RAM, and a minimum of two processors.
- Set **Enable Hibernation** as required.

Administrator account

- Select an appropriate **Authentication type**.

  SSH public key:

  - Enter **Username**.
  - Select **SSH public key source**. You can **Generate new key pair**. Alternatively, you can **Use existing key stored in Azure** and select **Stored Keys**.

    The SSH key pair is generated and made available as a `.pem` file that can be downloaded once the VM has been created.

  Password:

  - Enter **Username** and **Password**. Ensure that your password satisfies Microsoft's password requirements.

Inbound port rules

Unless otherwise required by your organizational policy, these settings can be left to the default. You can use the Networking tab later to create access rules for known IP addresses.

Click **Next** and move to the **Disks** tab.

Review + create

You can click **Review + create** at this point to review the basic configuration and create the VM.

However, you will still need to configure the **Disks**, **Networking** and **Management** tabs. We recommend that you configure these tabs first, the use **Review + create** at the end.

3.3 Configure the disk settings

Use the **Disks** tab to configure the disk options and data disks of your virtual machine.

VM disk encryption

- Set as per your subscription and the current policy of your organization.

OS disk

- The default **OS disk size** assigned to Azure VM is 64 GB. You can change this to a more suitable size, such as 128 GB or 256 GB.
- Configure other options as required.

Data disks

- If required, additional disks can be added or existing disks can be attached to this VM. For detailed instructions, refer to the appropriate Azure documentation.

Click **Next** and move to the **Networking** tab.

3.4 Configure the networking settings

Use the **Networking** tab to configure the network interface options of your virtual machine.

Network interface

- For **Virtual network**, select an existing virtual network. Alternatively, click **Create new** to add a new one.
- Select a virtual network as **Subnet**. The default network location is `10.0.0.0/24`. This is used internally and is not the public IP address that you will use to access your VM. This is specified by **Public IP**, which enables you to customize a name for access to the machine.
- For **NIC network security group**, we recommend the **Advanced** option with firewall rules configured as follows.

  Select an appropriate **Configure network security group** if available, or click **Create new** to set up a new group.

Priority	Name	Port	Protocol	Source	Destination
1000	Allow-ssh	22	TCP	<Your IP address>	VirtualNetwork

Priority	Name	Port	Protocol	Source	Destination
1010	Allow-admin-ui-access	443	TCP	<Your IP address>	VirtualNetwork
1020	Allow-cockpit-access	9090	TCP	<Your IP address>	VirtualNetwork
1030	Allow-smtp-in	25	TCP	Anywhere	VirtualNetwork

To configure the Firewall ports and protocols for the product, see Firewall ports in the Online Help for more information.

- Configure other options. Unless otherwise required by your organizational policy, these settings can be left to the default.

Load balancing

- Configure as required. Unless otherwise required by your organizational policy, these settings can be left to the default.

Click **Next** and move to the **Management** tab.

3.5 Configure the additional settings

The following tags are available to configure further options for your virtual machine.

Management

Monitoring

Advanced

Tags

The settings on these tabs depend on the current policy of your organization and your preferences.

For example, you might enable the **Auto-shutdown** option in the **Management** tab.

When ready, click **Review + create**.

3.6 Review and create the VM

Use the **Review + create** tab to check that your settings are correct and validation has passed. You can then create the virtual machine.

Check the VM configuration

- Scroll through the page to review the current configuration of your VM.

  If any settings need amending, click **Previous** and return to the required tab. After you have amended the setting, go to the **Review + create** tab again.
- Once satisfied, click **Create** to create the VM.

Generate new key pair

If you selected to access the VM using a newly generated **SSH public key** in the Basic tab, you are now prompted to download the new key.

- Click **Download private key and create resource**.
- When prompted, save the `.pem` file to a safe location.

When the deployment has been complete, click **Go to resource**.

3.7 Configure public IP address and DNS name

The **Overview** page displays the details of your virtual machine.

- Review your networking settings. Select your **Public IP address** and check its properties.
- From **Setting** > **Configuration**, change **IP address assignment** from **Dynamic** to **Static**.
- Enter **DNS name label**.
- **Save** your settings.

3.8 Increase the disk size

Azure virtual machines are automatically given a default disk size of 64 GB. You may need to stop the VM and increase the disk size.

If you have already allocated a sufficiently large disk size during the VM creation, resizing is not required at this point.

If you wish to increase the disk size after the VM creation:

- Wait for provisioning to finish, then stop the VM.
- Increase the disk size of the OS disk from the Azure portal.

  It is recommended that your disk size is large enough to accommodate two 20 GB partitions for `root` and `/opt`, and 200 GB for `/var`. Refer to the table of required partition size for more information.
- Start the VM.

3.9 Expand the OS partition

After increasing the disk size, you will need to resize the disk from the default size in Azure.

Follow the instructions at https://docs.microsoft.com/en-us/azure/virtual-machines/linux/resize-os-disk-gpt-partition for RHEL systems.

Required partition size

As a guidance, we recommend the following:

Partition	Required size
`root` and `/opt`	Minimum of 20 GB (per partition)
`/var`	Testing environment: Minimum of 80 GB Production environment: Minimum of 200 GB
`usr`	These partitions may already be using up to 20 GB of disk space
`temp`	
`home`	
`boot`	

`/opt` may be part of the `root` partition. If this is a case, you might set `root` to 40 GB to accommodate the sufficient size.

Increase the size of the partitions

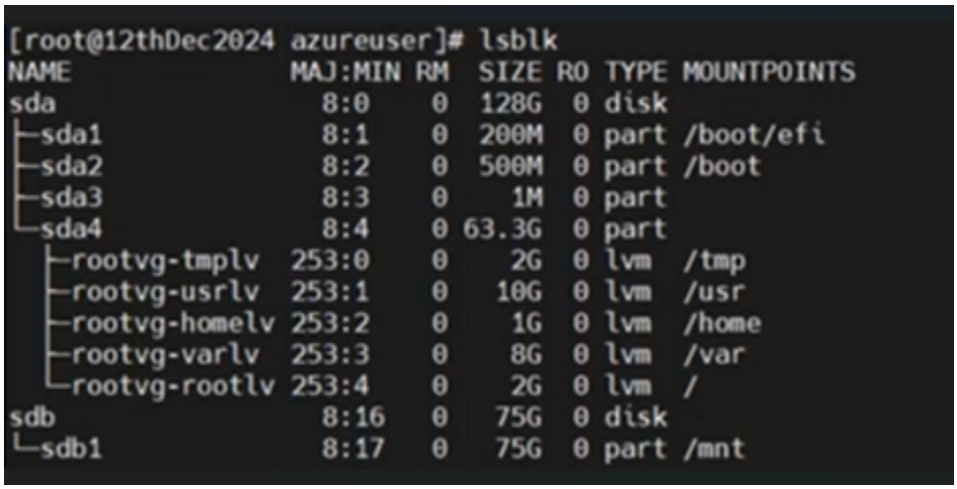
When the virtual machine has restarted, perform the following steps.

1. Access your VM as a root user by using the following command.

```
#sudo su
```

2. Use the `lsblk` command to determine which logical volume (LV) is mounted on the root of the file system.

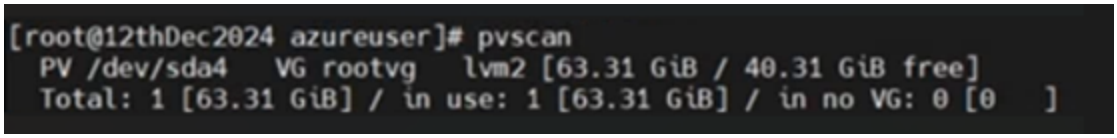
   In this example, it would be `rootvg-rootlv` in `sda4` which is currently reported as 63.3 GB.



Note that in this example, the `/opt` partition is mounted on `rootvg-rootlv`.

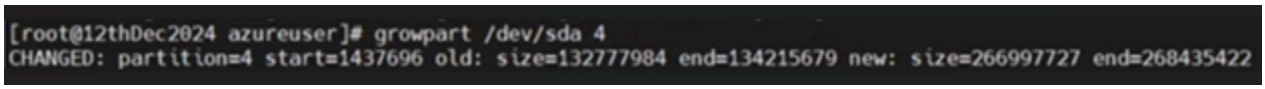
3. Use the `pvscan` command to determine which disk and partition holds the LVM physical volume or volumes (PV) in the volume group named `rootvg`.

   Note the size and free space listed between the square brackets, as [*size* / *free space*].



4. Expand the partition that contains this PV by using `growpart`, the device name, and the partition number.

   This expands the specified partition to use all the free contiguous space on the device.



5. Use the `lsblk` command again to verify that the partition has been resized as expected.

   In this example, `sda4` has changed from 63.3 GB to 127.3 GB.

```
[root@12thDec2024 azureuser]# lsblk
NAME                MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
sda                   8:0    0   128G  0 disk
├─sda1                8:1    0   200M  0 part /boot/efi
├─sda2                8:2    0   500M  0 part /boot
├─sda3                8:3    0     1M  0 part
└─sda4                8:4    0 127.3G  0 part
  ├─rootvg-tmplv    253:0    0     2G  0 lvm  /tmp
  ├─rootvg-usrlv    253:1    0    10G  0 lvm  /usr
  ├─rootvg-homelv   253:2    0     1G  0 lvm  /home
  ├─rootvg-varlv    253:3    0     8G  0 lvm  /var
  └─rootvg-rootlv   253:4    0     2G  0 lvm  /
sdb                   8:16   0    75G  0 disk
└─sdb1                8:17   0    75G  0 part /mnt
```

6. Use the `pvscan` command again to verify that the new size of the PV is as expected.

   Compare the new size with the original [*size* / *free space*] values.

```
[root@12thDec2024 azureuser]# pvscan
  PV /dev/sda4   VG rootvg   lvm2 [127.31 GiB / 104.31 GiB free]
  Total: 1 [127.31 GiB] / in use: 1 [127.31 GiB] / in no VG: 0 [0   ]
```

7. By using the `lvresize` commend, increase the size of the `root` partition as necessary.

   In this example, the `root` is currently 2 GB. According to the table of required partition size, extra 18 GB need to be added.

```
# lvresize -r -L +18GB /dev/mapper/rootvg-rootlv
```

```
[root@12thDec2024 azureuser]# lvresize -r -L +18GB /dev/mapper/rootvg-rootlv
  Size of logical volume rootvg/rootlv changed from 2.00 GiB (512 extents) to 20.00 GiB (5120 extents).
  File system xfs found on rootvg/rootlv mounted at /.
  Extending file system xfs to 20.00 GiB (21474836480 bytes) on rootvg/rootlv...
xfs_growfs /dev/rootvg/rootlv
meta-data=/dev/mapper/rootvg-rootlv isize=512    agcount=4, agsize=131072 blks
         =                       sectsz=4096  attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=1 inobtcount=1 nrext64=0
data     =                       bsize=4096   blocks=524288, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=16384, version=2
         =                       sectsz=4096  sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
data blocks changed from 524288 to 5242880
xfs_growfs done
  Extended file system xfs on rootvg/rootlv.
  Logical volume rootvg/rootlv successfully resized.
```

You can run the `lsblk` command to verify that the `rootvg-rootlv` size has been increased accordingly.

8. The size of `/opt` also needs to be increased. However, in this example, `/opt` is part of the `root` partition.

   To accommodate this, you may add further 20 GB to `root` and make this partition 40 GB.

```
# lvresize -r -L +20GB /dev/mapper/rootvg-rootlv
```

```
[root@12thDec2024 azureuser]# lvresize -r -L +20GB /dev/mapper/rootvg-rootlv
  Size of logical volume rootvg/rootlv changed from 20.00 GiB (5120 extents) to 40.00 GiB (10240 extents).
  File system xfs found on rootvg/rootlv mounted at /.
  Extending file system xfs to 40.00 GiB (42949672960 bytes) on rootvg/rootlv...
xfs_growfs /dev/rootvg/rootlv
meta-data=/dev/mapper/rootvg-rootlv isize=512    agcount=40, agsize=131072 blks
         =                       sectsz=4096  attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=1 inobtcount=1 nrext64=0
data     =                       bsize=4096   blocks=5242880, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=16384, version=2
         =                       sectsz=4096  sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
data blocks changed from 5242880 to 10485760
xfs_growfs done
  Extended file system xfs on rootvg/rootlv.
  Logical volume rootvg/rootlv successfully resized.
```

If you have a separate `/opt` partition, then, increase it to 20 GB, instead of increasing `root` to 40 GB.

For example, if you have `rootvg-optlv` which is 2 GB, add 18 GB to it.

```
# lvresize -r -L +18GB /dev/mapper/rootvg-optlv
```

9. Increase the size of `/var` as necessary.

   Check how much disk space you have by using the `pvscan` command. Also, refer to the table of required partition size.

```
# lvresize -r -L +<value>GB /dev/mapper/rootvg-varlv
```

   Enter a required number in the <value>. For example, to add 66 GB:

```
# lvresize -r -L +66GB /dev/mapper/rootvg-varlv
```

10. Use the following commends to verify whether the logical volumes have an increased file system size.

```
#df -Th /
#df -Th /var
```

If you have a separate `/opt` partition:

```
#df -Th /opt
```

4. Install Secure Email Gateway

You can install the Secure Email Gateway software using the following instructions.

Install from the Clearswift online repositories

To install Secure Email Gateway from repositories hosted online by Clearswift, you will need the Internet access to them.

> We recommend disabling or removing any existing repositories in `/etc/yum.repos.d/` on Secure Email Gateway as they may cause conflicts.

1. Assume root role at the command line.

   > When downloading and installing files, we recommend that you check the downloaded file can be verified against the vendor public key.

2. Download the packages containing the online repository configuration files:

   (Click  to open a page from where you can copy the commands and scripts.)

   ```
   curl -Of https://cs-products.fortra.com/rhel9/seg/cs-rhel9-mirrors-1.0.0.rpm

   curl -Of https://cs-products.fortra.com/rhel9/seg/cs-rhel9-email-repo-1.0.2.rpm
   ```

3. Download and install the Clearswift GPG public key:

   ```
   rpm --import https://cs-products.fortra.com/RPM-GPG-KEY-CS-PROD
   ```

4. Verify the downloaded packages:

   ```
   rpm --checksig --verbose cs-*.rpm
   ```

   This will display the results below, where all checks respond with OK:

```
cs-rhel9-mirrors-1.0.0.rpm:

Header V4 RSA/SHA256 Signature, key ID 9c75f096: OK
Header SHA256 digest: OK
Header SHA1 digest: OK
Payload SHA256 digest: OK
MD5 digest: OK
```

```
cs-rhel9-email-repo-1.0.2.rpm:

Header V4 RSA/SHA256 Signature, key ID 9c75f096: OK
Header SHA256 digest: OK
Header SHA1 digest: OK
Payload SHA256 digest: OK
MD5 digest: OK
```

5. Move Microsoft Update Repos from `/etc/yum.repos.d/` directory:

```
mv /etc/yum.repos.d/* /var/tmp
```

6. Install the downloaded repository-file packages:

```
dnf -y install cs-*.rpm
```

7. Remove rsyslog:

```
dnf -y remove rsyslog
```

8. Install the jemalloc package:

```
dnf install -y jemalloc --enablerepo=cs-*
```

9. Install the required product using the following command:

```
dnf install -y cs-email --enablerepo=cs-*
```

This command temporarily enables access to the online repositories, and installs Secure Email Gateway.

If this step fails due to additional conflicts, you might need to remove the conflicting packages first using:

```
dnf remove <package name>
```

10. Reboot Secure Email Gateway.
11. Go to the Configure Gateway chapter of this guide and continue.

5. Configure Secure Email Gateway

After the installation, you may need to perform some actions to set up your Secure Email Gateway, and then complete the Initial Setup Wizard.

Over this process:

- All system administration actions should be performed using Red Hat Cockpit.

> When you log in to Cockpit with the root user name for the first time after the installation, you might receive an error, stating that your user name and password are incorrect, even if you used the correct credentials. To resolve this, follow the steps in the Red Hat Documentation.

> You should avoid changing network configuration at the command line as Secure Email Gateway may not be notified of these changes.
>
> If changing network configuration at the command line is necessary, please contact Fortra's Clearswift support for more information.

Post-installation actions

We recommend that you consider the following after installing Secure Email Gateway, but before configuring its Initial Setup Wizard.

Set a password for Azure user

If you used an SSH key when you created the Azure virtual machine, you will need to set a user password, so that you can access Cockpit.

1. Connect to the VM using your SSH key.
2. Enter the following command:

```
passwd <username>
```

3. When prompted, enter the password.

You can now use the user name and password combination to log in to Cockpit.

Configure update repositories

By default, the Clearswift online repositories are disabled after installation. This means that any updates will need to be installed using the ISO of subsequent Secure Email Gateway releases.

Alternatively, if Secure Email Gateway has access to the Internet, it can receive updates from the online repositories. Switching from offline to the online repositories gives access to Red Hat security fixes, normally within 24 hours of their publication and subsequent testing to ensure there are no compatibility issues. We recommend this for most installations. However, you should only do this if you intend to also use the online repositories for future product upgrades.

Be aware that enabling the online repositories is an irreversible action.

To enable the online repositories:

1. Log in to Cockpit using the administrator credentials. Ensure that you have the **Administrative access** (not the **Limited access**) to the account.

   To access the Cockpit administration user interface, open a supported web browser and enter the IP address of your Secure Email Gateway, on port 9090:

   `https://<ip-address>:9090`
2. Navigate to **Clearswift**. From **Product Actions** > **Enable online repositories**, click **Enable**.

To check and install future updates

1. Navigate to **Software updates** to check and install updates.

Create administrator accounts

Before you start using the Gateway:

- Create a new (primary) administrator account
- Create a secondary administrator account - it is good practice, in case the password for the primary administrator account is lost.
- Disable the root user account as a security precaution

To do this:

1. Log in to Cockpit using the credentials created during the Red Hat installation. Ensure that you have the **Administrative access** (not the **Limited access**) to the account.

To access the Cockpit administration user interface, open a supported web browser and enter the IP address of your Secure Email Gateway, on port 9090:

`https://<ip-address>:9090`

2. Navigate to **Accounts** > **Create new account**.
   - Enter the name of the new administrator account and a strong password that meets the criteria defined in the password policy.
3. Click the new administrator account and enable the following role and policy:
   - Ensure that you assign appropriate **Groups** (e.g. `wheel`) to the account, so it has the administrator privileges. The administrator user can switch their privileges by selecting either the **Administrative access** or the **Limited access**.
   - In the **Options** section, click **edit**. In the **Account expiration** dialog, select **Never expire account** and click **Change**.
   - In the **Password** section, click **edit**. In the **Password expiration** dialog, select **Never expire password** and click **Change**.

If you set the password expiry for any created accounts, ensure that you keep a record of it, as Red Hat does not automatically notify the user when the password is due to expire. If the administrator account becomes locked out, the only resolution is to take the system offline and boot into single user mode.

4. Log out of Cockpit and log back in using the new administrator credentials. Ensure that you have the **Administrative access** (not the **Limited access**) to the account.
5. Navigate to **Accounts**.
   - Expand the options (**...**) for the root user, and select **Lock account** to disable it.

Complete the Initial Setup Wizard

Once you have gone through the post-installation actions above and have restarted Secure Email Gateway, run the Initial Setup Wizard.

1. To access the Secure Email Gateway's web user interface, open a supported web browser and enter the IP address of your Gateway:

   `https://<ip-address>`

2. The Initial Setup Wizard is displayed.

3. Complete the wizard to configure Secure Email Gateway.
4. The system might take around 5-10 minutes to apply the settings before you can use the Gateway. We recommend visiting the Configure Gateway topic in the Online Help when the interface is accessible.

Post-wizard actions

We recommend you consider the following after you ran the Initial Setup Wizard.

SSH access

If SSH access is required, you need to re-enable it through the web user interface. See SSH Access in the Online Help for more information.

Contact Fortra

For more information about the Fortra's Clearswift products and cybersecurity solutions, please visit our website.

You can contact us for questions, and to receive technical bulletins, updates, program fixes and other information on your Secure Email Gateway via email or Internet.

Fortra Support Portal

Fortra Support Portal offers various helpful resources, such as product documentation and knowledge articles. You can also contact our Technical Support, using the Fortra Support Portal.

For support issues, please:

- Check this guide's table of contents and topics for information that addresses your concern.
- Check the Knowledge Base in the Fortra Support Portal for information that addresses your concern.
- Gather and organize as much information as possible about the problem, including job/error logs, screenshots or anything else to document the issue.