ENTRUST

KeySafe 5

Keysafe 5 v1.2 OVA Installation Guide

8 April 2024

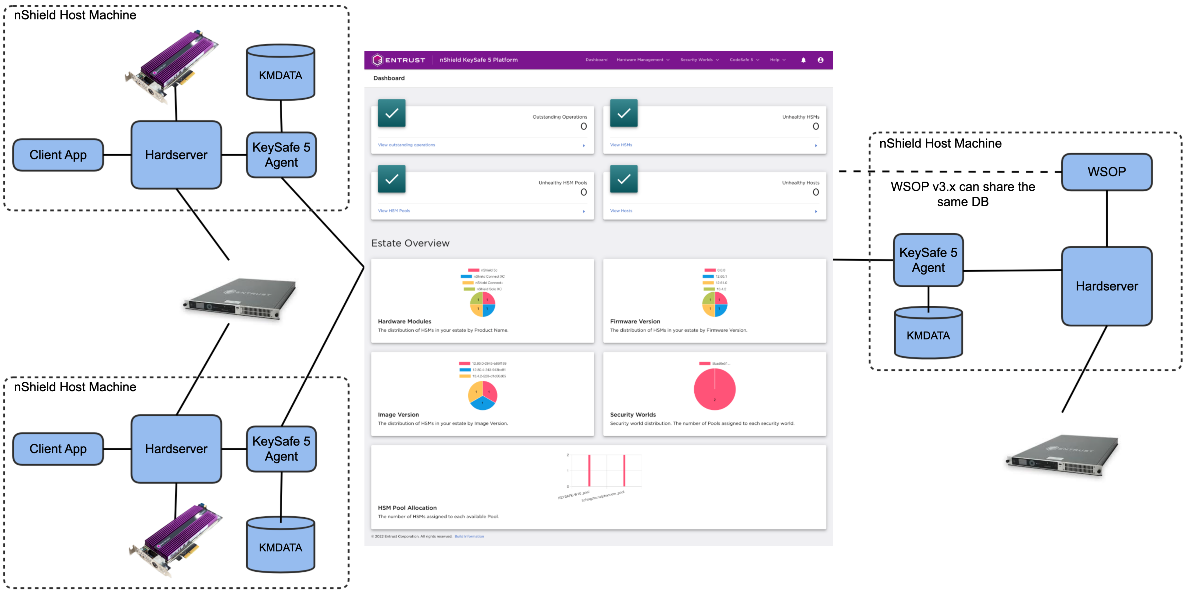
Table of Contents

1. Introduction

KeySafe 5 provides a centralized means to securely manage a distributed nShield HSM estate, including the creation and management of Security Worlds and associated resources (Softcards & Card Sets).

KeySafe 5 provides this capability in two forms: HTTP REST APIs for HSM Management and Security World management, and a graphical user interface. Only authenticated clients are permitted access to the service, providing assurance that your HSM and Security World data remain usable only by clients that are permitted access.

Typical KeySafe 5 deployment:



The main central management platform of KeySafe 5 is deployed as either a Kubernetes application or as a cluster of Virtual Machines (VMs).

For each nShield client machine that you want to manage using this platform, you must install a KeySafe 5 agent binary alongside the existing nShield hardserver. A KeySafe 5 agent is installed on the nShield Connect for nShield Connect images released with Security World v13.4 and later software.

2. OVA Installation Guide

Entrust provides a single virtual node in OVA format. You use this template to install KeySafe 5. See your selected hypervisors documentation for installation steps, as these may differ from those specified below.

> Entrust recommends a deployment of three KeySafe 5 nodes for High Availability. Single-node deployments are feasible but they are only recommended for demos, not for production environments. Other node counts are not recommended.

2.1. Install KeySafe 5 from an OVA template

For instructions, see the documentation from the VM vendor.

2.2. KeySafe 5 prerequisites to using the OVA template

Make sure that:

- You know the IP address and any required network connection information, such as the domain name and the DNS and gateway IP addresses, for the machine on which you are installing KeySafe 5.

  You must use an IPv4 address. KeySafe 5 does not support IPv6 addresses.

- You have the required permissions to install software on the target system.
- You must enable VM host affinity, affinity groups, or equivalent for the KeySafe 5 VM to avoid Admin Key Recovery if for some reason you have to migrate the host in the future.

  For the specific feature to enable during VM creation and for instructions, see the docu mentation from the VM vendor.

2.3. Starting the KeySafe 5 VM

1. If you selected the large installation configuration earlier in this procedure, you need to manually change the disk size alloted to the VM from the standard 80 GB to 160 GB. The OVA template sets the appropriate number of CPUs and the memory allocation but it cannot automatically change the standard disk size.
2. Power on the KeySafe 5 VM.

3. Configure the node as needed. For details, see one of the following:
   - If this is the first KeySafe 5 node in the system or if you want this to be a stand-alone node, follow the steps in Configuring the First KeySafe 5 Node.
   - If you are adding this node to an existing KeySafe 5 cluster, follow the steps in Adding a New KeySafe 5 Node to an Existing Cluster.

2.4. Configuring the First KeySafe 5 Node

This procedure explains how to configure this system as the first KeySafe 5 node in the system.

1. Log into the system on which you installed the KeySafe 5 software. The KeySafe 5 installer will automatically start running as soon as the VM is powered on.
2. Enter a password for the KeySafe 5 system administration account and press **Enter**. Password requirements are configured by a KeySafe 5 administrator in the System Settings.

   This password controls access to the Entrust KeySafe 5 System Console that allows users to perform some KeySafe 5 administration tasks. It does not permit a KeySafe 5 user to access the full OS.

   > Make sure you keep this password in a secure place. If you lose the password, you will need to contact Entrust Support. For security reasons, KeySafe 5 does not provide a user-accessible password recovery mechanism.

   The installer configures KeySafe 5 and then starts the appropriate services. This process can take up to 30 minutes to complete. When the installer has finished, KeySafe 5 displays a confirmation dialog stating that the setup was completed successfully.

3. Save the address of the KeySafe 5 UI (also known as the Management IP Address) from the confirmation dialog. You will need this address in the next step.

   When you are done, press **Enter** to finish the installation. KeySafe 5 displays the CentOS login prompt when the installation is complete.

4. To initialize the KeySafe 5 UI and finish the configuration of the first node, do the following:
   a. Use a web browser to navigate to `https://<node-ip-address>`, where *<node-ip-address>* is the Management IP address.

b. If prompted, add a security exception for the KeySafe 5 IP address and proceed to the KeySafe 5 Appliance Management UI.

   KeySafe 5 uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see KeySafe 5 Certificates.

c. On the **KeySafe 5 Login** page, enter `secroot` for both the username and password.

d. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.

e. On the Welcome to KeySafe 5 screen, click **Continue as a Standalone Node**.

f. On the **Change Password** page, enter a new password for the `secroot` account and click **Update Password**.

g. On the **Configure E-Mail and Mail Server Settings** page, specify your email settings.

   If you specify an email address, KeySafe 5 sends an email with the Admin Key for the new node. It also sends system alerts to this email address.

   To disable alerts, select the **Disable e-mail notifications** checkbox. You can then download the Admin Key from the Settings tab in the KeySafe 5 Appliance Management UI.

h. When you are done, click **Continue**.

i. On the Download Admin Key page, click the **Download** button to save the admin key locally. Keep the admin key in a safe place for later use. When KeySafe 5 prompts for an admin key to recover your KeySafe 5 system, you must provide this admin key to proceed. If you do not have your admin key, you may lose your data.

   > ℹ Whenever the admin key is regenerated, KeySafe 5 forces you to download the admin key.

j. On the **Authentication** page, select either:

   i. **Continue with Local Authentication** which enables the use of locally authenti cated user accounts for access control to the KeySafe 5 Appliance Management UI.

      > ⚠ Selecting this option means that the KeySafe 5 UI and its API will be unauthenticated. Entrust does not recommend this option.

ii. **Setup Authentication** which then presents the user with the ability to configure OpenID Connect Provider to protect the KeySafe 5 UI, its API and the KeySafe 5 Appliance Management UI. For more information, see the Configuring an OpenID Connect Provider section.

k. When you are finished, you are presented with the following options:

i. **Continue to Appliance Management** which will take you to the KeySafe 5 Appliance Management UI, for more information see Appliance Management Administration. From this point onwards access to the KeySafe 5 Appliance Management UI is via `https://<node-ip-address>/appliance`, where *<node-ip-address>* is the Management IP address.

ii. **Continue to nShield KeySafe 5** which will take you to the KeySafe 5 dashboard. At this stage the dashboard will be empty, to finish configuring KeySafe 5, see KeySafe 5 Administration.

2.5. Adding a New KeySafe 5 Node to an Existing Cluster

2.5.1. Before You Begin

1. Make sure you know the IP address of any KeySafe 5 node that is already part of the cluster you want to join.
2. If Startup Authentication is enabled, you cannot add a new KeySafe 5 node. You must disable Startup Authentication on the existing KeySafe 5 node, add the new node, and then re-enable Startup Authentication.

2.5.2. Procedure

1. Log into the VM on which you installed the KeySafe 5 software.
2. Enter a password for the KeySafe 5 system administration account and press **Enter**. Password requirements are configured by a KeySafe 5 administrator in the System Settings.

   This password controls access to the Entrust KeySafe 5 System Console that allows users to perform some KeySafe 5 administration tasks. It does not permit a KeySafe 5 user to access the full OS.

   > Make sure you keep this password in a secure place. If you lose the password, you will need to contact Entrust Support. For security reasons, KeySafe 5 does not provide a user-accessible password recovery mechanism.

3. Use a web browser to navigate to `https://<node-ip-address>`, where *<node-ip-address>* is the Management IP address you specified during installation.

   > If you do not know the Management IP address for the node, log into the system on which the node is installed as . KeySafe 5 displays the Entrust KeySafe 5 System Console. From the menu, select **Manage Network Settings > Show Current Network Configuration**.

4. If prompted, add a security exception for the KeySafe 5 IP address and proceed to the KeySafe 5 Appliance Management UI.

   KeySafe 5 uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see KeySafe 5 Certificates.

5. On the **KeySafe 5 Login** page, enter `secroot` for both the username and password.
6. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
7. On the Welcome to KeySafe 5 screen, click **Join an Existing Cluster**.

   The Join Existing Cluster window displays.

8. On the Get Started page, review the overview information to determine that you are ready to begin. This includes:
   a. Access to the cluster you are joining the node to. We recommend that you open the KeySafe 5 Appliance Management for the cluster in a different tab or browser window.
   b. Permissions on both this node and the cluster node so you can download and import the required certificates and files.
   c. A passphrase to use during the joining process. Passphrase requirements are configured by a KeySafe 5 administrator in the System Settings. This phrase is a temporary string used to encrypt the initial communication between this node and the existing KeySafe 5 cluster.
   d. Verifying that both this node and the cluster node are running the same KeySafe 5 version and build. The version number for the cluster node is on the **Settings > System Upgrade** page.
9. Click **Continue**.
10. On the Download CSR page, click **Generate and Download CSR**.
11. Click **Continue**.

12. Switch to one of the existing nodes in the cluster and navigate to the Cluster page.
13. Select **Actions > Add a Node**.
14. On the Add a Node window, upload the CSR that you downloaded from the new node (in .pem format) and enter a passphrase to use during the joining process.
15. Click **Save and Download Bundle** to download the certificate bundle from the cluster node.

    The certificate bundle is a .zip file you must unpack. It contains both an encrypted SSL certificate in .p12 format and a CA certificate in .pem format.

16. Click **OK** to close the Add a Node window.
17. Return to the new node and click **Continue**.
18. On the Node page, upload the encrypted SSL certificate and CA certificate that you downloaded from the cluster node, enter the IP address or hostname of any node in the existing cluster, and enter the passphrase that you selected.
19. Click **Join**.
    a. During the joining process, a status page is displayed on the new node. Do not refresh the browser while this is in process.
    b. The cluster will automatically be placed in maintenance mode.
    c. The node will restart after the join is complete.
20. When the node has successfully restarted, click **Login**.

3. OVA Upgrade Guide

Entrust provides a single upgrade kit in ISO format. You use this to upgrade KeySafe 5.

3.1. KeySafe 5 Supported Upgrade Paths

You can only upgrade between successive versions.

Supported upgrade paths are:

Current Version	Upgrade Path
v1.1	v1.2

3.2. Upgrading the KeySafe 5 cluster

You can upgrade the entire KeySafe 5 cluster from any node in the cluster using the KeySafe 5 Appliance Management UI. KeySafe 5 automatically applies the upgrade to all nodes in the cluster sequentially.

3.2.1. Before You Begin

- Make sure that the KeySafe 5 nodes can communicate with one another on port TCP/8443 and TCP/5432.
- We recommend you back up your KeySafe 5 cluster before you upgrade it. For details, see Backing Up KeySafe 5 Through the KeySafe 5 Appliance Management UI.
- Please download your Admin Key and store it in a safe place before you upgrade. If KeySafe 5 prompts for an admin key to recover your KeySafe 5 system, you must provide this admin key to proceed. If you do not have your admin key, you may lose your data. For details, see Downloading Your Admin Key Part.
- We recommend that you enable the support login on all cluster nodes before you start the upgrade. For details, see Enabling or Disabling the Support Login.
- Make sure your network connection to the KeySafe 5 node is as fast and as stable as possible. To begin the upgrade, you need to upload the upgrade ISO image to the KeySafe 5 node in one continuous session. If the upload times out or if connectivity to the KeySafe 5 node is lost during the upload, you will see error messages in KeySafe 5 and you must re-upload the file from scratch. KeySafe 5 cannot resume the upload from where it left off during a previous session.
- Make note of the KeySafe 5 agents listed by the product, this will be useful when re-

enrolling the KeySafe 5 agents during the upgrade procedure.

3.2.2. Procedure

1. Log into the KeySafe 5 Appliance Management UI using an account with Security Admin privileges
2. In the top menu bar, click **Cluster** and make sure the **Status** of the cluster is **Healthy**. If it is not, you must resolve those issues before you can upgrade the cluster.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **System Upgrade**.
5. Click **Browse**, navigate to the Entrust ISO upgrade file, and click **Open**.
6. Click **Upload File**. If the **Upload File** button is not active, make sure that you have selected an ISO file and that the cluster is healthy.

   After KeySafe 5 uploads and validates the ISO file, KeySafe 5 begins the automatic upgrade process by copying the ISO file from the current node to all of the other KeySafe 5 nodes in the cluster. After the ISO file has been copied, KeySafe 5 displays a Success message. Click **Close** to continue with the upgrade.

   KeySafe 5 displays a status message stating that the upgrade is in process along with a **Cancel Upgrade** button in case you want to stop the process.

7. Click **Finish Upgrade**.

   > Ensure you are still on the same node where you clicked **Upgrade File**.

   KeySafe 5 displays a message stating that the cluster will be put into maintenance mode during this procedure and that all nodes will be rebooted. While in maintenance mode no KeySafe 5 configuration changes can be made and no new VMs can be added.

8. Click **Proceed**.

   KeySafe 5 displays a status message stating that the cluster nodes are being rebooted. It may take a while for this process to run on all nodes except for the current node. When all of the other nodes have been upgraded and are back online, KeySafe 5 reboots the current node to finish the upgrade process on that node. At this point, you will be automatically logged out of the KeySafe 5 Appliance Management UI on that node. You can monitor the progress on the KeySafe 5 Appliance Management UI of the other nodes. This again may take a while to complete.

When any node is being upgraded, if you have access to the KeySafe 5 System Console, you can view the the CentOS upgrade messages.

> When KeySafe 5 reboots the current node, you may see a message that the application cannot connect to the server. The browser page may then display a "connection refused" message. Wait a few moments for the node to finish rebooting, then refresh your browser page. You should then see the KeySafe 5 Login page.

If Refresh does not work, try to access the KeySafe 5 Appliance Management UI on a different node in the cluster. If the KeySafe 5 Appliance Management UI fails for all nodes, the hardware signature for one or more nodes may have changed during the upgrade. To restore access to KeySafe 5, contact Entrust nShield Technical Support at nshield.support@entrust.com.

9. To verify the upgrade, return to **Settings > System Upgrade** and verify the settings for **Current Version** and **Previous Version**.
10. The KeySafe 5 agents can now be updated and re-enrolled into the system, for more information please see KeySafe 5 Agent Installation.

3.3. Agent Upgrade

To update the KeySafe 5 agent installed on a machine:

- Take a backup of the agent config directory located at `%NFAST_DATA_HOME%/keysafe5/conf`.
- Uninstall the existing KeySafe 5 agent as detailed in the KeySafe 5 Installation Guide for the currently installed version of the product.
- Install the new KeySafe 5 agent as detailed in chapter *KeySafe 5 Agent Installation*.
- Restore existing agent configuration and restart the agent.

3.4. Upgrading supporting software

3.4.1. Upgrade from KeySafe 5 1.1 recommended versions

KeySafe 5 1.1 recommended MongoDB 5.0.10. This section details how to upgrade the software from these versions to the latest recommended compatible versions.

3.4.2. MongoDB 5.0.10 to 5.0.19

To update a non-Kubernetes existing Mongo install to a Mongo 5.0.19 install, see the official documentation at Upgrade to the Latest Revision of MongoDB.

To update a Mongo 5.0.10 install deployed via Bitnami Helm Charts:

```
# Obtain details of currently deployed helm charts
# Substitute chart and namespace values in the commands below as required
helm list -A

# Fetch current MongoDB helm chart deployed values
helm -n mongons get values --all --output yaml mongo-chart > mongo-chart-values.yaml

# Obtain the names of the existing mongo secrets
# Substitute secret names in the commands below as required
kubectl get secrets -n mongons

# Make copies of the existing secrets, this is required as the existing ones will be removed during the upgrade
process
kubectl get secret mongodb-server-certificates -n=mongons -o yaml \
  | sed 's/mongodb-server-certificates/mongodb-server-certificates-upgrade/' \
  | kubectl apply -f -
kubectl get secret mongo-chart-mongodb -n=mongons -o yaml \
  | sed 's/mongo-chart-mongodb/mongo-chart-mongodb-upgrade/' \
  | kubectl apply -f -

# Upgrade helm chart based on existing deployed values
helm upgrade --install mongo-chart \
    --namespace=mongons \
    --values mongo-chart-values.yaml \
    --set image.tag=5.0.19-debian-11-r3 \
    --set auth.existingSecret=mongo-chart-mongodb-upgrade \
    --set tls.autoGenerated=false \
    --set tls.existingSecret=mongodb-server-certificates-upgrade\
    --wait --timeout 5m \
    bitnami/mongodb --version 12.1.31

# Obtain details of newly deployed helm charts
helm list -A
```

The helm listing for mongo-chart may fail to update app version from 5.0.10 to 5.0.19. This bug is only visual and the image will have updated successfully. This can be confirmed by using kubectl.

3.4.2.1. MongoDB User Configuration

To configure the MongoDB database correctly, access the MongoDB shell to create a user with the minimal permissions required for using the `codesafe-mgmt-db`, `hsm-mgmt-db` and `sw-mgmt-db` databases. See Database: User Roles.

Note that the username needs to match the subject of the client certificate, as found by the following command.

```
$ kubectl get secret --namespace nshieldkeysafe5 mongodb-client-certificates \
  -o jsonpath="{.data.tls\.crt}" | base64 --decode | \
  openssl x509 -out mongo-client-cert.pem
```

```
$ openssl x509 -in mongo-client-cert.pem -subject | head -n 1
```

In this example we will use ks5-mongo-user

We then run the mongo client container.

```
$ export MONGO1=mongo-chart-mongodb-0.mongo-chart-mongodb-headless.mongons.svc.cluster.local:27017
$ export MONGO2=mongo-chart-mongodb-1.mongo-chart-mongodb-headless.mongons.svc.cluster.local:27017
$ export MONGODB=${MONGO1},${MONGO2}
$ export MONGO_RUN="kubectl -n mongons exec mongo-chart-mongodb-0 0 -- "
$ export TLS_PRIVKEY="$(${MONGO_RUN} bash -c 'cat /certs/mongodb.pem')"
$ export TLS_CERT="$(${MONGO_RUN} bash -c 'cat /certs/mongodb-ca-cert')"
$ export MONGODB_ROOT_PASSWORD=$(kubectl get secret --namespace mongons \
  mongo-chart-mongodb-upgrade -o jsonpath="{.data.mongodb-root-password}" \
  | base64 --decode)
$ kubectl run --namespace mongons mongo-chart-mongodb-client \
  --rm --tty -i --restart='Never' --env="MONGODB_ROOT_PASSWORD=$MONGODB_ROOT_PASSWORD" \
  --env="TLS_PRIVKEY=$TLS_PRIVKEY" --env="TLS_CERT=$TLS_CERT" --env="MONGODB=$MONGODB" \
  --image bitnami/mongodb:5.0.19-debian-11-r3 --command -- bash
```

Once inside the mongo client container, we need to set up a connection to the server before we can start mongo admin and create the user. After we finish creating the user, we need to exit mongo admin, and then the mongo-client container.

```
$ echo "$TLS_CERT" > /tmp/tls.crt
$ echo "$TLS_PRIVKEY" > /tmp/tls.key
$ mongo admin --tls --tlsCAFile /tmp/tls.crt --tlsCertificateKeyFile /tmp/tls.key \
  --host $MONGODB --authenticationDatabase admin -u root -p $MONGODB_ROOT_PASSWORD

> use admin
> db.createRole(
  {
    role: "hsm-mgmt-db-user",
    privileges: [
        {
          "resource": {"db": "hsm-mgmt-db", "collection": ""},
          "actions": ["createIndex", "find", "insert", "remove", "update"]
        },
      ],
    roles: []
  }
)
> db.createRole(
  {
    role: "sw-mgmt-db-user",
    privileges: [
        {
          "resource": {"db": "sw-mgmt-db", "collection": ""},
          "actions": ["createIndex", "dropCollection", "find", "insert", "remove", "update"]
        },
      ],
    roles: []
  }
)
> db.createRole(
  {
    role: "codesafe-mgmt-db-user",
    privileges: [
        {
          "resource": {"db": "codesafe-mgmt-db", "collection": ""},
          "actions": ["createIndex", "find", "insert", "remove", "update"]
        },
      ],
    roles: []
  }
)
> use $external
> x509_user = {
   "roles" : [
     {"role": "codesafe-mgmt-db-user", "db": "admin" },
     {"role": "hsm-mgmt-db-user", "db": "admin" },
     {"role": "sw-mgmt-db-user", "db": "admin" },
   ]
 }
> db.updateUser("CN=ks5-mongo-user", x509_user)
> exit
$ exit
```

4. KeySafe 5 Agent Installation

4.1. Installation

The KeySafe 5 agent runs alongside the existing hardserver and enables the central management platform to manage all HSMs and Security Worlds visible to the hardserver.

> The KeySafe 5 agent is a privileged client of the hardserver. For more information on privileged clients, see the nShield Security World Software documentation.

The connection between the agent and the central monitoring platform is via the RabbitMQ message bus using the Advanced Message Queueing Protocol (AMQP). It is configured in the KeySafe 5 agent configuration file.

Ensure the system clock of the KeySafe 5 agent is synchronized with the central platform.

The KeySafe 5 agent ensures that all key management data, with the exception of keys, is synchronized between the nShield client machine and a central (MongoDB) database.

This means that when resources, such as Card Sets or Softcards, appear in the `kmdata/local` directory on a client machine, they are automatically stored in the central database. It also means that when a Card Set or Softcard is created via the new management tools, the resource also appears in `kmdata/local` on any host machine that is in the right Security World.

The Card Set or Softcard can then be used with the traditional nShield tools on each nShield client machine.

> If a resource is deleted via the KeySafe 5 application then it will be removed from `kmdata/local` for all client machines, and Connects, running a KeySafe 5 agent. If the resource is deleted locally on a nShield client machine then that deletion is not synchronized to other client machines in the same Security World.

The KeySafe 5 agent will also report on the status of CodeSafe 5 machines/certificates visible to the agent, and allow these resources to be managed via KeySafe 5. The amount of time taken for the agent to publish a CodeSafe 5 update message will increase by several seconds per CodeSafe 5 resource (machine or certificate) in the system. This means that in systems with many CodeSafe 5 machines/certificates present, KeySafe 5 will be slower to reflect local changes in the state of these resources.

If you are upgrading an existing KeySafe 5 Agent install, see Agent Upgrade.

4.2. Install on Linux

1. Untar the KeySafe 5 agent install package to the root directory of the machine. The agent install package can be found in `keysafe5-agent` directory of the KeySafe 5 release package.

   This unpacks the agent and associated scripts into the `/opt/nfast/` directory.

   ```
   $ cd /
   $ sudo tar -xf /path/to/keysafe5-1.2.0-Linux-keysafe5-agent.tar.gz
   ```

2. Configure this KeySafe 5 agent instance as described in Agent Configuration and AMQP authentication.
3. Run the appropriate install script depending on the state of the hardserver:
   - If the hardserver is running, use the KeySafe 5 specific install script so the hardserver is not restarted.

     ```
     sudo /opt/nfast/keysafe5/sbin/install
     ```

   - When the hardserver is not running, use the nShield install script to install both the KeySafe 5 agent and the hardserver.

     ```
     sudo /opt/nfast/sbin/install
     ```

> The agent must point to a working RabbitMQ otherwise it will fail to start.

The installer creates the following items, as required:

- Either a SysV-style init script or systemd script for automatically starting and stopping the service.
- The `keysafe5d` user.

  This user is dedicated to running the `keysafe5-agent` service, and is a member of the `nfast` and `nfastadmin` groups.

The KeySafe 5 agent is not affected by the standard nShield `/opt/nfast/sbin/init.d-ncipher` script. To stop, start, or restart the KeySafe 5 agent you may either:

- Use `/opt/nfast/scripts/init.d/keysafe5-agent`, or
- Use your standard init system scripts, addressing the `nc_keysafe5-agent` service.

4.3. Install on Windows

The KeySafe 5 Agent requires the hardserver TCP ports be enabled. To do this, either:

- Run `config-serverstartup.exe --port 9000 --privport 9001`, or
- Edit the file (located at `%NFAST_KMDATA%\config\config`) and set `nonpriv_port=9000` and `priv_port=9001`.

After enabling the hardserver TCP ports, you must restart the hardserver service.

If those ports are not available and different ports are set, then the environment variables `NFAST_SERVER_PORT` and `NFAST_SERVER_PRIVPORT` must also be set appropriately as described in the nShield documentation. They may be set globally in System Environment Variables, or only for this service by adding a `Multi-String Value` named `Environment` under `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\nShield KeySafe 5 Agent`, and to *Value data* adding the lines `NFAST_SERVER_PORT=port-number` and `NFAST_SERVER_PRIVPORT=port-number`. You may need to restart the computer after adding the System Environment Variables.

1. Launch the `Keysafe5-agent.msi` installer. The installer is in the `keysafe5-agent` directory of the KeySafe 5 release package.

   This msi creates the nShield KeySafe 5 agent service but does not start it.

2. Populate the KeySafe 5 agent configuration file as described in Agent Configuration and AMQP authentication.

   The nShield KeySafe 5 agent service will not start if the certificates are not installed.

   For instructions on the agent configuration file, see Obtaining the KeySafe 5 Agent Certificates.

4.4. Agent Configuration

The KeySafe 5 agent configuration file is located at `%NFAST_DATA_HOME%/keysafe5/conf/config.yaml`.

The install contains an example configuration file at `%NFAST_DATA_HOME%/keysafe5/conf/config.yaml.example`. Make a copy of it at the same location and rename the copy to `%NFAST_DATA_HOME%/keysafe5/conf/config.yaml`.

> Unless configured otherwise, `%NFAST_DATA_HOME%` is located at `/opt/nfast` on Linux and `%ProgramData%\nCipher` on Windows.

Configuration Key	Description	Example Value
override_hostname	Set the hostname for this agent. This appears as the Host resource name in KeySafe 5. The hostname is set by the operating system if not overridden here. This is not related to the hostname used by TLS authentication.	hostname
logging.level	Minimum severity level of log statements to output. Valid values: trace, debug, info, warning, error. The default is to output at info level and above.	info
logging.format	Format of the log statements. Valid values: json, logfmt. The default is to output in json format.	json
logging.file.enabled	To enable log output to file, set to true. The default is to output to file (true).	true
logging.file.path	The absolute path of the file that logs should be written to. The default is /opt/nfast/log/keysafe5-agent.log on Linux and %ProgramData%\nCipher\Log Files\KeySafe5-agent.log on Windows.	/opt/nfast/log/keysafe5-agent.log
amqp.url	The URL points to the AMQP service with its IP address or DNS name, including the port number. For an OVA install, this is the IP address or DNS name of the VM. IPv6 addresses must be in the form [host]:port. If required, a virtual host may be specified at the end of the address. This parameter is required, there is no default.	127.0.0.1:5671/nshieldvhost
amqp.auth_type	Authentication method for the AMQP connection. Valid values: none, pwd, tls. The default is to use TLS authentication.	tls
amqp.tls_username_location	For auth_type 'tls', the AMQP username is encoded in a field of the X.509 certificate. When a RabbitMQ server is configured to allow X.509 authentication, it is specified which field to extract the username from within the certificate. This agent configuration item identifies which field of the certificate contains the username and should match the setting on the RabbitMQ server. Valid values: DistinguishedName, CommonName, SAN-DNS-Field0 (the first DNS field in the Subject Alternative Name of the certificate).	SAN-DNS-Field0
amqp.disable_tls	To disable Mutual TLS for the AMQP connection, set to true. The default is to use Mutual TLS (false). Entrust recommends that this is always set to false.	false

Configuration Key	Description	Example Value
`amqp.min_protocol_version`	The minimum TLS protocol version that is used by the AMQP connection of the keysafe5 agent. The default is `TLSV1_2`.	`TLSV1_2`
`amqp.cipherSuites`	The available ciphersuites for the AMQP connection of the keysafe5 agent. The defaults are `ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-ECDSA-CHACHA20-POLY1305, ECDHE-RSA-CHACHA20-POLY1305`	`ECDHE-ECDSA-AES128-GCM-SHA256`
`kmdata_poll_interval`	The rate at which the agent polls the `kmdata` directory to look for changes. The format is as used for `update_interval`. The default is once a second.	`1s`
`update_interval`	The period of time between publishing data updates. The interval string is a sequence of decimal numbers, each with optional fraction and a unit suffix, such as "300ms", "1.5h" or "2h45m". Valid time units are "ns", "us" (or "µs"), "ms", "s", "m", "h". The default is once a minute.	`1m`
`max_update_message_response_time`	The maximum amount of time to allow the central plat form to pull update messages sent by this agent. Update messages published by this agent will expire after the lower of this time, or the configured update_interval. This setting impacts the freshness of the data processed by the central platform. The default is 1 minute.	`1m`
`health_interval`	The period of time between checking the underlying service health and attempting recovery if necessary. The format is as used for `update_interval`. The default is once a minute.	`1m`
`codesafe_update_interval`	The period of time between publishing CodeSafe 5 data updates. The format is as used for `update_interval`. The default is once every 5 minutes.	`3m`
`codesafe_cache_period`	The `codesafe_cache_period` specifies how often the CodeSafe 5 certificate cache will expire. The caching is performed to negate performance impacts of running unnecessary CodeSafe 5 certificate commands. Cache expiry may be performed earlier if approaching a time where a certificates validity status may change, that is, when it is approaching `NotBefore` or `NotAfter`. The cache is invalidated if there is a change in CodeSafe 5 certificates. The format is as used for `update_interval`. The default is 60 minutes.	`60m`

Configure the KeySafe 5 agent's AMQP connection to use the same RabbitMQ instance used by the central management platform that you want to connect to. In an OVA deployment the address of the RabbitMQ instance is the IP address or the DNS name of a node in the cluster.

4.5. AMQP authentication

You can configure the authentication method for the AMQP connection as one of the following options:

- `none` No authentication.
- `pwd` Username and password authentication.
- `tls` X.509 certificate authentication.

> ℹ Entrust recommends restricting access to files containing sensitive authentication details. On Linux, the KeySafe 5 agent installer will create the required files with appropriate permissions.

> ❗ The username must contain the KeySafe 5 agent's hostname (set either by `override_hostname` in the agent configuration file, or defaults to the machine's hostname). If the username does not contain the KeySafe 5 agent's hostname then the agent will not start.

4.5.1. TLS

You must create the `%NFAST_DATA_HOME%/keysafe5/conf/amqp/tls` directory manually so that you can store the TLS key and certificates for the agent's connection to AMQP there in the following files:

ca.crt The CA certificate.

tls.key The agent's private key.

tls.crt A valid certificate of the key signed by the Certificate Authority.

Your certificates will need to adhere to X.509 v3, sometimes known as a multiple-domain certificates, or SAN certificates. The X.509 extension Subject Alternative Name (SAN) allows specifying multiple hostnames, and has replaced Common Name as the source of the hostname.

The username extracted from the TLS client certificate (`tls.crt`) is defined by the agent configuration item `amqp.tls_username_location`. By default, this is set to `SAN-DNS-Field0` (the first DNS field in the Subject Alternative Name of the certificate) but can optionally be set to `Distinguished Name` or `CommonName` to match the TLS authentication settings on the RabbitMQ server.

> The extracted certificate username must contain the KeySafe 5 agent's hostname (set either by `override_hostname` in the agent configuration file, or defaults to the machine's hostname). If the username does not contain the KeySafe 5 agent's hostname then the agent will not start.

4.5.1.1. Generating a KeySafe 5 agent private key and TLS certificate

To generate a private key and certificate signing request (CSR) for a specific KeySafe 5 agent, use `%NFAST_HOME%/keysafe5/bin/amqptls`.

For instructions to create the files using a bespoke CSR file, see Obtaining the KeySafe 5 Agent Certificates.

1. Generate the agent's private key

   On Linux:

   ```
   $ /opt/nfast/keysafe5/bin/amqptls -keypath=/opt/nfast/keysafe5/conf/amqp/tls/tls.key -keygen
   Private key has been generated and saved to /opt/nfast/keysafe5/conf/amqp/tls/tls.key

   When configuring AMQP TLS for this KeySafe 5 agent, the key should be saved to
   /opt/nfast/keysafe5/conf/amqp/tls/tls.key with file permissions and ownership as documented in the KeySafe
   5 Installation Guide
   ```

   On Windows the command to write to `%NFAST_DATA_HOME%\keysafe5\conf\amqp\tls\tls.key` is:

   ```
   %NFAST_HOME%\bin\amqptls.exe -keypath=C:\ProgramData\nCipher\keysafe5\conf\amqp\tls\tls.key -keygen
   ```

   This will generate an ECDSA P-521 private key and save it to the file pointed to by the `keypath` option. If `keypath` is not specified the file `tls.key` is saved to the current directory.

2. Generate the CSR

   On Linux:

   ```
   $ /opt/nfast/keysafe5/bin/amqptls -keypath=/opt/nfast/keysafe5/conf/amqp/tls/tls.key -csrgen
   CSR has been generated and saved to ks5agent_demohost.csr
   ```

   On Windows the command is:

```
%NFAST_HOME%\bin\amqptls.exe -keypath=C:\ProgramData\nCipher\keysafe5\conf\amqp\tls\tls.key -csrgen
```

This will generate a certificate signing request and save it to `ks5agent_<agent_hostname>.csr` (where `<agent_hostname>` is the value of `override_hostname` in the KeySafe 5 agent configuration file, if set, or the host machines host name). Alternatively, the CSR can be printed to the console, rather than saved to a file, by specifying `-csr-stdout`.

The generated CSR requests a certificate that contains the agent hostname as the CommonName and as a DNS SubjectAlternativeName (SAN).

3. Create a TLS Certificate for this KeySafe 5 agent
    a. Log into the KeySafe 5 Appliance Management UI using an account with Security Admin privileges.
    b. In the top menu bar, click **Settings**.
    c. In the **Application Settings** section, click **KeySafe5 Settings**.
    d. Click **Downloads > nShield KeySafe 5 Agent Certificates**.
    e. In the **Upload CSR File** section, click **Load File** and select the CSR file you wish to use for certificate generation.
    f. Click **Generate and Download Certificate** to download the certificate bundle from the cluster node.

       The certificate bundle is a .zip file you must unpack. It contains both the CA certificate and a TLS certificate.

4. Configure the KeySafe 5 agent

   The resulting TLS certificate and accompanying CA certificate, along with the agent's private key should be stored within `%NFAST_DATA_HOME%/keysafe5/conf/amqp/tls` in the following files:

   - `ca.crt` - The CA certificate.
   - `tls.key` - The agent's private key.
   - `tls.crt` - A valid certificate of the key signed by the Certificate Authority.

4.6. KeySafe 5 agent on network-attached HSMs

A KeySafe 5 agent is installed on the nShield Connect for nShield Connect images released with Security World v13.4 and later software. This agent allows an nShield Connect to be monitored and managed without, or in addition to, the Connect being enrolled to a nShield host machine (a machine with nShield Security World software installed) which also has a

KeySafe 5 agent installed.

By default, the KeySafe 5 agent on the nShield Connect is disabled. It must be configured to communicate with the central KeySafe 5 platform, and enabled. The agent can only be configured via the nShield Connect serial console.

4.6.1. ks5agent command (only on serial console network-attached HSMs)

The KeySafe 5 agent is configured and managed on the Connect using the `ks5agent` Serial Console command.

```
(cli)help ks5agent

        Manage the KeySafe 5 agent

        USAGE
          ks5agent
          ks5agent enable
          ks5agent disable
          ks5agent version
          ks5agent logs [tail [linecount]]
          ks5agent cfg [amqp.url=x.x.x.x:5671]
          ks5agent resetcfg
          ks5agent amqpcsr
          ks5agent amqptls [ca.crt|tls.crt] [data]
          ks5agent amqpuser
          ks5agent amqppwd


        OPTIONS
          enable      Start the KeySafe 5 agent (setting will persist on reboot)
          disable     Stop the KeySafe 5 agent
          version     Show version information for the KeySafe 5 agent
          logs        Display the KeySafe 5 agent log file
          cfg         Configure the KeySafe 5 agent
          resetcfg    Restore the KeySafe 5 agent configuration file back to the default values for this Connect
          amqpcsr     Generate a Certificate Signing request for creation of KeySafe 5 agent TLS certificate
          amqptls     Show/set the TLS certificates for the KeySafe 5 Agent AMQP connection
          amqpuser    Show the agent's username for AMQP password or TLS based authentication
          amqppwd     Configure the password for the agent to use for AMQP password-based authentication

        If no action is specified, the current status of the KeySafe 5 agent will be
        displayed.
```

4.6.1.1. ks5agent cfg

The agent configuration can be displayed and set using the `ks5agent cfg` command.

```
(cli)ks5agent cfg
override_hostname: nshield_module_AAAA-AAAA-AAAA
logging:
  level: info
  format: json
  file:
    enabled: false
    path: /opt/nfast/log/keysafe5-agent.log
amqp:
  url: 127.0.0.1:5671
  auth_type: tls
  tls_username_location: SAN-DNS-Field0
  disable_tls: false
  minProtocolVersion: TLSV1_2
  cipherSuites:
  - ECDHE-ECDSA-AES128-GCM-SHA256
  - ECDHE-RSA-AES128-GCM-SHA256
  - ECDHE-ECDSA-AES256-GCM-SHA384
  - ECDHE-RSA-AES256-GCM-SHA384
  - ECDHE-ECDSA-CHACHA20-POLY1305
  - ECDHE-RSA-CHACHA20-POLY1305
kmdata_poll_interval: 1s
update_interval: 1m
max_update_message_response_time: 1m
health_interval: 1m
codesafe_update_interval: 3m
codesafe_cache_period: 60m

(cli)ks5agent cfg amqp.url=<IPADDRESS>:5671/nshieldvhost update_interval=2m
override_hostname: nshield_module_AAAA-AAAA-AAAA
logging:
  level: info
  format: json
  file:
    enabled: false
    path: /opt/nfast/log/keysafe5-agent.log
amqp:
  url: <IPADDRESS>:5671/nshieldvhost
  auth_type: tls
  tls_username_location: SAN-DNS-Field0
  disable_tls: false
  minProtocolVersion: TLSV1_2
  cipherSuites:
  - ECDHE-ECDSA-AES128-GCM-SHA256
  - ECDHE-RSA-AES128-GCM-SHA256
  - ECDHE-ECDSA-AES256-GCM-SHA384
  - ECDHE-RSA-AES256-GCM-SHA384
  - ECDHE-ECDSA-CHACHA20-POLY1305
  - ECDHE-RSA-CHACHA20-POLY1305
kmdata_poll_interval: 1s
update_interval: 2m
max_update_message_response_time: 1m
health_interval: 1m
codesafe_update_interval: 3m
codesafe_cache_period: 60m
```

> The agent configuration values for `override_hostname` and `logging.file` are fixed and can not be set on nShield Connect. The value for `override_hostname` will be set to `nshield_module_{esn}`.

Multiple configuration items may be set with a single command.

```
ks5agent cfg amqp.url=0.0.0.0:5671/nshieldvhost update_interval=5m
```

If no configuration update is provided, the contents of the KeySafe 5 agent config file are displayed.

To update a configuration item, use the format `key=value` using a `.` character for nested configuration items. Examples:

```
ks5agent cfg update_interval=5m
ks5agent cfg logging.level=debug
ks5agent cfg amqp.url=0.0.0.0:5672
```

If the agent is currently running, it will be restarted to pick up the change in configuration.

By default, you can only set values for keys that already exist in the configuration file. To force setting a key that does not currently exist in the configuration file, specify `--force`.

```
ks5agent cfg newkey=value --force
```

Running the `ks5agent resetcfg` command will reset the agent configuration to the default configuration for this agent on the nShield Connect.

4.6.1.2. AMQP authentication for ks5agent

The AMQP authentication method is configured using the `ks5agent cfg` command and setting the `amqp.auth_type` configuration item.

```
ks5agent cfg amqp.auth_type=tls
ks5agent cfg amqp.auth_type=pwd
ks5agent cfg amqp.auth_type=none
```

The username for password or TLS based authentication can be displayed using the `ks5agent amqpuser` command.

```
(cli)ks5agent amqpuser
ks5agent_nshield_module_AAAA-AAAA-AAAA
```

4.6.1.2.1. Password authentication

To configure password based authentication, use the `ks5agent amqppwd` command. This command will display the username that will be used for AMQP authentication, and then prompt for the password to be input.

```
(cli)ks5agent amqppwd
Configuring password to use for KeySafe 5 agent AQMP user 'ks5agent_nshield_module_AAAA-AAAA-AAAA'
This should match the passphrase configured for the user on the RabbitMQ server
New passphrase:
Confirm passphrase:
passphrase set
```

4.6.1.2.2. TLS

TLS certificate authentication is configured with the following workflow:

1. Generate a CSR for this agent using the `ks5agent amqpcsr` Serial Console command on the nShield Connect.
2. If using a RabbitMQ instance installed by the `deploy.sh` script, then the agent certificate can be generated using the `agentcert.sh` script that is shipped alongside the deployment scripts. See AMQP authentication for ks5agent.
3. Store the TLS certificate for this agent and the CA certificate using the `ks5agent amqptls` Serial Console command on the nShield Connect. These certificates must be entered in base64 encoded format. To create suitable input on a Unix system you can run `base64 --wrap=0 tls.crt`.

```
(cli)ks5agent amqpcsr
<output will contain the CSR>

# Obtain a TLS certificate for the above CSR

(cli)ks5agent amqptls ca.crt <base64encoded_data>
Saved ca.crt

(cli)ks5agent amqptls tls.crt <base64encoded_data>
Saved tls.crt
```

4.6.1.3. Status

To show the current status of the KeySafe 5 agent on the nShield Connect, run the `ks5agent` Serial Console command with no arguments.

```
(cli)ks5agent
KeySafe 5 agent is disabled
```

The agent can be enabled and disabled using the `ks5agent enable` and `ks5agent disable` commands. This setting will persist over reboots.

To identify the version of agent installed on the Connect, use the `ks5agent version` command.

```
(cli)ks5agent version
1.2.0-2752f5de
```

4.6.2. Logging

The agent logs of the KeySafe 5 agent running on the nShield Connect may be obtained by using the `ks5agent logs` Serial Console command.

By default, this will print the entire contents of the agent log file to the console. To display just the last 10 lines of the log file, use `ks5agent logs tail`. To display the last `n` lines of the log file, use `ks5agent logs tail <n>` where `<n>` is the number of lines to display.

```
(cli)ks5agent logs
(cli)ks5agent logs tail
(cli)ks5agent logs tail 20
```

If the nShield Connect is configured to append logs to the RFS, or configured to send logs to a Remote Syslog server, then the KeySafe 5 agent logs will be sent with these logs. For more information about configuring logging on the Connect, see the *nShield Connect User Guide*.

4.7. Obtaining the KeySafe 5 Agent Certificates

The KeySafe 5 Agent requires a set of TLS certificates, and a private key for the secure connection with the KeySafe 5 central platform. These certificates can be obtained by following the steps below.

4.7.1. Before You Begin

- Generation of an appropriate Certificate Signing Request (CSR) is required prior to following these steps, for more information on generating a CSR please see KeySafe 5 Agent CSR Generation.

4.7.2. Procedure

1. Log into the KeySafe 5 Appliance Management UI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **Application Settings** section, click **KeySafe5 Settings**.
4. Click **nShield KeySafe 5 Agent Certificates**.
5. In the **Upload CSR File** section, click **Load File** and select the CSR file you wish to use for certificate generation.
6. Click **Generate and Download Certificate** to download the certificate bundle from the cluster node.

   The certificate bundle is a .zip file you must unpack. It contains both the CA certificate and KeySafe 5 Agent's TLS certificate in .pem format.

7. The downloaded certificates can now be copied to the machine where the KeySafe 5 Agent is installed. For information about the location, see Install on Linux or Install on Windows.

4.8. Uninstall

Before uninstalling the nShield KeySafe 5 agent, Entrust recommends that you back up any configuration files and certificates from the install.

4.8.1. Linux

To remove the KeySafe 5 agent from a Linux host run the KeySafe 5 uninstaller:

```
/opt/nfast/keysafe5/sbin/install -u
```

Then proceed to remove the following files and directories:

- `/opt/nfast/keysafe5`
- `/opt/nfast/sbin/keysafe5-agent`
- `/opt/nfast/lib/versions/keysafe5-agent-atv.txt`
- `/opt/nfast/scripts/install.d/12keysafe5-agent`
- `/opt/nfast/log/keysafe5-agent.log`

> The agent log file will be located in a different location if you have changed the default value of `logging.file.path` in the agent configuration file.

If required, you can also remove the `keysafe5d` user that was created as part of the installation.

4.8.2. Windows

To remove the KeySafe 5 agent from a Windows host:

1. Stop the KeySafe 5 agent service using **Windows Service Manager**.
2. Open the **Control Panel** and select **Programs and Features**.
3. Select the **nShield KeySafe 5 Agent** package.

4. Select **Uninstall** and follow the on-screen instructions.

To remove any configuration files, delete the `%NFAST_DATA_HOME%\keysafe5` directory and remove the log file located at `C:\ProgramData\nCipher\Log Files\KeySafe5-agent.log`

> The agent log file will be located in a different location if you have changed the default value of `logging.file.path` in the agent configuration file.

5. KeySafe 5 Administration

This section is applicable to the KeySafe 5 Appliance Management component of the system.

Use a web browser to navigate to and then to log into the KeySafe 5 Appliance Management UI at `https://<node-ip-address>/appliance` using an account with Security Admin privileges

5.1. KeySafe 5 Settings

To view the current KeySafe 5 settings which indicates the MongoDB database mode and a means of downloading the KeySafe 5 Agent install media:

1. In the top menu bar, click **Settings**.
2. In the **Application Settings** section, click **KeySafe5 Settings**.

5.1.1. MongoDB Database

KeySafe 5 stores its data in MongoDB databases, these can be either be *internal* to the clus ter, or KeySafe 5 can be configured to point to an *external* MongoDB server.

5.1.1.1. Internal Database

> ! The default MongoDB installation requires use of the AVX instruction set on processors. For more information, see MongoDB Production Notes

If KeySafe 5 is configured to use an *internal* MongoDB server, then this will be indicated by the KeySafe 5 setting stating the following:

MongoDB Database Mode: Internal

The internal MongoDB database can be used with other Entrust products, such as the nShield Web Services product. This requires a set of TLS certificates, and a private key for the secure connection with the Internal MongoDB server. These certificates can be obtained by following the steps below.

5.1.1.2. Before You Begin

- Generation of an appropriate Certificate Signing Request (CSR) is required prior to following these steps, for more information on generating a CSR please see MongoDB CSR Generation.

5.1.1.3. Procedure

1. Log into the KeySafe 5 Appliance Management UI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **Application Settings** section, click **KeySafe5 Settings**.
4. Click **MongoDB Client Certificates**.
5. In the **Upload CSR File** section, click **Load File** and select the CSR file you wish to use for certificate generation.
6. Click **Generate and Download Certificate** to download the certificate bundle from the cluster node.

   The certificate bundle is a .zip file you must unpack. It contains both the CA certificate and a TLS certificate in .pem format.

7. The downloaded certificates can now be copied to the machine where the other Entrust product is installed. For information about the location, see the guide relevant to your system: *Installation and Upgrade Guide* or the *OVA Installation Guide*.

5.1.1.4. External Database

If KeySafe 5 is configured to use an *external* MongoDB server, then this will be indicated by the KeySafe 5 setting stating the following:

MongoDB Database Mode: External

To configure KeySafe 5 to use an external MongoDB Server please follow the steps below

5.1.1.5. Before You Begin

Ensure you have the following information:

- MongoDB server hostname or IP address
- MongoDB replica set name
- CA Certificate (in pem format)
- Client Certificate (in pem format)

- Client private key
- Client private key passphrase (if required)

Optionally you may require:

- Username
- Password
- Authentication database name

5.1.1.6. Procedure

> ❗ Entrust recommends that this procedure is performed on the master node.

1. Log into the KeySafe 5 Appliance Management UI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **Application Settings** section, click **KeySafe5 Settings**.
4. Click **Configuration Options > MongoDB**.
5. Select **External MongoDB Database** as the **MongoDB Database Mode**.
6. Populate the form using the information gathered above.
7. Click **Test Configuration** to verify the connection to the external MongoDB server.
   - If this fails, please verify the information entered is correct and that the KeySafe 5 cluster has network access to the external MongoDB server.
8. Click **Apply**
9. KeySafe 5 will now restart its internal services and distribute the configuration change to all other nodes, this will take a few minutes to complete.

6. Appliance Management Administration

This section is applicable to the KeySafe 5 Appliance Management component of the system. Use a web browser to navigate to `https://<node-ip-address>/appliance`, where *<node-ip-address>* is the management IP address to access.

6.1. System Configuration

6.1.1. Network Interface Configuration Options

When you install KeySafe 5, you have to specify a valid network connection to make sure the KeySafe 5 node can communicate with other KeySafe 5 nodes. If your network changes or if you want to use multiple NICs (Network Interface Cards), you can update your settings using **Manage Network Settings** from the Entrust KeySafe 5 System Console on the node whose network settings you want to change.

The **Manage Network Settings** menu includes the following options:

Option	Description
Show Current Network Configuration	Lets you view the current network configuration for the node. If the node has multiple NICs, this option allows you to select which NIC configuration you want to view.
Manage IP Address Settings	Lets you change the current network configuration. If the node has multiple NICs, this option allows you to select which NIC configuration you want to change. For details, see Multi-NIC Node Configuration.
Disable a Network Interface	If the node is configured with multiple NICs, this option lets you remove one or more NICs from the con figuration. For details, see Removing a NIC from the Configuration. Note: You cannot remove the management interface.
Manage DNS Settings	Lets you view and update your current DNS Settings. For details, see Configuring DNS Settings.
Manage NTP Settings	Lets you view and update your current NTP Settings. For details, see Configuring NTP Settings.

Option	Description
Manage Static Routes	Lets you add static routes for the KeySafe 5 node for environments where dynamic routing is not the optimal solution. For details, see Configuring Static Routes.
Network Diagnostic Tools	Lets you troubleshoot network issues. For details, see Troubleshooting Network Issues.

6.1.1.1. Multi-NIC Node Configuration

If you want to segregate the communication traffic across multiple channels, you can configure a KeySafe 5 node to use multiple virtual NICs (Network Interface Cards). For example, you may want one NIC to handle the communication between the KeySafe 5 Appliance Management UI and the KeySafe 5 nodes on TCP/443 while a second NIC handles the cluster traffic and the internal node management traffic on TCP/8443.

With multiple NICs, one NIC must be designated as the "management interface", and this interface must be able to communicate on port TCP/8443. KeySafe 5 uses the internal node management interface to:

- Determine the administrative MAC address for the node.
- Initializes the communication traffic between the nodes in the cluster.
- Handle any authentication requests that come into the cluster.

All management interface communication must take place on the management interface. You cannot split management communication across multiple interfaces.

6.1.1.1.1. Considerations

When you are configuring multiple NICs on a node, keep the following things in mind:

- KeySafe 5 supports a maximum of four virtual NICs. One NIC must be the management interface, as described above. In addition to the management interface, you can specify up to three additional NICs that can be used for inbound and outbound traffic. This includes inbound client and KeySafe 5 Appliance Management UI traffic as well as outbound syslog, NFS, and email traffic.
- All NICs must be of the same interface adapter type. For example, if the first NIC speci fied uses the adapter type VMXNET, all other NICs must be of type VMXNET.
- All NICs use global values for their DNS settings, NTP settings, default gateway, and DNS server list. Any change made to those settings on one NIC affects all NICs.

- When you deploy a new KeySafe 5 node through an OVA template, you must specify basic network information such as an IP address, domain, gateway, and DNS server list. When you do so, KeySafe 5 automatically designates that IP address as the management interface on port TCP/8443. We strongly recommend that you do not change this interface if the node is already part of a cluster.
- Adding additional NICs to the VM after deployment requires you to shut down the KeySafe 5 node while you add the NICs. You cannot add NICs to a running system.
- If the node is part of a cluster, the cluster will become degraded if the node is unreachable for too long.
- KeySafe 5 automatically restarts the network services on the node every time you change the configuration for a NIC. The node will be unavailable for a brief period until this process has finished.

6.1.1.1.2. Configuring Multiple NICs on an Existing KeySafe 5 Node

When you deploy a new KeySafe 5 node, you configure the management interface during that process. We strongly recommend that you do not change this interface after you have deployed the node if the node is part of a cluster.

The following procedure describes how to add and configure additional NICs on an already-deployed node. For details about deploying a new KeySafe 5 node, see OVA Installation Guide.

> ⚠ During the following procedure, the node will be unavailable at certain points. If the node is part of a cluster, the cluster will become degraded if the node is unreachable for too long.
>
> In addition, if the node is part of a cluster and you want to change the management interface, you must remove the node from the cluster first.

1. If the additional NICs you want to use have not yet been configured on the VM in which the KeySafe 5 node is running, do the following:
   a. If the KeySafe 5 node is powered on, shut it down using your hypervisor or the node's Entrust KeySafe 5 System Console. For details, see Using the Entrust KeySafe 5 System Console.
   b. In your hypervisor, add the new NICs to the KeySafe 5 VM and configure them using your corporate standards.

   > ℹ Make sure that the new NICs use the same adapter type as the existing NICs. For example, if the management interface NIC is

> of type VMXNET, the new NICs must be of type VMXNET as well.

c. Make a note of the MAC address you are using for each NIC. When the NICs are displayed in KeySafe 5, they are identified by their MAC address. Therefore, when you go to configure the NIC in KeySafe 5 later in this procedure, you will need to know its MAC address.

d. Power on the KeySafe 5 VM.

2. Log in as `htadmin` on the KeySafe 5 node whose NICs you want to configure.

   KeySafe 5 displays the Entrust KeySafe 5 System Console TUI (Text-based User Interface).

3. Select **Manage Network Settings**.
4. Select **Manage IP Address Settings**.
5. On the **Interfaces** screen, select the NIC you want to configure and press **Enter**.

   The NIC that is the current management interface has 'Current management interface' listed after the name. We strongly recommend that you do not change this interface after deployment if this node is part of a KeySafe 5 cluster. If you select the management interface, acknowledge the configuration request at the prompt.

6. On the **Secondary Network Configuration** screen, specify the static IP address and netmask for the KeySafe 5 node.

> ℹ
>
> - Changing the hostname on one NIC changes it for all NICs, including the management interface NIC. If this node is part of a cluster, you should not change the hostname for the node.
> - All NICs must use the same default gateway and DNS server list.
> - Make sure you specify a static IP address and netmask for the KeySafe 5 node.

7. When you have finished specifying the network information, select **OK** and press **Enter**.

   KeySafe 5 restarts the network services using the new configuration. Contact with the node via the KeySafe 5 Appliance Management UI will be unavailable until the restart is finished.

   When the network finishes restarting, KeySafe 5 displays the Entrust KeySafe 5 System Console.

8. Repeat the proceeding steps for any other NICs you want to configure. KeySafe 5 will restart the network services and the node will be unreachable for a short time after each configuration change.
9. If you want to verify the configuration information, select **Manage Network Settings**. From there, select **Show Current Network Configuration** to view a list of the configured NICs with their IP addresses and netmasks. The management interface IP address is shown as the main interface. Any additional interfaces that are configured are shown below.

6.1.1.1.3. Removing a NIC from the Configuration

If you want to remove a NIC that you have previously configured, you should use the Entrust KeySafe 5 System Console to disable that NIC in KeySafe 5 before you remove it from the VM.

In addition, if this node is part of a cluster we recommend that you remove it from the cluster before you remove the NIC. You can then re-join it with the cluster after the network configuration is complete.

> ⚠ This option is not reversible and it requires the node to reboot.

1. Log in as `htadmin` on the VM whose NIC you want to remove.

   KeySafe 5 displays the Entrust KeySafe 5 System Console TUI (Text-based User Interface).

2. Select **Manage Network Settings**.
3. Select **Disable Network Configuration**.
4. Select the interface you want to disable.

   > ℹ You cannot disable the management interface, so KeySafe 5 does not show that interface in the list.

5. Confirm at the prompt.
6. Press **Enter** to reboot the node.
7. If desired, select **Shutdown System** and then use your hypervisor to remove the NIC from the VM.

6.1.1.2. Configuring DNS Settings

1. Use your hypervisor to access one of the VMs in which KeySafe 5 is running, then log into the KeySafe 5 VM console as `htadmin`.

KeySafe 5 displays the Entrust KeySafe 5 System Console TUI (Text-based User Interface).

2. From the Entrust KeySafe 5 System Console, select **Manage Network Settings > Manage DNS Settings**.
3. On the **Modify DNS Settings** page, you can view your existing DNS settings. Select one of the following:
   - **No** — Exits the screen and returns to the **Manage Network Settings** page.
   - **Yes** — Opens the **Network Configuration** screen. Enter a comma-separated list of DNS addresses. Select **Ok** to save and then **Yes** on the confirmation screen. If you decide not to make changes, select **Cancel** to return to the **Manage Network Settings** page.

6.1.1.3. Configuring NTP Settings

1. Use your hypervisor to access one of the VMs in which KeySafe 5 is running, then log into the KeySafe 5 VM console as `htadmin`.

   KeySafe 5 displays the Entrust KeySafe 5 System Console TUI (Text-based User Interface).

2. From the Entrust KeySafe 5 System Console, select **Manage Network Settings > Manage NTP Settings**.
3. On the **Modify NTP Network Settings** page, you can view your existing NTP settings. Select one of the following:
   - **No** — Exits the screen and returns to the **Manage Network Settings** page.
   - **Yes** — Opens the **Network Configuration** screen. Enter a comma-separated list of NTP addresses. Select **Ok** to save and then **Yes** on the confirmation screen. If you decide not to make changes, select **Cancel** to return to the **Manage Network Settings** page.

6.1.1.4. Configuring Static Routes

In some network environments, it may be necessary to add static routes to KeySafe 5 rather than relying on dynamic routing.

1. Use your hypervisor to access one of the VMs in which KeySafe 5 is running, then log into the KeySafe 5 VM console as `htadmin`.

   KeySafe 5 displays the Entrust KeySafe 5 System Console TUI (Text-based User Interface).

2. From the Entrust KeySafe 5 System Console, select **Manage Network Settings > Manage Static Routes**.
3. From the **Static Routes** page, you can:
   - View a list of the defined routes by selecting **List Current Static Routes**.
   - Add a new route by selecting **Add Static Route** and entering the route network address and gateway in the Add Static Route page. KeySafe 5 displays a message that the route has been successfully added.
   - Delete a previously-defined static route by selecting **Delete Static Route** and specifying the network address and gateway of the route you want to delete. KeySafe 5 displays a message that the route has been deleted.

6.1.2. Configuring SSL Settings

Because each node hosts a standalone webserver, if you want to configure the SSL settings for a node you must log into the KeySafe 5 Appliance Management UI for that specific node.

1. Log into the KeySafe 5 Appliance Management UI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **SSL Configuration**.
4. On the **Protocol** tab, select the TLS authentication modes that you want to use (TLSv1.3 is not supported in the KeySafe 5 OVA):
   - TLSv1.0, TLSv1.1, TLSv1.2
   - TLSv1.0, TLSv1.2
   - TLSv1.2 only
5. Optionally, on the **Cipher Suite** tab, review the detailed list of available ciphers. If you want to remove ciphers from this list, click the X following the cipher name that you do not want to use. If you want to add a cipher, click in the bottom of the list box and enter a valid cipher name, then click **Reload**.
6. When you are finished, click **Apply**.

6.1.3. Setting Email Server Preferences

1. Log into the KeySafe 5 Appliance Management UI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.

3. In the **General Settings** section, click **Mail Server**.
4. On the **Mail** tab, specify the options you want to use.

Option	Description
Disable E-mail Notifications check box	If checked, no alert emails are sent to the user accounts in the system. If the Admin Key is regenerated, all security admins must manually download their key parts from the **Settings** tab. If this option is not selected, KeySafe 5 only sends alerts and new Admin Key parts through email. Security Admins can still download their Admin Key parts from the KeySafe 5 Appliance Management UI. For details about the Admin Key, see Admin Keys.
Server	The IP address or fully qualified domain name (FQDN) of the SMTP server. If your domain has an MX record configured, you can use KeySafe 5 to relay mail by setting the IP address to 127.0.0.1. This is the default behavior.
Port	The mail server port.
Login	If required, the user account with which KeySafe 5 should log into the email server.
Password	The password for the login account.
Sender	The sender that KeySafe 5 should use when send-ing email.
SMTPS	If this option is set to **On**, KeySafe 5 uses SMTP Secure (SMTPS). Important information such as alerts and admin keys are shared by email. Entrust highly recommend you set this option to use encryption with SMTP.

5. To test the email settings, click **Send Test Email**.

6.1.4. Setting KeySafe 5 Console Settings

If you do not remember the credentials of any user with the Security Administrator (`sec-root`) privilege, or if you are locked out of the KeySafe 5 Appliance Management UI, KeySafe 5 provides a self-service option using the KeySafe 5 System Console to reset the (`secroot`) user credentials with a temporary password. You can disable this option if you do not want this feature.

1. Log into the KeySafe 5 Appliance Management UI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **System Settings** section, click **KeySafe 5 Console Settings**.
4. On the **KeySafe 5 Console Settings** page, select one of the following:
   - Select **YES** to allow the `htadmin` user to reset the `secroot` password.
   - Select **NO** if you do not want to allow the `htadmin` user to reset the `secroot` password.
5. Click **Apply**.

6.1.5. KeySafe 5 Certificates

KeySafe 5 requires that an SSL certificate be installed on each KeySafe 5 node in a cluster. Each KeySafe 5 instance is installed with two web servers:

- An internal web server that manages the KeySafe 5 node to node cluster communication on port 8443.
- An external web server that manages the KeySafe 5 Web UI, the REST API interface, and the Policy agent communication on port 443.

By default, KeySafe 5 includes a component for creating a Root Certificate Authority (CA) that can generate digital certificates. When the first KeySafe 5 node is installed, it creates a Private and Public CA that it also stores in the KeySafe 5 object store.

The first KeySafe 5 node then uses the Private CA to create an SSL certificate that contains the hostname (FQDN) as well as the IP address of the KeySafe 5 node for the internal web server and Public CA to create an SSL certificate that contains the hostname, both short and FQDN, as well as the IP address of the KeySafe 5 node for the external web server. When the node reboots, KeySafe 5 checks the IP address and recreates the SSL certificate if the IP address has changed.

KeySafe 5 node to node communication is on a TLS channel and it uses SSL certificates issued by Private CA to secure communication. When additional KeySafe 5 nodes are added to the cluster, the first KeySafe 5 node shares the Private and Public CA through the KeySafe 5 object store over an HTTPS connection.

In this scenario, the Public CA installed on all the KeySafe 5 nodes is the same, ensuring that every KeySafe 5 node is able to verify SSL certificates generated by every other KeySafe 5 node in the cluster. However, this default OVA Internal CA signed SSL certificate is considered self-signed, which can lead to trust issues.

6.1.5.1. Viewing the Expiration Date for the Current KeySafe 5 SSL Certificate

It is critical to keep the KeySafe 5 certificate current.

Use the following procedure to view the expiration date for the current KeySafe 5 certificate on the selected KeySafe 5 node.

1. Log into the KeySafe 5 Appliance Management UI using an account with Domain Admin privileges.
2. In the top menu bar, click **Cluster**.
3. Click the **Servers** tab and select a KeySafe 5 node.
4. To view the SSL certificate configured for the internal web server, click the link next to **Internal Web server** in the Certificate detail.

   The link name is **Default** if the internal web server is using the default OVA Internal CA signed certificate and **Custom** if it is using a custom SSL certificate.

5. To view the SSL certificate configured for the external web server, click the link next to **External Web server** in the Certificate detail.

   The link name is **Default** if the external web server is using the default OVA Internal CA signed certificate and **Custom** if it is using a custom SSL certificate.

6. When you are done, click **Close**.
7. If you want to check the expiration date for the certificate on another KeySafe 5 node, select that node and repeat this procedure.

6.1.5.2. Creating a Certificate Signing Request

A certificate signing request (CSR) tells an external Certificate Authority (CA) that you want an SSL certificate generated and signed by that CA. The SSL certificate can then be uploaded to KeySafe 5 and used in place of the default self-signed certificate.

When you use KeySafe 5 to create the CSR, KeySafe 5 creates a key pair and uses that key pair in conjunction with the information you specify to create the CSR. KeySafe 5 then encrypts the key pair and stores it for later use.

You can use the resulting CSR to generate an SSL certificate from the external CA you want to use. After you receive the SSL certificate from that external CA, you can upload it to KeySafe 5. Because the key pair already exists on the system, you do not need to upload anything else.

If you create the CSR to generate an SSL certificate to be installed for internal web server, you must include the IP address of the KeySafe 5 node in **Subject Alternative Name**.

If you create the CSR outside of KeySafe 5, you need to upload both the SSL certificate and the matching private key file when you install the certificate on KeySafe 5.

1. Log into the KeySafe 5 Appliance Management UI using an account with Domain Admin privileges.
2. In the top menu bar, click **Cluster**.
3. Click the **Servers** tab and select a KeySafe 5 node.
4. Select **Actions > Create CSR**.
5. In the Generate Certificate Signing Request dialog box, specify the options you want to use.

Field	Description
Common Name	The name to associate with this request. By default, KeySafe 5 enters the selected server name in this field. You can edit the default name as needed.
Locality	The locale to associate with this request.
State	The state to associate with this request.
Subject Alternative Names	The host names that will be protected by this certificate. If you want to use the same certificate on multiple KeySafe 5 nodes in the system for the external web server, add all of the KeySafe 5 URLs to this list. By default, KeySafe 5 adds the URL of the selected KeySafe 5 node. You can change or delete the default URL as long as you end up specifying at least one KeySafe 5 node in this field.
Key Size	Select the key size that you want to use. The default is 4096 bytes.
Country	The country to associate with this request. The default is US.
Organization	The organization to associate with this request.
Organization Unit	The organizational unit associate with this request.

6. Click **Generate**.

7. When you receive the message that KeySafe 5 has created the CSR, click **Download** to save a copy of the CSR to your browser’s default download directory or click **Preview** to view the CSR in a pop-up window. You can copy the CSR from the Preview window to the clipboard if desired.
8. Use the CSR to request an SSL certificate from the external Certificate Authority you want to use. How you do this depends on the CA you are using.

After you receive the SSL certificate from the external CA, install it on KeySafe 5 as described in Installing a New External Certificate.

6.1.5.3. Installing a New External Certificate

Use this procedure to replace the current KeySafe 5 SSL certificate with a new externally-signed SSL certificate. If you want to use a new, OVA Internal CA signed ("self-signed") SSL certificate generated by the Public CA or Private CA included with KeySafe 5, see Installing a New OVA Internal CA signed Certificate.

6.1.5.3.1. Before You Begin

- If you generated the Certificate Signing Request (CSR) through KeySafe 5, you need to make sure you have the resulting SSL certificate and the CA certificate in Base64-encoded pem format files accessible to the KeySafe 5 node that you are logged into. If you generated the CSR through some other means, make sure you have both of the Base64-encoded pem format certificates and the Base64-encoded pem format private key file that goes with the certificates. KeySafe 5 supports only RSA private keys. For more information, see Creating a Certificate Signing Request.
- If you generated the SSL certificate from OpenSSL or other third-party tool, make sure the certificate is formatted as a web server certificate.
- The SSL certificate generated for the internal web server should be able to function as the Client and Server certificate.
- SSL certificates that contain an intermediate CA certificate chain are not supported for the internal web server. If there is a certificate chain, it must be specified in the CA cer tificate for the internal web server.

6.1.5.3.2. Procedure

1. Log into the KeySafe 5 Appliance Management UI using an account with Domain Admin privileges.
2. In the top menu bar, click **Cluster**.

3. Click the **Servers** tab and select a KeySafe 5 node.

   You can use SSL certificates signed by different certificate authorities on individual KeySafe 5 nodes. However, Entrust recommends that all of the SSL certificates be signed by the same Certificate Authority so that only one CA certificate is required to be trusted.

4. Select **Actions > Install Certificate**.
5. In the **Certificate** tab of the Certificate Installation dialog box, specify the options you want to use.

Field	Description
SSL Certificate	The SSL certificate file in Base64-encoded pem for mat. This certificate must be valid for the installation to succeed.
CA Certificate	The certificate of the CA that issued the SSL certifi cate in Base64-encoded pem format.
Web Server	Choose which web server to install the custom certificate. You can select both if you wish to install the same SSL certificate for the internal and the external web server. If the SSL certificate is used for both web servers, it should be able to function as a Client and Server certificate and it should have the KeySafe 5 IP address specified in SAN.

> ❗ Before KeySafe 5 installs the certificate, it checks with the certificate authority to make sure that the SSL certificate can be validated. If the CA certificate file you are uploading for the external web server contains just the certificate of the root certificate authority, make sure that the SSL certificate file contains the entire chain of intermediate CA certificates as well as the SSL certificate for the selected KeySafe 5 node.

6. If you did not create the certificate signing request with KeySafe 5:
   a. Click the **Private Key** tab and click **Load File**, then navigate to the private key file you want to use. KeySafe 5 never stores the private key in clear text.
   b. If the private key file is encrypted, enter the user-specified password for the key file in the **Password** field. This password is not stored in the KeySafe 5 object store or on the local file system.
7. Click **Install Certificate**.
8. If you install the SSL certificate for the internal web server, the web server automati-

cally restarts.

If you install the SSL certificate for the external web server, when the installation is complete, click **Restart Web Service** or select **Actions > Restart Web Service** and confirm the request at the prompt.

After the web service restarts, KeySafe 5 will use the new certificate.

KeySafe 5 restarts the web server which may interrupt the browser connection to the KeySafe 5 Appliance Management UI. When the restart is finished you are returned to the KeySafe 5 Appliance Management UI login page.

> If you are using Chrome, the connection status in your browser may still show as insecure. To fix this, open the KeySafe 5 Appliance Management UI login page in a new tab.

9. If you want to verify that the new certificate was properly installed, select the node and click the link next to **Internal/External web server**.

   If you already have custom certificate installed for external web server and the KeySafe 5 internal web server uses a default self signed SSL certificate, KeySafe 5 automatically detects and provides an option to use the same custom SSL certificate for internal web server if it meets the certificate requirements of internal web server. Select **Use external Web server SSL certificate for internal Web server** and click **Save** to install the same custom SSL certificate for the internal web server.

   If you already have custom certificate installed for internal web server and the KeySafe 5 external web server uses a default self signed SSL certificate, KeySafe 5 automatically detects it and provides an option to use the same custom SSL certificate for the external web server if it meets the certificate requirements of an external web server. Select **Use internal Web server SSL certificate for external Web server** and click **Save** to install the same custom SSL certificate for internal web server. When the installation is complete, click **Restart Web Service** or select **Actions > Restart Web Service**, then confirm the request at the prompt. After the web service restarts, KeySafe 5 will use the custom SSL certificate for external web server.

6.1.5.4. Installing a New OVA Internal CA signed Certificate

Use this procedure to replace the current KeySafe 5 certificate configured on internal or external web server with a new certificate signed by the certificate authority that is included with KeySafe 5.

> If you want to install an externally-signed SSL certificate from a

> Base64-encoded pem format file, see Installing a New External Certificate.

1. Log into the KeySafe 5 Appliance Management UI using an account with Domain Admin privileges.
2. In the top menu bar, click **Cluster**.
3. Click the **Servers** tab and select a KeySafe 5 node.

> ℹ You can use a different certificate on each KeySafe 5 node. In this case, however, Entrust recommends that all of the certificates be signed by the same Certificate Authority.

4. Select **Actions > Use Self-Signed Certificate**.
5. Select the web server on which the certificate is to be installed.
6. Click **Proceed** at the prompt.

   If you select the external web server, KeySafe 5 restarts the web server. This may interrupt the browser connection to the KeySafe 5 Appliance Management UI. When the restart is finished, you are returned to the KeySafe 5 Appliance Management UI login page.

7. If you want to verify that the new certificate was properly installed, select the node and click the link next to **Internal/External web server**.

6.1.6. Admin Keys

All KeySafe 5 data (policy information, user account information, and so on) are held in an encrypted object store that is shared across all KeySafe 5 nodes in the cluster.

The object store is ultimately protected (through multiple layers of key wrappings) by an Admin Key that KeySafe 5 generates and maintains. This key is required if you ever need to restore KeySafe 5 from a backup or you need to change the hardware configuration of a KeySafe 5 node.

When you install the first KeySafe 5 node in your system, KeySafe 5 generates an Admin Key as soon as you log into the KeySafe 5 Appliance Management UI for the first time. The initial key has a single part and is assigned to the default `secroot` user account. As you add additional Security Administrator accounts to the system, KeySafe 5 shifts to an "**n** of **m**" Admin Key backup model, where "**m**" is the number of user accounts with Security Admin privileges and "**n**" is a user-defined value that states how many key parts must be uploaded before KeySafe 5 considers the Admin Key to be valid.

For example, if you have five Security Admins and you set **n** to **3**, then at least three of the Security Admins will need to upload their Admin Key parts in order to restore KeySafe 5 from a backup. If you set **n** to **1**, then any one of the five Security Admins can restore KeySafe 5 without consulting with any of the other Security Admins.

While you can regenerate Admin Key parts at any time, in order to restore KeySafe 5 from a backup image you must have the required number of Admin Key parts that were valid when the backup was created. You cannot regenerate the Admin Key parts and then immediately use those new key parts to restore KeySafe 5 from a previously-created back up.

The Admin Key is assigned a generation count that is incremented each time a new Admin Key is generated. This generation count allows you to identify which Admin Key parts go together. The email that each Security Admin receives when a new Admin Key is generated contains the generation count. For example:

This current Key Part supersedes any you may have previously received from this cluster. The Key Part is associated by a "generation count" with its relevant backups. The generation count for this key is: 8

The generation count is also included in the Admin Key Part filename, which is attached to the email. The attachment name is *username_kc-ip-addr.key.gen#*, where *username* is the Security Admin’s KeySafe 5 account name, *kc-ip-addr* is the KeySafe 5 IP address from which the Admin Key was generated, and # is the generation count. For example, `sec-root_10.238.66.235.key.gen8`. This same naming convention is used if a Security Admin downloads their Admin Key Part from the KeySafe 5 Appliance Management UI.

If you want to restore KeySafe 5 from a backup created when the Admin Key shown above was valid, you must make sure that all the Admin Key Parts you upload have generation count = 8.

6.1.6.1. Generating the Admin Key

When KeySafe 5 generates an Admin Key, it cryptographically divides the key into parts and sends one part to each KeySafe 5 user account with Security Admin privileges.

KeySafe 5 automatically generates new Admin Key:

- During installation of the first KeySafe 5 node. In this case, the `secroot` user account gets an Admin Key with a single part.
- When a Security Admin user account is added or deleted. In this case, a new Admin Key is divided into a new number of parts, "m", and sent to all current Security Admins.

ℹ The value of "n" is not changed. If you add three Security Admins

> immediately after the initial installation, the Admin Key will be divided into four parts, but only one part will be required when restoring the system. The way you set the required number of parts is described below.

- When you explicitly generate a new Admin Key, as described below. In this case, the number of Admin Key parts is not changed.

> ℹ Whenever the admin key is regenerated, KeySafe 5 forces you to download the admin key.

6.1.6.1.1. Procedure

1. Log into the KeySafe 5 Appliance Management UI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Admin Key Parts**.
4. Verify the following options:

Option	Description
Minimum Key Parts	The minimum number of parts needed when you want to restore KeySafe 5 from a back up ("n").
Email Private Key on Gen erate	If **Enabled**, when you generate a new Admin Key, KeySafe 5 automatically sends each Security Admin their key part as an email attachment. The attachment name is *username_kc-ip-addr.key.gen#*, where *username* is the Security Admin's KeySafe 5 account name, *kc-ip-addr* is the KeySafe 5 IP address into which you are currently logged in, and # is the generation count. For example, `secroot_10.238.66.235.key.gen8`. If **Disabled**, when you generate a new Admin Key, KeySafe 5 sends each Security Admin an alert stating that the admin key has been changed and prompting them to download their key part.

5. Click **Generate New Key**. KeySafe 5 increases the generation count by one and creates a new key part for each Security Admin in the system. If you have configured an EKS, KeySafe 5 also saves the Admin key to the EKS.

   Based on the setting of the **Email Private Key on Generate** option, KeySafe 5 also sends each Security Admin in the system an email with their key part or an alert stating that there is a new key part ready for download.

> If you intend to back up KeySafe 5 in the immediate future, we rec-

> ommend that you notify your Security Admins that the new Admin Key part they just received is going to be tied to a backup image and they should download it to a secure location immediately. You cannot restore KeySafe 5 from a backup image unless you have the Admin Key parts that were valid when the back up was created, and you cannot download previous Admin Key parts from KeySafe 5.

6. Click **Close**.

6.1.6.2. Downloading Your Admin Key Part

Every user account with Security Admin privileges receives an encrypted Admin Key part. Certain KeySafe 5 functions, such as restoring the system from a backup, require that a certain number of parts be uploaded to KeySafe 5 within a certain amount of time. Once KeySafe 5 receives the correct number of parts, it can validate the Admin Key and perform the requested procedure. Once you download your key part, make sure you store it securely and that you can find it when needed.

> You also need to keep previous Admin Key parts and know when each part was created. If you need to restore a system from a previous backup, you must have the key parts that were valid when that backup was created. If the Admin keys have been regenerated, you cannot download the current Admin Key parts and use those to restore a previous version of KeySafe 5.

1. Log into the KeySafe 5 Appliance Management UI with your standard account credentials.
2. In the top menu bar, click **Settings**.
3. In the **Account Settings** section, click **Download Key**. KeySafe 5 downloads a file to your browser's default download location called *username_kc-ip-addr.key.gen#*, where username is the currently logged in KeySafe 5 account name, *kc-ip-addr* is the KeySafe 5 IP address into which you are currently logged in, and # is the generation count. For example, `secroot_10.238.66.235.key.gen8`.
4. If you want to remove the Admin Key part from the KeySafe 5 encrypted object store, click **Clear Key**. If you later attempt do download the key part after clearing it, you will get an error stating that the key part does not exist. You will need to regenerate the key as described in Generating the Admin Key.

6.1.7. Using the Entrust KeySafe 5 System Console

When you log into the KeySafe 5 VM console as htadmin, KeySafe 5 displays the Entrust KeySafe 5 System Console. This menu lets you configure the local KeySafe 5 server. In general, the changes you make here do not apply to any other KeySafe 5 node in the cluster.

The menu is a TUI (Text-based User Interface). You navigate through the TUI using the **Tab** key to move between fields and pressing **Enter** when the correct choice is highlighted. If the TUI screen has numbers at the start of the line, you can also press the corresponding number key and then press **Enter** to navigate through the menus.

To return to the main Entrust KeySafe 5 System Console screen, press **Esc** (Escape). Based on where you are in the menus, you may need to press **Esc** several times.

The Entrust KeySafe 5 System Console contains the following options:

Option	Name	Description
1	Manage Network Settings	View or change the current network configuration.
2	Manage htadmin and SSH Access	Manage the htadmin account for this KeySafe 5 node and enable or disable access to the Entrust KeySafe 5 System Console via SSH.
3	Manage Accounts	Enable or disable the full support login account (htsupport), the restricted login account (htrestricted), or the KeySafe 5 webGUI default account (secroot).
4	Manage HSM Client Account	Not applicable for this version of KeySafe 5
5	Download Internal Certificate	Download the Entrust-generated CA certificate being used on this KeySafe 5 node so that you can add that certificate to your web browser as a trusted site.
6	Gather Diagnostic Logs	Creates a support bundle with diagnostic information and log files that Entrust Support can use to diagnose issues with your KeySafe 5 cluster.
7	Manage KeySafe 5 Node	Allows you to delete internal snapshots created automatically during upgrade.

Option	Name	Description
8	Reboot or Shut Down KeySafe 5 Node	Reboots or shuts down the current KeySafe 5 node. If you plan to remove the node from the cluster or decommission it, see Removing a KeySafe 5 Node from a Cluster or Decommissioning a KeySafe 5 Node.
9	Manage Timeouts and Appearance	View or change the current timeout for the Entrust KeySafe 5 System Console. After this period of time elapses with no user input, KeySafe 5 closes the Entrust KeySafe 5 System Console and returns to the system login prompt. This option also lets you toggle the 3D appearance for the Entrust KeySafe 5 System Console.
10	Quit TUI Session	Close the Entrust KeySafe 5 System Console and return to the system login prompt.

6.2. Authentication

KeySafe 5 access can be authenticated in the following ways:

- OpenID Connect, KeySafe 5 supports user authentication through integration with an OpenID Connect provider. If a provider is configured, the KeySafe 5 login dialog contains not only the Sign In button but also a configurable button to start the authentication process using the provider.
- Locally, with a password stored in KeySafe 5. KeySafe 5 Security Admins can configure the password requirements and expiration options, as well as the maximum number of login attempts that are allowed before the KeySafe 5 account is disabled and an expira tion date after which the account will be automatically disabled.

⚠ Entrust does not recommend this option. This option means that the KeySafe 5 UI and its API will be unauthenticated.

6.2.1. Configuring Local Authentication Settings

This procedure describes how to configure the password and account security options for all locally-authenticated KeySafe 5 managed user accounts.

⚠ Entrust does not recommend this option. This option means that the KeySafe 5 UI and its API will be unauthenticated.

1. Log into the KeySafe 5 Appliance Management UI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Authentication**.
4. In the Type drop-down, select **Local (Password)**.
5. On the **Basic** tab, change the options as desired, then click **Apply** when finished.

Field	Description
Password Expiration	The maximum number of days that a password can be used before it expires. KeySafe 5 also uses this value to calculate the default password expiration date when a new local KeySafe 5 user is created. (Default: 60) Once a password expires, the user is prompted to change their account password the next them they log into the KeySafe 5 Appliance Management UI.
Max Failed Logins	The number of failed login attempts allowed before the user account is locked. (Default: 5) If the maximum number of logins is exceeded, the next time the user attempts to log in they receive a message informing them that the account is disabled and telling them to talk to a Security Administrator. The Security Administrator must then re-enable the account as described in Re-enabling a KeySafe 5 managed User Account.
Minimum Previous Passwords	The number of unique new passwords that must be associated with a user account before an old password can be used. (Default: 5)

6. On the **Strength** tab, click the desired value to change the setting, then click **Save** when finished. If you change one of these settings, KeySafe 5 applies the new requirements to any new passwords created for a KeySafe 5 account. It does not apply the requirements to any existing KeySafe 5 account passwords.

Field	Description
Minimum Password Length	The minimum number of characters that must be in a password. (Default: 8)
Minimum Uppercase Characters	The minimum number of characters that must be upper case. (Default: 1)
Minimum Special Characters	The minimum number of characters that must be something other than a-z, A-Z, or 0-9. (Default: 1)
Minimum Lowercase Characters	The minimum number of characters that must be lowercase. (Default: 1)
Minimum Required Digits	The minimum number of characters that must be numeric. (Default: 1)

7. When you are finished, click **Close**

6.2.1.1. Re-enabling a KeySafe 5 managed User Account

A KeySafe 5 managed user account can become disabled for the following reasons:

- The number of consecutive unsuccessful login attempts has exceeded the value set for Max Failed Logins. For more information, see Configuring Local Authentication Settings.
- A KeySafe 5 Security Admin has manually disabled the account.
- The expiration date associated with the account has passed.
- The Account Enabled check box was not selected when the user account was created.

> ! If you cannot log into any KeySafe 5 accounts with Security Admin privi leges, contact Entrust Support.

6.2.1.1.1. Procedure

1. Log into the KeySafe 5 Appliance Management UI using an account with Security Admin privileges.
2. In the top menu bar, click **Security**.
3. Select the account you want to re-enable in the list. The KeySafe 5 Appliance Management UI displays the details for the selected account below the table.
4. In the **Account Status** field, click **Disabled**.
5. Check the **Enabled?** check box and click Save.
6. Verify the expiration date in the **Account Expiration** field.

7. To change the account password, click the **Authentication** tab then click **Change Pass word**.

Your changes take effect immediately.

6.2.2. Configuring an OpenID Connect Provider

KeySafe 5 supports user authentication through an OpenID Connect provider. If a provider is configured, the KeySafe 5 login dialog contains not only the KeySafe 5 Sign In button but also a configurable button to start the authentication process using the provider.

6.2.2.1. Before You Begin

The OpenID Connect provider must be configured to accept the KeySafe 5 URLs. Each login dialog requires both a login and a logout URL, so for KeySafe 5, you have to configure numerous URLs for each node in the cluster. You have to configure the login and logout URL for KeySafe 5 itself.

In the following example of URL list for OpenID Connect provider, *<node-ip-address>* is the hostname or IP address of the KeySafe 5:

Login:

- `https://<node-ip-address>/callback`
- `https://<node-ip-address>/keysafe5`
- `https://<node-ip-address>/v5/oidc/callback`

Logout:

- `https://<node-ip-address>/callback`
- `https://<node-ip-address>/keysafe5`
- `https://<node-ip-address>/v5/kc/oidc/logout`

6.2.2.2. Procedure

1. Log into the KeySafe 5 Appliance Management UI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **Type** drop-down, select **OpenID Connect**.

Specify the options you want to use. When you are done, click **Apply**.

Field	Description
Client ID	The organizational identity assigned by the OpenID Connect provider when you sign up for the service.
Client Secret	A cryptographic component used to secure the organization’s access to the OpenID Connect provider. Client Secret is mandatory for **Authenticated Flow** and optional for **PKCE Flow**. ❗ This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.
Base URL	The URL that KeySafe 5 will use to contact the OpenID Connect provider to present the login page.
Name	A user-defined name for the OpenID Connect provider. KeySafe 5 displays this name on the button on the login dialogs. Only one global OIDC provider can be configured per KeySafe 5 cluster.

6.3. KeySafe 5 Cluster Maintenance

6.3.1. KeySafe 5 Nodes and Clusters

When you install KeySafe 5, the process creates a KeySafe 5 node that can operate singly or be joined with other KeySafe 5 nodes to form an active-active cluster. These nodes can be installed in different geographic locations, but they must be able to communicate with each other.

All KeySafe 5 nodes in a cluster share configuration settings, and data. Changes made on one node are automatically synced to all nodes in the cluster through an encrypted object store. This provides a failover mechanism in case a KeySafe 5 node becomes unreachable.

The KeySafe 5 nodes constantly exchange heartbeats to verify that every node in the cluster is reachable. If all nodes respond to the heartbeats, the cluster is considered "healthy". If one or more nodes stop responding for a given length of time, the cluster is considered "degraded". If a cluster is degraded, the active KeySafe 5 nodes can still serve requests but you cannot make changes to the nodes in the cluster.

The heartbeat interval and status thresholds are user-configurable for the cluster. For details, see Setting Cluster Options.

6.3.2. Viewing the Cluster Status

1. Log into the KeySafe 5 Appliance Management UI using an account with Domain Admin privileges.
2. In the top menu bar, look at the **Cluster** icon. If there is a green heart, the cluster is healthy. If there is a red X, the cluster is degraded. You can also look at the **Status** field on the **Cluster** tab.
3. To view the status of the individual servers in the cluster, click the **Servers** tab. The **Status** column shows the status for each server in the cluster:

Field	Description
Maintenance	Same as cluster status, going through rolling upgrade.
Offline	Unreachable and unavailable
Online	Reachable and available.
Unavailable	Server to server connection works but the KMIP Database is unavailable (port 5432).
Unreachable	Unable to connect to the server (port 8443).

4. A yellow star appears before the server name of the node that has been designated as the database master node. The other nodes in the cluster are replica nodes.

6.3.3. Setting Cluster Options

1. Log into the KeySafe 5 Appliance Management UI using an account with Domain Admin privileges.
2. In the top menu bar, click **Cluster** and specify the options you want to use.

Option	Description
Description	A user-defined description for the cluster.
Status	The status of the cluster. If this is **Healthy**, all KeySafe 5 nodes are functioning normally. If this is **Degraded**, KeySafe 5 can still serve requests but you cannot make changes to the nodes in the cluster.
Group Administrator	The KeySafe 5 administration group to which this cluster belongs. You cannot change this field.

Option	Description
Backup Hosts	The hostnames or IP addresses of systems that are allowed to access the KeySafe 5 backup directory through NFS. (0.0.0.0 means any server can have access) Any time you back up KeySafe 5, it automatically stores the backup file in a folder called /hcs/backup. If you issue an NFS mount command to that directory from another server, you can access any of the backup files. Make sure these backup images are securely stored in case you ever need to restore KeySafe 5.
Backup Over NFS	Whether backup over NFS is enabled. (Default: disabled)
Cluster Operation Timeout	The amount of time that a KeySafe 5 node waits to receive a response from another KeySafe 5 node. If a response is not received by the specified timeout, the KeySafe 5 cluster goes into degraded mode, which indicates a network connectivity problem. Enter a value between 1 and 30 seconds. (Default: 5 seconds) If a KeySafe 5 cluster frequently switches between degraded state and healthy state, you can increase this timeout. We recommend, however, that you keep the timeout as short as possible.
Heartbeat Timeout	The number of seconds to wait for a KeySafe 5 heartbeat response between KeySafe 5 nodes in the cluster. If this time is exceeded, the heartbeat fails. Enter a value between 2 and 15 seconds. (Default: 3 seconds)
Healthy Interval	The number of seconds between successful KeySafe 5 heartbeats for the cluster to be considered healthy. Enter a value between 1 and 10 seconds. (Default: 1 second)

Option	Description
Degraded Interval	The number of seconds between failed KeySafe 5 heartbeats for the cluster to be considered degraded. Enter a value between 1 and 10 seconds. (Default: 1 second)
Healthy Threshold	The number of successful consecutive heartbeats that must occur before KeySafe 5 determines that a degraded cluster is now healthy. Enter an integer between 2 and 10. (Default: 2)
Degraded Threshold	The number of failed consecutive heartbeats that must occur before KeySafe 5 determines that a healthy cluster is now degraded. Enter a value between 2 and 10. (Default: 2)

Any changes you make are communicated to all nodes in the cluster and take effect immediately.

6.3.4. Startup Authentication

You can choose to enable passphrase-based startup authentication to provide further protection for the master key for all nodes in the same cluster. With passphrase-based startup authentication, the KeySafe 5 node will enter Recovery Mode every time it is rebooted. You will need to enter the passphrase in the KeySafe 5 Appliance Management UI. See the Recovery using Passphrase section in Recovering Access to KeySafe 5.

Startup Authentication allows KeySafe 5 to be used in tactical kits in hostile environments. Onsite staff can simply power off the KeySafe 5 nodes, which make them unusable until a passphrase or admin key is provided.

Note: If Startup Authentication is enabled, you cannot add a new KeySafe 5 node. You must disable Startup Authentication first, add the new node, and then re-enable Startup Authentication.

6.3.4.1. Enabling Startup Authentication

1. Log into the KeySafe 5 Appliance Management UI using an account with Domain Admin privileges.

2. In the top menu bar, click **Cluster**.
3. Go to the **Cluster** tab.
4. Select **Actions > Startup Authentication**.
5. In the Startup Authentication window, click **Edit**.
6. In the Passphrase Based Startup Authentication field, select **Enabled**.
7. Enter and confirm your passphrase.

   The passphrase must be at least 12 characters long and include 1 digit, 1 uppercase character, 1 lowercase character, and 1 symbol.

8. Click **Apply**.

6.3.4.2. Disabling Startup Authentication

1. Log into the KeySafe 5 Appliance Management UI using an account with Domain Admin privileges.
2. In the top menu bar, click **Cluster**.
3. Go to the **Cluster** tab.
4. Select **Actions > Startup Authentication**.
5. In the Startup Authentication window, click **Edit**.
6. In the Passphrase Based Startup Authentication field, select **Disabled**.
7. Click **Apply**.

6.3.5. KeySafe 5 Backup and Restore

KeySafe 5 stores the configuration information and objects for all KeySafe 5 nodes in an encrypted object store that is shared among all nodes. Any changes you make on any KeySafe 5 node in the cluster is automatically disseminated to the other nodes in the cluster in a secure manner. This also allows you to backup all required information from any node in the cluster.

You can back up KeySafe 5 using:

- The KeySafe 5 Appliance Management UI. The encrypted backup files KeySafe 5 creates can be downloaded locally or accessed through NFS on authorized servers. For details, see Backing Up KeySafe 5 Through the KeySafe 5 Appliance Management UI.
- A third-party application that can take and restore system snapshots. You can restore KeySafe 5 at any time from a previous snapshot, but if any part of the VM changes you may be required to recover the Admin key as described in Recovering Access to

KeySafe 5. You can restore KeySafe 5 from a backup file using the KeySafe 5 Appliance Management UI. For details, see Restoring KeySafe 5 Through the KeySafe 5 Appliance Management UI.

6.3.5.1. Automatic Backup Feature

KeySafe 5 automatically creates a backup file once every 12 hours as long as the cluster is healthy. If this is the first time the automatic backup has completed successfully since the node was first initialized or restarted, KeySafe 5 records this information in the audit log. It does not send an alert or email to any KeySafe 5 users. It also does not record any subsequent successful backups.

The automatic backup schedule may change based on the following rules:

- If the cluster is in a degraded state, no automatic backup is attempted. The cluster must be healthy in order for KeySafe 5 to create a backup file.
- If the cluster is healthy but the automatic backup fails for some reason, KeySafe 5 retries the backup operation every hour. The first time the automatic backup fails KeySafe 5 records this information in the audit log and alerts all KeySafe 5 accounts with Domain Admin privileges. It does not record subsequent failed backup attempts.
- Changes to the KeySafe 5 configuration may trigger an automatic backup, but it is better to backup KeySafe 5 manually whenever you make changes to be certain that you have an up-to-date backup file available.

6.3.5.2. Backing Up KeySafe 5 Through the KeySafe 5 Appliance Management UI

This procedure creates an encrypted backup file that can be downloaded through NFS on authorized servers or downloaded via the KeySafe 5 Appliance Management UI to the administrator’s default download directory.

The backup file can later be used to restore KeySafe 5 to the state it was in when the backup was taken.

6.3.5.2.1. Procedure

1. Log into the KeySafe 5 Appliance Management UI using an account with Domain Admin privileges.
2. In the top menu bar, click **Cluster**.
3. Go to the **Cluster** tab.
4. If you want to make the backup file available through NFS:

   a. Make sure the **Backup Over NFS** option is set to **Enabled**.
   b. Verify the IP addresses in the **Backup Hosts** field. If you want any server to have access to the backup directory, enter 0.0.0.0.

5. Select **Actions > KeySafe 5 Backup**. KeySafe 5 displays the latest backup information if one exists.
6. Click Perform Backup. KeySafe 5 creates a new backup file in the backup directory on the server and updates the information in this dialog box.

   If you want to download the backup file locally, click **Download**. KeySafe 5 saves the encrypted backup file to your browser's default download location. The filename is in the format *<server-name>-<product_version>←datetimestamp>-<admin_key_version>.bu*.

   If you want to access the backup file through NFS, log into one of the servers listed in the **Backup Hosts** field and mount the directory using the mount command. For example, if your KeySafe 5 node IP address is 192.168.140.135, you would enter:

```
# mount -t nfs 192.168.140.135:/hcs/backup /backup
# ls -l /backup
total 506
lrwxrwxrwx  1 root root     30 Dec 16 14:57 htkc.bu -> testkc01-5.1-20191216092703-4.bu
-rw-r--r--  1 root root 191776 Dec 16 14:57 testkc01-5.1-20191216092703-4.bu
```

7. When you are done, click **Close**.

6.3.5.3. Accessing KeySafe 5 Backup Files

If you want to access an existing KeySafe 5 backup file, you can use the KeySafe 5 Appliance Management UI or, if you have configured an NFS server, you can use NFS.

6.3.5.3.1. Appliance Management UI Access

1. Log into the KeySafe 5 Appliance Management UI using an account with Domain Admin privileges.
2. In the top menu bar, click **Cluster**.
3. Go to the **Cluster** tab.
4. Select **Actions > KeySafe 5 Backup**. KeySafe 5 displays the latest backup information if one exists.
5. Click **Download**. KeySafe 5 saves the encrypted backup file to your browser's default download location. The filename is in the format *<server-name>-<product_version>←datetimestamp>-<admin_key_version>.bu*.

6. Click **Close**.

6.3.5.3.2. NFS Access

To access the backup file through NFS, log into one of the Backup Host servers configured for the cluster and mount the directory using the mount command. For example, if your KeySafe 5 node IP address is 192.168.140.135, you would enter:

```
# mount -t nfs 192.168.140.135:/hcs/backup /backup
# ls -l /backup
total 506
lrwxrwxrwx  1 root root     30 Dec 16 14:57 htkc.bu -> testkc01-5.1-20191216092703-4.bu
-rw-r--r--  1 root root 191776 Dec 16 14:57 testkc01-5.1-20191216092703-4.bu
```

6.3.5.4. Restoring KeySafe 5 Through the KeySafe 5 Appliance Management UI

Restoring from a KeySafe 5 backup should only be needed if there is a catastrophic failure in the KeySafe 5 cluster. If one KeySafe 5 node becomes unusable, for example due to hard ware failures, simply remove the node from the cluster and add a new node.

> ⚠ Restore is a destructive process. Any changes made to objects created since the backup image was taken will be lost. This includes policies, and KeySafe 5 user accounts. If the KeySafe 5 SSL certificate was changed since the backup was taken, the older SSL certificate will be restored along with the rest of the system and the current SSL certificate will be discarded.
>
> Custom SSL certificates for internal and external webservers will be restored only if the IP address specified in the certificate matches the KeySafe 5 IP address.

6.3.5.4.1. Procedure

1. Log into the KeySafe 5 Appliance Management UI using an account with Domain Admin privileges.
2. In the top menu bar, click **Cluster**.
3. If there are any other nodes in this cluster, you must remove them before you restore the node. To do so:
    a. Click on the **Servers** tab.
    b. Click on each of the other nodes in the cluster and select **Actions > Remove**.
    c. Click **Proceed** at the prompt to confirm the request.

4. Go to the **Cluster** tab.
5. Select **Actions > KeySafe 5 Restore**.
6. Click **Browse** and select the backup file from which you want to restore KeySafe 5. The name of the selected file appears next to the Browse button.
7. Click **Verify Image**. KeySafe 5 uploads the file and verifies that it is a valid backup file. It also displays a hint stating which Admin Key generation count goes with this backup file in case you need to upload the matching Admin Key parts. For example:

   Hint: Keypart generation version for this backup image is 16.

   For details, see Admin Keys.

8. Click **Restore Image**.
9. Click **Proceed** at the prompt to confirm the request. KeySafe 5 restores the system information from the backup file and reboots the server.
10. Verify the restoration by logging back into the KeySafe 5 Appliance Management UI.

> Remember that all user account information has been reverted back to whatever it was when the backup was taken. That means your account may not exist or that the password may have changed.

11. If the hardware has changed since the backup was taken, KeySafe 5 presents you with additional options.

Option	Description
Recovery using Keypart upload	Allows you to recover the Admin key by uploading the parts from local files. You must upload the required number of parts of the Admin key within 10 minutes to use this method. Important: All Admin key parts must have the key generation count that was valid when the back up was taken. For details, see Admin Keys.
Recovery from External key server	Allows you to recover the Admin key by connecting to an external KMIP (Key Management Interoperability Protocol) server or HSM (Hardware Security Module).
Decommission	Tells KeySafe 5 to decommission the server. For more information, see Decommissioning a KeySafe 5 Node.

12. If you removed any nodes from the cluster, re-join them as described in Joining or Re-joining a KeySafe 5 Cluster.

6.3.6. Removing a KeySafe 5 Node from a Cluster

1. Log into the KeySafe 5 Appliance Management UI on any node you are not removing using an account with Domain Admin privileges.
2. In the top menu bar, click **Cluster**.
3. Click the **Servers** tab.
4. Select the node you want to remove.
5. Select **Actions > Remove**.
6. Click **Proceed** at the prompt to confirm the request.
7. If this KeySafe 5 node is included in any KeySafe 5 Mappings, KeySafe 5 displays a mes sage stating which mappings it is a part of and giving you the following options. Select an option and click **Proceed** to continue.

Option	Description
Disable the KeySafe 5 node	Select this option if you are planning to re-join the node to the cluster later (for example, after upgrading it to a new KeySafe 5 version). You will need to manually re-enable the node in the Mapping after you re-join it with the cluster.
Remove the KeySafe 5 node	Select this option if you are removing the node permanently from the cluster.
Do not change the mapping	Select this option if you are planning to re-join the node with the cluster within a short time.

. KeySafe 5 removes the node and refreshes the **Servers** tab.

If you want to rejoin the node to an existing KeySafe 5 cluster, see Joining or Re-joining a KeySafe 5 Cluster.

If you want to remove the node permanently, see Decommissioning a KeySafe 5 Node.

6.3.7. Joining or Re-joining a KeySafe 5 Cluster

When you install KeySafe 5, you can specify whether you want to configure the node as the first node in the system (standalone) or add it to an existing cluster.

If you ever need to change the node's cluster assignment, or you need to re-join a node with its previous cluster, you can do so using the KeySafe 5 Appliance Management UI installed on the node. You do not need to re-install the KeySafe 5 software.

> ⚠ When a node is added to a cluster, any existing configuration and data are permanently deleted and cannot be restored. If this node was previously part of a different cluster or was used in standalone mode, make sure you do not need the data stored on this node before you add it to the new cluster.

6.3.7.1. Joining a KeySafe 5 Cluster

The following procedure describes how to configure a newly deployed node to join an exist ing KeySafe 5 cluster.

6.3.7.1.1. Before You Begin

- Make sure you know the IP address of any KeySafe 5 node that is already part of the cluster you want to join.
- If the node is currently part of a different cluster, you should remove the node from the original cluster so that the original cluster does not become degraded. For details, see Removing a KeySafe 5 Node from a Cluster.
- If you are re-joining a node to an existing cluster and you are using an externally signed SSL certificate for KeySafe 5, make sure that you use the same hostname for the KeySafe 5 node that it had originally. If you change the hostname, you will need to rein stall the externally signed SSL certificate on that node.
- A KeySafe 5 node cannot be joined to an existing KeySafe 5 cluster if the internal web server of the joining node is configured with a custom SSL certificate.
- Entrust recommends that you configure the KeySafe 5 node with a private IP address.

6.3.7.1.2. Procedure

1. Log into the KeySafe 5 Appliance Management UI on the KeySafe 5 node you want to join with the cluster.
2. On the Welcome to KeySafe 5 screen, click **Join an Existing Cluster**.

   The Join Existing Cluster window displays.

3. On the Get Started page, review the overview information to determine that you are ready to begin. This includes:

   - Access to the cluster you are joining the node to. We recommend that you open the KeySafe 5 Appliance Management UI for the cluster in a different tab or browser window.
   - Permissions on both this node and the cluster node so you can download and import the required certificates and files.
   - A passphrase to use during the joining process. Passphrase requirements are configured by a KeySafe 5 administrator in the System Settings. This phrase is a temporary string used to encrypt the initial communication between this node and the existing KeySafe 5 cluster.
   - Verifying that both this node and the cluster node are running the same KeySafe 5 version and build. The version number for the cluster node is on the **Settings > System Upgrade** page.

4. Click **Continue**.
5. On the Download CSR page, click **Generate and Download CSR**.
6. Click **Continue**.
7. Switch to one of the existing nodes in the cluster and navigate to the **Cluster** page.
8. Select **Actions > Add a Node**.
9. On the Add a Node window, upload the CSR that you downloaded from the new node (in .pem format) and enter a passphrase to use during the joining process.
10. Click **Save and Download Bundle** to download the certificate bundle from the cluster node.

    The certificate bundle is a .zip file you must unpack. It contains both an encrypted SSL certificate in .p12 format and a CA certificate in .pem format.

11. Click **OK** to close the Add a Node window.
12. Return to the new node and click **Continue**.
13. On the Node page, upload the encrypted SSL certificate and CA certificate that you downloaded from the cluster node, enter the IP address or hostname of any node in the existing cluster, and enter the passphrase that you selected.
14. Click **Join**.

    During the joining process, a status page is displayed on the new node. Do not refresh the browser while this is in process.

    The cluster will automatically be placed in maintenance mode.

    The node will restart after the join is complete.

15. When the node has successfully restarted, click **Login**.

6.3.7.2. Re-Joining a KeySafe 5 Cluster

The following procedure describes how to configure a node that has been in use as either a standalone node or part of a cluster to join another existing KeySafe 5 cluster.

❗ This process will destroy all data on the node.

6.3.7.2.1. Before You Begin

- Make sure you know the IP address of any KeySafe 5 node that is already part of the cluster you want to join.
- If the node is currently part of a different cluster, you should remove the node from the original cluster so that the original cluster does not become degraded. For details, see Removing a KeySafe 5 Node from a Cluster.
- If you are re-joining a node to an existing cluster and you are using an externally signed SSL certificate for KeySafe 5, make sure that you use the same hostname for the KeySafe 5 node that it had originally. If you change the hostname, you will need to rein stall the externally signed SSL certificate on that node.

6.3.7.2.2. Procedure

1. Log into the KeySafe 5 Appliance Management UI on the KeySafe 5 node you want to join with the cluster.
2. In the top menu bar, click **Cluster**.
3. Select **Actions > Join a Cluster**.

   The Join Existing Cluster window displays.

4. On the Get Started page, review the overview information to determine that you are ready to begin. This includes:
   - Access to the cluster you are joining the node to. We recommend that you open the KeySafe 5 Appliance Management UI for the cluster in a different tab or browser window.
   - Permissions on both this node and the cluster node so you can download and import the required certificates and files.
   - A passphrase to use during the joining process. The passphrase must contain 12 alphanumeric characters. It cannot contain spaces or special characters. This phrase is a temporary string used to encrypt the initial communication between this node and the existing KeySafe 5 cluster.
   - Verifying that both this node and the cluster node are running the same KeySafe 5 version and build. The version number for the cluster node is on the **Settings > Sys**

tem Upgrade page.

5. Confirm that you understand that all existing data on this node will be deleted by typing "delete my data".
6. Click **Continue**.
7. On the Download CSR page, click **Generate and Download CSR**.
8. Click **Continue**.
9. Switch to one of the existing nodes in the cluster and navigate to the Cluster page.
10. Select **Actions > Add a Node**.
11. On the Add a Node window, upload the CSR that you downloaded from the new node (in .pem format) and enter a passphrase to use during the joining process.
12. Click **Save and Download Bundle** to download the certificate bundle from the cluster node.

    The certificate bundle is a .zip file you must unpack. It contains both an encrypted SSL certificate in .p12 format and a CA certificate in .pem format.

13. Click **OK** to close the Add a Node window.
14. Return to the new node and click **Continue**.
15. On the Node page, upload the encrypted SSL certificate and CA certificate that you downloaded from the cluster node, enter the IP address or hostname of any node in the existing cluster, and enter the passphrase that you selected.
16. Click **Join**.

    During the joining process, a status page is displayed on the new node. Do not refresh the browser while this is in process.

    The cluster will automatically be placed in maintenance mode.

    The node will restart after the join is complete.

17. When the node has successfully restarted, click **Login**.

6.3.8. Rebooting a KeySafe 5 Node

You can only reboot the node that you are currently using.

1. Log into the KeySafe 5 Appliance Management UI using an account with Domain Admin privileges.
2. In the top menu bar, click **Cluster**.
3. Go to the **Servers** tab.

4. Select **Actions > System Reboot**.
5. Click **Proceed** to acknowledge the warning message.

6.3.9. Decommissioning a KeySafe 5 Node

6.3.9.1. Before You Begin

- Make sure the node is not part of a cluster before you decommission it. For details, see Removing a KeySafe 5 Node from a Cluster.
- Make sure you have access to all of the key parts for the Admin key that was generated for this system. All of the parts need to be uploaded within 10 minutes of the first file upload in order for the decommission to work.

  If there are multiple system administrators, each administrator has one of the key parts. You can either collect the parts and have one administrator upload them all or you can have each administrator log in and upload their part simultaneously.

  For this procedure you must use the Admin Key parts that were sent to the Security Administrators. You cannot use the Admin Key stored on an external key server.

> ⚠ When you decommission a KeySafe 5 node, KeySafe 5 uses zeroization to completely erase the data on the disks where the KeySafe 5 software and the object store are located. This is a non-reversible procedure.

6.3.9.2. Procedure

1. Log into the KeySafe 5 Appliance Management UI on the node you want to decommission using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **System Settings** section, click **System Decommission**.
4. Click **Browse** to upload the first part of the admin key. Navigate to the key part and click **Choose**. The filename of the key part replaces the text of the **Browse** button.
5. Click **Upload File**.
6. If there is only one admin key part, KeySafe 5 immediately logs you out of the system and zeroes out the disks associated with the KeySafe 5 node. If there are multiple key parts, KeySafe 5 starts a 10 minute timer. All admin key parts must be uploaded within the 10 minutes before KeySafe 5 will decommission the node.
7. If you need to restart the process, click **Reset**. You will need to re-upload all key parts to complete the process.

6.4. System Maintenance and Troubleshooting

6.4.1. Increasing KeySafe 5 Storage in a VM

If you installed KeySafe 5 in a VM, you can increase the amount of storage available without reinstalling KeySafe 5. You just need to increase the size of the underlying disk and reboot the KeySafe 5 node.

1. Increase the size of the virtual disk in which KeySafe 5 is installed using your hypervisor tools.

   Note: You may need to shut down the VM before you can resize the disk. For details, see your hypervisor documentation.

2. Log into the KeySafe 5 Appliance Management UI using an account with Domain Admin privileges.
3. In the top menu bar, click **Cluster**.
4. Select the KeySafe 5 node whose disk you just resized in the list.
5. Select **Actions > System Reboot**.
6. If necessary, log back into the KeySafe 5 Appliance Management UI after the KeySafe 5 node has rebooted.
7. Review the Audit Log messages. The node should report the new size upon success or provide information if the resize failed.

6.4.2. Troubleshooting Network Issues

The KeySafe 5 System Console provides diagnostics that let you test the link between a KeySafe 5 node and external servers such as DNS servers, NTP servers, other KeySafe 5 node servers, or servers running third-party applications such as OIDC servers.

1. Use your hypervisor to access one of the VMs in which KeySafe 5 is running, then log into the KeySafe 5 VM console as `htroot`.
2. KeySafe 5 displays the Entrust KeySafe 5 System Console TUI (Text-based User Interface).
3. Select **Manage Network Settings** and press **Enter**.
4. Select **Network Diagnostic Tools** and press **Enter**.
5. On the Network Diagnostics page, select one of the following options:

Option	Description
Verify DNS Server Response	Enter a comma-separated list of IP address that you want KeySafe 5 to verify as a DNS server. KeySafe 5 responds with one verification line per specified server. This test can be used to verify that the KeySafe 5 node can communicate through the firewall on the correct port to the specified IP addresses.
Verify NTP Server Response	Enter a comma-separated list of IP address or host-names that you want KeySafe 5 to verify. KeySafe 5 responds with one verification line per specified server.
Test Remote Server is Reachable	This option sends a simple ping (ICMP) to another server to see if that server is up and responding. This test does not prove that the current KeySafe 5 node can actually communicate with the target server. It just means that the target server exists and is online.

Option	Description
Test Inbound Ports of Another Server	This option tests whether the current KeySafe 5 node can communicate with the target server on the specified ports (the default port is 8443 for KeySafe 5 to KeySafe 5 communication). If you want to specify multiple ports, separate the port numbers with a space. The test returns one of the following responses for each specified port: **OK** — The current node can communicate with the target server on the specified port. This response does not mean, however, that the target server can communicate back to the current node. If the target is another KeySafe 5 node with which you want to form a cluster, you need to log into the target node and run this test again using the target node as the base. If the test passes on both servers, then the two KeySafe 5 nodes can be joined in a single cluster. **Connection Refused** — The current node cannot communicate with the target node through the specified port. **Operation Timed Out** — The target node did not respond to the communication request from the current node.
Return to Main Menu	Closes the Network Diagnostics page and returns to the main Entrust KeySafe 5 System Console page.

6.4.3. Support Access and Log Files

Entrust provides two methods of support access:

- Restricted support — Customers can access support logs and run simple diagnostic tools through a limited SSH-accessible shell that can be invoked from the Entrust KeySafe 5 System Console. For details, see Using the Restricted Shell.
- Full support — The Entrust support staff can access and troubleshoot the customer's system. Full support access requires multi-factor authentication between the KeySafe 5 Administrator at the customer site and Entrust Support. If such access is required, Entrust Support will guide you through the process.

6.4.3.1. Using the Restricted Shell

The restricted support login provides a limited SFTP-accessible shell in which the KeySafe 5 administrator can gather diagnostic information. It is disabled by default.

6.4.3.2. Creating a Support Bundle with the KeySafe 5 Appliance Management UI

In certain circumstances it may be necessary to gather diagnostic information and logs from KeySafe 5 that can be sent to Entrust support for further analysis. The following procedure describes how to create a log bundle using the KeySafe 5 Appliance Management UI.

1. Log into the KeySafe 5 Appliance Management UI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **Support** section, click **Download Logs**.
4. If a log has not yet been created for this cluster or if you want to generate a new log, click **Create Bundle**.
5. In the Logs dialog box, enter the following information:

Option	Description
Include Audit Log	If Yes, KeySafe 5 includes the full audit log in the bundle. The default is Yes.
Include All Cluster Logs	If Yes, KeySafe 5 includes the log bundle from every KeySafe 5 node in the cluster. If No, KeySafe 5 only includes the log bundle from the current node. The default is No.
Include Core Files	If Yes, KeySafe 5 includes core files in the bundle. The default is No.
Passphrase	If you specify a passphrase, KeySafe 5 encrypts the bundle with an AES 256-bit key using the provided passphrase.

6. When you are done, click **Create**. KeySafe 5 creates the log file and then refreshes the information about the log bundle it created.
7. To download the bundle, click **Download**.

6.4.3.3. Enabling or Disabling Support Logins

You must enable support accounts before support personnel from Entrust can access your system. When the account is enabled, support personnel have full access to the system to carry out diagnosis and repairs in exceptional situations.

You can disable the support account after, for example, a successful upgrade. The support login will be disabled automatically after 24 hours.

1. Log into the KeySafe 5 Appliance Management UI using an account with Security Admin privileges.
2. In the top menu bar, click **Cluster**.
3. Click the **Servers** tab.
4. Select the node you want to modify.
5. Select **Actions > Support Login Settings**.
6. On the Support Login Settings page, check the **Enable Support Login** checkbox.
7. Enter and confirm the password for the support login.

   The password must be at least 8 characters long, including 1 digit, 1 uppercase character, 1 lowercase character, and 1 symbol.

8. Click **Save**.
9. If the support login is enabled, you can disable it by checking the **Disable Support Login** checkbox and clicking **Save**.

6.4.4. Recovering Access to KeySafe 5

There are times when you will need to recover your KeySafe 5 system, such as when you increase the number of CPUs allotted to a KeySafe 5 server, change the network hardware address, migrate KeySafe 5 to a different host, or restore from a backup to a newly-created VM. The system recovery process prevents rogue administrators from making unauthorized changes to, or copies of, KeySafe 5 disks.

- When you make a change that affects the hardware signature, the KeySafe 5 Appliance Management UI displays the System Recovery dialog box.
- For backup/restore, the KeySafe 5 Appliance Management UI displays the System Recovery Options dialog box.

6.4.4.1. Procedure

1. Select the method you want to use to recover your system. The options are:

Option	Description
Recovery using Keypart Upload	Allows you to upload the minimum number of required Admin Key parts that were sent to the Security Admins in the system. If you select this option, the KeySafe 5 Appliance Management UI displays the Recover Admin Key page. To upload a part, click **Browse** and select the appro priate recovery_key file. The Browse button should change to show the name of the selected file. When the correct file is displayed, click **Upload file**. Make sure that all Admin Key parts you upload have the same generation count. This information can be found in the email accompanying the Admin Key part. For details, see Admin Keys. When the required number of parts have been uploaded, KeySafe 5 recovers the system and displays the Recovery Success message. Click Proceed to return to the KeySafe 5 Appliance Management login page.
Recovery using Passphrase	Allows you to recover your system when you are using passphrase-based authentication. If you select this option, the UI displays the Recovery Passphrase page. Enter your passphrase and click Recover. For more information, see Startup Authentication.
Decommission	If you want to decommission your KeySafe 5 system, see Decommissioning a KeySafe 5 Node.

2. If there are multiple KeySafe 5 nodes in the cluster, re-join those nodes with the node you just recovered. For details, see Joining or Re-joining a KeySafe 5 Cluster.

7. Security Guidance

Your nShield HSM protects the confidentiality and integrity of your Security World keys. KeySafe 5 allows an authorized client to remotely configure and manage an estate of nShield HSMs. All network traffic between KeySafe 5 and clients using the UI, the REST API, or both, passes through a secure channel. This TLS based secure channel is set up using token-based client authentication. The administrator of the KeySafe 5 system must remain diligent concerning the entities who are given access to the system and the secure configu ration of the system.

Entrust recommends the following security-related actions for KeySafe 5 deployments:

- Ensure that log levels are set appropriately for your environment.

  More verbose log levels might expose information that is useful for auditing users of KeySafe 5, but the log information also reveals which REST API operations were performed. While this log information might be useful for diagnostics, it could also be considered sensitive and should be suitably protected when stored.
- Rotate the logs regularly. The log files could grow quickly if left unattended for a long time. The system administrator is responsible for log rotation.
- Verify the integrity of the KeySafe 5 tar file before executing it. You can verify the integrity of this file with the hash provided with the software download.
- Suitably protect the network environment of KeySafe 5 to maintain its availability, for example using firewalls and intrusion detection and prevention systems.
- Ensure that the KeySafe 5 platform's system clock is set accurately and only authorized system administrators can modify it so that the platform correctly interprets certificate and token lifetimes.
- Ensure that only authorized system administrators have access to the KeySafe 5 system, and only trusted software is run on the platform hosting KeySafe 5.
- Take standard virus prevention and detection measures on the platform hosting KeySafe 5.
- The system administrator should consider whether threats in the KeySafe 5 deployment environment would justify the encryption of the sensitive configuration data held in Kubernetes secrets, see Kubernetes documentation.

8. Certificate Signing Request Generation

The generation of a Certificate Signing Request (CSR) is required for the KeySafe 5 Agent and optionally for using the internal MongoDB database with other Entrust products, such as the nShield Web Services product.

8.1. KeySafe 5 Agent CSR Generation

> These steps are provided as an example, Entrust recommends that the values are adjusted to your organization's needs.

1. Generate a private key

```
openssl genrsa -out tls.key 4096
```

> Entrust recommends that the private key is created on the machine where you are installing the KeySafe 5 Agent and that access to the file is restricted.

2. Generate a CSR.

   a. Create a file called agent_csr.cnf with the following. The DNS.1 entry must match the hostname that the KeySafe 5 agent identifies as and must be the first entry in the [alt_names] section. IP.1 is the IP address of the KeySafe 5 agent host.

```
[req]
distinguished_name = req_distinguished_name
req_extensions = req_ext
prompt = no

[req_distinguished_name]
C   = UK
ST  = Cambs
L   = Cambridge
O   = Entrust
OU  = nShield
CN  = www.entrust.com

[req_ext]
subjectAltName = @alt_names

[alt_names]
DNS.1 = keysafe5.ncipher.com
IP.1 = 111.222.333.444
```

   b. Generate the CSR request.

```
openssl req -new -key tls.key -out tls.csr -config agent_csr.cnf
```

The CSR generated can then be supplied during the Obtaining the KeySafe 5 Agent Certificates procedure.

8.2. MongoDB CSR Generation

> ℹ These steps are provided as an example, Entrust recommends that the values are adjusted to your organization’s needs.

1. Generate a private key

   ```
   openssl genrsa -out tls.key 4096
   ```

   > ❗ Entrust recommends that access to the private key file is restricted.

2. Generate a CSR.

   a. Create a file called mongo_csr.cnf with the following. The "subject" of the CSR must match the value "OU = mongodb, CN = keysafe5-mongo".

   ```
   [req]
   distinguished_name = req_distinguished_name
   req_extensions = req_ext
   prompt = no

   [req_distinguished_name]
   OU = mongodb
   CN = keysafe5-mongo

   [req_ext]
   subjectAltName = @alt_names

   [alt_names]
   DNS.1 = keysafe5.ncipher.com
   IP.1 = 111.222.333.444
   ```

   b. Generate the CSR request.

   ```
   openssl req -new -key tls.key -out tls.csr -config mongo_csr.cnf
   ```

The CSR generated can then be supplied during the MongoDB Database: Internal Database procedure.

9. Database

All persistent data for KeySafe 5 is stored in the MongoDB database.

9.1. Databases

KeySafe 5 stores data in three different databases within MongoDB. One database for storing HSM Management related data, one database for storing Security World Management related data and one for storing CodeSafe Management related data.

The names of the databases used within MongoDB are defined by the `helm-keysafe5-backend` Helm chart.

Key	Description	Default value
codesafe_mgmt.dbName	Name of the database to use for storing persistent CodeSafe data	codesafe-mgmt-db
hsm_mgmt.dbName	Name of the database to use for storing persistent HSM data	hsm-mgmt-db
sw_mgmt.dbName	Name of the database to use for storing persistent Security World data	sw-mgmt-db

9.2. Collections

9.2.1. HSM Management database

KeySafe 5 stores nShield HSM related data in the following collections:

- hsms
- pools
- hosts
- hardservers
- features

9.2.2. Security World Management database

KeySafe 5 stores nShield Security World data in the following collections:

- worlds

For each Security World known to KeySafe 5, the following collections are automatically cre ated, where each collection name is prefixed by the ID of the Security World database record that the collection corresponds to:

- <id>_actions
- <id>_authorizations
- <id>_authorized_pools
- <id>_cards
- <id>_cardsets
- <id>_domains
- <id>_groups
- <id>_keys
- <id>_module_certs
- <id>_operations
- <id>_p11objects
- <id>_softcards

9.2.3. CodeSafe Management database

KeySafe 5 stores nShield CodeSafe related data in the following collections:

- images
- machines
- certificates
- certificatestatus
- operations
- steps

9.3. User Roles

MongoDB has the notion of roles, where each role has a defined set of allowed actions. A user of a MongoDB database can be given a role which then determines what the user can and cannot do to the data.

For details about MongoDB roles, see the MongoDB documentation.

From a security point of view we want to give KeySafe 5 as a user of the MongoDB database the least privileges which suffice for the functionality it requires from the MongoDB database.

The documentation below details the minimum privileges required for a KeySafe 5 MongoDB user for each database created by KeySafe 5.

9.3.1. HSM Management database

The following actions are required by KeySafe 5 for the operation of MongoDB for the HSM Management collections:

- createIndex
- find
- insert
- remove
- update

The MongoDB administrator will configure the HSM Management database with the following actions and privileges for KeySafe 5 `hsm-mgmt-db-user` role:

```
use admin
db.createRole(
  {
    role: "hsm-mgmt-db-user",
    privileges: [
        {
          "resource": {"db": "hsm-mgmt-db", "collection": ""},
          "actions": ["createIndex", "find", "insert", "remove", "update"]
        },
      ],
    roles: []
  }
)
```

9.3.2. Security World Management database

As KeySafe 5 creates new collections in the Security World Management Database as new Security Worlds are introduced to the system, RBAC (Role-based access control) must be applied at the database level rather than individual collections.

The following actions are required by KeySafe 5 for the operation of MongoDB for the Security World Management collections:

- createIndex
- dropCollection
- find

- insert
- remove
- update

The MongoDB administrator will configure the Security World Management database with the following actions and privileges for KeySafe 5 `sw-mgmt-db-user` role:

```
use admin
db.createRole(
  {
    role: "sw-mgmt-db-user",
    privileges: [
        {
          "resource": {"db": "sw-mgmt-db", "collection": ""},
          "actions": ["createIndex", "dropCollection", "find", "insert", "remove", "update"]
        },
      ],
    roles: []
  }
)
```

9.3.3. CodeSafe Management database

The following actions are required by KeySafe 5 for the operation of MongoDB for the Code Safe Management collections:

- createIndex
- find
- insert
- remove
- update

The MongoDB administrator will configure the CodeSafe Management database with the following actions and privileges for KeySafe 5 `codesafe-mgmt-db-user` role:

```
use admin
db.createRole(
  {
    role: "codesafe-mgmt-db-user",
    privileges: [
        {
          "resource": {"db": "codesafe-mgmt-db", "collection": ""},
          "actions": ["createIndex", "find", "insert", "remove", "update"]
        },
      ],
    roles: []
  }
)
```

9.3.4. Creating a MongoDB user with the User-defined roles

The MongoDB administrator may create a user for the KeySafe 5 application to access the KeySafe 5 databases by using the `db.createUser` command in the MongoDB shell.

```
ks5_user = {
   "user" : "ks5username",
   "roles" : [
     {"role": "codesafe-mgmt-db-user", "db": "admin" },
     {"role": "hsm-mgmt-db-user", "db": "admin" },
     {"role": "sw-mgmt-db-user", "db": "admin" },
   ]
 }
> db.createUser(ks5_user)
```

Note that when using TLS authentication for MongoDB, the username needs to match the subject of the client certificate.

9.4. Authentication Methods

KeySafe 5 supports the following authentication mechanisms for access to the MongoDB server:

- No authentication
- SCRAM
- X.509 certificate authentication

The type of authentication is specified by `database.mongo.auth.type` value in the `helm-keysafe5-backend` Helm chart.

9.4.1. No Authentication

This option is used during development. It should not be used during production.

9.4.2. SCRAM

Using Salted Challenge Response Authentication Mechanism (SCRAM), MongoDB verifies the supplied credentials against the MongoDB's username, password and authentication database.

In the `helm-keysafe5-backend` Helm chart:

- `database.mongo.auth.type` must be set to `pwd`.

- `database.mongo.auth.existingSecret` must be set to the name of an existing Kubernetes Secret that contains the username and password to use (the Secret must contain a value for `username` and `password` keys).
- `database.mongo.auth.authDatabase` must be set to the name of MongoDB's authentica tion database.

9.4.3. X.509 Certificate Authentication

KeySafe 5 can use X.509 certificates instead of usernames and passwords to authenticate to the MongoDB database.

In the `helm-keysafe5-backend` Helm chart:

- `database.mongo.auth.type` must be set to `tls`.
- `database.mongo.tls.enabled` must be set to `true`.
- `database.mongo.tls.existingSecret` must be set to the name of an existing Kubernetes Secret that contains the TLS certificates to use (the Secret must contain the keys `tls.crt`, `tls.key` and `ca.crt`).

9.5. Backup

To be able to restore the KeySafe 5 application, Entrust recommends that you regularly backup the MongoDB database as suggested in the MongoDB documentation.

9.6. Maintenance

> ❗ The KeySafe 5 application (`helm-keysafe5-backend` Helm chart) does not support having database collections removed while the application is running.

If deleting collections, or replacing the MongoDB server that KeySafe 5 uses, then please stop the `helm-keysafe5-backend` Helm chart before performing database maintenance and restart the application once the database maintenance is complete.