SyMRI®

SyntheticMR AB

2026-01-13

SyConnect

Installation and System Administration Guide
Version: 2.8.7.207.945

SyntheticMR

Contents

1 Introduction

SyConnect is a system that can run automated workloads based on input and rules.

SyConnect® is the property of and produced by SyntheticMR AB.

SyConnect uses other 3rd party products/packages. A full list can be found in the SyConnect's About view when logged in as an administrator.

The SyMRI logo is the copyright of SyntheticMR AB.

2 System Requirements

SyConnect can be installed in two forms: as a Virtual Appliance or directly on physical hardware. The requirements for physical hardware is higher to account for increased demands in the future.

2.1 Virtual Appliance

Requirement	Description
Processor	x86-64-v2 or newer, 4 cores or more
Memory	Memory requirement depends on the size of the data loaded, the in-plane resolution and number of slices: • 16 GB minimum, up to 256x256x190 • 24 GB recommended, up to 256x256x190 • 40 GB recommended, up to 512x512x380
Disk	300 GB or larger
TPM	Virtual TPM 2.0 (vTPM) required for encryption
Internet	3Mbps download speed, for upgrades to be downloaded before timeout
Hypervisor	Type 1 Hypervisor with EFI support

2.2 Physical Hardware

Requirement	Description
Processor	x86-64-v2 or newer, 8 cores or more
Memory	64 GB
Disk	1 TB or larger
TPM	TPM 2.0 required for encryption
Internet	3Mbps download speed, for upgrades to be downloaded before timeout

2.3 Network

SyConnect is configured to use the following listening ports by default.

Port	Description
8443	First time installation (FTI), disabled after FTI is complete
443	HTTPS dashboard and administrative web UI
104	DICOM (port number configurable)
80	HTTP to HTTPS redirect
22	SSH for CLI administration

A single NIC can be assigned to the VM. A static IP address or fixed DHCP is required, system defaults to DHCP. DNS access is required. Internet access is required.

2.4 External Endpoints Required

For SyConnect to install and later update itself, it needs access to the following external endpoints.

For sites in the EU:

- https://syconnect-containers.syconnect-home-eu.syntheticmr.com
- https://syconnect-management.syconnect-home-eu.syntheticmr.com
- https://syconnect-packages.syconnect-home-eu.syntheticmr.com

For sites in the US:

- https://syconnect-containers.syconnect-home-us.syntheticmr.com
- https://syconnect-management.syconnect-home-us.syntheticmr.com
- https://syconnect-packages.syconnect-home-us.syntheticmr.com

In order to synchronize time, SyConnect also needs access to the following endpoints:

- 0.ubuntu.pool.ntp.org
- 1.ubuntu.pool.ntp.org
- 3.ubuntu.pool.ntp.org

Optional, for future components:

- https://*.syntheticmr.com

2.5 EFI and Secure Boot

SyConnect requires EFI firmware. For VMware platforms, EFI settings are embedded in the OVA. For other virtualization platforms, EFI firmware may need to be enabled after deploying the OVA. For physical hardware, the BIOS may have to be configured to support EFI boot.

SyConnect optionally supports Secure Boot. For VMware platforms, Secure Boot is enabled by default. For other virtualization platforms, Secure Boot may be enabled after deploying the OVA.

Contact your hypervisor provider to learn what options are available to you.

2.6 Security Recommendations

DICOM network communication established by SyConnect is not encrypted. It is strongly advised to only run the application on dedicated secured networks, preferably with point-to-point encryption between the nodes.

It is strongly advised to have the hypervisor encrypt the virtual machines' virtual drives as part of its storage policy. In VMware vSphere, the feature is called "Virtual Machine Encryption". Nutanix calls the feature "Data-at-Rest Encryption (DaRE)". Similar effects can be accomplished with Proxmox.

SyConnect uses TPM to manage secrets. For VMware vCenter Server 7.0 Update 2 and later, configured with a key provider, settings for a virtual TPM device is embedded in the OVA. For other virtualization platforms, a virtual TPM device may be added after deploying the OVA.

Contact your hypervisor provider to learn what options are available to you.

3 Installation Steps

SyConnect can either be installed as a Virtual Appliance or directly on physical hardware. For both forms of installations, an Installation Token provided by a SyntheticMR representative is needed. This is used to register your instance with the SyntheticMR SyConnect Management System and acquire a SyConnect license. The license will be automatically renewed daily.

Download the latest version of the OVA, for installation in virtual environment, or ISO file, for installation directly on physical hardware, from:

- SyConnect Europe Download Site
- SyConnect US Download Site

3.1 Virtual Appliance

1. Download the provided zip archive, syconnect-<version>.zip. Extract the OVA file from the archive.
2. Create a virtual machine in your virtualization solution using the `syconnect.ova` appliance file. Take special care to allocate CPU and RAM based on your expected workload, see 2 System Requirements. Take note of the IP and/or FQDN. See section 7.1 Log In for information about how to log in to the virtual machine.
3. Visit `https://<IP/FQDN>:8443` in a browser, a warning about insecure connection due to self-signed certificates will be displayed, this can be safely ignored. If the IP-address is unreachable, a change in network configuration might be needed. See section 6.4 Network Configuration. Now you are ready to begin the First Time Installation (FTI), this process can usually be completed in one hour.

3.2 Physical Hardware

For physical hardware installation, a 4GB+ USB-stick is needed as installation medium.

`Note:` *It is important to understand that this installation process will erase all content on the USB-stick and on the target computer's HDD.*

1. Download the provided ISO file, syconnect-<version>.iso.
2. Create the installation medium. The instructions cover the use of the open source application Rufus (link) to create a bootable USB-stick with the ISO-image. Other applications, may produce similar results. When using Rufus, select the ISO file as the source by pressing `SELECT`. Choose

the USB-stick as the target from the `DEVICE` drop-down menu. See Figure 3.1 for an example of a Rufus configuration. Click on `START` to create the bootable USB-stick. In the dialog that asks about write mode, select "Write in DD Image mode", see Figure 3.2.

3. Insert the USB-stick into the target computer and boot from it.

4. Let the boot process complete. It will after a while complete with a prompt: "syconnect login:", enter `syconnect` as both user name and password, the password will have to be entered twice.

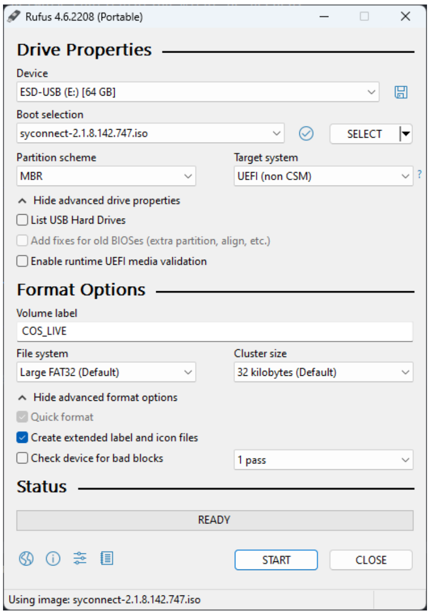
5. Find the HDD device by running: `lsblk -pd` and note the device name. Look at the SIZE column, with a single HDD system only one device will be larger than 300GB. In the example 3.1 the output shows the device: `/dev/nvme0n1` as the only device that fulfill the criteria.

```
syconnect@syconnect:~$ lsblk -pd
NAME         MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
/dev/loop0     7:0    0   1.4G  1 loop /run/rootfsbase
/dev/sda       8:16   1  14.6G  0 disk
/dev/nvme0n1 259:0    0 953.9G  0 disk
```

Listing 3.1: Example of lsblk output

6. Install SyConnect onto the HDD by running: `sudo elemental install <device-name>`. Using the example 3.1 the command would be `sudo elemental install /dev/nvme0n1`. When finished, reboot the computer by running: `sudo reboot`.

7. Visit `https://<IP/FQDN>:8443` in a browser, a warning about insecure connection due to self-signed certificates will be displayed, this can be safely ignored. If the IP-address is unreachable, a change in network configuration might be needed. See section 6.4 Network Configuration. Now you are ready to begin the First Time Installation (FTI), this process can usually be completed in one hour.


Rufus 4.6.2208 (Portable)

Drive Properties

Device: ESD-USB (E:) [64 GB]

Boot selection: syconnect-2.1.8.142.747.iso

Partition scheme: MBR

Target system: UEFI (non CSM)

Hide advanced drive properties

□ List USB Hard Drives

□ Add fixes for old BIOSes (extra partition, align, etc.)

□ Enable runtime UEFI media validation

Format Options

Volume label: COS_LIVE

File system: Large FAT32 (Default)

Cluster size: 32 kilobytes (Default)

Hide advanced format options

☑ Quick format

☑ Create extended label and icon files

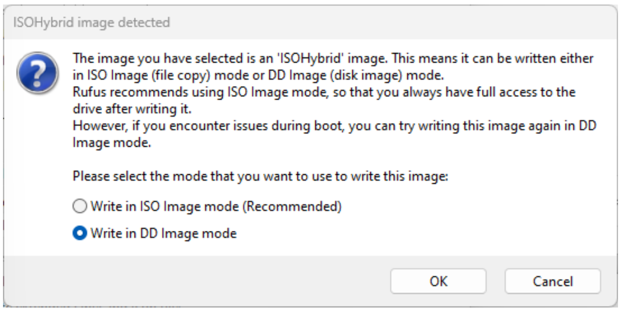
□ Check device for bad blocks — 1 pass

Status

READY

Using image: syconnect-2.1.8.142.747.iso

Figure 3.1: Example configuration of Rufus


ISOHybrid image detected

The image you have selected is an 'ISOHybrid' image. This means it can be written either in ISO Image (file copy) mode or DD Image (disk image) mode.
Rufus recommends using ISO Image mode, so that you always have full access to the drive after writing it.
However, if you encounter issues during boot, you can try writing this image again in DD Image mode.

Please select the mode that you want to use to write this image:

○ Write in ISO Image mode (Recommended)

● Write in DD Image mode

Figure 3.2: Rufus Write Mode

3.3 First Time Installation

This section describes the First Time Installation steps.

3.3.1 Start

A page displaying the versions of the FTI and OVA.

3.3.2 Encryption Keys

In the case TPM 2.0 or virtual TPM 2.0 (vTPM) is available for SyConnect, certain information in the system will be encrypted. In that case, a master key will be generated and displayed. Make sure to store it in a safe place, it will be needed if you export the configuration of SyConnect to another instance. The master key is stored in the TPM and will *not* be part of an exported configuration.

If a configuration import is to be done during the FTI, from a SyConnect instance with TPM available, the master key from the instance from which the export was done must be imported in this step. If the incorrect master key is provided, the configuration import will fail. See section 6.6 Encryption for more information.

3.3.3 License

Here the Installation Token must be submitted to automatically register your SyConnect instance. Also, a requirement check is done that verifies that the system requirements are met, see 2 System Requirements. If the requirements are not met, it is still possible to continue the installation.

3.3.4 Check for Updates

If the FTI component is out-of-date, the latest version will be downloaded and the FTI will be restarted.

3.3.5 Configuration

This page lets you configure these settings:

- `OS Administrator Password` Password of the local OS user `syconnect`. Will be used for e.g. SSH access.
- `SyConnect Administrator Password` Password of the SyConnect Portal user `admin`.
- `Hostname`
- `Description` The description of this SyConnect instance, e.g. 'Production' or 'Test'.
- `Timezone`

The passwords must be sufficiently strong to be accepted, the strength is calculated according to `https://github.com/dropbox/zxcvbn`.

3.3.6 Import SyConnect Configuration

Here you have the option to continue the installation using a default configuration or import a previously exported configuration. See 3.6 Migrating Configuration for more information.

3.3.7 Summary

Displays a summary of the configurations and lets you start the installation.

3.3.8 Finalizing Installation

The SyConnect components are now being downloaded. A progressbar shows the progress. Once the process is complete SyConnect will be ready to use and a link will appear, letting you access the SyConnect Portal at `https://<IP/FQDN>`. Log in to the SyConnect Portal with the username `admin` and the password you chose during FTI.

3.4 Request and Install SyMRI Licenses

Follow these steps to request and then install a SyMRI license file.

1. Log in to the SyConnect Portal with an administrative user.
2. Click on `Administration` and then click on `Licenses`.
3. Click on `SHOW SYMRI HARDWARE ID`.

   Copy the output and provide it to a SyntheticMR sales representative.
4. A SyntheticMR sales representative will create a SyMRI license file and provide it to you.
5. Click on `UPLOAD SYMRI LICENSES` and select the file that was provided to you.
6. Ensure that the license is shown in the list below these buttons after upload has finished.

3.5 Upgrade

The SyConnect appliance will update automatically by default at 3 AM every night. See section 5.7 Automatic Upgrades for more information on the configuration options available.

`Note:` *Interruption in service will occur during upgrade.*

To upgrade SyConnect manually:

```
sudo systemctl start syconnect-upgrade
```

To recover from an aborted or interrupted upgrade where the above command don't succeed, follow these steps:

1. Optional: Run `syconnectctl update --check-only` to see if there are any updates.

2. Run `syconnectctl update-utils` to update utility versions. You might need to manually restart the nomad service by running `sudo systemctl restart nomad.service`.

   Run `syconnectctl update` to update to the latest version. SyConnect will be stopped during the update process.

   Run `syconnectctl upgrade-system` to upgrade the system image to the latest version. If a new image is available, a reboot is required for the new image to become active.

   When the process has finished the system should be up and running.

   It is now possible to visit the SyConnect portal on `https://<virtualhost>` and log in using the credentials you created in the previous steps.

3.6 Migrating Configuration

To migrate configuration from one SyConnect instance to another, begin by exporting configuration from the current instance:

1. Log in to the SyConnect Portal with an administrative user.
2. Click on `Administration` and then click on `Configuration File`.
3. Click on `Export System Configuration` to download the configuration bundle.

During the FTI of the new SyConnect instance, when prompted for configuration, upload the configuration bundle.

`Note:` *When migrating from SyConnect 1.x to SyConnect 2.x, there are no encryption keys to migrate. Instead, use the FTI to generate new keys.*

3.7 Reset

The SyConnect VM contains a recovery image. Booting the recovery image does not modify the systems state. To exit recovery mode, reboot the VM.

The recovery image contains tooling that can be used to reset the VM to its initial state, the way it was when it was first installed:

1. Reboot the system and select "SyConnect recovery" at the boot prompt.
2. When the login prompt appears, log in using username `syconnect`. Set a password. This password is temporary and is valid for this session only.
3. Run `sudo elemental reset --reset-persistent --reboot`
4. Wait for the reset process to complete. The system will automatically reboot when the process is complete.

4 System Overview

4.1 System Components

SyConnect is a containerized system that contains several components. The following are some of these components.

Service	Purpose
Queue	Handles all events in the system
Storage	Contains data for all services, such as input data and intermediate data
DicomReceiver	Receives DICOM data and stores it in Storage
RuleEngine	Responsible for providing rules to the WorkorderFactory
WorkorderFactory	Creates workorders based in incoming data
WorkorderRunner	Runs workorders serially
Symri Action	Processes DICOM data with SyMRI
DicomSender Action	Sends DICOM data
DicomFilter Action	Filters DICOM data

4.2 Workorders

SyConnect executes workorders that are defined by rules containing conditions and actions.

A workorder is created based on input conditions and contains a list of actions to run.

When SyConnect receives an input event (that may contain DICOM data for example), for each rule where all the conditions are met, it creates and executes a workorder with the defined actions.

A rule consists of a *name*, a set of *conditions* which all need to be met for the rule to be triggered, and a list of *actions* that is run, in the order they are listed, if the rule is triggered.

5 Configuration

The configuration of SyConnect is stored in YAML format and can be accessed via the Web UI or the `syconnectctl` tool.

5.1 Encryption of Sensitive Configuration Values

In the case TPM 2.0 or virtual TPM 2.0 (vTPM) is available for SyConnect, configuration values deemed sensitive, as passwords, will be encrypted. The rest of the configuration will be stored in clear-text.

Encryption will be done on startup and when the configuration is modified.

In the case a TPM is *not* available, no encryption of configuration values will be attempted by the system.

5.1.1 Encryption Scheme

The sensitive configuration values are encrypted using AES (Rijndael) with a 256 bit key in EAX mode. A random nonce is used during encryption. A MAC tag is generated in order to being able to verify data integrity and match between encryption key and encrypted value. The nonce, ciphertext and MAC tag are stored together as an *encrypted value*.

5.1.2 Working with Encrypted Configuration Values

Let's assume the configuration contain the following before encryption:

```
...
auth:
  secret: my-very-secret-password
  issuer: an-issuer
...
```

Listing 5.1: Configuration YAML example before encryption

The same section will look like something like the following after encryption of sensitive values:

```
...
auth:
  secret: Encrypted_0x01234567_0x0123456789abcdef_0x1234
  issuer: an-issuer
...
```

Listing 5.2: Configuration YAML example after encryption

The value `my-very-secret-password` was replaced with a text string beginning with `Encrypted`, representing its ciphertext. Values *not* deemed to be secret was kept unchanged.

While editing configuration, encrypted values may *not* be:

- Partly changed. This will invalidate it.
- Copied from configuration encrypted with a different data encryption key.

To change an encrypted value in configuration, simply replace it on whole with the new value in clear-text. The clear-text will be encrypted upon saving.

5.1.3 Export and Import

To import configuration with encrypted values, the master key of the instance from which the configuration was exported must first be set. The master key is stored in the TPM and is *not* part of the exported configuration. For this reason, it is important to keep track of the active master key of all SyConnect instances.

For more information about how to manage master keys see 6.6.1.

5.2 DICOM Receiver

DicomReceiver is the service responsible for receiving DICOM studies that are sent to SyConnect.

The config can be found under the *dicomReceivers* key. Multiple DicomReceivers can be configured, each with a unique port and name. The following example shows a config for a DicomReceiver named *myDicomReceiver*.

```
dicomReceivers:
  myDicomReceiver:
    callingAeTitleAllowlist: null          # Set to null to accept all.
    calledAeTitleAllowlist:
    - AE1
    - AE2
    studyCompletedThresholdSeconds: 300
    port: 104
```

Listing 5.3: DICOM receiver config

The *studyCompletedThresholdSeconds* setting is used to determine when a complete study has been received. When the configured amount of seconds have passed since the latest DICOM instance for a study was received, the study will be considered complete and will be matched against the defined rules.

5.3 Actions

Actions can be specified to run when a rule is triggered. They are run in series and when one action is done, the next action is started. Outputs from previous actions can be used as inputs to later actions. Each action can be configured with presets, and the preset name is used in the rules to specify a certain action configuration.

5.3.1 SyMRI Action

The SyMRI Action is used to process DICOM series with SyMRI and the config can be found under the *symriAction* key.

Images that SyMRI can create can be defined under the *images* key. The example config contains some already defined images, but they can be customized and new ones can be added by the user. Multiple images can be grouped together under the *layouts* key and multiple layouts can be selected for each preset.

To accommodate for different population groups, *referenceCurveDatumId* can be set to 0 or 1 to affect structured report and reference curve graphs. See SyMRI user manual for more information. This feature will only have an effect when using SyMRI 11.3.11, SyMRI 12.1.11 or later versions.

```
actions:
  symriAction:
    licenseServerFqdn: symri-licenseserver.syconnect.internal
    licenseServerPort: 4242

    symriInstances:
    - version: 15.0.19

    presets:
      mySymriPreset:                  # Preset name
        layouts:                      # List of layouts
        - myDefaultContrasts
        saveSymaps: false
        saveStructuredReport: false
        symriExtraOptions: ''
        symriTimeoutSeconds: 300
        referenceCurveDatumId: 0

    layouts:
      myDefaultContrasts:             # Layout name
        images:
        - myT1W

    images:
      myT1W:                          # Image name
        echoTime: 10
        repetitionTime: 650
        inversionTime: 0
        doubleInversionTime: 0
        icvEdge: false
        color: false
        background: true
        psir: false
        inversion: false
        doubleInversion: false
        type: Contrast
        windowingCenter: null
        windowingWidth: null
        orientation: null
        guidelines: false
```

Listing 5.4: SyMRI config example

Image keys:

- *background*: Show contrast image behind overlay.
- *type*: Image type, possible values are:
  - *Contrast*: Regular contrast image
  - *WM*: White matter segmentation overlay
  - *GM*: Gray matter segmentation overlay
  - *CSF*: Cerebrospinal segmentation overlay
  - *MY*: Myelin segmentation overlay
  - *NON*: Non-WM/GM/CSF segmentation overlay
  - *SegmentationTable*: Segmentation table
  - *QTable*: Quantification table
  - *BPFPlot*: BPF (BPV / ICV) reference curve
  - *MYFPlot*: MyCPF (MyC / BPV) reference curve

  - *ICVPlot*: ICV reference curve
  - *BPVPlot*: BPV reference curve
  - *CSFVPlot*: CSF reference curve
  - *MYVPlot*: MY reference curve
  - *R1*: R1 parametric map
  - *R2*: R2 parametric map
  - *T1*: T1 parametric map
  - *T2*: T2 parametric map
  - *PD*: PD parametric map

- *windowingCenter/windowingWidth*: Windowing parameters, remove or set to *null* to use autoscaling.
- *orientation*: Reformatting orientation. Can be *AX*, *SAG* or *COR*. Remove or set to *null* to use acquisition orientation.
- *guidelines*: Show orientation guidelines.

`Note:` *Some of the keys may not be available, depending on which SyMRI licenses/versions are installed*

The *symriInstances* key configures which version(s) of SyMRI that should be available in SyConnect. Currently supported versions are:

- 11.3.11
- 12.1.11
- 15.0.8
- 15.0.14
- 15.0.19
- 315.0.19
- 0.61.0 (15.0 Beta 1)

5.3.2 cMRI Action

The cMRI Action provides fully automated brain MRI quantification. To be able to use the cMRI Action it must first be enabled by a SyntheticMR representative.

It is recommended to use a processor with 16 cores as it will allow to run the algorithms in a single pass. It is possible to run the processing with even less cores (8 minimum), but it will add some minutes to the processing time. The cMRI Action memory requirements are 24 GB (recommended), 16 GB (minimum).

Requirements for the input data:

- Brain MRI scan
- Basic requirements
  - Images must be acquired with 1.5T or 3.0T scanner
  - Image volumes should cover the whole head
  - Recommended to acquire images in the sagittal or axial plane
- Mandatory sequence: 3D T1W gradient echo (GE)
  - In-plane resolution: 1 x 1 mm (rejected if >1.2 mm)
  - Slice thickness: 1.2 mm or less (rejected if >1.3 mm)
- Optional sequence: T2-FLAIR turbo spin echo (TSE)
  - 3D FLAIR recommended
  - Limited support for 2D FLAIR (no support for longitudinal with 2D images)
- Other
  - Limited support for contrast imaging (only lesions reported)

Processing times can change depending on the input image size and if there are two time points. Typical processing time 20 min, max processing time 60 min. The config key *actionTimeoutInSeconds* must be set high enough to accommodate the processing time.

The action config can be found under the *cmriAction* key.

```
actions:
  cmriAction:
    cmriTimeoutSeconds: 1800

    cmriInstances:
    - version: 2.3.6-7

    presets:
      myCmriActionPreset:
        region: EU
        reportLanguage: en-GB
        reportDicomFormat: EncapsulatedPdf
        secondaryCaptureTransferSyntax: RLELossless
        reportHidePatientNameId: false
        outputOrientationT1: Native
        outputOrientationFlair: Native
        reportingDomains:
        - Dementia
        - MS
        - TBI
        - Epilepsy
        - Parkinson
        - Brainhealth
        - Atrophy_lesions
        reportModality: DOC
```

Listing 5.5: cMRI config example

Configuration keys:

- *cmriInstances*: Configures which version(s) of cMRI that should be available in SyConnect. Currently supported versions are:
  - 2.3.6-7
- *region*: EU or US. Based on the quantified images, cMRI estimate three visual scores (MTA, GCA and Fazekas) that are widely used in the EU. The estimates are called computed MTA (cMTA), computed GCA (cGCA) and computed Fazekas (cFazekas). In the US region, instead of the computed MTA and GCA values, cMRI provides z-scored values of them called hippocampal atrophy index (HAI) and the cortical atrophy index (CAI). White matter hyperintensities are only reported as volumes in the US.
- *reportLanguage*: Possible values: da-DK, de-DE, en-GB, es-ES, fi-FI, fr-FR, it-IT, sv-SE.
- *reportDicomFormat*: EncapsulatedPdf or SecondaryCapture.
- *secondaryCaptureTransferSyntax*: RLELossless (TransferSyntaxUID: 1.2.840.10008.1.2.5)
- *reportHidePatientNameId*: Set to 'true' to hide patient name and patient id.
- *outputOrientationT1, outputOrientationFlair*: Determines the orientation in which the segmentation DICOMs are generated. The parameters are available for both T1 and FLAIR segmentations. The re-oriented DICOMs from originals will be produced if using any other than native orientation. Possible values:
  - *Native*: Native (original) orientation
  - *Sagittal, Coronal, Axial*: Re-oriented in respective orientation
  - *SagittalACPC, CoronalACPC, AxialACPC*: Image aligned with AC-PC plane in respective orientation
- *reportModality*: Which modality to save the report as, e.g. DOC or MR.

5.3.3 DicomSender Action

The DicomSender Action is used to send DICOM instances to a C-STORE SCP and the config can be found under the *dicomSenderAction* key. IP/hostname, port, CallingAeTitle and CalledAeTitle can be specified for each preset.

```
actions:
  dicomSenderAction:
    presets:
      myDicomSenderPreset:
        fqdn: 192.0.2.1                # Remote server IP/hostname
        port: 104                      # Remote server port
        callingAeTitle: SyConnect
        calledAeTitle: archive
```

Listing 5.6: DicomSender config example

5.3.4 DicomFilter Action

The DicomFilter Action is used to filter DICOM files and the config can be found under the *dicomFilterAction* key. The config consists of a list of rules similar to those in 5.4 Rules. The rules are evaluated in order for each file and the first matching rule is applied to the series that the file belongs to. If no rule matches, the series is kept.

Possible values for the *filter* key are: *keep* and *remove*.

```
actions:
  dicomFilterAction:
    presets:
      myDicomFilterPreset:
        rules:
        - filter: keep
          tagPath: (0008,103E)
          comparator: match
          value: MDME
          type: string
        - filter: remove
          tagPath: (0008,103E)
          comparator: match
          value: .*
          type: string
```

Listing 5.7: DicomFilter config example

5.3.5 DownloadArea Action

The DownloadArea action is used to temporarily store files and make them available for download using the Web UI. The configuration allows for creating multiple named areas, with individual access permissions and retention times.

After an area has been configured for use, the DownloadArea Action can be configured as part of a workflow using presets, and store the files that it gets as inputs.

```
rules:
- name: Store SyMRI output in Download Area
  conditions:
    metadata: []
  actions:
  - name: Run SyMRI
    type: symri.15.0.19.action
    input:
    - workorderinput
    config:
      preset: mySymriPreset
  - name: Store in Download Area
    type: downloadarea.action
    input:
    - Run SyMRI
    config:
      preset: myDownloadAreaPreset
```

Listing 5.8: DownloadArea rule example

In the example below, an area named “My Area” is defined, accessible to all administrators, and with a retention policy of 72 hours. The provided description is visible to the user on the Web UI.

```
actions:
  downloadAreaAction:
    downloadLimitInGiB: 1
    areas:
      My Area:
        access: [Admin]
        retentionTimeInHours: 72
        description: Some extra information about the content stored
    presets:
      myDownloadAreaPreset:
        areaName: My Area
        fileNameRegexes:
        - .*\\.pdf
```

Listing 5.9: DownloadArea config example

- Area config:
  - *access*: List of user-roles (User, Admin) that should have access to the files.
  - *retentionTimeInHours*: For how long stored files should be retained before they are automatically removed.
  - *description*: A text description that are shown to the users on the download page.
- Preset config:
  - *areaName*: The name of the download area the files should be stored in.
  - *fileNameRegexes*: A list of regular expressions that are matched against the file name. *null* can be used to store all files. It is enough that one of the regular expressions in the list matches the file's name for it to be included.
- General config:
  - *downloadLimitInGiB*: The size limit when downloading all files in an area or entry.

5.3.6 ReportGenerator Action

The ReportGenerator Action produces a Quantitative Neuro Report from DICOM files, and the default configurations are provided with a preset for this purpose. Output from SyMRI are used as input to this action. It can only be used with SyMRI 11.3.11/12.1.11 or newer. The report can be saved as Encapsulated PDF and/or Secondary Capture. If saved as Secondary Capture, the Transfer Syntax can also be configured.

```
rules:
- name: Generate report
  conditions:
    metadata:
    - key: callingAeTitle
    value: Modality1
    comparator: equal
    type: string
actions:
- name: Run SyMRI
  type: symri.15.0.19.action
  input:
  - workorderinput
  config:
    preset: reportInputPreset
- name: Generate report
  type: reportgenerator.action
  input:
  - Run SyMRI
  config:
    preset: myReportGeneratorPreset
- name: Send to PACS
  type: dicomsender.action
  input:
  - Generate report
  config:
    preset: myDicomSenderPreset
```

Listing 5.10: ReportGenerator Action example

```
actions:
  reportGeneratorAction:
    presets:
      myReportGeneratorPreset:
        saveAsEncapsulatedPdf: true
        saveAsSecondaryCapture: false
        secondaryCaptureTransferSyntax: Jpeg2000Lossless
        language: en-US
        longitudinalHiddenSections: []
        longitudinalSubtitle: ''
```

Listing 5.11: ReportGenerator config example

- *secondaryCaptureTransferSyntax*: Possible values:
  - *Jpeg2000Lossless*: UID: 1.2.840.10008.1.2.4.90
  - *JpegSv1Lossless*: UID: 1.2.840.10008.1.2.4.70
  - *ExplicitVrLittleEndian*: UID: 1.2.840.10008.1.2.1
- *language*: Possible values: en-US, bg-BG, cs-CZ, da-DK, de-DE, el-GR, es-ES, et-EE, fi-FI, fr-FR, hr-HR, hu-HU, it-IT, ja-JP, ko-KR, lt-LT, lv-LV, nb-NO, nl-NL, pt-BR, pt-PT, ro-RO, sk-SK, sv-SE, tr-TR, zh-CN.
- *longitudinalHiddenSections*: List of sections to exclude in the Longitudinal report. Possible values: ComparisonHistory, ComparisonPrevious, ExcludedStudies, Guidelines, ReferenceCurves, ReferenceValues, ReportSettings, ScannerSettings.
- *longitudinalSubtitle*: Custom subtitle for the Longitudinal report.

5.3.7 Longitudinal Action

The Longitudinal Action can be used to create a Longitudinal report that contains volumetric data from multiple studies. When a study is processed by the Longitudinal Action some information is stored encrypted on the SyConnect server. This information includes: patient information(name, id, sex, birthdate and age), study information(accession nr, date/time, instance UID), scanner information(model, protocol name, sequence parameters etc). The information is encrypted at rest using AES with a 256-bit key.

`Note:` *Even though the longitudinal information is always encrypted at rest, TPM (see 6.6 Encryption) must be enabled to also secure the encryption key.*

To use the Longitudinal Action it must first be enabled in the SyConnect license. Contact a SyntheticMR representative to do so. Then it must also be enabled in the config and SyConnect must be restarted.

To manage the stored longitudinal data, go to the web UI, `Administration`, `Longitudinal`. There it is possible to query all data for a specific patient, using the Patient ID. Please note that the Patient ID must be an exact match for the query to succeed. Each study can be manually disabled to exclude it from the report. The stored data can't be modified, but it can be overwritten and updated by sending the same study again to SyConnect and processing it with the Longitudinal Action. It is possible to delete the data of a single patient and all patients.

```
rules:
- name: Create Longitudinal report and send to PACS
  conditions:
    metadata: []
  actions:
  - name: Run SyMRI
    type: symri.15.0.19.action
    input:
    - workorderinput
    config:
      preset: longitudinalReportInputPreset
  - name: Longitudinal
    type: longitudinal.action
    input:
    - Run SyMRI
    config:
      preset: myLongitudinalPreset
  - name: Generate report
    type: reportgenerator.action
    input:
      - Longitudinal
    config:
      preset: myReportGeneratorPreset
  - name: Send to PACS
    type: dicomsender.action
    input:
    - Generate report
    config:
      preset: myDicomSenderPreset
```

Listing 5.12: Longitudinal Action example

```
actions:
  longitudinalAction:
    enabled: true
    presets:
      myLongitudinalPreset:
        filterStudyCount: 0
        filterStudyWindowYears: 0
        filterStudyDateOfBirth: true
        filterStudyVersion: true
        filterEnabledValues: null
        referenceCurveDatumId: null
        referenceCurveConfig:
          scaleModeX: Symri
          scaleModeY: Symri
          symriScaleX: Scale90Years
          symriScaleY: Medium
          dynamicScalePaddingX:
            left: 5
            right: 5
          dynamicScalePaddingY:
            up: 5
            down: 5
          fixedScaleX:
            min: 0
            max: 80
          fixedScaleY:
            min: 0
            max: 100
          unitX: Years
          showUnitX: true
          showUnitY: true
          heading: Value
          language: en-US
```

Listing 5.13: Longitudinal config example

- *enabled*: Set to *true* to enable the Longitudinal feature. This will store encrypted patient data on the SyConnect server.

- *filterStudyCount*: Maximum count of studies to include in the report, set to *0* to disable the filter.

- *filterStudyWindowYears*: Size in years of the window around the current study, studies within the window are included in the report. Set to *0* to disable the filter. Decimal values are allowed.

- *filterStudyDateOfBirth*: This option should be set to *true* for all normal uses. Set to *false* to include studies that has a different date of birth compared to the current study. This should only be done for research data where anonymization can cause the date of birth to vary.

- *filterStudyVersion*: This option should be set to *true* for all normal uses. Set to *false* to include studies processed with non-compatible SyMRI versions. This should only be done in research contexts where SyMRI cross version use is important.

- *filterEnabledValues*: List of volumetric values to include in the report. Set to *null* to include all. Possible values: Bpf, MyCpf, MyC, Csf, Bpv, Icv, Gm, Gmpf, Wm, Wmpf, Csff.

- *referenceCurveDatumId*: Which dataset to use for the reference curves. Set to *null* to use the same as the current study.

- *scaleModeX* and *scaleModeY*: Controls how the reference curves should be scaled. Possible values:

  - *Symri*: Similar scaling as SyMRI. Use *symriScaleX* and *symriScaleY* to control the scaling.
  - *Dynamic*: Changes the scaling according to the maximum/minimum values of the included studies. Use *dynamicScalePaddingX* and *dynamicScalePaddingY* to control the padding.
  - *Fixed*: Fixed scaling. Use *fixedScaleX* and *fixedScaleY* to control the scaling.

- *symriScaleX*: Scales the x-axis in 3 different ranges, 0-4 years, 0-20 years and 0-90 years. Possible values: Scale4Years, Scale20Years and Scale90Years.

- *symriScaleY*: Possible values: Small, Medium and Large.

- *dynamicScalePaddingX*: Sets the horizontal padding, the unit is the same as *unitX*.

- *dynamicScalePaddingY*: Sets the vertical padding in percent.

- *fixedScaleX*: Sets the horizontal fixed scaling, the unit is the same as *unitX*.

- *fixedScaleY*: Sets the vertical fixed scaling in percent.

- *unitX*: Unit of x-axis. Possible values: Days, Weeks, Months, Years.

- *showUnitX*: Toggle display of x-axis unit.

- *showUnitY*: Toggle display of y-axis unit.

- *heading*: Reference curve heading. Possible values:
  - *Value*: Show the value of the current study.
  - *Type*: Show the full name of the volumetric type.
- *language*: Language in reference curves. Possible values: en-US, bg-BG, cs-CZ, da-DK, de-DE, el-GR, es-ES, et-EE, fi-FI, fr-FR, hr-HR, hu-HU, it-IT, ja-JP, ko-KR, lt-LT, lv-LV, nb-NO, nl-NL, pt-BR, pt-PT, ro-RO, sk-SK, sv-SE, tr-TR, zh-CN.

5.4 Rules

The workorder rules are defined under the *rules* key.

The following shows how to define a rule which is triggered when a study is sent to SyConnect from an Application Entity named *Modality1*. The rule first filters the data using the preset *myDicomFilterPreset* and then runs SyMRI 15.0.19 using the preset *mySymriPreset*. It will then send the output data from SyMRI to the DICOM server defined in the preset *myDicomSenderPreset*.

```
rules:
- name: Run SyMRI and send data to PACS
  conditions:
    metadata:
    - key: callingAeTitle
      value: Modality1
      comparator: equal
      type: string
  actions:
  - name: Filter data
    type: dicomfilter.action
    input:
    - workorderinput
    config:
      preset: myDicomFilterPreset
  - name: Run SyMRI
    type: symri.15.0.19.action
    input:
    - Filter data
    config:
      preset: mySymriPreset
  - name: Send to PACS
    type: dicomsender.action
    input:
    - Run SyMRI
    config:
      preset: myDicomSenderPreset
```

Listing 5.14: Rule example

To let the output of an action be the input to another action, use the name of the action for the *input* key, as shown above. The name *workorderinput* means the study that triggered the rule.

SyConnect evaluates conditions using a comparator. The comparator is defined with the key *comparator* and the right-hand operand is defined in *value*. The left-hand value is the value fetched from either the metadata or dicom tag.

It can be viewed as *<left-hand-value> <comparator> <right-hand-value>*, for example *3 lessThan 4*, where 3 is fetched from whatever value was requested in the rule, and 4 is taken from the value tag in the rule.

Supported comparators are:

equal: Checks if the operands are equal

match: Checks if string from input matches the regex pattern in *value*. Only available for strings. Uses the .NET regular expression engine. Expressions can be tested at https://regex101.com/.

lessThan: Checks if the left-hand operand is less than the right-hand operand

lessThanOrEqual: Checks if the left-hand operand is less than or equal to the right-hand operand

greaterThan: Checks if the left-hand operand is greater than the right-hand operand

greaterThanOrEqual: Checks if the left-hand operand is greater than or equal to the right-hand operand

Supported values for the *type* key are: *string*, *number*, *date*, *time* and *dateTime*.

The types *date*, *time* and *dateTime* must be specified according to the DICOM standards.

In short, *date*: YYYYMMDD, *time*: HHMMSS and *dateTime*: YYYYMMDDHHMMSS.

Conditions can inspect different types of input data and can be mixed in the same rule. Supported conditions are:

metadata: Gets the string input from stored metadata. Keys:

key: Name of metadata key, e.g. callingAeTitle or calledAeTitle

dicom: Gets the string input from stored dicom files. The condition is true if at least one dicom file matches all the tags. Keys:

tagPath: Specifies the tag using the format (group,element), e.g. (0008,103E). Tags in sequences can be specified using the format (group,element) [itemposition] (group,element), e.g. (0008,1111) [1] (0008,1150) which gets the tag (0008,1150) from the first item in sequence (0008,1111). The tag path can be used to get nested tags in any level.

To define a rule that is always triggered for every study, use an empty metadata or dicom condition, i.e. "metadata: []" or "dicom: []".

The following rule is triggered if the SeriesDescription contains the string *SyMRI* and the magnetic field strength is *3* for at least one of the DICOM series in the study.

```
rules:
- name: Send data to PACS
  conditions:
    dicom:
    - tagPath: (0008,103E)
      comparator: match
      value: SyMRI
      type: string
    - tagPath: (0018,0087)
      comparator: equal
      value: "3"
      type: number
  actions:
  - name: Send to PACS
```

```
    type: dicomsender.action
    input:
    - workorderinput
    config:
      preset: myDicomSenderPreset
```

Listing 5.15: Rule with DICOM condition

5.5 CA Certificates

Extra CA certificates which should be trusted may be placed in the directory */etc/syntheticmr/syconnect/extra_certificates*. These certificates will then be used for TLS verification when making external requests, such as to an LDAP server for authentication, in addition to the default CA bundle. The extra certificates must be in PEM format and have the extension `.crt`.

5.6 Authentication

One or more user authentication providers may be configured to allow users access to the SyConnect Portal. When a user attempts to log in an authentication attempt will be made against each provider in the order specified in the configuration.

5.6.1 Configuration File Based Users

```
auth:
  identificationBackends:
  - type: local
```

Listing 5.16: Example of local authentication provider configuration

Please see 3 Installation Steps for instructions on how to create new configuration file based users.

5.6.2 LDAP

One or more LDAP servers may be configured to authenticate and authorize users. Note that the SyConnect LDAP integration is strictly read-only, and the SyConnect administration tools do not support creating or modifying users.

The LDAP client will not perform referral chasing. As such, the system must be configured to communicate directly with the LDAP server that will be performing the authentication.

5.6.2.1 Certificate Management

To disable LDAP TLS certificate validation, set *no_validate_ldap_cert* to *true* under the *package* key and then restart SyConnect.

If your LDAP server uses a self-signed certificate please see 5.5 CA Certificates for configuration of certificate trust.

5.6.2.2 Provider Configuration

```
auth:
  identificationBackends:
  - type: ldap
    serverName: MyLdapServer
    host: ldap.example.com
    port: 389
    tlsMode: StartTls
    searchBaseUserDn: "CN=Users,DC=example,DC=com"
    searchUserDn: "CN=SyConnectUserReader,CN=Users,DC=example,DC=com"
    searchUserPassword: SyConnectUserPassword
    searchUserFilter: "(sAMAccountName=%s)"
    groupSearchFilterUserAttribute: "dn"
    groupSearchFilter: "(member:1.2.840.113556.1.4.1941:=%s)"
    groupSearchBaseDn: "OU=groups,DC=example,DC=com"
    roleMapping:
      Admin: "CN=SyConnectAdministrators,OU=groups,DC=example,DC=com"
      User: "*"
    attributes:
      memberOf: "memberOf"
      username: "sAMAccountName"
```

Listing 5.17: Example of LDAP configuration

type: This must always be set to *ldap*.

serverName: Arbitrary label for a specific LDAP server.

host: Host of the LDAP server. LDAP scheme must *not* be included.

port: Port number of the LDAP server. By default will use *389*.

tlsMode: TLS variant to use. Valid values are *None*, *StartTls* or *Ssl*. By default will use *None*.

searchBaseUserDn: Base DN to search for users.

searchUserDn: DN of user to be used for searching. If an expression can be provided which may match all possible users, a placeholder (%s) may be used in the style of *CN=%s,CN=Users,DC=example,DC=com*, where the username of the user attempting to login will replace the placeholder. This allows for logging in using a single bind operation, and removes the necessity to set up a search user. Providing *searchUserPassword* will then not be necessary, but the user logging in must have the necessary permissions to query *searchBaseUserDn*, as well as *groupSearchBaseDn*, if provided.

searchUserPassword: Password of user to be used for searching. Not required if *searchUserDn* is specified with a placeholder.

searchUserFilter: Query filter with placeholder (%s) to match against a username.

groupSearchFilterUserAttribute: The attribute of the user to be used when querying for group memberships. By default will use *dn*.

groupSearchFilter: Query filter with placeholder (%s) to search for group memberships. Placeholder will be replaced with the value of the *groupSearch-*

FilterUserAttribute attribute of the user. If not specified group memberships will instead be determined by checking for the *memberOf* attribute of the user.

groupSearchBaseDn: Base DN to search for groups. If not specified, will reuse *searchBaseUserDn*. Not required if *groupSearchFilter* is not specified.

roleMapping: Map SyConnect roles to LDAP groups. A wildcard * may be specified to assign a role to any user which successfully binds, regardless of group memberships.

attributes: Map user attribute names

username: Attribute to use as username within SyConnect. By default will use *sAMAccountName*

memberOf: Attribute to check for group memberships. By default will use *memberOf*. Not required if *groupSearchFilter* is specified.

5.6.3 Token Configuration

After authenticating the user will be provided with an authentication token, which will automatically be passed when making further requests to the SyConnect Portal. Configuration is generated on install, but may under some circumstances need to be changed.

```
auth:
  secret:
    8zzGvJzp0Xjp93sa4mGxrH0JHC1iIAanRglKp89gYPm7rjJsFBJPsCYre2pPMuvy
  issuer: https://syconnect.example.com
  audience: SyConnect
  jwtClockSkewToleranceInSeconds: 60
```

Listing 5.18: Example of authentication token configuration

secret: Text string which will be used to sign and verify that authentication tokens are authentic. This is highly sensitive, and should be changed immediately if it becomes known non-authorized parties have had access to it. Note that changing it will cause any currently logged in users to be logged out. This should be set to a randomly generated 64 character string containing numbers and upper- and lowercase letters. By default a sufficiently secure secret will be generated during installation.

issuer: The address where the tokens are issued from. This should match the domain at which SyConnect is located, and should be changed if the domain is changed. Note that changing it will cause any currently logged in users to be logged out. By default will be set to *https://<virtualhost>*, where virtualhost is the option set during installation.

audience: Name of the system intended to read the authentication token. This should in almost all circumstances be set to *SyConnect*, which is also the default value.

jwtClockSkewToleranceInSeconds: This option may be set if the server hosting SyConnect is known to have issues with clock drift, which may cause issues with authentication token validation. This will generally not need to be set, and by default it set to *0*.

5.7 Automatic Upgrades

The system can be set to automatically upgrade SyConnect, the operating system and other installed packages once per day. If necessary, the system will reboot when the upgrade is complete. As such it is heavily recommended to perform the upgrade when the system is not in use.

The specified upgrade time will run in the time zone configured for the system. See 6.9 Time Zone for more details. The upgrade procedure will start at the designated time but may take longer if the download speed of new assets is slow. In a worst case scenario, the upgrade procedure can take up to 4 hours.

`Note:` *Configuration of automatic upgrades is only applied when syconnectd starts, and will have to be restarted in order to apply configuration changes.*

```
automaticUpgrades:
  enabled: true
  runUpgradesAt: "03:00"
```

Listing 5.19: Example of automatic upgrades configuration

enabled: Whether automatic upgrades are enabled at all. Defaults to *true*.

runUpgradesAt: The time at which to run upgrades. Should be formatted as *"HH:SS"* using 24-hour notation. Note that this is the time when available upgrades will be checked, downloaded, and installed. Note that a random delay of up to five minutes will be added, to avoid traffic congestion. Defaults to *"03:00"*

5.8 Firewall

The system will by default set up a firewall to only allow incoming traffic on necessary ports. This includes SSH, if enabled, as well as HTTP (port 80), HTTPS (port 443), as well as any ports configured for DICOM receivers. See 5.2 DICOM Receiver for details.

```
firewall:
  enabled: true
  allow_ssh: true
```

Listing 5.20: Example of firewall configuration

5.9 Storage

A minimum free disk space resource limitation can be set to prevent the disk from filling up. The size is expressed as whole number of GiB. It is also possible to configure how long temporary data is stored, the default is 24 hours.

```
package:
  storage:
    minimumFreeDiskSizeInGiB: 6

storageCustodian:
  storageRetentionTimeInHours: 24
```

Listing 5.21: Example of storage configuration

5.10 Workorder Log

The Accession Number can be shown in the Workorders page by configuring the settings. It is disabled by default and can be enabled by an administrator.

```
workorderLog:
  accessionNumber:
    capture: true
    displayForRoles: [Admin, User]
```

Listing 5.22: Example of workorder log configuration

capture: Set to *true* to capture the Accession Number of received datasets in SyConnect. Does not affect already received datasets. Note that the Accession Number is stored unencrypted. Defaults to *false*.

displayForRoles: The user roles which should be able to see the Accession Number. Defaults to an empty list *[]*.

6 System Administration

6.1 System Image

SyConnect uses static system images to deliver its operating system. These images are stored as file on disk. There are three image slots, one for each of the active, passive and recovery images.

The active image holds the current version of SyConnect. Should the active image fail to boot, the passive image is attempted instead. The recovery image is used for recovery operations, such as to Reset the system.

When the system image is upgraded, the current active image becomes passive and a new active image is written to disk. The system must be rebooted for the new image to become active.

An upgrade of the system image replaces the entire system image. Interactive customization of the system is not possible, as such changes are overwritten by the upgrade process. Customization is instead done using cloud-init style configuration files. To reflect their static nature, the system images are mounted read-only.

The system and its packages are kept up-to-date by periodically updating the system image.

6.2 Active and Passive Mode

The active image is preferred and is the pre-selected boot choice unless it has failed a boot assessment. A boot assessment is initiated by the bootloader and completed by `elemental-boot-assessment.service`. If the boot sequence reaches this service, the boot assessment pass.

Boot assessments are performed following an upgrade, install or reset of a system image. Assessments are then performed each boot until the active image successfully completes an assessment.

If the boot assessment fails, the passive image is selected. If no passive image is available, the recovery image is selected. Following a successful boot of one of these images, the active image is attempted again next boot.

The currently running image is never replaced. In case the active image fails its boot assessment, the passive image can safely be used to upgrade the active image.

To determine what image is currently running, see the message at the login prompt or run `cat /etc/issue`.

6.3 cloud-init

The system can be customized by placing cloud-init style configuration files under `/oem`. Configuration is applied in lexicographical order. Configuration expressed this way persists the system image upgrade process as it is applied every time the system boots.

Example configuration:

```
name: Set NTP configuration
stages:
  network:
    - name: Set NTP configuration
      files:
        - path: /etc/systemd/timesyncd.conf
          content: |
            [Time]
            NTP=0.ntp.corp.org 1.ntp.corp.org
          permissions: 0644
      commands:
        - systemctl restart systemd-timesyncd
```

Listing 6.1: Set NTP configuration

To apply the above example:

1. Edit the configuration using `sudo nano /oem/90_ntp.yaml` and input the configuration. Note that the file ending must be `.yaml`.
2. Test the configuration by running `sudo elemental cloud-init --stage network /oem/90_ntp.yaml`.

Examples of cloud-init style configuration files can be found in `/examples/oem/` in the filesystem of the instance.

Elemental toolkit, which provides the cloud-init style customization capability, is a 3rd party component developed by SUSE LLC. Advanced documentation on the configuration:

1. https://rancher.github.io/elemental-toolkit/docs/customizing/stages/
2. https://rancher.github.io/elemental-toolkit/docs/reference/cloud_init/

6.4 Network Configuration

The appliance is configured to use DHCP by default. If needed, the default configuration can be overridden by placing cloud-init style configuration files in the directory `/oem/`.

Recommended steps for overriding the default network configuration:

1. Look in the directory `/examples/oem/` for a file that best represents the desired network configuration.

   For example `/examples/oem/10_network.static_ip.yaml`.

2. Create or edit the file `/oem/10_network.yaml`.

   If the file does not exist already, it can be copied directly from the directory `/examples/oem/`. The initial `10_` of the file name *is* significant as it determines the file's place in the sequence of config files to be processed. The rest of the filename is *not* significant. We do however recommend that the filename reflects its purpose and content.

3. Use the selected example file as starting point. Edit the content-section to suit the needs at hand. Make extra note of the text's indentation, since both the cloud-init file and the netplan definition uses YAML as its configuration format.

4. To apply the changes, run:

   ```
   sudo elemental cloud-init --stage initramfs /oem/10_network.yaml
   ```

   Alternatively, reboot the system.

More information about network configuration can be found here:

https://ubuntu.com/server/docs/network-configuration

6.4.1 HTTP Proxy

Active HTTP Proxy settings are configured using cloud-init style configuration.

1. Copy `/examples/oem/06_http_proxy.yaml` to `/oem/06_http_proxy.yaml`.
2. Edit `/oem/06_http_proxy.yaml` and specify the proxy's URL and port. The same values will need to be specified in multiple places in the file.
3. Reboot the system for the changes to take effect.

6.5 NTP

NTP settings are configured using cloud-init style configuration.

1. Copy `/examples/oem/90_ntp.yaml` to `/oem/90_ntp.yaml`.
2. Edit `/oem/90_ntp.yaml` and specify the correct URL.
3. Test the configuration by running `sudo elemental cloud-init --stage network /oem/90_ntp.yaml`. Check that the configuration had the desired effect using `timedatectl timesync-status`.

6.6 Encryption

In the case TPM 2.0 or virtual TPM 2.0 (vTPM) is available for SyConnect, certain information in the system will be encrypted. If TPM is *not* available for SyConnect, sensitive configuration values, as passwords, will be stored in clear-text on disk.

The information in this section is only relevant for SyConnect instances with TPM available.

6.6.1 Encryption Keys

The encryption *master key* is stored in the TPM; never on disk. The master key is used to encrypt a *data encryption key*, which in turn is used to encrypt secrets in the system. The data encryption key is stored encrypted on disk.

The encryption keys are generated by the TPM. The master key has a size of 128 bit, while the data encryption key size is 256 bit.

The data encryption key is encrypted using AES (Rijndael) with a 128 bit key in EAX mode. A random nonce is used during encryption. A MAC tag is generated in order to being able to verify the decryption of the value. The nonce, ciphertext and MAC tag are stored together on disk.

6.6.2 Master Key Access

In order to fetch the active master key of a SyConnect instance, use the following command: `syconnectctl secrets master-key`

In order to set the active master key of a SyConnect instance, use the following command: `syconnectctl secrets set-master-key [master-key]`

The encrypted configuration values will still be valid after changing the master key.

6.6.3 Key Rotation

In order to accommodate key rotation, a two slot scheme is used. For each slot, there is a master key and a data encryption key. One of the slots are *active* and the other one is *passive*.

The active slot is stored along with configuration on disk.

When a *master key rotation* is initiated, the system will perform the following steps:

- The data encryption key of the active slot is decrypted using the master key of the active slot.

- A new master key is generated and written to the passive slot.
- The decrypted active data encryption key is encrypted using the master key in the passive slot and written to the passive slot.
- The passive slot is made active by updating the configuration file.

To rotate master keys, use the following command:

```
syconnectctl secrets rotate-master-key
```

Make sure to fetch and store the new master key in a safe place.

When a *data encryption key rotation* is initiated, the system will perform the following steps:

- The master key of the active slot is copied to the passive slot.
- A new data encryption key is generated for the passive slot.
- The sensitive configuration values are decrypted using the active data encryption key, and encrypted using the passive data encryption key. At this step the passive slot is made active.

To rotate the data encryption key, issue the following command:

```
syconnectctl secrets rotate-data-key
```

A data encryption key rotation will *not* change the master key.

6.6.4 Master Key Tracking

It is important that system administrators keep track of the active master keys of all SyConnect instances. The active master keys should be stored in a safe place. See 6.6.2 for more information on how to access the active master key. The master key of a SyConnect instance may *never* be stored in the instances file system.

The active master key should be recorded in the following situations:

- While accepting or providing a master key during FTI.
- After running the `syconnectctl secrets rotate-master-key` command.
- After running the `syconnectctl secrets set-master-key` command.

The master key of a SyConnect instance will *not* change without administrator interaction.

6.7 General Service Commands

Command	Description
`syconnectctl start`	Start SyConnect service.
`syconnectctl stop`	Stop SyConnect service.
`syconnectctl restart`	Restart SyConnect service.
`syconnectctl status`	Show SyConnect status.
`syconnectctl update`	Update SyConnect.
`syconnectctl update-utils`	Update utilities such as Nomad.
`syconnectctl upgrade-system`	Upgrade system image.
`syconnectctl config validate`	Validate the configuration.
`syconnectctl config migrate`	Migrate the configuration to the latest compatible version.
`syconnectctl config export`	Export all configuration.

6.8 Nomad Commands

SyConnect uses Nomad as its container orchestration framework. Use the following commands to interact with it.

Command	Description
`syconnectctl diag nomad --`	Run nomad command

Find more information about the nomad command in the nomad CLI documentation.

6.9 Time Zone

By default the system will be configured using the UTC timezone. The time zone can be set using the web UI, `Administration`, `System`.

The time zone can also be configured by logging in using SSH, and set using the following commands:

Command	Description
`timedatectl list-timezones`	List available timezones.
`sudo timedatectl set-timezone [zone]`	Set system time zone to the specified zone.

6.10 System Logs

All log messages in the system are written to `systemd-journald`.

The most recent of SyConnect's modules logs can be accessed using the Web UI, `Administration`, `Diagnostics`.

`systemd-journald` is configured by file on disk. The default configuration is located at `/etc/systemd/journald.conf`. The default configuration is re-created on system start and can not be permanently modified.

Overrides to the default configuration making it suitable for use as part of SyConnect is located at `/etc/systemd/journald.conf.d/10-syconnect.conf`.

Custom overrides are possible by creating a file `/etc/systemd/journald.conf.d/20-custom.conf`. See the default configuration file for a list of available options, such as log retention time and size.

Any time configuration is changed, `systemd-journald` must be reloaded by running: `sudo systemctl force-reload systemd-journald`.

6.11 Systemd Services

The following list shows the systemd services created by SyConnect. Services that are run periodically has a corresponding timer unit.

- *syconnect-license-renew.service*: Renews the SyConnect license.
- *syconnect-license-renew.timer*: Runs daily at a random time.
- *syconnect-report-statistics.service*: Reports SyConnect statistics to SyntheticMR.
- *syconnect-report-statistics.timer*: Runs daily around 02:00 and 14:00.

- *syconnect-sbom-scan.service*: Creates the Software Bill of Materials list.
- *syconnect-upgrade.service*: Perform SyConnect core, utilities, and packages upgrades and operating system upgrade.
- *syconnect-upgrade.timer*: User configurable, runs daily around 03:00 by default.
- *syconnectd.service*: SyConnect daemon.
- *sysstat-log.service*: Logs a summary of the current state of the system.
- *sysstat-log.timer*: Runs every 10 minutes.

6.12 Data Sharing

A daily report of operational metrics is sent to SyntheticMR to improve the SyConnect product, provide quicker and better support, and to monitor compliance with terms and conditions for SyConnect use. The report contains statistics about Workorders and Actions, and can be seen in the Web UI as an Admin by browsing to `Administration` and selecting `Statistics`.

The *syconnect-upgrade.service*, sends a report to SyntheticMR when it runs. The report contains success/failure status and the cause of the failure.

6.13 Storage

The storage service saves data on the VM's logical data volume (`/dev/mapper/data-var`). The data directory can be found at path `/var/opt/syntheticmr/syconnect/storage/`.

6.13.1 Configure Resource Limits

To avoid filling up the disk, a minimum free disk space can be configured. See section 5.9 for configuration details.

When the limit is reached, the DICOM receivers will stop accepting data transfer and the system will stop processing workorders. See also section 7.10 for more information.

6.13.2 Calculate Needed Disk Size

For large datasets, high volume of cases, or long retention time, increased storage size might be needed. The below formula can be used to approximate the disk size required. For complex workflows an even wider margin is needed.

disk size $> 164GiB + 2.5 *$average study size$*$studies per hour$*$retention time

6.13.3 Extend the Disk

1. Expand the VMs disk in your virtualization solution.
2. Reboot the VM. The system will automatically expand to use the extra space during boot.

6.14 Air Gap

Running SyConnect in an air-gapped environment without access to the Internet is possible, but there are some things to keep in mind.

- While completing First Time Installation (FTI), the server must have access to the Internet. Only after the installation has completed can the server be air-gapped. This applies to both OVA and ISO installations.
- Automatic upgrades should be disabled, see 5.7 Automatic Upgrades.
- It is important to upgrade regularly to keep the system secure. Manual upgrades are recommended to be performed at least every six months. If the system isn't upgraded for one year, there is a risk of service interruptions in SyConnect due to expired internal certificates. Perform a manual upgrade by following these steps:
  1. Connect SyConnect to the Internet.
  2. Run `syconnectctl manage renew-license`.
  3. Run `syconnectctl statistics report`.
  4. Run `sudo systemctl start syconnect-upgrade.service`. This can take a while and might cause the system to reboot.
  5. Run `syconnectctl manage renew-license`.
- There might be recurring errors in the logs about failure to renew license and report statistics. These are expected when no internet access exist and can be safely ignored.

7 Troubleshooting

7.1 Log In

The appliance can be administered by logging in directly in the virtualization console, or using SSH. The default username is `syconnect`. The password for this user is selected during First Time Installation.

If First Time Installation has not yet been performed, the system will ask for a password for this user. This password is then used for subsequent logins. The password is changed once First Time Installation is performed.

7.2 Diagnostic Commands

To diagnose problems, first log in to the system. The system can then be inspected by using the following commands:

Run `syconnectctl status -v` or `syconnectctl status -vv` for detailed system status. Use these commands to find the allocation ids that might have problems. More information about these allocations can be found by running `syconnectctl diag nomad alloc status <allocation-id>` and `syconnectctl diag nomad alloc logs <allocation-id>`.

If options for the nomad call are required write the command as `syconnectctl diag nomad -- status -verbose syconnect` for example.

More commands can be found by running `syconnectctl diag nomad -- -help`.

7.3 Unable to Import SyConnect OVA

For a few virtualization environments, some minor modifications to the OVA might be necessary to successfully import it.

When importing, if there is a problem with `StorageControllers` and `PIIX4` these sections can be modified.

1. Extract the OVA file using for example 7zip and it should produce two files, syconnect.ovf and syconnect.vmdk.
2. Open the .ovf file with your favorite editor.
3. Remove the lines containing: `<rasd:ResourceSubType>PIIX4</rasd:ResourceSubType>`
4. Remove the entire section beginning with `<StorageControllers>` and ending with `</StorageControllers>`

5. Try to import using these modified .ovf and .vmdk files.

7.4 Unable to Reach SyConnect Appliance

If the SyConnect Appliance is unreachable, verify that the network settings are appropriate for your virtual environment. See section 6.4 Network Configuration for more information.

7.5 Unable to Access Internet

If the SyConnect Appliance is unable to connect to the Internet, verify that the network settings, see 6.4 Network Configuration, are appropriate for your virtual environment. Specifically, routing and DNS.

If your LAN uses a HTTP Proxy for Internet access, see 6.4.1 HTTP Proxy for details on that configuration.

7.6 Docker Subnet Configuration

If the network environment is colliding with the default Docker subnet `172.17.0.0/16`, the First Time Installation and/or SyConnect may be unresponsive. Docker's default subnet can be changed by following these steps:

1. Log in to the system directly in the virtualization console, or using SSH.
2. Create/edit the docker configuration file by running:
   `sudo nano /etc/docker/daemon.json`
3. Enter the following in the text editor. Replace the subnet according to your network requirements.

```
{
  "default-address-pools":
  [
    {"base":"10.10.0.0/16","size":24}
  ]
}
```

Listing 7.1: daemon.json

4. If SyConnect is running, run:
   `syconnectctl stop`
5. Run and enter your credentials when requested:
   `sudo systemctl restart docker`
6. Run:
   `docker network prune -f`

7. If SyConnect was running, run:

   ```
   syconnectctl start
   ```

7.7 Access Logs

If the system is up and running, logs can be viewed in the Web UI as an Admin, by browsing to `Administration` and selecting `Diagnostics`.

If the web-UI is inaccessible, the SyConnect logs can be viewed via console/SSH by running `syconnectctl diag logs <module>`, and the available modules can be listed by running `syconnectctl diag modules`. For more help, see `syconnectctl diag logs --help`.

The systemd-based service logs can also be viewed by running `journalctl -u <service>`, and the available services can be listed by running `journalctl --field _SYSTEMD_UNIT | grep syconnect`. For additional use, see `man journalctl`.

The Docker-based service logs can also be viewed by running `docker logs <container>`, and the available containers can be listed by running `docker ps`.

7.8 SyConnect Is Not Updating

If you notice that SyConnect is not being updated, please contact a SyntheticMR representative.

The representative might provide a new Installation Token. This can be installed by browsing to `Administration` and selecting `System`. In the `Installation Token` section, input your installation token and press `Apply`.

7.9 Reset Web Admin User Password

The user password can be reset by running `syconnectctl users modify set-password <username> --password <new-password>`. The new password must be sufficiently strong, otherwise the command will fail. The users can be listed by running `syconnectctl users list`.

7.10 Insufficient Free Space

If the free storage space goes under *minimumFreeDiskSizeInGiB * 1.25*, the system event *InsufficientFreeSpaceSuspendOps* will be posted. When in this state, DICOM receivers will not accept further data transfer and the system will stop processing workorders. Should the free storage space go under *minimumFreeDiskSizeInGiB*, the system event *InsufficientFreeSpace* will be posted and SyConnect will stop storing new data. Once the free storage space goes over *minimumFreeDiskSizeInGiB * 1.5* the system event *SufficientFreeSpaceResumeOps* will be posted and SyConnect will return to normal operation. See also section 6.13 for more information.

7.11 Installing Extra Tools

The main filesystem is read-only and does not allow installation of extra tooling. A toolbox environment is available that allow installation of temporary tools that can be used for troubleshooting.

To start the toolbox, run the command `start-toolbox`. Enter `exit` to leave the toolbox.

The toolbox environment's filesystem is segmented off from the main filesystem. Only `/home` is shared.

Ubuntu packages can be installed using regular commands such as `apt update` and `apt install <package>`. All modifications done in the toolbox will be lost on exit. Hence, the toolbox should only be used to install temporary tools strictly used for troubleshooting. The toolbox comes equipped with a set of standard tools for network-, DICOM-, and LDAP-troubleshooting.

If an active HTTP proxy is used on the network, that need to be manually configured in the toolbox environment every time it is started.

SyMRI®

SyntheticMR AB

2026-01-13

SyConnect

SyntheticMR AB
Storgatan 11
SE-582 23 Linköping, SWEDEN
www.syntheticmr.com
support@syntheticmr.com

SyntheticMR