Table of Contents:

AWS AMI: Install Luminoso Daylight and Luminoso Compass Onsite

Background

Luminoso provides virtual appliances to run Luminoso Compass and Luminoso Daylight in clients' data center. Follow these instructions to install the virtual appliance so you can configure and use the product.

Launch a new instance from the AMI shared by Luminoso

Luminoso offers several methods for delivering Onsite images to clients. This document assumes you provided Luminoso with your AWS account number and that the AMI is shared with your account.

1. Log into your AWS Account and navigate to EC2. The EC2 Dashboard opens.
2. Under *Images* select **AMIs** and search for the AMI using the AMI ID that Luminoso provided.

3. Select the AMI that matches your build number and click **Launch** to open the Launch Wizard.
4. Choose an Instance Type. At minimum, Luminoso recommends an instance type that has at least 4 vCPUs and 16GiB of memory. If you select an instance type below this level, Luminoso functionality does not run properly.
5. Click **Next: Configure Instance Details.** The Step 3: Configure Instance Details page opens.
6. Use the options to configure your instance based on your company requirements.
7. Click **Add New Volume** to add and configure the data disk.
   ○ **For new installations,** change the size of the additional volume. Disk size depends on the number of projects processed. Your Luminoso Account Manager is responsible for communicating the recommended size of the data disk
     ■ Select "Delete on Termination" or "Encryption" based on your company requirements.
   ○ **For upgrades,** enter the Snapshot ID of the previous instances' data volume snapshot so the new system starts with a data volume based off that snapshot.
8. Click Next: Add Tags. Step 5: Add Tags opens.
9. Add tags as applicable to your organization. If you don't need tags, skip this step. Within AWS, tags allow you to place arbitrary labels on resources that help you report. If you have a tagging policy that says "every resource needs to have a tag" then you can see what resources everyone is using
10. Click Next: Configure Security Groups.
11. Configure security groups as required by your organization.
12. Click **Review and Launch**. The Review Instance Launch page opens.
13. Review the details and confirm that the settings you selected are correct.
14. Click Launch. A Select an existing key pair or create a new key pair window opens.
15. Select **Proceed without a key pair**. The Luminoso Daylight image is prepopulated with credentials that your CSM provides.
16. Click Launch Instances. Your instance begins the launch process.
17. For configuration steps, refer to the appropriate Luminoso Daylight or Compass Onsite product documentation.

Upgrade Procedure for AMI Deployment

1. Shut down the previous onsite VM.
2. Click Volumes and select the data volume of your old instance.
3. Go through the steps on the Create Snapshot page. Click **Create Snapshot** and record the snapshot ID provided on the page.
4. Follow the steps in the installation guide to create a new Onsite VM. Instead of adding a new data disk, attach the snapshot from the previous on-site version.
   a. On the Add Storage page, select the same storage size that you used for your previous instance. You must change the device name when you add this disk.

b. Difference between sdb and sdf. These are how you address the disk.
5. Start the new VM and connect via ssh with admin credentials. The system runs any necessary data migrations. If the upgrade involves large schema changes, or if you have many existing projects, this may take a while. We recommend running it overnight.
Note: The new admin password should work, so you don't need to remember the admin password for the previous machine.
6. Check the configuration to ensure that your settings were imported correctly.
7. Start the application.

KVM/QEMU: Install Luminoso Daylight and Luminoso Compass Onsite

There are many ways to use KVM and QEMU and many ways to interact with hypervisor systems, so this installation guide only offers high-level directions.

Copy the Appliance file

1. Copy the onsite file to a location where your virtualization management software can access it.
2. Uncompress the file.
3. After the file is uncompressed, check that it is available in the storage location you selected.

Create the Virtual Machine

These instructions assume you are using Virtual Machine Manager (virt-manager). The image Luminoso provides uses qcow2, so these instructions assume that you also use qcow2.
1. Open the Virtual Machine Manager and create a new virtual machine. A New VM wizard opens.
2. Select **Import existing disk image** and click **Next**.
3. Locate and select the new VM image storage path you uploaded in the prior section. It should have:
    ○ OS Type: Linux.
    ○ Version: Ubuntu 18.04 LTS (Bionic Beaver).
4. Select memory and core options. At minimum, Luminoso recommends an instance type that has at least 4 vCPUs and 16GiB of memory. Luminoso functionality does not run properly on instance types below this level. Depending on your project size, you may need to select larger options to avoid build failures. Click **Forward**.
5. Provide a name for your VM and select **Customize configuration before install.**
6. Click **Finish.**
7. Add a data storage device for application data. If you're upgrading from a previous version, skip this step. Find out your storage size information from your Luminoso Account Manager.
    ○ Format must be: 'qcow2'

- Bus type must be: 'VirtIO'
8. Attach newly added data storage or re-attach your existing data storage device.
9. Select network configuration options appropriate to your environment.
10. Review configuration and confirm that the settings correspond with your virtualization environment.
11. Open Advanced options and:
    - Change root drive to format 'qcow2'
    - Change Bus type to 'VirtIO'
12. Click Begin Installation to start your onsite instance.
13. For configuration steps, refer to the appropriate Luminoso Daylight or Compass Onsite product documentation for the configuration steps.

Upgrade Procedure for KVM/QEMU

1. Shut down the previous onsite VM and create a copy of the data disk.
2. Follow the steps in the installation guide to create a new onsite VM. Instead of adding a new data disk, attach the data disk from the previous onsite version.
3. Start the new VM and connect via ssh with admin credentials. The system runs any necessary data migrations. If the upgrade involves large schema changes, or if you have many existing projects, this may take a while. We recommend running it overnight.
   Note: The new admin password should work, so you don't need to remember the admin password for the previous machine.
4. Check the configuration to ensure that your settings were imported correctly.
5. Start the application.

VirtualBox: Install Luminoso Daylight and Luminoso Compass Onsite

Because there are many ways to interact with hypervisor systems, this installation guide only offers high-level directions.

Create the Virtual Machine

1. Launch VirtualBox.
2. Click I**mport Appliance…** in the File menu and select the OVA file.
3. Adjust the CPU and RAM settings for the new virtual appliance. At minimum, Luminoso recommends an instance type that has at least 4 vCPUs and 16GiB of memory. Luminoso functionality does not run properly on instance types below this level. Depending on your project size, you may need to select larger options to avoid build failures.
4. Click **Import**. It may take a few minutes for your system to load the virtual disk image.
5. Select the newly imported VM and choose **Settings**.
6. Add a name for your VM.

7. Add a data storage device for application data. If you're upgrading from a previous version, skip this step. This storage device is for application data only. Your Luminoso Account Manager communicates storage size to you.
8. Select network configuration options appropriate to your environment.
9. Click **OK** to save the updated settings.
10. Start your new Luminoso onsite instance.
11. Refer to the appropriate Luminoso Daylight or Compass Onsite product documentation for the configuration steps.

Upgrade Procedure for VirtualBox

1. Shut down the previous onsite VM and create a copy of the data disk.
2. Follow the steps in the installation guide to create a new onsite VM. Instead of adding a new data disk, attach the data disk from the previous onsite version.
3. Start the new VM and connect via ssh with admin credentials. The system runs any necessary data migrations. If the upgrade involves large schema changes, or if you have many existing projects, this may take a while. We recommend running it overnight.
    Note: The new admin password should work, so you don't need to remember the admin password for the previous machine.
4. Check the configuration to ensure that your settings were imported correctly.
5. Start the application.

VMware: Install Luminoso Daylight and Luminoso Compass Onsite

Upload the virtual appliance

This document assumes you have the most recent Luminoso on-site image(s) available in your environment. The upload process uses VMware's vSphere product for transferring the image to vCenter. These instructions were developed using vCenter 6.7. If you're using a different version of VCenter, your options may be slightly different.

1. Log into vCenter using vSphere.
2. Right click on the esxi host you would like to deploy to and select **Deploy OVF Template...** The Deploy OVF Template wizard opens.
3. Click **Choose File** and select the image file. File name format is [product name]_vmware-version-ID-[client]. For example, *daylight_vmware-1.0-201602221217-acme.*
4. Click Open.
5. Click **Next** and complete the wizard with information applicable to your environment.
6. Review your choices and click **Finish** to close the wizard. The VM begins to deploy. View the build progress in the Recent Tasks pane.

Create Data Disk

Our software requires you to use a disk separate from the OS disk to store all Luminoso data and configuration files. At minimum, Luminoso recommends an instance type that has at least 4 vCPUs and 16GiB of memory. Luminoso functionality does not run properly on instance types below this level. Depending on your project size, you may need to select larger options to avoid build failures.

1. Create a data disk and attach it to the Luminoso Onsite virtual machine you just deployed.

Start the VM

1. Right click the VM instance and select **Power** > **Power on the virtual machine.**
2. Refer to the appropriate Luminoso Daylight or Compass Onsite product documentation for the configuration steps.

Upgrade Procedure for VMware
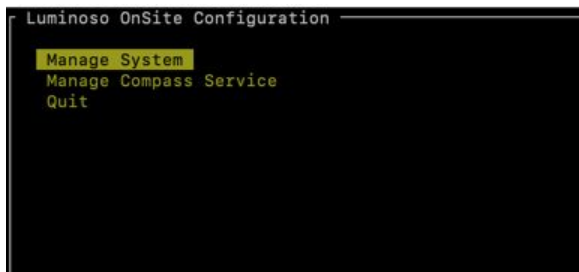
1. Shut down your old machine.
2. Deploy a new machine and keep both machines powered off.

3. In Storage, under the correct datastore, select the directory of your old virtual machine.
4. Select your data disk and click **Copy to** and copy the data drive from your old Luminoso virtual machine directory to the new one. The copy progress displays in the Recent Tasks pane.
5. Right click your new machine and select **Edit Settings**. The Edit Settings window opens.
6. Click **Add New Device** and select **Add Hard Disk**. A file explorer opens.
7. In the Datastores column, select your new virtual machine. In the Contents column, select the disk you copied from your previous machine.
8. Click **OK**. The File explorer closes.
9. Click **OK**. The Edit Settings window closes.
10. Power on your new machine.

Luminoso Compass Onsite: Configuration Guide
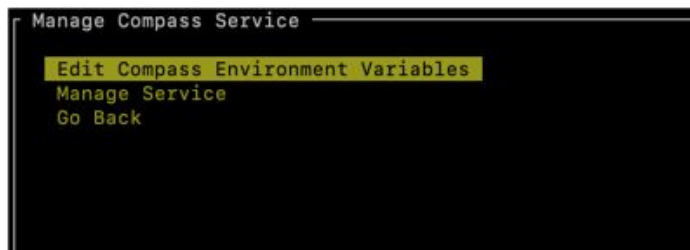
Getting Started with Compass

1. Select `Manage Compass Service` from the `Main Menu` and press `ENTER`. The Manage Compass Service menu opens.

2. Select `Edit Compass Environment Variables`.

A list of available variables displays with blank slots for you to fill in. ALLOWED_HOSTS is used for a (list of) domain/host name(s) where you access the Compass service. If you use multiple hostnames, separate them with commas.

```
┌ Edit Compass Environment Variables ─────

  ALLOWED_HOSTS              █


```

Note: Do not enclose values in quotation marks. Tab to the OK button in the bottom right and press ENTER to finish and save your values. If you press CANCEL, you exit without saving changes and erase all values.
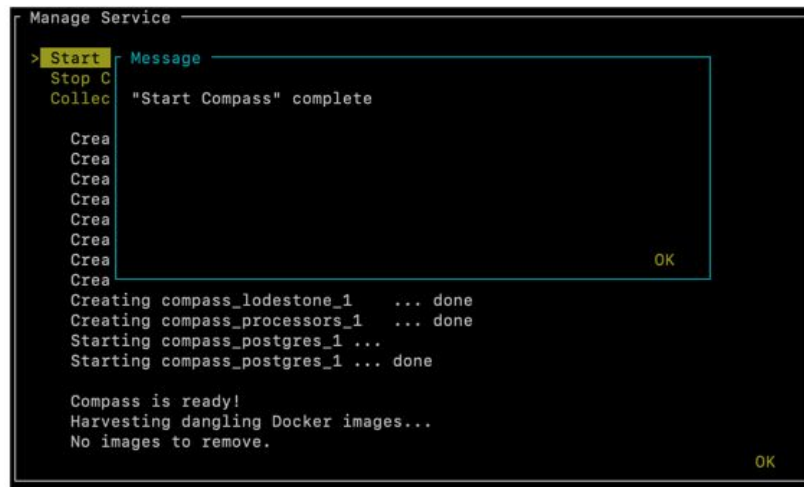
3. You are now ready to start the Compass service. Select Manage Compass
4. Service -> Manage Service -> Start Compass. The startup sequence begins. This may take up to two minutes during the first deployment.

```
┌ Manage Compass Service ─────

    Edit Compass Environment Variables
    Configure HTTPS
    Start/Stop Service
    Advanced Options
    Go Back

```

The names of the services being started appear on the screen. A screen like this appears when the sequence is finished:

```
┌ Manage Service ─────

 > Start  ┌ Message ─────
   Stop C │
   Collec │  "Start Compass" complete
          │
   Crea   │
   Crea   │
   Crea   │
   Crea   │
   Crea   │
   Crea   │
   Crea   │                                OK
   Crea   └───────────────────────────────
   Creating compass_lodestone_1    ... done
   Creating compass_processors_1   ... done
   Starting compass_postgres_1 ...
   Starting compass_postgres_1 ... done

   Compass is ready!
   Harvesting dangling Docker images...
   No images to remove.
                                            OK
```

5. Tab to the OK button and press ENTER. A screen like the following appears:

```
┌ Manage Service ─────

   Start Compass
   Stop Compass
   Collect Support Logs

   Creating compass_redis_1        ... done
   Creating compass_proxy_1        ... done
   Creating compass_db-migrator_1  ... done
   Creating compass_luminosoData_1 ... done
   Creating compass_lodestone_1    ...
   Creating compass_scheduler_1    ...
   Creating compass_processors_1   ...
   Creating compass_scheduler_1    ... done
   Creating compass_lodestone_1    ... done
   Creating compass_processors_1   ... done
   Starting compass_postgres_1 ...
   Starting compass_postgres_1 ... done

   Compass is ready!
   Harvesting dangling Docker images...
   No images to remove.
                                            OK
```

6. Use tab to highlight the OK button and press ENTER to return to the main menu. Your Compass Service is now ready to use.

7. Log in to the application using the name *master* and password *master*.
   Note: We recommend changing the password for *master* after you first log in.

Additional Configuration Options

To complete any of these tasks, you must log in to the on-site virtual machine using admin credentials.

To make system changes:
1. Select **Manage System** from the menu.
2. Select the appropriate menu option, make the necessary changes, and click **OK**.

Change Hostname

1. Open **Manage System -> Configure Networking -> Configure Hostname**
2. Change the fully-qualified domain name to your preferred domain name.
3. Select **OK**.
   NOTE: If you have DHCP and are changing the hostname, you must reboot the machine to report the new hostname to the DHCP server.

Change DHCP to Static IP

1. Open **Manage System -> Configure Networking -> Configure Interface**
2. Change "DHCP" to "Static".
3. Enter the desired IP address, Netmask, Gateway, and DNS Server. These fields are only valid if you have selected "Static" above.
4. Select **OK**.

Use an internal NTP server

1. Open **Manage System -> Configure Networking -> Configure NTP**
2. Change "DHCP" to "Static".
3. Enter the domain name of the NTP server you wish to use.
4. Select **OK**.
   NOTE: You must already have successfully changed to a static IP address in order to configure a static NTP server.

Change admin password

1. Open **Manage System -> Change admin password**
2. Change the admin password.
3. Select **OK**.
   NOTE: You cannot log into the Compass software as "admin", but must log in as one of the created users.

Configure HTTPS

1. Open **Manage Compass Service -> Configure HTTPS**
2. Select "Enable HTTPS".
3. Upload your certificate and key to the Virtual Machine via sftp using a command similar to
   ```
   sftp certcopy@[hostname]:https <<< $'put
   [/path/to/certificate.pem]'
   ```
   If prompted for a password, use the admin password.
4. Your certificate and key should both appear in the lists below; select the certificate file in the "Select Certificate File" list and the associated key in the "Select Key File" list.
5. Select **OK**.

Proxy Settings

If your deployment requires one or more http reverse proxies in front of Luminoso on-site, we recommend configuring all proxies so that requests are limited to 200 MiB in size. 200 MiB is Luminoso's internal limit.

Compass Documentation: Managing Users and Accounts

Manage Accounts and Users via API commands on your Compass admin account. For a detailed list of endpoints, refer to the [Compass API Reference](#), which outlines how to accomplish typical user management tasks.

Note: You can access the DRF via browser to the Compass API. The screenshots displayed used here were taken with DRF.

You can log in to the application with login name *master* and password *master*. We recommend you change the password for *master* after you first log in.

Overview

Action	Details
Step 1: Add an Account	You can create one or more accounts in Compass. Accounts are containers for projects and users receive permissioned access to accounts. Typically, accounts segregate users and their projects to specific groups or departments.

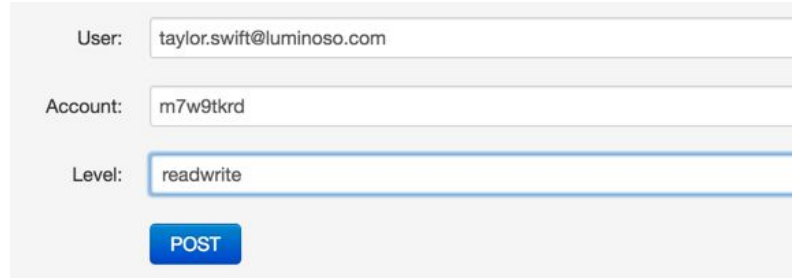|	

	Use the POST /api/accounts/ endpoint to create and specify the name of the account ("Marketing" in the example below).
	
	``
	POST /api/accounts/
	
	HTTP 201 CREATED
	Location: http://compass-master-staging.int.luminoso.com/api/accounts/m7w9tkrd/
	Content-Type: application/json
	Vary: Accept
	Allow: GET, POST, HEAD, OPTIONS
	
	{
	    "url": "http://compass-master-staging.int.luminoso.com/api/accounts/m7w9tkrd/",
	    "id": "m7w9tkrd",
	    "name": "Marketing"
	}
	``
	
	Save or copy the ID of the account for future steps.

Step 2: Add a User	Use the POST /api/users endpoint to add a user and specify the user's email, name, default account and admin option. Once you call the endpoint, it creates the user (as seen below)
	
	Email: taylor.swift@luminoso.com
	name: Taylor Swift
	Default account: m7w9tkrd
	Admin: ☐
	
	Note: Since admin users have full access to the system, including creating other users and accounts assign the option sparingly.
	
	``
	HTTP 201 CREATED
	Location: http://compass-master-staging.int.luminoso.com/api/users/taylor.swift%40luminoso.com/
	Content-Type: application/json
	Vary: Accept
	Allow: GET, POST, HEAD, OPTIONS
	
	{
	    "url": "http://compass-master-staging.int.luminoso.com/api/users/taylor.swift%40luminoso.com/",
	    "email": "taylor.swift@luminoso.com", user id
	    "name": "Taylor Swift",
	    "default_account": "m7w9tkrd",
	    "permissions": [],
	    "admin": false,
	    "must_reset_password": true,
	    "password": "kngvhrr42szqn9j" temporary password
	}
	``
	
	IMPORTANT: Save the user id and temporary password for future steps.
	
	Note: If you forget to save the temporary password, call this endpoint to reset it: /api/users/USERID/password/reset

Step 3: Assigning Permissions	Grant the user you created a permission on the account. The available permissions are: ● read: provides read-only access to projects, can only view projects, not create or edit them ● readwrite: provides create and edit permissions on projects

in the account
- manage: (to be expanded in the future, but for now the same as readwrite) provides create and edit permissions on projects in the account
- listener: reserved, do not use

To give the user a permission on the account, use the POST /api/permissions/ endpoint and specify
the User ID from Step 2, the account from Step 1 and the Level.

User:	taylor.swift@luminoso.com
Account:	m7w9tkrd
Level:	readwrite

POST

Now the user is granted a permission to the account:

```
HTTP 201 CREATED
Location: http://compass-master-staging.int.luminoso.com/api/permissions/5/
Content-Type: application/json
Vary: Accept
Allow: GET, POST, HEAD, OPTIONS

{
    "url": "http://compass-master-staging.int.luminoso.com/api/permissions/5/",
    "user": "taylor.swift@luminoso.com",
    "account": "m7w9tkrd",
    "level": "readwrite"
}
```

You have now created an account, a user, and have given the user desired access to the account. Lastly, tell the user their temporary password that you set in Step 2.

Note: if you forget to save the temporary password, you can reset it by calling this endpoint: /api/users/USERID/password/reset

Luminoso Daylight Onsite Configuration Guide

Getting Started

After installing the Luminoso Daylight Onsite Virtual Appliance, connect to it via ssh using the username 'admin' and the associated password that Luminoso support provided. After you log in, a menu appears where you can configure various properties of the machine.

Configuring the Virtual Appliance

The following steps configure the Onsite Appliance to match your data center environment. For example, the network card defaults to DHCP. If your data center environment requires static IPs, you can change it using the **Manage System** menu in the Onsite Menu.

Other system configuration options:

Manage System	Configure hostname
	Configure interface
	Configure inactivity timeout
	Configure NTP
	Change admin password
	Configure root certificate
	Configure SMTP
	Configure system notifications

	Configure application notifications
	Configure HTTPS
	Configure SAML
	Configure rsylog server
	Support Shell
Manage Users	List Users
	Create User
	Delete User
	Change User Access
	Change Account
	Delete Account
	Rename Accounts
Manage Service	Start Daylight
	Stop Daylight
	Collect Support Logs
Quit	

Update Luminoso Daylight Settings:

To complete any of the following tasks, you must log in to the on-site virtual machine using admin credentials.

To make system changes:

1. Select **Manage System** from the menu, select the appropriate menu option, and make any necessary changes,
2. Click **OK**.

Change Hostname

1. Open **Manage System -> Configure Hostname**
2. Change the fully-qualified domain name to your preferred domain name.
3. Select **OK**.
   NOTE: If you have DHCP and are changing the hostname, you will have to reboot the machine to report the new hostname to the DHCP server.

Change DHCP to Static IP

1. Open: **Manage System -> Configure Interface**
2. Change "DHCP" to "Static".
3. Enter the desired IP address, Netmask, Gateway, and DNS Server. These fields are only valid if you selected "Static" above.
4. Select **OK**.

Change the Inactivity Timeout

1. Open **Manage System -> Configure Inactivity Timeout**
2. Update the Inactivity Timeout and Maximum session length values in seconds.
3. Select **OK**.

Use an internal NTP server

1. Open **Manage System -> Configure NTP**
2. Change "DHCP" to "Static".
3. Enter the fully-qualified domain name of the NTP server you wish to use.
4. Select OK.
   NOTE: You cannot use NTP via DHCP if you are not using DHCP to assign an IP address.

Change admin password

1. Open **Manage System -> Change admin password**
2. Change the admin password
3. Select OK.
   NOTE: You cannot log into the Daylight Web Interface as "admin", but must log in as one of the created users (see "Accounts and Users").

Configure root certificate

1. Open **Manage System -> Configure root certificate**
2. Upload your root certificate to the Virtual Machine via sftp using a command similar to

   ```
   sftp certcopy@[hostname]:ssl <<< '$put
   [/path/to/certificate.pem]'
   ```
   If prompted for a password, use the admin password.
3. The new certificate should appear in the list below "Clear existing certificate"; select it.
4. Select **OK**.

Configure SMTP

1. Open **Manage System -> Configure SMTP**
2. Enter the SMTP host name and the SMTP port.

3. Select "Use StartTLS" and "Require valid certificate" if you would like to encrypt your connection to the SMTP server.
4. Enter the SMTP username and the associated SMTP password, if required by your SMTP server.
5. Select **OK**.
   NOTE: In order to use TLS, you may need to configure your root certificate.

Configure System Notifications

1. Open **Manage System -> Configure system notifications**
2. Enter the email address *to* which system alerts should be sent (probably your own email address).
3. Enter the email address *from* which system alerts should be sent.
4. Select **OK**.
   NOTE: In order to have the Virtual Machine send alert emails, you need to have configured SMTP.

Configure Application Notifications

1. Open **Manage System -> Configure application notifications**
2. Enter the email address from which application notifications (for instance, "forgot email" notifications) should be sent.
3. Enter the URL for the Luminoso Daylight UI, so that links will work in application notification emails.
4. Select OK.
   NOTE: In order to have the Virtual Machine send alert emails, you need to have configured SMTP.

Configure HTTPS

1. Open **Manage System -> Configure HTTPS**
2. Select "Enable HTTPS".
3. Upload your certificate and key to the Virtual Machine via sftp using a command similar to

   ```
           sftp certcopy@[hostname]:https <<< $'put
   [/path/to/certificate.pem]'
   ```
   If prompted for a password, use the admin password.
4. Your certificate and key should both appear in the lists below; select the certificate file in the "Select Certificate File" list and the associated key in the "Select Key File" list.
5. Select OK.

Configure SAML

The Luminoso Daylight implementation of the SAML2 Single Sign-on Profile uses the HTTP Redirect (GET) and HTTP POST Bindings on our Single Login and Assertion Consumer Endpoints.

You must configure the Identity Provider to send the attribute 'lumi_username' containing the user's Luminoso Daylight username in the SAMLResponse sent to the Assertion Consumer Service upon login.

Each task assumes that you have logged in to the virtual machine using admin credentials.

1. Open **Manage System** -> **Configure SAML** and select **Use SAML**.
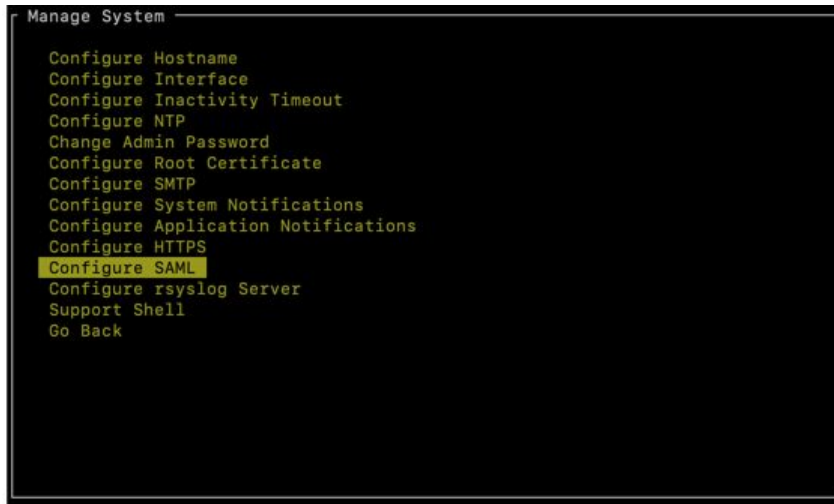
2. Select the SAML Response and Authentication Request signing and encryption options that match your policies and IDP configuration.
Note: Selecting "Support password authentication in addition to SAML" allows local accounts to log in as well as SAML accounts. If you deselect it, only SAML users can log in to the system.
3. Enter the Identity Provider Entity ID, and Single Sign-on URLs.
You can get this information from your Identity Providers SAML 2.0 Identity Provider Metadata by looking for:
   a. `EntityDescriptor entityID="[IDP Entity ID]"`
   b. `SingleSignOnService`
      `Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"`
      `Location="[IDP Single Signon URL]"`
   c. `dsig:X509Certificate`
4. Generate a public certificate and private key in PEM format for SAML using a command similar to:
      `openssl req -new -x509 -days 365 -nodes -out sp_cert.pem -keyout`
   `sp_key.pem`
5. Ensure that all the file are world readable before uploading them by running a command similar to:
      `chmod 644 *.pem`
6. Upload your identity provider certificate, newly generated certificate and private key to the Virtual Machine via sftp using commands similar to:
      `sftp certcopy@[hostname]:saml <<< $'put`
   `[/path/to/idp.cert|sp_cert.pem|sp_key.pem]'`
   If the system prompts you for a password, use the admin password. The new

certificates and key appear in the list below "IDP Certificate File", "SP Certificate File", and "SP Private Key File"

7. Select the new certificate files and key.
8. Select **OK**.

Send Logs to an rsyslog Server

1. Open **Manage System -> Configure rsyslog Server**
2. Enter the name of your rsyslog server.
3. Select **OK**.

Start an instance of Daylight Onsite

1. Go to: **Manage Service**
2. Select **Start Daylight**.
3. Select **OK** from the popup, and then **OK** in the menu.
   NOTE: It may take up to five minutes for the application's services to fully start.

Collect Support Logs

1. Go to: **Manage Service**
2. Select **Collect Support Logs**. After the logs are collected, instructions on how to download them from the appliance appear on screen.

Daylight Onsite: Accounts and Users

To complete any of these tasks, you must log in to the on-site virtual machine using admin credentials.

Create a user

1. Go to: **Manage Users and Accounts -> Create User**
2. Enter username and password.
   > **NOTE:** A username should be the user's email address; this ensures that the user receives the correct notifications and alerts.
3. Select OK.
   Note: Make sure your created users are granted permissions (see next step). A user without permissions is directed to an empty page with no options upon login.

Create account

1. Go to: **Manage Users and Accounts -> Create Account**
2. Enter the human-readable name of the account you wish to create.
3. Select **OK**.

Grant/Change user permissions

1. Go to: **Manage Users and Account -> Change User Access**.
2. Enter the username of the user whose permissions you wish to change.
3. For each account, check the permissions you wish to give the user.
4. To remove permissions, use the space bar instead of the enter key.
5. Select **OK**.
   Note: Users with Global permissions have those permissions on all projects in all accounts, though they are not explicitly listed.

Change a user's password

1. Go to: **Manage Users and Account -> Change User Password**
2. Enter the username of the user whose password you wish to change, as well as the new password.
3. Select **OK**.

Delete a user

1. Go to: **Manage Users and Account -> Delete User**
2. Enter the username of the user you wish to delete.
3. Select **OK**.

Delete an account

1. Go to: **Manage Users and Account -> Delete Account**

2. Select the account you wish to delete.
   Note: To prevent accidental data loss, do not delete accounts that contain projects. To delete such an account, start by deleting everything it owns through the UI.
3. Select OK.

Rename accounts

1. Go to: **Manage Users and Account -> Rename Accounts**
2. Select an account and enter the new name.
3. Select **OK**.

Proxy Settings

If your deployment requires the use of one or more http reverse proxies in front of Luminoso Onsite, Luminoso recommends configuring any and all proxies so that requests may be up to 200 MiB in size. 200 MiB is the limit Luminoso imposes internally.