Curie™ Integration Guide

Software Version 1.1

Table of Contents

Revision History

Date	Revision	Description
October 17, 2021	A	Initial Document Release
April 26, 2022	B	Post-Release Updates
August 31, 2022	C	Post-Release Refinements
September 7, 2022	D	Post-Release Refinements

Purpose

This document contains the important system integration information for the client regarding integration of Curie™ *Standardize* and the Enlitic Enterprise Backup Policy, the Enlitic Enterprise Security & AV Policy, Enlitic LDAP Policy, the assumed responsibilities of Enlitic and assumed responsibilities of the client.

Enlitic Enterprise Backup Policy

Option 1

Backup the entire VM using a 3rd-party product, such as Veeam, Veritas backup exec, etc.

Option 2

Backup the Curie™ & Linux OS folders to a “backup share on client network” every week.

- /var/local/curie/ldap
- /var/local/curie/wildfly
- /var/local/curie/keycloak
- /var/local/curie/elasticsearch
- /home/[username]/curie/*.yml, *. versions
- /etc/fstab
- /etc/netplan

Enlitic Enterprise Security & Antivirus Policy

Ports to have open on Ubuntu/Linux Server

TCP Ports

Internal Network Ports	80	Hypertext Transfer Protocol (HTTP)
	389	curie-ldap - Lightweight Directory Access Protocol (LDAP)
	636	curie-ldap - Secure Lightweight Directory Access Protocol (LDAP)
	2575	curie-arc
	2762	curie-arc
	5432	postgres / DB
	5601	Kibana
	6263	model-standardize
	6514	logstash
	8080	curie-arc HTTP
	8514	logstash
	8880	keycloak - HTTP
	8990	keycloak - Management HTTP
	9200	Elasticsearch
	9300	Elasticsearch
	9990	curie-arc
	12575	curie-arc
Required External Ports	22	Secure Shell (SSH), secure logins, file transfers (scp, sftp), port forwarding
	8443	curie-arc - HTTPS
	8643	Kibana
	443	Hypertext Transfer Protocol Secure (HTTPS)
	8843	keycloak - HTTPS
	8993	keycloak - Management HTTPS
	9993	curie-arc admin
	11112	curie-arc DICOM

UDP Ports

UDP Ports to Have Open on Ubuntu/Linux Server	
I - 8514	curie-arc
I - 12201	curie-arc

AV Exclusions on Ubuntu/Linux Server

- /var/local/curie/*

Antivirus Scan Policy

The use of commercial antivirus software and the application of security patches is a major concern for healthcare facilities. This document outlines the policies and procedures used for the administration of Curie™ in these areas. The Antivirus Scan Policy is an extract of the Curie™ Product Specification and defines the use, setup and application of antivirus software packages on Curie™ systems.

General Policy

A virus protection strategy on the Curie™ software system is very important. Antivirus software is available from many companies, such as Symantec, Cylance, or McAfee. These companies put significant resources towards researching new and existing viruses. Antivirus software can look at existing files for existing viruses. It can monitor memory resident viruses. It can even monitor all files that enter or leave a server for virus signatures. Antivirus software companies provide frequent updates for newer viruses.

A virus protection strategy is best designed at an enterprise level by a competent customer IT staff. For this reason, and because there are so many different antivirus software manufacturers, Enlitic does not recommend any specific antivirus software.

Curie™ is tested with virus protection software during the product release testing. However, this does not mean that any specific antivirus software is validated for use with Curie™. We recommend that either the customer or the responsible implementation party test the selected antivirus software on the Curie™ test system before rolling the software into production using the recommended procedure detailed in the next section.

The recommendation is that connected and/or integrated storage to Curie™ be scanned by a regularly scheduled file system virus scan. However, this process should be configured to scan only files that are vulnerable to virus infections. This can be done by filtering the scanning process based on the file extension. This is an option in most commercial antivirus software. Database drive and database installation directory must not be scanned due to the known issues described in the later section.

In addition to the Curie™ servers, all workstations used to access Curie™ must be managed by the customer per their enterprise antivirus policy.

Known Issues of Antivirus Software with Curie™

Real-Time Scanning

If antivirus software is installed and running a resident scan of every file that enters or leaves a Curie™ server, image retrieval or AI processing performance will likely be affected. The image retrieval process on the Curie™ server may also cause image retrieval/processing errors, which do not delete, corrupt, or change images on the server.

Scanning for Archived Images

Long-term archives virus protection is the responsibility of the customer.

Live Database Scanning

Files in a live database are constantly updated with transactions and expect to have a reasonable time of accessibility. Some antivirus software locks files during the scan and can create a serious database problem such as database corruption.

Scanning on Database Installation Directory

If database installation and cache directories are scanned by antivirus software, files will lock during the scan. If some database activities happen during the scan, it may result in a database error, or database corruption. To prevent these issues in the database, it is strongly recommended not scanning database drives.

Recommended Test Procedure

Two test cases are sufficient for testing antivirus software with Curie™ servers. The first one is to access Curie™ during the scheduled scan and make sure Curie™ is available during the virus-scan. The second is to access Curie™ after the scheduled scan and make sure that the virus-scan does not affect the behavior of Curie™. This test does not evaluate the performance of the antivirus software itself.

Testing should be performed on the Curie™ test server before installing antivirus protection onto the production servers.

1. Configure antivirus software on the Curie™ server as described in the previous section.

2. Send images before the virus scan:

- Images should include CT studies with over 100 images per study and CR images
- Verify images have been stored within Curie™

3. Start the virus scan. During the virus scan, make sure no errors occur, and attempt to:

- Send images including CT and CR
- Access stored images via Curie™

4. After the virus scan completes, display the same images. Make sure there are no errors or performance issues.

5. Configure antivirus software on the Curie™ server as described in the previous section.

- Send images before the virus scan
- Images should include CT studies with over 1OO images per study and CR images
- Verify images have been stored within Curie™

6. Start the virus scan. During the virus scan, make sure no errors occur and attempt to:

- Send images including CT and CR
- Access stored images via Curie™

7. After the virus has been completed, display the same images and again, make sure there are no errors.

OS Critical Patch Installation Policy

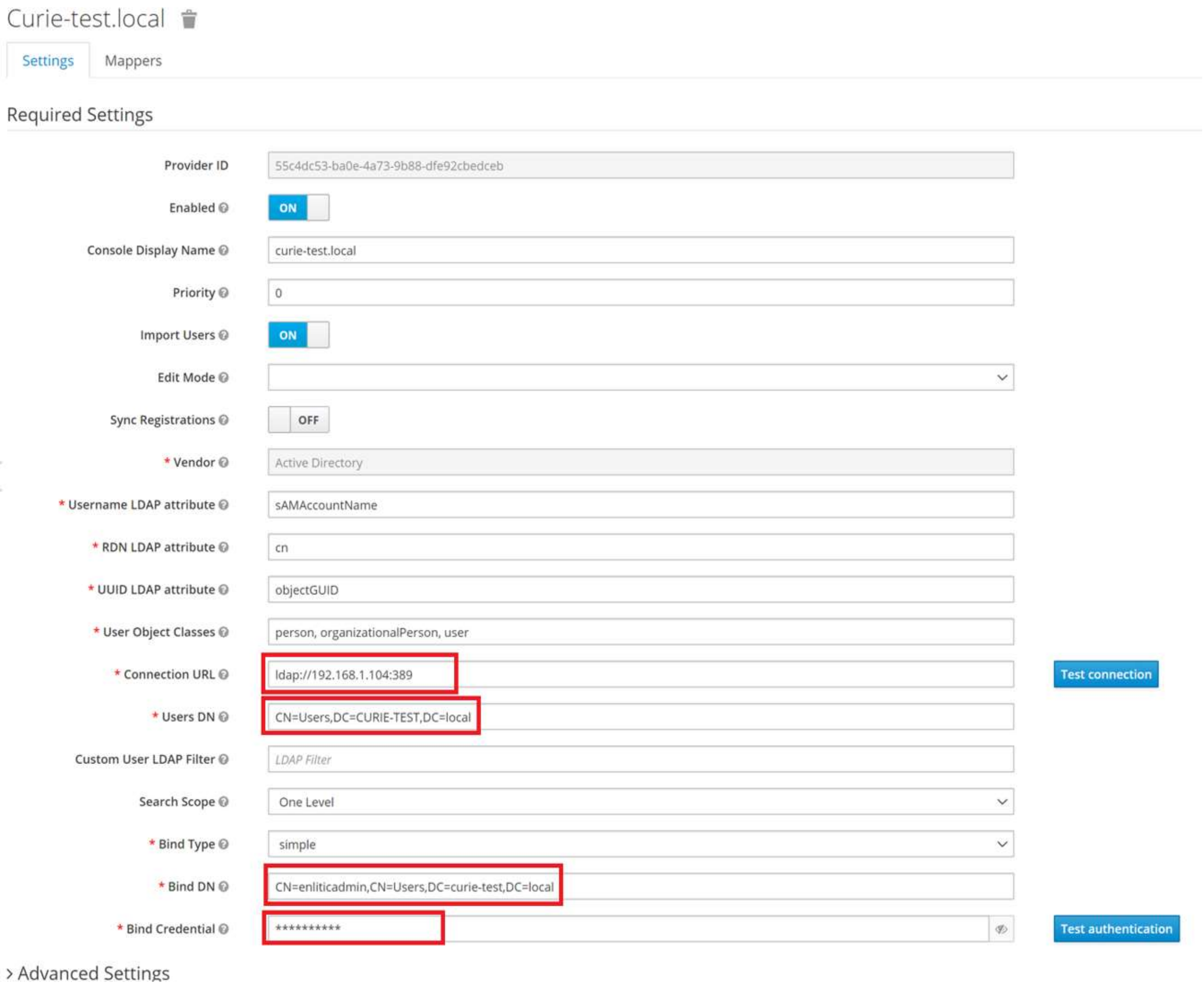
Operating system security holes can cause major problems for servers and networks. OS vendors frequently release patches and service releases to address threats to security. While Enlitic makes every attempt to validate product conformance to released patches, it is the responsibility of the customer to validate the patch in a controlled environment to make sure it does not adversely affect product operation.

Enlitic LDAP Policy

Please provide the following to the Implementation Engineer regarding your Active Directory for LDAP integration to Curie™ *Standardize*.

- Connection URL
- Users DN
- Bind DN
- Bind Credential

Please Note: LDAP Service Account for Bind DN to authenticate is needed and it is recommended that the password does not expire.



Curie-test.local

Required Settings

Provider ID	55c4dc53-ba0e-4a73-9b88-dfe92cbedceb
Enabled	ON
Console Display Name	curie-test.local
Priority	0
Import Users	ON
Edit Mode	
Sync Registrations	OFF
* Vendor	Active Directory
* Username LDAP attribute	sAMAccountName
* RDN LDAP attribute	cn
* UUID LDAP attribute	objectGUID
* User Object Classes	person, organizationalPerson, user
* Connection URL	ldap://192.168.1.104:389
* Users DN	CN=Users,DC=CURIE-TEST,DC=local
Custom User LDAP Filter	LDAP Filter
Search Scope	One Level
* Bind Type	simple
* Bind DN	CN=enliticadmin,CN=Users,DC=curie-test,DC=local
* Bind Credential	**********

Assumed Responsibilities of Enlitic

- Implementation of Curie™ *Standardize* as per the Project SOW

Assumed Responsibilities of the Client

- Curie™ user account creation, deletion, and access control
- Enforce user account access, and password enforcement based on their AD security policies
- Store usernames and passwords in a secure system
- Maintain different usernames and passwords for production and backup systems
- Backups of Ubuntu and Curie™ configuration based on Enlitic Enterprise Backup Policy
- Backup of Image Share or cache location for Curie™; Optional
- SSL Certificate purchase for encrypting Curie™ web portal, including cert renewals
- Ubuntu Server OS, Updates & Firewall
- Ubuntu Server Antivirus. Antivirus Exclusions based on Enlitic Antivirus Exclusions Policy
- Customer is responsible to enforce policy to have data at rest encrypted
- Configured by the site and defined during deployment by integration with the identity services
- Customer is responsible for providing an NFS share for images in distributed Curie™ environments