GE Healthcare

MC3 1.1 Advanced Cyber Security_DoD Service Manual

Revision History

Revision	Date	Reason for Change
1	April 17, 2020	Initial release.

Contents

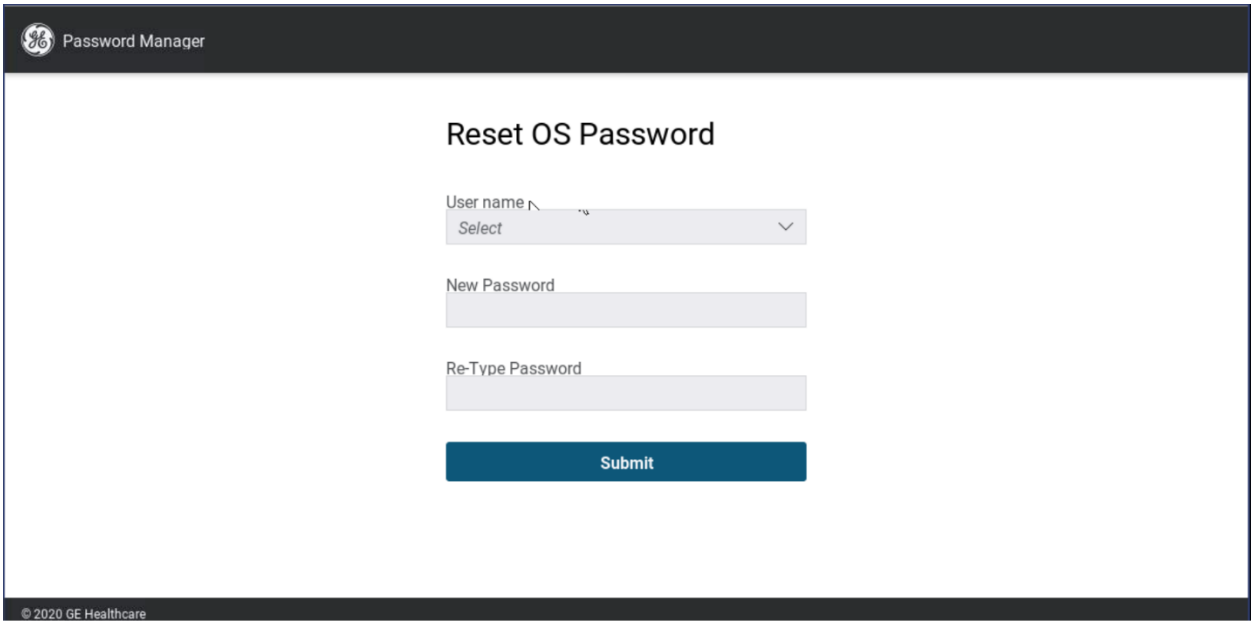
1. INTRODUCTION

This document descripts the install or setting procedure for the features:

- DOD mode installation and configure (Advanced cyber security controls)
- Malware Protection (manager mode)
- Malware Protection (standalone license mode)

2. CHANGE OS PASSWORD AT FIRST BOOT UP IN DOD MODE

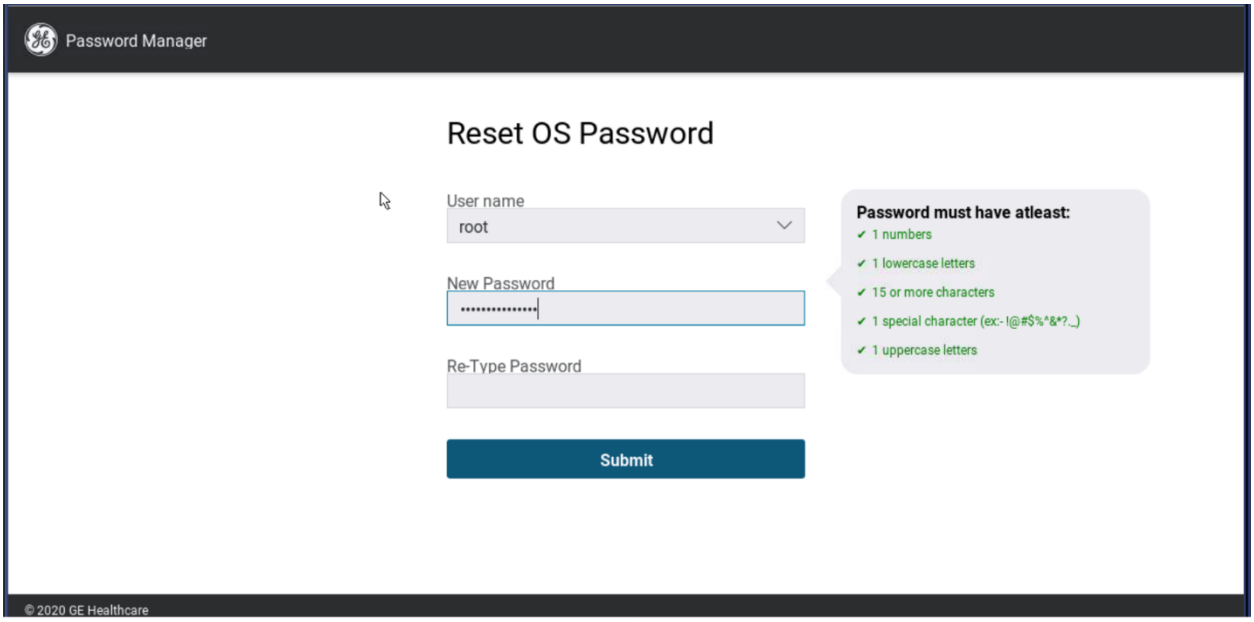
1. Install Advanced cyber security control option by license.
2. Wait for 7 to 10 minutes to complete DoD installation then reboot the system to apply DoD configurations.
3. Once application start, the "OS Password reset" UI screen will get displayed.



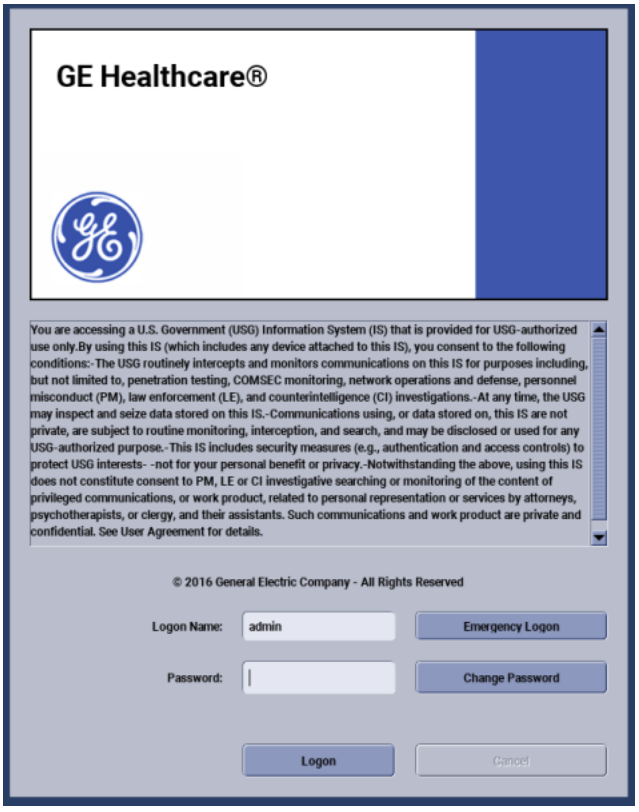
4. Change the OS password for root and ctuser.

   System enforces the following password strength rules:

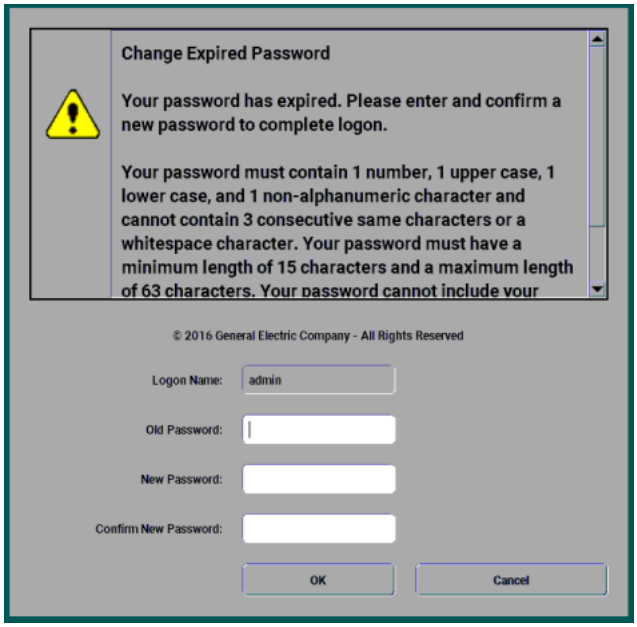
   a. All passwords must have a minimum of 15 alphanumeric characters.
   b. All passwords must have at least one uppercase alphabetic character
   c. All passwords must have at least one lowercase alphabetic character
   d. All passwords must have at least one numeric character
   e. All passwords must have at least one non-alphanumeric special character
   f. Passwords must not contain more than three consecutive repeating characters
   g. The default passwords cannot be used



5. Application starts automatically once the OS password change is successful.
6. System will display the EA3 Login UI with DoD banner.



7. Login as admin. Once successfully authenticated, system enforces to change admin default password.



8. After successfully changed admin default password, login as admin again with new password. The CT apps will start.

3. CHANGING AN OS ACCOUNT PASSWORD

It is recommended that site user administrators change the default OS user account passwords after every SW installation for root, ctuser and insite.

OS Password Change UI allows user with administrator or GE service privileges to change OS password for root, ctuser and insite user accounts.

Once software is installed, Site administrator or GE Service user can change the OS Passwords anytime at their discretion. Following are the steps to be followed:

1. Login to HIPAA/EA3 as a user with administrator or GE Service privileges.
2. From the Utilities Menu, select Service to open the service desktop application.
3. Select Utilities Tab, select Security Center.

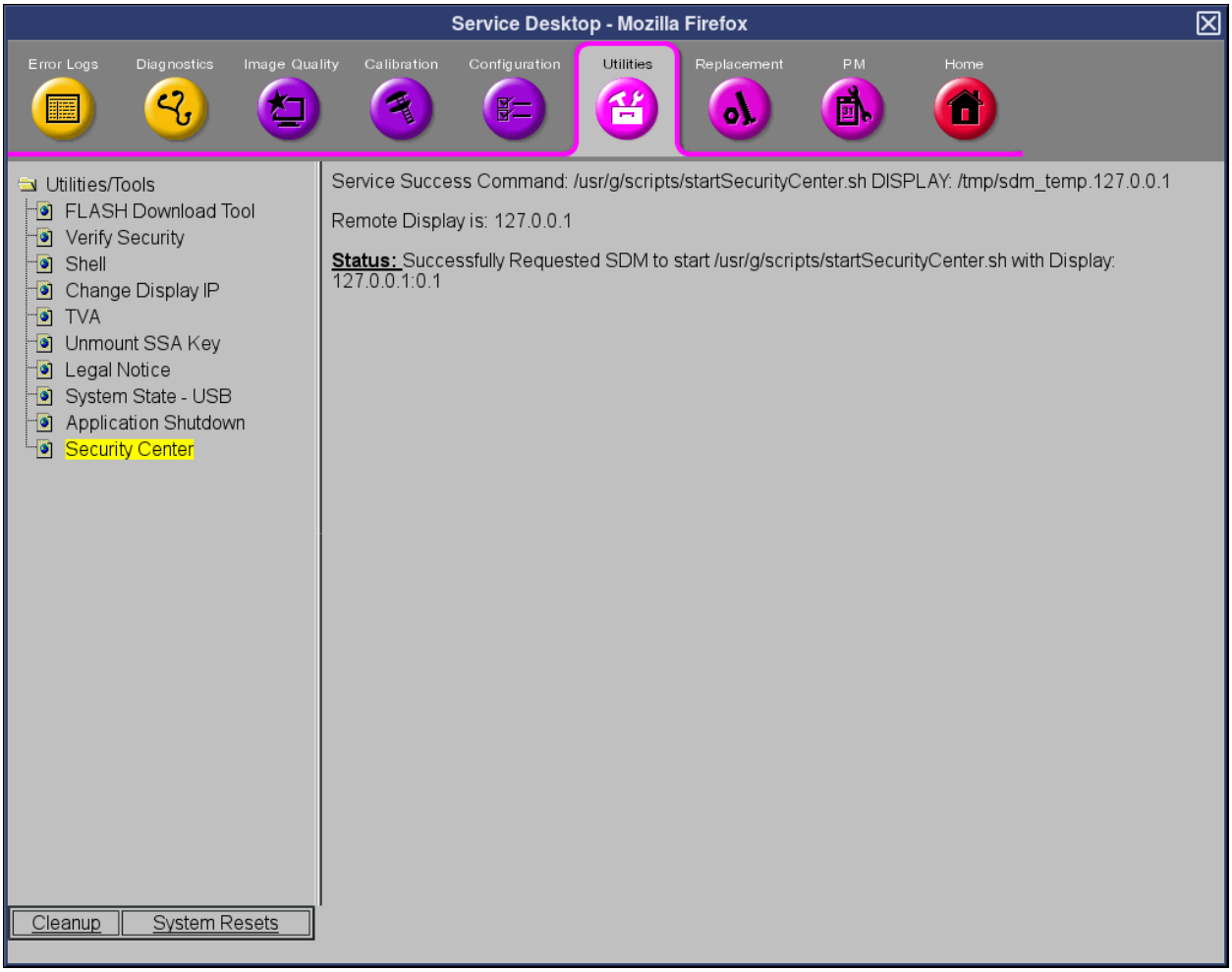


Figure 1: Service Desktop

4. On Security Center Dashboard, select OS Password Change from Application Tab.

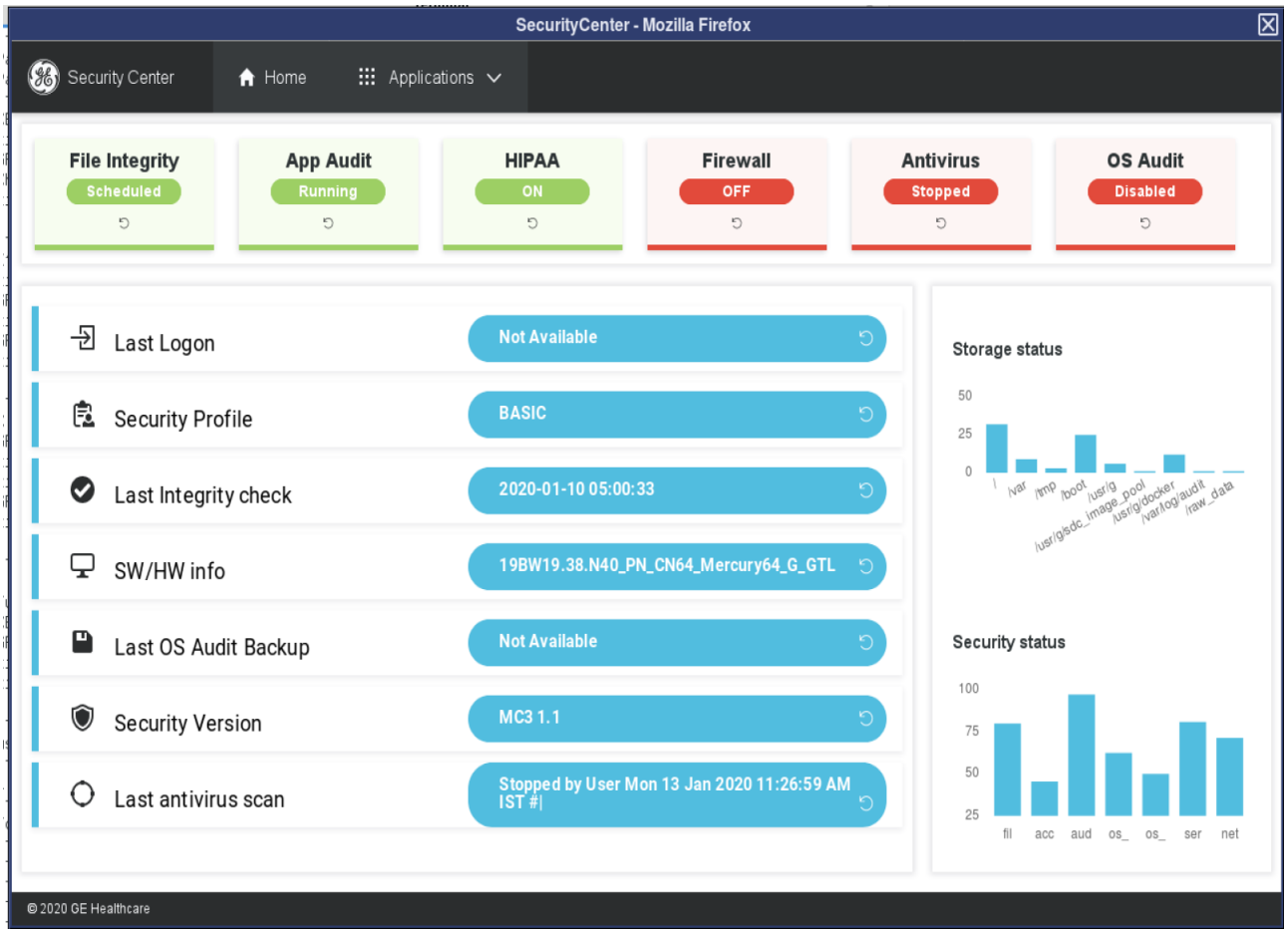


Figure 2: Security Center

Note:

1) Application tab is not displayed when the current user doesn't have EA3 admin or GE Service role.
2) In Advanced Cyber Security Control mode security profile will be shown DOD.
3) In Advanced Cyber Security Control mode insite user will not be there in the username drop down since it has disabled in DoD mode.

5. Select the OS user account (root, ctuser, insite [Disabled in DoD Mode]) from User Name drop down
6. Enter the Old Password
7. Enter the New Password that complies with rules defined in **Error! Reference source not found.** chapter in the New Password field and Retype New Password
8. Click Submit. A message will be displayed to indicate that password changed successfully or why the password change was not accepted.

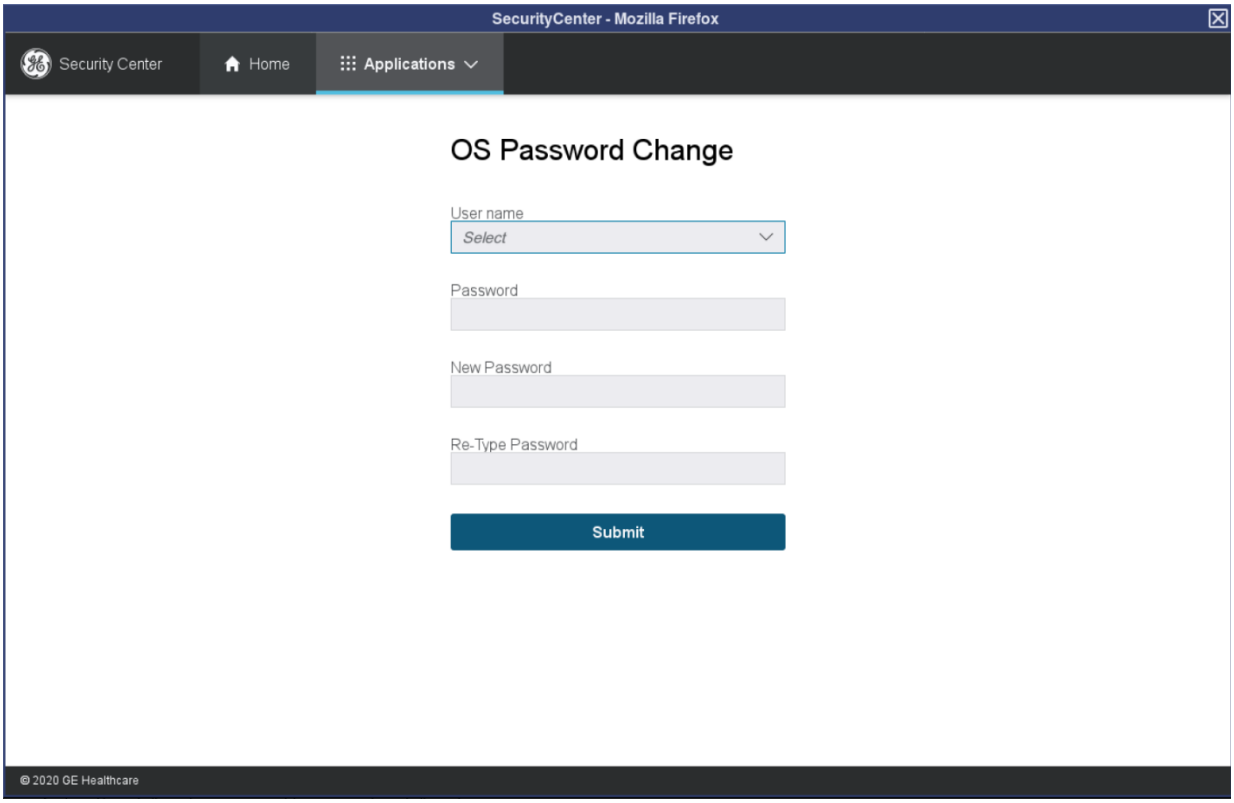


Figure 3: OS Password Change GUI

System enforces the following password strength rules in Basic mode:

a. All passwords must have a minimum of 8 (normal) alphanumeric characters.
b. All passwords must have at least one uppercase alphabetic character
c. All passwords must have at least one lowercase alphabetic character
d. All passwords must have at least one numeric character
e. All passwords must have at least one non-alphanumeric special character
f. Passwords must not contain more than three consecutive repeating characters
g. The default passwords cannot be used
h. Password must require the change of at least four (4) of the total number of characters when passwords are changed.

System enforces the following password strength rules in Advanced cyber security control mode:

a. All passwords must have a minimum of 15 alphanumeric characters.
b. All passwords must have at least one uppercase alphabetic character
c. All passwords must have at least one lowercase alphabetic character
d. All passwords must have at least one numeric character
e. All passwords must have at least one non-alphanumeric special character
f. Passwords must not contain more than three consecutive repeating characters
g. The default passwords cannot be used
h. Password must require the change of at least eight (8) of the total number of characters when passwords are changed.

If new password does not meet the above stated "password strength rules", the system displays an error message as shown below and the password is not changed.

4. RESETTING AN OS USER ACCOUNT PASSWORD

Forgot Password / OS Password Reset UI allows user with administrator and service privileges to reset OS password for root and ctuser user accounts when the present passwords for those accounts are not known or forgotten

1) Login to EA3/HIPAA authentication page as administrator role or GE service role
2) From **Utilities Menu**, select **Service**, to open the **service desktop**.
3) Select **Utilities Tab**, select **Security Center**.
4) Select **OS Password Reset** menu item from Application Tab.

   Note: Application tab is not displayed when the current user doesn't have EA3 admin or GE Service role.

5) Select the **user account** (root, ctuser, insite) from **User Name** drop down
6) Enter the New Password that complies with rules defined in *Error! Reference source not found.* **chapter** in the **New Password** field and **Retype New Password**

If new password does not meet the password strength rules, the system displays an error message and the password is not changed.

7) Click **Submit button**. A message will be displayed to indicate Password Changed Successfully or why the password change was not accepted.
8) Close the SecurityCenter once done.

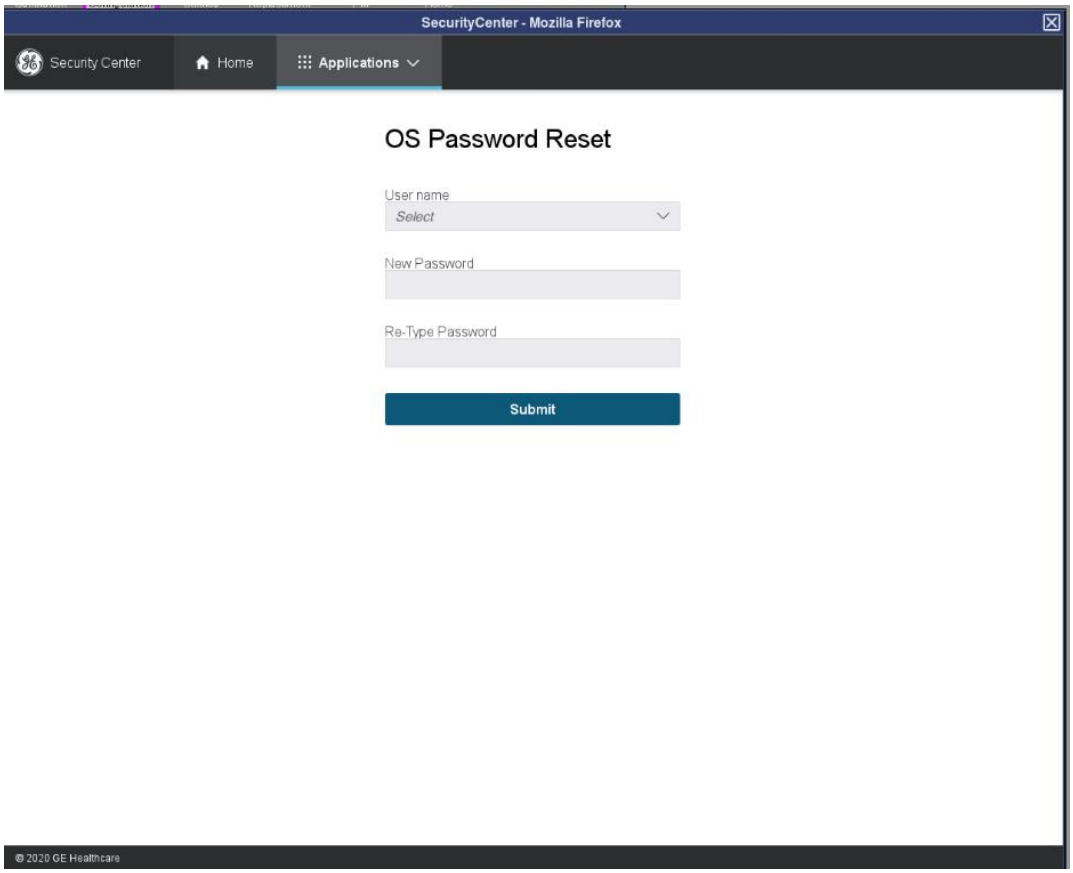


Figure 4: Reset OS Password UI

5. RESETTING AN APPLICATION ADMINISTRATOR PASSWORD

When Site Administrator forgets the EA3 admin password, admin activities such as creating new user cannot be performed accounts. Following procedure can be used to reset admin password. Note OS root password is required to successfully reset the EA3 admin password

1) Log in as service user at EA3 prompt
2) Save System State from Service Desktop
3) Open a Unix Terminal
4) Become root by executing "su – "<enter OS root password>
5) Reset Admin password using /usr/g/scripts/resetAdminPassword.sh
6) Logout from the session
7) Login as admin user (with default password "install@install") and reset the admin password
8) System is back to working state.

Recommendation: System should have at least two user admin accounts. One would act as back up account.

Note: Doing LFC when the root password is lost is not the most desirable solution. There is a possible solution to recovery the root password using the rescue mode capability provided in the SLES OS disk.

6. RESETTING AN APPLICATION NON-ADMINISTRATOR PASSWORDS

A user administrator can reset all users' passwords without knowing old password using the EA3 administration GUI shown in the previous section. The first password that is set for non-admin user accounts should be temporary password. User Administrator should force the user to change the password on next successful login after account creation and the new password shall be compliant with rules.

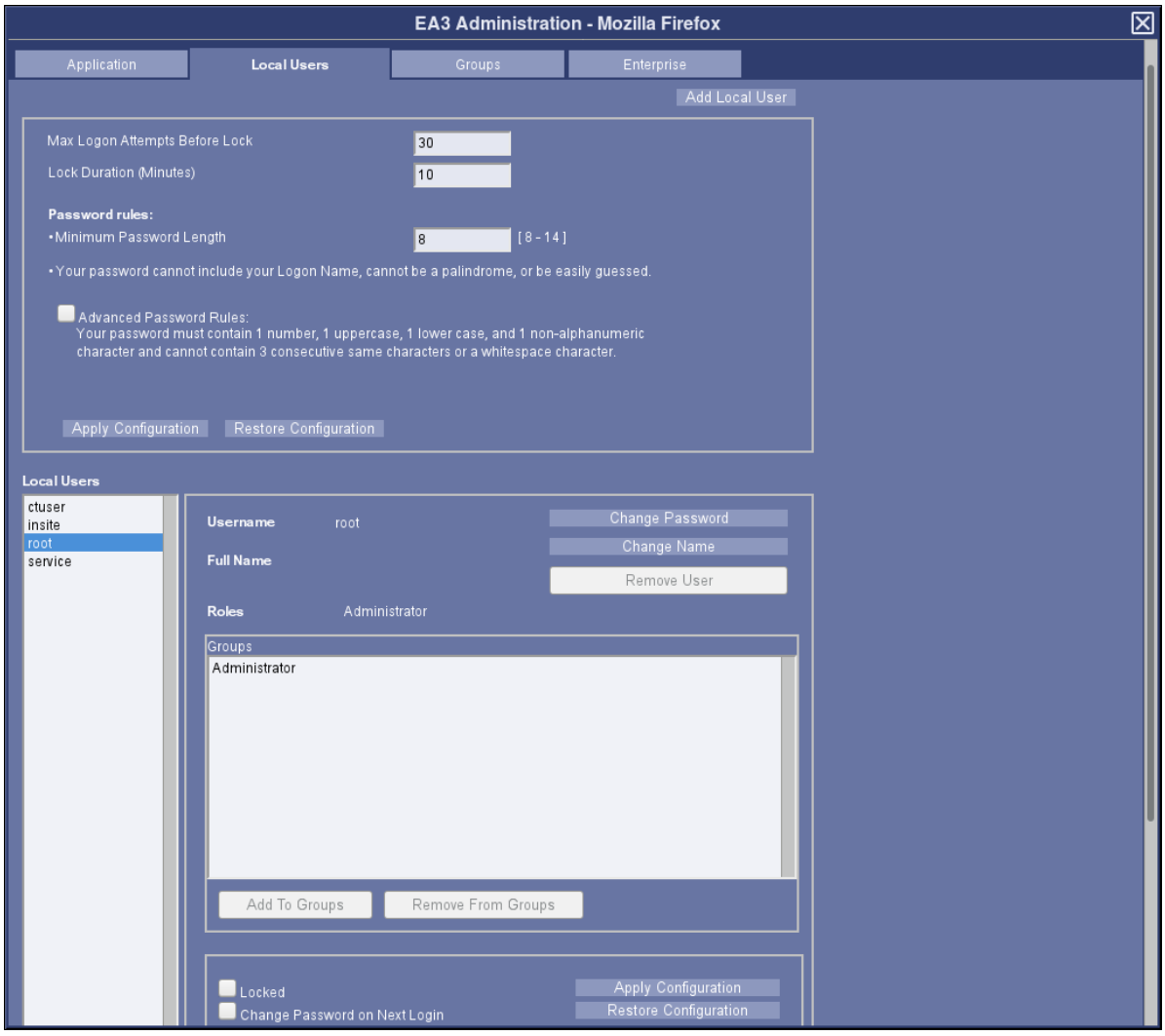


Figure 5 EA3 Administration Page in Basic Mode

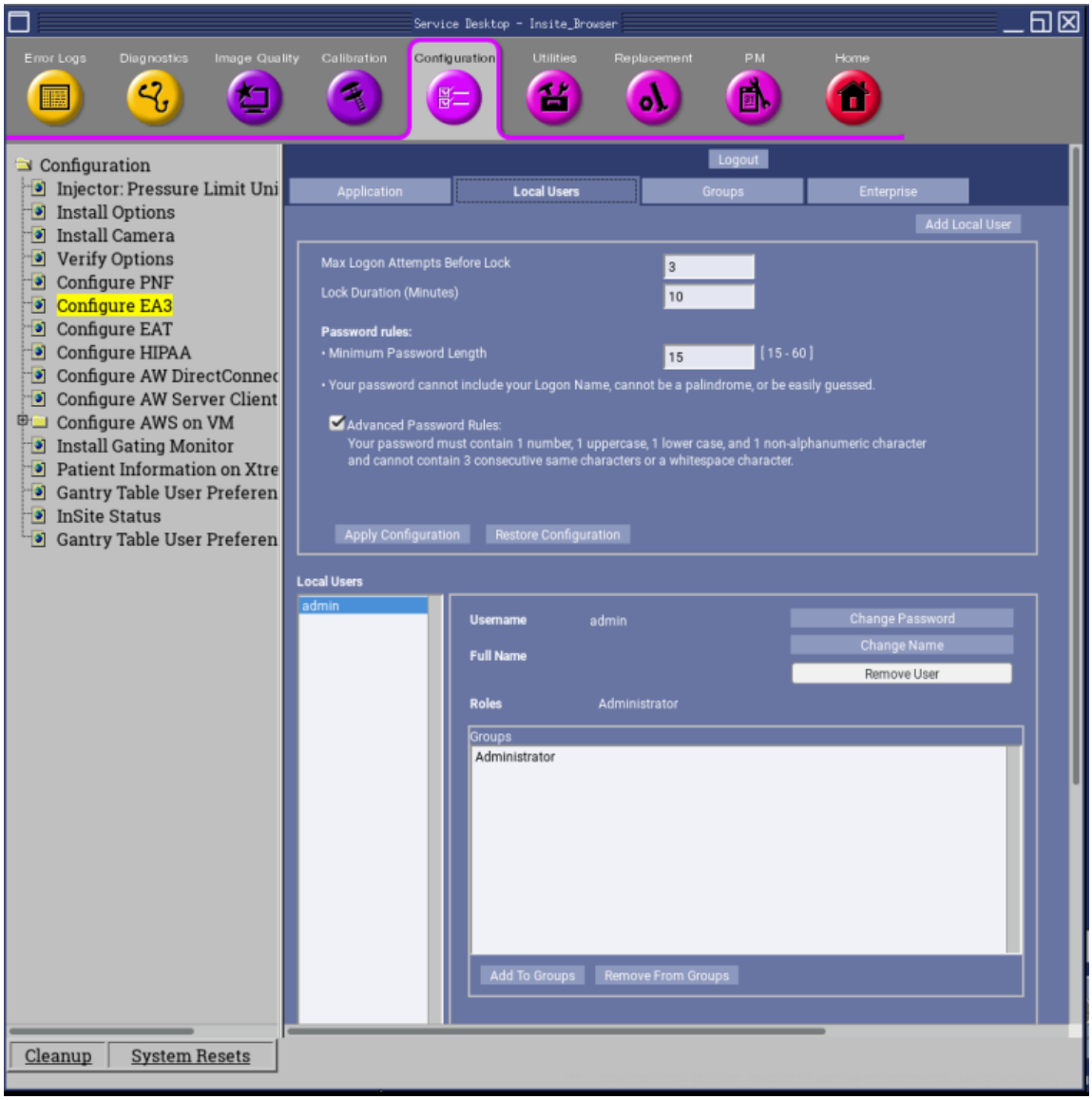


Figure 6: EA3 Administration Page in Advanced CyberSecurity Controls Mode

1. Launch EA3 administration Page from System tools→Access Controls→User Admin Tool
2. Login as EA3 administrator
3. Choose the local user and select the Change password
4. Enter the new password twice and confirm change
5. It is recommended to select "Change Password on next login" checkbox
6. Click on Apply Configuration

7. CERTIFICATE MANAGEMENT UI

The Certificate Management UI is designed for organizing public and private SSL certificates. It allows application on the scanner desktop to connect to the external servers securely using the SSL/TLS certificates that are imported into the Certificate Management application.

7.1. Generate Host Certificates

To generate certificates using below command

Login as EA3 Admin
Open an xterm
Run the following command as root

 # openssl req -newkey rsa:2048 -nodes -keyout hostkey.pem -x509 -days 365 -out hostcert.pem

When run this command two certificates will generate

1) hostkey.pem -- Private Key (This can be used in Device/Server itself)
2) hostcert.pem – Public Certificate (It can be used for to connect other devices)

7.2.Copy the certificates into USB

mountUSB
cd /USB
copy <path to certificates> /USB

7.3.Launch Certificate Management UI

1) Login to EA3/HIPAA authentication page as administrator role or GE service role
2) From Utilities Menu, select Service, to open the service desktop.
3) Select Utilities Tab, select Security Center.
4) Select Certificate management GUI menu item from Application Tab.

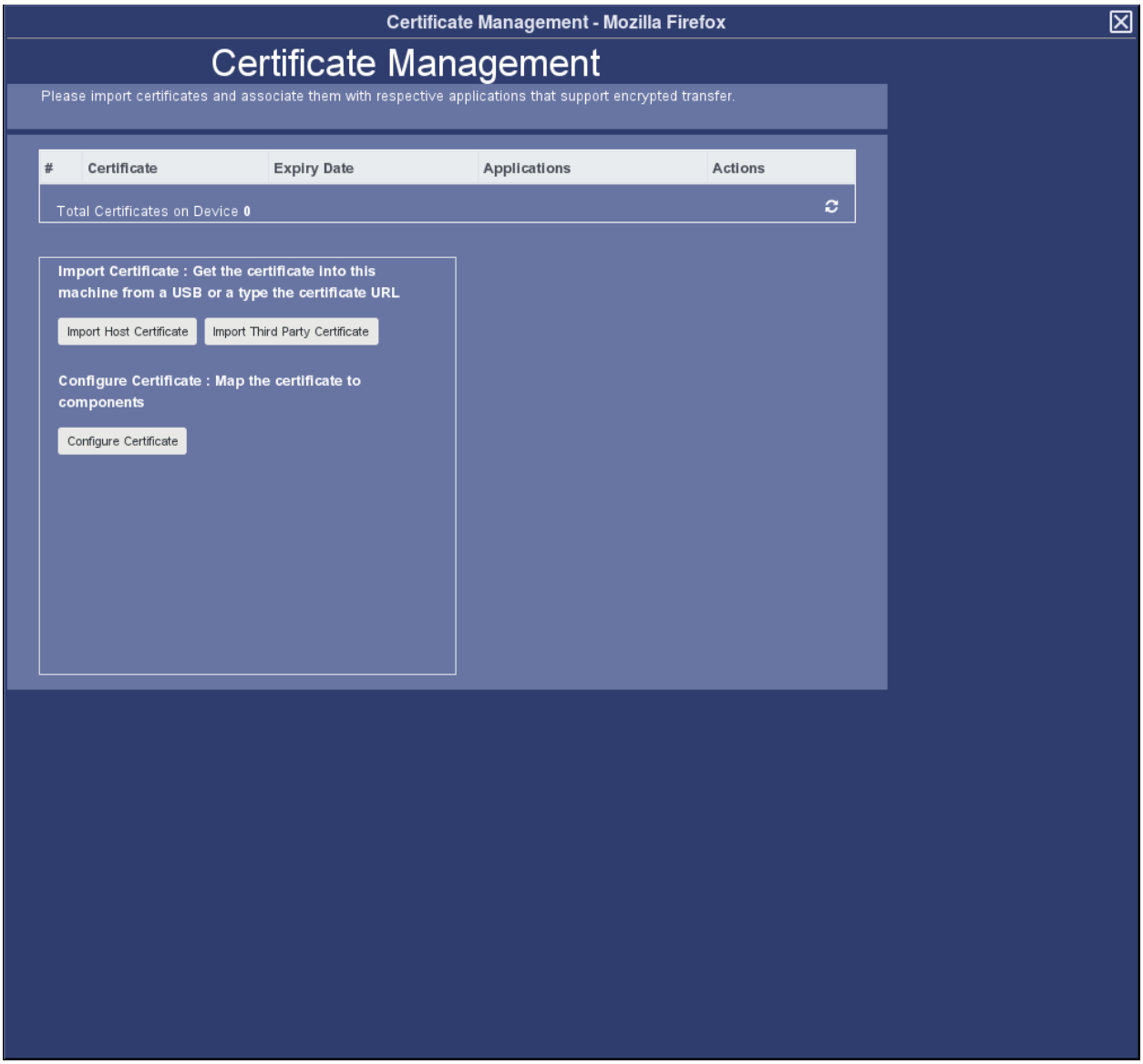


Figure 7: Certificate Management

Note: Application tab is not displayed when the current user doesn't have EA3 admin or GE Service role.

7.4.Importing Certificate

7.4.1 Import Host certificate:

1. Host certificate needs to be imported using USB.
2. After clicking on Import host certificate button following UI will be displayed:

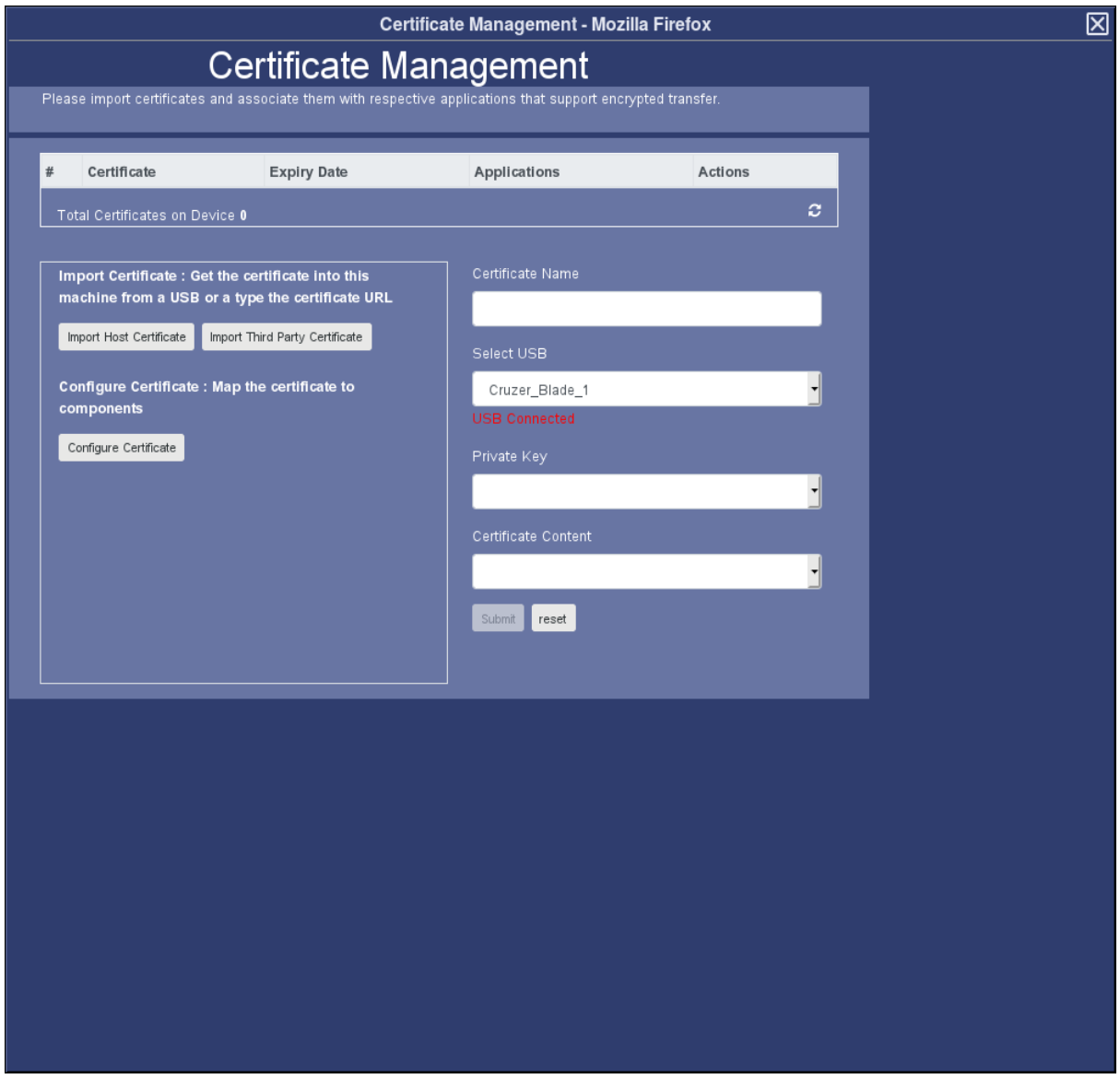


Figure 8: Certificate Management- Import Host Certificate

3. Enter certificate name.
4. select USB from dropdown
5. select the private key from dropdown
6. select the certificate content from dropdown and click on submit.
7. If certificate imported successfully then it will show success message.
8. The imported certificates will display in the table as shown below:

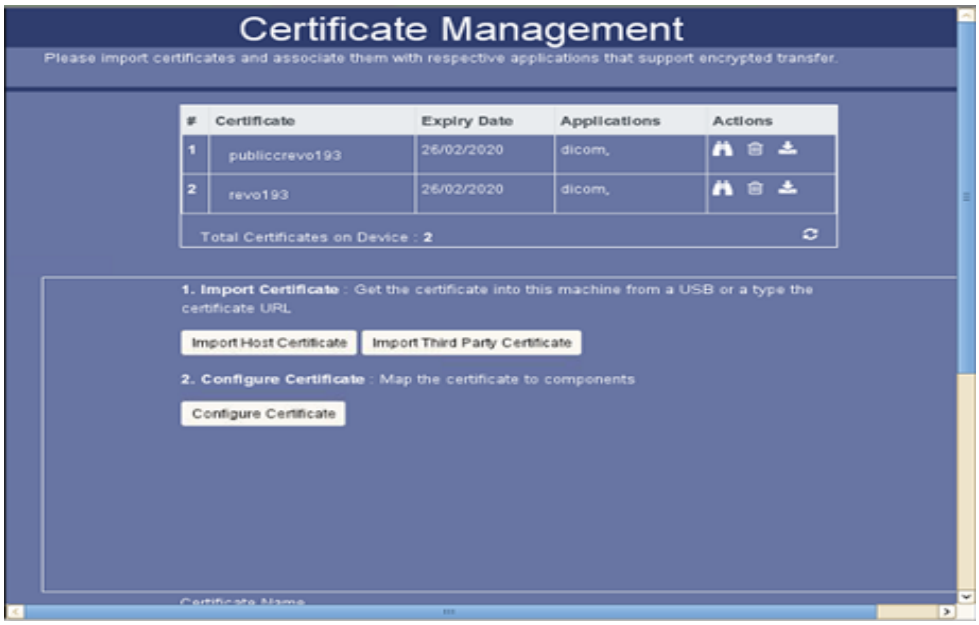


Figure 9: Certificate Management- Imported Host Certificate

7.4.2 Import Third-party certificate:

1. Third-Party certificates can be imported using USB or URL.
2. After clicking on the "Import Third party certificate" button below screen will be displayed:

Figure 10: Certificate Management- Import Third party Certificate

Steps to import Third party certificate using USB:

1. Enter certificate name.

2. Select USB from dropdown
3. Select the certificate content from dropdown and click on submit

Steps to import Third party certificate using URL:

1. Provide certificate name.
2. Provide certificate URL

7.5.Configuring certificate to Applications

After clicking on the Configure certificate below screen will be displayed.

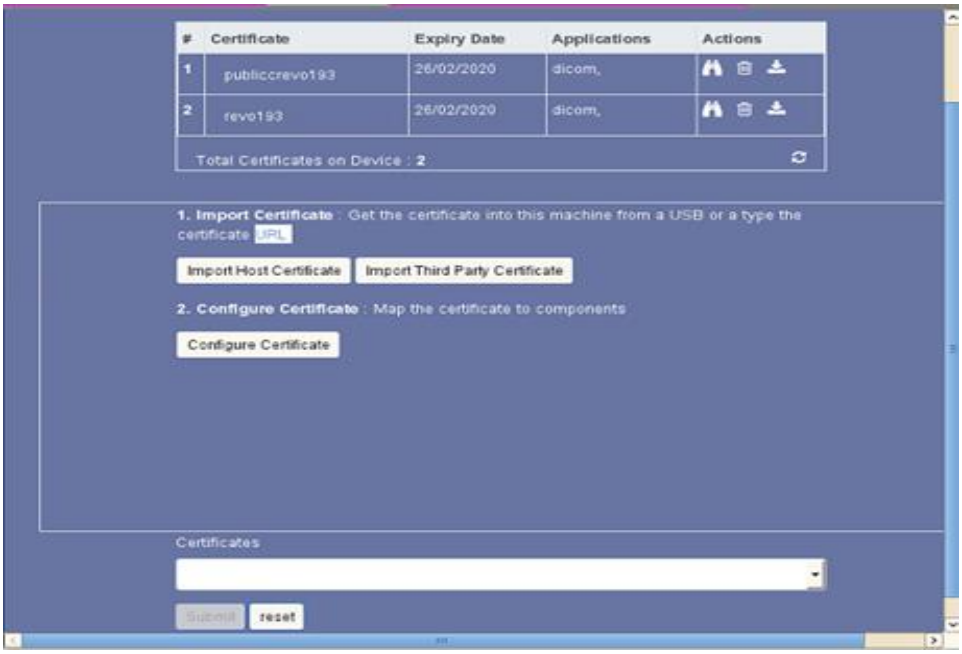


Figure 11: Configure Certificate

To configure certificates, select the certificate and check the checkbox to which application that particular certificate should be configured.

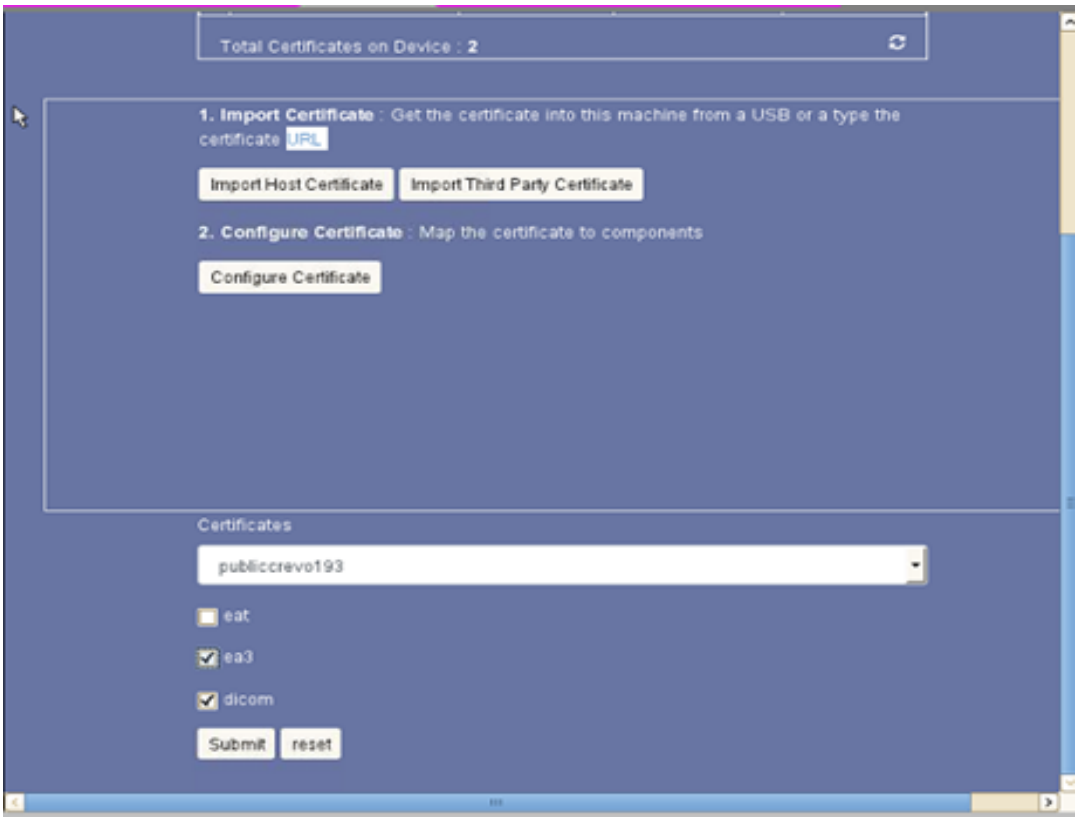
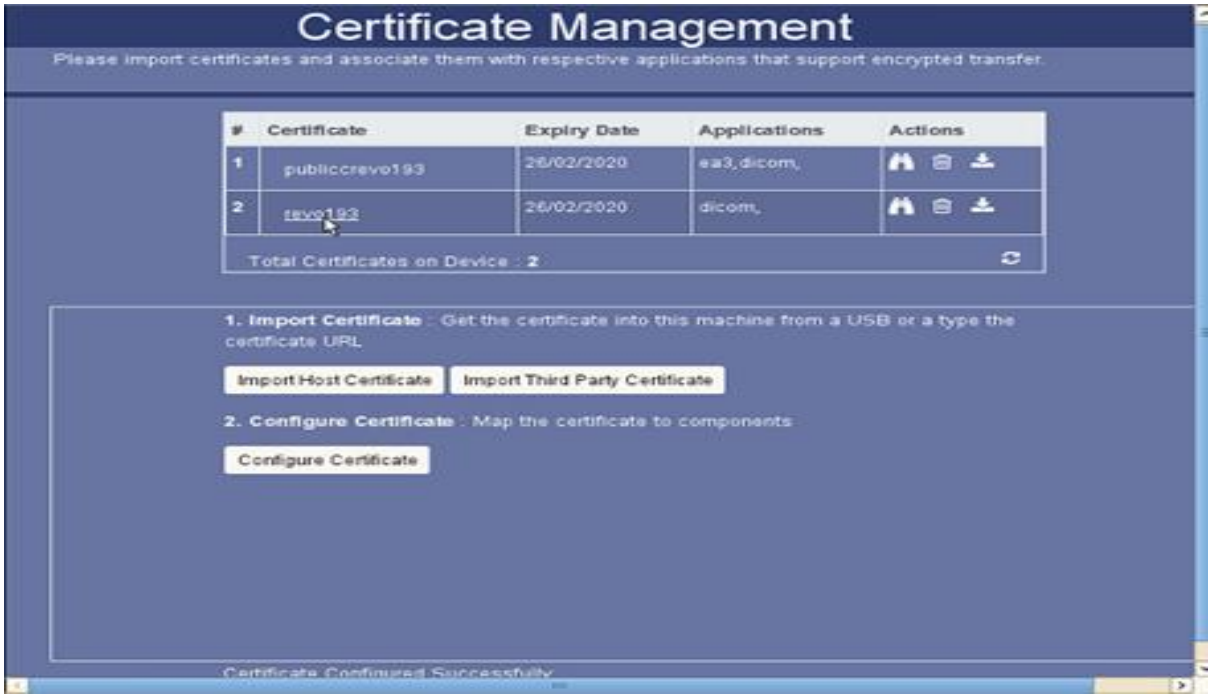


Figure 12: Configure Certificate -based on selection

After configuring it will display the success message and after refreshing the table the applications configured to particular certificates will display in the table.



7.6.View certificate screen:

After clicking on the view icon of any certificate below screen will display

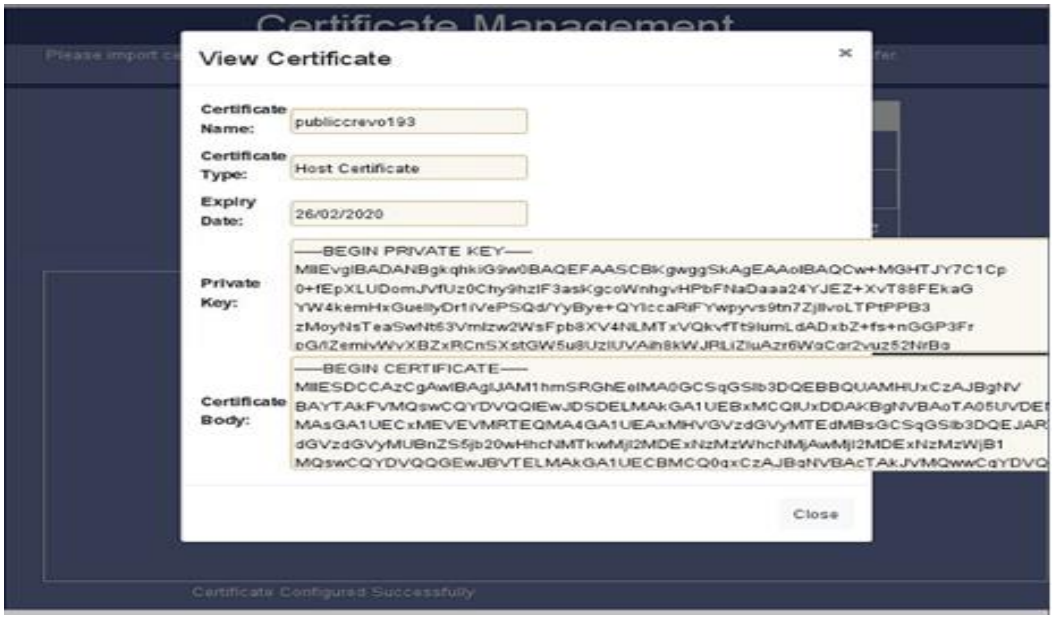


Figure 13: View Configured Certificates

7.7.Delete certificate screen:

After clicking on the delete icon of any certificate below screen will display

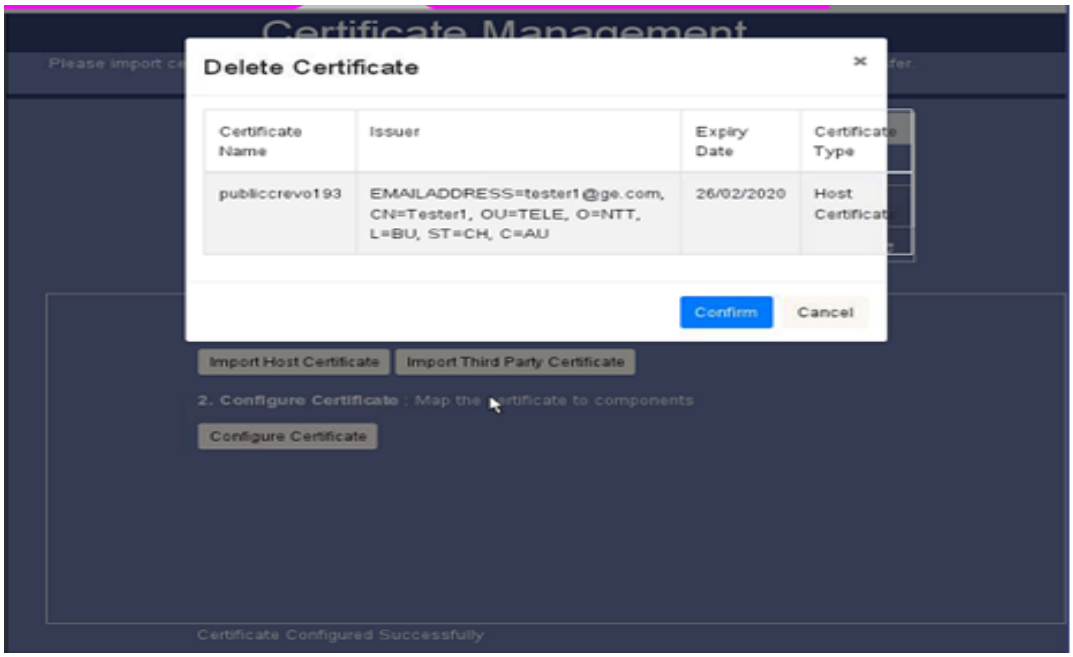
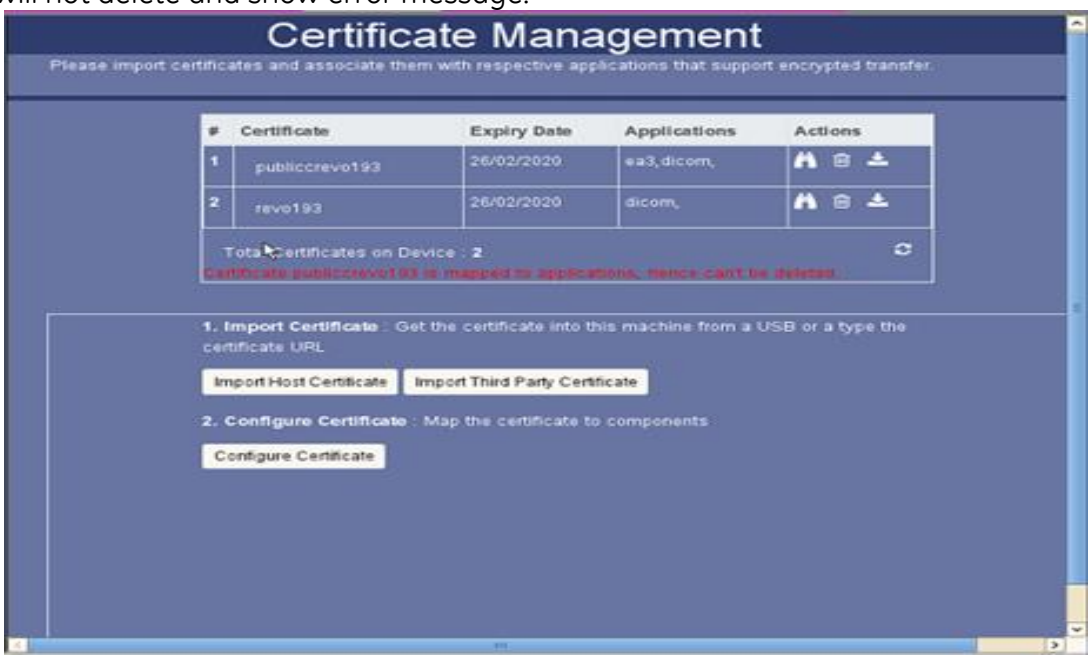


Figure 14: Delete Configured Certificates

Upon clicking on the confirm button, certificate will be deleted.

If certificate is configured to some applications and if we try to delete that certificate, it will not delete and show error message.



If we try to import already existing certificate it will display error message.

7.8.Configure a TLS capable DICOM network host

Follow the below steps to configure DICOM Image transfer over TLS.

1. From ImageWorks screen, select Tools >> Network Configuration

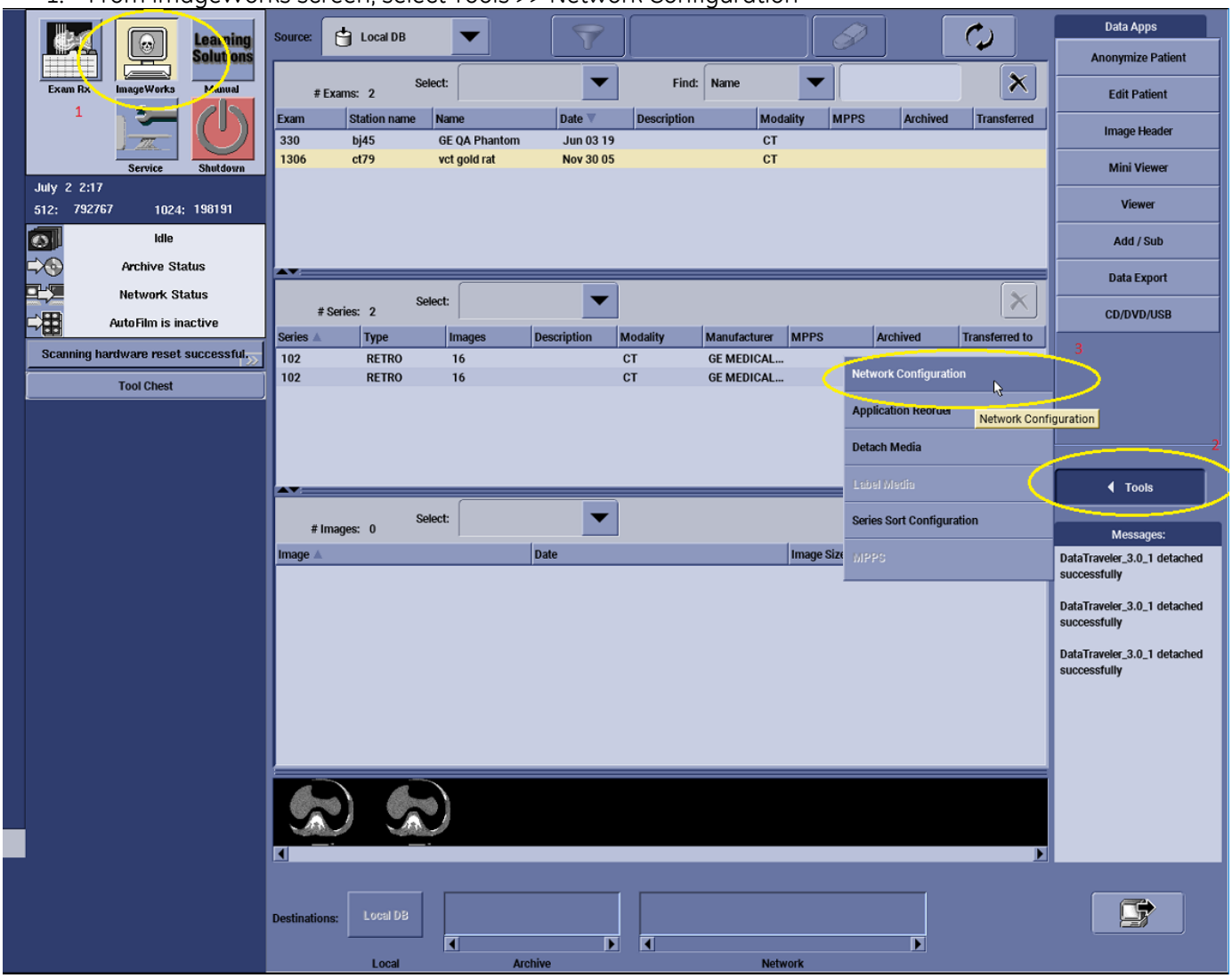


Figure 15: Configure TLS Capable DICOM Host

2. The following popup titled ***Configure Network Hosts*** dialog will get displayed:

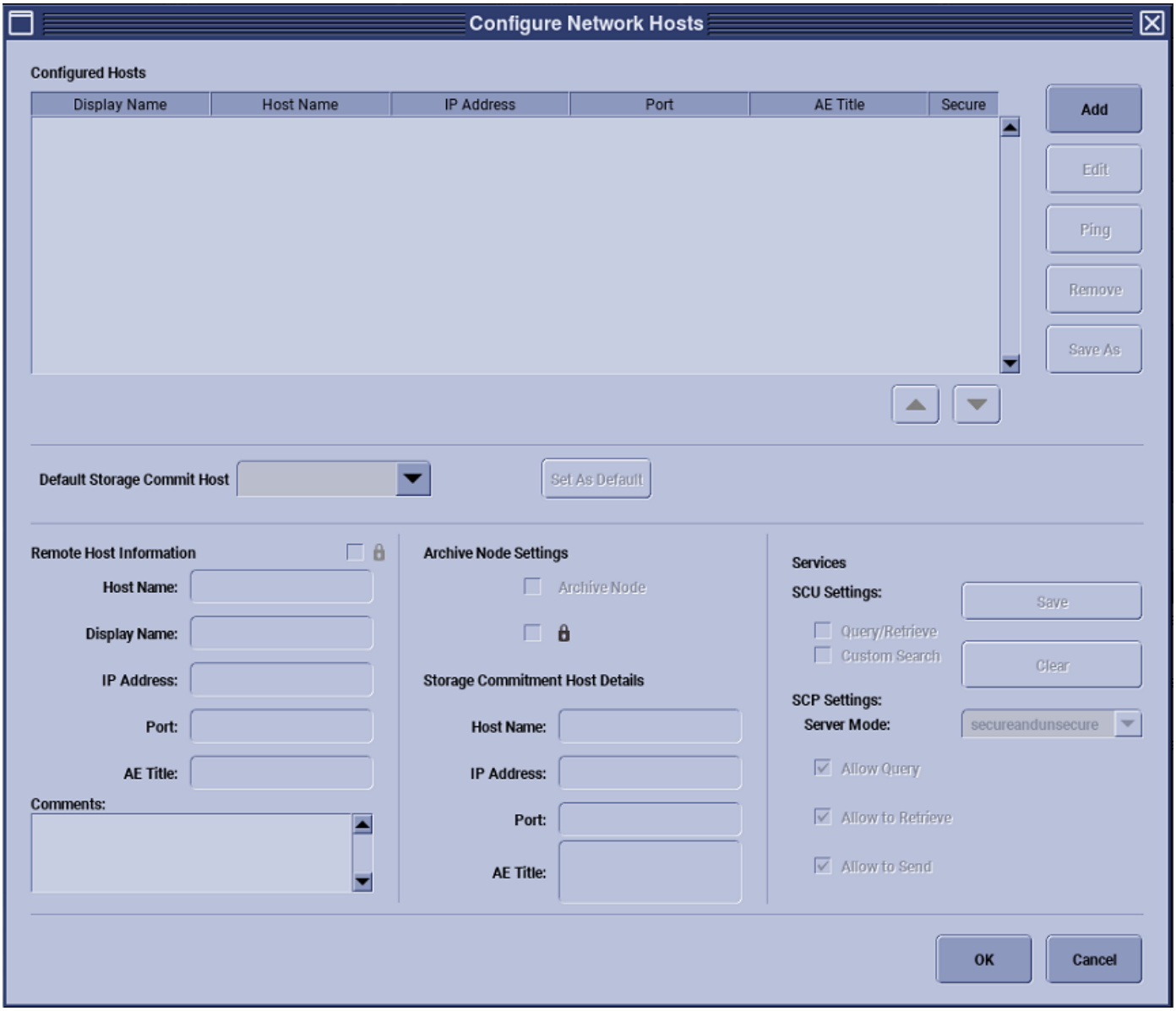


Figure 16: Configure Network Hosts

3. Click on ***Add*** button in the ***Configure Network hosts*** UI.

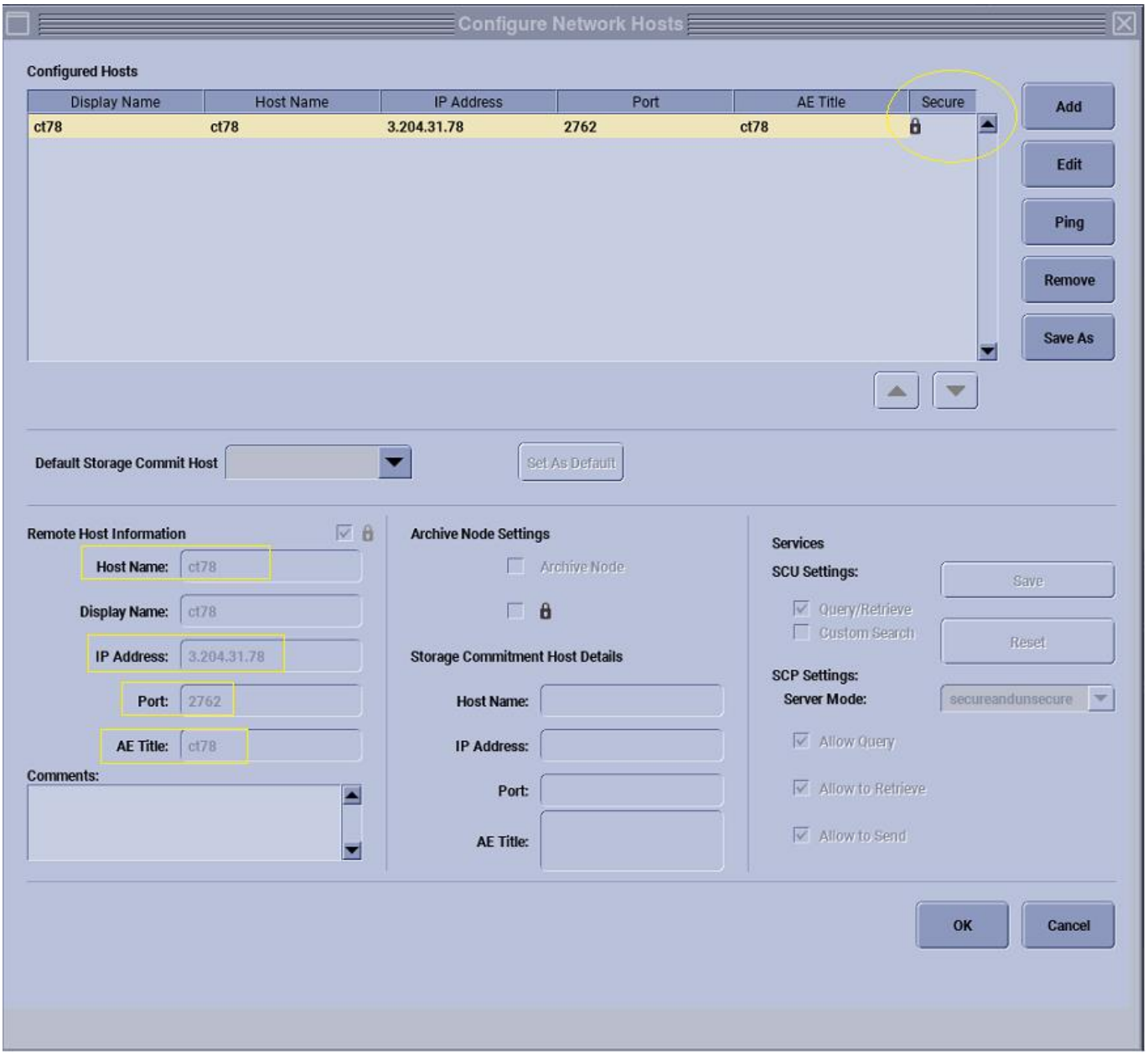


Figure 17: Configured Network Hosts

4. Select the ***Secure Lock*** ( ) checkbox under Remote Host Information.
5. Enter IPv4 address.
6. Enter ***Hostname***
7. Enter (or edit the default if needed) the ***Port*** number on which the remote DICOM TLS server is listening
8. Enter AE title
9. Click ok

10. Make sure the ***secure lock*** icon is displayed in the network host entry in the configured hosts list
11. Select configured network host entry and click on ***Ping***. Ensure that remote host is alive. select Exam/Series/Image and perform any network operation on the configured host

8. PROCEDURE TO RUN VULNERABILITY SCAN

Security Vulnerability scanning is done on the CT System using Nessus Security Center before release of the product. All Identified vulnerabilities are mitigated as appropriate based on risk they pose to the product.
Critical and High-risk vulnerabilities, if any, are mitigated before the software is released.
CT system in the target configuration would not allow any connections other than those from pre-configured IP address and ports/protocols. This will prevent vulnerability scanning on the CT system.
To generate a good vulnerability scan report, following steps are to be followed:

1. Login as Admin user from EA3 Login UI.
2. Open a Xterm
3. Become OS root user by executing “su – “
4. Execute the following command
   - /usr/g/.security/mc3/legacy_security/scripts/configVulnerabilityScan.sh --enable
5. Above command creates a temporary user called “vsuser” and password for that user account will be displayed at the command prompt
6. Use the vsuser and the password for configure the vulnerability scanner for vulnerability scanning
7. Note: Please note that above user's credentials will be valid for 2 days from the time of creation.
   Once Vulnerability Scan is complete, run the following command to remove the user and put system back to the original/factory settings

   - /usr/g/.security/mc3/legacy_security/scripts/configVulnerabilityScan.sh --disable

GE HC service engineer should contact GE if any critical issues are found.

For privacy and security concerns regarding GE products, please see http://www.ge.com/security

Product Vulnerability & Incident Reporting

Data & Network Security Reporting

To report a potential vulnerability or security incident involving a GE product, contact GE Product Security Incident Response Team (GE PSIRT) using the form below. Following submission, GE PSIRT will review the report and respond back with next steps. GE customers with questions or concerns regarding cyber vulnerabilities in a GE product may also contact GE PSIRT through this form.

To report a potential threat to GE's data or network, or if you believe you have discovered an incident involving either, contact GE Cyber Incident Response Team (GE CIRT) using the form below. GE CIRT will implement corrective action as appropriate.

Report a Product Issue

Report a Network Issue

9. PNF CONFIGURATION REQUIRED FOR CYBER SECURITY INSTALLATION

System Firewall:

1. System firewall must be turned "On" **at all times**.
2. To check the firewall status, perform the following:
   - Open Service Tools > Common Service Desktop (CSD)
   - Click on [Configuration] Tab and select [Configure PNF].
   - Confirm status of Firewall.

Figure 18: PNF Configuration

Any existing filters on the system will be displayed. Review and remove any filters that are not needed.

By default, all inbound connections are blocked by the CT System's internal firewall, with the exemptions listed in the table below.

The column "*Recommended configuration of network infrastructure*" describes the suggested configuration of the network infrastructure regarding the different network services.

Local port	Allowed Remote IP	Protocol	Recommended configuration of network infrastructure	Network service
4006	Any	TCP	Open to all HDO approved / authorized DICOM server(s) configured on the system. This is by default configured in the DICOM tab.	DICOM
8081*	Any	TCP	In PNF, Expert tab add new filter as below Name: ePO <Any name> Allowed IP: <Enter IPv4 address of ePO Server Allowed Port: <8081 or Agent Communication port> Protocol: TCP	McAfee ePO agent
2762	Any	TCP	Open to all HDO approved / authorized DICOM server(s) capable of TLS communication configured on the system.	DICOM over TLS
514*	Any	TCP	No PNF configuration needed on CT Console client side. Syslog-ng uses TCP port 514 (Default), User can configure different TCP port on the Server	Syslog-NG log transfer to remote Log Server

Table: Inbound firewall configuration for CT System

*Note that ports configured can be different from defaults listed above. Firewall configuration should be updated accordingly.

10. MALWARE PROTECTION

10.1. Overview

Anti-virus is a software used to prevent, detect, and remove malware / viruses.

McAfee Endpoint Security for Linux Threat Prevention as an option. Once installed, the Antivirus software starts protecting your CT system from threats. The software uses the latest anti-malware

engine from McAfee.

When enabled, the software checks for viruses, trojans, unwanted programs and other threats by scanning files and folders on local drives, network-mounted volumes and removable media whenever a file is created or accessed. On Access scans are disabled by default for performance reasons.

You can also run scans on demand. An on-demand scan can be initiated from the Security Center by clicking the Antivirus menu item in the left navigation area.

McAfee Endpoint Security (ENSL) is installed when "AntiMalware_McAfee_standalone" or "AntiMalware_McAfee_EPO" option is installed. ENSL can be configured to work in the two modes: Managed mode (i.e., with ePO Server) or Standalone mode (i.e., without ePO server). For managed systems - ePO administrator configures and manage the protection configuration policies using these servers.

- McAfee® ePolicy Orchestrator® (McAfee ePO™)
- McAfee® ePolicy Orchestrator® Cloud (McAfee ePO™ Cloud)

Following are the acronyms used in this section:

DAT: McAfee DAT Signature Database
ENSL: McAfee Endpoint Security for Linux
EPO: McAfee ePolicy Orchestrator
MSA: McAfee Security Agent

ENSL provides the following Virus Scan methods.

- **Custom On-Demand Scan**

  Custom On-Demand scan must be scheduled from EPO. It schedules a task defined by the user to scan on files and directories at specific times.

- **On-Access Scan**

  This type of scan is disabled because it causes high system load and affect CT functionalities.

- **Policy-Based On-Demand Scan client tasks** — Run a Quick Scan or Full Scan on the client from McAfee ePO. Configure the behavior of these scans in the policy settings for an on-demand scan

To integrate with ePO, additional configuration procedure is required in EPO side. Server-side procedure/methods for configuration of ePO Server are not in scope of this document and need to refer to McAfee Installation / Product Guide for details.

When ePO Server is configured, Virus signature database (DAT) should be updated or scheduled using ePO. Virus scans should also be scheduled from the ePO Server

WARNING: Antivirus scans on CT Scanners are compute intensive and takes significant amount CPU, memory and disk resources that can potentially interfere with normal operating functions of CT Scanners including but not limited to scan acquisition, calibrations and image reconstructions. Users might perceive significant slowness of the system if Antivirus scans are run in the background. It is recommended to not run Antivirus scanning when the system is used for normal clinical operations. The IT or hospital administrator responsible for Antivirus scans

must coordinate with technologists/users of the CT scanners for proper downtime to complete Antivirus scans.

When an user starts a patient scanning session by clicking the accept button and if the system detects an antivirus scan in the background, the system will first stop the antivirus scan before proceeding into patient scanning session.

10.2. Managed Mode (Manage from ePO Server)

10.2.1 Installation of Anti-Malware solution

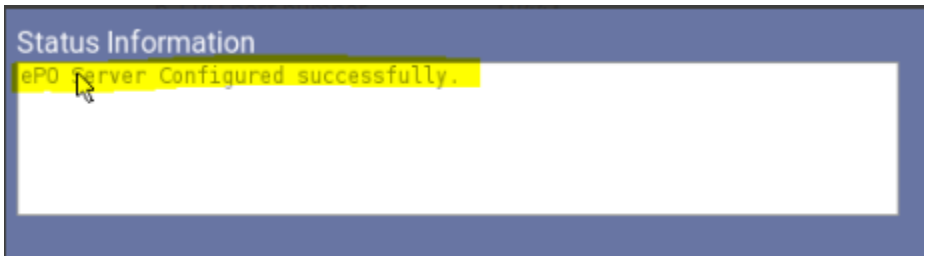
When "AntiMalware_McAfee_EPO" option is installed, McAfee Endpoint Security (ENSL) is installed by default.
For option installation please refer to the install option procedure.

10.2.2 Configure McAfee Agent for Managed Mode

1. Login as user with Administrator privileges in EA3
2. Launch Antivirus UI from Security Center. Click on Antivirus EPO Setup Tab

Figure 19: Antivirus EPO Setup

1. Fill in the following details
   - EPO server IP address : ePO IP Address
   - EPO port number : ePO port number
   - User Name : ePO server administrator Username>
   - EPO password : ePO server administrator Password>
2. Apply the configured EPO settings. Check the Status Information box



3. Login to the ePO server
4. Ensure that the configured system is listed in the system tree in ePO Server

Note:
McAfee Agent uses port 8081 and 8443 on EPO server and 8081 on CT for Agent-Client communication. Open port for access. Port can be configured in EPO server. If default port is not used, refer EPO server configuration and open appropriate port.

For managed systems, the configurations that you set using the command line is overwritten during the policy enforcement.

Refer to Firewall section on how to add ports 8081 and 8443 to whitelist in order to allow communication between ePO server and McAfee agent.

10.2.3 Schedule an On-Demand virus scan from ePO server

Refer to McAfee Installation / Product Guide for details on how to schedule an on-demand scan

Important Note:

- On-demand scan will take 15-30 min (depends on system load, number of files) if scan all files under / directory. Scan will be aborted if system is shutdown or rebooted during scan
- Virus Scan consumes amount of CPU resources and it may affect CT system performance (slowdown, etc). Consider when Virus Scan is executed.
- Virus Scan result can be queried and report can be created on ePO.

  ePo > Queries & Reports
- On-demand scan will be executed during a patient exam

10.2.4 Schedule creation for Virus Signature (.DAT file) update on ePO Server

Refer to McAfee Installation / Product Guide for details on how to schedule an on-demand scan

Note: Master Repository shall be updated daily as Server Task. It is scheduled as default but need to review Server Task Log and confirm DAT is latest on Dashboard.

10.3. Standalone license mode (when ePO server doesn't exist)

10.3.1 Installation of Anti-Malware solution

When "AntiMalware_McAfee_standalone" option is installed, McAfee Endpoint Security (ENSL) is installed by default with a full license.

10.3.2 Launching McAfee Agent in Stand-alone Mode

1. Login as user with Administrator privileges in EA3
2. Launch Antivirus UI from Security Center. Click on Antivirus Non-EPO Setup Tab

Figure 20: Launching Antivirus application in Stans-alone mode

10.3.3 Stand-alone Mode Cron jobs

When "AntiMalware_McAfee_standalone" option is installed, a weekly cron job is scheduled to run the antivirus scans and engine & DAT updates.

The user can specify the antivirus scan time by running /usr/g/scripts/schedule_antivirus.sh. The default scan time is 3:00 AM every Friday.

10.3.4 Start Anti-virus scan manually

1. Login as user with Administrator or GE Service privileges in EA3
2. Launch Antivirus UI from Security Center. Click on Antivirus Scan Tab

3. Click on Start Scan

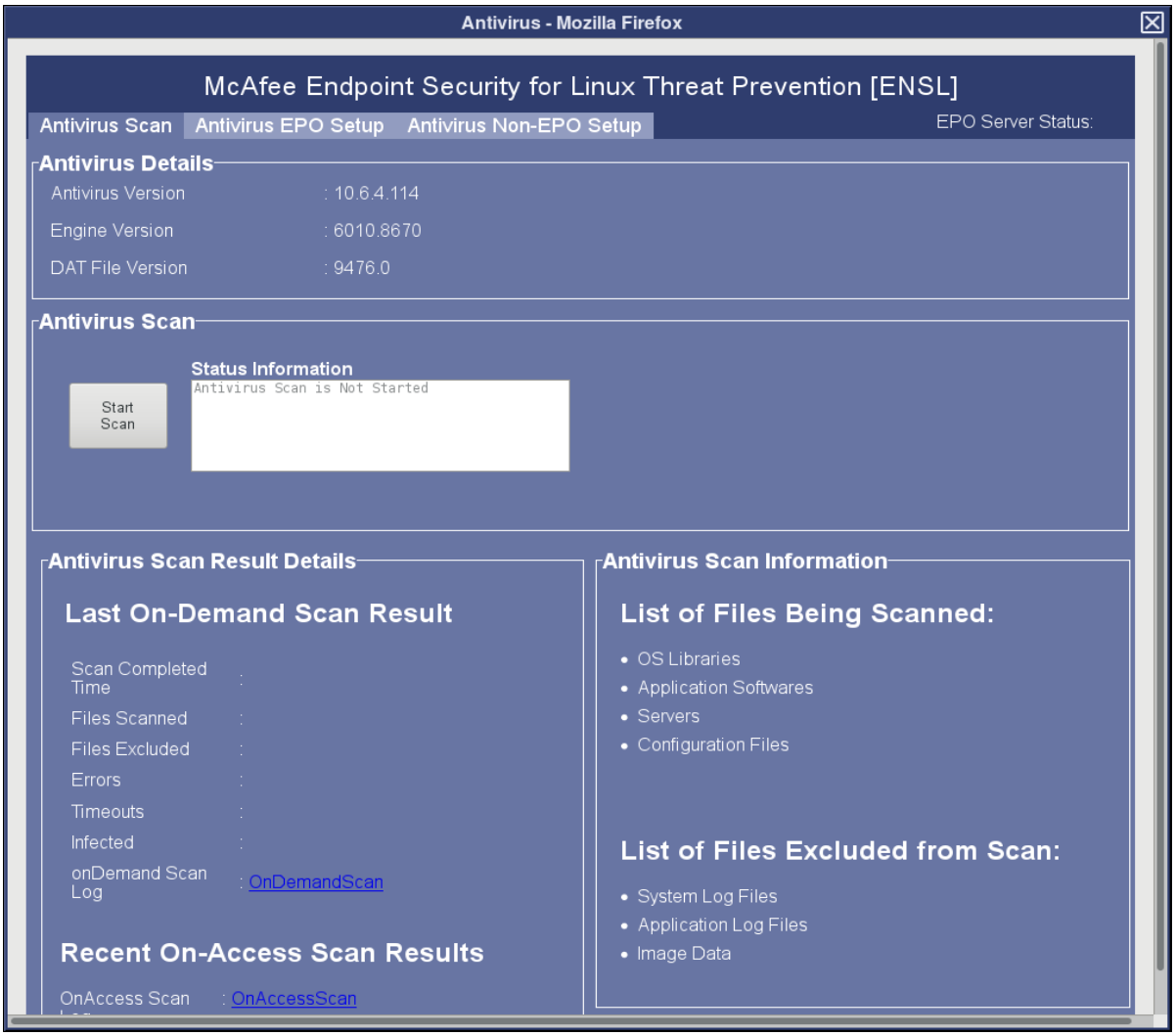


Figure 21: Start Anti-virus scan in Standalone mode

4. Once user click on “Start Scan” , Anti-virus scan will be running state

Figure 22: Anti-virus scan is running in Standalone mode

Anti-virus scan will take 30min ~1 Hour or more based on System available resources. Please wait to complete anti-virus scan

5. Once Virus scan completed, message “Antivirus scan is completed” will be shown in Status Information pane.

Figure 23: Anti-virus scan completed in Standalone mode

If any virus detected during anti-virus scan, then it will through attention pop-up with following message "WARNING: VIRUSES WERE DETECTED. Call GE Service


Attention
WARNING: VIRUSES WERE DETECTED. Call GE Service
OK