keyon

true-Xtender
Luna SA Monitor Service

Manual

Release 2.2.0

Unleash Microsoft PKI

Version	Autor	Date	
2.2.0	Keyon	January 2016	Release 2.2.0 with Luna SA 6 support

Content

1 Overview

1.1 What is the keyon / Luna SA Monitor Service

The Luna SA Monitor Service is a Windows Service for the observation of Luna SA HSM Slots which are used in the High-Availability mode.

The Luna SA Monitor Service observes each member of a HA group and logs its status to the Windows Application Event Log.

In addition to the observation of the network availability of the HSM Slots, the Luna SA Monitor Service also checks the private key access of a certificate. A signature test is performed using the Luna SA Crypto-Service Provider or the SafeNet Key Storage Provider for a specified key on an HSM slot and the result is logged to the Windows Application Event Log.

1.2 General Design

The Luna SA Monitor Service is running as a Windows Service and does periodically execute the Luna SA Monitor Processes. All log entries are written to the Windows Application Event Log.

1.3 Release Notes 2.1.0

SHA-2 support

SHA-2 is used as Hash algorithm for the signature check of CNG keys. SHA-1 is used as Hash algorithm for the signature check of legacy CSP keys.

1.4 Release Notes 2.2.0

Luna SA 6 support

The PKCS#11 cryptoki Library of the Luna SA 6 client is now supported. Older version as Luna SA 4 or Luna SA 5 are still supported in legacy mode.

2 Installation

2.1 Prerequisites

2.1.1 Operating System

One of the following operating system is installed:

- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

2.1.2 .Net Framework

The following Software is installed on the server:

- Microsoft .Net Framework 4.5.1

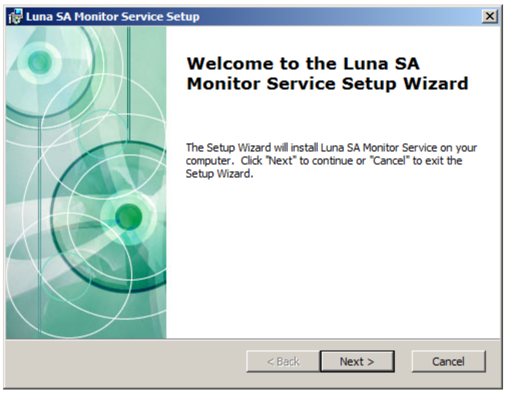
2.2 Installation Luna SA Monitor Service

2.2.1 Execute Installer Package

The keyon / Luna SA Monitor Service is shipped as a Windows Installer (MSI) package. Simply double click the installation file provided.

The installation is then started and shows mainly the following four screens:

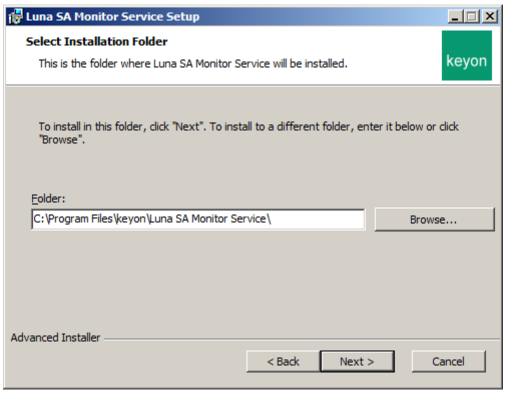
1.



Welcome to the Luna SA Monitor Service Setup Wizard

The Setup Wizard will install Luna SA Monitor Service on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

2.



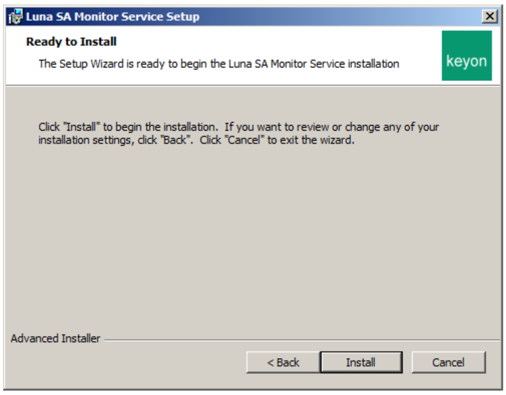
Select Installation Folder

This is the folder where Luna SA Monitor Service will be installed.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\keyon\Luna SA Monitor Service\

3.

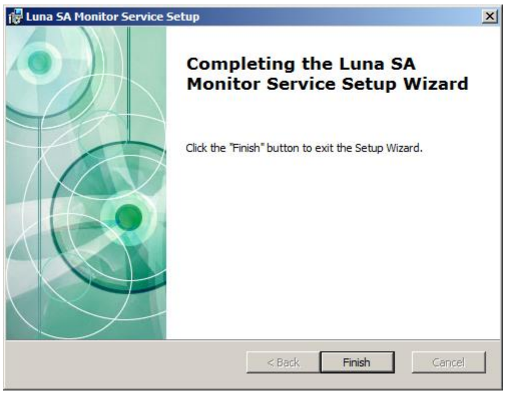


Ready to Install

The Setup Wizard is ready to begin the Luna SA Monitor Service installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

4.



Completing the Luna SA Monitor Service Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

You can use *Add or Remove Programs* in the Windows control panel to repair or remove the keyon / Certificate Luna SA Monitor Service installation.

2.2.2 XML Configuration

Navigate to the installation location of the Luna SA Monitor Service and open the “config” Folder.

Rename the file “LunaSAMonitorConfiguration.xml_new” to “LunaSAMonitorConfiguration.xml” and rename the file “LunaSAMonitorConfiguration.xsd_new” to “LunaSAMonitorConfiguration.xsd”.

2.2.3 License file

Copy the license file to the installation location of the Luna SA Monitor Service.

2.2.4 Luna SA PKCS#11 Libary

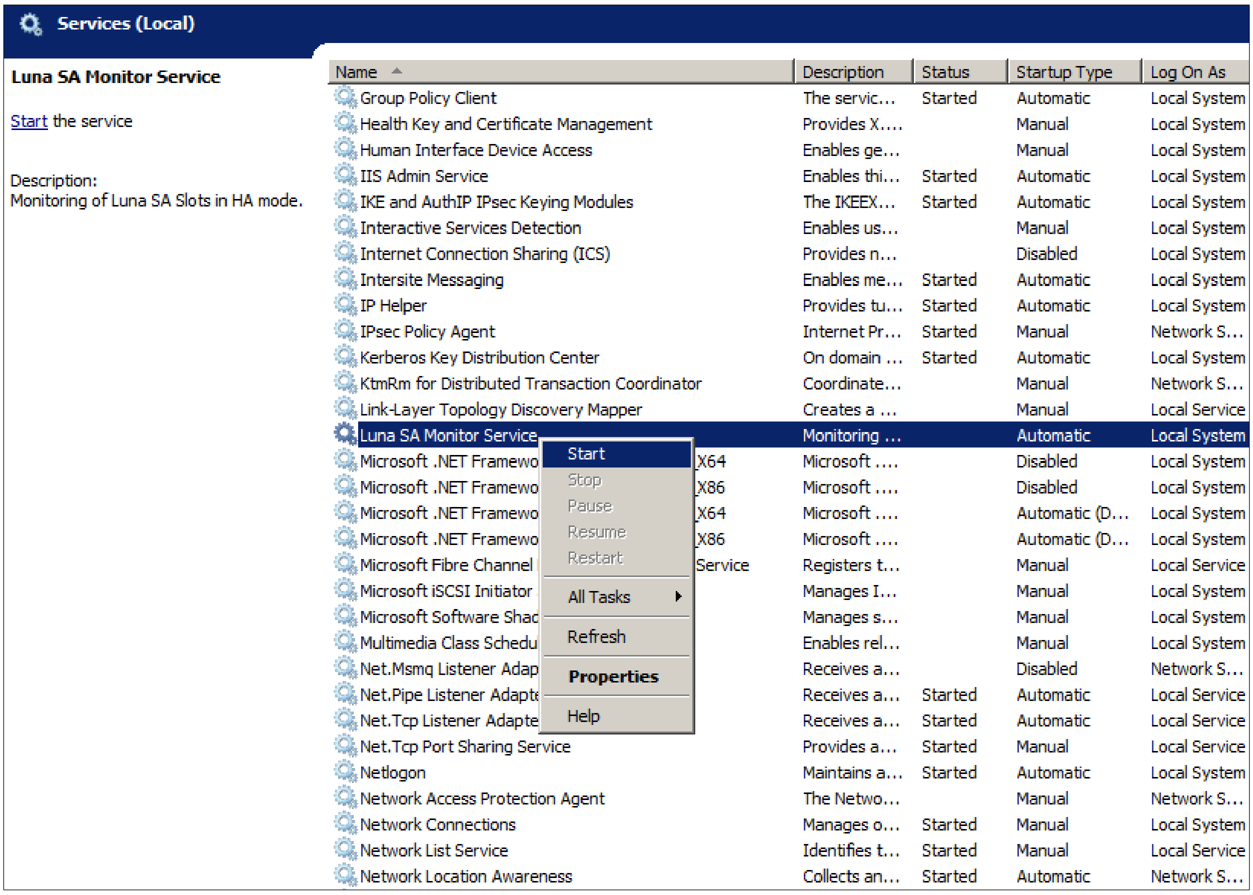
Create a copy of the Luna SA PKCS#11 Library (in most cases C:\Program Files\SafeNet\LunaClient\crystoki.dll) and name it keyon_lunasa_monitor.dll. This copied PKCS#11 library must be referenced in the configuration as described in chapter 3.1.1.

2.2.5 Windows Service Configuration

Open the Windows Services View of the server (start → Administrative Tools → Services) and select the Luna SA Monitor Service.

Check that the Luna SA Monitor service runs under NT Authority/System resp. the local system account.

Start the Luna SA Monitor Service in the Windows Service View.



Luna SA Monitor Service

Start the service

Description:
Monitoring of Luna SA Slots in HA mode.

Name	Description	Status	Startup Type	Log On As
Group Policy Client	The servic...	Started	Automatic	Local System
Health Key and Certificate Management	Provides X....		Manual	Local System
Human Interface Device Access	Enables ge...		Manual	Local System
IIS Admin Service	Enables thi...	Started	Automatic	Local System
IKE and AuthIP IPsec Keying Modules	The IKEEX...	Started	Automatic	Local System
Interactive Services Detection	Enables us...		Manual	Local System
Internet Connection Sharing (ICS)	Provides n...		Disabled	Local System
Intersite Messaging	Enables me...	Started	Automatic	Local System
IP Helper	Provides tu...	Started	Automatic	Local System
IPsec Policy Agent	Internet Pr...	Started	Manual	Network S...
Kerberos Key Distribution Center	On domain ...	Started	Automatic	Local System
KtmRm for Distributed Transaction Coordinator	Coordinate...		Manual	Network S...
Link-Layer Topology Discovery Mapper	Creates a ...		Manual	Local Service
Luna SA Monitor Service	Monitoring ...		Automatic	Local System
Microsoft .NET Framewo X64	Microsoft		Disabled	Local System
Microsoft .NET Framewo X86	Microsoft		Disabled	Local System
Microsoft .NET Framewo X64	Microsoft		Automatic (D...	Local System
Microsoft .NET Framewo X86	Microsoft		Automatic (D...	Local System
Microsoft Fibre Channel Service	Registers t...		Manual	Local Service
Microsoft iSCSI Initiator	Manages I...		Manual	Local System
Microsoft Software Shac	Manages s...		Manual	Local System
Multimedia Class Schedu	Enables rel...		Manual	Local System
Net.Msmq Listener Adap	Receives a...		Disabled	Network S...
Net.Pipe Listener Adapte	Receives a...	Started	Automatic	Local Service
Net.Tcp Listener Adapte	Receives a...	Started	Automatic	Local Service
Net.Tcp Port Sharing Service	Provides a...	Started	Manual	Local Service
Netlogon	Maintains a...	Started	Automatic	Local System
Network Access Protection Agent	The Netwo...		Manual	Network S...
Network Connections	Manages o...	Started	Manual	Local System
Network List Service	Identifies t...	Started	Manual	Local Service
Network Location Awareness	Collects an...	Started	Automatic	Network S...

Open the Event Viewer (start → Administrative Tools → Event Viewer) and check the Windows Application Log for Information / Warning / Error Logs of the Luna SA Monitor Service.

3 Configuration

The entire configuration of the Luna SA Monitor Service is configured in an XML configuration file.

3.1 XML Configuration Settings

The following settings have to be configured for the Luna SA Monitor Service:

- Service Configuration
- Monitor Configuration List
- Service Event Log Configuration

3.1.1 Service Configuration

Setting	Description

Pkcs11 Library Path	Defines the path to the SafeNet Luna SA Cryptoki library.
	Example:
	`<Pkcs11LibraryPath>`
	`  C:\Program Files\LunaSA\keyon_lunasa_monitor.dll`
	`</Pkcs11LibraryPath>`

Pkcs11 Library Legacy Mode	Defines whether the referenced Luna SA Cryptoki library is version 4 or 5 (Legacy mode) or version 6.
	Example:
	`<Pkcs11LibraryLegacyMode>`
	`  true`
	`</Pkcs11LibraryLegacyMode>`

Scheduler Cron Pattern	Defines the execution time interval of the monitor process. See chapter 3.3 for a detailed description of the scheduler cron pattern.
	Example:
	`Service starts the process execution all 30 minutes.`
	`<SchedulerCronPattern>0 0 0/1 * * ?</SchedulerCronPattern>`

License File Path	Defines the path to the license file.
	Example:
	`<LicenseFilePath>`
	`  C:\Program Files\keyon\Luna SA Monitor Service\config\license.pem`
	`</LicenseFilePath>`

3.1.2 Monitor Configuration List

The Monitor Configuration List must contain at least one monitor configuration.

3.1.2.1 Monitor Config

Setting	Description

HA Group Identifier	The identifier of the HA group. This can be the label or the serial number of the HA group.
	Example:
	`The label of the HA group is "HATestGroup"`
	`<HAGroupIdentifier>HATestGroup</HAGroupIdentifier>`

Warning Treshold	The threshold for members of HA group with failed state from which the log level warning is used. Example: `<WarningTreshold>1</WarningTreshold>`
Error Treshold	The threshold for members of HA group with failed state from which the log level error is used. Example: `<ErrorTreshold>2</ErrorTreshold>`
Key Identifier List	The list of key identifier elements as described in next section. Example:

3.1.2.2 Key Identifier List

Setting	Description

Key Identifier	The serial number of the certificate in local computer store to perform a signature test.
	Example:
	`The serial number of the certificate in local computer store is 716ff2001f83ef894bdae984088a56fc`
	`<KeyIdentifier>`
	`  716ff2001f83ef894bdae984088a56fc`
	`</KeyIdentifier>`

3.1.3 Service Event Log Configuration

Setting	Description

EventLogSourceName	Defines the Event Log source name
	Example:
	`The Event Log source name is "Luna SA Monitor Service"`
	`<EventLogSourceName>`
	`      Luna SA Monitor Service`
	`</EventLogSourceName>`

EventLogDestinationName	Defines the Event Log destination name
	Example:
	`The Event Log destination name is Application`
	`<EventLogDestinationName>`
	`      Application`
	`</EventLogDestinationName>`

3.2 XML Configuration Example

```
<LunaSAMonitorServiceConfiguration>
       <ServiceConfig>
             <Pkcs11LibraryPath>C:\Program Files\LunaSA\keyon_lunasa_monitor.dll
             </Pkcs11LibraryPath>
             <Pkcs11LibraryLegacyMode>true </Pkcs11LibraryLegacyMode>
             <SchedulerCronPattern>0 0 0/1 * * ?</SchedulerCronPattern>
       </ServiceConfig>

    <MonitorConfigurationList>
         <MonitorConfig>
               <HAGroupIdentifier>HaTestGroup</HAGroupIdentifier>
               <WarningTreshold>1</WarningTreshold>
               <ErrorTreshold>1</ErrorTreshold>
               <KeyIdentifierList>
                    <KeyIdentifier>12ecd0aec368b1bd4ec9a5b5023222af</KeyIdentifier>
               </KeyIdentifierList>
         </MonitorConfig>
       </MonitorConfigurationList>

       <ServiceEventLogConfig>
             <EventLogSourceName>Luna SA Monitoring Service</EventLogSourceName>
             <EventLogDestinationName>Application</EventLogDestinationName>
       </ServiceEventLogConfig>
</LunaSAMonitorServiceConfiguration>
```

3.3 Scheduler Cron Pattern Configuration

The Luna SA Monitor Service is using the Quartz Library to schedule the monitor process. The cron pattern is based on the well-known Unix Tool. Scheduling capabilities of cron are powerful and proven. Detailed information about the cron pattern ans its configuration scope can be found here:

http://quartz-scheduler.org/documentation/quartz-2.1.x/tutorials/crontrigger

3.3.1 Format

A cron expression is a string comprised of 6 or 7 fields separated by white space. Fields can contain any of the allowed values, along with various combinations of the allowed special characters for that field. The fields are as follows:

Field name	Mandatory	Allowed Values	Allowed Special Characters
Seconds	YES	0-59	, - * /
Minutes	YES	0-59	, - * /
Hours	YES	0-23	, - * /
Day of month	YES	1-31	, - * ? / L W
Month	YES	1-12 or JAN-DEC	, - * /
Day of week	YES	1-7 or SUN-SAT	, - * ? / L #
Year	NO	empty, 1970-2099	, - * /

3.3.2 Examples

Field name	Mandatory
0 0 12 * * ?	Fire at 12pm (noon) every day
0 15 10 ? * *	Fire at 10:15am every day
0 0/5 * * * ?	Fire every 5 minutes.
0 0 0/1 * * ?	Fire every hour.

4 Logging

The Luna SA Monitor Service logs all actions to the Windows Application Event Log.

4.1 Log Entries

The event log source name and the event log destination name can be configured via the XML Configuration (see chapter 0). The following table describes the Event Log IDs, used by the Luna SA Monitor Service.

Event Log ID	Log Level	Description
1	Info	Luna SA Monitor processor is scheduled for next execution at <execution time>.
10	Info	The status for token with identifier <identifier>is: Member with serial 951389011 has status: OK Member with serial 951389001 has status: OK Elapsed time for monitoring token with identifier <identifier> is <execution time>.
11	Info	Successfully checked private key access for identifier <identifier>with subject name <subject name>. Elapsed time for private key access check for identifier <identifier> is <execution time>.
101	Warning	The status for token with identifier <identifier> is: Member with serial 951389011 has status: OK Member with serial 951389001 has status: TOKEN_NOT_PRESENT Elapsed time for monitoring token with identifier <identifier> is <execution time>.
201	Error	The status for token with identifier <identifier> is: Member with serial 951389011 has status: TOKEN_NOT_PRESENT Member with serial 951389001 has status: TOKEN_NOT_PRESENT Elapsed time for monitoring token with identifier <identifier> is <execution time>.
202	Error	Failed to check private key access for identifier <identifier>. Elapsed time for private key access check for identifier <identifier> is <execution time>.

4.2 Monitoring the service

It is recommended to monitor the Windows Application Event Log entries described in chapter 4.1

Most monitoring solutions support the tracking of windows event log entries.

If no monitoring solution is in place, the Windows Task Scheduler can be used to track windows event log entries and execute different actions, for example sending emails.