Preface

© 2012 SafeNet, Inc. All rights reserved.

Part Number: 007-011498-001 (Rev A, 05/2012)

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of SafeNet.

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address below.
SafeNet, Inc.

4690 Millennium Drive
Belcamp, Maryland 21017
USA

Limitations

This document does not include the steps to set up the third-party software. The steps given in this document must be modified accordingly. Refer to Luna SA documentation for general Luna setup procedures.

Disclaimers

The foregoing integration was performed and tested only with the specific versions of equipment and software and only in the configuration indicated. If your setup matches exactly, you should expect no trouble, and Customer Support can assist with any missteps. If your setup differs, then the foregoing is merely a template and you will need to adjust the instructions to fit your situation. Customer Support will attempt to assist, but cannot guarantee success in setups that we have not tested.

Technical Support

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, please contact your supplier or SafeNet support.

SafeNet support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Technical Support Contact Information:
Phone: 800-545-6608, 410-931-7520
Email: support@safenet-inc.com
# Table of Contents

**Preface** .............................................................................................................................................................. i  
**Chapter 1 Introduction** ........................................................................................................................................ 1  
Luna SA Setup: ......................................................................................................................................................... 2  
**Chapter 2 Integrating MS Forefront Unified Access Gateway 2010 with Luna SA** .................. 3  
Generating a SSL Certificate used for HTTPS trunk configuration using Luna Cryptographic Service Provider (CSP) .............................................................................................................................. 4
Chapter 1
Introduction

This document outlines the steps to configure and integrate Microsoft Forefront Unified Access Gateway 2010 with Luna SA.

Microsoft Forefront Unified Access Gateway 2010 (UAG) delivers comprehensive, secure remote access to corporate resources for employees, partners, and vendors on both managed and unmanaged PCs and mobile devices. Utilizing a combination of connectivity options, ranging from SSL VPN to DirectAccess, as well as built in configurations and policies, UAG provides centralized and easy management of an organization’s complete anywhere access offering.

Microsoft Forefront Unified Access Gateway 2010 will use the Luna SA Cryptographic Service Provider (CSP) to store the SSL keys on Luna SA HSM.

Scope
3rd Party Application Details

- Microsoft Forefront Unified Access Gateway 2010

Supported Platforms

The following platforms are supported for Luna SA:

- Windows Server 2008 R2 (running on Microsoft Hyper-V and VMWare ESXi v4.1.0)

HSM and Firmware Version

- K6 HSM f/w 6.2.1 (Luna SA v5.1)

Distributions

- Luna SA 1U Appliance s/w 5.1
- Luna SA Client s/w v5.1 (64-bit)
Prerequisites

Luna SA Setup:

Please refer to the Luna SA documentation for installation steps and details regarding configuring and setting up the box on Windows systems. Before you get started ensure the following:

- Luna SA appliance and a secure admin password
- Luna SA, and a hostname, suitable for your network
- Luna SA network parameters are set to work with your network
- Initialize the HSM on the Luna SA appliance
- Create and exchange certificates between the Luna SA and your "Client" system (registered the Client with the Partition).
- Create a partition on the HSM and remember the partition password that will be later used by the SQL Server 2008 R2. Run the command, vtl verify to display a partition from Luna SA. The general form of command is C:\Program Files\Luna SA > vtl verify.
- Enable Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to Luna SA with Trusted Path Authentication [which is FIPS 140-2 level 3] only).
Chapter 2
Integrating MS Forefront Unified Access Gateway 2010 with Luna SA

This chapter outlines the steps to install and integrate Microsoft Forefront Unified Access Gateway 2010 with Luna SA.

Before You Begin

Setup
- The setup consists of two systems in a private network as per the table below:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Applications and Services</th>
<th>Description</th>
<th>Computer Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server® 2008 R2</td>
<td>Active Directory, Domain Name System (DNS), Active Directory Certificate Services</td>
<td>Domain Controller DNS, Certificate Authority</td>
<td>UAG-DC</td>
</tr>
<tr>
<td>Enterprise</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server® 2008 R2</td>
<td>Microsoft Forefront Unified Access Gateway 2010</td>
<td>UAG Server</td>
<td>UAG-SRV</td>
</tr>
<tr>
<td>Enterprise</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **UAG-DC** is configured as domain controller with domain LunaUAG.com and a Certificate Authority with Certification Authority Web Enrollment and Certificate Enrollment Web Services.
- Join **UAG-SRV** to the LunaUAG.com domain.
- Install the UAG2010 on **UAG-SRV**. To install the UAG2010 please refer the Microsoft documentation or the following link: [http://technet.microsoft.com/en-us/library/gg502549](http://technet.microsoft.com/en-us/library/gg502549)

**Note**: After installation and initial configuration of UAG 2010, you need to create a new access rule using TMG Management Console to communicate with Luna SA on the port 1792.
Generating a SSL Certificate used for HTTPS trunk configuration using Luna Cryptographic Service Provider (CSP)

Create a certificate request using Luna CSP

1. Log on to the **UAG-DC** as a Domain Administrator.

2. Open the Server Manager and expand Roles-> Active Directory Certificate Services console.

3. Click on Certificate Templates and locate Web Server template in the Template Display Name.

4. Right click on the Web Server template and select Duplicate Template.

5. Select Windows Server 2003 enterprise and click OK.

6. Enter the name UAG in the Template Display name.

7. On the Request Handling tab, click on CSPs and select “Request can use any CSP available on the subject’s computer”.

8. Click OK twice to finish.

9. Click on the Start-> Administrative Tools-> Certificate Authority and double click on the server name to expand the tree.


11. Select the custom certificate template created above i.e. UAG and click OK.

12. Double click on the Certificate Template and verify that UAG is added in the list.

13. Log on to the **UAG-SRV** as Domain Administrator.

14. Open the MMC (Microsoft Management Console) window and click File-> Add/Remove Snap-in.

15. Select Certificates and click Add.


17. Select “Local Computer” and click Finish.

18. Click OK and navigate to "Certificates (Local Computer) " -> "Personal" -> "Certificates"

19. Click on the right area where the certificates are shown.

20. Right click -> "All Tasks" -> "Advanced Operations" -> "Create Custom Request"

21. "Next" -> select "Active Directory Enrollment Policy" -> "Next"

22. Select the custom created certificate template from the drop-down menu i.e. UAG.

23. "Next" -> "Details" -> "Properties"

24. Insert a "General Name" (Friendly Name) and a "Description" in the "General" Tab

25. Add a "Common Name" on the "Subject" Tab
26. Select the "Luna Cryptographic Services Provider" on the Private Key Page.

27. Click OK to close the window and then click Next.

28. Click Browse and Save the base64 encoded certificate request in a file.

**Installing the certificate**

After creating the certificate request, open the CA web interface and submit the request to the CA.

1. Open the browser and type http://UAG-DC/certsrv. Provide username and password for authentication.
2. Click on Request a certificate -> Advanced Certificate Request -> Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
3. Paste the certificate request under Saved Request and Select Certificate Template, click Submit.
4. Download the certificate and save the certificate.
5. Open the MMC and click File-> Add/Remove Snap-in.
6. Select Certificates and click Add.
7. Select "Computer Account" and click Next.
8. Select "Local Computer" and click Finish.
9. Click OK and navigate to "Certificates (Local Computer)" -> "Personal" -> "Certificates"
10. Right click on the Certificates-> All Tasks-> Import.
11. Click Next, Browse and select the downloaded certificate.
12. Click Next, Select certificate store as Personal click Next and then Finish to Import the certificate.
Creating a HTTPS trunk

1. Open the Microsoft UAG management console on UAG-SRV.

2. On the left side of the pane, select the HTTPS connections.
3. Right click on the HTTPS connection and select New Trunk to open the Create Trunk Wizard and Click Next.
4. Select Trunk Type in Step 1 and Click Next.
5. Enter the details under Setting the Trunk such as Trunk Name and Public Host Name in Step 2.
6. Click Next and click Add to enter the details for Authentication Server.
7. Select UAG-DC as the authentication server in Step 3.
8. Select the HSM certificate in Step 4.
11. Click Finish to complete the wizard.
12. Save the UAG configuration.

We have successfully created the HTTPS trunk using the HSM certificate whose keys are saved on Luna SA.