SafeNet Authentication Service
Integration Guide

Using SafeNet Authentication Service as an Identity Provider for Citrix NetScaler Gateway 12.0
All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2017 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.
Third-Party Software Acknowledgement ................................................................. 4
Description .............................................................................................................. 4
Applicability ............................................................................................................ 4
Environment ........................................................................................................... 4
Audience .................................................................................................................. 5
SAML Authentication using SafeNet Authentication Service Cloud ..................... 5
SAML Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE ............................................................................. 5
SAML Authentication Flow using SafeNet Authentication Service ....................... 6
SAML Prerequisites ................................................................................................. 6
Downloading the SafeNet Authentication Service Metadata ................................. 6
Downloading the SafeNet Identity Provider Certificate ........................................ 6
Configuring Citrix NetScaler Gateway 12.0 .......................................................... 7
Installing SafeNet Identity Provider Certificate in Citrix NetScaler Gateway 12.0 ... 7
Creating the Authentication Server ......................................................................... 8
Creating the Authentication Policy ......................................................................... 9
Assigning the SAML Policy to the NetScaler Virtual Server ................................ 11
Configuring SafeNet Authentication Service .......................................................... 13
Synchronizing Users Stores to SafeNet Authentication Service ......................... 13
Assigning an Authenticator in SafeNet Authentication Service ......................... 13
Adding Citrix NetScaler Gateway 12.0 as a Service Provider (SP) in SafeNet Authentication Service ................................................................. 14
Enabling SAML Services in SafeNet Authentication Service .............................. 18
Running the Solution .............................................................................................. 22
Support Contacts .................................................................................................... 23
Customer Support Portal ...................................................................................... 23
Telephone Support ................................................................................................ 23
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Citrix NetScaler Gateway 12.0.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from the third-party software will be acknowledged as such.

Description

SafeNet Authentication Service (SAS) delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

Citrix NetScaler Gateway is a secure application and data access solution that gives IT administrators a single point to manage access control and limit actions within sessions based on both user identity and the endpoint device. New threats, risks, and vulnerabilities as well as evolving business requirements underscore the need for a strong authentication approach based on the multi-factor authentication.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Citrix NetScaler Gateway 12.0 using SafeNet one-time password (OTP) authenticators managed by SafeNet Authentication Service.
- Configure SAML authentication in Citrix NetScaler Gateway 12.0 using SafeNet Authentication Service as an identity provider.

It is assumed that the Citrix NetScaler Gateway 12.0 environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Citrix NetScaler Gateway 12.0 can be configured to support multi-factor authentication in several modes. The SAML authentication will be used for the purpose of working with SafeNet Authentication Service.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—SafeNet's cloud-based authentication service
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—A server version that is used by Service providers to deploy instances of SafeNet Authentication Service
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A server version that is used to deploy the solution on-premises in the organization

Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Service**
- **Citrix NetScaler Gateway — Version 12.0**
Audience

This document is targeted to system administrators who are familiar with Citrix NetScaler Gateway 12.0, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service (SAS).

SAML Authentication using SafeNet Authentication Service Cloud

SafeNet Authentication Service (SAS) Cloud provides a service for SAML authentication that is already implemented in the SAS Cloud environment and can be used without any installation.

SAML Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE

In addition to the pure cloud-based offering, SafeNet Authentication Service (SAS) comes with two on-premises versions:

- **SafeNet Authentication Service – Service Provider Edition (SPE)**—An on-premises version of SafeNet Authentication Service targeted at service providers interested in hosting SAS in their data center.
- **SafeNet Authentication Service – Private Cloud Edition (PCE)**—An on-premises version of SafeNet Authentication Service targeted at organizations interested in hosting SAS in their private cloud environment.

For both on-premises versions, SAS can be integrated with the Shibboleth infrastructure, which uses a special on-premises agent called SafeNet Authentication Service Agent for Shibboleth.

For more information on how to install and configure the SafeNet Authentication Service Agent for Shibboleth, refer to the SafeNet Support Portal.
SAML Authentication Flow using SafeNet Authentication Service

SafeNet Authentication Service (SAS) communicates with a large number of service providers and cloud-based services solutions using the SAML protocol.

The image below describes the dataflow of a multi-factor authentication transaction for Citrix NetScaler Gateway 12.0.

1. A user attempts to log on to Citrix NetScaler Gateway 12.0. The user is redirected to SafeNet Authentication Service. SAS collects and evaluates the user’s credentials.
2. SAS returns a response to Citrix NetScaler Gateway 12.0, accepting or rejecting the user’s authentication request.

SAML Prerequisites

To enable SafeNet Authentication Service (SAS) to receive SAML authentication requests from Citrix NetScaler Gateway 12.0, ensure that the end users can authenticate from the Citrix NetScaler Gateway 12.0 environment with a static password.

Downloading the SafeNet Authentication Service Metadata

Browse to the https://idp1.cryptocard.com/idp/shibboleth URL. The SafeNet Authentication Service metadata will be downloaded automatically. Save it locally on your machine.

Downloading the SafeNet Identity Provider Certificate

Browse to the https://cloud.safenet-inc.com/console/cert/idp.crt URL. The SafeNet identity provider certificate will be downloaded automatically. Save it locally on your machine.
Configuring Citrix NetScaler Gateway 12.0

Adding SafeNet Authentication Service (SAS) as an Identity Provider in Citrix NetScaler Gateway 12.0 requires:

- Installing SafeNet Identity Provider Certificate in Citrix NetScaler Gateway 12.0, page 7
- Creating the Authentication Server, page 8
- Creating the Authentication Policy, page 9
- Assigning the SAML Policy to the NetScaler Virtual Server, page 11

Installing SafeNet Identity Provider Certificate in Citrix NetScaler Gateway 12.0

1. Log in to the Citrix NetScaler administrator console.
2. On the Citrix NetScaler administrator console, on the Configuration tab, perform the following steps:
   a. In the left pane, click Traffic Management > SSL > Certificates > CA Certificates.
   b. In the right pane, under CA Certificates, click Install.

3. On the Install CA Certificate window, perform the following steps:
   a. In the Certificate-Key Pair Name field, enter a name for the certificate.
   b. Under Certificate File Name, next to Choose File, click , and select local.
   c. Search for and select the SAS IDP certificate that you downloaded earlier in “Downloading the SafeNet Identity Provider Certificate” on page 6.
Creating the Authentication Server

Perform the following steps to create the authentication server:

1. On the Citrix NetScaler administrator console, on the Configuration tab, perform the following steps:
   a. In the left pane, click NetScaler Gateway > Policies > Authentication > SAML.
   b. In the right pane, under SAML, on the Servers tab, click Add.

![Citrix NetScaler Configuration Screen](https://example.com/citrix_screen.png)  
(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)

2. On the Create Authentication SAML Server window, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the server (for example, samlserver).</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDP Certificate Name</td>
<td>Select the IDP certificate that you installed earlier in step 3 of &quot;Installing SafeNet Identity Provider Certificate in Citrix NetScaler Gateway 12.0&quot;.</td>
</tr>
<tr>
<td>Redirect URL</td>
<td>Enter the identity provider (IdP) HTTP-POST login URL (for example, <a href="https://idp1.cryptocard.com/idp/profile/SAML2/POST/SSO">https://idp1.cryptocard.com/idp/profile/SAML2/POST/SSO</a>). The URL is provided in the SAS metadata that you downloaded earlier in &quot;Downloading the SafeNet Authentication Service Metadata, on page 6.&quot;</td>
</tr>
</tbody>
</table>
Issuer Name

Enter the NetScaler virtual server URL (for example, https://test.safenetdemos.com).

3. Click Create.

Creating the Authentication Policy

Perform the following steps to create the authentication policy:

1. On the Citrix NetScaler administrator console, click the Configuration tab, and then perform the following steps:
   a. In the left pane, click NetScaler Gateway > Policies > Authentication > SAML.
b. In the right pane, under **SAML**, on the **Policies** tab, click **Add**.

![Citrix NetScaler VPX (1000)](image)

(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)

2. On the **Create Authentication SAML Policy** window, complete the following fields, and then click **Create**.

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter a name for the policy (for example, <code>saml</code>).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server</strong></td>
<td>Select the server (for example, <code>samlserver</code>) that you created earlier in step 2 of “Creating the Authentication Server.”</td>
</tr>
<tr>
<td><strong>Expression</strong></td>
<td>Enter the logical expression you want to use (for example, <code>ns_true</code>).</td>
</tr>
</tbody>
</table>

![Citrix NetScaler VPX (1000)](image)

(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)
Assigning the SAML Policy to the NetScaler Virtual Server

1. On the Citrix NetScaler administrator console, on the Configuration tab, perform the following steps:
   a. In the left pane, click NetScaler Gateway > Virtual Servers.
   b. In the right pane under NetScaler Gateway Virtual Servers, select the virtual server (for example, test) to which you want to assign the SAML policy.
   c. Click Edit.

   ![NetScaler Gateway Virtual Servers](image)

   *(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)*

2. On the VPN Virtual Server window, under Basic Authentication, click *

   ![VPN Virtual Server](image)

   *(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)*

3. On the Choose Type window, complete following fields:

<table>
<thead>
<tr>
<th>Choose Policy</th>
<th>Select SAML.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose Type</td>
<td>Select Primary</td>
</tr>
</tbody>
</table>

   ![Choose Type](image)

   *(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)*
4. Click **Continue**.

5. Under **Policy Binding**, in the **Select Policy** field, click ![Select Policy](image1)

6. On the **SAML Policies** window, in the table, select the authentication policy (for example, **saml**) that you created earlier in step 2 of "Creating the Authentication Policy", and then click **Select**.

7. On the **Choose Type** window, click **Bind**.

8. Click **Done**.

9. On the **Citrix NetScaler administrator** console, on the top right-hand side corner, click ![Save Configuration](image2) to save the configuration.
Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with Citrix NetScaler Gateway 12.0 using SAML authentication requires:

- Synchronizing Users Stores to SafeNet Authentication Service, page 13
- Assigning an Authenticator in SafeNet Authentication Service, page 13
- Adding Citrix NetScaler Gateway 12.0 as a Service Provider (SP) in SafeNet Authentication Service. page 14
- Enabling SAML Services in SafeNet Authentication Service, page 18

Synchronizing Users Stores to SafeNet Authentication Service

Before SafeNet Authentication Service (SAS) can authenticate any user in your organization, you need to create a user store in SAS that reflects the users that would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- Manually, one user at a time using the Create User shortcut
- Manually, by importing one or more user records via a flat file
- Automatically, by synchronizing with your Active Directory/LDAP server using the SAS Synchronization Agent

For further details on importing users to SafeNet Authentication Service, refer to “Creating Users” in the SafeNet Authentication Service Subscriber Account Operator Guide:


All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.

Assigning an Authenticator in SafeNet Authentication Service

SafeNet Authentication Service (SAS) supports a number of authentication methods that can be used as a second authentication factor for users authenticating through Citrix NetScaler Gateway 12.0.

The following authenticators are supported:

- eToken PASS
- RB-1 keypad token
- KT-4 token
- SafeNet GOLD
- SMS tokens
Authenticators can be assigned to users in two ways:

- **Manual provisioning**—Assign an authenticator to users one at a time.
- **Provisioning rules**—The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change. An authenticator will be assigned automatically to the user.

Refer to “Provisioning” in the *SafeNet Authentication Service - Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.


**Adding Citrix NetScaler Gateway 12.0 as a Service Provider (SP) in SafeNet Authentication Service**

Add a service provider entry in the SafeNet Authentication Service (SAS) SAML Service Providers module to prepare it to receive SAML authentication requests from Citrix NetScaler Gateway 12.0. You will need the Issuer ID and assertion consumer URL location of Citrix NetScaler Gateway 12.0.

Perform the following steps to add Citrix NetScaler Gateway 12.0 as a Service Provider in SafeNet Authentication Service:

1. Log in to the SafeNet Authentication Service console with an Operator account.
2. Click the **COMMS** tab, and then click **SAML Service Providers**.

   ![Image of COMMS tab]

3. In the **SAML Service Providers** module, click on the **SAML 2.0 Settings** link.

   ![Image of SAML Service Providers]

4. Click **Add**.

   ![Image of SAML Service Providers with Add button highlighted]
5. Under **Add SAML 2.0 Settings**, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friendly Name</td>
<td>Enter the Citrix NetScaler Gateway 12.0 name.</td>
</tr>
<tr>
<td>SAML 2.0 Metadata</td>
<td>Select <strong>Create New Metadata File</strong>.</td>
</tr>
<tr>
<td>Entity ID</td>
<td>Enter the <strong>Issuer Name</strong> (for example, <a href="https://test.safenetdemos.com">https://test.safenetdemos.com</a>) that you entered in step 2 of “Creating the Authentication Server” on page 8.</td>
</tr>
<tr>
<td>Location</td>
<td>Enter the <strong>Assertion Consumer URL</strong> in the below format:</td>
</tr>
<tr>
<td></td>
<td><strong>https://&lt;domain name of the virtual server/cgi/samlauth</strong></td>
</tr>
<tr>
<td></td>
<td>For example, <strong><a href="https://test.safenetdemos.com/cgi/samlauth">https://test.safenetdemos.com/cgi/samlauth</a></strong>.</td>
</tr>
</tbody>
</table>

![Add SAML 2.0 Setting]

**NOTE:** The remaining options are used to customize the appearance of the logon page presented to the user. For more information on logon page customization, refer to “Configure SAML Service Providers” in the **SAML Authentication Quick Start Guide**:


Under **Return Attributes**, add add the following attributes, and then click **Apply**:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</a></td>
<td>According to the third-party product requirements.</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/claims/EmailAddress">http://schemas.xmlsoap.org/claims/EmailAddress</a></td>
<td>According to the third-party product requirements.</td>
</tr>
<tr>
<td>Name</td>
<td>Value</td>
</tr>
<tr>
<td>------</td>
<td>-------</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</a></td>
<td>According to the third-party product requirements.</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</a></td>
<td>According to the third-party product requirements.</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/claims/CommonName">http://schemas.xmlsoap.org/claims/CommonName</a></td>
<td>According to the third-party product requirements.</td>
</tr>
<tr>
<td>principal</td>
<td>According to the third-party product requirements.</td>
</tr>
</tbody>
</table>

Citrix NetScaler Gateway 12.0 is added as a service provider in the system.
Enabling SAML Services in SafeNet Authentication Service

After Citrix NetScaler Gateway 12.0 has been added to SafeNet Authentication Service (SAS) as a service provider, the users should be granted permission to use this service provider with SAML authentication.

There are two methods to enable the user to use the service provider:

- Manually, one user at a time, using SAML Services module
- Automatically, by defining groups of users, using SAML Provisioning Rules

Using the SAML Services Module

Manually enable a single user to authenticate against one or more configured SAML Service providers.

1. Log in to the SafeNet Authentication Service console with an Operator account.

2. Click the ASSIGNMENT tab, and then search for the required user.
3. Click the appropriate user in the **User ID** column.

![Search User](image1)

4. Click **SAML Services**.

![Manage IMC](image2)

5. Click **Add**.

![SAML Services](image3)
6. Under **Add SAML Service**, perform the following steps:
   a. From the **Service** menu, select the Citrix NetScaler Gateway 12.0 service provider.
   b. In **SAML Login ID** field, select the type of login ID (**User ID**, **E-mail**, or **Custom**) to be sent as a User ID to Citrix NetScaler Gateway 12.0 in the response.
   c. Click **Add**.

   The user can now authenticate to Citrix NetScaler Gateway 12.0 using SAML authentication.

---

**Using SAML Provisioning Rules**

Use this module to enable groups of users to authenticate to SAML service providers.

1. Log in to the SafeNet Authentication Service console with an Operator account.
2. Click the **POLICY** tab, and then click **Automation Policies**.

3. Click the **SAML Provisioning Rules** link.

4. Click **New Rule**.

5. Configure the following fields, and then click **Add**:

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User is in container</strong></td>
<td>Select a container as per your preferred configuration. Users affected by the rule must be in the selected container.</td>
</tr>
<tr>
<td><strong>Groups</strong></td>
<td>The <strong>Virtual Server groups</strong> box lists all groups. Click the user groups that will be affected by the rule, and then click the right arrow to move it to the <strong>Used by rule</strong> box.</td>
</tr>
<tr>
<td><strong>Parties</strong></td>
<td>The <strong>Relying Parties</strong> box lists all service providers. Click the service providers that the groups of users will authenticate to, and then click the right arrow to move it to <strong>Rule Parties</strong> box.</td>
</tr>
</tbody>
</table>
SAML Login ID

Select **User ID**. The **User ID** will be returned to the service provider in the SAML assertion.

Running the Solution

1. In a web browser, open the Citrix NetScaler Access Gateway login page.
2. You will be redirected to the SAS IDP login page. Enter your username and the token passcode.

3. After a successful authentication, you will be redirected to access Citrix StoreFront.

*(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)*
Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support.

Gemalto Customer 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 Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.gemalto.com, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

**NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the REGISTER link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Customer Support by telephone. Calls to Customer Support are handled on a priority basis.

<table>
<thead>
<tr>
<th>Region</th>
<th>Telephone number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>+1-410-931-7520</td>
</tr>
<tr>
<td>Australia</td>
<td>1800.020.183</td>
</tr>
</tbody>
</table>
| China     | North: 10800-713-1971  
<p>|           | South: 10800-1301-932 |
| France    | 0800-912-857     |
| Germany   | 0800-181-6374    |
| India     | 000.800.100.4290 |
| Israel    | 180-931-5798     |
| Italy     | 800-786-421      |
| Japan     | 0066 3382 1699   |
| Korea     | +82 2 3429 1055  |</p>
<table>
<thead>
<tr>
<th>Region</th>
<th>Telephone number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netherlands</td>
<td>0800.022.2996</td>
</tr>
<tr>
<td>New Zealand</td>
<td>0800.440.359</td>
</tr>
<tr>
<td>Portugal</td>
<td>800.863.499</td>
</tr>
<tr>
<td>Singapore</td>
<td>800.1302.029</td>
</tr>
<tr>
<td>Spain</td>
<td>900.938.717</td>
</tr>
<tr>
<td>Sweden</td>
<td>020.791.028</td>
</tr>
<tr>
<td>Switzerland</td>
<td>0800.564.849</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>0800.056.3158</td>
</tr>
<tr>
<td>United States</td>
<td>(800) 545-6608</td>
</tr>
</tbody>
</table>