

**THALES**

# SafeNet Agent for Siebel 1.2.0

## INSTALLATION AND CONFIGURATION GUIDE



All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates 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 Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as "Thales") 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, Thales 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, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

**Thales 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 Thales 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.**

**Thales 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 Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales 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.**

Copyright © 2018-2020 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

# CONTENTS

Preface: About the SafeNet Agent for Siebel 1.2.0 Guide .....	4
Customer Release Notes .....	4
Audience .....	4
Document Conventions .....	4
Command Syntax and Typeface Conventions .....	4
Notifications and Alerts .....	5
Support Contacts .....	6
Chapter 1: Overview .....	7
User Flow .....	7
Compatibility and Component Information .....	7
Supported Siebel Version .....	7
Authentication Server .....	8
Network .....	8
Supported Web Browsers .....	8
Additional Web Browser Requirements .....	8
Supported Authentication Methods .....	8
Chapter 2: Installing the SafeNet Agent for Siebel .....	9
Prerequisites .....	9
Installing and Configuring Siebel Server .....	9
Configuring Custom Authentication .....	10
Configuring LDAP Adapter .....	14
Configuring Custom Parameters .....	14
Troubleshooting .....	16
Error .....	16
Page not Loading .....	16
No Log File .....	16

# PREFACE: About the SafeNet Agent for Siebel 1.2.0 Guide

## Customer Release Notes

---

The customer release notes (CRN) provide important information about this release that is not included in the customer documentation. It is strongly recommended that you read the CRN to fully understand the capabilities, limitations, and known issues for this release.

## Audience

---

This document is intended for personnel responsible for maintaining your organization's security infrastructure.

All products manufactured and distributed by Thales Group are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

It is assumed that the users of this document are proficient with security concepts.

## Document Conventions

---

This section describes the conventions used in this document.

### Command Syntax and Typeface Conventions

This document uses the following conventions for command syntax descriptions, and to highlight elements of the user interface.

Format	Convention
<b>bold</b>	<p>The bold attribute is used to indicate the following:</p> <ul style="list-style-type: none"><li>&gt; Command-line commands and options that you enter verbatim (Type <b>dir /p</b>.)</li><li>&gt; Button names (Click <b>Save As</b>.)</li><li>&gt; Check box and radio button names (Select the <b>Print Duplex</b> check box.)</li><li>&gt; Dialog box titles (On the <b>Protect Document</b> dialog box, click <b>Yes</b>.)</li><li>&gt; Field names (<b>User Name</b>: Enter the name of the user.)</li><li>&gt; Menu names (On the <b>File</b> menu, click <b>Save</b>.) (Click <b>Menu &gt; Go To &gt; Folders</b>.)</li><li>&gt; User input (In the <b>Date</b> box, type <b>April 1</b>.)</li></ul>

Format	Convention
<i>italics</i>	In type, the italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[ <b>optional</b> ] [<optional>]	Represent optional <b>keywords</b> or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
{ <b>a b c</b> } {<a> <b> <c>}	Represent required alternate <b>keywords</b> or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.
[ <b>a b c</b> ] [<a> <b> <c>]	Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

## Notifications and Alerts

Notifications and alerts are used to highlight important information or alert you to the potential for data loss or personal injury.

### Tips

Tips are used to highlight information that helps to complete a task more efficiently.

**TIP** This is some information that will allow you to complete your task more efficiently.

### Notes

Notes are used to highlight important or helpful information.

**NOTE** Take note. Contains important or helpful information.

### Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss.

**CAUTION!** Exercise caution. Contains important information that may help prevent unexpected results or data loss.

### Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury.

**\*\*WARNING\*\*** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

## Support Contacts

---

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or [Thales Group Customer Support](#).

Thales Group 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 Thales Group 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.thalesgroup.com>, is 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

The support portal also lists telephone numbers for voice contact ([Contact Us](#)).

# CHAPTER 1: Overview

The SafeNet Agent for Siebel is a Two-Factor Authentication (2FA) solution that helps Siebel customers ensure that valuable resources are accessible only to authorized users. The use of 2FA when accessing network resources, instead of traditional static passwords, is a critical measure for information security.

The SafeNet Agent for Siebel enables you to configure authentication rules in the policy domains and policies that protect your resources. The authentication rules contain authentication schemes, which provide methods for verifying a user's identity.

The SafeNet Agent for Siebel uses the Siebel's CRM architecture and extend the interfaces provided for authentication.

When there is an authentication request at the Siebel CRM solution, the app's authentication module is looked up and the configured adapter is triggered.

- > For existing authentication adapters, such as Active Directory Service Interfaces (ADSI)/ LDAP or Oracle, the existing authentication modules handle the configuration.
- > For custom authentication adapters, it looks up the module (the dynamic library) and loads it.

The user credentials are passed to the authentication module and a return code is expected. The return code is then mapped to a Siebel error or a success message, and rendered on the screen.

## User Flow

---

The 2FA parameters are passed from the Siebel application to the SafeNet Authentication Service (SAS) server:

1. The user authenticates with LDAP credentials on the landing screen.
2. If the LDAP authentication is successful, the user receives an SMS message.
3. On the Siebel CRM interface, the users is prompted to enter the SAS OTP.
4. If the user does not provide SAS OTP (within 60 seconds), they are prompted to authenticate with their LDAP credentials again.

## Compatibility and Component Information

---

### Supported Siebel Version

- > Innovation Pack 2015 (IP15)
- > Innovation Pack 2016 (IP16)
- > Innovation Pack 2018 (IP18)

## Authentication Server

- > SafeNet Authentication Service PCE/SPE 3.7 and later
- > SafeNet Authentication Service Cloud

## Network

TCP Port 80 or 443

## Supported Web Browsers

- > Supports all browsers supported by native Siebel CRM.

## Additional Web Browser Requirements

- > Cookies must be enabled.
- > JavaScript must be enabled.

## Supported Authentication Methods

Except Push OTP, all tokens and authentication methods supported by SafeNet.



# CHAPTER 2: Installing the SafeNet Agent for Siebel

## Prerequisites

- > The Siebel environment is up and running.
- > The application that requires 2FA is integrated with the LDAP server.
- > All the anonymous users must be added in the LDAP directory, and must only be assigned limited, required permissions.

## Installing and Configuring Siebel Server

To install the SafeNet Agent for Siebel, extract its package file (***SiebelAgent-1.1.0.<build number>.tar***), and copy the agent files to folders on the Siebel server.

1. Stop the Siebel server, using the following commands:

```
cd /export/home/siebel/sia/siebsrvr
. ./siebenv.sh
cd bin
stop_server all
```

2. Create a folder (***/usr/local***) and ensure that you have administrator rights to install at the location.

**NOTE** If you do not have administrator rights to install at the location, you can install the SafeNet Agent for Siebel package in a different location. In this case, change the paths in the following steps accordingly.

3. Navigate to the folder (***/usr/local***) by executing the following command:

```
cd /usr/local
```

4. Extract the SafeNet Agent for Siebel package ***SafeNet-Authentication-Service-Agent-For-Siebel-<Version number>.tar*** file:

```
tar -xvf SafeNet-Authentication-Service-Agent-For-Siebel-<Version number>.tar
```

The SafeNet Agent for Siebel will be installed in the following folder: ***/usr/local/gemalto/siebel***

5. Navigate to the following path:

```
cd /<Siebel install directory>/sia/siebsrvr/lib
```

6. Create a backup of the **libSiebel** file. Copy the **libSiebel.so.<version>** file from the Siebel agent package to the current location:

```
cp /usr/local/gemalto/siebel/lib/libSiebel.so.<version> ./
```

7. Create the soft link of the file (as copied in step 6) by executing the following command:

```
ln -s libSiebel.so.<version> libSiebel.so  
Example: ln -s libSiebel.so.1.2.0.18 libSiebel.so
```

8. Copy the **libcurl.so.3** file from the Siebel agent package to the current location:

```
cp /usr/local/gemalto/siebel/lib/libcurl.so.3 ./
```

9. Navigate to the following path:

```
cd /<Siebel install directory>/Sia/siebsrvr/webtempl/ouiwebtempl
```

10. Create a backup of the **SWELogin.swt** file. Copy the **SWELogin.swt** file from the package to the current location:

```
cp /usr/local/gemalto/siebel/SWELogin.swt ./
```

11. Start the server, using the following commands:

```
cd /export/home/siebel/sia/siebsrvr  
./siebenv.sh  
cd bin  
start_server all
```


12. (Optional) In case of a Solaris server start, execute the step first:

```
cd /export/home/siebel/sia/gtwysrvr  
./siebenv.sh  
cd bin  
start_ns
```


**NOTE** Starting the server is a CPU intensive operation. Before accessing the app with the Siebel SDK agent, ensure that the server is started completely.

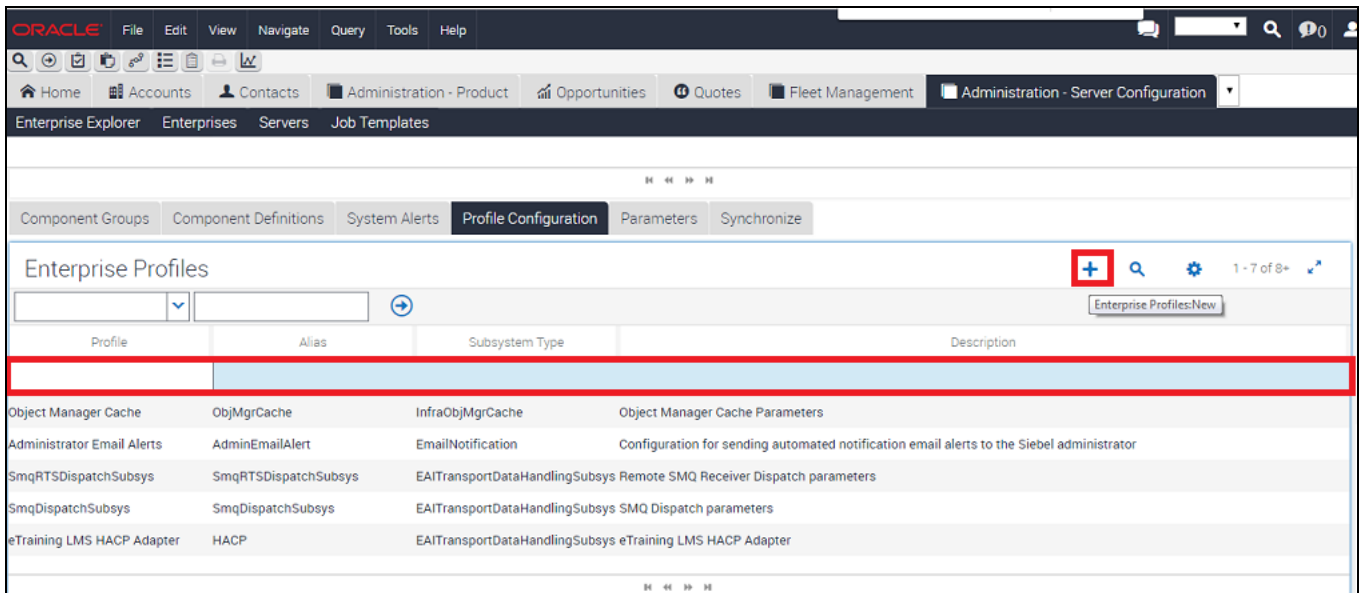
## Configuring Custom Authentication

1. Log in to the Siebel Call Center application as an administrator.

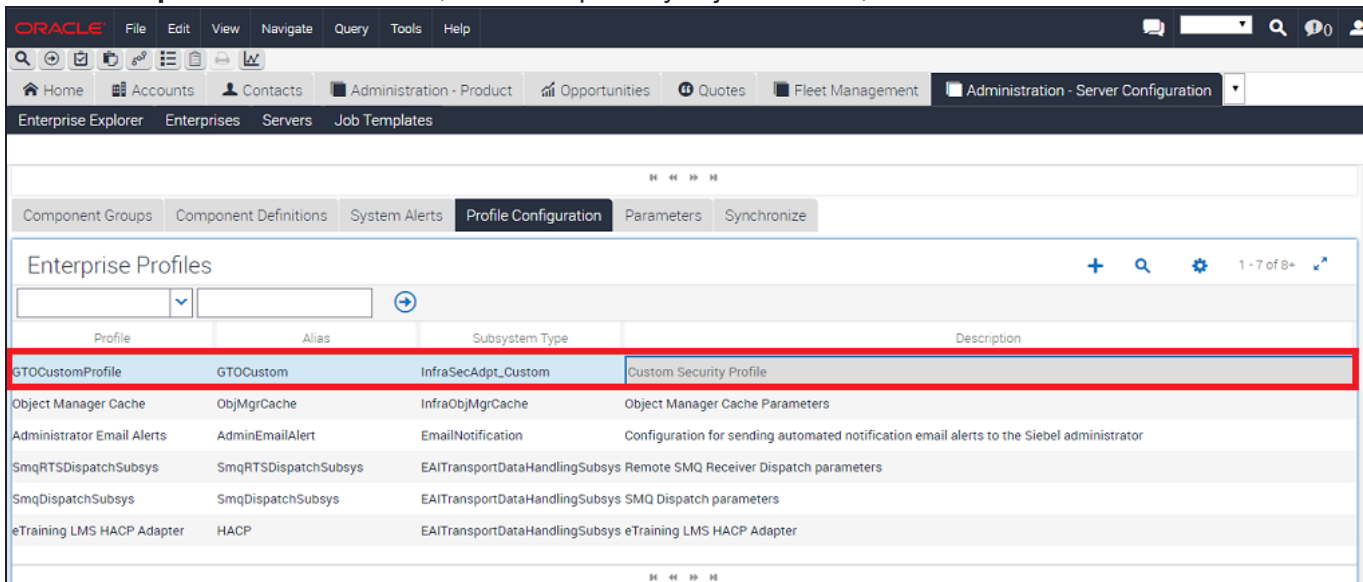
2. From the **Home** page, click the **Site Map** icon .
3. On the **Screens** section, search and select the **Administration - Server Configuration** option.
4. Under **Administration - Server Configuration**, click **Enterprises > Profile Configuration**.

Name	Alias	Number of Comp	Enable state	Description
Siebel Financial Services	Fins	9	Enabled	Siebel Financial Services Components
Siebel High Tech Industrial Manufacturing	HTIM	2	Enabled	Siebel High Tech Industrial Manufacturing Components
PIM Server Integration Management	PIMSI	2	Disabled	Siebel PIM Server Integration Components
Marketing Server	MktgSrv	1	Enabled	Marketing Server Components
Field Service	FieldSvc	9	Enabled	Field Service Components
Workflow Management	Workflow	6	Enabled	Workflow Management Components
Application Deployment Manager	ADM	3	Enabled	Application Deployment Manager Components

5. In the **Enterprise Profiles** section, click **Enterprise Profiles:New** icon  to create a new profile with the following details:
  - a. Profile
  - b. Alias
  - c. Subsystem Type
  - d. Description



6. In the **Enterprise Profiles** section, select the profile you just created, and scroll-down.



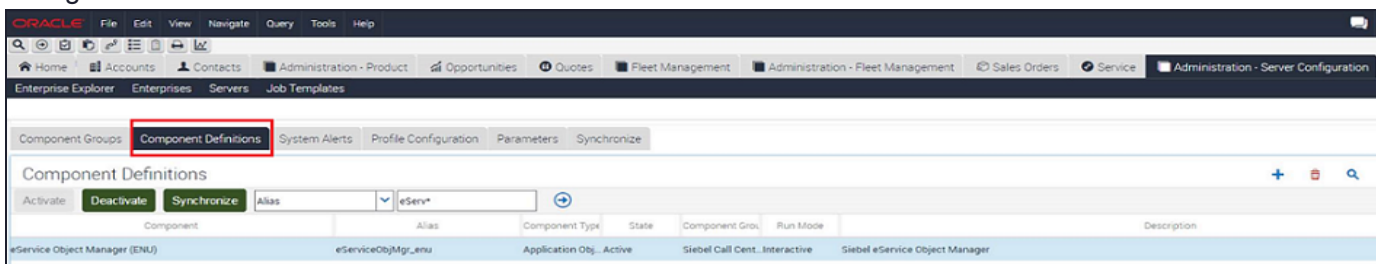
7. Navigate to the **Profile Parameters** section and edit the **Value(s)** of the following **Name** fields:
- Security Adapter DII Name:** Change to *libSiebel*.
  - Config File Name:** Change to *customsecurity.cfg*.
  - Config Section Name:** Change to *customparam*.
  - Propagate Change:** Ensure that the value is set as *False*, as the LDAP user creation is not supported by the Siebel agent.

Profile Parameters

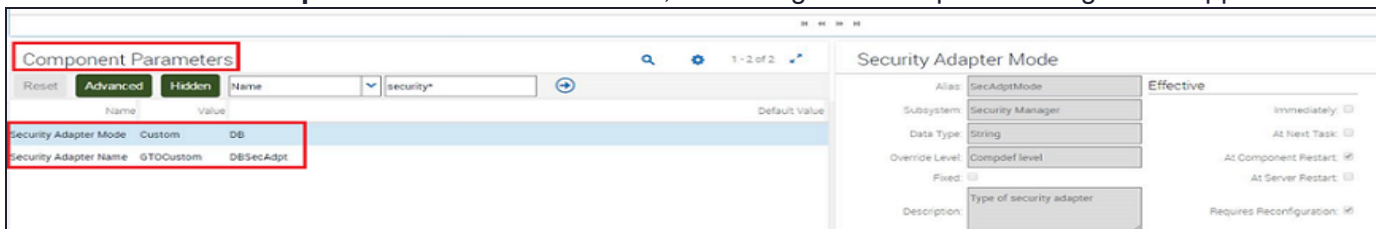
Delete Parameter Override    Reset    **Advanced**    Hidden

Name	Alias	Data Type	Value	Description
CRC	CustomSecAdpt_CRC	String	*****	Security adapter checksum
Security Adapter Dll Name	CustomSecAdpt_SecAdptDllName	String	libSiebel	Security adapter dll name
Config File Name	ConfigFileName	String	customsecurity.cfg	Custom security adapter configuration file name
User Password Hash Algorithm	CustomSecAdpt_HashAlgorithm	String	RSASHA1	The hash algorithm used to hash password when HashUserPwd is set to TRUE...
Hash DB Cred	CustomSecAdpt_HashDBPwd	Boolean	False	If set to TRUE, then siebel authentication system will hash the db password an...
Hash User Password	CustomSecAdpt_HashUserPwd	Boolean	False	If set to TRUE, then user's password will be hashed before sent to authenticati...
Propagate Change	CustomSecAdpt_PropagateChange	Boolean	False	Propagate user changes to external user repository
Salt User Password	CustomSecAdpt_SaltUserPwd	Boolean	False	If set to TRUE, then user's password will be prefixed with salt before hashing. I...
Config Section Name	ConfigSectionName	String	customparam	Custom security adapter configuration section name
Single Sign On	CustomSecAdpt_SingleSignOn	Boolean	False	Web SSO is enabled

8. Scroll-up and click the **Component Definitions** tab. Search and select the application that you need to configure for custom authentication.

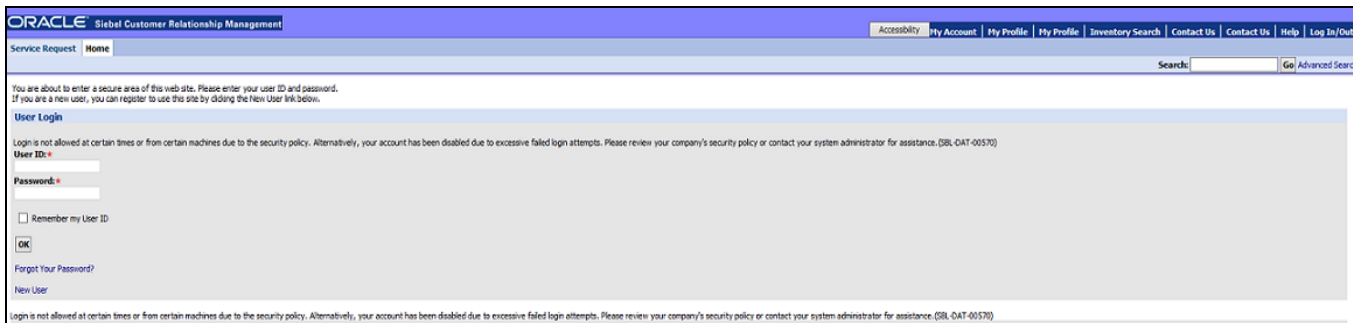


9. Scroll-down to the **Component Parameters** section, and configure the required setting for the application:



In the new Siebel subsystem **GTOCustom**, change **Custom** parameter value of the **Security Adapter Name** to **GTOCustom**.

The post LDAP login screen appears:



## Configuring LDAP Adapter

### Configuring Custom Parameters

To configure parameters, refer the *sample\_customSecurity.cfg* configuration file included in the SafeNet Agent for Siebel package.

#### 1. Add your LDAP binding credentials:

```
ldapBindAccount="<user name>"
ldapBindPassword="<password>"
```

Use the following username and password for a bind:

- For Sun LDAP, use the uid of the user account.
- For Microsoft AD, use a simple name (with no details) since it does not use filters.

#### 2. Configure BaseDN for LDAP users:

```
ldapBaseDN="<LDAP base DN>"
```

For example: `ldapBaseDN="OU=users,OU=bccs,O=stc,C=sa,DC=stc,DC=com"`

**NOTE** The **BaseDN** should mention **Country Name** before **Domain Controller**.

#### 3. Configure the LDAP port and IP address, and the database username and password:

```
ldapPort=389
ldapServerIP="<LDAP server IP address>"
dbusername="<database username>"
dbpassword="<database password>"
```

#### 4. For SSL, disable the default as 0:

```
ldapSSL="0"
```

#### 5. Add the UID for LDAP query values:

```
ldapUID="<value>"
```

Common values are:

- cn
- UID
- sAMAccountName

#### 6. For Microsoft AD, set the value to 1:

```
ldmicrosoftad="0"
```

```
sasEncryptionKeyFile="/home/siebel/sia/siebsrvr/bin/Agent.bsidgey"
sasprimaryhost="<IP of the SAS primary host>"
sasprimaryport="<80 for http or 443 for https>"
sasprimarypath="/TokenValidator/TokenValidator.asmx"
sasprimaryisssl="0"
sassecondaryhost="<IP of the SAS secondary host>"
sassecondaryport="<80 for http or 443 for https>"
sassecondarypath="/TokenValidator/TokenValidator.asmx"
sassecondaryisssl="0"
```

#### 7. Enable or disable SafeNet (OTP) authentication for users in LDAP groups:

```
ldapForceOTPGroupEnabled="1"
```

- Set the value to **1** (or any other value) to enforce OTP authentication.
- Set the value to **0** (or Blank) to disable OTP authentication.

**NOTE** Irrespective of whether you set the value to **1** or **0**, you must provide value(s) for mandatory, related attributes.

**8.** Enter group names for SafeNet authentication in a comma-separated list:

```
ldapForceOTPGroup="<group1>,<group2>"
```

**NOTE** SAS authentication is only applied to defined groups if `ldapForceOTPGroupEnabled="1"` (as defined in step 7).

**9.** Set the LDAP attribute used to search and identify users defined in LDAP groups (as defined in step 8):

```
ldapForceOTPMember="member"
```

**10.** Enable or disable LDAP authentication:

```
ldapenabled="1"
```

**NOTE** Set value to **1** to enable or **0** to disable the LDAP authentication.

**11.** Set the BaseDN for user groups (as defined in Step 8):

```
ldapgroupbasedn
```

For example: `ldapgroupbasedn="OU=bccs,O=stc,C=sa,DC=stc,DC=com"`

**12.** Enter all anonymous users for SafeNet authentication in a comma-separated list:

```
anonusername="<user1>,<user2>"
```

**NOTE** The SafeNet two factor authentication will not be applicable for anonymous users.

**13.** Set **validateCertificate** value as 0 or 1. The value **1** ensures that the security certificate checks will be forced, while communicating with the SAS servers. If the value is left at default (**0**), the certificate check will be ignored. This parameter is only valid for the HTTPS protocol.

```
validateCertificate="1"
```

**14.** Set log level:

```
logLevel="<value>"
```

**NOTE** Set the value to **1** for **Info** logs. Set the value to **2** for **Debug** logs.

## Troubleshooting

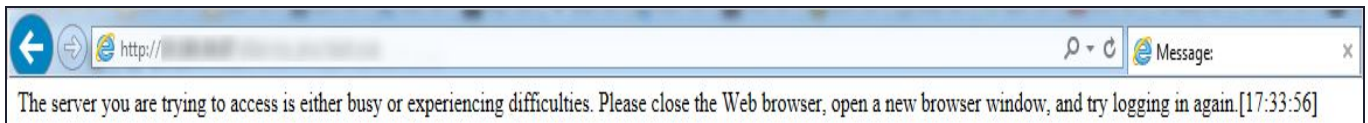
### Error

If an error is encountered, it usually means that either the server didn't start correctly, or the Gateway Server isn't running.

### Solution

Restart the Gateway Server, and then start the Siebel Server.

If needed, reboot the machine, start the Gateway Server, and then start the Siebel Server (you must do it, in the exact specified sequence).



### Page not Loading

If the page is not loading, check the log file created at the following location: ***/tmp/siebelCRM.log***

### No Log File

If the log file is not being created, it means that an issue occurred on the Siebel CRM Admin console while configuring the adapter. Check the logs for the corresponding object manager under the enterprise directory.