

Utilizing External Directory Services for IBM Sterling Control Center User Authentication

April 1, 2011



This edition applies to the 5.2.03 Version of IBM® Sterling Control Center.

Before using this information and the product it supports, read the information in *Notices on page 17*.

Licensed Materials - Property of IBM

IBM® Sterling Control Center

© Copyright IBM Corp. 2003, 2011. All Rights Reserved.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Overview

IBM® Sterling Control Center has the ability to validate its users via its own internal store of User IDs and passwords and/or other credentials, or, via Lightweight Directory Access Protocol (LDAP) accessible directories, such as OpenLDAP™, IBM® Tivoli® Directory Server, and Microsoft Active Directory™. This “External Authentication” is accomplished by Sterling Control Center via a IBM® Sterling External Authentication Server. Users not configured for “External Authentication” are validated via Control Center’s own internal store of User IDs and passwords and/or other credentials. Users with IDs configured for “External Authentication” are validated via a Sterling External Authentication Server.

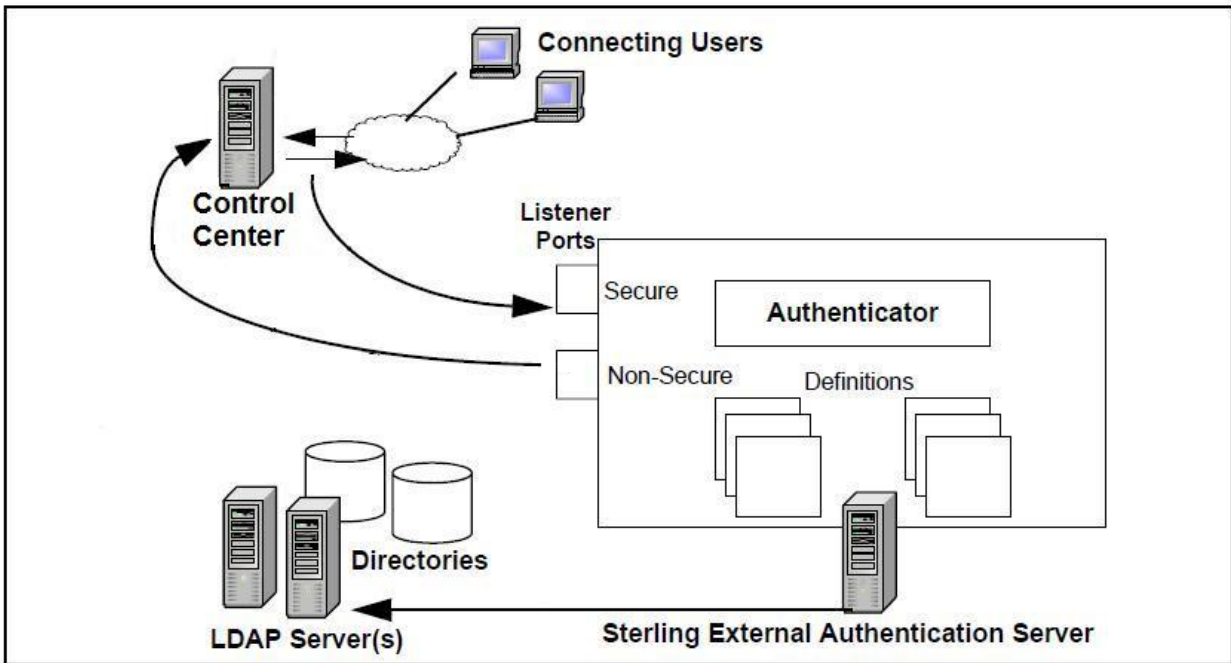
Users, for which external authentication is used, do not have to maintain their passwords in Sterling Control Center.

To use this feature, you must upgrade to Sterling Control Center 5.2.03.

Details

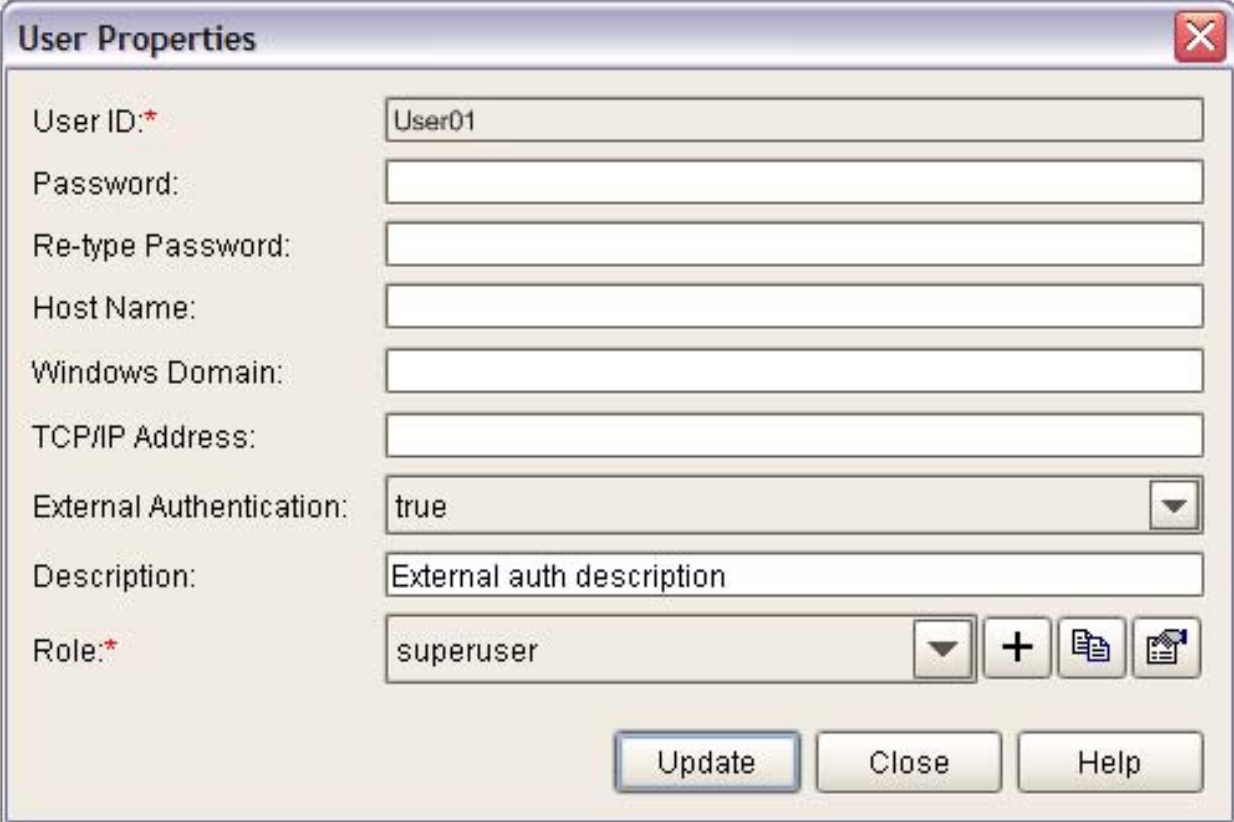
Sterling Control Center is able to utilize LDAP accessible directories to validate the credentials of users that connect to it via any of its supported interfaces, including the Sterling Control Center Console, the Sterling Control Center Web Console, the Sterling Control Center Batch Creation utility, and the Java-based Node Configuration Application Programming Interface (CCNCAPi).

When users attempt to connect to the Sterling Control Center engine, the engine checks to see if the user ID is to be externally authenticated or not, and for those that are, Sterling Control Center communicates with the Sterling External Authentication Server it is configured to use to perform the user credential validation task.



Control Center Users

Below is a screen shot of the User Properties for a Sterling Control Center user configured to be externally authenticated. External authentication for the user named User01 will be performed because the External Authentication attribute is set to true:



The screenshot shows a 'User Properties' dialog box with the following fields and values:

User ID:*	User01
Password:	
Re-type Password:	
Host Name:	
Windows Domain:	
TCP/IP Address:	
External Authentication:	true
Description:	External auth description
Role:*	superuser

Buttons: Update, Close, Help

To tell Sterling Control Center to validate user credentials via its own store of User IDs and passwords, set the External Authentication attribute to false.

You may specify values for one, or more, of the following attributes, whether External Authentication is set true or false, and they will be validated:

- Password
- Host Name
- Windows Domain
- TCP/IP Address

Note if the External Authentication attribute is true, you may not specify a password value.

The default is to not use external authentication for Sterling Control Center users.

Refer to the *IBM® Sterling Control Center Administration Guide* chapter titled Manage Roles and Users for further instructions on creating and maintaining Sterling Control Center users.

Sterling External Authentication Server Connections

To perform external authentication of user credentials, in addition to setting up users to be externally authenticated, Sterling Control Center must be configured to communicate with a Sterling External Authentication Server (version 2.3.01 or later). Sterling Control Center may be configured with both a Primary, and Alternate, Sterling External Authentication Server to use for user credential validation via its System Settings.

The screenshot shows a window titled "System Settings" with a red close button in the top right corner. The window has a tabbed interface with the following tabs: Database, E-mail, SNMP Hosts, Application Log, Services, Engine Connection, and Console. The "External Authentication Server" tab is selected and active. Below the tabs, there are two sub-tabs: "License Management" and "File Agent". The "External Authentication Server" sub-tab is selected. The main content area of the dialog is titled "External Authentication Server" and contains the following fields:

- Primary Address: * (text input field)
- Primary Port: * (text input field)
- Alternate Address: (text input field)
- Alternate Port: (text input field)
- Profile Name: * (text input field)
- Secure Connection: (dropdown menu showing "true")

At the bottom of the dialog, there are three buttons: "Update", "Cancel", and "Help".

When a connection is unable to be made to the Sterling External Authentication Server at the Primary Address and Port by the engine to validate user credentials, Sterling Control Center will attempt to connect to the Sterling External Authentication Server at the Alternate Address and Port, if specified.

Note if all Sterling Control Center users are configured for External Authentication, and the Sterling Control Center engine is unable to connect with a Sterling External Authentication Server to perform user credential validation, no users will be able to log on to Sterling Control Center. You may want to leave at least one Sterling Control Center user, capable of performing administrative tasks, not externally authenticated for just such occasions.

Refer to the *IBM Sterling Control Center Administration Guide* chapter titled Sterling Control Center Settings for further instructions on setting and maintaining Sterling Control Center System Settings.

Secure Connections to a Sterling External Authentication Server

When a secure connection between Sterling Control Center and a Sterling External Authentication Server is to be used, and you are strongly advised to do so to keep passwords safe, additional configuration must be done for both the Sterling Control Center and the Sterling External Authentication Server. For Sterling Control Center, both a Key Store and Trust Store must be configured for its use in order to establish a secure connection between it and a Sterling External Authentication Server. Likewise, for the Sterling External Authentication Server, the System Settings for Secure Listener must be set and enabled, and a Key Store and Trust Store must also be configured.

Note only one Key and Trust store may be configured for Sterling Control Center's use. I.e., the same Key and Trust Store configured for use by secure Sterling Control Center client connections, and for secure connections to monitored servers by Sterling Control Center, is also used for communications between Sterling Control Center and a Sterling External Authentication Server.

To configure the Key Store and Trust Store, use the Sterling Control Center configCC utility.

```
C:\WINDOWS\system32\cmd.exe - configcc

-----
Config step : Keystore / Trust Store configuration ...
Warning: Please specify a valid keystore.<See the documentation to
build one>
Otherwise the 'secure' connectors may not start.
-----

Keystore and Trust Store have been already configured.
Do you want to re-configure Keystore and Trust Store<Y/N>?y
Are you sure<Y/N>?y
Keystore and Trust Store configuration ...
Please provide path to java keystore [..\conf\security\CCenter.keystore] :
Please provide password to the keystore <at least 6 chars, no blanks> :
Re-enter Password :
Please provide path to trust store [c:\jdk1.6.0_21\jre\lib\security\cacerts] :
Please provide hostname of the engine install [dander2010] :

You have provided the following value(s)
Path to Keystore : ..\conf\security\CCenter.keystore
Password for Keystore : *****
Path to Trust Store(optional): c:\jdk1.6.0_21\jre\lib\security\cacerts
Password for Trust Store : *****
Hostname of engine install : dander2010

Are these correct<Y/N>?[Y]
```

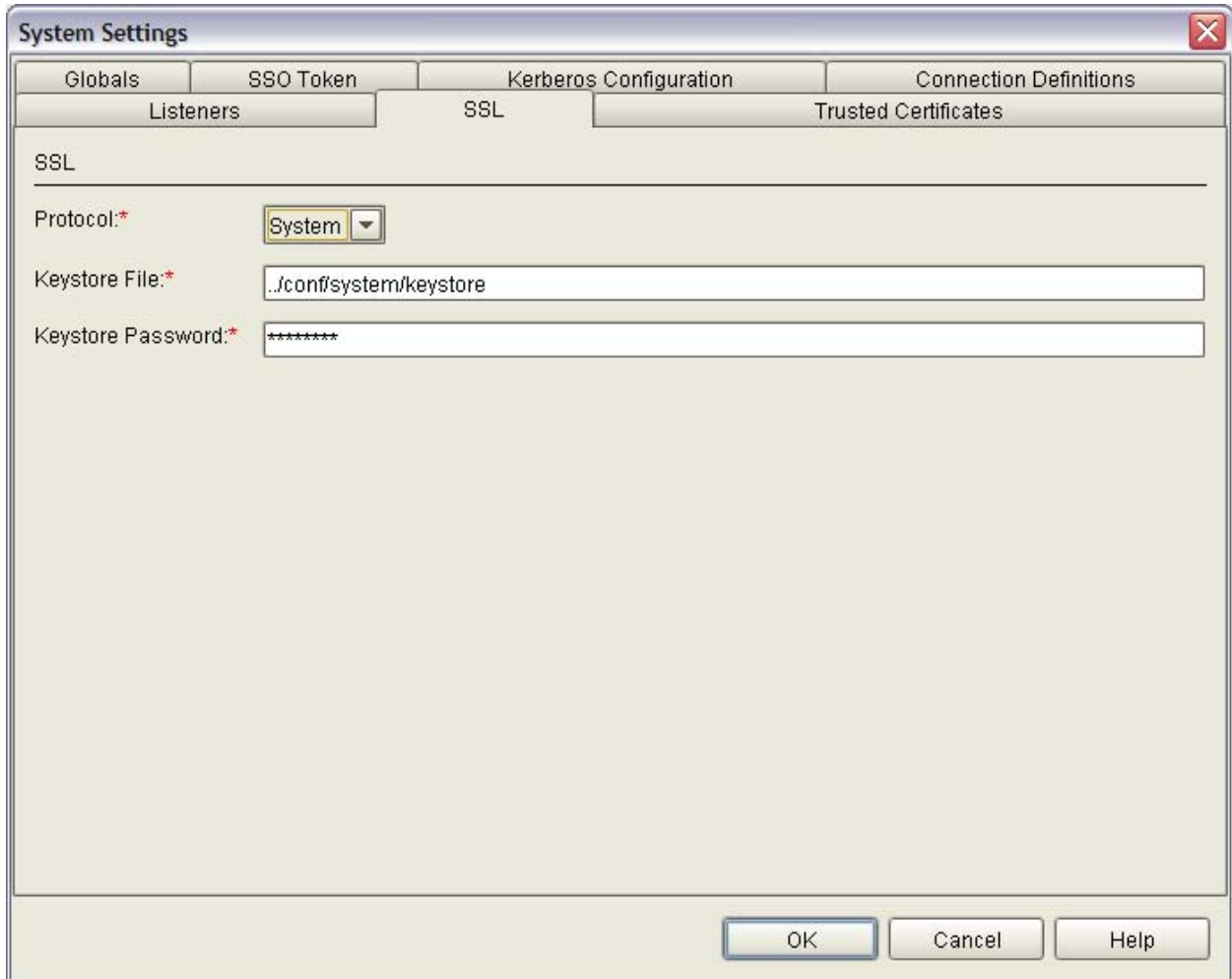

Refer to the section named Change Engine Settings After Installation in the *IBM Sterling Control Center Getting Started Guide* chapter titled Install Sterling Control Center for further instructions on running configCC.

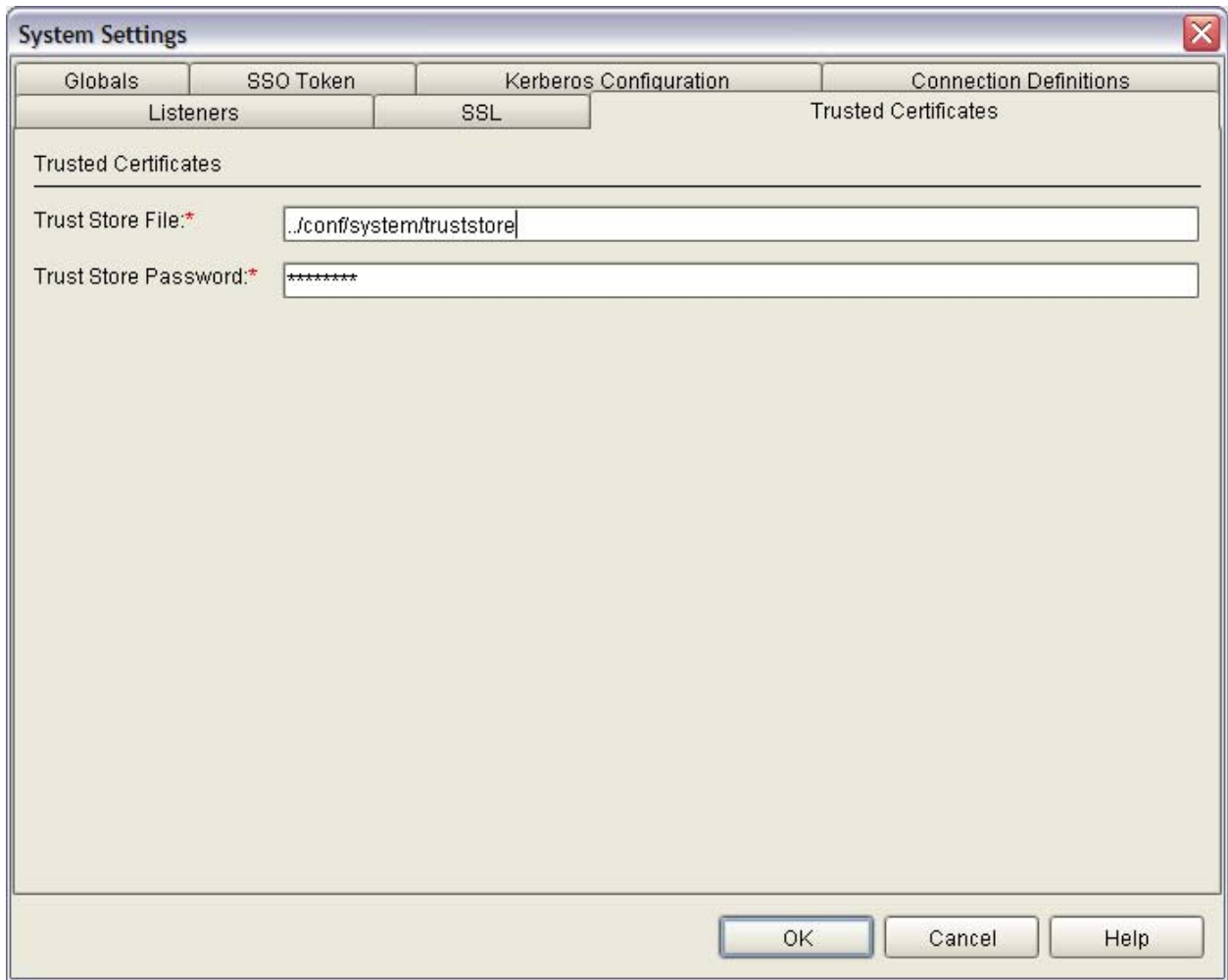
For the Sterling External Authentication Server, the Sterling External Authentication Server GUI must be used to enable it to accept secure connections. Refer to the *Sterling External Authentication Server Implementation Guide* chapter Configure System Resources for instructions on how to configure this.

At a minimum, a Secure Listener port must be specified and enabled via the Sterling External Authentication Server GUI:

The screenshot shows a 'System Settings' dialog box with a tabbed interface. The 'Listeners' tab is active, and the 'SSL' sub-tab is selected. The 'Secure Listener' section includes an empty 'IP Address' field, a 'Port:*' field containing '61366', an empty 'Keystore Alias' field, and a checked 'Enabled' checkbox. The 'Non-Secure Listener' section includes an empty 'IP Address' field, a 'Port:*' field containing '61365', and a checked 'Enabled' checkbox. At the bottom right, there are 'OK', 'Cancel', and 'Help' buttons.

A Key Store and Trust Store File must also be configured via the Sterling External Authentication Server GUI:



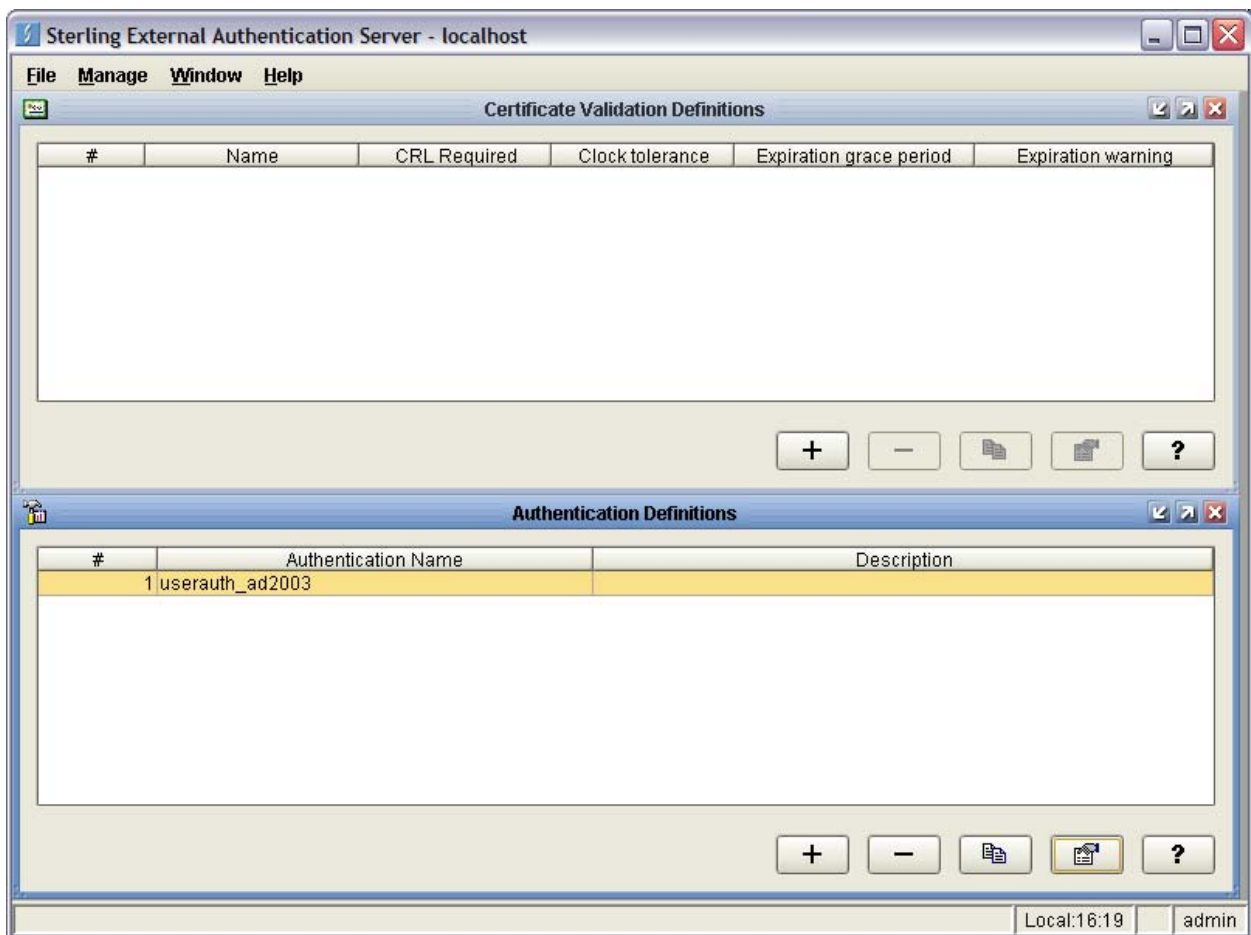


Sterling External Authentication Server Profiles

A Sterling External Authentication Server Profile Name, which identifies a Sterling External Authentication Server Authentication Definition for the Sterling External Authentication Server to use when validating credentials for Sterling Control Center, must be set in addition to configuring the address and port of the Sterling External Authentication Server servers to utilize for credential validation in the Sterling Control Center External Authentication Server System Settings. This Sterling External Authentication Server Profile Name specified must also be preconfigured in the Sterling External Authentication Server used by Sterling Control Center for external authentication to succeed.

Refer to the *Sterling External Authentication Server Implementation Guide* chapter Create and Manage LDAP Authentication Definitions for instructions on how to create and edit Authentication Definitions.

Below are screen shots of the Sterling External Authentication Server GUI with the Authentication Definition referred to by the Sterling Control Center External Authentication System Setting Profile Name. This particular Profile, or Authentication Definition, named userauth_ad2003 was actually used with a Microsoft Active Directory™ 2003 server:



LDAP Authentication properties for Authentication Definition userauth_ad2003:

The screenshot shows a dialog box titled "Update authentication definition" with a close button in the top right corner. The dialog has a tabbed interface with four tabs: "Attribute Query Definitions", "Application Output Definition", "Attribute Assertion Definitions", and "Summary". The "LDAP Authentication" tab is selected, and it contains sub-sections for "LDAP Connection Settings" and "Change Password Settings". The main content area is titled "LDAP Authentication" and includes a small icon and the text "userauth_ad2003".

Profile name*: userauth_ad2003

Description:

Authentication type: LDAP

Protocol: ldap://

Host: xx.xx.xxx.xxx

Port: xxx

LDAP principal to bind:

- User ID from request
- Search for user DN ...
- Specify user DN cn=(userid), CN=Users,DC=TestDomain,DC=Test
- DN from Certificate Validation
- Other principal format

Buttons: OK, Cancel, Help

LDAP Connection Settings properties for Authentication Definition userauth_ad2003:

The screenshot shows a dialog box titled "Update authentication definition" with a close button (X) in the top right corner. The dialog has four tabs: "Attribute Query Definitions", "Application Output Definition", "Attribute Assertion Definitions", and "Summary". The "LDAP Authentication" sub-tab is active, and within it, the "LDAP Connection Settings" sub-tab is selected. The "Change Password Settings" sub-tab is also visible. The main content area is titled "LDAP Connection Settings" and includes a small icon and the text "userauth_ad2003". The settings are as follows:

- Authentication Method: Simple (dropdown)
- Principal Name: cn={userid},CN=Users,DC= TestDomain,DC= Test (text field)
- Principal Password: [Redacted with asterisks] (password field)
- Client Key Certificate Alias: [Empty] (text field)
- LDAP Version: [Empty] (dropdown)
- Start TLS: No (dropdown)
- Referral Action: Follow (dropdown)
- Advanced options: [Ellipsis button]

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

Nothing was specified for Change Password Settings, Attribute Query Definitions, Application Output Definition, or Attribute Assertion Definitions in this Authentication Definition.

Trouble Shooting

Be sure you are using a Sterling External Authentication Server version 2.3.01 or later.

Users configured for External Authentication may see the following error when attempting to logon to the Sterling Control Center engine:



This error may occur simply because an invalid password was entered or because of a communication problem between the Sterling Control Center engine and the Sterling External Authentication Server it is configured to use. To know if the problem is caused by a communications problem, refer to the Sterling Control Center engine log file.

Whenever Sterling Control Center connects to the Sterling External Authentication Server, log file records will be written indicating whether a secure, or non secure connection is to be established, whether the Primary Sterling External Authentication Server or Alternate Sterling External Authentication Server is being connected to, the address and port of the Sterling External Authentication Server being connected to, and for secure connections, the type and location of the Key and Trust Store used:

```
25 Mar 2011 08:23:01,984 86875 [Thread-422] INFO SeasService - SeasService about to initiate
Secure connection to SEAS
25 Mar 2011 08:23:01,984 86875 [Thread-422] INFO SeasService - javax.net.ssl.keyStore =
|c:\Program Files\Sterling Commerce\SEAS\conf\system\keystore|
25 Mar 2011 08:23:01,984 86875 [Thread-422] INFO SeasService - javax.net.ssl.keyStoreType =
|jks|
25 Mar 2011 08:23:01,984 86875 [Thread-422] INFO SeasService - javax.net.ssl.trustStore =
|c:\Program Files\Sterling Commerce\SEAS\conf\system\truststore|
25 Mar 2011 08:23:01,984 86875 [Thread-422] INFO SeasService - Attempting to connect to Primary
SEAS host:port = 127.0.0.1:61366
25 Mar 2011 08:23:02,625 87516 [Thread-422] INFO SeasService - Connected to Primary SEAS
25 Mar 2011 08:23:02,921 87812 [Thread-422] INFO SccContextChecker - successful extended
validation attempt for dander from userid(dander) domain(DANDER2010) host(dander2010)
ip(9.65.32.41)
```

A Log file record like the following is simply an indication of an invalid password being used for a user being externally authenticated:

```
25 Mar 2011 10:25:59,750 7464641 [Thread-47776] ERROR SccContextChecker -
    java.lang.Exception: Client external authentication password check failed
    Stack Trace:
    java.lang.Exception: Client external authentication password check failed
    at
com.sterlingcommerce.scc.agent.services.jmx.SccContextChecker.extendedValidate(SccContextChecker.
java:377)
    at
com.sterlingcommerce.scc.agent.services.security.AccessControl.isExtendedAuthAllowed(AccessContro
l.java:1025)
    at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
    at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:39)
    at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:25)
    at java.lang.reflect.Method.invoke(Method.java:597)
    at
com.sun.jmx.mbeanserver.StandardMBeanIntrospector.invokeM2(StandardMBeanIntrospector.java:93)
    at
com.sun.jmx.mbeanserver.StandardMBeanIntrospector.invokeM2(StandardMBeanIntrospector.java:27)
    at com.sun.jmx.mbeanserver.MBeanIntrospector.invokeM(MBeanIntrospector.java:208)
    at com.sun.jmx.mbeanserver.PerInterface.noSuchMethod(PerInterface.java:193)
    at com.sun.jmx.mbeanserver.PerInterface.invoke(PerInterface.java:94)
    at com.sun.jmx.mbeanserver.MBeanSupport.invoke(MBeanSupport.java:262)
    at
com.sun.jmx.interceptor.DefaultMBeanServerInterceptor.invoke(DefaultMBeanServerInterceptor.java:8
36)
    at com.sun.jmx.mbeanserver.JmxMBeanServer.invoke(JmxMBeanServer.java:761)
    at com.sun.jdmk.MBeanServerForwarder.invoke(MBeanServerForwarder.java:281)
    at com.sun.jdmk.MBeanServerChecker.invoke(MBeanServerChecker.java:337)
    at
com.sterlingcommerce.scc.agent.services.jmx.SccContextChecker.invoke(SccContextChecker.java:305)
    at com.sun.jdmk.comm.GenericHttpRequestHandler.invoke(GenericHttpRequestHandler.java:559)
    at
com.sun.jdmk.comm.GenericHttpRequestHandler.doOperation(GenericHttpRequestHandler.java:285)
    at
com.sun.jdmk.comm.GenericHttpRequestHandler.processPostRequest(GenericHttpRequestHandler.java:235
)
    at
com.sun.jdmk.comm.GenericHttpClientHandler.processRequest(GenericHttpClientHandler.java:193)
    at com.sun.jdmk.comm.GenericHttpClientHandler.doRun(GenericHttpClientHandler.java:113)
    at com.sun.jdmk.comm.ClientHandler.run(ClientHandler.java:135)
    at java.lang.Thread.run(Thread.java:619)
```

Log file records like the following indicate an issue with the secure connection configuration setup between Sterling Control Center and the Sterling External Authentication Server:

```
25 Mar 2011 10:29:35,578 7680469 [Thread-49180] ERROR SeasService - Unable to connect to either
Primary or Alternate SEAS: javax.net.ssl.SSLHandshakeException: Remote host closed connection
during handshake
25 Mar 2011 10:29:35,578 7680469 [Thread-49180] ERROR SeasService - Exception occurred validating
password for user: dander - javax.net.ssl.SSLHandshakeException: Remote host closed connection
during handshake
```

You should revisit the port values configured for secure connections, as well as the trust and key store locations and contents, if this error is incurred.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual

Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

1623-14, Shimotsuruma, Yamato-shi

Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT,

MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA __95141-1003

U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM

products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available. This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© IBM 2011. Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. 2011.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Connect Control Center®, Connect:Direct®, Connect:Enterprise, Gentran®, Gentran:Basic®, Gentran:Control®, Gentran:Director®, Gentran:Plus®, Gentran:Realtime®, Gentran:Server®, Gentran:Viewpoint®, Sterling Commerce™, Sterling Information Broker®, and Sterling Integrator® are trademarks or registered trademarks of Sterling Commerce, Inc., an IBM Company.

Other company, product, and service names may be trademarks or service marks of others.