



Sparx Systems Keystore Service (SSKS) User Guide

This booklet describes the Sparx Systems Keystore Service facilities for Enterprise Architect.

The Sparx Systems Keystore Service is used to manage the registration keys issued with the Floating Licenses purchased for Enterprise Architect Corporate, Business & Software Engineering, Systems Engineering, and Ultimate editions, and for related MDG products.



Sparx Systems Keystore Service User Guide

© 2005-2012 Sparx Systems Pty Ltd

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Printed: May 2012

Publisher

Sparx Systems

Managing Editor

Geoffrey Sparks

Technical Editor

Michael Fraser

Special thanks to:

All the people who have contributed suggestions, examples, bug reports and assistance in the development of the Sparx Systems Keystore Service. The task of developing and maintaining this tool has been greatly enhanced by their contribution.

Table of Contents

Foreword	1
Introduction	2
Copyright Notice	3
End User License Agreement	4
Support	7
Your Feedback	8
Install the Keystore Service	9
Start/Stop the Keystore Service	11
Configure the Keystore Service	12
Active Directory Configuration File	15
SSKS Configuration File	17
Keystore Service Administration	19
Connect To a Remote Keystore	20
Add Shared Keys	21
Set Issue Periods for the Keys	22
Migrate Shared Keys From File-Based Keystore	24
Release Shared Keys	26
Delete Shared Keys	27
Configure Enterprise Architect to Acquire Keys From Keystore	28
Activity Logs	29
Troubleshooting	30
Index	33

Foreword

The Sparx Systems Keystore Service is used to manage the registration keys issued with the Floating Licenses purchased for Enterprise Architect Corporate, Business and Software Engineering, Systems Engineering, and Ultimate editions, and for related MDG products.

1 Introduction

The *Sparx Systems Keystore Service* (SSKS) helps you to manage the use of registration keys issued with the Floating Licenses purchased for Enterprise Architect Corporate, Business & Software Engineering, Systems Engineering, and Ultimate editions, and for related MDG products.

Using the Sparx Systems Keystore Service application, an administrator can create a key store in a network file location that enables licenses with a finite (administrator-defined) issue period to be assigned to specific workstations. The key store also enables the administrator to quickly determine which user has a particular key, and to see the date on which the key expires.

Note:

Each Enterprise Architect workstation can be associated with only one key store at a time.

See Also

- [Copyright Notice](#) ^[3]
- [End User Licensing Agreement](#) ^[4]
- [Support](#) ^[7]
- [Your Feedback](#) ^[8]
- [Install the Keystore Service](#) ^[9]
- [Start/Stop the Keystore Service](#) ^[11]
- [Configure the Keystore Service](#) ^[12]
- [Sparx Systems Keystore Service Administration](#) ^[19]
- [Configure Enterprise Architect to Acquire Keys from Keystore](#) ^[28]
- [Activity Logs](#) ^[29]
- [Troubleshooting](#) ^[30]

1.1 Copyright Notice

Copyright © 1998-2012 Sparx Systems Pty. Ltd. All rights reserved

The software contains proprietary information of Sparx Systems Pty Ltd. It is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law. Reverse engineering of the software is prohibited. Please read the [license agreement](#)⁴ for full details.

Due to continued product development, this information can change without notice. The information and intellectual property contained herein is confidential between Sparx Systems and the client and remains the exclusive property of Sparx Systems. If you find any problems in the documentation, please report them to us in writing. Sparx Systems does not warrant that this document is error-free. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of Sparx Systems. Licensed users are granted the right to print a single hardcopy of the user manual per licensed copy of the software, but may not sell, distribute or otherwise dispose of the hardcopy without written consent of Sparx Systems.

Sparx Systems Pty. Ltd.

7 Curtis St,
Creswick, Victoria 3363,
AUSTRALIA

Phone: +61 (3) 5345 1140

Fax: +61 (3) 5345 1104

Support Email: support@sparxsystems.com

Sales Email: sales@sparxsystems.com

Website: www.sparxsystems.com

1.2 End User License Agreement

Sparx Systems Keystore Service (SSKS)

Copyright (C) 1998-2012 Sparx Systems Pty Ltd. All Rights Reserved

IMPORTANT- READ CAREFULLY: This End User License Agreement ("EULA") is a legal agreement between YOU as Licensee and SPARX for the SOFTWARE PRODUCT identified above. By installing, copying, or otherwise using the SOFTWARE PRODUCT, YOU agree to be bound by the terms of this EULA. If YOU do not agree to the terms of this EULA, promptly return the unused SOFTWARE PRODUCT to the place of purchase for a full refund.

The copyright in the SOFTWARE PRODUCT and its documentation is owned by Sparx Systems Pty Ltd A.C.N 085 034 546. Subject to the terms of this EULA, YOU are granted a non-exclusive right for the duration of the EULA to use the SOFTWARE PRODUCT. YOU do not acquire ownership of copyright or other intellectual property rights in any part of the SOFTWARE PRODUCT by virtue of this EULA.

Your use of this software indicates your acceptance of this EULA and warranty.

DEFINITIONS

In this End User License Agreement, unless the contrary intention appears:

- "EULA" means this End User License Agreement.
- "SPARX" means Sparx Systems Pty Ltd A.C.N 085 034 546.
- "Licensee" means YOU, or the organization (if any) on whose behalf YOU are taking the EULA.
- "SOFTWARE PRODUCT" or "SOFTWARE" means Sparx Systems Keystore Service, which includes computer software and associated media and printed materials, and may include online or electronic documentation.
- "Support Services" means email based support provided by SPARX, including advice on usage of Sparx Systems Keystore Service, investigation of bugs, fixes, repairs of models if and when appropriate, and general product support.
- "SPARX support engineers" means employees of SPARX who provide on-line support services.

GRANT OF LICENSE

In accordance with the terms of this EULA YOU are granted the following rights:

- a) To install and use one copy of the SOFTWARE PRODUCT or, in its place, any prior version for the same operating system, on a single computer. As the primary user of the computer on which the SOFTWARE PRODUCT is installed, YOU may make a second copy for your exclusive use on either a home or portable computer.
- b) To store or install a copy of the SOFTWARE PRODUCT on a storage device, such as a network server, used only to install or run the SOFTWARE PRODUCT over an internal network. If YOU want to increase the number of users entitled to concurrently access the SOFTWARE PRODUCT, YOU must notify SPARX and agree to pay an additional fee.
- c) To make copies of the SOFTWARE PRODUCT for backup and archival purposes.

ADDITIONAL RIGHTS AND LIMITATIONS

YOU hereby undertake not to sell, rent, lease, translate, adapt, vary, modify, decompile, disassemble, reverse engineer, create derivative works of, modify, sub-license, loan or distribute the SOFTWARE PRODUCT other than as expressly authorized by this EULA.

YOU further undertake not to reproduce or distribute license key-codes except under the express and written permission of SPARX.

ASSIGNMENT

YOU may only assign all your rights and obligations under this EULA to another party if YOU supply to the transferee a copy of this EULA and all other documentation including proof of ownership. Your license is then terminated.

TERMINATION

Without prejudice to any other rights, SPARX may terminate this EULA if YOU fail to comply with the terms and conditions. Upon termination YOU or YOUR representative shall destroy all copies of the SOFTWARE PRODUCT and all of its component parts or otherwise return or dispose of such material in the manner directed by SPARX.

WARRANTIES AND LIABILITY

WARRANTIES

SPARX warrants that the SOFTWARE PRODUCT will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt, and any Support Services provided by SPARX shall be substantially as described in applicable written materials provided to YOU by SPARX, and SPARX support engineers will make commercially reasonable efforts to solve any problems associated with the SOFTWARE PRODUCT.

EXCLUSIONS

To the maximum extent permitted by law, SPARX excludes, for itself and for any supplier of software incorporated in the SOFTWARE PRODUCT, all liability for all claims, expenses, losses, damages and costs made against or incurred or suffered by YOU directly or indirectly (including without limitation lost costs, profits and data) arising out of:

- YOUR use or misuse of the SOFTWARE PRODUCT
- YOUR inability to use or obtain access to the SOFTWARE PRODUCT
- Negligence of SPARX or its employees, contractors or agents, or of any supplier of software incorporated in the SOFTWARE PRODUCT, in connection with the performance of SPARX' obligations under this EULA, or
- Termination of this EULA by either party for any reason.

LIMITATION

The SOFTWARE PRODUCT and any documentation are provided "AS IS" and all warranties whether express, implied, statutory or otherwise, relating in any way to the subject matter of this EULA or to this EULA generally, including without limitation, warranties as to: quality, fitness; merchantability, correctness; accuracy; reliability; correspondence with any description or sample, meeting your or any other requirements; uninterrupted use; compliance with any relevant legislation and being error or virus free are excluded. Where any legislation implies in this EULA any term, and that legislation avoids or prohibits provisions in a contract excluding or modifying such a term, such term shall be deemed to be included in this EULA. However, the liability of SPARX for any breach of such term shall if permitted by legislation be limited, at SPARX's option to any one or more of the following upon return of the SOFTWARE PRODUCT and a copy of the receipt:

- If the breach relates to the SOFTWARE PRODUCT:
 - the replacement of the SOFTWARE PRODUCT or the supply of an equivalent SOFTWARE PRODUCT
 - the repair of such SOFTWARE PRODUCT
 - the payment of the cost of replacing the SOFTWARE PRODUCT or of acquiring an equivalent SOFTWARE PRODUCT, or
 - the payment of the cost of having the SOFTWARE PRODUCT repaired.
- If the breach relates to services in relation to the SOFTWARE PRODUCT:
 - the supplying of the services again, or
 - the payment of the cost of having the services supplied again.

TRADEMARKS

All names of products and companies used in this EULA, the SOFTWARE PRODUCT, or the enclosed documentation may be trademarks of their corresponding owners. Their use in this EULA is intended to be in compliance with the respective guidelines and licenses.

Windows®, Windows 98, Windows NT, Windows ME, Windows XP, Windows Vista, Windows 2000 and Windows 2003 Server are trademarks of Microsoft®.

GOVERNING LAW

This agreement shall be construed in accordance with the laws of the Commonwealth of AUSTRALIA.

1.3 Support

Technical support for Sparx Systems Keystore Service is available to registered users. Responses to support queries are sent by email. Sparx Systems endeavors to provide a rapid response to all product-related questions or concerns.

Registered users can lodge a support request, by visiting: http://www.sparxsystems.com/registered/reg_support.html.

An online user forum is also available for your questions and perusal, at <http://www.sparxsystems.com/cgi-bin/yabb/YaBB.cgi>.

1.4 Your Feedback

Sparx Systems likes to stay in touch with what the Sparx Systems Keystore Service users require in order to accomplish their tasks efficiently and effectively. We value any suggestions, feedback and comments you might have regarding this product, documentation or install process.

You can access our online feedback pages at:

- www.sparxsystems.com/bug_report.htm and
- www.sparxsystems.com/feature_request.htm.

Alternatively, you can contact Sparx Systems by email at: support@sparxsystems.com.

2 Install the Keystore Service

When you purchase a floating license product that uses the Sparx Systems Keystore Service, you receive an email from Sparx Systems Sales that provides:

- The installation instructions for the Keystore Service
- The location of the installer executable file (*sparxkeystore.exe*) to download
- The password that enables you to run the executable.

If you do not received the password, or have lost a previous password, please contact Sparx Systems Sales at sales@sparxsystems.com

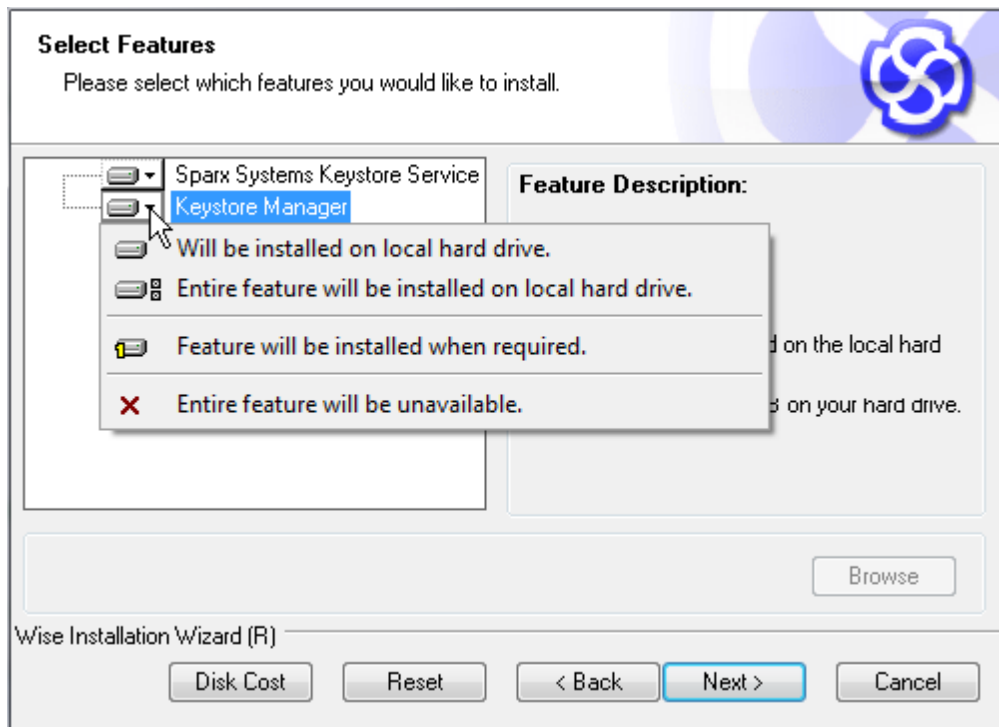
To install the Keystore Service, download and run the executable file, and enter the password.



Note: Vista/Windows 7 users

Please ensure that the installer is run with administrator permissions, by right-clicking on the *SparxKeystoreService.exe* installer file and selecting the **Run as Administrator** context menu option.

Review the license agreement and readme information, clicking on the **Next** button as you finish reading each document. The **Select Features** page displays, from which you select the features to install.

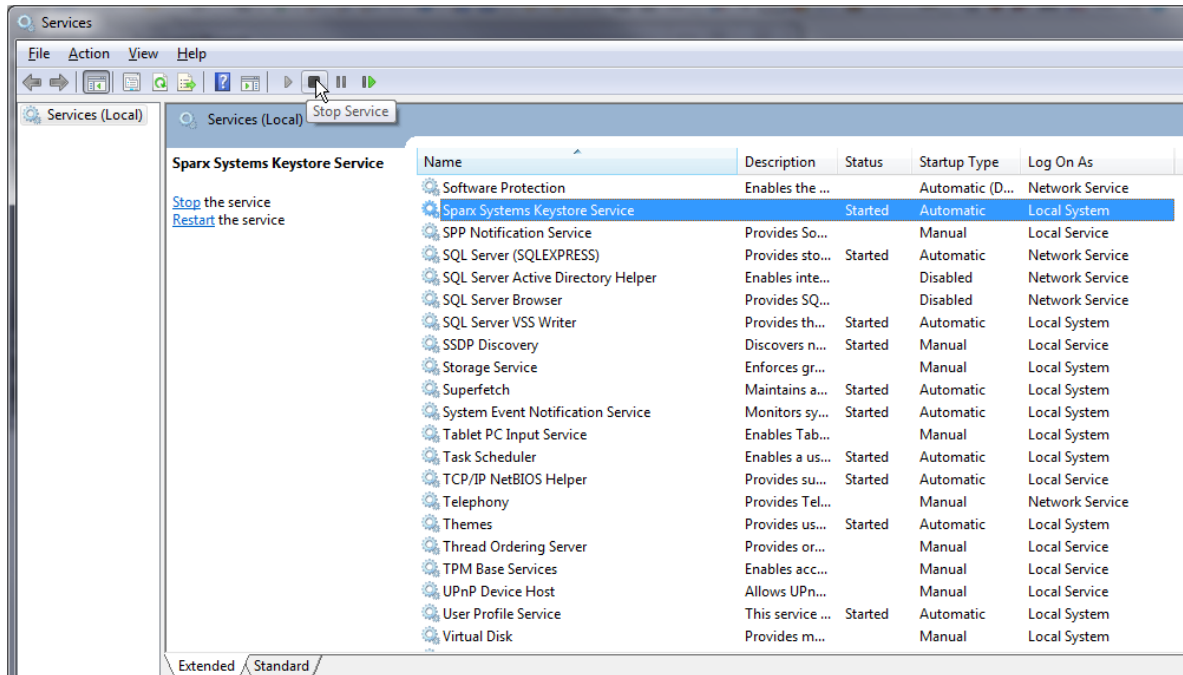


Option	Description
Sparx Systems Keystore Service	A TCP/IP service that exposes shared key management functions to remote Enterprise Architect clients. Install this feature if you would like the host machine to act as the Keystore server.
Keystore Manager	An application that facilitates administration ^[19] of a remote or local keystore (e.g. adding, removing and releasing keys). Install this feature if you would like to administer local or remote Sparx Systems Keystore Service keystores (or legacy file-based keystores) from the host machine.

Continue through the installation prompts and screens to finalize the installation. If you installed the **Sparx Systems Keystore Service** feature, the installer attempts to start the service at the end of the installation process, using the default configuration. For further information on configuring the service, please see the [Configure the Keystore Service](#)^[12] topic.

3 Start/Stop the Keystore Service

You can start and stop the Sparx Systems Keystore Service through Microsoft Windows' **Services** console. You access the **Services** console either through the **Control Panel** (under **Administrative Tools**), or by running the command `services.msc` from the command line.



Locate the **Sparx Systems Keystore Service** entry in the **Services** console and start, stop or restart it through the console toolbar buttons or context menu options.

4 Configure the Keystore Service

When starting up, the Sparx Systems Keystore Service scans its installation directory for the file *keystoreService.config*, which contains a list of properties and values used to configure the server. The properties and their descriptions are provided below.

Property	Description
SERVER_PORT	The TCP/IP port on which the service is configured to listen for incoming connections. By default the Sparx Systems Keystore Service is configured to run on port 7770 .
AUTHMETHOD	<p>The method used to authenticate Keystore Service users connecting to the service. The value of this method affects how the property AUTHMETHOD_OPTIONS is interpreted (below).</p> <p>Valid AUTHMETHOD values are:</p> <ul style="list-style-type: none"> • AM_GLOBALPASSWORD - Users authenticate with a single, global password; the password is specified in the AUTHMETHOD_OPTIONS property and can be left blank. • AM_ACTIVEDIRECTORY - Users authenticate according to Active Directory group membership; the permitted group is specified by a common name in the AUTHMETHOD_OPTIONS property, for example: <p style="text-align: center;">AUTHMETHOD_OPTIONS=SSKS_USERGROUP</p> <p>Where SSKS_USERGROUP is the Active Directory group that is authorized to use the keystore.</p> • AM_ACTIVEDIRECTORYEX - Users authenticate according to Active Directory group membership; the keys available to different groups is configured in the filename specified in the AUTHMETHOD_OPTIONS property, for example: <p style="text-align: center;">AUTHMETHOD_OPTIONS=%SERVICE_PATH%\keystoreService.adconfig</p> <p>For instructions on defining this file see: Active Directory Configuration File ^[15].</p> • AM_SSKSGROUP - Users authenticate with a group name and password; the groups and the keys available to each are specified in the filename specified in the AUTHMETHOD_OPTIONS property, for example: <p style="text-align: center;">AUTHMETHOD_OPTIONS=%SERVICE_PATH%\keystoreService.ssksgroupconfig</p> <p>For instructions on defining this file see: SSKS Configuration File ^[17].</p>
AUTHMETHOD_OPTIONS	The value of this property depends on the value specified in the AUTHMETHOD property (above); please see the description for AUTHMETHOD for more details.
KESTORE_PATH	The path to the keystore file. By default the service is configured to check

Property	Description
	<p>keys in and out from the <i>sskeys.dat</i> file, located in the installer directory.</p> <p>Note:</p> <p>The user the service is set to run as must be granted read/write permissions to the keystore file specified by KEYSTORE_PATH. If a service is set to run as the user LOCALSYSTEM, it generally has read/write access to its installation directory.</p>
MINIMUM_EA_BUILD	The minimum build of Enterprise Architect that can be serviced by the keystore. You can use this keystore server setting to deny older builds of Enterprise Architect the shared keys from this keystore.
AUDIT_TIME_PERIOD	<p>The time period (in seconds) to wait between logging audit reports. Audit reports are logged at the INFO level.</p> <p>To turn auditing off, set this property to 0 (zero).</p>
LOG_LEVEL	<p>The level of messages that are written to the log file. Higher log levels include messages from the lower levels that precede them. Valid log levels, from lowest to highest, are:</p> <ol style="list-style-type: none"> 1. FATAL - Events that result in termination of the service's execution. 2. WARNING - Events outside the normal scope of the service's operation, but that are not fatal (such as a wrong password supplied by a client). 3. REPORT - Events generated by the keystore's internal auditing mechanism. 4. INFO - Events generated within the normal scope of the service's operation (such as key checkin and checkout). 5. SYSTEM - Detailed system level events (such as client connection/disconnection, and service module startup). 6.
LOG_DIRECTORY	<p>The path to which the log files are written.</p> <p>Notes:</p> <ul style="list-style-type: none"> • This directory must already exist at service start time. • The user the service is set to run as must be granted read/write permissions to the directory specified by LOG_DIRECTORY. If a service is set to run as the user LOCALSYSTEM, it generally has read/write access to its installation directory.
LOG_FILECOUNT	<p>The number of rolling log files that the service keeps.</p> <p>Log files are kept in First-In-First-Out (FIFO) order, with the oldest log file being deleted once the LOG_FILECOUNT threshold is reached.</p>

Property	Description
LOG_FILESIZE	The size (in bytes) a log file can reach before the logging framework rolls the log files over.

Other system-level properties, such as the service startup condition and service user account, can be configured through the Microsoft Windows' **Service** console. (See the [Start/Stop the Keystore Service](#)^[11] topic for details on how to access the **Service** console.)

4.1 Active Directory Configuration File

When using the **AM_ACTIVEDIRECTORYEX** authentication method an additional configuration file is specified by the **AUTHMETHOD_OPTIONS** property. This file defines any number of groups and the permissions that each group receives. Each group is defined between **GROUP** and **END GROUP** as shown in the example below. Permissions are accumulated across all groups that a user is a member of.

```
GROUP
  Name=human_resources

  NamingContext=

  IsManager=false

  ENTITLEMENT
    Product=BusinessSuite

    Academic=false

    Limit=10
  END ENTITLEMENT
END GROUP
```

The properties belonging directly to a group are described below.

Property	Description
Name	The common name of the Active Directory group.
NamingContext	The LDAP path that represents the container that the group resides in (leave blank to use the domain's default naming context).
IsManager	Specifies whether members of this group are permitted to perform management operations (such as add/remove keys) on the keystore.

Within each group a list of entitlements may also be defined between **ENTITLEMENT** and **END ENTITLEMENT** as shown in the example above. The properties belonging to an entitlement are described below.

Property	Description
Product	The name of the product that this entitlement gives access to for users of this group. Available strings are: <ul style="list-style-type: none"> • UltimateSuite • BusinessSuite • RealTimeSuite • Corporate • Professional • Desktop

Property	Description
	<ul style="list-style-type: none">• VSIntegration• MDGLinkVS• EclipseIntegration• MDGLinkEclipse• MDGDoors• MDGSysML• MDGDDS• MDGZachman• MDGUPDM• MDGTogaf• MDGRealTime• MDGCodeAnalysis• TCSEIntegration• TCSESuite• RaQuest
Academic	Determines if this group should be given academic keys.
Limit	Optionally restrict the number of keys of this type available to this group to a subset of the keys available in the keystore.

4.2 SSKS Configuration File

When using the **AM_SSKSGROUP** authentication method an additional configuration file is specified by the **AUTHMETHOD_OPTIONS** property. This file defines any number of groups and the permissions that each group receives. Each group is defined between **GROUP** and **END GROUP** as shown in the example below.

```
GROUP
    Name=International Robotics Convention 2012

    UserName=robot2012

    Password=danger

    StartDate=2012-03-01

    EndDate=2012-03-31

    ENTITLEMENT

        Product=RealTimeSuite

        Academic=false

    END ENTITLEMENT
END GROUP
```

The properties belonging directly to a group are described below.

Property	Description
Name	A friendly name for this group.
UserName	The username that needs to be appended to the connection string when connecting as a member of this group.
Password	The password to connect to the keystore with this group.
StartDate	Optionally restrict access for this group to be allowed only after the given date. Specified as YYYY-MM-DD.
EndDate	Optionally restrict access for this group to be allowed only before the given date. Specified as YYYY-MM-DD.

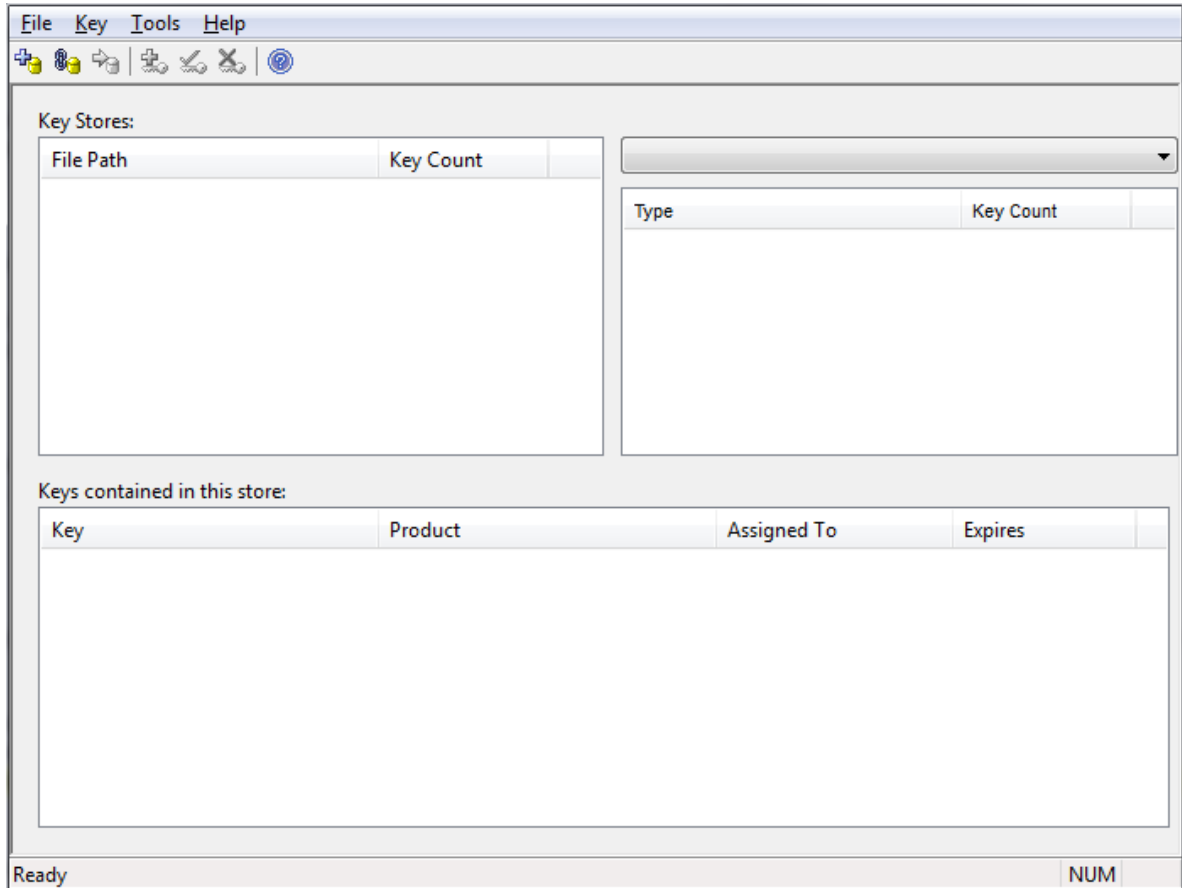
Within each group a list of entitlements may also be defined between **ENTITLEMENT** and **END ENTITLEMENT** as shown in the example above. The properties belonging to an entitlement are described below.

Property	Description
Product	The name of the product that this entitlement gives access to for users of this group. Available strings are: <ul style="list-style-type: none"> UltimateSuite

Property	Description
	<ul style="list-style-type: none">• BusinessSuite• RealTimeSuite• Corporate• Professional• Desktop• VSIntegration• MDGLinkVS• EclipseIntegration• MDGLinkEclipse• MDGDoors• MDGSysML• MDGDDS• MDGZachman• MDGUPDM• MDGTogaf• MDGRealTime• MDGCodeAnalysis• TCSEIntegration• TCSESuite• RaQuest
Academic	Determines if this group should be given academic keys.
Limit	Optionally restrict the number of keys of this type available to this group to a subset of the keys available in the keystore.

5 Keystore Service Administration

The management of shared keys within a keystore is performed through the *Keystore Manager* application, which operates through the **Sparx Systems Key Store** dialog.

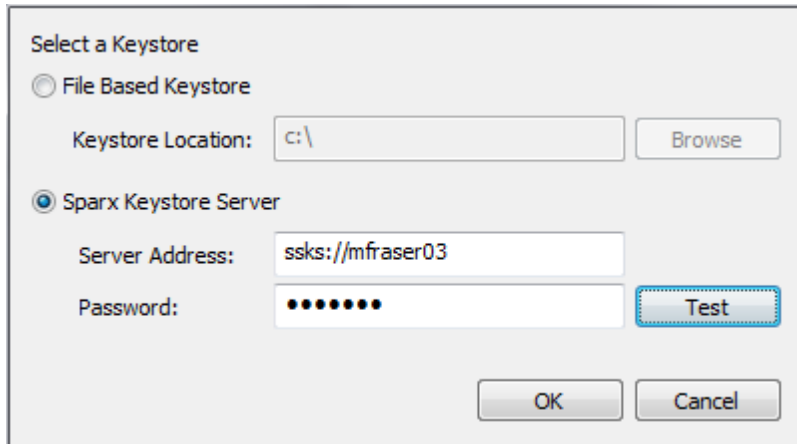


To manage a remote keystore, you must first [connect](#)^[20] the application to it and to any number of other remote keystores as required. The Keystore Manager then enables you, the administrator, to:

- [Add Shared Keys](#)^[21]
- [Set Issue Periods for Shared Keys](#)^[22]
- [Migrate Shared Keys from a Legacy File-Based Keystore](#)^[24]
- [Release Shared Keys](#)^[26]
- [Delete Shared Keys](#)^[27]

5.1 Connect To a Remote Keystore

To connect to a remote keystore, select the **File | Link To** menu option on the **Sparx Systems Key Store** dialog. The **Shared Keystore Selection** dialog displays.



Select a Keystore

File Based Keystore

Keystore Location:

Sparx Keystore Server

Server Address:

Password:

(Alternatively, to display this dialog click on the **Link to existing store** icon in the toolbar, or right-click in the **Key Stores** panel and select the **Link to** context menu option.)

Select the **Sparx Keystore Server** radio button to indicate that you want to connect to a remote service. (The **File Based Keystore** option is there to provide backwards compatibility with legacy file-based keystores; see *Migrate Shared Keys from a Legacy File-Based Keystore*, below.)

In the **Server Address** field, type the URI to the Sparx Systems Keystore Service server. If the authentication module you choose requires a password, type that into the **Password** field.

To test connectivity to the server with the credentials you have entered, click on the **Test** button. If the connection fails, review the address, password and permissions. Once the connection succeeds, click on the **OK** button to finalize the connection to the server.

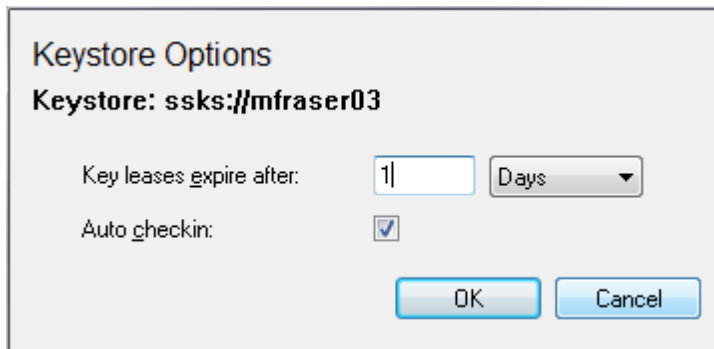
The **Sparx Systems Key Store** dialog redisplay with the path of the remote keystore in the **Keystores** panel.

5.3 Set Issue Periods for the Keys

The Sparx Systems Keystore Service helps you to:

- Ensure that the number of people using Enterprise Architect is limited to the number of floating licenses that have been purchased
- Enable people to operate Enterprise Architect using a floating license while disconnected (e.g. using a laptop computer).

To achieve this, select the key store from the **Key Stores** section of the **Sparx Systems Keystore Service** dialog, and then select the **Tools | Options** menu option. The **Options** dialog displays.



(Alternatively, to display this dialog right-click on the keystore name in the **Key Stores** panel and select the **Options** context menu option.)

When most people close Enterprise Architect they no longer require their license. Therefore there is little point in continuing to allocate the license to a user who is not actually using Enterprise Architect.

- On the **Options** dialog, you select the **Auto checkin** checkbox so that any license in the key store is automatically returned to the key store when the user closes Enterprise Architect. Click on the **OK** button to confirm your selection. When the user closes Enterprise Architect, the key is then available to the next user who wants to do some work in Enterprise Architect.

However, a laptop user, having closed Enterprise Architect, might still want to use the license off-site, with no access to the key store and therefore no way to request another key. While the laptop user can put their machine into *standby* or *hibernate* mode while leaving Enterprise Architect running, there is the risk that the laptop might have to be rebooted. Once Enterprise Architect restarts it will report the lack of a license - the license having been automatically checked in.

- To enable such users to have access to Enterprise Architect, you could *deselect* the **Auto checkin** checkbox for the keys in the key store. Click on the **OK** button to confirm your selection.

This acts against the purpose of having the checkbox. It is therefore advisable to create *two* key stores, each with a different setting for **Auto checkin**:

Target	Auto checkin
Mobile users who want to use Enterprise Architect from home or other disconnected locations.	Not selected
Fixed users who leave their computers at work.	Selected

If a user has a key with no automatic check-in, they then have use of the key for a theoretically unlimited time. However, the Sparx Systems Keystore Service also enables an administrator to limit use by setting an issue period for the keys in the key store. The period is counted as continuous time spent away from the network connection to the key store. The issue period can be set in either weeks or days

For example, if a user has a license with an issue period of one week and is away from an active connection to the key store for more than one week, they cannot use Enterprise Architect until they obtain another key.

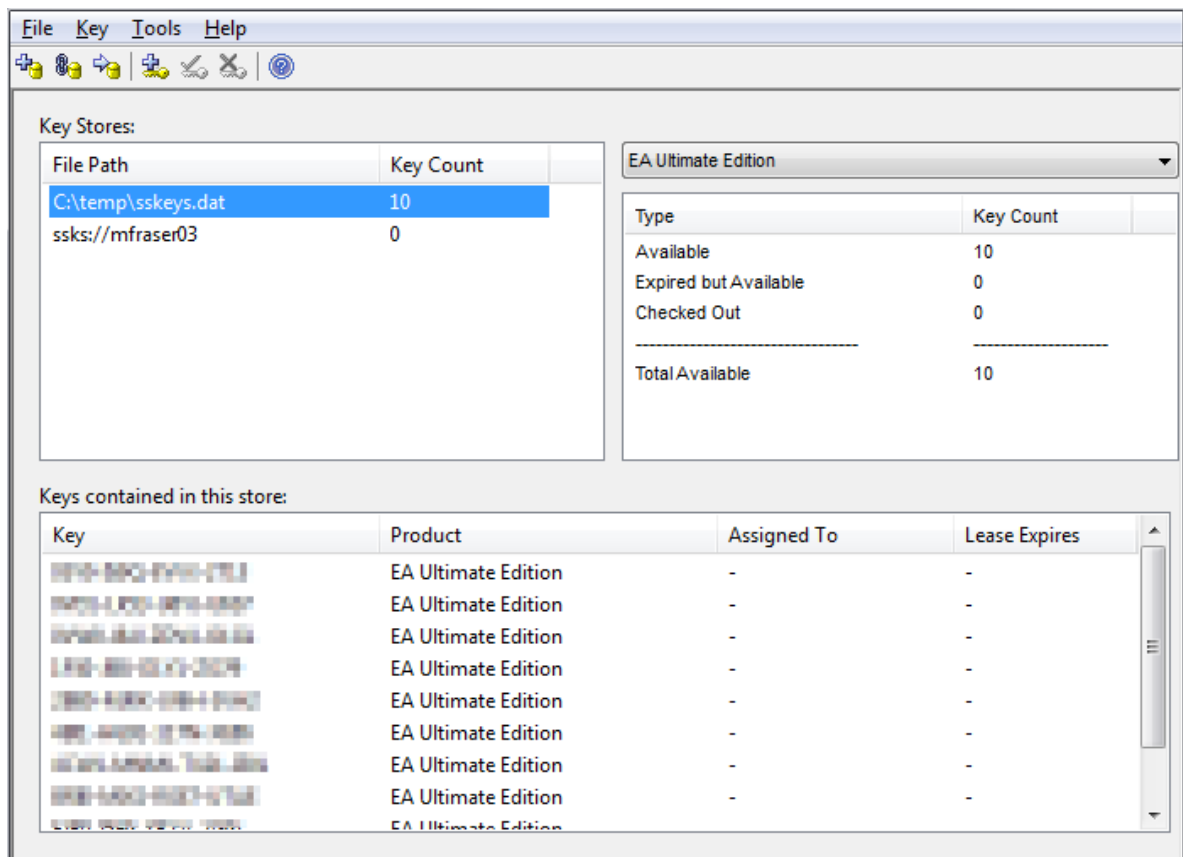
To set the issue period for the keys in the key store:

- In the first **Keys leases expire after** field, type the required *number* of units; in the second field, click on the drop-down arrow and select the unit - **Days** or **Weeks**. Click on the **OK** button to confirm your selection.

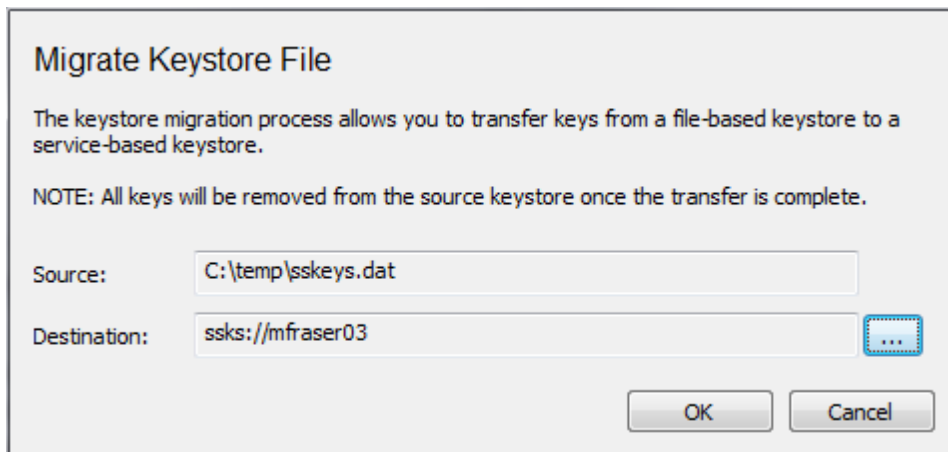
5.4 Migrate Shared Keys From File-Based Keystore

You might want to upgrade from a legacy file-based keystore and migrate your keys to a new network-based keystore. This process effectively *removes* all keys from the file-based keystore, leaving it empty, and places the keys into the network-based keystore.

To migrate the shared keys, select the **File | Link To** menu option on the **Sparx Systems Key Store** dialog (or use the [toolbar icon or context menu option](#)^[20]) and select the **File Based Keystore** option, then browse for the local keystore and click on the **OK** button to connect to it. The **Sparx Systems Key Store** dialog now resembles the following:



In the **Key Stores** panel, click on the file-based keystore path and then on the **File | Migrate To** menu option. The **Migrate Keystore File** dialog displays, with the local keystore file path in the **Source** field.



(Alternatively, to display this dialog click on the **Migrate key store** icon in the toolbar, or right-click in the **Key Stores** panel and select the **Migrate to** context menu option.)

Click on the [...] button to the right of the **Destination** field, and browse for the name of the network-based keystore into which the shared keys are to be transferred. Click on the **OK** button to migrate the shared keys from the source file-based keystore to the target service-based keystore.

5.5 Release Shared Keys

It is usually not necessary to manually release a shared key from a workstation, as this happens automatically if:

- The keystore's [AutoCheckin](#)^[22] option has been enabled and you close all running instances of Enterprise Architect on your workstation
- The lease on the key expires.

However, if further users want to access Enterprise Architect and there is some technical anomaly that has prevented the return of a key, you can manually release the key using the [Sparx Systems Key Store](#) dialog.

To release a key from active association with a particular workstation, click on the key in the [Keys contained in this store](#) panel, and then select the **Key | Release** menu option.

(Alternatively, click on the **Release Key** icon in the toolbar, or right-click on the key and select the **Release** context menu option.)

5.6 Delete Shared Keys

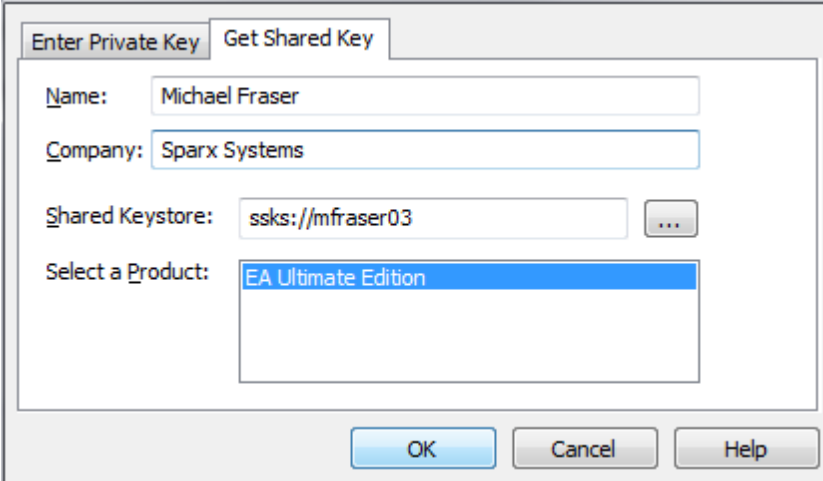
To delete a key from the keystore, open the **Sparx Systems Key Store** dialog, click on the key in the **Keys contained in this store** panel, and then select the **Key | Delete** menu option.

(Alternatively, click on the **Delete Key** icon in the toolbar, or right-click on the key and select the **Delete** context menu option.)

6 Configure Enterprise Architect to Acquire Keys From Keystore

Shared keys are available through the purchase of floating licenses for the Corporate edition of Enterprise Architect version 4.51 or later, and also the Business & Software Engineering, Systems Engineering and Ultimate editions of Enterprise Architect version 7.5 or later.

1. From the workstation, start Enterprise Architect and select the **Help | Register and Manage License Key(s)** menu option. The **License Management** dialog displays.
2. Click on the **Add Key** button; the **Add Registration Key** dialog displays.



The screenshot shows a dialog box titled "Add Registration Key" with two tabs: "Enter Private Key" and "Get Shared Key". The "Get Shared Key" tab is selected. The dialog contains the following fields and controls:

- Name:** Michael Fraser
- Company:** Sparx Systems
- Shared Keystore:** ssk://mfraser03 (with a browse button "...")
- Select a Product:** EA Ultimate Edition (with a dropdown menu)
- Buttons:** OK, Cancel, Help

3. Select the **Get Shared Key** tab.
4. In the **Name** and **Company** fields, type your user name and company name.
5. Click on the [...] button to the left of the **Shared Keystore** field and browse to the network location of the shared key store.

When connecting to a keystore using the **AM_SSKSGROUP** authentication method, the user will need to append the group name they have been given to the server path in the following format:

```
ssks://<server name>?user=<user name>
```

6. In the **Select a Product** field, select the licensed product and then click on the **OK** button.

If keys are available, one is allocated to you and you are able to continue working in Enterprise Architect.

If keys are not available, you cannot work in Enterprise Architect and must wait until another user closes Enterprise Architect and releases their key.

7 Activity Logs

The activity of the Sparx Systems Keystore Service is logged to file according to the options specified in the keystore [configuration](#) [12]. The log content resembles the following:

```

2010-03-11 15:29:11 [INFO]: #####
2010-03-11 15:29:11 [INFO]: # Sparx Systems Keystore Service #
2010-03-11 15:29:11 [INFO]: #####
2010-03-11 15:29:11 [INFO]: # Protocol Version: 1.0 #
2010-03-11 15:29:11 [INFO]: # Start Time: 2010-03-11 15:29:11 #
2010-03-11 15:29:11 [INFO]: # Operating System: Windows 6.01 #
2010-03-11 15:29:11 [INFO]: # #
2010-03-11 15:29:11 [INFO]: # Service Path: C:\EA\Addins\SparxServices\Current\Debug #
2010-03-11 15:29:11 [INFO]: # Logging Dir: C:\EA\Addins\SparxServices\Current\Debug\Logs #
2010-03-11 15:29:11 [INFO]: #####
2010-03-11 15:29:11 [INFO]: ** Starting up!
2010-03-11 15:29:11 [SYSTEM]: SUCCESS Started GlobalPassword Authentication Module
2010-03-11 15:29:11 [SYSTEM]: SUCCESS Started AuthenticationManager
2010-03-11 15:29:11 [SYSTEM]: SUCCESS Started keystore manager
2010-03-11 15:29:11 [SYSTEM]: SUCCESS Management thread started
2010-03-11 15:29:11 [SYSTEM]: SUCCESS Bound and listening on port 7771
2010-03-11 15:29:11 [SYSTEM]: SUCCESS Socket acceptor thread started
2010-03-11 15:29:11 [INFO]: ** Now listening for connections
2010-03-11 15:29:16 [SYSTEM]: Client connected from 172.16.17.96
2010-03-11 15:29:16 [SYSTEM]: SUCCESS: Client from 172.16.17.96 authenticated (User Name: mfraser, Product: Sparx Systems Enterprise Architect build 854)
2010-03-11 15:29:16 [SYSTEM]: Client disconnected from 172.16.17.96
2010-03-11 15:29:16 [SYSTEM]: Client connected from 172.16.17.96
2010-03-11 15:29:16 [SYSTEM]: SUCCESS: Client from 172.16.17.96 authenticated (User Name: mfraser, Product: Sparx Systems Enterprise Architect build 854)
2010-03-11 15:29:16 [INFO]: CHECKOUT SUCCESS, mfraser, Sparx Systems Enterprise Architect build 854, [REDACTED], EA Ultimate Edition, MFRASER03\m
2010-03-11 15:29:16 [SYSTEM]: SUCCESS Checked out [EA Ultimate Edition] key for MFRASER03\mfraser
2010-03-11 15:29:16 [SYSTEM]: Client disconnected from 172.16.17.96
2010-03-11 15:29:23 [SYSTEM]: Client connected from 172.16.17.96
2010-03-11 15:29:23 [SYSTEM]: SUCCESS: Client from 172.16.17.96 authenticated (User Name: mfraser, Product: Sparx Systems Enterprise Architect build 854)
2010-03-11 15:29:23 [INFO]: CHECKIN SUCCESS, mfraser, Sparx Systems Enterprise Architect build 854, [REDACTED], EA Ultimate Edition
2010-03-11 15:29:23 [SYSTEM]: SUCCESS Client at 172.16.17.96 checked in key [REDACTED]
2010-03-11 15:29:23 [SYSTEM]: Client disconnected from 172.16.17.96

```


8 Troubleshooting

The best source of troubleshooting information can be found in the Sparx Systems Keystore Service [log files](#) [29]. The log file location and level of detail are configured through the [configuration](#) [12] file. It is recommended that, for trouble shooting, the **LOG_LEVEL** property be set to the highest level, **SYSTEM**, so that the greatest amount of information is available to the administrator.

Initialization Failures

Reported Error	Cause
Could not open keystore at [FilePath]. The file does not exist and could not be created.	The service was unable to open the keystore file specified by the KEYSTORE_PATH property in the configuration file. Ensure that this path exists, and that the user account the Sparx Systems Keystore Service runs under has the necessary permissions to read and write to the file.
Could not open keystore, no keystore file specified.	No file path was specified in the property in the configuration file. Type a file path into the KEYSTORE_PATH configuration property that the user account the Sparx Systems Keystore Service runs under can read and write to.
Invalid or missing keystore file - Keystore file cannot be opened by this version of the service or the file has been corrupted.	The keystore file specified by the configuration property KEYSTORE_PATH is either incompatible with the current version of the keystore service, or has somehow been corrupted on the file system. Restore the keystore file specified in the configuration property KEYSTORE_PATH from a recent backup, or contact Sparx Systems Support for assistance.
Key file has been moved.	The keystore file specified by the configuration property KEYSTORE_PATH is locked to the serial number of the hard drive it is created on. If the keystore file is moved from this hard drive, the service is unable to open it. If the keystore file has been moved, restore the file to its initial location. Certain RAID configurations can affect how the hard drive's serial number is presented to the keystore service. Thus, it is recommended that you house the keystore file on a non RAID drive, wherever possible.

Checkout Failures

Reported Error	Cause
There are no more available keys for this product in the key store.	Keys for this product exist; however, they are all checked out to other users. If this error is frequently reported, consider limiting the use of the product across your enterprise or purchasing more keys to meet the demand for the product.
The key store does not contain any keys for this product.	This keystore does not contain keys for the requested product. Keys for the product might have been provided by the keystore in the past, but have since been removed. Uninstall the product and return any shared keys on the client machine.

Checkin Failures

Reported Error	Cause
Key not found in keystore.	<p>The key being checked in has either been deleted since it was checked out, or was checked out from another keystore.</p> <p>Ensure that users return any shared keys to the keystore they were leased from before swapping keystores.</p>

Authentication Failures - Global Password

Reported Error	Cause
GlobalPasswordAM::Authenticate() failed due to an invalid password.	<p>The user failed to authenticate with the keystore, as they provided a password that did not match the server password specified in the configuration property AUTHMETHOD_OPTIONS.</p> <p>Ensure that the password is entered correctly (passwords are case sensitive), otherwise contact your Sparx Systems Keystore Service administrator for the correct password.</p>

Authentication Failures - Active Directory

Reported Error	Cause
Could not get DefaultNamingContext.	<p>The Active Directory authentication module failed to initialize as it could not resolve the Default Naming Context for the current domain.</p> <p>Ensure that the machine the Sparx Systems Keystore Service is installed on is able to contact the Active Directory domain controller and has the necessary permissions to query the domain's Active Directory.</p>
Could not open root DSE.	<p>The Active Directory authentication module failed to initialize as it could not open the domain's root DSA (Directory Server Agent) Specific Entry (DSE) at <i>ldap://rootDSE</i>. The root DSE entry provides information about the contents and capabilities of the Active Directory domain controller.</p> <p>Ensure that the machine the Sparx Systems Keystore Service is installed on is able to contact the Active Directory domain controller and has the necessary permissions to query the domain's Active Directory.</p>
Could not initialize the Active Directory COM interface.	<p>The Active Directory authentication module failed to initialize as it could not open or access the Active Directory COM interface.</p> <p>Ensure that the machine hosting the user account that the Sparx Systems Keystore Service runs under has the necessary permissions to create and communicate with the Active Directory COM interface.</p>
No permitted ActiveDirectory group name provided in the AUTHMETHOD_OPTIONS configuration property.	<p>The Active Directory authentication module failed to initialize as the configuration property AUTHMETHOD_OPTIONS was left blank.</p> <p>Enter a valid Active Directory group in the AUTHMETHOD_OPTIONS property in the service configuration file, or use the AM_GLOBALPASSWORD authentication module if you do not want keystore access to be restricted to a particular Active Directory group.</p>
Group [Group Name] not found.	<p>The Active Directory authentication module failed to initialize as the Active Directory group specified in the configuration property AUTHMETHOD_OPTIONS could not be resolved.</p>

Reported Error	Cause
	<p>Ensure that the group name specified in the configuration property AUTHMETHOD_OPTIONS exists and is spelt correctly.</p>
<p>User [User Name] is not a member of any permitted groups.</p>	<p>The user failed to authenticate with the keystore as they are not a member of the Active Directory group specified in the configuration property AUTHMETHOD_OPTIONS.</p> <p>Add the user to the group specified in the configuration property AUTHMETHOD_OPTIONS.</p>
<p>Account name [User Name] not found.</p>	<p>The user name requesting to authenticate with the keystore could not be found on the domain.</p> <p>Add the user to domain.</p>

Index

- A -

- Activity Logs 29
- Add Keys Dialog 21
- Add Shared Keys 21
- Assign
 - Key To Workstation 28
- Authentication Failures - Active Directory 30
- Authentication Failures - Global Password 30
- Auto Checkin Option 22

- C -

- Checkin Failures 30
- Checkout Failures 30
- Compiled 19 March 2010 2
- Configure
 - Keystore Service Properties 12
- Copyright Notice 3

- D -

- Delete Shared Keys 27

- E -

- End User License Agreement 4

- F -

- Floating License
 - Editions of Enterprise Architect 2
 - MDG Products 2

- I -

- Initialization Failures 30
- Install
 - Sparx Systems Keystore Service 9
- Introduction
 - License Agreement 4
 - Support 7
 - To Sparx Systems Keystore Service 2
- Issue Period 22

- K -

- Keys
 - Assign To Workstation 28
 - Expire After 22
 - For Floating Licenses 28
 - Lease Expiry 22
 - Register Product Key In Enterprise Architect 28
 - Set Auto Checkin 22
 - Set Issue Period 22
 - Shared, Using 28
- Keystore Manager 19
 - Select Feature 9
- Keystore Server Option 20

- L -

- License
 - Agreement 4

- M -

- Migrate Keys To Remote Keystore 24
- Migrate Keystore File Dialog 24

- O -

- Options Dialog 22

- R -

- Register 28
 - Product Key 28
 - Product Key In Enterprise Architect 28
- Release Shared Keys 26

- S -

- Services Console
 - Windows 11
- Shared Key Store Selection Dialog 20
- Shared Keys
 - Assign To Workstation 28
 - Using 28
- Software Product License Agreement 4
- Sparx Systems Key Store Dialog 19
- Sparx Systems Keystore Service
 - Assign Key To Workstation 28

Sparx Systems Keystore Service

- Configure 12
- Copyright Notice 3
- End User License Agreement 4
- Install 9
- Introduction 2
- License Agreement 4
- Online User Guide 2
- Options Dialog 22
- Properties 12
- Restart 11
- Select Feature 9
- Set Auto Checkin 22
- Set Issue Period 22
- Software Product License Agreement 4
- Start 11
- Stop 11
- Support 7
- User Feedback 8
- Using Shared Keys 28

Sparx Systems Keystore Services

- Activity Logs 29
- Add Shared Keys To Keystore 21
- Administration 19
- Authentication Failures - Active Directory 30
- Authentication Failures - Global Password 30
- Checkin Failures 30
- Checkout Failures 30
- Connect To Local Keystore 24
- Connect To Remote Keystore 20
- Delete Shared Keys 27
- Initialization Failures 30
- Migrate Keys Between Keystores 24
- Release Shared Keys 26
- Troubleshooting 30

SSKS

- Introduction 2
- Online User Guide 2

Support

- For Registered Users 7

- T -

Troubleshooting

- Authentication Failures - Active Directory 30
- Authentication Failures - Global Password 30
- Checkin Failures 30
- Checkout Failures 30
- Initialization Failures 30

- U -

- User Feedback 8
- User Forum 7

- W -

- Workstation
 - Assign Key To 28

Sparx Systems Keystore Service User Guide

www.sparxsystems.com