



Installing

TrustBroker Secure Client
for Servers

Version 4.5.0

for use with SAP NetWeaver® AS for ABAP

Reference: **I-CSTBSCS-SAPNWABAP-450**

19 November 2016

Copyright

Copyright © 2001-2016, CyberSafe Limited.
All Rights Reserved.

CyberSafe®, the CyberSafe logo, **TrustBroker®**, and the **TrustBroker®** logo are registered trademarks of CyberSafe Limited. All other product names, logos, or company names are used for identification purposes only, and may be trademarks or service marks of their respective owners.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of CyberSafe Limited. The information contained herein may be changed without prior notice.

If associated software has been purchased with this publication, then the purchaser's rights regarding this publication shall be in accordance with the terms of the associated software license.

Table of Contents

Copyright	2
Table of Contents	3
About This Guide	4
Purpose	4
Conventions.....	4
Contacting CyberSafe	5
Technical Support & Feedback	5
Contact Details.....	5
Requirements	6
Software Prerequisites.....	6
Versions of SAP NetWeaver® AS for ABAP	6
Platforms.....	6
Authentication Servers	7
Other Needs	9
Additional Requirements	9
Installation Steps	10
Step 1 – Preparation	10
Licensing details.....	10
Which package to install.....	10
How to identify the package	11
Where to install	11
Check whether the SAP system needs to be stopped.....	11
Step 2 – If required, uninstall old CSTB package	11
Step 3 – Install the operating system package.....	12
Step 4 – Install the TrustBroker® license key file	13
Step 5 – Configure the <sid>adm user environment.....	13
Step 6 – Decide on a principal naming convention	14
Step 7 – Create a key table entry	15
Step 8 – Test key table entries.....	16
Step 9 – Configure the SAP Instance profile.....	17
Step 10 – Start the SAP system and check work process logs	18
Troubleshooting.....	19
Example 1	19
Example 2	19
Background Information.....	20
CyberSafe	20
Kerberos	20
TrustBroker®	20




About This Guide

Purpose

This guide contains instructions for installing (or upgrading to, if an older version is currently installed) version 4.5.0 of the **TrustBroker® Secure Client for Servers** product on servers that already have **SAP NetWeaver® AS for ABAP** installed.

Conventions

Before you start reading this guide, it is important to understand the typographical conventions used:

Style / Icon	Represents
Bold	Menus, menu options, tabs, radio buttons, check boxes, command buttons, commands, and product names.
<i>Italic</i>	Buttons on the screen and Keys on the keyboard.
Hyperlink	A link or an external reference.
 NOTE	A note, providing additional information about a certain section/topic.
	An important message, not to be ignored.
 SYNTAX	Example command or parameter syntax.
<div>Output text</div>	Textual computer output.
File Name	File names and locations.

Contacting CyberSafe

This section provides information about whom to contact in CyberSafe, in case you have any need for assistance, or any questions, comments or feedback.

Technical Support & Feedback

If you experience any technical problems or have questions regarding the **TrustBroker®** products, or have feedback to give us on this documentation, use one of the methods described on the CyberSafe Website at <https://CyberSafe.com/Support>.

If you have a technical problem, it is particularly important that you provide us with useful information when you make initial contact. For example, if an error occurs, please provide details of the error message, explain what you did to get the error, and provide any logs or traces which you think might be useful for us to understand the problem and help you.

Contact Details

If you need to talk to somebody from CyberSafe using the telephone, or need to send us information via post, you can use the contact details provided below:

Address	Other Contact Details:
CyberSafe Limited Abbey House 450 Bath Road Longford Middlesex UB7 0EB United Kingdom	Telephone: United Kingdom: +44 203 510 6333 United States: +1 929 333 4499 Fax: +44 207 681 2299 Web: https://CyberSafe.com

Requirements

Software Prerequisites

Versions of SAP NetWeaver® AS for ABAP

The versions of **SAP NetWeaver** supported when using version 4.5.0 of the **TrustBroker® Secure Client for Servers** product are listed below:

- **SAP NetWeaver 2004**, SP12 or later (SP20 or later recommended)
- **SAP NetWeaver 7.0** (2004s) (SP12 or later recommended)
- **SAP NetWeaver 7.1, 7.2, 7.3, 7.4, 7.5** or later

Platforms

The following table lists the platforms (e.g. operating systems, operating system versions, and architectures) that are supported for use with version 4.5.0 of the **TrustBroker® Secure Client for Servers** product:

Vendor	Operating System	Version(s)	Architecture(s)	# bits
Sun	Solaris	8,9,10,11	Sparc	64-bit & 32-bit
Sun	Solaris	10,11	x86 x86_64 AMD64 EM64T	64-bit & 32-bit
IBM	AIX	5.1,5.2,5.3, 6.1,7.x	PowerPC (Power 5 or 6) IBM System p	64-bit & 32-bit
IBM	I5/OS	V5r3 or later	PowerPC	64-bit
IBM	zLinux (SuSE Linux Enterprise Server)	9,10,11	s390 IBM System z	31-bit
IBM	zLinux (SuSE Linux Enterprise Server)	9,10,11	s390x IBM System z	64-bit
IBM	zLinux (Red Hat Enterprise Linux)	4,5,6,7	s390 IBM System z	31-bit
IBM	zLinux (Red Hat Enterprise Linux)	4,5,6,7	s390x IBM System z	64-bit
Hewlett-Packard	HP-UX	11i v1 or v2	PA-RISC	64-bit & 32-bit
Hewlett-Packard	HP-UX	11i v2 or v3	Itanium IA-64	64-bit & 32-bit
Microsoft	Windows	2000 SP4 or later	x86	32-bit

Vendor	Operating System	Version(s)	Architecture(s)	# bits
Microsoft	Windows	Server 2003	x86 x86_64 AMD64 EM64T	64-bit & 32-bit
Microsoft	Windows	Server 2008 or Server 2008 R2	x86 x86_64 AMD64 EM64T	64-bit & 32-bit
Microsoft	Windows	Server 2008 or Server 2008 R2	Itanium IA-64	64-bit
Microsoft	Windows	Server 2012 or Server 2012 R2	x86 x86_64 AMD64 EM64T	64-bit & 32-bit
Red Hat	Enterprise Linux	4,5,6,7	x86_64 AMD64 EM64T IBM System x	64-bit & 32-bit
Red Hat	Enterprise Linux	4,5,6,7	PowerPC IBM System i IBM System p	64-bit & 32-bit
Novell	SuSE Linux Enterprise Server	9,10,11,12	x86_64 AMD64 EM64T IBM System x	64-bit & 32-bit
Novell	SuSE Linux Enterprise Server	9,10,11,12	PowerPC IBM System i IBM System p	64-bit & 32-bit

Authentication Servers

Kerberos

When the **TrustBroker® Secure Client** product is used to authenticate a user, it can use an authentication server which implements the Kerberos, version 5 protocol. The servers that are supported are listed below:

Vendor	Operating System	Version(s)	Product	Encryption Types
Microsoft	Windows	2000 Server Editions	Active Directory	RC4, DES
Microsoft	Windows	Server 2003	Active Directory	RC4, DES
Microsoft	Windows	Server 2003 x64 Edition	Active Directory	RC4, DES

Vendor	Operating System	Version(s)	Product	Encryption Types
Microsoft	Windows	Server 2008	Active Directory	AES, RC4, DES
Microsoft	Windows	Server 2008 x64 Edition	Active Directory	AES, RC4, DES
Microsoft	Windows	Server 2012	Active Directory	AES, RC4, DES
Microsoft	Windows	Server 2012 x64 Edition	Active Directory	AES, RC4, DES

The “R2 Editions” of the Microsoft authentication servers listed above are also supported.

Other, non-Microsoft authentication servers are supported, and listed below:

Vendor	Operating System	Product / Version(s)	Encryption Types
Novell	SuSE Linux Enterprise Server 10	Open Enterprise Server 2, SP1 with Domain Services for Windows	RC4, DES
MIT	Unix, Linux	Open Source Kerberos V5	AES, RC4, DES
Heimdal	Unix, Linux	Open Source Kerberos V5	AES, RC4, DES

Kerberos Encryption Types

The **TrustBroker® Secure Client**, Version 4.3.1.SR2 or later, supports the following encryption types:

- 168-bit Triple DES (3DES) encryption, with CBC and MD5 checksum
- 128-bit RSA RC4 encryption, with HMAC and MD5 checksum
- Exportable 56-bit RSA RC4 encryption, with HMAC and MD5 checksum
- 56-bit DES encryption, with CBC and MD5 checksum
- 56-bit DES encryption, with CBC and CRC checksum
- 256-bit AES encryption in CTS mode, with 96-bit HMAC and SHA-1 checksum
- 128-bit AES encryption in CTS mode, with 96-bit HMAC and SHA-1 checksum

Each of the supported authentication servers is able to use different encryption types (shown in the **Encryption Types** column in the tables above). If the version of **TrustBroker®** used, and the authentication server you are using support the same encryption type, this encryption type can be used by the **TrustBroker®** product when authenticating users. The strongest encryption type supported by the authentication server will be used.

Two-Factor

When using two-factor authentication methods the following authentication servers can be used:

Vendor	Product / Version(s)
RSA	Authentication Manager Version 6.1.2 or later, 7.1 SP2, 7.1 SP3, 8.x or later Note: TrustBroker Secure Client uses RSA SDK 8.1 SP3
Any	RADIUS server

Other Needs

If you have a need for us to support other authentication servers, operating systems, architectures, or operating system versions, please [Contact CyberSafe Support](#) to discuss, and check availability.

Additional Requirements

- **Free Hard Disk Space** – When installing the **TrustBroker® Secure Client for Servers** product, approximately 5MB to 17MB of free disk space is required, depending on the operating system used. Additional free space is required for key table, logs, and configuration data.

Installation Steps

To install and prepare the software for use, the steps described below need to be followed. Within each step detailed instructions are provided. If you are not happy with the results from a specific step, we recommend that you do not proceed to the next step.

If you are upgrading from a previous version of **TrustBroker® Secure Client**, certain installation steps need to be re-done after the operating system package has been upgraded, in which case, this is mentioned in the instructions.

You should [Contact CyberSafe Support](#) if you are having difficulty, or do not understand any step described in this **Installation Guide**.



*This guide includes example output, and example commands that are applicable to **SAP NetWeaver** systems installed on the CyberSafe company network. Instead of using the exact names given, adjust them to suit your environment. For example, you might need to use a different hostname, domain, REALM and SAP SID.*

*The examples mostly refer to two SAP systems on a **Linux** host called **sapn1a.kerby.com**. These systems have a SAP System ID ("SID") of **N1A** (an **AS ABAP** system) and **N1J** (an **AS Java** system). Another SAP system was used, which was on a **Windows Server** with hostname **sapw02.dev.local** and with a SAP SID of **W02**. The **Active Directory®** domain used in most of the examples is called **kerby.com** (Kerberos realm= **KERBY.COM**) with a sub domain called **emea.kerby.com** (Kerberos realm= **EMEA.KERBY.COM**).*

Step 1 – Preparation

Licensing details

The **TrustBroker® Secure Client** product needs to be licensed for the appropriate number of users, or the appropriate number of operating system instances before the operating system package is installed on the host(s) where **SAP NetWeaver AS for ABAP** instances are running.

Which package to install

The **TrustBroker® Secure Client for Servers** product is often installed using the operating system package named **CSTBscs**, but can also be installed using the **CSTBoc** or **CSTBsapwa** packages.

The **TrustBroker® Secure Client** files and libraries are included in multiple operating system packages in case you have multiple **TrustBroker®** products licensed and need to use them on the same host.

A summary of the operating system packages and the **TrustBroker®** products included in them, is provided below:

Operating System Package Name	Products Included in Package
CSTBoc	TrustBroker® One Credential TrustBroker® Adapter TrustBroker® Secure Client for Servers
CSTBsapwa	TrustBroker® Adapter TrustBroker® Secure Client for Servers
CSTBscs	TrustBroker® Secure Client for Servers

For example, if there is an **SAP NetWeaver AS for Java** system on the same host as the **AS for ABAP** system, and the **TrustBroker® Adapter** product is licensed on this **AS for Java** system, you can install the **CSTBsapwa** package instead of **CSTBscs**.

You might prefer to install the same operating system package on each host, just for consistency across your SAP system landscape. If you do this, you must make sure that any products installed are licensed if you use them. For example, if you install the **CSTBoc** package, you might use the **TrustBroker® Secure Client** product, but you might not have purchased a license to use the **TrustBroker® One Credential** product. This is allowed, but if you use the **TrustBroker® One Credential** product you must buy a license for it.

How to identify the package

The operating system package required to install the **TrustBroker® Secure Client** product is provided by CyberSafe, along with a **README** file and other product related files, in an archive file.

For example, the **CSTBscs** package for **Red Hat Enterprise Linux 6** will be in an archive file called **CSTBscs-4.5.0-38075.rhel6.Linux.x86_64.tar.Z** and the **Windows Server** package in an archive file called **CSTBscs-4.5.0-38075.Windows.x86_64.zip**

Where to install

The operating system specific installation package needs to be installed on the hosts where **SAP NetWeaver AS for ABAP** instances are running. For a distributed system the package needs to be installed on all hosts running **AS for ABAP** dialog instances or the central instance.

When the package is installed onto a **Unix** or **Linux** host, files are put into the `/opt/krb5` directory, then a symbolic link `/krb5` is created which links to the installation directory. When installing on **Windows Servers** the files are normally installed into `C:\Program Files\CyberSafe` (and into `C:\Program Files (x86)\CyberSafe` if installing onto an x64 edition of **Windows Server**).

Check whether the SAP system needs to be stopped

You need to stop the SAP system if all of the following apply:

1. The host has an older version of the **CSTBscs**, **CSTBsapwa** or **CSTBoc** package installed.
2. The SAP system profile for any SAP systems on the host, contains the profile parameter **snc/enable=1**

When the SAP system has stopped, or if you don't need to stop the SAP system, you can continue from [Step 2](#).

Step 2 – If required, uninstall old CSTB package

If you are upgrading from a previous version of the **TrustBroker® Secure Client** product on **Unix** or **Linux**, first you need to uninstall the old version of the operating system package. Then, you can install the 4.5.0 version of the operating system package using the instructions given in [Step 3](#). On **Windows Servers** the old version of the operating system package is automatically uninstalled when the new version is installed.

If you need to uninstall any **CSTB** package, you need to use the **cstb_remove** script if the product is on **Unix** or **Linux**, or using **Programs and Features** or **Add/Remove Programs** if the product is on a **Windows Server**.

Step 3 – Install the operating system package

You must install version 4.5.0 of the operating system package, unless it is already installed.

On each host, you need to install the operating system package using the instructions provided below, using the **CSTBscs** package as an example:

On a Unix or Linux Server:

Logon to the server as **root**, and use **gunzip** and **tar** to extract files from the archive and then use the **cstb_install** script to install the software, as shown below:

```
[root@sapnla tmp]# ls
CSTBscs-4.5.0-38075.rhel6.Linux.x86_64.tar.Z
[root@sapnla tmp]# gunzip CSTBscs-4.5.0-38075.rhel6.Linux.x86_64.tar.Z
[root@sapnla tmp]# ls
CSTBscs-4.5.0-38075.rhel6.Linux.x86_64.tar
[root@sapnla tmp]# tar -xvf CSTBscs-4.5.0-38075.rhel6.Linux.x86_64.tar
CSTBscs-4.5.0-38075.rhel6.Linux.x86_64/
CSTBscs-4.5.0-38075.rhel6.Linux.x86_64/README.CSTBscs-4.5.0-38075.rhel6.Linux.x86_64
CSTBscs-4.5.0-38075.rhel6.Linux.x86_64/Package/
CSTBscs-4.5.0-38075.rhel6.Linux.x86_64/Package/cstb_install
CSTBscs-4.5.0-38075.rhel6.Linux.x86_64/Package/cstb_remove
CSTBscs-4.5.0-38075.rhel6.Linux.x86_64/Package/CSTBscs-4.5.0-38075.rhel6.Linux.x86_64.rpm
[root@sapnla tmp]# cd CSTBscs-4.5.0-38075.rhel6.Linux.x86_64
[root@sapnla CSTBscs-4.5.0-38075.rhel6.Linux.x86_64]# ls
Package  README.CSTBscs-4.5.0-38075.rhel6.Linux.x86_64
[root@sapnla CSTBscs-4.5.0-38075.rhel6.Linux.x86_64]# cd Package/
[root@sapnla Package]# ls
cstb_install  cstb_remove  CSTBscs-4.5.0-38075.rhel6.Linux.x86_64.rpm
[root@sapnla Package]# ./cstb_install
Installing package : CSTBscs
Preparing...          ##### [ 100% ]
 1:CSTBscs            ##### [ 100% ]
[root@sapnla Package]#
```

On some versions of **Unix** or **Linux**, the output shown may differ from the above.

On a Windows Server:

Logon to the server as an Administrator user (or a normal user if you are using **Windows Server 2008** or **2012** with UAC enabled), double-click the **.msi** package which is in the **Package** folder, and then follow the instructions provided on the screen.

You can also install the package silently or from a command line if you use **msiexec**.

Step 4 – Install the TrustBroker® license key file

A license key file is provided by CyberSafe, which you need to install in order to use the **TrustBroker® Secure Client for Servers** product. If you don't have this file, please contact CyberSafe, and ask for your license key file (called `cstb.lic`).

To install the license key, you need to copy the file into the `/krb5/license` directory if it is a **Unix** or **Linux** Server, into the `C:\ProgramData\CyberSafe\license` folder if it is running **Windows Server 2008, 2008 R2, 2012 or 2012 R2**, or the `C:\Documents and Settings\All Users\Application Data\CyberSafe\license` folder if it is running **Windows Server 2003**.

On **Windows**, if you put the license key file in the same directory as the `.msi` package, when the package is installed, the license key file will be copied into the correct license folder for you.



*On **Windows Server 2008, 2008 R2, 2012 or 2012 R2**, the `C:\ProgramData` folder might not be visible. This folder is hidden by default when the Windows operating system is installed, so you will have to unhide it or enter the full path of the folder into the address bar of **File Explorer** in order to copy the license key file into the `C:\ProgramData\CyberSafe\license` folder.*

Step 5 – Configure the <sid>adm user environment

The environment under which the **SAP NetWeaver AS for ABAP** instance runs needs to be configured so that the **TrustBroker Secure Client for Servers** product will use a memory based credentials cache. The memory used for this cache is specific to each **SAP NetWeaver** work process, so each work process will have its own cache, thereby improving performance.

The instructions for making this configuration change are given below:

On a Windows Server:

In the archive file which you used in [Step 3](#) in a folder named `Configuration` you will find **Windows Registry** files (`.reg` files). One of them is called `SAP NetWeaver AS for ABAP.reg`.

You should run the `.reg` file to merge changes with your existing **Windows Registry**. If you have **Registry** entries configured from a previous version (e.g. before version 4.5.0) you should remove these first using the `reg_reset.bat` script (run from an Administrator Command Window).

On a Unix or Linux Server:

Create a new script in your **<sid>adm** home directory, called `trustbroker_env.sh`. Then add the following code to the script:

```
# Setup TrustBroker environment, so that a memory
# credentials cache is used instead of a file cache.
CSFC5CCNAME=MEMORY:sap; export CSFC5CCNAME
```

Create a new script in your **<sid>adm** home directory, called `trustbroker_env.csh`. Then add the following code to the script:

```
# Setup TrustBroker environment, so that a memory
# credentials cache is used instead of a file cache.
setenv CSFC5CCNAME MEMORY:sap
```

Make the `trustbroker_env.sh` and `trustbroker_env.csh` scripts executable.

```
sapnla:nlaadm 10> chmod u+x trustbroker_env.*
```

```
sapn1a:nlaadm 11>
```

Edit the `.profile` file found in your **<sid>adm** home directory, so that it runs the `trustbroker_env.sh` script you just created. For example, add the following code:

```
# TrustBroker
if [ -f $HOME/trustbroker_env.sh ]; then
    . $HOME/trustbroker_env.sh
fi
```

Edit the `.cshrc` file found in your **<sid>adm** home directory, so that it runs the `trustbroker_env.csh` script you just created. For example, add the following code:

```
# TrustBroker
if ( -e $HOME/trustbroker_env.csh ) then
    source $HOME/trustbroker_env.csh
endif
```

Log off **<sid>adm**, then log on again and check the environment using:

```
sapn1a:nlaadm 12> echo $CSFC5CCNAME
MEMORY:sap
sapn1a:nlaadm 13>
```

Step 6 – Decide on a principal naming convention

Each instance of an **AS for ABAP SAP System** needs a unique identity in **Active Directory**. This identity is used for SAP SNC authentication and security, and is actually a Kerberos service principal name. The name needs to be decided, and then you can use **ktutil** to create a key table entry for this principal name (see [Step 7](#)).

For best practice you should use a naming convention that includes the following elements, to ensure that the identity is unique:

- The SAP System ID (SID)
- The hostname, or an alias hostname

For example, a naming convention such as **sap<sid>/<hostname>** would mean that a SAP system with SID = **N1A** on a server with hostname **sapn1a.kerby.com** would use a principal name of **sapn1a/sapn1a.kerby.com**. The part of the name after the / doesn't need to match the actual hostname of the server, and can be an alias or something else which is unique and meaningful to you.

When you create this principal identity using **ktutil** you will need to create it in a specific Active Directory domain (a.k.a. Kerberos realm). The Kerberos realm name is ALWAYS in upper case and included after an @. So if the Active Directory domain is **emea.kerby.com**, the full principal name would be **sapn1a/sapn1a.kerby.com@EMEA.KERBY.COM**.

Step 7 – Create a key table entry

You need to use **ktutil** to create a key table entry. If you haven't already, we recommend you refer to the following document, where you will learn about how key tables are used and about the different methods available when creating key table entries:

Reference	Document Title
H-CSTB-AD-450	How TrustBroker products work with Active Directory

On a Windows Server:

Open a Command Window, and then run the **ktutil** command according to the detailed instructions found in the **H-CSTB-AD-450** document. For example, like this:

```
C:\>ktutil -x sapnla/sapnla.kerby.com@EMEA.KERBY.COM
```

On a Unix or Linux Server:

Run the **ktutil** command according to the detailed instructions found in the **H-CSTB-AD-450** document. For example, like this:

```
[root@sapnla ~]# ktutil -x sapnla/sapnla.kerby.com@EMEA.KERBY.COM
```

If you were logged on as **root** when you created the key table entry, you will need to check the permissions on the key table (file `/krb5/v5srvtab`) to be sure that the **<sid>adm** user has read access to this file.

The easiest way to check the permissions is to run **ktutil** whilst logged onto the **<sid>adm** user. If you get a list of key table entries, then the permissions are correct. See example **ktutil** output below:

```
sapnla:nlaadm 52> /krb5/sbin/64/ktutil
Key Table: FILE:/krb5/v5srvtab

KVNO  EType  Timestamp                Principal
----  -
  2    17    Fri 06 May 2016 17:10:25 BST sapnla/sapnla.kerby.com@EMEA.KERBY.COM
  2    18    Fri 06 May 2016 17:10:25 BST sapnla/sapnla.kerby.com@EMEA.KERBY.COM
  2    23    Fri 06 May 2016 17:10:25 BST sapnla/sapnla.kerby.com@EMEA.KERBY.COM
sapnla:nlaadm 53>
```

If there is a problem with permissions, you might get an error like this:

```
sapnla:nlaadm 54> /krb5/sbin/64/ktutil
Key Table: FILE:/krb5/v5srvtab
Error occurred in ktutil while starting key table scan ( 0x00000880 2176 )
You don't have permission to read from the key table
sapnla:nlaadm 55>
```

If you do, then you need to change the permissions on this file so that it is readable by the **<sid>adm** user. This can be done by logging on as **root** and running the command **chmod 644 /krb5/v5srvtab**

Step 8 – Test key table entries

The **ktutil** tool can be used to confirm that the keys in the key table match the keys generated from the computer account password in the Active Directory domain, and check that the encryption types supported by the domain have corresponding entries in the key table, and that key version numbers are aligned.

The command is shown below:

On a Windows Server:

Open a Command Window, and then run the **ktutil** command, like this example:

```
C:\Program Files\CyberSafe\bin\> ktutil --test 15
```

On a Unix or Linux Server:

Run the **ktutil** command, like this example:

```
sapnla:nlaadm 56> /krb5/sbin/64/ktutil --test 15
```

If the testing completes without any errors, then you will see output like this:

```
Testing key table entries...

Encryption Type Test Summary:
Principal: sapnla/sapnla.kerby.com@EMEA.KERBY.COM
Encryption Types:          18      17      23
KDC Host: dc1-1-3.emea.kerby.com
  Initial Ticket:           Yes      Yes      Yes
  Service Ticket:          Yes      Yes      Yes

Key Version Number Test Summary:
Principal: sapnla/sapnla.kerby.com@EMEA.KERBY.COM
KDC Host: dc1-1-3.emea.kerby.com
KDC      Key Table Match
16      16      Yes

Principal Exists Test Summary:
Principal: sapnla/sapnla.kerby.com@EMEA.KERBY.COM
KDC Host: dc1-1-3.emea.kerby.com
Exists
Yes

Testing key table entries completed successfully.
```

If you get any errors and you cannot resolve them yourself, please [Contact CyberSafe Support](#) for assistance. It is very important that the key table entries are correct before you make any changes to the SAP system as explained in [Step 9](#) onwards.

Step 9 – Configure the SAP Instance profile

You need to edit the instance profile for your SAP system (using transaction RZ10) and add the following entries:

On **Unix, Linux** or **Windows Servers**:

```
snc/enable = 1
snc/identity/as = p/krb5:<principal name used in Step 5>
snc/data_protection/max = 3
snc/data_protection/min = 2
snc/data_protection/use = 3
snc/r3int_rfc_secure = 0
snc/r3int_rfc_qop = 8
snc/accept_insecure_cplic = 1
snc/accept_insecure_gui = 1
snc/accept_insecure_r3int_rfc = 1
snc/accept_insecure_rfc = 1
snc/permit_insecure_start = 1
snc/force_login_screen = 0
snc/extid_login_diag = 1
snc/extid_login_rfc = 1
```

On 64-bit **Unix** (except **HP-UX**) or **Linux Servers**:

```
snc/gssapi_lib = /krb5/appsec-rt/lib/64/libsncl.so
```

On 32-bit **Unix** (except **HP-UX**) or **Linux Servers**:

```
snc/gssapi_lib = /krb5/appsec-rt/lib/libsncl.so
```

On 64-bit **HP-UX Servers**:

```
snc/gssapi_lib = /krb5/appsec-rt/lib/64/libsncl.sl
```

On 32-bit **HP-UX Servers**:

```
snc/gssapi_lib = /krb5/appsec-rt/lib/libsncl.sl
```

On 64-bit **Windows Servers**:

```
snc/gssapi_lib = snclgss64.dll
```

On 32-bit **Windows Servers**:

```
snc/gssapi_lib = snclgss32.dll
```

The parameters described above will allow your users to login using SAP user id and password, or using SNC. You can therefore SNC enable your SAP systems without requiring all users to use SNC authentication, and you can gradually introduce SNC authentication to the other users.

Step 10 – Start the SAP system and check work process logs

You can now start (or restart) your SAP system.

To check that SNC has been configured and enabled correctly, you need to look at the work process log files on your system. These are normally found in the `/usr/sap/<SID>/<INSTANCE>/work` folder and named `dev_w0`, `dev_w1` etc.

An example of the entries in a work process log are shown below:

On a Windows Server:

```
M Fri Mar 25 14:04:37 2016
M rdisp/reinitialize_code_page :0 -> 0
N SncInit(): found snc/data_protection/max=3, using 3 (Privacy Level)
N SncInit(): found snc/data_protection/min=2, using 2 (Integrity Level)
N SncInit(): found snc/data_protection/use=3, using 3 (Privacy Level)
N SncInit(): found snc/gssapi_lib=sncgss64.dll
N File "sncgss64.dll" dynamically loaded as SNC-Adapter.
N The Adapter identifies as:
N External SNC-Adapter to CyberSafe TrustBroker Secure Client Kerberos 5/GSS-API v2 Library Version
4.5.0-38075
N SncInit(): found snc/identity/as= p/krb5:sapw02/sapw02.dev.local@DEV.LOCAL
N SncInit(): Accepting Credentials available, lifetime=Indefinite
N SncInit(): Initiating Credentials available, lifetime=07h 59m 59s
M SNC (Secure Network Communication) enabled
```

On a Unix or Linux Server:

```
N SncInit(): Initializing Secure Network Communication (SNC)
N AMD/Intel x86_64 with Linux (st,ascii,SAP_UC/size_t/void* = 16/64/64)
N SncInit(): found snc/data_protection/max=3, using 3 (Privacy Level)
N SncInit(): found snc/data_protection/min=2, using 2 (Integrity Level)
N SncInit(): found snc/data_protection/use=3, using 3 (Privacy Level)
N SncInit(): found snc/gssapi_lib=/krb5/appsec-rt/lib/64/libsncl.so
N File "/krb5/appsec-rt/lib/64/libsncl.so" dynamically loaded as external SNC-Adapter.
N The SNC-Adapter identifies as:
N External SNC-Adapter to CyberSafe TrustBroker Secure Client Kerberos 5/GSS-API v2 Library Version
4.5.0-38075
N SncInit(): found snc/identity/as= p/krb5:sapnla/sapnla.kerby.com@EMEA.KERBY.COM
N
N Fri Mar 25 17:48:24 2016
N SncInit(): Accepting Credentials available, lifetime=Indefinite
N SncInit(): Initiating Credentials available, lifetime=10h 00m 00s
M ***LOG R1Q=> p/krb5:sapnla/sapnla.kerby.com@EMEA.KERBY.COM [thxxsnc.c 264]
M SNC (Secure Network Communication) enabled
```

The message “**SNC (Secure Network Communication) enabled**” means that SNC has been configured correctly and is enabled. If you do not see this message then you need to look for an error message and determine what is wrong, or check your configuration to be sure you have followed the steps in this guide.

You can use the section below as a reference to fix issues caused by common mistakes. If you cannot fix the issue yourself, you should [Contact CyberSafe Support](#) for assistance.

Troubleshooting

The examples below show various problems that you might encounter when looking in the **SAP NetWeaver AS for ABAP** work process logs after completing the installation steps described in this guide.

Example 1

When checking the work process log, if you see:

```
N *** ERROR => SncPacquireCred()==SNCERR_GSSAPI [sncxxall.c 1510]
N      GSS-API(maj): GSS: No credentials were supplied
N      GSS-API(min): Key table entry with given principal name not found
N      Could't acquire ACCEPTING credentials for
```

This means that you have configured a value for the instance profile parameter **snc/identity/as** which does not match an entry in the key table which you created in [Step 7](#). You need to make the names match and restart the SAP system.

Example 2

If you see messages like this in the work process log:

```
N *** ERROR => SncPacquireCred()==SNCERR_GSSAPI [sncxxall.c 1439]
N      GSS-API(maj): GSS: No credentials were supplied
N      GSS-API(min): Permission denied
N      Could't acquire ACCEPTING credentials for
```

This means you have not checked the key table permissions, as explained in [Step 7](#). You need to fix the permissions on the file and then restart the SAP system.

Background Information

CyberSafe

CyberSafe was founded in 1991, and quickly established a solid reputation for its expertise in the development and use of the Kerberos protocol. CyberSafe was the first company to offer a commercial Kerberos-based security product in 1993, and the first to provide critical security interoperability between **Microsoft Windows** and non-Microsoft operating systems and applications. Till date, this experience in commercially supported Kerberos-based authentication and security is unsurpassed.

In 2001 the company re-branded itself as “The Kerberos Solution Provider”, and focused on making the **TrustBroker®** products meet the needs of companies who run their business primarily using applications from SAP AG (<http://www.sap.com>) and SAP software partners. The products allow the company to improve the security of their applications, implement security policy and audit guidelines, and adhere to regulatory compliance, whilst improving user productivity and reducing costs. CyberSafe also provides a high quality support service that customers can rely on.

Kerberos

Kerberos is a platform independent, strategic and standards-based protocol, and does not require passwords to be stored, or transmitted across the network. The protocol also provides data integrity to ensure messages are not tampered with on the network, and privacy (encryption) to ensure messages are not visible to eavesdroppers on the network. Kerberos can support many user authentication methods, such as user name & password, a hardware token device, or an X.509 v3 certificate.

Kerberos is included in **Microsoft Windows** and used to authenticate users when they logon to a **Microsoft Active Directory** domain. The credentials obtained during this initial logon are used to securely authenticate the logged on user to various Microsoft applications installed on **Windows Servers** without them needing to re-authenticate, thus providing Single Sign-On to the user. When using a Web browser, Microsoft refers to this as **Integrated Windows Authentication**.

TrustBroker®

The CyberSafe products are known as **TrustBroker®** and include an implementation of the Kerberos protocol, developed by CyberSafe, and designed to be robust and scale to the needs of customers using critical business applications.

The **TrustBroker®** products are available for **Microsoft Windows** and popular versions of the **Unix** and **Linux** operating systems. They are primarily used to Kerberos enable the business applications from SAP and from SAP software partners, and by doing so they improve application security and compliance, reduce costs, and improve user productivity. They are often used for Secure Single Sign-On, but sometimes Single Sign-On is not required or possible, so they can be configured to provide Multiple Sign-On instead. It is also possible for Single Sign-On to be used by some users, and have Multiple Sign-On used by a different group of users in the same company.

The **TrustBroker®** products are all designed to be easy to install and configure, scalable, and commercially supported.