BIS Installation and Update

Version: 6.5.2 SP55

February 2, 2018

SEEBURGER
BUSINESS INTEGRATION

Table of Contents

Note: False configuration and/or improper use of communication components may result in significant charges from your telecommunication provider. Also consider configuration changes initiated by your telecommunication provider. SEEBURGER is not liable for related additional costs.

Note: Please refer to the Knowledgebase article 13379 for an important notice concerning possible incurred charges from your telecommunication provider.

Note: Export-/Import Regulations

The SEEBURGER AG is a German corporate with subsidiaries in countries worldwide. In daily trading with our customers and partners, each SEEBURGER corporate deals in compliance with the local export and import regulations of the specific country.

SEEBURGER standard software is partly based on US technology (tomcat, Red Hat JBoss, Oracle Java etc.). To be compliant with the US Export Administration Regulation and the Treasury Department regulations SEEBURGER software and/or technical data may NOT be exported /reexported, either directly or indirectly, to any destination subject to U.S. embargos or trade sanctions unless formally authorized by the U.S. Government. Note that said embargoed destinations are subject to change and the scope of what technology is included in the embargo is specific to each embargoed country. For the most current information on U.S. embargoed and sanctioned countries, please contact the U.S. Export Administration Regulations and Treasury Department regulations.

Note: We expressly declare that the document **"SEEBURGER Legal Information"** (delivered also with your BIS installation media) is part of this documentation.

1 Introduction

SEEBURGER Business Integration Server (BIS) is SEEBURGER’s platform for business integration. With BIS, SEEBURGER developed a tool that provides a great number of services, and supports a wide range of deployment scenarios.

The main services in the BIS architecture are:

- Process Engine (BPEL engine with extensions)
- Conversion service (Business Integration Converter)
- Worklist Handler (load distribution, queuing, resource management)
- Gateways and adapters (communication)
- Component services (encryption, compression, data handling, reporting, etc.)

In this book you learn how to install new systems and instances or upgrade (extend) existing instances as well as update existing instances with service packs or patches.

2 System Requirements

The related software, database, operating system, system software and hardware requirements are described in the *Release Notes* available for each BIS 6 release. Please make sure to check the *Release Notes* for up-to-date information on requirements .

To allow you to plan your installation better, please also refer to the following additional documents:

- BIS Developer Studio (Installation Manual)
- BIS 6 Hardware Sizing
- BIS 6 Failover Cluster
- License Manager
- SEEBURGER Knowledgebase https://servicedesk.seeburger.de/ (Category: BIS6)

File system Requirements

Availability and reliability of the BIS system depends on the underlying file system. SEEBURGER does not specifically certify file systems. The Installation Planning and Concepts Guide contains some general advice on data storage.

The following minimum properties must be present for a filesystem in order to be used as installation or data directory for BIS:

- POSIX filesystem semantics with Windows or Linux/Unix path separators. NTFS limitations are acceptable.
- durability guarantee of fsync()
- Atomic renames (within the same file system but across directories)
- Close-to-Open session semantics which guarantee as soon as the file is closed (and renamed) it must be visible with no latency to all clients
- Does not propagate intermediate network or storage problems to the Java file system API (NFS is safe in this regard, SMB >3.x with ContinouslyAvailable feature)
- Large File Support (for Java applications) (minimum 4GB but at least as big as largest file payload required)
- Support for Java mmap/NIO functions including java.nio.channels.FileLock on regions
- Stale lock detection (FileLock is released by server as soon as client machine is restarted)
- When used as a shared file store the above properties must be usable between all machines which use this store

Note: Typically, not all replicated or networked file systems cover all aspects. (for example *DFS Replication* (DFSR) cannot be used as it does not provide close-to-open semantic or locking across replicas).

Please consult the DB vendor documentation in regards to selecting a file system for the system database server.

3 Installation Overview

The actual installation course depends on the following criteria:

- Type of installation: Initial installation, upgrade or update
- Operating system
- Which database management system will be used, and the extent of its preparation
- Modules to be installed
- System landscape (number and location of components)

You typically have to coordinate preparation work as well as the order in which instances are installed. The installation itself is guided by the setup tool

Note: The installation can be aborted in any phase of the procedure.
If the installation dialogs include a *Cancel* button you can abort the procedure.

Warning: If you cancel or abort the installation you should not re-try the installation into the same directory (as the installer assumes you want to update, which only works if the installation was successful). You should remove the partial installation and database schema first.

See also

Installing BIS for a scenario which has high demand for performance or business continuity and availability requires proper planning. This affects the selection and sizing of infrastructure components. We recommend you consult the *Concepts and Installation Planning* guide in this early planning phase. Besides defining concepts and terms, the guide is mainly concerned with planning the landscape for an installation which can scale out and support operating with minimal downtime.

In order to prepare the requirements for the actual installation, this *Installation and Update Manual and* the *BIS6 Release Notes* need to be consulted. Details about preparing the system database can be found in the *System Database manual* for Microsoft SQL Server or Oracle Database. Details about network connections within a distributed system can be found in the *Network Configuration manual*.

Requirements for Adapters and communication are described in the *Master Adapter Guide* and the *Networking Configuration* Guide. We also provide you with the *Data Transmission Guide*, which explains some concepts and background information about supported communication protocols.

Document Conventions

This manual will use screen shots from a *Microsoft Windows* installation. Using the graphical installer has the same steps (unless noted otherwise). Each step (screen) in the installation process is described, and details under which criteria the step is required.

Product names, trademarks or defined terms are typically in *italic*, constants, file-names or commands are typically in `constant-width` fonts.

The following placeholders (inside < >) are used in the installation manual when sample commands or locations are mentioned:

`<MEDIA>` The directory or Windows drive where the extracted files of the installation media are located.

`<BIS_HOME>` The absolute path to the directory where the BIS instance is being installed. Also called the instance home or target directory.

`seeasown`, `seeadm` Sample user or group names. You can use your own naming conventions, it is recommended to have a common prefix for the application/vendor and maybe encode properties like landscape (prod/test) or differentiate between human and service accounts.

When giving a list of alternatives (for example scripts might have the .bat suffix on Windows and .sh on Linux/Unix) the .{bat,sh} syntax is used. Optional input is typically enclosed in [ ].

4 Preparing the Installation

This is the procedure for preparing and installing a BIS system with multiple instances:

1. Consult the *Concepts and Installation Planning* Guide as well as the *Hardware Scaling* guide to do your landscape planning.
2. Check the *SEEBURGER Knowledge Base* (http://servicedesk.seeburger.de) for the latest update to the *BIS6 Release Notes*.
3. Check whether the requirements are fulfilled (refer to the *System Requirements (page 2)* paragraph and the *Release Notes*).
4. Read the *Master Adapter Configuration* Guide for additional information on the installation of SEEBURGER communication adapters.
5. Check the *Software and System Prerequisites (page 6)* list for time intensive preparation steps
6. You must shut down an already running BIS instance before you can update or upgrade it.
7. The target machine for the installation requires access to all the files on the installation media. It is recommended to copy the content to a local directory for faster and more reliable installation.
8. You need to prepare the operating environment (system settings, runtime user, installation directory) before installing each instance (local adminsitration or root priveledges might be required).
9. In case of an upgrade it is recommended to have a backup of the database and the BIS 6 instance directory.
10. Begin with installing the system database (which is part of installing an instance of the role *Admin Server* and *B2B Portal*).
11. Optional: add further instances according to planned landscape.
12. Optional: set up an external WebDAV server or shared filesystem (NFS, Cluster Filesystem) for large attachment storage (by default the WebDAV server inside the Admin Server role is used, but this will require processing down-time while patching the Admin Server)

Note: SEEBURGER does not support running BIS with an on-access (background) anti-virus or malware scanner. Degraded performance and in-stable system operations can be caused by those products. At least exclude the installation directory from the list of monitored folders. This is also true for the database server system. It may be required to re-start the system after modification of the virus scan software configuration.

4.1 Software and System Prerequisites

The following sections will describe prerequisites and steps you need to execute before you can start with the installation. Please review the steps well ahead of the actual installation because some steps might involve waiting for external parties (like system, storage or database administrators) or consume some download time.

4.1.1 Providing the Installation Media

SEEBURGER software is shipped as a physical installation media (DVD) or via electronic download. In both cases you need access to the files and directories hierarchy inside. The media is required for for installing instances of role Admin Server or Portal.

Sample command to retrieve a ISO image file from a SEEBURGER download location with the *curl* tool on Unix/Linux. (The URL is only a sample to visualize the command, you will receive a valid URL from SEEBURGER.) Instead of *curl* you can also use a Web browser based download.

```
$ curl -O  'https://mft.seeburger.de/portal-seefx/~public/abcdef?download'
```

To make the content of this image file available you need to mount the ISO file (or physical media) or uncompress the ISO file to a local directory.

Using a local copy of the installation media is the preferred method. You can use an operating system specific tool like *7-zip File Manager* (on Windows) or *bsdtar* (on Linux/Unix) to extract the ISO image files. Using a remote file share or an actual optical media will slow the installation down and increases the risk of failure.

The expanded installation media will use up to 5GB of temporary storage. The manuals refer to this extracted directory with the <MEDIA> place holder.

Alternative method to unpacking the media file is to mount it directly. This will slow down the installation and requires administrative privileges, but it has the advantage of not requiring additional space to unpack the software distribution.

⚠ **Warning**: Before you mount the file system on an ISO, it is strongly recommended to verify the integrity of the image. For this purpose, check the file size and checksum.

- For recent Windows-based systems you can directly mount an ISO image as a virtual drive by double clicking it in explorer. For older versions or more options you can use a virtual drive utility like the free *Microsoft Virtual CD-ROM Control Panel* (*VCdControlTool.exe* - search at *download.microsoft.com*).
- For *Linux* -based systems, you can apply the the loop back file mount (included in usual Linux distributions) with the following command (as root):

```
# mkdir /media/dvd                                      # any empty mount point is fine
# mount -t iso9660 -o ro,loop /home/seeasown/BIS_6.iso /media/dvd

... Now you can install from /media/dvd as <MEDIA> source

# umount /media/dvd
```

- For Solaris-based systems, the following command sequence can be used. (Run as root, replace the absolute path to the ISO image file and note the allocated *lofi*device number. We use /mnt as the mount point, you can use any other empty existing directory):

```
# lofiadm -a /export/home/seeasown/BIS_6.iso
/dev/lofi/1
# mount -F hsfs -o ro /dev/lofi/1 /mnt

... Now you can install from /mnt as <MEDIA> source

# umount /mnt
# lofiadm -d /dev/lofi/1
```

4.1.2 Article Codes / Order confirmation

It is important to note, that you also need to have the SEEBURGER order confirmation available if you plan to do the installation, it will contain key codes for selecting the actual licensed articles. While installing the system you will need to request a license file. If you do not receive this in time (since it requires manual confirmation) you can also request a trial license (which is sent automatically) and later on replace it with a permanent one.

4.1.3 JCE Unlimited Strength Policy

For IBM JDK on AIX and the HP/UX JDK you use the downloadable JCE policy files to enable unrestricted crypto. They need to be installed under `runtime/jvm64/jre/lib/security/`.

- Download for IBM JDK: http://www.ibm.com/developerworks/java/jdk/security/index.html

⚠ **Warning**: For Oracle JVM (Windows, Linux) the JDK is shipped on the installation media and the configuration is done via `vm.properties` file. See the JCE Policy chapter (page 85) in the appendix for details. You must review your local law and regulations if you are allowed to use the unlimited cryptography.

4.1.4 Java Runtime Installation

For Windows and Linux the installer includes the supported Oracle Java SE runtime on the installation media. For all other operating systems you need to provide a recent Java virtual machine. Check the *release notes* and knowledge base (we also provide updates for the JRE for stability and security reasons) for the actual supported and recommended versions. The JDK or Server JRE distribution archives must be unpacked at the `<BIS_HOME>/runtime/jvm64/` directory when the installer asks for it.

You can either install a copy of the software or make this directory a symbolic link to the system Java. Using a directory copy has the advantage, that you can update it independently from the operating system maintenance schedules. In some situations (installing the JCE policy files, enabling legacy SSL3 support or switching random number sources) you might have to modify the content in this directory.

On *IBM AIX* the following command will copy the system-wide Java home (after you have installed the image JDK8 with smitty):

```
$ rm -rf <BIS_HOME>/runtime/jvm64
$ cp -r /usr/java8_64 <BIS_HOME>/runtime/jvm64
```

4.1.5 Oracle Database Driver

If you are planning to use Oracle as the system database, you also need to get the instant client archive of the latest supported version. Make sure to pick the "basiclite" version appropriate for your operating system. Please unpack the ZIP file (e.g. *instantclient-basiclite-linux.x64-12.2.0.1.0.zip*) into an otherwise empty folder. You need to provide this to the setup in a later step. See the *System Database manual* for details.

4.1.6 Operating Environment Preparation

Before you can start the installation process, you need to prepare the operating environment. This typically involves setting up a system parameters, system user for the application (runtime user) and an installation target folder.

4.1.6.1 System Time

It is important that all machines in a BIS system have the same time. This means the clocks should not differ more than two seconds. It is best achieved by snychronizing the clocks of all machines against a authoritative time server. It is recommended to use *ntpd* or *chrony* on Linux or Windows Domain mode (*W32Time*). In a mixed environment, it is possible to synchronize the domain master with an NTP server to ensure that Windows and Unix / Linux systems use the same time source.

No matter which time synchronization you use, it is important that this mechanism does not step time time backwards. If you need to correct a machines clock which is ahead of time all Software needs to be shut down on that machine first. Note that virtualisation products usually offer a clock synchronization tool. This should be turned off because it leads to time steps forward and backward. It is also not a good idea to use a regularly started time synchronization client (like *ntpdate* from *cron*), this does introduce the risk for time-stepping.

Currently all Instances within a BIS system need to have the same time zone setting. If the system time zone can not be adjusted make sure to pass the `-Duser.timezone=UTC` parameter to all instances (`vm.properties` file).

4.1.6.2 Windows Fileystem tuning

On Windows Server the NTFS file system is supported for installing and running BIS. Typically you use a disk/ volume seperate from the system drive.

You should configure the windows system according to Microsoft recommendations. This is documented in the “Performance Tuning Guidelines for Windows Server 2008 R2” or “Performance Tuning Guidelines for Windows Server 2012 R2” on the Microsoft home page.

The harddisk parameters (chapter “Tuning parameters for NFS file servers” in the above mentioned guideline) should be checked by the customer, e.g. the “NtfsDisable8dot3NameCreation” is by default set to 2 on Windows 2012, but should be set to 1. Explanation of these values and notes from the guideline:

Value and Meaning

- 0 NTFS creates short file names. This setting enables applications that cannot process long file names and computers that use different code pages to find the files.
- 1 NTFS does not create short file names. Although this setting increases file performance, applications that cannot process long file names, and computers that use different code pages, might not be able to find the files
- 2 NTFS sets the 8.3 naming convention creation on a per volume basis.
- 3 NTFS disables 8dot3 name creation on all volumes except the system volume.

Note: The system volume has 8dot3 enabled by default. All other volumes in Windows Server 2012 and Windows Server 2012 R2 have 8dot3 disabled by default. Changing this value does not change the contents of a file, but it avoids the short-name attribute creation for the file, which also changes how NTFS displays and manages the file. For most file servers, the recommended setting is 1 (disabled).

4.1.6.3 Windows Dynamic Port Range

BIS communication adapters and BIS system communication rely on beeing able to quickly open and close new TCP connections. This requires a larger pool for dynamically selected ports. This range of ports should not overlap with any statically assigned listener port.

The following commands can be used to check the number of ports and the start port:

```
netsh.exe int ipv4 show dynamicportrange tcp
netsh.exe int ipv6 show dynamicportrange tcp
```

Typically the default private/dynamic IANA port range (49152 - 65535) is large enough and does not overlap. On a busy system you might see errors like "`(10055) An operation on a socket could not be performed because the system lacked sufficient buffer space or because a queue was full.`" or "`java.net.BindException` ". In this case you need to increase the number of dynamic ports.

Note: Older Windows versions (this applies to updated machines as well) had a small port range of 5000 starting at port 1024. This is not only too small and will cause errors about used ports, but also the start port 1024 may conflict with startup listeners. If must be modified to the IANA range as stated above.

The number of ports should be at least 16000 and the start port should be above 20000. To set a new range use the following command:

```
netsh.exe int ipv4 set dynamicportrange tcp start=49152 number=16384
netsh.exe int ipv6 set dynamicportrange tcp start=49152 number=16384
```

If you need to use a larger number make sure that start+number does not exceed 65536 and is included in the higher port range. For example to double the range use:

```
netsh.exe int ipv4 set dynamicportrange tcp start=33536 number=32000
netsh.exe int ipv6 set dynamicportrange tcp start=33536 number=32000
```

You should also check that there are no (major) port exclusions in this port range (not supported with Windows 2008 (R2)):

```
netsh.exe int ipv4 show excludedportrange tcp
netsh.exe int ipv6 show excludedportrange tcp
```

If you need to make your dynamic port range very big you might need to use the port exclusion feature to reserve some well known listener ports (like 15000) inside this range.

Please be aware that changing this range will impact the ports selected for outgoing network connections and might therefore have to be coordinated with firewall administration and network security.

4.1.6.4 Configuring File Handles for Unix Systems

In order to run the system without any trouble of limited file handles in your Unix system, we expect the configuration to be increased to **16384 open files**.

The current settings can be displayed over the *ulimit -n* and *ulimit -Hn* command, both values must be at least **16384**.

The section "Creating the runtime user on Linux" already contains a description how to make this setting permanent.

4.1.6.5 Random Number Generator

Various components (especially SSL/TLS, UUID or token generation, database drivers and cryptographic operations like key generation, signing or encryption) require a fair number of cryptographically secure random bytes. In BIS, the default *Java SE SecureRandom* facility is used for most of these components. Depending on the operating system and JVM vendor there are different implementations:

On **Microsoft Windows** the default SecureRandom Provider used is the `SHA1PRNG` algorithm of the `SUN` JCE provider. In case of Windows each random number generator is seeded from a master SHA1PRNG seed source. And this source reads true random bytes from the Microsoft Crypto API. This API is typically fast enough to keep up with the entropy demand at startup, so you need no further configuration for Java 8 based BIS installations on supported Microsoft Windows server products.

On **Linux/Unix (*Linux*, *Solaris*, *HP-UX*)** when the *Oracle Java SE* runtime is used the default SecureRandom provider is `NativePRNG` in mixed mode provided by the SUN JCE provider. In mixed mode new random bytes are read from /dev/urandom (combined with an internal SHA1PRNG bit stream). Access to random seed bytes of the SecureRandom instance will be requested from `/dev/random`. This can possibly block of not enough available entropy is present.

On all operating systems the default SecureRandom implementation and seed configuration depends on the `securerandom.source` security property. It should normally not be changed (the meaning of the `securerandom.source=file:/dev/random` default is described above). In order to overwrite this configuration the JVM can be altered with the system property `java.security.egd` (would be specified in `vm.options` file). By default this property should not be specified (i.e. not overwrite the `securerandom.source`).

With the default setting it is important to make sure the operating environment (OS kernel) can collect random numbers from real hardware events (interrupt timing) or software sources. On virtualized guests or server machines with no user input devices (headless) the stream of fresh entropy is limited. For this reason it is important to make sure additional sources of entropy exist - especially on Linux.

Note: if the random number generator is waiting for additional random data this can severely affect performance or stability of the BIS system. SEEBURGER therefore requires customer to provide enough random entropy by approperiate operating environment configuration.

For **SuSE Enterprise Linux Server (SLES)** the `haveged` service is installed. This will collect timing differences for executing benchmarks. It will (starting with Version 1.5) check those measurements for proper randomness and add the measured random bits to the kernel entropy pool every time the pool is drained (less than 1024 bits by default). SEEBURGER has good performance results with this service. Details can be found in the *SuSE/Novell Support Knowledgebase* #7011351. If the daemon is not installed the following commands can be used to install and activate it from the official SLES repositories:

```
# zypper install haveged
# chkconfig haveged on
# /etc/init.d/haveged start
```

The same package also exists on **Enterprise Linux (RHEL, OEL, CentOS)**. The package is available from the *Enterprise Linux Extra Packages* repository (EPEL). See the EPEL Wiki "How can I use these extra packages?" for details on how to enable this community repository: http://fedoraproject.org/wiki/EPEL#How_can_I_use_these_extra_packages.3F

The following is a sample procedure to install and activate it on EL 6.8:

```
# rpm -Uvh http://download.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.noarch.rpm
# yum install haveged
# /sbin/chkconfig haveged on
# /etc/init.d/haveged start
```

Any other reliable source of random entropy is possible as well. This especially includes hardware tokens or TPMs to generate random numbers. Both normally require the *rngd* daemon from the *rng-tools* package. Recent Linux kernels and the KVM hypervisor also introduced a para-virtualized random number device which can be used to propagate random bytes from the hypervisor to the guests. Of course this means the actual hypervisor machine also needs enough random entropy available.

If you want to validate number of random bytes available you can use the following command to get the size of entropy bits from the Linux kernel:

```
# /sbin/sysctl kernel.random.entropy_avail
```

The printed number should be all time bigger than 1000 bit. If it is 200 or below this means there is no steady stream of additional entropy.

With the following multi-line command you can request a typical amount of random bytes. Each `dd` result shows the runtime and should be below 100ms. Be careful not to drain the random number device on production machines with this command.

Testing random device on Linux:

```
for i in $(yes | head -10); do
    dd if=/dev/random of=/dev/null bs=32 count=3 iflag=fullblock;
done
```

Testing random device on AIX or Solaris:

```
for i in $(yes | head -10); do
    time dd if=/dev/random of=/dev/null bs=32 count=3;
done
```

While executing this command loop, make sure all execution times are below 100ms and the number of read bytes should be 96 for all iterations.

Testing random device on Solaris (w/ companion utilities)

If you have installed the Solaris companion utilities (*SFWcoreu*) then you can use the *GNU dd* tool which has more features:

```
for i in $(yes | head -10); do
    /opt/sfw/bin/dd if=/dev/random of=/dev/null bs=32 count=3 iflag=fullblock
done
```

4.1.6.6 Host Name Configuration

The configured host name for each instance is communicated to other machines in the BIS system while operations. It is therefore important that all machines can resolve the hostnames into the correct IP address of all other machines.

On Unix machines it is also important that the hostname is listed in the /etc/hosts file beside a IP address which is different from 127.0.0.1 (aka localhost).

Reliability and performance of name->address and address->name resolution for all machine names and addresses used in a BIS landscape is important. A simple solution for this is to configure the names/addresses of ALL machines used in a BIS system on all machines (i.e. same hosts file).

hosts file (Windows: `%SYSTEM32%\Drivers\etc\hosts`, Linux/Unix: `/etc/hosts`) should contain one entry for each machine in a BIS installation. This should be the IP address used for internal communication. Add the hostname unqualified and with the domain suffix qualified to the line.

4.1.6.7 Creating the runtime user on Linux

The following is a sample sequence for creating an OS user for BIS runtime (which is also used to install the Software to ensure all files and directories are owned by this user). In the following examples a user named `seeasown` in the group `seeadm` is created:

For RHEL and SLES:

```
# /usr/sbin/groupadd seeadm
# /usr/sbin/useradd --home /home/seeasown -m --shell /bin/bash -c "SEEBURGER BIS 6" -g
 seeadm seeasown
# grep see /etc/{passwd,group}
/etc/passwd:seeasown:x:500:501:SEEBURGER BIS 6:/home/seeasown:/bin/bash
/etc/group:seeadm:x:500:
# passwd seeasown
Changing password for user seeasown.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Note: if you plan to use NFS or similiar shared filesystems it is essential that the numerical user and group IDs are the same on all machines.

The BIS runtime user should have unrestricted resource limits. You typically do this by adding the following lines to /etc/security/limits.conf

```
seeasown soft nproc 16384
seeasown hard nproc 16384
seeasown soft nofile 65535
seeasown hard nofile 65535
seeasown soft core unlimited
seeasown hard core unlimited
seeasown soft fsize unlimited
seeasown hard fsize unlimited
```

After making changes to this file and logging in as `seeasown` user you can use the "`ulimit -Sa`" command to see if the limits are removed. You can also use "`cat /proc/<pid>/limits`" (with the process ID of the java appserver) to see the current limits in effect. nproc should be at least 4000 processes for each BIS instance running under the same user, you can also set it to `unlimited`.

4.1.6.8 Creating the runtime user on Solaris

```
# /usr/sbin/groupadd seeadm
# /usr/sbin/useradd -s /bin/bash -c "SEEBURGER BIS 6" -g seeadm seeasown
64 blocks
# passwd seeasown
New Password:
passwd: password successfully changed for seeasown
```

If you receive the error message *UX: /usr/sbin/useradd: ERROR: Unable to create the home directory: Operation not applicable,* this most often means that the creation of directories under the base directory (here: */home)* fails. This is due to an auto-mounter setup. You can create the home directory in a different location by appending *-d /export/home/seeasown*.

See the "Creating runtime user on Linux" section for the user limits to set. In Solaris the hard limits for file handles are configured in /etc/system. Add the following lines and reboot:

```
set rlim_fd_max=65536
set rlim_fd_cur=65536
```

With the "`plimit <pid>`" command you can read the currently effective limits for a running process. It is recommended to check this after BIS process is started. You might need to set some project limits to get the correct reading for the BIS runtime user.

4.1.6.9 Creating the runtime user on Windows

Use the Windows System tools to add a new local user in the Group `Users`. This will require local adminsitrative priveldges. (If you install the Software later on as a System Service this user will also get the permission for logging in as a service granted). Under Windows you typically log into this user to make system maintenance, therefore the User should have the right to Login interactively, and you also should allow to open Remote Desktop Sessions for this user.

It is also possible to use a Domain account for this. This is especially needed in a failover cluster environment, in case you want to access remote file shares or you want to use the password-less authentication with Microsoft SQL Server database.

Make sure to follow best practice for application/service users. Do not use an account associated with a person, as it might happen the account gets locked or removed in the future. Also make sure the account has no critical password-change policy enforced.

4.1.7 Creating the installation folder on Windows

The BIS setup application will ask for the target installation directory (<BIS_HOME>). This directory should be a short path name and be located on a dedicated drive/volume. If you install multiple instances/products on the same machine it is recommended to use a common base directory as the parent (like `E:\app` or `D:\seeburger`).

If the installation user is member of the local administrators group the BIS setup application will automatically request admin priviledges and will create the instalaltion directory.

However if you run the setup as the BIS runtime user (which should not be a local administrator) you might need to create the installation folder (and base parent) manually and allow the BIS installation user as well as the BIS runtime user to write files into it.

You can use the Windows Explorer to create the base directory. To configure permissions click on the base directory, under Properties you switch to the *Security* tab and *Edit* permissions. Add the BIS runtime user with Full or Change permissions.

Instead of Windows Explorer you can also use the following command line input to create a new directory and grant the runtime user ("seeasown" in our example) full permision on this folder.

```
C:> mkdir e:\app\BIS
C:> icacls "e:\app\BIS" /grant seeasown:(OI)(CI)F
```

Depending on the Windows version and configuration you might need administrative permissions to generate the folder and modify owner and permissions. Make sure to not depend on "CREATOR OWNER" permissions but assign the permissions for the runtime user (e.g. `seeasown`) explicitely. The further installation steps can be done by logging in as the future BIS application runtime user (seeasown).

Note: Even If you execute the BIS setup application as a user with local administrator privileges, you need to add permissions for write/change or Full permissions for the runtime user to the whole directory tree. You can do this after you finished the installation.

The following restrictions for choosing the installation folder apply for Windows:

- System folders (`C:\`, `\Windows\`) cannot be used.
- If you use the users home directory as base directory you do not have to prepare permissions and do not need a local administrator for this.
- Some standard locations (`C:\Program Files`, `C:\ProgramData`) you may not be used as the installation path, the installer will not adjust access permissions.
- It is recommended to install on a separate data/application volume, not the system drive (C:)
- A maximum length of 64 bytes for the name of the installation home directory is supported [issue_b#51967].

- Should be a local disk or a cluster failover volume. NTFS or ReFS are tested.
- The installation path should consist only of letters A-Z, a-z digits 0-9 as well as '-' (minus), '_' (underscore) and ' ' (blank), path seperator and drive letter. Any national symbol or symbols like { [(! " # % & § must not be used. [issue_b#12315, issue_b#51974].

Sample installation directory (assuming instance.id="AIO1"): **D:\seeburger\BIS-AIO1\** (22 bytes)

4.1.7.1 Creating the installation folder on Unix/Linux

In the following example a logical volume is mounted on the mount point /app/seeburger. We create the installation directory /app/seeburger/BIS inside and make sure the runtime user is the owner. Setting up the base directory and mount points is typically a task for the system administrator (root user). You can use the `lsblk` and `df` commands to explore device and file system topology.

```
# lsblk
...
# df -H /app/seeburger
Filesystem             Size   Used  Avail Use% Mounted on
/dev/vg0/app_lv        200G     1M   199G   1% /app/seeburger
# umask 002
# mdkir /app/seeburger/BIS
# chown seeasown:seeadm /app/seeburger/BIS
# ls -ld /app /app/seeburger /app/seeburger/BIS
drwxr-xr-x  3 root     root     1024 Jun 22 12:44 /app/
drwxr-xr-x  2 root     root     1024 Jun 22 12:44 /app/seeburger
drwxrwxr-x  2 seeasown seeadm   1024 Jun 22 12:44 /app/seeburger/BIS
```

4.1.7.2 System preparation Windows

If BIS is installed on Windows Server 2008 R2 (or Windows 7) it is known to trigger a Microsoft Windows Bug about "leaking kernel sockets". You are required to install the Hotfix from Microsoft KB Article ID 2577795. The afd.sys driver file must be newer than 2011-07-08 (details see article).

We recommend to reduce the time for TCP keep-alive to be activated (5min in ms). This is especially needed for connections of the database driver to the system database, in case the database uses an fail-over cluster.

Insert a new DWORD key named "`KeepAliveTime`" with the decimal value `300000` into `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`. The Parameter for the retry time `KeepAliveIntervall` (1000ms) and maximum number of retries `TcpMaxDataRetransmissions` (5) normally do not need to be changed. This should be configured on all machines running BIS or Database instances.

4.1.7.3 System preparation AIX

Please ensure the following system configurations are in place to run BIS instances on AIX. They will allow the process to scale with load and they are needed to do better troubleshooting (especially JVM crash) if necessary.

IBM Java will write system dumps (core dumps) to the runtime log directory of BIS. Therefore, you need to make sure to have enough space for those dumps (typically at least 2 times the available RAM). In order to make sure the dumps contain full information and no legacy format, set the following settings as root:

```
# chdev -l sys0 -a fullcore='true' -a pre430core='false'
```

The same option can be set with the Smitty administration tool (System Environments > Change/Show Characteristics of Operating System). You can read about details in the IBM Java Diagnostics Guide 6 in section Problem determination > AIX problem determination > Setting up and checking your AIX environment > Enabling full AIX core files.

In addition to that the maximum core file (ulimit -c) should be unlimited to avoid truncation. This also means the filesystem which contains the `<BIS_HOME>/log/run` directory must be large enough to hold multiple memory dumps with the size of the maximum Java heap.

Please see the section for setting up the Linux runtime users on required resource limits. For AIX the changes are done in the `/etc/securtiy/limits` file. You should re-login and check with the `ulimit` command if the limits are in effect.

You must enable large file support on the file system. You can use Smitty to configure this for all relevant file systems.

4.1.7.4 System preparation Linux

The following system wide parameters should be configured. Find the settings in `/etc/sysctl.conf`:

```
fs.file-max = 6815744
fs.aio-max-nr = 3145728
net.ipv4.ip_local_port_range = 16000 61000
kernel.threads-max = 250000
net.ipv4.tcp_keepalive_time = 180
```

The default setting for file-max is calculated by the kernel based on available memory (100 files / 1 MB RAM). This is fine on systems with 64GB or more. For smaller systems you should use the specified value or more.

The large limit for aio-max-nr is especially required if Oracle is running on the same machine. However since the memory for the handles is allocated dynamically it does not consume memory if you use a large limit. Use the specified value or more.

The port range is specified in "min max" format. For Linux you normally use an upper bound of 61000 (to reserve some NAT ports) and the difference to the lower bound should be at least 16000 on small systems and 32000 on large systems. The lower bound should ideally be above the highest server port used by BIS.

The threads-max is calculated based on the available memory, you should use at minimum 4000 threads for each BIS instance on the machine. The default is fine for systems with 16 GB and more RAM. Use the specified value as a minimum, more if you run multiple BIS instances.

We recommend to reduce the time for TCP keep-alive to be activated (2-5 min in seconds). This is especially needed for connections of the database driver to the system database. But also helps when you experience regular network problems between instances or machine/ip failovers. This should be configured on all machines running BIS or Database instances (also see Dead Client Detection for Oracle database in the System Database manual).

You must reboot your machine and verify, that the settings are actually in effect. The following command can be used to read the current settings:

```
# sysctl fs.file-max fs.aio-max-nr net.ipv4.ip_local_port_range kernel.threads-max
 net.ipv4.tcp_keepalive_time
fs.file-max = 6815744
fs.aio-max-nr = 3145728
net.ipv4.ip_local_port_range = 16000 61000
kernel.threads-max = 250000
net.ipv4.tcp_keepalive_time = 180
```

You can also use `sysctl` command to set the new values, however this change is not permanent. This is why you need to add the setting to the `sysctl.conf` file which is read after boot. If the numbers are different check if some packages (for example "orarun" and "sapinit" on SLES) specify different values. Those values can typically be configured in /etc/sysconf/* (or in case of SLES with the Yast tool in the "System -> /etc/sysconfig Editor" menu).

When using recent *systemd*-based distributions (like **SLES 12 SP2**) you need to disable the systemd/cgroups based task limit:

- Modify `/etc/systemd/system.conf` and remove the hash ('#') before `DefaultTasksMax` and set the value to `infinite`. This should result in the following line:
  `DefaultTasksMax=infinity`
- Reload the *systemd* configuration after you changed the setting (or restart the machine)
  `sudo systemctl daemon-reload`

With `systemctl -l status <servicename>` you can check if there is a task limit active (it should print something like "`Tasks: 109`" not "`Tasks: 109 (limit 512)`").

4.1.7.5 Software Packages

There are some Linux packages which allow easy and comfortable system maintenance as well as trouble shooting. It is recommended to install them (but they are not required for normal operation): nc, tcpdump, lsof, screen, openssl, strace, perf, sudo, Xvnc, zip, unzip, curl, pv.

Installing those packages can significantly speed up troubleshooting.

Commands for RedHat or Oracle Enterprise Linux to install the packages from the repositories:

```
# yum install nc tcpdump lsof screen openssl strace perf sudo zip unzip curl dstat sysstat
# yum install tigervnc-server                                 # for remote graphical
 installation
```

Commands for SuSE Linux Enterprise Server:

```
# zypper install nc tcpdump lsof screen openssl strace perf sudo zip unzip curl sysstat
# zypper install tightvnc                                     # for remote graphical
 installation
```

4.1.7.6 Validation steps on Linux/Unix

As a first step you need to verify the installation platform: Operating System (vendor, version, patch level, edition) and hardware architecture. Please compare this with the system requirements from the (updated) release notes. On RHEL/OEL make sure the BIS runtime user is not confined by a SELinux policy and that only "target" policy is in effect (See Security Enhanced Linux (SELinux))

```
$ uname -sri
Linux 3.8.13-16.3.1.el6uek.x86_64 x86_64
$ cat /etc/oracle-release /etc/SuSE-release /etc/redhat-release
...
$ lsb_release -a
...
$ free -m
...
$ id -Z
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
$ sestatus
...
Loaded policy name:             targeted
```

Note: the BIS setup for Linux requires a 64-bit system (x86_64). If you execute the installer on a 32-bit platform (x86, i586, i686) you will get an error message after "Starting Installer" - see the Troubleshooting section later in this document.

4.1.8 Running Pre-Installation Checks

After unpacking the installation source it is possible to run the prerequisite check program. Please set JAVA_HOME environment variable to an existing Java 8 runtime environment and execute the following commands. Make sure to log in as the BIS runtime OS user:

Unix/Linux:

```
$ JAVA_HOME=/usr/lib/jvm/jre-1.8.0
$ export JAVA_HOME
$ cd /<MEDIA>/installer/_precheck
$ ./precheck.sh                                # for GUI version, requires DISPLAY/xhost
$ DISPLAY= ./precheck.sh -iface console | more # for Text-only version
```

Windows:

```
> set JAVA_HOME=C:\Program Files\Java\jre1.8.0
> cd /d <MEDIA>:\installer\_precheck
> .\precheck.cmd
```

A number of checks will verify settings like hostname, java version and temporary file directory as well as userid. The check for the Java version uses the JAVA_HOME you have specified, which might not be relevant as it is not the JRE shipped with the BIS installer.

5 Using the Installer

This section applies to running the software installer (setup) on any of the instances in your system for the purpose of initial installation or update/upgrade.

5.1 Setup Types

The software installer supports three types of user interface:

- The graphical user interface is best suited for a guided installation. It is available for Windows or Linux/ Unix (if you have access to the X-Window system).
- If you have only remote shell access to a machine, you can use the text mode (console) interface. It will interactively ask you for configuration settings, but does not offer graphical support for this.
- If you want to automate/script the Installer, you can use the "silent" mode. This is non-interactive and you need to provide a response file with all configuration questions. Silent installations are not subject of this guide (however the general description of screens and parameters can be used). Typically you finish an interactive installation (which will generate you a response file) and then use this (adjusted) response file to replicate the installation in production.

5.2 Graphical Setup with Unix/Linux

If you want to use the graphics mode for the software installer, you need to make sure you can run and display X-Window applications. There are multiple options for this. We recommend you use the first one, as it is the most reliable (in case of network problems you can reconnect to the still running session):

1. Virtual X11 Server running on machine; you connect with any VNC viewer from Windows
2. Machine has Physical X11 Server; you see the console or connect over Gnome or KDE desktop sharing (usually VNC as well)
3. Running a Windows-based X11 Terminal Emulator (like XMing server) and configuring the DISPLAY to connect to it (directly or via SSH forwarding)

The last option requires port forwarding or an open network connection from server to your workstation. It also requires to install a X-Window Server (like XMing). It is sensitive to network problems, because they will terminate the running installation program. It is therefore only recommended when required by pre-existing infrastructure.

I **Note**: Some Windows terminal emulation software (especially *XMing* with the default "-multiwindows" option) have problems when you want to enter text or select check boxes in the installer.

For *XMing* it helps to use the root window mode. In this case you do not have seamless integration with decorated windows which you can move around, but it offers enough functionality to finish the installer process.
Sample command line to start this mode: `"C:\Program Files (x86)\Xming\xming.exe" -wr –clipboard –screen 0 1024x768`
XMing will pick in this case a free display number (usually :0.0 (display 0, screen 0) and show it to you in the title of the XMing Window. You need to use this number for the DISPLAY setting (and it determined the port to forward, if X11 forwarding in SSH is used).

The *Software Packages* section in the last chapter already listed packages for a vncserver (*tigervnc-server* on RHEL and *tightvnc* on SLES). Please consult the manuals of your Linux distribution on how to setup and enable the vncserver. You might need to open host firewall ports. If you only need it to run the installer, it might not be needed to register the vncserver as a system process. In this case a command like the following can be used to start an ad-hoc session for the current user (this has to be the bis runtime user):

```
> vncserver -geometry 1024x768 -depth 16
```

As you can see preparing X-Window access can take some time, so ask your system administrators to setup a working graphical environment before the actual installation day.

It is important, that the setup tool can actually be executed as the prepared runtime user. This means you have to login as this user (or use `sudo` to start the installer with different user permissions. In this case you need to configure the actual X-window system to allow access for different users).

We recommend you test your GUI environment with the following commands (none of them should hang/ timeout):

```
$ echo $DISPLAY
:10.0
$ xhost
access control enabled, only authorized clients can connect
$ sudo seeasown -c xterm   # after this command you must see a new terminal window
                           # running as the installation user
```

If you have trouble setting up a graphical environment, or want a minimal server system it is better to run the installer in console (text) mode. This is documented in the appendix (page 74).

In a Microsoft Windows environment graphical installer can usually be operated by any remote desktop or console solution.

5.3 Starting the Installer

The installer application (setup routine) guides you through the setup of each instance.

In order to install the first instance of role Admin Server or B2B Portal the whole installation media is required. All other instances only need the setup executable and network access to the Admin Server role. The Admin Server and B2B Portal require the whole source media content. You find a compatible setup executable on the installation media or in `BIS_HOME/software/spm-repository/installer/` on the Admin Server instance.

The setup installer will self-extract all setup code and a Java Runtime to run. This is done by default into the system temporary directory (it uses `/tmp` on Linux/Unix). For this reason the temporary directory needs to have at least 1 GB free disk space and it must allow to execute commands. If you have a hardening policy that /tmp directory is mounted with `noexec` flag, or execution of scripts and executable in this directory is otherwise forbidden, then you need to overwrite the unpack location with the environment variable `IATEMPDIR`. Specify an existing directory with enough free disk space. The installer will create a installer.dir.* subdirectory.

You can use the `mount` and `df` commands to check the /tmp filesystem:

```
$ df -Th /tmp         # show fs type and human readable available size
$ mount -l | grep tmp
```

The installer should be executed as the (new) application user, otherwise the file permissions and ownership will not be correct. You can log-on with the correct runtime user or use su/sudo to switch to this user (if you use su/sudo you might need to grant X-Window system access with xhost on Linux/Unix).

Check the current user before starting the installer (Linux/Unix):

```
$ id
uid=1005(seeasown) gid=1013(seeadm) groups=10(wheel)
$ ulimit -Sa
...<unlimited>...
```

On Windows- or Linux/Unix-type operating systems with a graphical file browser, double click the *setup* file. Otherwise, you need to start the installer from the command line (also see the advanced options below). You are required to set up your operating environment (page 6) (user, system settings and target directory) first.

Note: If you use the graphical file browser, the installer will be started with the current log-in desktop user, make sure this is the runtime user you want to use later on for running the application.

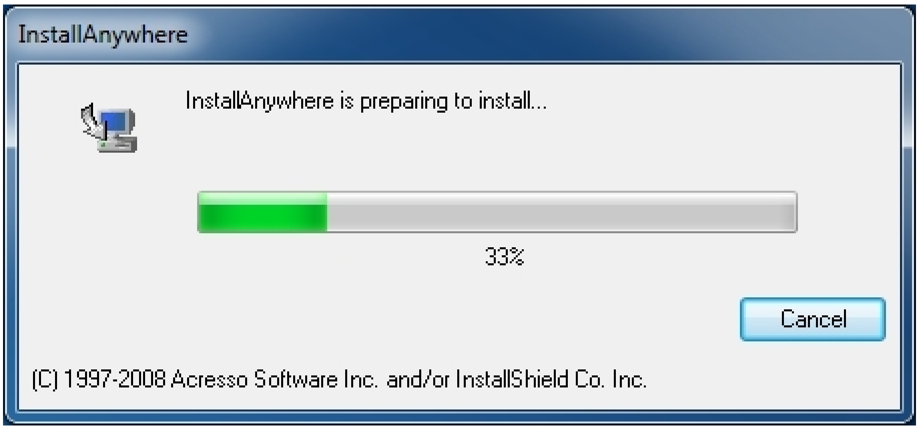
Platform	Installer Executable
Windows x64 (64-bit)	<MEDIA>\installer\win64\setup.exe
Linux x64 (64-bit)	<MEDIA>/installer/linux64/setup.bin
Unix	<MEDIA>/installer/unix/setup.bin
AIX	<MEDIA>/installer/aix/setup.bin
HP/UX	<MEDIA>/installer/hpux/setup.bin
Solaris	<MEDIA>/installer/solaris/setup.bin

The installer is Java-based. Only for 64-bit Windows and Linux operating systems it includes and unpacks a Java runtime. If you get error messages about missing libraries, or if the system JVM cannot be found in the system's search PATH, you might need to install some dependencies or specify a different JVM path. Please see the section *Installer JRE Troubleshooting*.

For AIX, HP/UX and Solaris the Java version from the current PATH is used. Please install a JDK provided by your OS vendor and make sure the right version is found in the PATH prior to launching the setup.bin script. You can also use the LAX_VM options (as described below) to specify the correct Java home.

```
$ which java
/usr/bin/java
$ /usr/bin/java -version
java version "1.7.0_51"
```

To illustrate the setup procedure we will show screen shots of the graphical installation on Microsoft Windows:



InstallAnywhere

InstallAnywhere is preparing to install...

33%

(C) 1997-2008 Acresso Software Inc. and/or InstallShield Co. Inc.

The following sections specify some special cases and troubleshooting, you can skip them if you succeeded starting the installer, proceed to the section *Language Selection (page 25)* in this case.

5.3.1 Installer Troubleshooting

If the error message *command not found* is displayed, make sure a Java Runtime Environment is installed and pre-pend its *bin* directory temporary to the search PATH:

```
$ java -version
sh: java: command not found
$ PATH=/usr/lib/lava-1.7.0/bin:$PATH
$ java -version java version "1.7.0_05"
Java(TM) Runtime Environment ...
```

If the error message *library not found* or *linkage error* is displayed,verify that the JRE is properly installed. Particularly, missing shared library dependencies are responsible for those kind of errors. The message "*JRE libraries are missing or not compatible*" is also printed, if the /tmp file system does not allow to execute binaries.

On Windows-based systems, there might be a system Java executable in one of the system directories. This is usually a stub which is checking the registry for the actual JRE version to use. With some broken installations (like stale registry entries), we recommend re-installing the system JRE or Java plug-in. It also helps removing the system-wide Java executable from the Windows base directory and adds a selected version directly to user's *PATH* environment variable or use LAX_VM argument as described below.

On Linux/Unix, If you receive the following error message when you try to start the setup: */setup.bin: line 1008: /tmp/env.properties.xxxxx* (with xxxxx representing digits) then you need to delete the corresponding temporary file and try the installation again. This step might require root permissions if your installation failed with the wrong user before.

The BIS6 Setup GUI mode might fail on Linux SUSE OS. The Setup would start with the language selection screen. After choosing the language and trying to continue it would fail with an error output in the terminal. The error message should contain lines similar to the following excerpt:

```
# Problematic frame:
# C  [ld-linux-x86-64.so.2+0x136a0]  _dl_x86_64_save_sse+0x30
```

Setting the LD_BIND_NOW environment variable avoids the issue. Please execute the command:

export LD_BIND_NOW=1

before launching the installer.

5.3.2 Advanced Installer Parameters

On *Linux/Unix*-based systems, the *execute* permissions for this script might not be set or the shell command might not be recognized. Then, specify a shell to execute the executable file directly (replacing *<MEDIA>* with the mount point of the installation media or the location of the unpacked distribution):

```
$ /bin/sh /<MEDIA>/installer/linux64/setup.bin
```

If you want to start the setup procedure with a specific VM, enter the following in the console (replacing <*JAVA*> with the full path to the Java executable):

```
$ /bin/sh /<MEDIA>/installer/linux64/setup.bin LAX_VM <JAVA_HOME>/bin/java
```

⚠ The LAX_VM target executable must be at least Java version 1.7.0_05.

If you want to start the setup procedure in the command line mode (i.e. without GUI), enter the following in the console:

```
$ unset DISPLAY
$ /bin/sh /<MEDIA>/installer/linux64/setup.bin -i console
```

Note that the setup procedure will unpack itself in the system's temporary directory, you can overwrite this with the IATEMPDIR environment variable. This is usefull if the free space on this device is too small or the file system does not allow to execute commands. The following example shows how to use /var/tmp instead of the /tmp default:

```
$ IATEMPDIR=/var/tmp /bin/sh /<MEDIA>/installer/linux64/setup.bin
```

If the setup procedure refuses to start, you might want to set the LAX_DEBUG environment variable, in order to get verbose output:

```
$ LAX_DEBUG=true /bin/sh /<MEDIA>/installer/linux64/setup.bin
```

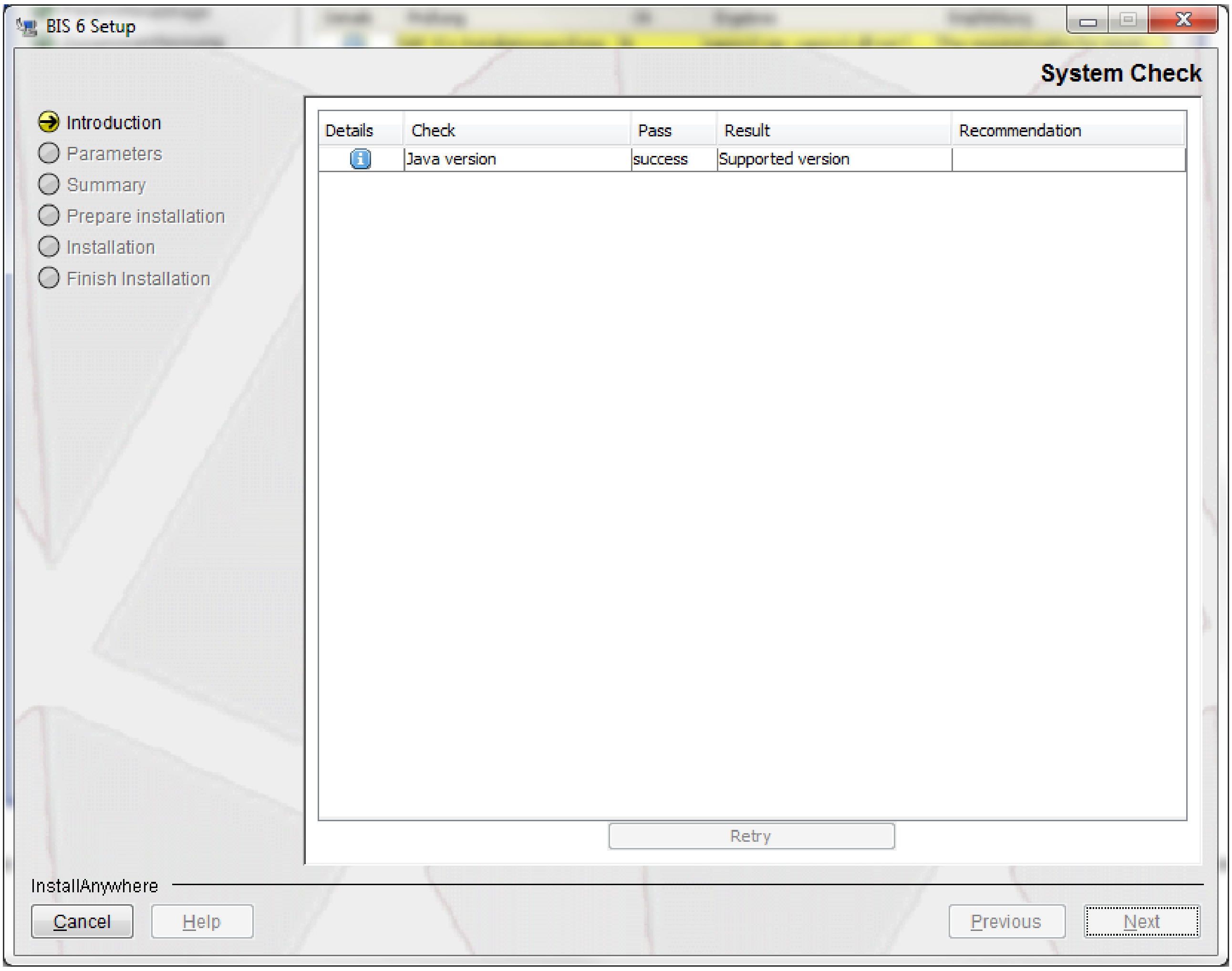
To specify the language of the installer, you can use the -l option with **de** (German), **en** (English), or **zh_cn** (Simplified Chinese).

Note: This setting does not affect the initial unpacking progress bar, and the Chinese version is only supported if you use the APAC product version provided by SEEBURGER APAC or an authorized partner:

```
$ /bin/sh /<MEDIA>/installer/linux64/setup.bin -l en
```

5.4 General Setup Dialog: System Checks

System checks are executed during the setup at various key points. The following is a sample screenshot of the initial check. If any step does not show success you can click on the details icon to get a detailed description. Correct the problem and retry the system check again. Do not ignore the warnings as this will most likely abort the installation at later steps.



Details	Check	Pass	Result	Recommendation
ℹ	Java version	success	Supported version	

The GUI Setup Prerequisite checks have an improper visualization update behavior with the following case[**issue_b#66669**]. If any of the prerequisite checks fails the user can do the requested actions for the according check and select the retry button in order for the check to be verified again and show the successful status. If the user selects involuntarily the next button before fixing the issue there is still an option to get back to the prerequisite panel and then perform the required actions. However, after selecting the retry button the already fixed check would still show the error/warning status. The user might still continue the installation or re-run the BIS Setup in order to be sure that they have the proper prerequisite status.

6 Installation of First Instance (Admin Server)

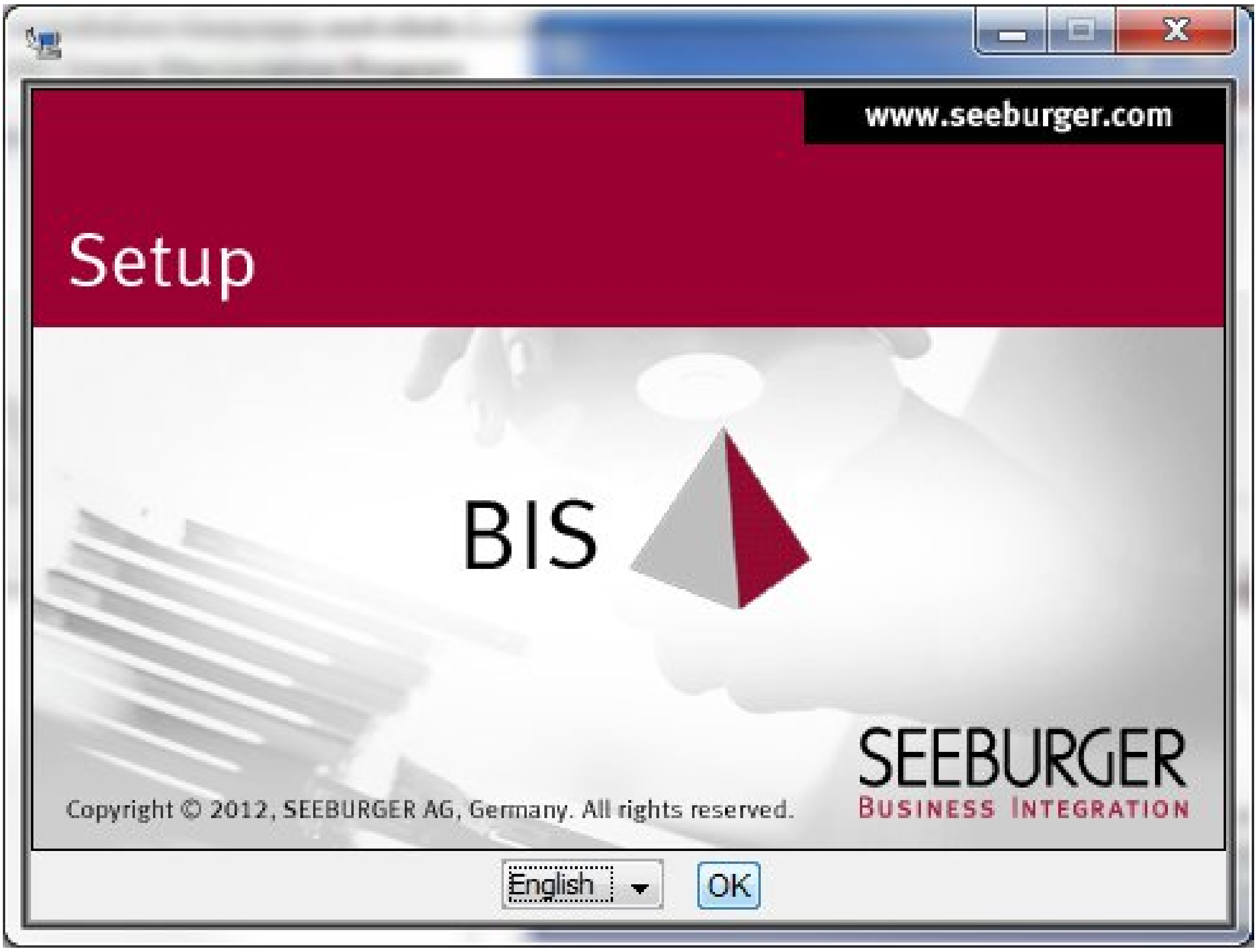
6.1 Introduction

The BIS platform needs at least one instance of role Admin Server which is providing management features. The administrative Front-End connects to this application server.This instance needs to be installed first. In this installation step the system database schema is created, the licensing file is requested and the instance with the Admin Server role is also responsible for providing a software repository for installing all further instances.

As a general rule, all installed instances should be started before you install the next instance. If you have multiple instances on the same host the setup can verify port usage only, if all configured instances on that machine are already running when configuring the ports for the next instance.

Note: For installing multiple instances on the same host there is a "port offset" setting which allows to change all listening ports by a specified offset to make them unique. This port offset does not mean you can simply increase it by 1 for each instance. For example if you install a second instance with portoffset = 1, then the management port 9999 of that instance will become 10000 and conflict with the first instance. You can use offsets like 102 and 202 instead.

6.2 Language Selection



Select your preferred installation language and click the *OK* button. The selected language **only** affects the installer GUI's language, i.e. you can freely choose the language that you prefer.

6.3 Installation Folder Selection

Note: The installation path you specify should not contain spaces and the max length is 64 characters. On a *Unix/Linux* you typically create the directory as root and own it to the BIS runtime user (which also must be used for the installation).

1. Enter or select the folder where you would like to install BIS.
2. Click the *Next* button.

Note: In the following chapters, we use *<BIS6_HOME>* as a place holder for the actual installation directory.

6.4 Role Selection AdminServer

Each Instance can fulfill different roles within a BIS System. One instance can have multiple roles. For each role, there can be multiple instances supporting that role, except for the roles WLH and AdminServer. See the *Concepts and Installation Planning* guide for details on planning your system landscape.

1. Select the Admin Server role and other additional roles you want to assign to this instance.
2. Click Next to continue.

Note: See the Maintenance Procedures (page 95) chapter for changing location, names or roles of existing instances (on Update).

6.5 Patch, Upgrade/Extend and Repair Selection

If BIS is already installed in the specified directory, the setup routine will guide you through a patch, update/extend and repair procedure.

The newly introduced method "Patch" for update of systems is only supported from release 6.5.2 installed. For updates on installed versions earlier than 6.5.2 the "Upgrade/Extend" option must be used instead.

Attention: Refer to the *Release Notes* to check whether the version to be upgraded complies with the version you are upgrading with. You may cause data loss, if the versions are not compliant, or not upgradeable.

1. Select whether you want to patch, update/extend or repair a present installation.
2. Click the *Next* button.

if you select "Patch", it is not possible to change parameters of your instance or extend the instance with new articles. Installed files will only be overwritten if a newer article package was present. This option is the normal option for software update.

If you select "Update/Extend", then installed files will only be overwritten if a newer article package was present. This is the normal mode to update a software installation. It is also possible to extend the instance with new articles.

In "Repair" mode, all files will be overwritten with the versions from the installation source. This is more risky as it might downgrade installed articles (remove hotfixes) and might undo custom modifications. Use this mode only if you need to recover a damaged installation.

Attention: Using the "Repair" mode might overwrite custom modifications or remove patches and hotfixes. If you extend the Installation with new articles, you have to reinstall the latest installed patch.

6.6 Creating the System Database

Please check the *Release Notes* for currently supported specific database versions.

Follow these steps:

1. Select the appropriate database management system from the displayed list (see the radio buttons).

2. Click the *Next* button.

Note: These dialog is not displayed, if you are updating or repairing your version.

- For *Microsoft SQL Server,* we ship a JDBC driver (based on *jTDS*). The SQL Server Instance has to be installed and must be running for the setup to continue.
- For *Oracle* Database, you need to download the corresponding *Oracle Instant Client* software. The DBA of the Oracle database has to set up table spaces for the new database objects, and the schema user has to be created. Please refer to the *Oracle as System Database for SEEBURGER BIS 6* Manual for details.

In the next screen you can specify some basic options on how you want to create the system schema. You need to install and prepare the system database management system before you can continue. See the *System Database* manual on details for the supported database products.

Microsoft SQL Server

1. Select whether a database connection check has to be performed (you should not skip this)
2. Select the authentication type for the database server. In order to create a new database, this login is used. You can chose between Windows authentication or SQL authentication (with the "SA" user and corresponding password). In order to use Windows (also called NT) authentication, the Windows user executing the installer and create scripts must be known and authorized on the SQL Server. Users in the local Windows Administrators group of the Windows server will have this permission. If the server is remote, this requires a Domain user (or you copy and execute the create script on the server machine as local administrator).
3. Check whether you want the setup to execute SQL DDL scripts. If automatic execution is not applicable, remove the check marks. In this case, you need to setup database and users manually (you can use and modify the created command file `<BIS6_HOME>/software/installdb/create-MSSQL2000-sa.cmd`. It must be executed with `sqlcmd.exe` on the search PATH).

Oracle Database

1. Select whether a database connection check has to be performed (you should not skip this)
2. Check whether you want the setup to execute SQL DDL scripts. If automatic execution is not applicable, remove the check marks. In this case, a SQL script file which can be executed with SQL*Plus is generated. This must be executed manually.
3. Select the directory which includes the basic-lite Oracle Instantclient (for version requirements, see *Release Notes*).

6.7 Installation Type

You can install the SEEBURGER BIS6 admin server instance as a standard- or clustered instance.

If you intend to install SEEBURGER BIS6 on a Failover-Cluster, please check "Cluster Installation" and enter the requested hostnames. The setup routine will assist you with providing the virtual hostname as a property during the installation routine.

The virtual hostname is used, instead of the real hostname, as the default “connect to” address in ports.properties. The real hostnames 1 und 2 are needed for the License Request Manager.

After the installation BIS can be activated to run as a service (please refer to Installation as Service on Microsoft Windows (page 105)).

6.8 Pre-Installation Summary

A *Pre-Installation Summary* dialog is opened.

1. Check whether the displayed installation directories correspond to the intended ones.
2. The shortcut folder might not be used on your platform (only *Windows*).
3. If the settings are OK, click the *Install* button.
   Otherwise, click the *Previous* button to correct the settings by following the steps that are described in the previous topics

At this point of the installation process, the setup will start to write files to the new installation destination. Keep this in mind, if you cancel the setup after this point. At least the software repository will be updated with the modules from the installation media (location: *software/spm-repository*).

6.9 Installation Start/Create Repository Dialog

After you click the *Install* button, the installation process will begin copying the files to the target system. The progression is represented by a progress bar in the bottom area of the dialog.

Besides copying all BIS modules to the target system, the process also copies the runtime components (*Java Virtual Machine*, *Apache Ant*, and *JBoss*). If you use *Microsoft SQL Server for* database management system, the appropriate JDBC drivers will also be copied to the target system. The installation files will be copied to *<BIS6_HOME>\software\spm-repository.*

Follow these steps:

1. A description of the applied action and its progress will be displayed. You have to wait until the process bar is filled. Then the next dialog is displayed.
2. Otherwise, wait for the completion of the procedures. If the dialog to enter article keys is displayed, you need to register all purchased modules by entering the (case-sensitive) article keys. The keys are provided with the delivery note for the BIS modules.
3. Click the *OK* button.
4. If applicable, repeat step 2 and 3 for the remaining articles/modules correspondingly.
5. Select the module(s) which you want to install. You can select either individual modules or any available (over the *all articles* check box).
6. If several options are displayed, select the one that applies for your system. (*Other VM / jdk_dummy* is an empty package, i.e. you do not want to use the provided *Java Development Kit* version).
7. If your article key is rejected, check for spelling errors (especially casing). Some articles may also refer to different installation media (especially the Developer Studio, or the additional media for the Business Integration Portal).
8. Click on the button *Next.* A summary screen will list the selected options.
9. Click the *Next* button. The (packed) files will be extracted then. A corresponding progress bar is displayed.
10. We provide a Java Development Kit for *Microsoft Windows* and *Linux* 64-bit operating systems. For other operating systems, the JDK has to be copied to the *runtime\jvm* directory. Follow the instructions given in the dialog.

6.10 Setting Profile Properties

In the following screen you can adjust the profile settings.

1. Please enter an Instance ID here.
2. Click the *Next* button.

The instanceID has to be unique for all instances in the same system. The systemID has to be the same for all instances in a system (you pick the systemID while installing the Admin Server role and the other instances do not allow to change it. As a default value the Admin Server will use its hostname however it is recommended to use a more descriptive value like COMPANY-PROD.

You can group multiple instances into a instance group. All instances with the same group name are in the same group.

⚠ **Attention:** For the B2B Portal you can chose the systemID freely, but it **must not** be the same systemID the BIS landscape uses.

6.11 Java Runtime Parameters (vm.properties)

In the following screen you can adjust settings for the Java Virtual Machine.

The button *Show Expert Settings* switches to the expert mode. For a detailed description of the parameters listed in the *Expert Mode* please refer to the documentation of the used Java Virtual Machine.

There are a number of properties, at runtime the JVM vendor and Bit-size will determine which properties are used. It is typically a concatenation of the SSL properties, the **vmoptions64** and **vmoptions.VENDOR64**. All vendor-specific options should therefore go to the more specific properties in order to allow reuse of the complete file on different architectures.

The main thing to configure here is the maximum heap size **-Xmx** parameter in **vmoptions64**. Make sure all Java machines can be run at the same time completely in RAM. The maximum heap size is only one component of the VM size. A running Java machine typically needs 20% (minimum 2GB) additional memory. See the RAM and Heap-Size section in the **Hardware Scaling** manual for details.

The `software/vm.properties` file (which is edited in this step) is read by the `software/register.{sh,bat}` script to create start scripts for the application server. This means that changes to this file will only take affect after stopping, registering and starting the application server.

⚠ **Caution:** Erroneous settings in the expert mode can lead to a defect and unstable BIS system. Please do not modify settings you are not familiar with. All properties need to be a single (possible long) line with no line breaks.

Oracle/HP Java Configuration

The Oracle Java VM is configured with **vmoptions64** and **vmoptions.SUN64**. On a HP/UX machine the HP provided Java is configured with **vmoptions64** and **vmoptions.HP64**. Since the HP JVM is based on the Oracle version they are both essentially configured in the same way.

Make sure to enable the detailed garbage collection logging with date stamps and log rotation, by adding flags (this must result in a single line for all options):

```
-Xloggc:log/app.vgc
  -XX:GCLogFileSize=10M -XX:NumberOfGCLogFiles=10 -XX:+UseGCLogFileRotation
  -XX:+PrintGCDetails -XX:+PrintGCDateStamps -XX:-PrintGCTimeStamps
```

IBM Java Configuration

It is recommended to always produce verbose garbage collection logfiles. With the following parameters you can ensure the logfiles will not be overwritten on restart and the files are rotated for long-running processes:

```
-Xverbosegclog:gc.%pid.%seq.log,10,10000
```

It is also recommended to use compressed references and large pages for performance reasons. You can use 64k pages without further system configuration and larger pages if you setup (reserve) the memory regions. See the IBM Java User guides for details.

```
-Xlp64k -Xcompressedrefs -Xclassgc
```

In order to make sure full information is captured in case you need to troubleshoot, the following settings are recommended:

```
-Xdump:heap:none
-Xdump:system:events=systhrow,filter=java/lang/OutOfMemoryError -Xdump:system:abort
```

Producing `javacore` files with the `kill -QUIT` signal is a lightweight method to get insight into the system. Therefore we turn off generating java dumps (PHD format) because they are less useful. In case you need to work on memory related issues you might want to add generating full system heap dumps (this is slow and needs lot of disk storage, therefore do not enable it by default. The above settings will write system heap dumps when a OOM Error occurs or you abort the process):

```
-Xdump:system:user
```

6.12 Database Configuration

The database access is configured in the next step. There are different requirements for database configuration, depending on the applied type of database.

Note: With an upgrade installation, the greyed out fields can not be edited. If you made a change to a field which had a default value, the field will be marked with a yellow background so you can verify if you need to adopt the value to a possible better default.

Attention: For Oracle make sure the schema is uncompressed before upgrading, as otherwise the setup cannot execute schema changes.

In order to continue the setup procedure, you require a working database instance and administrator-type access to create the schema owner (*Oracle Database*) or the database (*Microsoft SQL Server*) respectively. Depending on the database type and installation option, you also need to manually set up the BIS runtime user and database owner before you can continue.

For MSSQL Server you must use a password with a minimal lenght of 6 characters.

Make sure to enter username and password in the correct case since credentials might be case sensitive.

If you want to have a back-up of the master data on updates, please select the option "Backup database on upgrade" in the expert settings.

The selected options will be verified, i.e. you cannot continue if anything is missing.

Note: For information on supported DBMS versions and platforms, please refer to the most recent *Release Notes* for your BIS version.

Note: A few database passwords are incompatible with this BIS version, due to a bug related to the Application Server. The Setup program will notify you if you're using an incompatible password. You can also check it by calling $BISAS_HOME/software/encode-password.{bat/sh}. [**issue_b#16033**]

6.12.1 Microsoft SQL Server

Note: Please note that BIS 6 supports only TCP/IP connections with static ports.

Via the button *Show Expert Settings*, you can switch to the expert mode.

Note: Erroneous settings in the expert mode can lead to a defect and unstable BIS system.

If you are using named instances, you will need to add the name of the instance in the ***Named DB instance*** field. Please do not forget to enter the according instance port number in ***DB port*** field.

1. Ensure that the *Microsoft SQL Server* application is running locally or remotely.
2. In the *Database Configuration* dialog, enter the required information.

Note : Please use the fully qualified host name instead of *localhost*.

3. Select database authentication type
   I. Non NT-authentication
      i. SQL Server 2008 expects a complex password. This means:

      - The password does not contain all or part of the account name of the user. Part of an account name is defined as three or more consecutive alphanumeric characters delimited on both ends by white space such as space, tab, and return, or any of the following characters: comma (,), period (.), hyphen (-), underscore (_), or number sign (#).
      - The password is at least eight characters long.
      - The password contains characters from three of the following four categories:
        - Latin uppercase letters (A through Z)
        - Latin lowercase letters (a through z)
        - Base 10 digits (0 through 9)
        - Non-alphanumeric characters such as: exclamation point (!), dollar sign ($), number sign (#), or percent (%). You can find this information on the corresponding *Microsoft*® web site.

      ii. If no such password is provided, *create-mssql2000.cmd* fails.

Note: This is only a warning. You can ignore this message if your database does not use complex passwords.

II. NT-authentication (available only in Windows installation). It requires a Windows user with database administrative permissions.

Select NT authentication ckeckbox. The following fields will be disabled: "Schema user password", "Runtime user", "Runtime password".
Use Schema name for data base schema name. Windows logged in user is used for database authentication.

Note: Selecting NT-authentication will not create schema (dbo) and runtime user. Windows logged in user will be used instead.

4. Click the *Next* button. The following verification steps will be carried out:
   - Verification of the database host name and the database name. E.g. the host name must not contain “_” (underscore) symbols.
   - Verification of the database location (*local* or *remote* type):
     - If database host = server’s host name (local) # local installation.
     - If database host = server’s host name (remote) # remote installation.
     - *Microsoft SQL Server* access:
     - No access: Please start the *Microsoft SQL Server*.
5. The installer will test the database connection.
6. Depending on the database parameters' verification result, perform the following action:
   - Message *Not available* or *SQL connection error* is displayed: Go back to the parameter configuration dialog of the database, correct the settings and follow the previous steps analogously.
   - If the database is available: Resume with the registration of the BIS modules on the application server.

Security Note: The sa-password is not saved in the *create-mssql2000-sa.cmd* file, but has to be entered on the remote server during the execution due to security reasons. For local automatic installation, it will be transferred to the script by the installer.

.

6.12.2 Oracle Database

The following is only a short summary, please consult the *Oracle as System Database* manual for extensive description.

1. Ensure that the following information is known before starting the installation:
   - The **database instance** must be available and accessible.
   - You need to know the **host address** and **port** of the database listener.
   - You need to know the **SID** or **Service Name** of the running instance. (If you want to specify more complex connection parameters like *service name* or *RAC options*, you need to use the Expert option or modify the *register.properties* file later on manually and run the *register* function again). Typically, the SID is the *RAC service name* with a trailing '1'.
   - You need to know the **name and password of the schema owner user**. This user has to be created on the database server and requires the permissions to create tables and views. This user also needs at least one table space with enough quota to store the initial tables.

- Normally you should use the **ANSI** database encoding (i.e. columns are created with *VARCHAR2* types). Then make sure that the database character set parameter is set to a character set that can store any symbol that is required/desired for input of configuration parameters. This includes the *ALE 32UTF8* character set. We recommend to prefer this option over the *UNICODE* encoding, which will create text columns with the *NVARCHAR2* type instead.

2. In the related *Database Configuration* dialog, enter the required information.
   Via the button *Show Expert Settings* you can switch to the expert mode

Note: Erroneous settings in the expert mode can lead to a defect and unstable BIS system

3. Click on the button *Next* to continue.
   The installer will then test the database connection.
4. Depending on the database parameters' verification results, perform the following action:
   - **If the database is not available:**
     Go back to the *Parameter Configuration* dialog of the database, correct the settings and follow the previous steps analogously.
   - **If the database is available:**
     Resume with the registration of the BIS modules on the application server.

6.13 Change Ports Properties

The network configuration of the instance is done in the `software/ports.properties` file. The setup will ask about settings for services of the application server as well as settings for connecting to other instances of the system. The default values for instances are read from the Admin Server. Just like the other properties files changes to this file are only applied after running register.{sh,bat}.

You can change the settings for the ports here. Via the button *Show Expert Settings*, you can switch to the expert mode.

Note: Erroneous settings in the expert mode can lead to a defective and unstable BIS system.

Port offset

In general you should avoid installing more than one instances on the same machine. In order to allow the setup to detect port conflicts you should always start all previously installed instances on the same machine before installing another one.

There is a property `port.offset` which is numerically added to all server ports in order to allow quick and easy configuration of multiple instances on the same machine. Good candidates for the offset are 102 or 202 (port.offset=1 does not work, because this will make port 9999 + 1 conflict with the port 10000 of another instance).

Ports calculated with the port offset are:

- remoting.port
- remoting.osgi.port
- rmi.port
- snmp.listener_port
- hornetq.remoting_netty_port
- jboss.transaction_recovery_port
- jboss.management_native_port
- jboss.management_http_port

- management.http.port
- admin.rest.port
- datastore.port
- portal.port
- dc.connect.port
- md.cache.connect.port
- inbox.network.port

However the listeners for the properties `http.port` and `https.port` are not calculated with the port offset. These both ports are only bound on the AdminServer and not on any other instance. Therefore you will not run into any conflict when having other instances in parallel with the AdminServer on the same machine. If you need to install two instances of the role AdminServer on the same machine you need to modify http.port and https.port in addition to a port offset for all other server ports.

6.13.1 Installing BIS with Virtual IP Addresses

If you are installing BIS 6 instances on a system with virtual IP addresses, the ports check might incorrectly show that some of the BIS ports are already occupied. This is because the setup verifies each port using the master IP (standing for localhost) instead of the virtual IP, which hosts the according instance. You can ignore this check, after manually verifying for port collisions (e.g. "`netstat -an| grep <port-no>`") [**issue_b#53952**]

6.14 Registering BIS Modules on the Application Server

The various BIS modules will now be registered on the application server and the configurations will be created, according to the settings from the files *profile.properties, register.properties*, *vm.properties* and *ports.properties* from the *<BIS6_HOME>/software/* directory.

For the upgrade procedure, the required database modifications are detected and displayed. For the *Microsoft® SQL Server®* in *expert* mode, the creation of the database will be skipped; the tables will be created with the authorization rights of the *dbo user* and the data will be saved.

The *create-mssql2000-sa.cmd* file will be generated in an automatic mode. If the installation has been carried out locally, then it will be executed immediately. Otherwise, the user will be prompted to execute the script on the application server. The successful creation of the database is displayed, if the installation has been carried out locally.

In the case of a *Microsoft® SQL Server®* installation: If the database is not already present, follow the steps described in the topic *Remote Installation of Microsoft SQL Server (page 35).*

6.14.1 Remote Installation of Microsoft SQL Server

1. Expert mode: Manually create the database and the *dbo* user. This is followed by the database check and the preparations for the creation of the tables and the repository storage of the data (the *expert* mode is available for the local installation of the *Microsoft SQL Server*).
2. On the server, enter/execute `create-mssql2000-sa.cmd` to create the database. This is carried out during the registration of the BIS modules on the application server. If the applied DBMS does not support NT authentication, start the script with the *askme* parameter applied. Use the *sa* password.
3. If the database is located on a remote server, enter the corresponding values for the database host, the port number, the user and the password. The system will check whether the user is able to register on the database.
   - *Failed*:
     Reports that a connection could not be established, and that the script has to be executed on the remote server. Go back to the notification screen *Remote Installation*.

- *Successful*:
  Resume with the registration of the BIS modules on the application server.

6.14.2 Local Installation of Microsoft SQL Server

If the database does not exist, and the option *Check connection* was selected, the database is automatically created.

There are multiple reasons why this step can fail: It requires *sqlcmd.exe* in the user's PATH environment variable. The sqlcmd*.exe* version must be compatible with the targeted SQL Server. The *sa* password must be correct (and *sa* authentication via mixed mode must be allowed), or the local user must be part of the SQL Server administrators.

The local user must be logged to the right domain. Database names should be unique. If the above screen shows any error it is best to switch to the console and open the script. You can configure various options (especially the *%OP%* variable).

6.15 BIS Setup Database Changes on Upgrade

Database Changes on Upgrade

⚠ **Attention**: During the setup routine, only master data (no runtime data) is backed up. **In case of an upgrade, it is recommended to have a full backup of the database.**

If you have checked the option "Backup database on upgrade" in Expert Settings of Database Configuration screen, a back-up of the master data in the database is created during an upgrade installation.

After a successful back-up the new database structure is compared to the current database. During this comparison the changes to the database are listed in the file *<BIS6_HOME>/log/install/diffdb.log*.

If errors occur during this comparison they are listed in a screen. Please follow the displayed instructions in such a case.

Should you have to make changes to the database, a screen opens after the comparison of the two structures:

1. Select the option you want to do next.
2. We recommend to deploy the changes automatically. If you deploy the changes automatically the screen *BIS Database Update Test* appears again and the changes are now executed.
3. Click on the button *Next*, when the build was successful. The previous saved data is written back to the database.

6.16 Database Initialization

This installation step performs automatically. Database-specific scripts for generating tables and saving the system master data are executed in this step. After each partial step has been carried out, a log file will be displayed.

1. Then continue with the next step by clicking *Resume/Continue*.

If the first step has problems (for example missing authorization), it will be retried. You can fix the error condition in the background and try the step again. Fixing the problem includes modifying the register.properties file, or actually modifying or configuring objects in the SQL server. At this stage you also have time to reconfigure and run the *create-MSSQL2000-sa.cmd* command if needed.

The default values will be written to the corresponding database tables.

If you have deselected the option *automatic SQL Import*, you are prompted to execute the SQL scripts. These scripts have to be executed before the installation is continued.

6.17 Finish Installation (Licensing)

Finally, a link to third-party licenses is displayed. With *Microsoft® Windows®* operating systems, the corresponding directory will be opened if you click on the link.

In the dialog, click the *Next* button. Now *License Manager* will be started.

(For the initial BIS installation, the license list is empty.) Please request a license and import it with the *License Manager*.
The license is required for operating the BIS software. For initial BIS operation, a trial license can be used, which is valid for 30 days. For more information on licensing, refer to the separate documentation License Manager.

After this, the installed solutions will be registered.

6.18 Register Solution

In BIS releases before 6.5.2 the last step of the installer was executing the register-solution script. This is no longer done automatically in order to allow to manage the content deployed on BIS (solutions) independent of software installation and updates.

Solution archives are provided with the initial installation or as a specific hotfix. Then you need to invoke the `register-solution.{bat,sh}` or `deploy-solution.{bat,sh}` script. See the dedicated solution installation chapter in the *Release Notes*.

6.19 Finish Installation

In the dialog, a message informs whether the installation has been successful or not.

1. If no error occurred, click the *Done* button.
2. Otherwise, click the *Previous* button and correct the settings in the dialogs that are described in the previous topics.

When the installation is completed, the log files that have been generated during the installation process will be moved to a shared directory with a name containing a time stamp of the installation.

7 Instance Setup

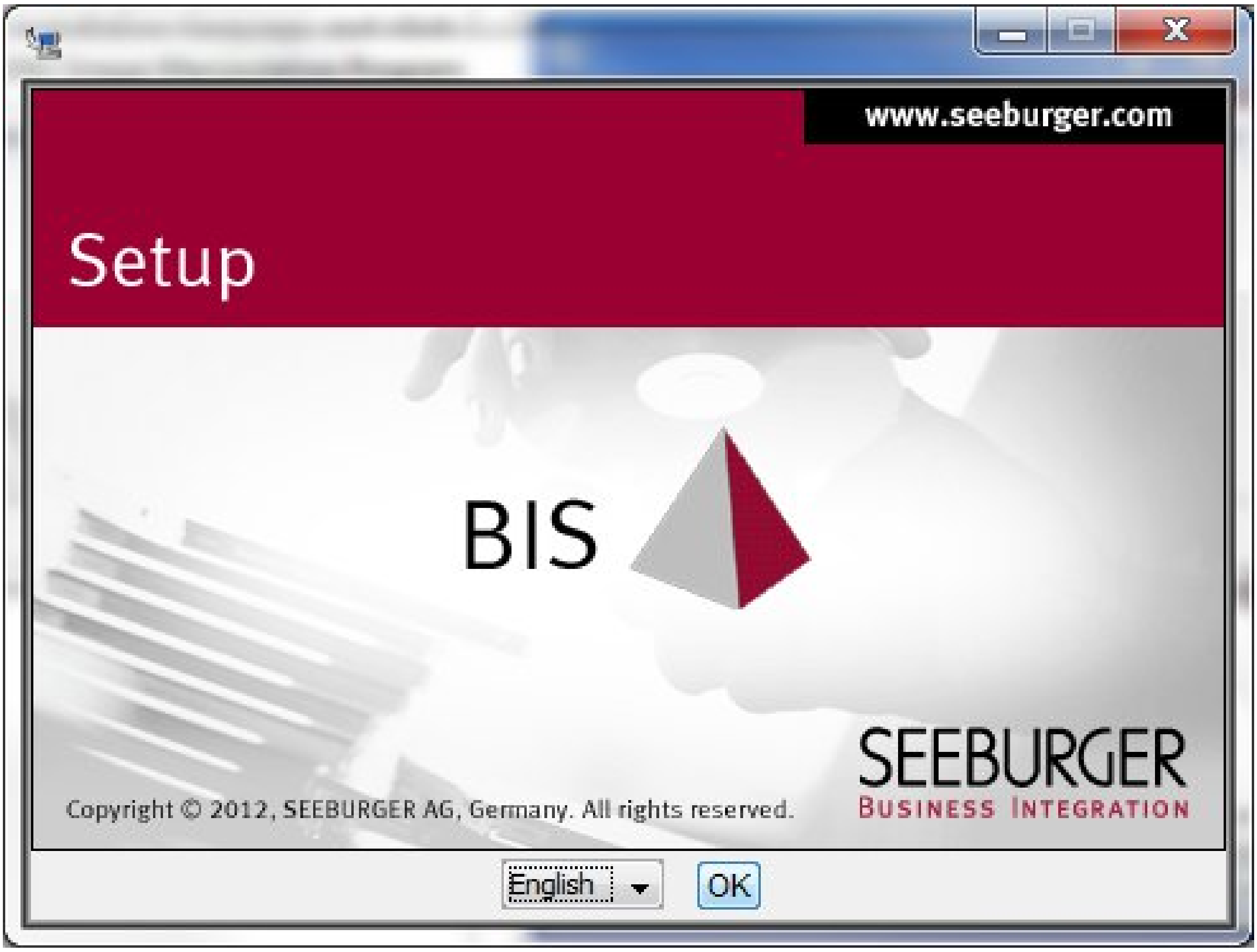
After installing the first instance (which has to have the Admin Server role), you can install further instances. For this to work, the instance with the Admin Server role must be running and reachable on the http or https port.

You copy the setup executable from the Admin Server instance, or you use the installation media on the machine for the further instance installation. In both cases, you start the executable and have to de-select the Admin Server role (in order to make the setup ask for a connection to the Admin Server instance).

The instances can be a Process Engine role (for running the process engine), an Adapter Engine role (for running one or more adapters) or a WLH (Worklist Handler) role for managing legacy queues. You can have more than one instances with the role Admin Server. In order to install another Admin Server, you must also select the Additional Instance option for the Admin Server role.

You can have maximum one instance with the role WLH and in order to install multiple process engine instances you need a special licensing option. A single instance can be of multiple roles.

7.1 Language Selection



1. From the combo box (located on the bottom), select the language that you prefer.
2. Click the *OK* button. The BIS Instance Setup's *Introduction* screen is displayed then.
3. Click on the button *Next*. The *Choose install folder* dialog is displayed then.

7.2 Installation Folder Selection

Note: The installation path you specify should not contain spaces and the max length is 64 characters. On a *Unix/Linux* you typically create the directory as root and own it to the BIS runtime user (which also must be used for the installation).

1. Enter or select the folder where you like to install the BIS6 Instance.
2. Click the *Next* button.

Note: In this manual we use <INSTANCE_HOME> as a place holder for the installation directory of the instance. If you have multiple instances, you need to repeat the steps described in the manual for all installations. If an Instance is already installed in the specified directory, the setup routine will guide you through an update/repair procedure.

7.3 Role Selection

Each Instance can fulfill different roles within a BIS System. One instance can have multiple roles. For each role, there can be multiple instances supporting that role, except for the role WLH. See the *Concepts and Installation Planning* guide for details on planning your system landscape.

1. Select the role(s) you want to assign to this instance.
2. For an additional Admin Server select the Additional Instance.
3. Click Next to continue.

7.4 Pre-Installation Summary

1. On the Installation Summary you can see the Product Name, Install Folder, Shortcut Folder and the Role(s).
2. If the displayed summary corresponds to the intended settings, click the *Install* button.
3. Otherwise, click the *Previous* button and correct the settings in the dialogs that are described in the previous topics.

7.5 Installation Start/Create Repository Dialog

After the activation of the *Install* button, the installation process will begin copying files to the target system. The progression is represented by a process bar in the bottom area of the dialog.

1. Wait until the progress bar is filled. The next dialog will be automatically displayed. There, select the repository for copying the required files either per *HTTP* transfer, or per copy procedure from a local repository.
2. Click the *Next* button. The selected repository will be checked and dowloaded to your install folder.
3. If you have selected the role **AdapterEngine** the purchased articles are listed then in a check box. You need to check all entries which should be installed.
4. If several options are listed, select the one that applies to your system.
5. After completing the selection, click the button *Next*. The dialog that is then displayed shows a list of the articles selected for installation.
6. On Upgrade the setup will show the articles to be upgraded.
7. Click the *Next* button. The (packed) files are then extracted. A progress bar and a message that describes the action are displayed.
8. We provide a *Oracle Java SDK* only for *Microsoft Windows* and *Linux* 64-bit operating systems. For other operating systems, the *Java Virtual Machine* has to be copied to the *runtime\jvm*64 directory. Follow the instructions given in the dialog.
9. Click the *Next* button. Now the various BIS instance will be registered.

7.6 Change Properties

Note: With an in-place update installation some of the fields are disabled and can not be edited.

Profile Properties

The profile properties configure the *group name* and *instance ID* of the new instance and also make the instance part of a specific system (determined by the *system ID* inherited from the Admin Server instance).

Configure a mandatory and unique instance ID. Optionally, you can specify the name of an existing or new instance group to join. You are responsible for only adding instances into a group if they have the same function and can stand in for each other - as defined in the landscape planning.

Ports Properties

You can make changes to the settings for the ports.

Via the button *Show Expert Settings* you can switch to the expert mode.

Note: Erroneous settings in the expert mode can lead to a defect and unstable instance.

VM Properties

You can make changes to the settings for the Java® VM here.

Via the button *Show Expert Settings,* you can switch to the expert mode.

Note: Erroneous settings in the expert mode can lead to a defect and unstable instance.

BIS MT webservice configuration for profiles

You can make changes on settings to get BIS MT search profiles.

This configuration is only available if new MT UI is installed.

Note: Erroneous settings will be presented on application access.

BIS MT webservice configuration for data

You can make changes on settings to get BIS MT data from configured data source.

This configuration is only available if Information Layer is installed.

Note: Erroneous settings will be presented on application access.

7.7 Registering BIS Modules

In the next dialog, the performed steps are displayed. When this procedure is completed, the *Next* button is available again, click this button.

7.8 Finish Installation

In the dialog, a message informs whether the installation has been successful or not.

1. If no error occurred, click the *Done* button.
2. Otherwise, click the *Previous* button and correct the settings in the dialogs that are described in the previous topics.

When the installation is completed, the log files that have been generated during the installation process will be moved to a shared directory with a name containing a time stamp of the installation.

8 Advanced Portal Setup

8.1 Reverse Proxy

B2B Portal may be operated behind a *reverse proxy* due to the following reasons:

- Restricting access to certain resources
- Masquerading logical systems
- Providing a central access point

When a reverse proxy is involved, users can not directly access B2B Portal, but only through the reverse proxy. This can be used for **restricting access** to the certain applications only to a certain group of users. A reverse proxy may also do additional security checks for incoming requests, in that case the proxy is usually called a *Web Application Firewall*. If an installation has more than one logical system, it may be desirable to assign one domain or sub-domain to each logical system (**masquerading**). Some companies organize all their Web applications in a central Portal installation which has a single host, domain or sub-domain reserved and acts as **central access point**.

The communication between reverse proxy and B2B Portal takes place using one of these protocols:

- Hypertext Transfer Protocol (HTTP) (optionally the secured HTTPS)
- Apache JServ Protocol (AJP)

HTTP is the standard protocol of the World Wide Web used by Web Browsers for accessing Web servers. Since this is the standard protocol, it is supported by any reverse proxy device, software or hardware. AJP originates in the Open Source community and originally served for integration with the very popular Apache HTTP server, which can also act as reverse proxy. Being specifically designed for reverse proxy operation, AJP features increased performance and simpler installation over HTTP.

8.1.1 Restricting Access

In B2B Portal, users are authenticated and have to be authorized for accessing applications. So a reverse proxy for restricting access is not necessary, only in cases where access to certain applications must be restricted by time patterns, or to IP address ranges. An example would be limiting access to the *Administration* to users from the local Intranet.

In the case of a reverse proxy being used for restricting access, rules have to be configured on the reverse proxy. These rules are usually URL patterns, with allow or deny flags. Each application has its own distinct URL prefix. The available applications and prefixes can be looked up in the *Administration* | *Portal* | *Portal Applications*.

While a usual reverse proxy just forwards user requests, a *Web Application Firewall* also does content inspection in order to find malicious patterns. Such software tries to prevent *Cross Site Scripting (XSS)* or *SQL Injection* attacks reaching the target system.

8.1.2 Masquerading Logical Systems

If there is more than one logical system, the target logical system is usually chosen at the login page. Since each web request targeting B2B Portal must be matched to a logical system, usually the login page from the default logical system is shown. If the logical systems do not share a common design, it may be desirable to choose the logical system even before the login page is shown. This can be achieved as follows:

- Passing the query parameter *env=[name of the logical system]* with the first request.
- Using a reverse proxy to pass the HTTP header *X-SMARTI-Env=[name of the logical system]* with requests.

Passing the query parameter *env* is usually done by placing a link *http://portal/security/login?env=[name of the logical system]* on a portal page and letting users access this page. A reverse proxy provides more flexibility, for example it allows for matching host names, domain names, or sub-domain names with logical systems. The reverse proxy does this by inserting the *X-SMARTI-Env* HTTP header with its value based on the matched name.

8.1.3 Providing a Central Access Point

Central company portals that integrate software from different vendors typically require that applications are accessible under a central access point. There are two different kind of central access points:

- Sub-domain based
  Each application is reachable via its own sub-domain, like *http://* **accounting** *.example.com* for the accounting software and *http://* **hr***.example.com* for human resources. B2B Portal should not need any additional configuration in this case. Please refer to the description of the *REDIRECT_HOST* parameter in the *Administration* manual if there are problems after submitting forms.

- URL-based
  Each application is reachable via its own directory on the central access point, like *http://example.com/* **accounting** */* for the accounting software and *http://example.com/* **hr** */* for human resources. B2B Portal must use so-called relative URLs in this case. Please refer to the description of the *USE_RELATIVE_URLS* parameter in the *Administration* manual.

- URL-based with context prefix
  In case the reverse proxy is not able to modify the external to the internal url, it is possible to add a prefix to all urls of the applications. The application server will be provide the application with the url like *http://example.com/accounting/* and all installed applications below this base url. This is configured by an additional entry *context.prefix* in the file *software/vm.properties*, which has the additional context path prefix like *accounting*. Afterwards call *register.bat/.sh* and modify all urls in the applications (Portal applications, Message Tracking urls, ...).

8.1.4 Reverse Proxy Integration

B2B Portal can support any reverse proxy that supports the HTTP/1.1 web standard, including software-based solutions such as *Microsoft IIS*, *Microsoft ISA* or *Apache HTTPd 2*. If supported by the reverse proxy hardware device or software, using the AJP protocol is recommended over HTTP.

A reverse proxy software solution commonly runs directly on either the B2B Portal host or is provided as a central service by the IT department. If the reverse proxy is used as an additional security measure, the network landscape must make sure that the reverse proxy cannot be circumvented. This can be achieved with a firewall device that is put in place between the B2B host and the network, or a firewall software on the B2B Portal host.

8.1.4.1 Apache HTTPd

If Apache HTTPd is to be used as reverse proxy software, the modules *mod_proxy* and *mod_proxy_ajp* are recommended in conjunction with the following configuration directives:

```
ProxyPass         /  ajp://portal:8009/
ProxyPreserveHost on
```

Request header modification (e.g. for masquerading logical systems behind domains) is possible using the module *mod_headers* and the following directive:

```
RequestHeader    set   X-SMARTI-Env  default
```

8.2 Kerberos Single Sign On

B2B Portal can be integrated with Kerberos in order to use the Single Sign On capability of this protocol. With Single Sign On, users only need to authenticate once at their workstations and then are automatically granted access to other services in the Intranet. This protocol is automatically available when Windows Domains are used.

When a user first accesses B2B Portal with Kerberos Single Sign On enabled, a new user account is created for that user. The administrator can either define default roles to be assigned to these users, or assign roles and groups manually. The user does not need to remember a password because authentication is handled between the Web Browser and B2B Portal via cryptographically secured tickets.

Note: The Kerberos protocol provides transport security, but this is not the case if it is used it with web applications. The authentication itself is secure, but if protection of the data is also required, you must enable SSL additionally.

8.2.1 Prerequisites

A working Kerberos installation is mandatory for this feature. Kerberos is provided by a Windows Domain or can be installed as an add-on package in UNIX installations.

- Windows Support Tools must be installed from either the Windows Server CD or Microsoft Download Center.
- The Windows Server Resource Kit contains useful debugging tools (*kerbtray* and *klist*).

8.2.2 Environment Setup

For using Kerberos, a user account must created for the B2B Portal. That user account must be mapped to a so-called *Service Principal Name (SPN)*. Using the SPN, Web Browsers accessing B2B Portal resolve a cryptographic key that is used to transport the user identity securely to B2B Portal. The SPN must be based on the fully qualified Domain Name System (DNS) name of the B2B Portal server in the following form.
HTTP/fully.qualified.host.name@REALM-NAME

- *HTTP* is the protocol, which stays the same even if HTTP over SSL (HTTPS) is used.
- *fully.qualified.host.name* is the host name including DNS Domain Name of the B2B Portal Server. It must match the *a* record of the server in DNS.

- *REALM-NAME i*s the name of the Kerberos Realm (or Windows 2000+ Domain Name) in upper-case.

This section contains examples where B2B Portal is installed on a server with the host name *b2bportal01.example.com*. Users will access this server with their Web browsers by using an alias name, http://*portal.example.com* (*CNAME* record in DNS). The Windows domain respective Kerberos Realm name used in the examples is *EXAMPLE.COM*.

8.2.2.1 Windows Domain Setup

In a Windows domain, a user account must be created in Active Directory for the B2B Portal. Then, a *Service Principal Name* (SPN) must be assigned to the account using a tool that is available on the Domain Controller (*setspn.exe*). The following tasks must be conducted by a person with domain administrator rights, usually one from the IT department:

1. Create a new user account in the *Active Directory.*
   - *Login name* is *portal* in this example.
   - *Account/Password never expires* should be checked.
   - Use a secure password, this user account can technically be used for logging into workstations.
2. Create the SPN mapping. In this example, users will access the server with the URL *http://portal.example.com*, but the real host name is *b2bportal01.example.com*.

   ```
   C:\>setspn -a http/b2bportal01.example.com portal
   Registering ServicePrincipalNames for CN=portal,CN=Users,DC=example,DC=com
           http/b2bportal01.example.com
   Updated object
   ```

   Please note that the protocol part of the Service Principal Name must be in *all lower case*!
3. Verify that *b2bportal01.example.com* is an a record in the DNS, and that *portal.example.com* is a *CNAME* record referring to *b2bportal01*.
4. The domain administrator must now communicate the name and password of the server account. The domain administrator must also communicate the name of the Windows domain and the host name(s) of the Domain Controller(s).

How this information will be used on the B2B Portal server is described in the next section.

Known Issues:

- *Windows Server 2008*: The service principal mapping is incorrect, see *KB951191* for a hot fix.

8.2.2.2 Unix/Linux Kerberos Setup

With Kerberos under Unix/Linux, a Service Principal Name (SPN) is created directly. For added security, the SPN will be assigned a random password which is written into a so-called *keytab* file. A person with Kerberos administrator rights must conduct the following steps:

1. Create a service principal:

   ```
   # kadmin
   > addprinc -randkey HTTP/b2bportal01.example.com
   > ktadd -k .keytab HTTP/b2bportal01.example.com
   ```
2. This creates a file *.keytab* in the current working directory. The administrator must send both this file and communicate the Kerberos Realm name and the host name(s) of all relevant KDC server(s).
3. Verify that *b2bportal01.example.com* is an a record in the DNS and that *portal.example.com* is a *CNAME* record referring to *b2bportal01*.

How this information will be used on the B2B Portal server is described in the next section.

8.2.3 B2B Portal Server Setup

The following steps must be conducted on the B2B Portal server.

8.2.3.1 General Kerberos Setup

For Kerberos to work with *Java*-based software, a file *%WINDIR%\krb5.ini* (Windows) or */etc/krb5.conf* (Unix/Linux) is required. This file must contain the name of the Windows domain or Kerberos Realm and the KDC servers.

The file must be created if it does not already exist:

```
[realms]
EXAMPLE.COM = {
    kdc = kerberos01.example.com
}
```

8.2.3.2 Keytab Setup

Next, the B2B Portal requires the user name and password of the user account, or the service principal name in the form of a *keytab* file.

- Within a Windows domain, the *keytab* file must be created on the B2B Portal Server using Java tools:

  ```
  [PORTAL_HOME]>runtime\jvm\bin\ktab.exe -k conf\keys\.keytab -a portal@EXAMPLE.COM
  Password for portal@EXAMPLE.COM: <password of user account>
  Done!
  Service key for portal@EXAMPLE.COM is saved in conf\keys\.keytab
  ```

- With Unix/Linux, the file was already created by the administrator, and can be copied to *[PORTAL_HOME]/conf/keys/.keytab*.

The keytab file should now be checked using the *Java* tools bundled with the B2B Portal. This ensures that there is no error that prevents using the keytab file in B2B Portal later on.

The command under Windows is as follows:

```
[PORTAL_HOME]>runtime\jvm\bin\kinit.exe -k -t conf\keys\.keytab portal@EXAMPLE.COM
New ticket is stored in cache file ...
```

The command under Unix/Linux is as follows:

```
[PORTAL_HOME]# runtime/jvm/bin/kinit -k -t conf/keys/.keytab HTTP/
b2bportal01.example.com@EXAMPLE.COM
```

8.2.3.3 B2B Portal Setup

1. Shut down B2B Portal.
2. The file domain.xml in *[PORTAL_HOME]/software/deployer/domain/pieces* must be extended with the following code. Add the code next to the definition of the security domain for *BIS*. Replace *portal@EXAMPLE.COM* with the principal used in your environment.

```
<security-domain name="krb5sso" cache-type="default">
    <authentication>
        <login-module code="Kerberos" flag="required">
            <module-option name="refreshKrb5Config" value="true" />
            <module-option name="principal" value="
                        portal@EXAMPLE.COM
                    " />
            <module-option name="doNotPrompt" value="true" />
            <module-option name="storeKey" value="true" />
            <module-option name="useKeyTab" value="true" />
            <module-option name="keyTab" value="@bisas.conf@/keys/.keytab" />
        </login-module>
    </authentication>
</security-domain>
```

3. You might need to have the unlimited JCE policy activated if you need AES 256bit encryption. Check the installation procedure for details.
4. Execute the appropriate script *[PORTAL_HOME]/software/register.bat* or *[PORTAL_HOME]/software/register.sh*.
5. Start the B2B Portal.
6. In the *Administration*, set the *Global Parameter LOGIN_MODULES* as follows:

```
com.seeburger.smarti.core.login.credentials.KerberosModule,
com.seeburger.smarti.core.login.credentials.LoginnamePasswordModule
```

7. You may want to configure the *SSO_** parameters that control if and how new B2B Portal users are created upon their first successful authentication.

The server-side setup is now finished.

8.2.3.4 B2B Portal Users

B2B Portal users are mapped to Kerberos users via the login name. The format of the login name is Username@REALM-NAME. By default, a new user account is created automatically when the Kerberos authenticated user accesses B2B Portal for the first time.

Please note that in B2B Portal the login names are restricted to 50 characters.

8.2.4 Client Web Browser Setup

Users must use the fully qualified domain name to access the B2B Portal, like *http://portal.example.com/* (*http://portal/* will not work)*.* The user sitting in front of the client computer must be signed on at the Kerberos Server. With a Windows domain, this happens automatically when the user logs in at the Windows domain. Please note that Kerberos requires special support in the Web browser, and not all available browsers offer this feature (Opera currently does not, for example).

8.2.4.1 Internet Explorer

- *Windows Integrated Authentication* must be enabled (this is the default).
- The B2B Portal server must be added to the *Local Intranet* zone if this is not automatically detected.
- The zone policy must allow *Automatic Logon* (default for the *Local Intranet* and *Trusted Sites* zones).

More information can be found on this website:
http://msdn.microsoft.com/en-us/library/ms995329.aspx

8.2.4.2 Firefox

Open the URL *about:config* and add your domain to the list of trusted sites for Kerberos authentication (comma-separated list):

```
network.negotiate-auth.trusted-uris = .example.com
```

8.2.5 Troubleshooting

Kerberos is a complex protocol with many possible error sources. The following is a list of common error messages and their meanings:

Error Message	Meaning
KrbException: Cannot get kdc for realm EXAMPLE	*%WINDIR%\krb5.ini* or */etc/krb5.conf* on the B2B Portal server is missing or information about the realm is missing in that file.
Failure unspecified at GSS-API level (Mechanism level: Checksum failed).	The service account has been changed, but the client browser still uses the old key (try *kinit purge*).
Defective token detected (Mechanism level: GSSHeader did not find the right tag).	NTLM authentication was used instead of Kerberos - either the web browser does not support Kerberos, or Kerberos has been disabled, or the Kerberos service principal of the B2B Portal server is invalid.
Mechanism level: Invalid argument (400) - Cannot find the key of the appropriate type to decrypt AP REP - ...	The *.keytab* file does not contain a key for the negotiated encryption type. Create a new *.keytab* file that contains keys for all supported crypto algorithms.
Encryption type ... ... mode with ... is not supported/ enabled.	Some stronger encryption types require the *JCE Unlimited Strength Policy* being installed into the Java VM.
Client not found in Kerberos database (6) - CLIENT_NOT_FOUND	The client machine or the authenticated user belongs to a different Kerberos realm/domain than the server.
Pre-authentication information was invalid (24).	The service account has been changed. Create a new *.keytab* file.
Unable to obtain principal name for authentication.	Either no *.keytab* file has been installed or the service principal has changed and the *[PORTAL_HOME]/ software/register* script was not run.
Unable to obtain password from user.	• The entry for the principal in the *[PORTAL_HOME]/software/deployer/domain/pieces/domain.xml* is wrong • The service principal has changed and the *[PORTAL_HOME]/ software/register* script was not run.
Mechanism level: Specified version of key is not available (44)	The KVNO value in the Keytab file does not match the KVNO value stored on the Kerberos server. This error only happens when *ktab.exe* is used and the Java Runtime has been upgraded to a newer version than the one bundled with B2B Portal. The KVNO value in the Keytab file can be changed using *ktab.exe* with the same principal name and the additional parameter *-n <KVNO>*. The correct KVNO is stored in Active Directory in the attribute *msDS-KeyVersionNumber* of the service user. You can also try to use the value 0 for the KVNO as a match for any value.

8.3 Managing SSL Certificates

For running B2B Portal in SSL mode, an SSL private encryption key, and a certificate are needed. During installation, an encryption key and a self-signed certificate are generated, but the latter must be forwarded to a Certification Authority for signing, and then be imported again before it is fully usable.

⚠ **Warning:** Self-signed certificates are not suitable for production use. Self-signed certificates provide no host authentication to users and thus enable man-in-the-middle attacks. Some browsers reject communicating with servers that do not have a certificate from a trusted Certification Authority installed.

Note: SSL Certificate management currently requires using the Java™ Platform tools on a command line. The working directory is expected to be the installation destination directory.

Configuring SSL protocol versions and cipher suits

In order to configure protocol versions and associated cipher suits, the portal.xml file should be modified - {Portal}/software/deployer/domain/pieces/role-merge/portal.xml.

1. Stop the instance

2. In subsystem "urn:jboss:domain:web:1.1", find connectors "https" and "rest" and modify the ssl attributes "protocol" and "cypher-suit"

3. Execute register and start the instance again.

After upgrade this protocol and cypher suits will be overwritten by the default provided ones. In order to avoid this, an xml snippet containing the changes should be placed in {Portal}software/deployer/domain/pieces/user-config folder. It will remain after an upgrade.

By default, the following protocols : TLSv1.1, TLSv1.2

and cypher suits :

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,

TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA,

TLS_EMPTY_RENEGOTIATION_INFO_SCSV, TLS_FALLBACK_SCSV are provided.

Forwarding a Self-signed Certificate to a Certification Authority

In order to become accepted by browsers, a self-signed certificate must be sent to a trusted Certification Authority for signing. For the following steps, please ensure that the current working directory is the installation destination directory.

1. Execute

   ```
   runtime/jvm/bin/keytool -certreq -alias central -keystore conf/keys/.keystore -storepass
    seeburger -file central.csr
   ```

2. A Certificate Signing Request (CSR) is stored as file *central.csr*, which must be forwarded to the Certification Authority (CA)

Forwarding the CSR to the CA is either done by pasting the contents of *central.csr* into a web form, or by sending the file per e-mail. The CA will send back a signed certificate.

Importing a Signed Certificate from a Certification Authority

After signing, the Certificate Authority returns a valid certificate that must be imported. This process needs to be repeated from time to time, since all certificates have an expiration date and Certification Authorities issue new signed certificate at regular intervals. For the following steps, please ensure that the current working directory is the installation destination directory.

1. Save the signed certificate from the Certification Authority (CA) as file *central.crt*
2. Execute

   ```
   runtime/jvm/bin/keytool -import -alias central -keystore conf/keys/.keystore -storepass
    seeburger -file central.crt
   ```

3. Restart B2B Portal to activate the new certificate.

Possible problems:

Problem	Description
keytool error: java.lang.Exception: Public keys in reply and keystore don't match	The certificate that is to be imported does not fit to the encryption key on the system. Probably a certificate was tried to be imported that was intended for a different system.

Keytool error: java.lang.Exception: Failed to establish chain from reply	The Certification Authority is not in the list of trusted Certification Authorities. Having the CA's certificate in the file *ca.crt,* it can be imported by executing:
	`runtime/jvm/bin/keytool -import -alias ca -keystore conf/`
	`keys/.keystore -storepass seeburger`
	`-file ca.crt`

Keytool error: java.io.IOException: Invalid keystore format	The JavaKeytool offers different options for importing certificates of different format. For details please refer to the documentation of the Java Keytools provided with Java. In case the format of the certificate is not supported, OpenSSL (http://www.openssl.org/) might help.
After having successfully imported a signed certificate, when accessing the system using SSL the web browser displays a security warning or rejects the connection	This typically happens if either the certificate is expired, or the certificate host name is incorrect. • *If the certificate is expired*, the Certification Authority needs to issue a new signed certificate which must then be imported. • *If the host name doesn't match*, a new self-signed certificate needs to be created. Please contact SEEBURGER support in that case. The host name must be the publicly visible fully-qualified host name of the system, and this name must be used for accessing the system with the web browser. A certificate can only contain one host name.

Create a new Private Key

During installation, each B2B Portal is given its own Private Key. The confidentiality of this key is mandatory to keep the data transmission secure. In very rare cases, it is necessary to replace the key created during installation with a new one, like:

- The Private Key has been stolen or published accidently
- The Private Key has become too weak, i.e. does not match the current security requirements any more

Warning: a Signed Certificate is always bound to one specific Private Key. When changing the key, the Signed Certificate immediately becomes non-usable. Please always contact your Certification Authority to have any Signed Certificates revoked which you are not using any more.

For the following steps, please ensure that the current working directory is the installation destination directory.

1. Delete or rename the file *conf/keys/.keystore*
2. Execute:

   ```
   runtime/jvm/bin/keytool -genkeypair -alias central -keystore conf/keys/.keystore -
   storepass seeburger -keysize 2048 -keyalg RSA -validity 365 -dname "CN=www.example.com"
   ```

   (replace www.example.com with the real public host name)
3. Restart B2B Portal to activate the new key.

Note: At this point, all users will see a certificate warning until the next steps have been completed.

4. Follow the steps Forwarding a Self-signed Certificate to a Certification Authority (page 51) and Importing a Signed Certificate from a Certification Authority (page 53) .

Importing a Signed Certificate and the private key from an PFX file

In case the customer provides a key and signed certificat as pfx file, both must be imported using the following command. Please use the correct file name for the input file.

1. Delete or rename the file *conf/keys/.keystore*
2. Execute:

```
runtime/jvm/bin/keytool -importkeystore -srckeystore mypfxfile.pfx -srcstoretype
 pkcs12 -srcstorepass mypfxpass -destkeystore conf/keys/.keystore -deststoretype JKS -
deststorepass seeburger()
```

(replace mypfxfile.pfx with the real file name and mypfxpass with the password for this file)

1. Restart B2B Portal to activate the new key.

9 Update Instructions

9.1 Pre-Update Checklist

Verify System Integrity

Before you can start the update procedure it is important to check that the currently running system is in a functional state. Updating a system with partial or failed updates, inconsistent database schema or systems which do not start up is not supported. Especially test the following:

1. Run *diffDB* on the old system, no pending database modifications should be reported. If in doubt, involve SEEBURGER Customer Service to review the diffdb,log files. This can and should be done with some buffer before scheduling the actual update.
2. Make sure you can actually start the front-end and login.
3. Review machine logs for hardware errors and make sure all file systems have enough spare capacity.
4. Make sure all known instances are up and running and can be used (there should be no stale instance entry in the dashboard's landscape view)
5. Check the version of all instances. They have to be on the same service pack and hotfix level. You need to complete or revert a partial update before upgrading to a new version. Failed rolling updates need to be completed in offline mode.
6. Make sure external dependencies (database, BIS Secure Proxy Control Server, BIS FX, BIS B2B Portal (MT, TM), SIL, ...) are up and running

If any of those conditions are not met, you must repair the existing system before beginning an update or upgrade. This is especially true if you plan a rolling update on a productive system with no downtime window.

Installation Requirements also apply to Updates

It is important to check the pre-installation requirements of the new version. They might be different from the requirements for older releases. The system must be prepared with those new requirements in mind before starting the update procedure.

This especially includes Operating System version, system parameters as well as database minimum version (Oracle 11.2.0.4), database parameters, roles, profiles and object permissions.

You find those requirements in this **Release Notes** document, as well as topic specific manuals (**System Database manual**, **DT Adapter Master Guide**). Also review the section about manually updating the Oracle JDBC driver (page 121).

Java Runtime

For Linux and Windows SEEBURGER delivers an up-to-date version of the Java Virtual Machine (Java Server Runtime). However, for other operating systems (HP/UX, IBM AIX, Solaris) you need to manually provided an updated Installation. The JVM need to be unpacked to `<BIS_HOME>/runtime/jvm64` while the instance is shut down.

Version specific instructions can also be found on the SEEBURGER Service Desk in the Knowledge Base article 20141114-0406.

If you are using a JavaVM provided by SEEBURGER and need to upgrade, all processes that use this JavaVM should be stopped. Otherwise, the upgrade might fail. [**issue_b#63536**]

To check if there are running processes that use this JavaVM, the following commands might be helpful:

- For Linux: ps aux | grep "<PATH_TO_BIS_JAVA>" | grep -v "grep"
- For Windows: wmic process get ProcessID,description,executablepath | find "<PATH_TO_BIS_JAVA>"

Verify Symbolic Links

If you use symbolic links under Linux/Unix (for clustering or application of multiple file systems), ensure that all of them (below the installation directory) are **absolute** (not relative). If the links are relative (i.e. containing ".."), contact SEEBURGER Support because your file database must be fixed first! [issue_b #17428]

In order to list all symbolic links, use the following command (replacing *BIS6_HOME* with the applied installation directory):

```
$ find /BIS6_HOME/ -type l -ls
```

Verify File and Folder Permissions

Ensure you do not have permission problems in your installation. All files and directories must be owned by the **application owner** user. The file owner must have read and write permissions on all files and directories.

To display a list of all files that are **not** owned by the application user, enter the following command (replacing *BIS6_HOME* with the applied installation directory and *BISOWNER* with the actual Unix user name):

```
find /BIS6_HOME/ \! -user BISOWNER -ls
```

(If your *find* command does not support the *-ls* switch, try *gfind* or use *-print* | *xargs ls* instead).

For windows installations it is recommended the whole filesystem tree inherits permissions from the base installation folder. The application owner must have full permissions on this folder.

Reset Log Files

Before upgrading, it is recommended that the user backs up and deletes all logfiles. This is not mandatory but makes log file analysis much easier.

6.3.5	**6.5.2**
log/adapters	log/INSTANCE_ID/adapters
log/audit	log/INSTANCE_ID/audit
log/bic	log/INSTANCE_ID/bic

log/changerequests	log/INSTANCE_ID/changerequests
log/reorg	log/INSTANCE_ID/reorg

Automatic Upgrade of the Database

During an upgrade installation, changes between the current database structure and the new one will be detected automatically. This process is automatically called after the register step.

Upgrades using the patch mode will not allow you to review and manually execute the database modifications. If you have custom changes to your database or expect manual intervention it is recommended to use the update installation mode instead.

The update installation will provided you with several options if only valid changes have to be applied:

- *Deploy changes automatically* - it will automatically compensate all differences (no tables will be dropped though). [**recommended option**]
- *Generate SQL script for manual execution* - it will generate an SQL script to compensate the changes. The script has to be executed manually afterwards. Please see the **System Database manual** for details on how to execute this script (specifically you cannot use `sqlplus` with Oracle).

In case of Oracle Database, you must run script software/installdb/prepare-orace-runtimeuser.sql after applying the changes manually.

- *Check database after manual changes again* - it will compare the current database with the new required structure again.

Running the diffDB process will delete custom schema modifications (INDEX). Make sure to re-create those objects if needed.

Note: If you are using Oracle, please ensure that your user does not have a DBA role assigned during the automatic database upgrade.

Warning: If the BIS system being upgraded uses an older version of the Oracle database (e.g. Oracle 10g), it is necessary to change the instant client to a supported version in accordance with the requirements for Supported Systems in the *Release Notes*. The instant client must be replaced in the directory `<BIS_HOME>/runtime/instantclient` before the BIS upgrade procedure is started.
When the instant client is replaced with a newer version, it is a critical issue of the update procedure that no parts of the old instant client remain, and that the old client is replaced completely with the new one. See the *Oracle JDBC driver update* section.

Before you can update or patch an existing installation you should run the diffDB tool in `<BIS_HOME>/software/installdb/diffdb.{bat,sh}` and review the output in `<BIS_HOME>/log/install/diffdb.log`. This will compare your current database structure against the expected database structure of the (old) installed version. Upgrades from a specific version are only tested with the original database structure. If you made manual modifications or missed database schema updates in the past your version might not have the desired state and upgrades or patches should not be applied without contacting SEEBURGER support to review your differences.

Update from SP28 or earlier

During update/patch from a version SP28 and before there is an error on running DiffDB and update the table TSMT_PROFILEBOX.
Regarding [issue_b#69866] the old table need to be dropped and recreated or altered by with the following commands.

Oracle:

```
alter table TSMT_PROFILEBOX modify CPROFILEBOXTECHNICALNAME set default 'TO_DEFINE';
```

MSSql:

```
ALTER TABLE TSMT_PROFILEBOX
ALTER COLUMN CPROFILEBOXTECHNICALNAME SET DEFAULT 'TO_DEFINE'
```

9.2 Rolling Update

9.2.1 Overview

With BIS 6.5.2, you have a system where OS / hardware changes, software hotfixes, patches, service packs, version updates and solution deployments (including libraries) as well as module/article upgrades (i.e. new articles) can be installed without affecting the visible availability of the system.

In the following, we will concentrate on the use case where you want to apply a new software patch or update to BIS 6.5.2.

In a rolling update, one instance at a time is cleanly shut down, then patched and finally started up again. You should monitor your system at this point to ensure the updated instance is correctly working. It could make sense to check the log files produced by the updated instance for any unexpected warnings or errors. Then the next instance is brought down and updated until the whole system (each instance in your landscape) is running on the same software patch level.

SEEBURGER tests patches for BIS 6.5.2 for rolling update compliance. We usually try to provide only rolling update compliant patches. In the event that a patch is not rolling update compliant, it can’t be installed in the way described in this document. In this case, you have to shut down all instances in your BIS6 system and patch all of them before starting up again.

Note: Rolling updates are supported and tested for updates of versions, that are at most 10 service packs older than the version to update to.
This means you can and should update at least every 10 service packs.
If you want to update an older version using rolling update, you can still achieve a rolling update without affecting the visible availability of the system, but you need to take intermediate steps.
Example: Installed version is SP22 and you want to update to SP36. This is not directly supported, since the gap is larger than 10 SPs. To achieve a rolling update, you first need to update to the latest supported intermediate version. In this example, that would be SP32. After the whole system is updated to this intermediate version, you can continue to update to the final target version - SP36 in this example.
If the gap is even larger, you need to take several intermediate steps or consider updating during a downtime.
Note: SEEBURGER's recommendation though is to keep the system up-to-date in the defined version range of 10 SPs to avoid such situations upfront.

Note: Using the Rolling Upgrade mode allows to update the system without impacting the availability. However the procedure requires more preparation, takes longer and there is more risk involved since the steps need to be coordinated and tested. It is therefore recommended to use a traditional offline approach if you have a maintenance window.

9.2.2 Prerequisites for Installation Planning

In BIS 6.5.2, we have defined instances of different roles. One instance reflects one software home. You can have multiple installations on one machine. Most likely you will use different machines for performance and reliability reasons. One instance could belong to several roles.

There is the Admin Server role, which is primarily the backend of the GUI and also used as WebDAV server. WebDAV is an HTTP based protocol mainly used in BIS for storing payload which would be, by configuration, too big to directly store to the database. BIS 6.5.2 is limited to support only one active Admin Server instance.

To avoid breaking the processing of the BIS 6.5.2 environment when the Admin Server is shut down, you need to make sure your attachments are not stored in the Admin Server's WebDAV store. Instead you need to setup a shared filesystem or a dedicated WebDAV server for all DIAF pools. For information on how to install Apache HTTP and configure it as a WebDAV server in the BIS 6.5.2 environment, please refer to the Configuring Attachment Store (page 110) chapter.

While the Admin Server role is down, you cannot use your BIS FrontEnd to monitor the system.

There is also only one instance of role WLH (WorklistHandler) in your BIS 6.5.2 environment. We do not support more than one active WLH at a time. If you need high availability, install a cold standby. If you shut down this instance, all processes configured to use a WLH queue will be interrupted until this instance is restarted. SEEBURGER highly recommends limiting the scenarios where you make use of WLH queues. Most of the components (adapters), can be configured to use the new “direct queues” mode. A “direct queue” is not managed by the WLH instance and therefore is not affected by the absence of this instance. WLH queues are typically configured when you need queuing and you have to manage limited resources like ISDN channels. OFTP over ISDN is a candidate, while OFTP over TCP is not.

You have to ensure, that you always have enough remaining instances of type Process Engine or Adapter Engine in each instance group. If you take one out of service for applying new software the remaining capacity must be enough to process your workload.

In a minimum scenario, you would only install one instance that contains all roles to get a fully working environment. A minimum environment like that, would **NOT** work for the Rolling Update feature, because you do not have a second or third instance belonging to the same role(s) which would take over the load of the instance that is down for update. When you plan your BIS 6.5.2 infrastructure, you have to consider that you do not always have all instances available. So make it powerful enough to cope with your load in the event that you shut down one instance for a maintenance task like a software update.

Refer to the BIS *Concepts and Installation Planning* Book for more details about the BIS 6.5.2 system, landscape and instance roles and groups.

SEEBURGER highly recommends to setup a system for testing which is comparable to your production landscape. Please start to apply new software using the rolling update procedure on your testing environment. After verification that the whole testing environment was updated correctly, continue to update your production environment. Make sure the testing environment includes all special configurations (firewalls, cluster, monitoring, OS version) as well as a representative sample of the production processing and workload.

9.2.3 The Rolling-Update Process

⚠ Never stop the next instance in your landscape before the previous instance has fully started and you have checked that it is back in service.

⚠ Apply the update for all instances one after the other. After the update procedure is finished, all instances must have the same version.

You always begin with upgrading the instance that contains the Admin Server role, after that the following order should be applied:

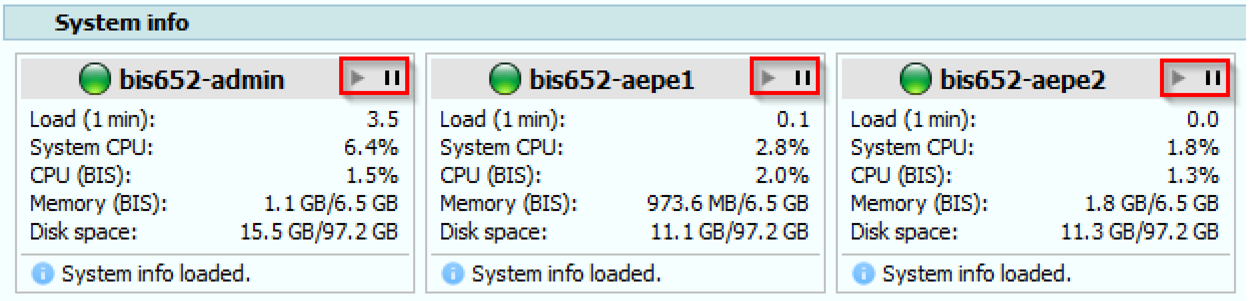
1. Datastore
2. Worklist Handler
3. SIL Backend
4. Adapter Engine
5. ProcessEngine
6. UserManagement
7. PortalEngine

If multiple roles are installed on an instance, the highest priority wins, so for example an instance with Adapter Engine and Process Engine should be updated before an instance with only Process Engine installed but after instances with only Adapter Engine installed.

9.2.3.1 Clean Shutdown

Do a clean shutdown to minimize the impact to the processing of other instances and the amount of recovery that may be necessary when an upgraded instance is back to work. A clean shutdown means that you stop the inflow of new orders / tasks to an instance, and that you wait until the processing of already associated tasks is finished.

In order to achieve this, the respective instance can be set into a draining mode. In that mode the instance will still fulfill all running orders / tasks but will not accept new incoming connections. Enabling the drain mode can be done in several ways.

- Enable drain mode via BIS GUI - Dashboard
  - In the Dashboard, check the *System info* dashlet, which contains play and pause buttons to enable (pause) or disable (play) the drain mode for that particular instance, see below screenshot
  - 

    System info

    bis652-admin

Load (1 min):	3.5
System CPU:	6.4%
CPU (BIS):	1.5%
Memory (BIS):	1.1 GB/6.5 GB
Disk space:	15.5 GB/97.2 GB

    System info loaded.

    bis652-aepe1

Load (1 min):	0.1
System CPU:	2.8%
CPU (BIS):	2.0%
Memory (BIS):	973.6 MB/6.5 GB
Disk space:	11.1 GB/97.2 GB

    System info loaded.

    bis652-aepe2

Load (1 min):	0.0
System CPU:	1.8%
CPU (BIS):	1.3%
Memory (BIS):	1.8 GB/6.5 GB
Disk space:	11.3 GB/97.2 GB

    System info loaded.
  - Monitor the state of the respective instance's dashlet until the instance is in state *Drained*. You can also monitor the *Landscape* dashlet, which should also expose the states *Draining* and *Drained* accordingly.
- Enable drain mode via commandline
  - Execute the script `BIS_HOME/bin/prepareShutdown.{bat,sh}` .
  - Check the draining state via `BIS_HOME/bin/drbis/checkServerStatus.{bat,sh}` - if the script returns "OK - Drained" the instance has finished all pending tasks
  - In order to cancel the draining mode, call `BIS_HOME/bin/prepareShutdown.{bat,sh} -cancel`.
- Enable drain mode via JMX
  - Visit the MBean `com.seeburger.landscape.impl.jmx:service=LandscapeManagement`
  - Execute the MBeans method `triggerInstanceDraining` with the respective instance id
  - In case you need to cancel the draining mode, there is also a method `cancelInstanceDraining`.

The drain mode changes the instance's state to Draining until no more pending tasks are running. You can check the progress also in the various components. I.e. in the adapter control center, *Drained* adapters will show the status message *Adapter is drained*.

After an instance is drained, it can be safely shutdown with the regular means.

9.2.4 Applying the software update

Before you start to execute the patch installer, consider the following:

⚠ **Warning**: All customized configuration changes made beyond the routine set-up should be documented and saved before installing any update, as the execution of the `register.{bat,sh}` script could result in the loss of those customized changes.

The software patch (installation media) must be available to the admin server machine. This will update the built-in SPM repository. All other instances will read the software packages via the Admin Server.

Start to patch the instance that contains the Admin Server role.

The following is the general procedure:

1. Stop processing of the instance (see clean shutdown above)
2. Wait until the instance state is *Drained*.
3. Shutdown your instance
4. Execute the installer with: `<installation media>/installer/<os>/setup.{exe,bin}` and use patch mode.
5. If you’re unsure about some questions asked by the installer, use the suggested defaults.
6. Restart the updated instance
7. Monitor the processing of this instance and review log files for critical errors

Continue with the next instance in your system - repeat the steps. Never shut down more than one instance at a time.

On the Admin Server role the installer will also detect if a patch ships database schema modifications. In this case it will run the *diffDB* command to apply those changes. This means the database schema is upgraded as the first step in a rolling update. You may not proceed before this step has succeeded.

With a GUI upgrade, input fields of the property files that differ from the new default value are highlighted in yellow. It is recommended to adopt the new values and to make any changes.

If you have performed a silent or patch upgrade, please check the install.log in the <BISAS_HOME> / log / install folder for WARNING entries.

If there are entries such as e.g. "WARNING: Property vmoptions.SUN64 from vm.properties is changed by user! Can not set to default value. " , please check the specified properties in the corresponding files and adjust them if necessary. If these values have not been adjusted during a previous installation, please use the default value from the sample file. (E.g., sample.vm.properties).

Faulty and outdated properties can lead to an unstable system!

9.2.4.1 Hotfixes

Hotfixes must be applied in the same order as the updates are executed, starting with the instance containing the AdminServer role, followed by the other roles. Nevertheless SEEBURGER will only test service packs for rolling update compatibility. Hotfixes are usually included in the next service pack.

9.2.4.2 Limitations

- When doing a rolling update from a version prior to SP41, the Control Center statistics will not show any data as long as all AdapterEngine instances are not updated at least to SP41.
- When doing a rolling update from a version prior to SP41, the AdapterEngine instances will not recognize any master data change as long as all instances are not updated at least to SP41. The instances still work with master data, but they do not recognize any newly added, so you have to postpone any master data changes until the rolling update is finished.
- When doing a rolling update from a version prior to SP44, the SSL statistics MBean will no longer collect any data from the not yet updated instances.
- When creating new security profiles during the rolling update process using the master data, only ciphers for already updated instances are shown. This is only valid when updating from a version prior to SP38.

9.3 Updating existing BIS 6.3 installation

The following section describes things to consider before, while and after upgrading a BIS 6.3.5 Q3, Q4 (and limited available BIS 6.5.1 or 6.5.2 Q1) installation to BIS 6.5.2.

Follow the following procedure for an upgrade

- Review Limitations, Requirements and Manual steps in documentation
- Execute Pre-Update Checklist (page 54)
- Produce Backup/Snapshot of existing installation and database
- Shutdown all BIS 6.3 instances (no rolling updates supported)
- Use setup tool from installation media to update all instances (starting with the Admin Server). Make sure to start Admin Server after update.
- Execute Post-Update Checklist
- Start All instances

Major Changes to System Architecture when Upgrading from BIS 6.3.5 to BIS 6.5.2

Compared to BIS 6.3.5 Releases, there are some serious changes in the internal architecture of BIS 6.5.2 (e.g. HornetQ as JMS Provider)

Those changes might take effect on your system in regards to:

- Disaster Recovery
- Performance
- System Operations
- Custom Code / Development
- System Monitoring

Expected effects are:

- With BIS 6.5 the load on the system database caused by the JMS provider is lower, however on the Process Engine and Admin Server instances the new local JMS server increases I/O operations used.
- The Application Server used with BIS 6.5 starts 3 instead of one JVM

New Features compared to 6.3.5

Installing **multiple process engines** is a new license option for BIS 6.5.2. It allows to run multiple process engines in a active-active mode. This also allows to patch the system while it is partially online (Rolling Upgrades). In order to better support this new system landscape "Server" (CI) and "Node" (DI) is renamed to "Instances" with multiple roles. The former Node is now an Instance with the role "Adapter Engine" and the former server is now split in one Instance with the role "Admin Server" and multiple instances of role "Process Engine". For more information on possible combinations and further roles (and especially for planning a installation which can be upgraded online) see the new **Concepts and Planning** manual.

The BIS 6.5 releases are based on an updated **Application Server** version. This introduces some changes to the file layout (directories modules/ and domain/. This also means a BIS instance consists now of 3 Java processes, the Process Controller is the Parent for one HostController and One Application Server. This is the typical JBoss AS 7.1.1 "domain mode". However this combination is repeated for every instance (i.e. there is no Domain spanning multiple instances and no Domain Master for all). This might affect your system monitoring or operation toolings.

In order to support an active/active installation the **Scheduler** has been enhanced with cluster support. All instances in a system run their own schedulers. A scheduler task can be run independent on each instance ("Each Mode") or as a Task coordinated in the cluster. In later case all potential Schedulers will agree for each Job execution where the Job will be executed. In order to allow better monitoring in a distributed environment all Job executions are logged to a history table and can be inspected. All tasks have a new field which controls for which subset of instances they are valid (the instance selector). After an upgrade all tasks are automatically upgraded to the new layout. For user tasks you might need to pick the mode and selector the next time you want to save the tasks. Internally we moved to a new scheduling engine, the most visible change to this is that the many scheduler threads which existed before have been replaced with a smaller worker pool.

Since there is no longer the concept of a central instance/server (CI) which can be used at runtime for resources which should be maintained in a single instance there is a new component called the **resource repository**. This is used to replace the existing webdav based repository. The resource repository stores reports, scripts, user libraries (for script executor, adapters as well as XPath extensions), mappings and the TPM schema. You can use the software/bisadm-resrepo.{bat,sh} tool for listing and changing this repository. The content is stored in the database, versioned and distributed in the BIS system.

In order to support **Rolling Updates** the hotfix installer have been enhanced to be able to check Hotfixed and Patch Bundles if they can actually be applied while other instances are still running. This is called the "Online" mode. By default the hotfix installer assumes you are in Online mode (i.e. the current instance you want to patch is shut down, all other instances are running). If the hotfix installer tells you a patch bundle cant be applied (because it does not support online installation), you have to shut down all instances in a BIS system and then invoke the installer with the `--offline` option.

The following is a changes of more (visible) changes in the system core:

- In the Frontend some menus are restructured. A new Service Interface view is introduced (used for Process and Web Service Gateway Ports). The Worklist Handler Tab is renamed to Queueing, since some operations like Direct Mode or Batch Queues no longer need any Worklist Handler.
- Batch Queues (for aggregating message content over time) does no longer require a Worklist Handler. The Batch queue is stored in database and all process engine instances can queue and dequeue orders for batch queues. There are new database tables for Batch Queues and orders, existing forms will be automatically adjusted. The batched orders are stored in tBatchOrders of data source DS_RT.
- Direct mode orders are now retried dependent on the "retry-able" element in the fault. Up to now each direct mode order was retried dependent on the retry configuration and has ignored the "retryable" element. This has changed with this version. Now we have the same behaviour as in WLH mode.
  You may face here a different behavior in your process execution compared to one of the previous releases.
- HTTP listeners can now be configured to provide basic authentication. The authentication is handled based on user/password, LDAP or portal. See Master Adapter Configuration Guide for more details.

- Transaction monitor does no longer create a statistics on each filter request. Instead you can select whether you want to calculate the statistics or not. Not calculating the statistics speeds up the performance of the monitor.
- There is no longer the need to define the direct queue name with prefix "queue/" in the destination part of the business process.
  Instead of "async:queue/MyQueue" you can use "async:MyQueue"
- Direct mode queues are now created automatically, if they do not exist. This is the same behavior as in Worklisthandler mode. When defining any queue name in the destination part of the business process, the queue is now created automatically. For using the new queue you still have to assign it to a running node.
- The Node adapter user-configuration is no longer stored on the file system. Instead it is stored in the database as it is already done on the CI.
  During an upgrade, the config files are automatically imported to the DB.
  To change the adapter user-config, use the Control Center or call software/export-config script on any instance you like. The user-config files are then exported to directories separated by instanceID.
- If you use export/import-config on the Admin Server the configuration specific to all nodes are exported to different directories. This allows you to centrally change the configuration for all instances.
- BIS 6.5.2 has a number of logical datasources which can point to the same or different database schemas, depending on the instances installed. This allows for additional scalability. Logical Datasources and Database Accounts are managed (besides the initial setting in database.properties) via the BIS Frontend.
- On startup of a BIS instance, it will check existence of the file `conf/state/safemode.flag`. If this file is present the autostart setting for the adapters is ignored. Also processing of Process Engine queues will not be started. This can be used in upgrade scenarios to test an instance in maintenance mode. If you delete the file while an instance is running it will detect the change within a few seconds and resume normal operation. This removes the need for switching autostart off before an upgrade and turning it on later on.

The following changes affect adapters and components:

- The Mail and HTTP adapter are no longer installed per default on all adapter engines. Before, these adapters were installed on any "node" (i.e. adapter engines). You can now select for each instance of role adapter engine what adapters will be installed. For the Admin Server role some management adapters (HTTP, Mail Client) will be installed by default, they are not used in any business process. They are available for the Mail alert and the CRL Update.
- During setup of an Adapter Engine there is no default http listener created. To use any HTTP controller based adapter you first have to create now some HTTP listener using the system configuration menu in BIS Frontend.
- JCo based adapters (IDoc Client / Controller and RFC Client / Controller) now provide JCo traces in a separate file. For more information refer to JCOTracePath user configuration the adapter documentation.
- All JCo based adapters (including BAPI Converter) now use SAP JCo 3 library, see **Upgrade Instructions** for details.
- ScriptExecutor now only returns a logging attachment if the script did log something by default. The behavior can be changed by setting ScriptExecutor's configuration key "loggingMode" to either ALWAYS, NEVER or AUTO, where AUTO represents the default behavior. (6.5.1)
- Adapter specific log files are now moved from log/adapters to log/<InstanceId>/adapters/<AdapterId> directory. Each adapter now has its own subdirectory within the adapters directory. Also the log files are renamed. They now contain the instanceID in their name.
- ProcessInfo log files are no longer created. All information are written now to the adapter log file. The ProcessInfo trace is reformatted. All information are now written to a single line.
- S/MIME adapter is no longer deployed with default autostart enabled. The autostart of all adapters have to be enabled in the control center.

Solution Deployment:

For using SEEBURGER Standard Solutions or Custom Solutions the installation and update process has changed. Solutions can be shipped by SEEBURGER as hotfix files and they are no longer deployed by the setup program. This is done in order to allow a release cycle independent from the BIS installation media and to allow to install various solutions into different logical systems.

Some solutions require a configured datasource to access the message tracking database. This datasource needs to be named *SmartiDS*. There already is a pre-configured datasource named *BISMTImport*. This datasource is pre-configured to access the database defined during setup. To let solutions that need access to the message tracking database run, a new datasource *SmartiDS* needs to be created, which can be a copy of the existing *BISMTImport* datasource.

Database Schema Modifications

It is generally good practice to run the diffDB schema comparison with the old software installation before starting the update. The reason for this is, that updates are only tested against the actual desired database layout and your installation might have left-overs from earlier versions. Make sure there are no pending changes and allow SEEBURGER Customer Support to review pending chnages well ahead of the update schedule.

Denied IMAGE -> VARBINARY Changes for MS SQL Server and older schema

The database update will not automatically modify the type of IMAGE columns into the VARBINARY(max) format which is used on SQL Server. You can find those ALTER TABLE statements in the `log/install/intermediate-processed-denied.sql` script after you applied the acceptable changes from the setup.

In the diffDB logfiles you will see entries like:

```
    Name of table    : tTable
    Fields changed   : quantity = 1
                       cColumn (image(-1), null) -> (varbinary(-1), null)
```

And in the intermediate-processed-denied.sql the proposed statement looks like (depending on table name, column name and if the column is nullable):

```
  ALTER TABLE tTable ALTER COLUMN cColumn varbinary (max)  NULL;
```

You can execute those statements manually, but keep in mind depending on the size of existing data this can take a long time and takes a lot of log space to complete. If you have such old/big schema it is better to start with a fresh installation and a clean database or re-create the affected tables. If you do not apply the changes BIS will continue to function (but future database updates might require you to switch).

Components Not Yet Available

- EBICS Server Adapter (introduced with 6.3.5 Q4) is not available on BIS 6.5.2.

Removed and Replaced Functionality

- The stand-alone WebStart Application "RemoteEditor" is not available with this version anymore. (Inside the BIS Front-End you can use the remote utilities to view files, edit files and inspect logfiles. Only the stand-alone URL which was used by external tools like the message tracker is currently not available.
- With 6.5.2 Q1 the DMZ security (SSH tunnel) is removed from the installation. There is no more the option to tunnel all the connections between Instances. One option to secure network connections is to use the **BIS Secure Proxy** as an reverse proxy. The Adapter Engines no longer need to be exposed on the DMZ in that case
- The *DMZ (file) encryption* is still supported. So the option to encrypt all the file on the DMZ instance can still be used. The DMZ encryption can still be configured using the user-configuration file. But there is no

more option to enable the DMZ encryption during setup time. Instead you have to install the BIS without the encryption and then later change it in the user-configuration. See chapter **DMZ Encryption** in the ***Master Adapter Configuration Guide*** .

- It is no longer possible to provide the logical system on a system listener via the request uri.
- Up to 6.5.1 Q1 it was possible to use for example /SeeburgerHTTP/HTTPController/333 to define the logical system. Now you have to create a new listener on the logical system or use the ?ls=333 param.
- The SOAP, AS1, AS3 adapters and the Web Service Gateway v1.0 are not available anymore in 6.5.2 Q1. All WebService functionality is provided by the new Web Service Gateway article.
- The *BIC Sequence Checker* component that has been supported for legacy reasons up to BIS 6.3.5 has been discontinued in BIS 6.5.1.
- Application Center link is removed from the portal web page. To start and stop the adapter you now have to use the Control Center from BIS Front-end.
- DrBIS: Some of the command line scripts for Windows and Unix systems no longer work with this version of BIS due to the changed (JMS) server architecture and infrastructure. A list of the non-working cmd/sh scripts follows:
  - Dump Blob Content (dumpBlobs.cmd/.sh)

```
dumpBlobs.cmd/sh -t tJMSMessages -col cMessageBlob -d SeeAS_User -sql "cMessageId=0"
```

- The following Nagios scripts also not work with this version [issue_b#46343]:
  - queryDB_Check_DLQ.sh
  - queryDB_JMS_ENGINE_QUEUES.sh
  - queryDB_JMS_QUEUE_DYN.sh
  - queryDB_JMS_TOTAL_QUEUES.sh
  - queryJMX_ACTIVE_THREAD_COUNT.sh
  - queryJMX_FREE_CONNECTION_POOL.sh
  - queryJMX_FREE_MEMORY.sh
  - queryJMX_WAITING_THREAD_COUNT.sh

Requires Manual Action/Reconfiguration

- The Recovery Timer configuration in the System settings of the master data is removed. The recovery timers now have to be managed by the scheduler configuration.

  See chapter **Recovery Timer** in the **Master Adapter Configuration Guide** for details about the configuration. Existing timers will no longer work and will be replaced by a new default timer in the scheduler configuration. In upgrade case you have to migrate your existing configurations then to new scheduler tasks.
- The Adapter Error/Warning/Recovery *alert monitor* no longer provides the option for aggregated events over all instances. Up to now, there was a configuration to monitor the events in an aggregated way.
  So the alert was triggered when the rule has matched on the adapter-aggregated events. The ALL ADAPTERS option no longer works in aggregation mode. Instead, the alert is triggered in case one of the installed adapters exceeds the configured limit. See the alerting documentation for details about the alert monitors.
- With the *AS2 Adapter* it is no longer possible to specify a map defining the default Content Transfer Encoding for a specific partner in the user configuration. The field Content Transfer Encoding available in the AS2 Partner Address master data must be used instead.
- FTP Controller has no longer a custom message languages user configuration property. The messages are searched in the classpath in a corresponding properties file (FTPStatus_"language".properties) to each specified language. This is done by the (Apache) FTP Server component on startup.
- The unsupported `pathInfo` field in the HTTP Controllers server info element of the request message is no longer filled. Use instead the `requestUri` which is always the same from release to release.

- Due to changes to the internal message parsing (JAXB) the validation of Process Messages is stricter in some cases, see Update Instructions for details.
- When upgrading from 6.5.2 Q1 or Q2 and you added an explicit configuration for discovery of instances (e.g. hazelcast-bis.xml), then this is not necessary anymore and in fact will be ignored and a warning in the log will get issued. Connections are now built-up automatically point-to-point, which resolves issues with routers not being capable of or configured for routing multicast messages.
- When updating from BIS 6.3.5Qx version you have to call `software/keystore-upgrade` script right after the upgrade to fix the MLLP master data. Otherwise, your MLLP master data will not be visible in the Front-end. Your business processes will still work, but you are not able to change the master data.
- Reorganization configurations after upgrade from 6.3.4 Q1
  In cases of sequential upgrades from version 6.3.3 Qx to version 6.3.4 Q1 and then to 6.3.5 Q1 and later, it is possible that old reorganization configurations had remained in the Database. These are usually QueryReorganizations like *"ReorgMonitorError"* and *"ReorgMonitorWarning"*.
  The effect is that upon triggering of those reorganizations from the corresponding scheduler task, a warning is given, saying:
  [QueryReorganisation#reorg] WARNING: .... Will try to connect to 'WorkflowDS'..

  What to do to get rid of this warning:

  1. Open the JMX console and scroll down to com.seeburger.reorg.jmx
  2. Open every listed reorganization and replace "java:/WORKFLOWDB" with "WorkflowDS" where seen for field DataSource.
- BIC Jasper Reports Processor: Font extension JAR files created with iReport (or other tools) that under BIS 6.3.5 needed to be placed manually in directories `${BISROOT}/jboss/SeeBisAs/lib/ext/`, `${BISROOT}/lib/ext/`, `${NODEROOT}/shared/lib/` and `${NODEROOT}/software/lib/ext/` now need to be placed in BIS Server and Node directory: `${BISROOT}/lib/font_extensions/` At run-time, the fonts in the JAR will be loaded from there and embedded in the PDF document. The directory does not exist at BIS install time and needs to be created manually
- B2B Portal Message Search: The location and structure of the index files has changed. The files are now in `${bisas.data}/msgsearch/<clientid>` instead of `${bisas.data}/msgsearch/local/<clientid>`. The directory `${bisas.data}/msgsearch/shared` is obsolete. The index must be moved during update. There should be no (write) access to the index while it is moved to the new location or while a backup is made. Otherwise, the copy of the index could get corrupted with a message like "`com.seeburger.smarti.job.JobException: java.io.FileNotFoundException: D:\BIS_Insight\BIS_Portal_QA\data\msgsearch\1\segments_a6 (No such file or directory)`".
- B2B Portal Message Search: In case of an update from Version 6.3.5 Q3 or 6.3.5 Q4, the table tMsgSearch_ICMonitoring must be deleted. [issue_b#67586]
- Make sure to read the installation instructions on the JCE Policy files as the mechanism has changed in BIS 6.5.2 SP52.

Move Third party artifacts

When you are using third party artifacts like some JMS providers, VCOM or any special DB driver, then these jars are not automatically migrated to the new BIS version. You have to copy them manually each to a separated directory in software/external directory and delete the old version from lib/ext. Check the adapters manual for details about which file you have to copy to which directory.

SAP JCo-based adapters like IDoc Client/Controller and RFC Client/Controller are not affected, as the existing libraries are moved by the setup to the new, correct location. **Nonetheless it may be needed to update SAP JCo to a more current version than the one used in older BIS versions.** Refer to the "Installation" chapter of the respective adapter manual.

If you do not copy these files manually the adapters like JMS, VCOM, DB Client or DB Controller may no longer work as expected

SAP JCo 3 Update (IDoc Adapter 2010B6, BAPI Converter 3080B6)

The IDoc Adapter now uses SAP Java Connector 3 (SAP JCo 3) for communicating with SAP systems. At least version **3.0.9** of SAP JCo is needed. Older versions of SAP JCo 3 and of course SAP JCo 2 are not supported.

The memory usage of the JCo3-based IDoc connector has changed. Therefore the Java Heap Space settings have to be adapted to the new memory usage.

The general rule that the sizing of the BIS installation for certain IDoc record sizes depends both on the Java Heap Space and the Native Heap Space is no longer valid.

Furthermore, SAP JCo 3 now allocates all needed memory for both the Java and the native libraries **inside** the Java Heap Space of the Java Virtual Machine. This makes the sizing in general easier, as the Native Heap Space is no longer required for the calculation.

Now the simple rule applies: The more IDoc records there are to be processed, the more Java Heap Space has to be available.

For receiving IDocs from SAP (direction SAP outbound) the required memory decreased. Unicode IDocs need 25%, non-Unicode IDocs 40%, less than SAP JCo2.

For sending IDocs to SAP (direction SAP inbound) there is no significant change between SAP JCo 2 and SAP JCo 3. The sending of Unicode IDocs with SAP JCo 3 needs about 5% more memory, and the sending of non-Unicode IDocs needs 5% less than SAP JCo 2 did.

Please refer to the memory sizing chapter in the **IDoc Connector manual**.

The IDoc Client memory pooling also uses different default values. It may be necessary to review those settings, if the pooling has been customized before.

If data is received from SAP (direction SAP outbound) and the connected SAP system has a Unicode kernel, the default code page used by SAP JCo 3 is UTF-16. This means that, e.g. received IDoc files are sent to BIS 6 with the code page UTF-16. These files contain a Byte Order Mark (BOM) which indicates the used byte order. These characters may cause problems in post-processing of such IDoc files, e.g. when a BIC mapping with a hard-coded encoding is used. Check article ID [**13884**] on the *SEEBURGER Knowledge Base* (https://servicedesk.seeburger.de).

The *CPIC_MAXCONV* environment setting has been moved from an environment variable to a Java system property. The new default value is 204. If a different value has been used, it is necessary to adjust the system property *jco.cpic_maxconv* during upgrade installation.

TLS/SSL

When upgrading from an older Java runtime (Java 6/7 to Java 8) there might be some changes to default algorithms, minimum key sizes and enabled cipher suites. This can affect the ability to communicate with some partners via TLS/SSL, especially if they have older software which has only a limited feature set. Generally we follow the defaults of the Java runtime installed as an industry best practice. But you can configure the settings to be more strict or more relaxed. In all cases you should test key partners before configuring the new policy.

Instance IDs must be unique

The instance IDs of all instances in a BIS system (with the same systemID) need to be unique.
In case you have an existing B2B Portal installation with an overlapping instance ID you need to modify the old installation before update. For details please refer to BIS / B2B Portal Landscape integration. Also make sure that the B2B Portal uses a different systemID than the BIS system.

In case the instance ID of two BIS instances (formerly nodes) overlap, you should install a new instance with a unique ID.

Note: changing the instance ID of a BIS instance this way is not supported. Changing the instance ID will affect the name of the SSL Certificate Store for the HTTP/S listener.

Instance IDs must not be longer than 50 characters

InstanceIDs with a size longer than 50 characters are not supported by BIS6 and will cause problems. Please shorten them if necessary but ensure that they are still unique - see the previous topic for further details.

Java Cryptography Extension (JCE)

When updating an installation you must decide if you want to use the unlimited strength policy for the Oracle JVM (see JCE policy chapter (page 85) in Appendix).

For other JVMs you need to download and provide unlimited policy files matching the new Java 8 version. The two JAR files from the downloaded archive have to be placed in `<BIS_HOME>/runtime/jvm64/jre/lib/security/`

- For the HP JDK, the files can be downloaded from *http://java.sun.com/javase/downloads.*
- For the *IBM* JDK, the files can be downloaded from *http://www.ibm.com/developerworks/java/jdk/security.*

Windows Service Installation

Note: Remove former BIS service installation (with the existing tooling of the old version of BIS) before running a new BIS installation. For BIS 6.3.5 this is `run-bisas -service -remove`.

There is a new method to start the central instance as a Windows service, as described in *Starting Instance with Operating System (page 105)* . When updating from the former service integration, you should ensure that all previous service configurations are migrated. This is generally only necessary when your previous service configuration differs from the settings in `vm.properties`, register.properties and `ports.properties`.

In some situations stopping or unregistering the service might fail. Sometimes this requires a restart of the machine in order to free the reservation on the service before it can succeed.

Stricter message checks

With 6.5.2Q1 the request messages are also validated against its wsdl/schema file during runtime. In previous BIS releases there was only some base validation on the process, we now have some more detailed validation.To get existing processes running which today do not match the schema file, there are some defined default expression rules for the validation.

For example, all length definitions in the schema are not validated. They will just be ignored.Otherwise, a process will fail due to some fields filled with too much/less letters for example. In some case the default expression rules are not enough and your process will fail after the upgrade to BIS 6.5.2Q1. In this case you should try to fix and redeploy your business process. If this does not work or this is not an option you can define your own expression rule in the adapter user config for the schema validation.

Add the child node "validationRules" to the "frameWork" node in the user-config of the adapter. Then add for each new rule another child with any name. In this child define a new property called "expression". Here define the regular expression which should be executed on the validation error to check whether the validation should be stopped or not. If the expression matches the validation error, the error is skipped and parsing is continued. If the expression does not match the validation error then the error stops the whole message parsing.

```
...
<node name="frameWork">
    <node name="validationRules">
        <node name="max length rule">
            <property name="expression">.*cvc-maxLength-valid.*</property>
        </node>
        <node name="length rule">
            <property name="expression">.*cvc-length-valid.*</property>
        </node>
        ....
    </validationRules>
</frameWork>
```

Process Redeployment is needed for all process templates deployed on BIS version 6.3.4 Q2 or earlier

All the process templates deployed on BIS version 6.3.4 Q2, as well as on older BIS versions, are no longer compatible with 6.5.1 Q1. The same issue applies for sequential upgrades to 6.3.5 Qx from versions 6.3.2 Qx, 6.3.3 Qx or 6.3.4 Qx, that are later upgraded to version 6.5.1 Q1. In this scenario, all of the process templates deployed on 6.3.2 Qx, 6.3.3 Qx or 6.3.4 Qx and then not redeployed under 6.3.5 Qx won't work under version 6.5.1 Q1. In order to solve this, all the process templates/zips should be redeployed. Redeployment can be performed in two ways (Please select one of them):

1. Go to *[BIS_HOME]/data/webdav/repository/zip/<LS>* folder and cut all the .zip files. Then paste them into *[BIS_HOME]/data/webdav/repository/hotdeploy/<LS>* folder and wait until they get deployed. (recommended)
2. Deploy all the actual versions of the process templates using Process Designer. (Process templates must be deployed to the test system before being placed on a production system).

Process Template View

The table in the Inbound tab of the process template view showing the events a process can handle and the rules table below are empty for process templates deployed prior than 6.3.5Q4 and process templates deployed in 6.5.1Q1. In order to see the events in the Inbound tab and the rules it is necessary to re-deploy the process template. This issue has no impact on the runtime behaviour: Process templates deployed in former versions will work, this is only a display issue.

BIC Mapping Repository Redeployment

For upgrades from 6.3.5Q3 and newer no redeployment is necessary, but there are two exceptions:

1. Mappings using the command gotoNextLookupDB and deployed with 6.3.5Q4 and older have to be redeployed.

2. Mappings using bapi commands and deployed with 6.3.5Q4 and older have to be redeployed. If the mappings still thrown an error after redeployment, please check if the adapter 3080B6 (BIC Bapi adapter) is installed.

It is recommended, after upgrading from older versions than 6.3.5Q3 of BIS, to redeploy all global procedures and mappings in the BIC repository via the GUI front end *Mapping Management* and *Global Procedures* GUIs. Depending on the version of the server you are upgrading from, there may be changes in the underlying converter that require recompilation of mappings and global procedures due to the mechanism of resolving methods in the BIC type system.

If mappings use external java functionality (database driver, own java implementations), the classes must be available in the 6.5 environment: This is described in manual *BIC Operation* chapter *Using External Java Classes -> BIS Adapter Server, Adapter Engine and Process Engine*.

Changing B2B Portal instance ID

If you follow the recommendation you should have unique instance IDs in one tier (production, integration, ...) of your landscape. However if you have installed a B2B Portal with the default "CENTRAL" you might want to change it:

You need to shutdown the application, make changes to the properties file and run register.{sh|bat} after your changes. For 6.3.5 installations, you can modify the `instance.id` property in the `software/vm.properties` file. For an existing 6.5.2 installation the property is named `instance.id` in `software/profiles.properties` (this is not visible in propedit tool).

After you have changed the instance ID, you also need to rename the sysinfo file, and remove the instance ID from the name. For example if your old B2B Portal as installed with the instance ID "CENTRAL", rename `<PORTAL_HOME>/software/spm-repository/sysinfo_CENTRAL.xml` to `<PORTAL_HOME>/software/spm-repository/sysinfo.xml`.

Migration of Process Templates after Migration from 6.3.5

If BIS is installed as upgrade installation with BIS 6.3.5 as source, the process templates will be migrated on first access after the upgrade. This means the very first usage of each template may take longer than usual. If you want to spare this migration during execution, you may also redeploy the templates after the upgrade to 6.5.2. [issue_b#67813]

TPM Entities Explorer

In case of an update from 6.3.5 to 6.5.2 and in case in TPM schemas icons from BIS resource pool are used. These images will not be found anymore a green bullet will be shown instead. [issue_b#62264]

Workaround: Copy needed image and translation files from SEEBURGER resource pool (com/seeburger/resourcepool/*) to folder <BIS>/conf/custom/icons/com/seeburger/* and <BIS>/conf/custom/icons/translations/com/seeburger/*.

10 Appendix

10.1 Encrypted Storage of Credentials

10.1.1 Basics

Seeburger BIS stores master data in the system database. This includes sensitive credentials (i.e. username/password combinations) for certain communication protocols like Internet Mail (POP3, IMAP, SMTP), file transfer protocols (FTP, SFTP) or VAN accounts.

It is not possible to store these credentials one-way hashed (like you would do with Login account passwords). The cleartext password is needed as it has to be sent as is to the respective peer for authentication purposes. To protect such secret password credentials against attackers having read access either to the database (or parts of it) or to database backups, the passwords need to be stored in a secured way.

Starting with BIS release 6.3.5Q3 these credentials are stored obfuscated in the database by default. This mechanism is fully backward compatible to prior BIS releases. This obfuscation mode will be referred to as `S0` mode and is used by default.

For a maximum security level, SEEBURGER Wallet is available. It is able to encrypt passwords in a cryptographically strong way using the AESWrap algorithm. This strong encryption mode will be referred to as `S2` mode.

For additional details about the used mechanisms and algorithms, please refer to the “Technical Specification” chapter of this document.

10.1.2 Initial Configuration

For activating the S2 mode a master key must be created. The following steps need to be implemented.

10.1.2.1 Initial Configuration for BIS AdminServer

If the password encryption is activated for the first time, a new and empty file `[BIS_HOME]/conf/keys/masterwallet.properties` must be generated manually. Use exactly the above name and location! See the recommended commands for creating an empty file below.

Recommended commands for generating an empty file:

- Linux: `touch <BIS_HOME>/conf/keys/masterwallet.properties`
- Windows (command line): `type NUL >> <BIS_HOME>\conf\keys\masterwallet.properties`

If the file exists, it will be manged with the `<BIS_HOME>/bin/manage-wallet.{sh,bat}` script. It describes a procedure which can be used when all BIS instances are online. If you can shut down the whole system you can stop the intermediate step to distribute the not-activated key:

- Create a new master key. Make sure, that *0000* is a 4-digit hexadecimal key identifier. It is recommended to start with *0000*. The key size of the generated AES key is 128 bit by default.
  - `manage-wallet.{bat,sh} create password.secret.0000 128`
- You now have to distribute this wallet file securely to all running machines (to all instance homes). If the BIS system is shut down while you create the wallet you can skip this step.
- Now you pick the master secret to use (the active keyid, in our case 0000).
  - `manage-wallet.{bat,sh} set password.protectionkey=0000`
- And then you can activate the strong password encryption (mode `S2`):
  - `manage-wallet.{bat,sh} set password.protectionmode=S2`
- You need to select a key and enable S2 mode on all instances. Before you can do it on any instance the key has to be present on all instances. (As mentioned above, copy the file with the keys before activating them in case you cannot shut down the BIS system.)

⚠ **NEVER** delete the wallet file itself or try to manipulate it with any other means than the manage-wallet script, as all passwords encrypted with keys in this file **will be lost unrecoverably**.

10.1.2.2 Configuration for External Instances

ℹ Distribute the file `<BIS_HOME>/conf/keys/masterwallet.properties` to ALL External instances connected to this BIS installation.

⚠ After each change in the `masterwallet.properties` by the above script on the BIS AdminServer, it is vitally needed to keep all copies of this file on the External Instances synchronized with the BIS AdminServer `masterwallet.properties` (see next paragraph).

10.1.2.3 Gradual Key Transition

The master key, which is used to encrypted newly stored passwords, can be renewed gradually. This means, it is possible to generate and activate a new master key after a certain period of time. All credentials in database or files which still use the old key can still be used. The above described commands `create password.secret.0001` (with any unsuded key ID, 0001 in this example) and `set password.protectionkey=0001` should be used for such a procedure. Again the created but not activated key has to be distributed (copy the `masterwallet.properties` file securely) before it is used.

ℹ Note that this new key is only applied to newly stored database records. All unmodified records (and files) will remain encrypted (and of course recoverable/readable) by the key that has been active before. You should therefore not remove old keys and not recycle key Ids.

10.1.2.4 Switching the Protection Mode

It is possible to deactivate the strong `S2` encryption after it has once being activated. All passwords of newly stored master data records will be stored in `S0` obfuscation mode again. But you need to keep all password.secret.xxxx entries, as long as the database contains keys using those key Ids.

⚠ Therefore **NEVER** delete the wallet file itself or try to manipulate it with any other means than the manage-wallet script, as all passwords encrypted with keys in this file will be lost unrecoverable.

For switching the protection mode use:

```
manage-wallet.{bat,sh} set password.protectionmode={S0,S2}
```

10.1.2.5 Back-up Copy

The `masterwallet.properties` file is backed up before each change to it by the manage-wallet script. The back-up copy is named `masterwallet.properties.bak` and is located in the same directory than the `masterwallet.properties`. Only one generation is kept.

An unwanted change to the masterwallet.properties may be rolled back manually by using this back-up file.

In such a case also **NEVER** delete any file, but rename them only. If you are in doubt about the state of the `masterwallet.properties`, contact Seeburger Support.

You might want to archive the `masterwallet.properties` file independent from the database backup, since otherwise the credentials in the database backup could be decrypted.

10.1.2.6 Log File

The script manage-wallet creates a log file named `<BIS_HOME>/log/install/manage-wallet.lgw`. Furthermore the last executed command is also added to the `masterwallet.properties` file as a comment.

10.1.3 Restrictions

- In order to get all existing master data records secured by the strong `S2` mode, it is currently needed to open and save the respective master dataset forms manually in BIS front-end.
- The BIS front-end currently re-encrypts already encrypted password fields again, when the record is saved via BIS front-end. This will lead to a different value for the password property in the respective database table column. Although the value is different, the encrypted password itself is of course still the same. The technical reason for the changed value is caused by the secure random (salt) bytes that are additionally applied to the password before encrypting it.
  This is expected behaviour and applies to both `S0` and `S2` mode!
- If the `masterwallet.properties` file is lost or damaged, the encrypted passwords can never be recovered anymore.
- The BIS front-end (and BIS communication adapters) will not be able the decrypt to password again, if the key is or the `masterwallet.properties` itself is lost. In order to recover the data sets the current limitation is to re-set the password in the corresponding DB tables. Please contact Seeburger Support in such a case.
- The access to the `masterwallet.properties` must be secured by file system means. We recommend limiting the access to this file to read-only for the BIS runtime OS user. For editing/managing the file, the OS user executing the script needs write access to the file on all BIS instances.

10.1.4 Technical specification

10.1.4.1 Password encryption (S2)

AESWrap is a NIST recommended cipher for wrapping cryptographic keys. It uses the AES cipher in a special block mode. SEEBURGERWallet uses an AES key with the length 128, 192 or 256 bits and an 8 byte secure random salt value for encrypting passwords. The padding, which Seeburger Wallet uses for the passwords, is compliant to RFC 3537. This padding allows to store up to 255 bytes long UTF-8 strings. Keyid and encryption mode are visible in the password fields of the database as *$S2$nnnn* (nnnn is the Key Id for the required master secret) prefix. The master keys are always obfuscated with S0 mode in the wallet file.

10.1.4.2 Password obfuscation (S0)

The password obfuscation uses a 4 byte secure random salt value to obfuscate the passwords and stores them in a Base64-encoded string with a *$S0$* prefix.

10.2 Console Setup

Note: The console setup is for experts only!
The database must already be available. For MSSQL, the console setup cannot create a database.

On some systems the console installer causes redraw problems on the console [**issue_b#22727**]. Ensure you configure your terminal to use backspace (Ctrl+H) as the erase character, otherwise the progress bar of the installer will cause redraw problems on the console. With putty you can set the key in the menu *Terminal* | *Keyboard* | "*The Backspace Key=Ctrl+H*". You can use the output of the "*stty -a*" command to verify your current terminal uses "*erase ^h*".

Start Console Setup

You can start the console installer with the following command on the commandline:

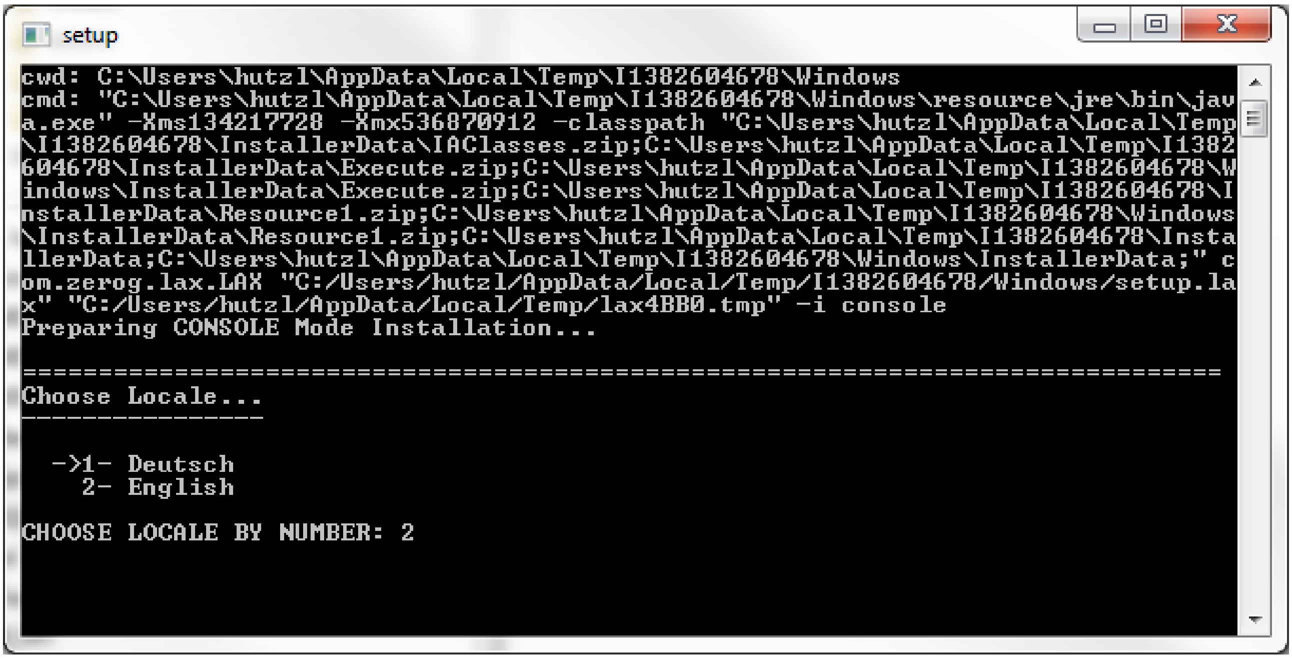
On *Linux/Unix*-based systems type

```
$ unset DISPLAY
$ /bin/sh /<MEDIA>/installer/linux64/setup.bin -i console
```

On Windows systems type

```
> <MEDIA>/installer/win64/setup.bin -i console
```

Language Selection

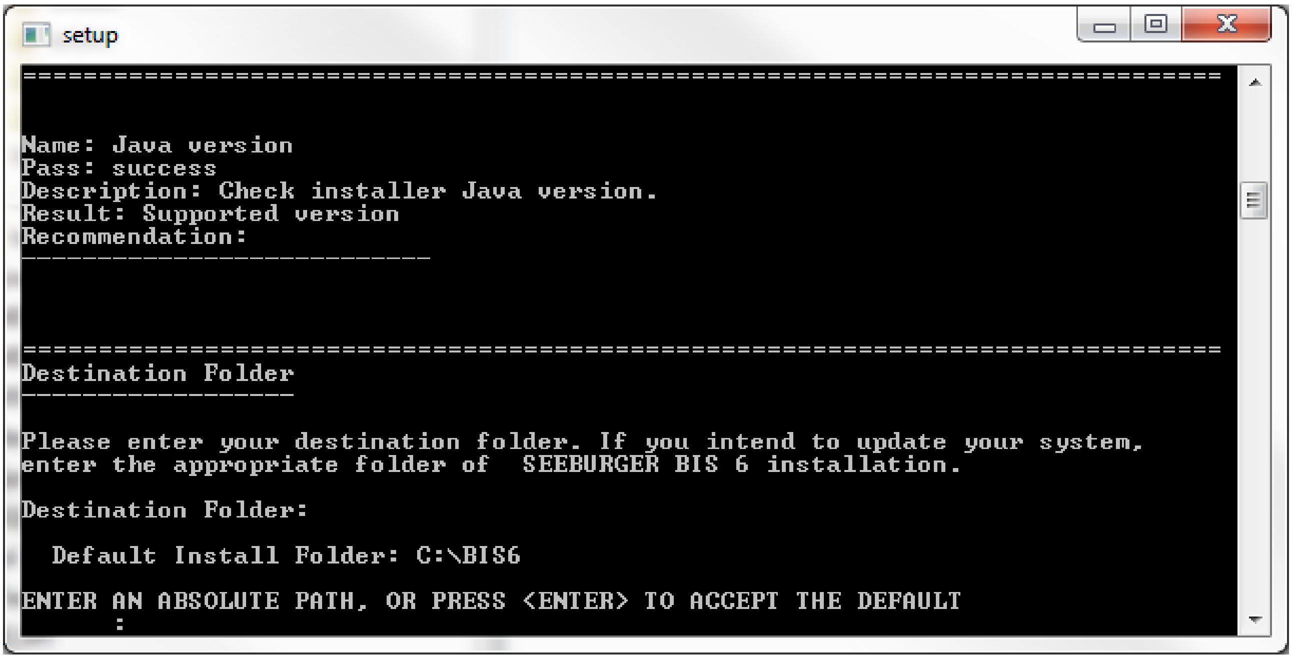


```
cwd: C:\Users\hutzl\AppData\Local\Temp\I1382604678\Windows
cmd: "C:\Users\hutzl\AppData\Local\Temp\I1382604678\Windows\resource\jre\bin\jav
a.exe" -Xms134217728 -Xmx536870912 -classpath "C:\Users\hutzl\AppData\Local\Temp
\I1382604678\InstallerData\IAClasses.zip;C:\Users\hutzl\AppData\Local\Temp\I1382
604678\InstallerData\Execute.zip;C:\Users\hutzl\AppData\Local\Temp\I1382604678\W
indows\InstallerData\Execute.zip;C:\Users\hutzl\AppData\Local\Temp\I1382604678\I
nstallerData\Resource1.zip;C:\Users\hutzl\AppData\Local\Temp\I1382604678\Windows
\InstallerData\Resource1.zip;C:\Users\hutzl\AppData\Local\Temp\I1382604678\Insta
llerData;C:\Users\hutzl\AppData\Local\Temp\I1382604678\Windows\InstallerData;" c
om.zerog.lax.LAX "C:/Users/hutzl/AppData/Local/Temp/I1382604678/Windows/setup.la
x" "C:/Users/hutzl/AppData/Local/Temp/lax4BB0.tmp" -i console
Preparing CONSOLE Mode Installation...

===============================================================================
Choose Locale...
----------------

  ->1- Deutsch
    2- English

CHOOSE LOCALE BY NUMBER: 2
```

1. After starting the console setup please select the preferred language by enter the number or press Enter to accept the default.
2. Press Enter to continue.

Destination Folder

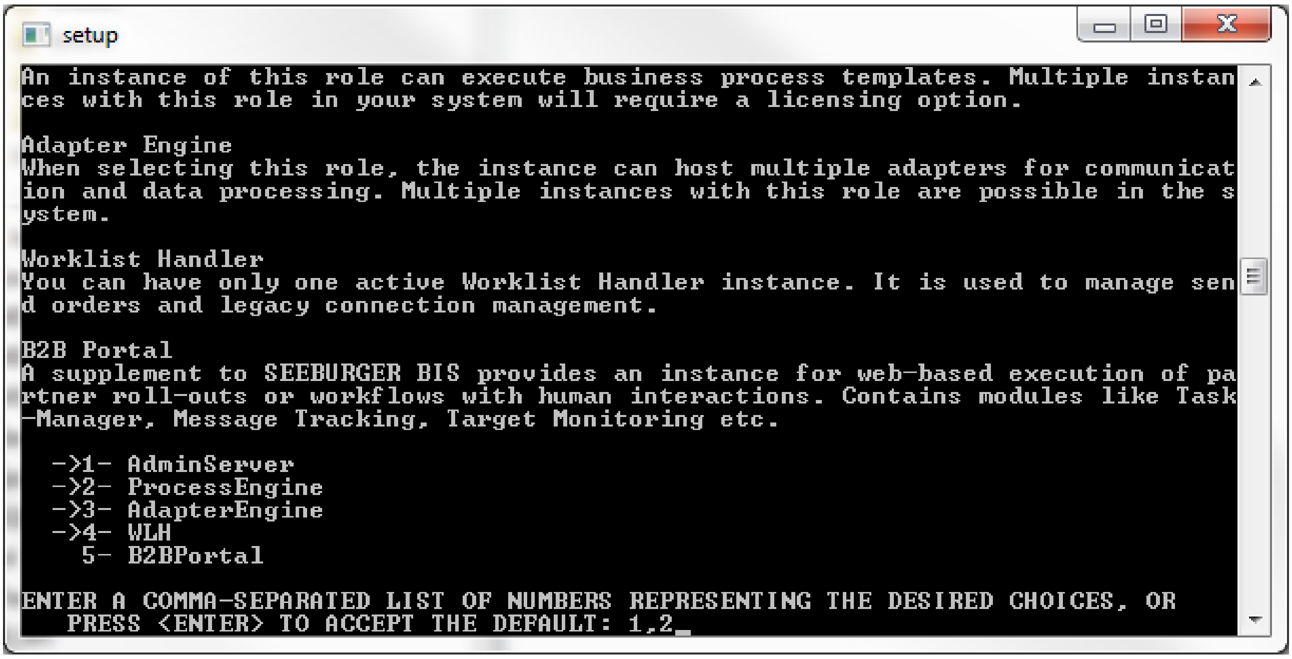
Note: The installation path you specify should not contain spaces and the max length is 64 characters. On a *Unix/Linux* you typically create the directory as root and own it to the BIS runtime user (which also must be used for the installation).



```
===============================================================================


Name: Java version
Pass: success
Description: Check installer Java version.
Result: Supported version
Recommendation:
---------------------------




===============================================================================
Destination Folder
------------------

Please enter your destination folder. If you intend to update your system,
enter the appropriate folder of  SEEBURGER BIS 6 installation.

Destination Folder:

  Default Install Folder: C:\BIS6

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
      :
```

1. Please enter the destination folder you want to install SEEBURGER BIS6.
   You can press Enter to accept the default folder.
2. Press Enter to continue.

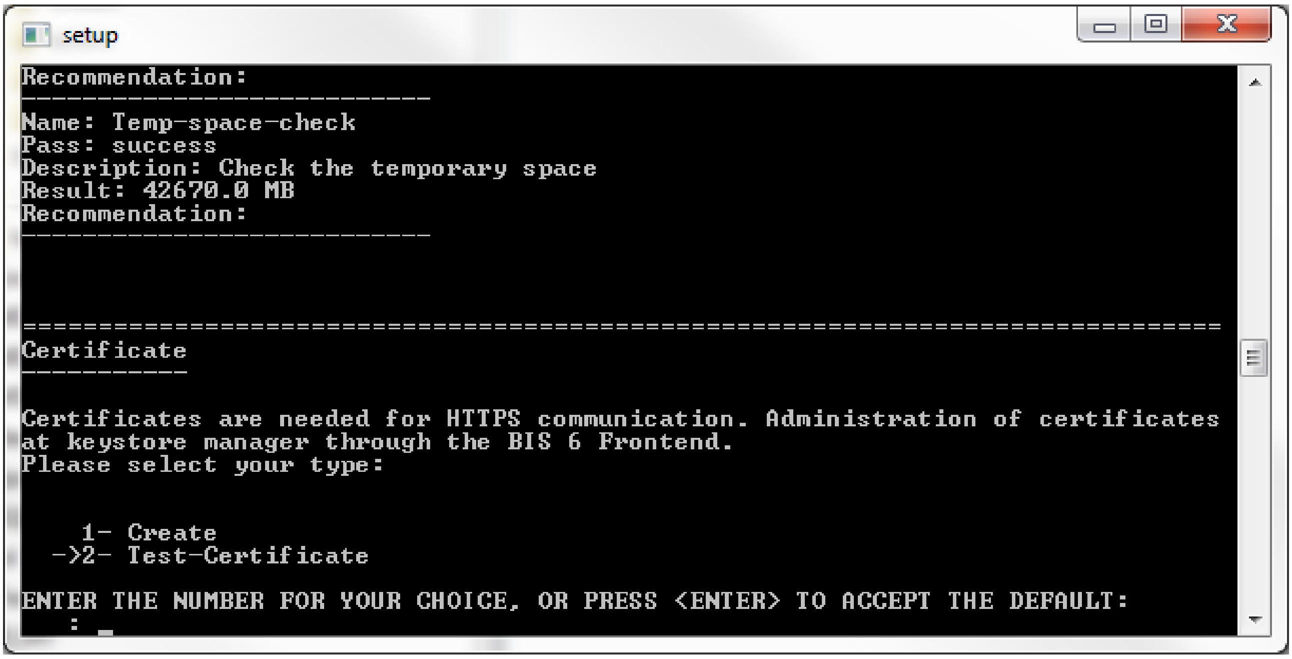
Role Selection



```
An instance of this role can execute business process templates. Multiple instan
ces with this role in your system will require a licensing option.

Adapter Engine
When selecting this role, the instance can host multiple adapters for communicat
ion and data processing. Multiple instances with this role are possible in the s
ystem.

Worklist Handler
You can have only one active Worklist Handler instance. It is used to manage sen
d orders and legacy connection management.

B2B Portal
A supplement to SEEBURGER BIS provides an instance for web-based execution of pa
rtner roll-outs or workflows with human interactions. Contains modules like Task
-Manager, Message Tracking, Target Monitoring etc.

  ->1- AdminServer
  ->2- ProcessEngine
  ->3- AdapterEngine
  ->4- WLH
    5- B2BPortal

ENTER A COMMA-SEPARATED LIST OF NUMBERS REPRESENTING THE DESIRED CHOICES, OR
   PRESS <ENTER> TO ACCEPT THE DEFAULT: 1,2_
```

1. Enter a comma separated list of numbers presenting the roles you want to install, or press Enter to accept the default.
2. Press Enter to continue.

Certificate



```
Recommendation:
---------------------------
Name: Temp-space-check
Pass: success
Description: Check the temporary space
Result: 42670.0 MB
Recommendation:
---------------------------



===============================================================================
Certificate
-----------

Certificates are needed for HTTPS communication. Administration of certificates
at keystore manager through the BIS 6 Frontend.
Please select your type:


    1- Create
  ->2- Test-Certificate

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
   : _
```

1. Select whether a certificate for HTTPS communication, or a test certificate should be created.
2. Press Enter to continue.

Note: This dialog is not displayed, if you are upgrading or repairing your version.

The Create Certificate Option

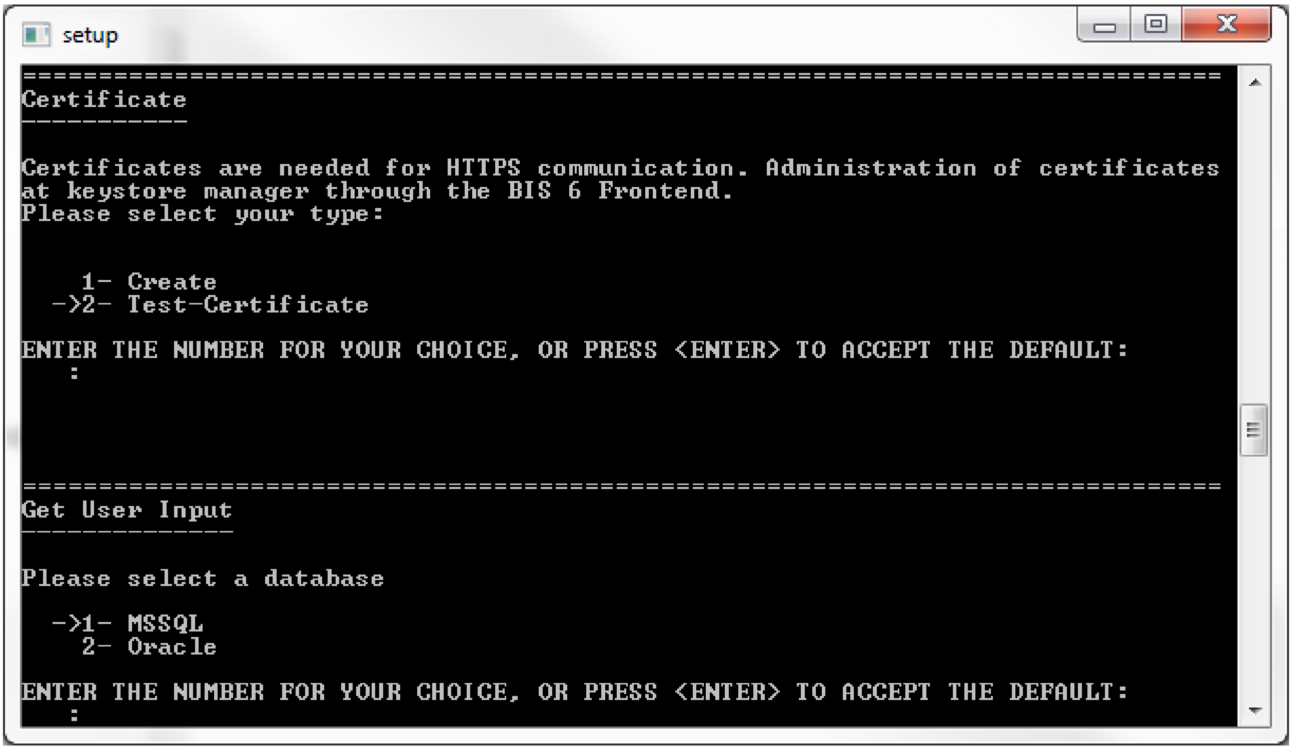
The *Create certificate* option can be used to generate a new self-signed certificate. The next dialog will ask you for the attributes and generate the required key pair as specified. You can later on manage and replace this certificate, or generate a Certificate Signing Request (CSR) as well as import the actual signed certificate from your official Certification Authority (CA), if you have one. All this is done in the Keystore Manager's GUI (KSM).

In the fields, please enter the required information. The *Common Name* field is obligatory and should correspond to the fully qualified host name.

The Create SEEBURGER Test Certificate Option

For test installations, the *Seeburger Test Certificate* can be used. This is a self-signed dummy certificate. It should not be used for production systems since no attributes can be configured. However, this is the preferred method to get a basic system installed, since you can change and manage the certificate (including generation of a Certificate Signing Request for external Certification Authorities) in the installed product with the Key Store Manager GUI.

Select Database

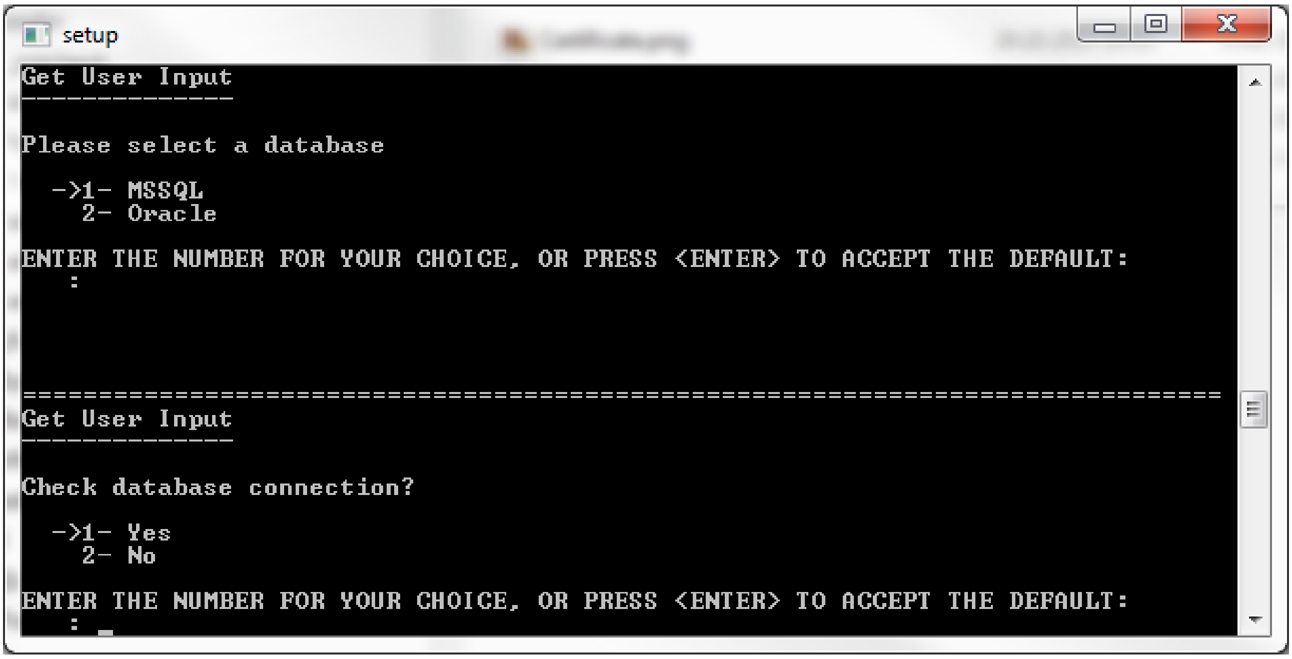


```
===============================================================================
Certificate
-----------

Certificates are needed for HTTPS communication. Administration of certificates
at keystore manager through the BIS 6 Frontend.
Please select your type:


    1- Create
  ->2- Test-Certificate

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
   :



===============================================================================
Get User Input
--------------

Please select a database

  ->1- MSSQL
    2- Oracle

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
   :
```

Please check the *Release Notes* for currently supported specific database versions.

1. Enter the number for the appropriate database management system from the displayed list, or press Enter to accept the default.
2. Press Enter to continue.

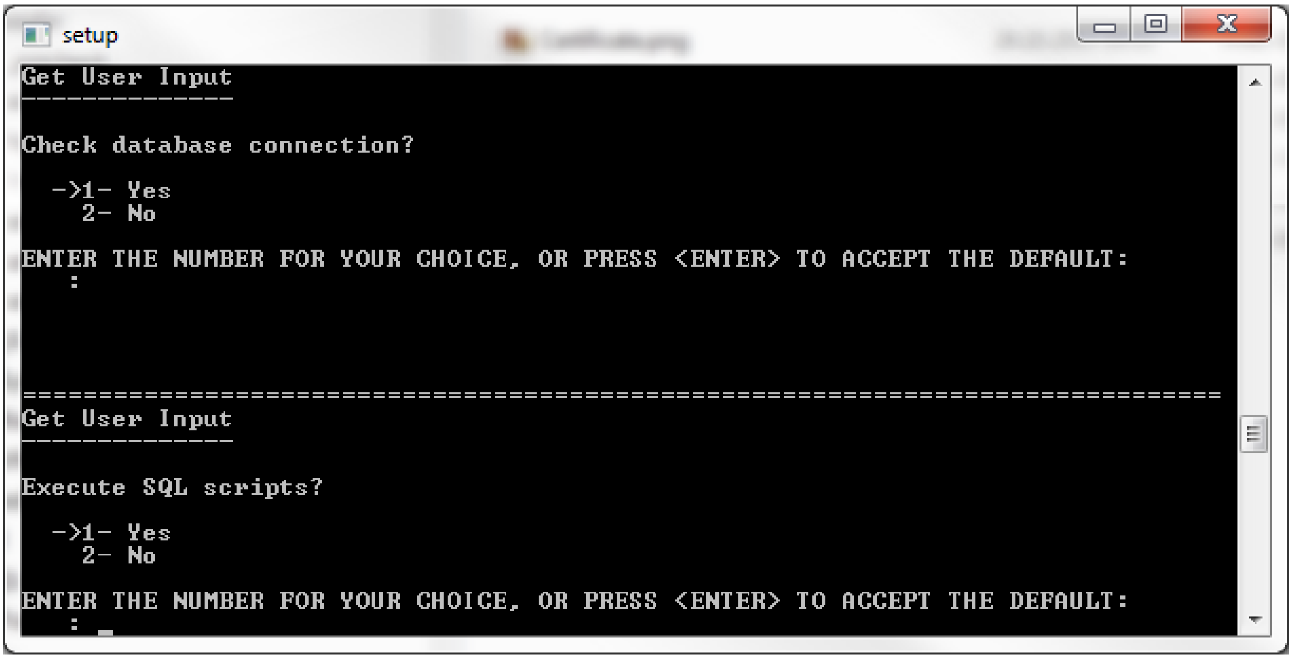
Note: This dialog is not displayed, if you are upgrading or repairing your version.



```
Get User Input
--------------

Please select a database

  ->1- MSSQL
    2- Oracle

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
   :



===============================================================================
Get User Input
--------------

Check database connection?

  ->1- Yes
    2- No

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
   : _
```

1. Select whether a database connection check has to be performed.
2. Press Enter to continue.

Note: This dialog is not displayed, if you are upgrading or repairing your version.

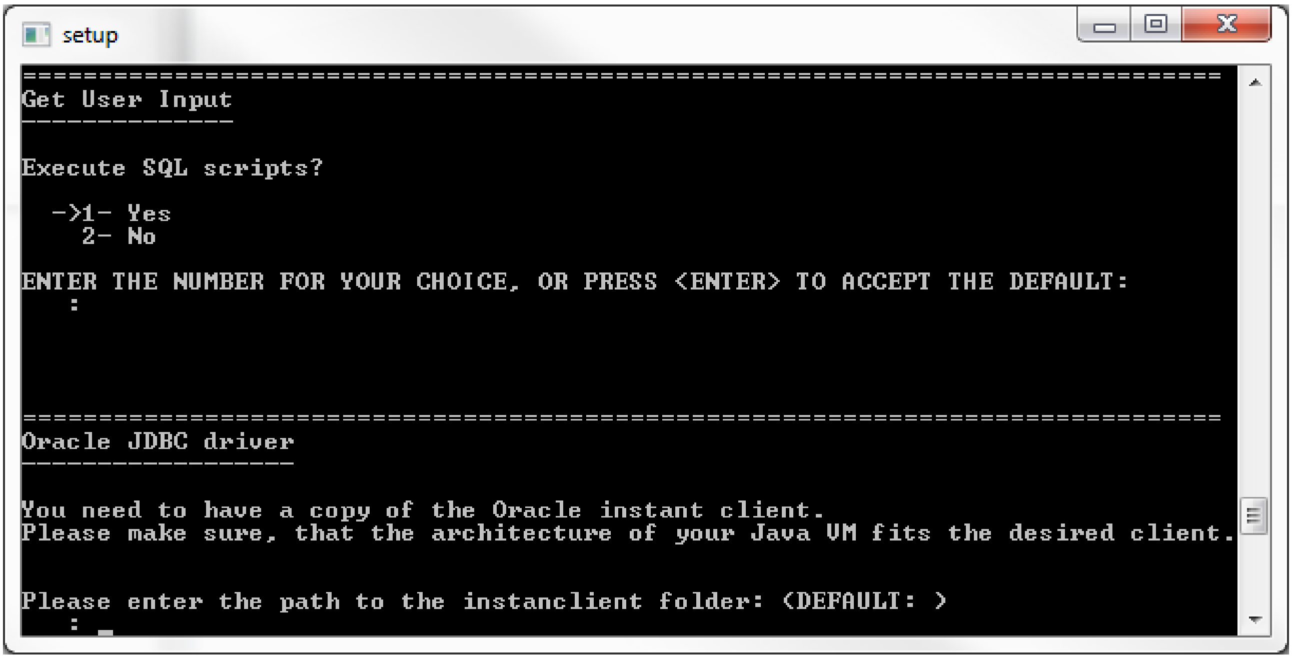


```
Get User Input
--------------

Check database connection?

  ->1- Yes
    2- No

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
   :



===============================================================================
Get User Input
--------------

Execute SQL scripts?

  ->1- Yes
    2- No

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
   : _
```

1. Select whether SQL scripts have to be executed. If execution is not applicable, select No. In this case, an SQL script is generated which must be executed manually.
2. Press Enter to continue.

Note: This dialog is not displayed, if you are upgrading or repairing your version.

Oracle



```
===============================================================================
Get User Input
--------------

Execute SQL scripts?

  ->1- Yes
    2- No

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
   :



===============================================================================
Oracle JDBC driver
------------------

You need to have a copy of the Oracle instant client.
Please make sure, that the architecture of your Java VM fits the desired client.


Please enter the path to the instanclient folder: (DEFAULT: )
   : _
```

1. Enter the directory which includes Oracle Instantclient.
2. Press Enter to continue.

Note: This dialog is not displayed, if you are upgrading or repairing your version.

Pre-Installation Summary

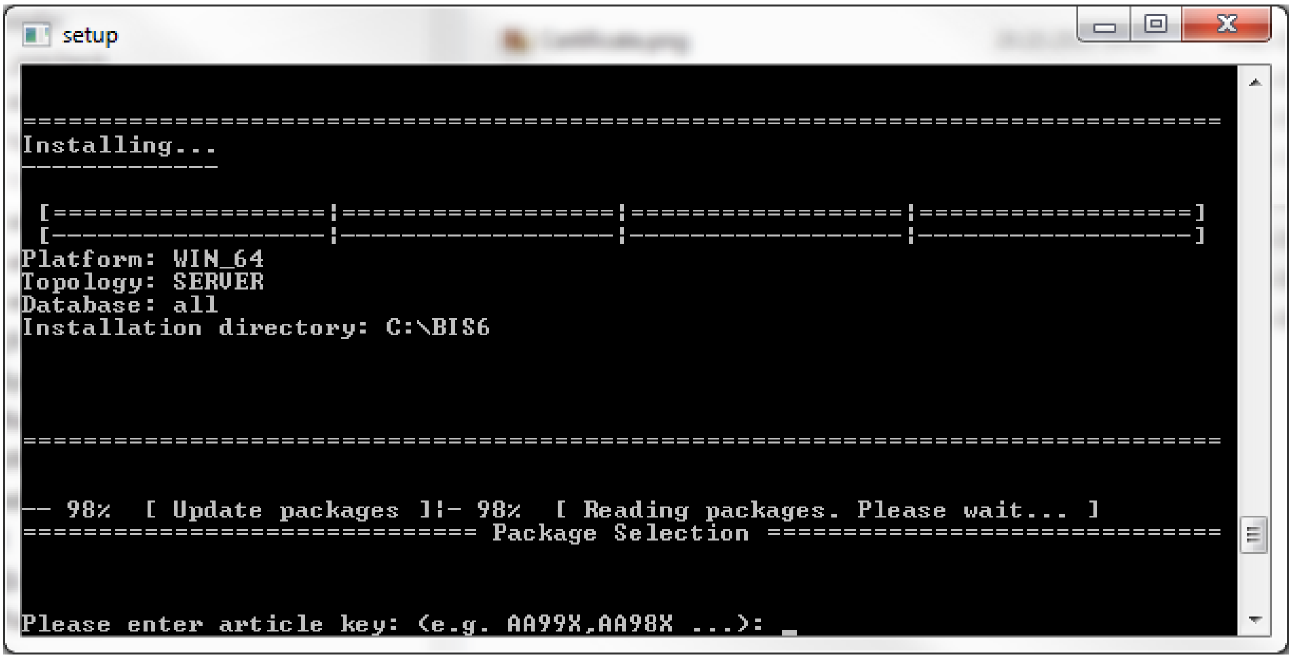
A *Pre-Installation Summary* is displayed.

1. Check whether the displayed information correspond to the intended ones.
2. If the settings are OK, press Enter to continue the installation.

At this point of the installation process, the setup will start to write files to the new installation destination. Keep this in mind, if you cancel the setup after this point. At least the software repository will be updated with the modules from the installation media (location: *software/spm-repository*).

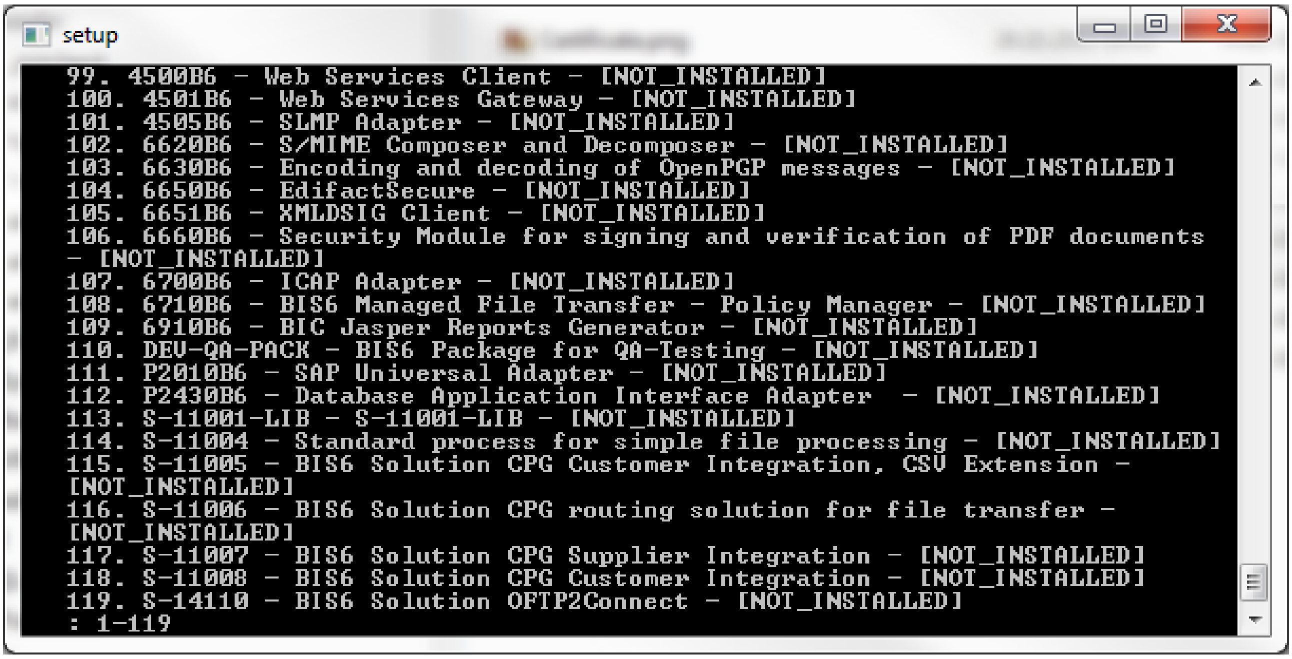
Activate Articles

If the dialog to enter article keys is displayed, you need to register all purchased modules by entering the (case-sensitive) article keys. The keys are provided with the delivery note for the BIS modules.



```
================================================================================
Installing...
-------------

 [==================|==================|==================|==================]
 [------------------|------------------|------------------|------------------]
Platform: WIN_64
Topology: SERVER
Database: all
Installation directory: C:\BIS6




================================================================================


-- 98%  [ Update packages ]|- 98%  [ Reading packages. Please wait... ]
============================== Package Selection ==============================


Please enter article key: (e.g. AA99X,AA98X ...): _
```

1. Please enter the article keys as comma separated list.
2. Press Enter to continue.
3. A question is displayed. If you want to activate more articles enter Y otherwise enter N.
4. Press Enter to continue.



```
   99. 4500B6 - Web Services Client - [NOT_INSTALLED]
   100. 4501B6 - Web Services Gateway - [NOT_INSTALLED]
   101. 4505B6 - SLMP Adapter - [NOT_INSTALLED]
   102. 6620B6 - S/MIME Composer and Decomposer - [NOT_INSTALLED]
   103. 6630B6 - Encoding and decoding of OpenPGP messages - [NOT_INSTALLED]
   104. 6650B6 - EdifactSecure - [NOT_INSTALLED]
   105. 6651B6 - XMLDSIG Client - [NOT_INSTALLED]
   106. 6660B6 - Security Module for signing and verification of PDF documents
   - [NOT_INSTALLED]
   107. 6700B6 - ICAP Adapter - [NOT_INSTALLED]
   108. 6710B6 - BIS6 Managed File Transfer - Policy Manager - [NOT_INSTALLED]
   109. 6910B6 - BIC Jasper Reports Generator - [NOT_INSTALLED]
   110. DEV-QA-PACK - BIS6 Package for QA-Testing - [NOT_INSTALLED]
   111. P2010B6 - SAP Universal Adapter - [NOT_INSTALLED]
   112. P2430B6 - Database Application Interface Adapter  - [NOT_INSTALLED]
   113. S-11001-LIB - S-11001-LIB - [NOT_INSTALLED]
   114. S-11004 - Standard process for simple file processing - [NOT_INSTALLED]
   115. S-11005 - BIS6 Solution CPG Customer Integration, CSV Extension -
   [NOT_INSTALLED]
   116. S-11006 - BIS6 Solution CPG routing solution for file transfer -
   [NOT_INSTALLED]
   117. S-11007 - BIS6 Solution CPG Supplier Integration - [NOT_INSTALLED]
   118. S-11008 - BIS6 Solution CPG Customer Integration - [NOT_INSTALLED]
   119. S-14110 - BIS6 Solution OFTP2Connect - [NOT_INSTALLED]
   : 1-119
```

Enter the numbers corresponding to the module(s) which you want to install. You can enter either individual modules or any available.

1. Enter the numbers as a comma/dash separated list (e.g. 1-119 or 1,2,3,4,...)
2. Press Enter to continue.

A question is displayed. If you are sure you want to install the selected articles enter Y.

If several options are displayed, enter the number(s) corresponding to the one that applies for your system. (*Other VM / jdk_dummy* is an empty package, i.e. you do not want to use the provided *Java Development Kit* version).

1. Answer the displayed questions.
2. Press Enter to continue.

The (packed) files will be extracted then. We provide a Java Development Kit for *Microsoft Windows* and *Linux* 64-bit operating systems. For other operating systems, the JDK has to be copied to the *runtime\jvm* directory. Follow the instructions displaed on the console.

Note: The maximum number of input characters is limited [**issue_b#20666**]. This particularly affects the activation and selection of articles (large amounts). To resolve this problem, activate the articles in more than one comma-separated list (activation) and select the articles to be installed in interval-type syntax (e.g. *[1-51]*)

Properties Editor

Note: All editors are displayed in expert mode. Erroneous settings in the expert mode can lead to a defect and unstable instance.

The default values are displayed. If you want to use these values press enter to continue.

Profile Properties

You can make changes to the profile settings.

You must enter an Instance ID.

Ports Properties

You can make changes to the settings for the ports.

VM Properties

You can make changes to the settings for the Java® VM here.

Database Properties

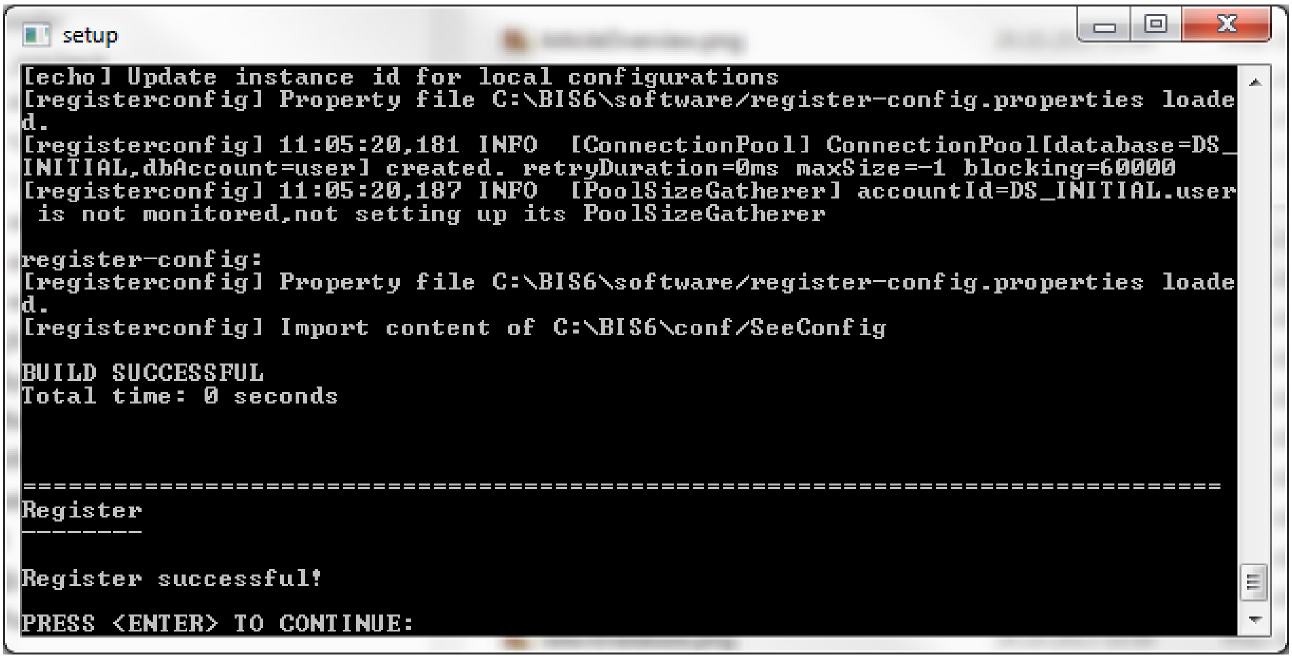
The database has to be configured now. There are different requirements for database configuration, depending on the applied type of database.

In order to continue the setup procedure now, you require a working database instance and administrator-type access to create the schema owner (*Oracle Database*). You need to manually set up the BIS runtime user and database owner before you can continue.

The entered options will be verified, i.e. you cannot continue if anything is missing.

Note: For information on supported DBMS versions and platforms, please refer to the most recent *Release Notes* for your BIS version.

Registering BIS Modules on the Application Server

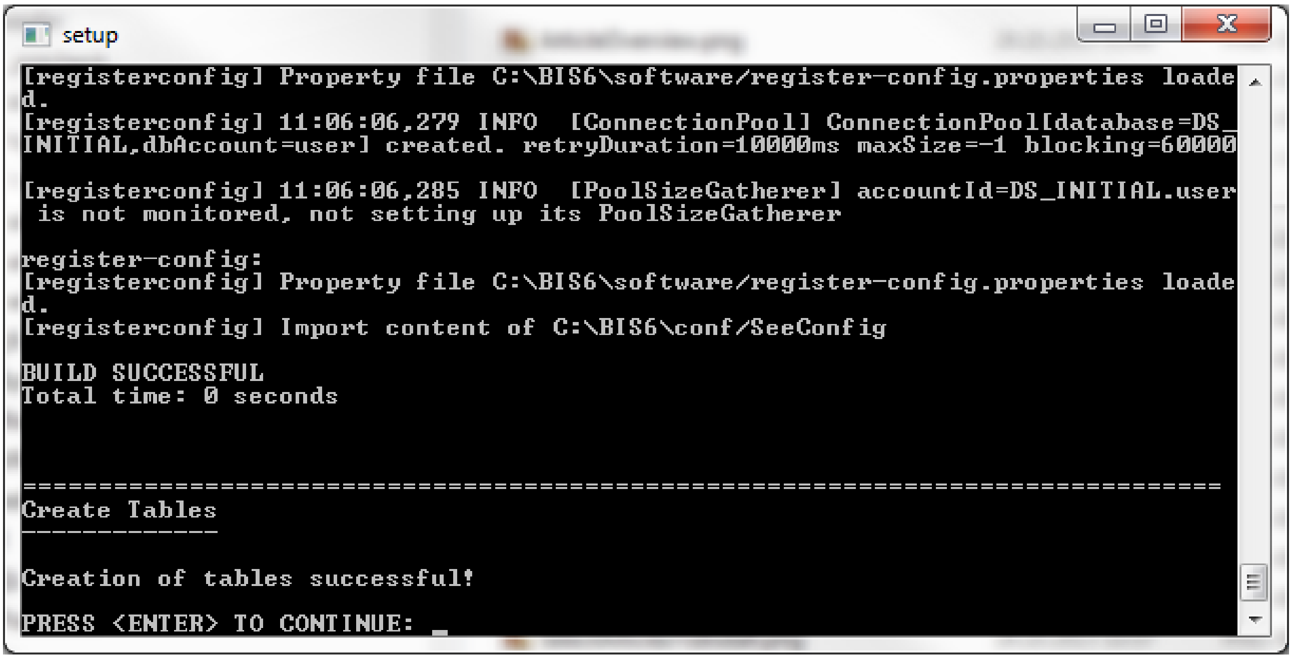


```
[echo] Update instance id for local configurations
[registerconfig] Property file C:\BIS6\software/register-config.properties loade
d.
[registerconfig] 11:05:20,181 INFO  [ConnectionPool] ConnectionPool[database=DS_
INITIAL,dbAccount=user] created. retryDuration=0ms maxSize=-1 blocking=60000
[registerconfig] 11:05:20,187 INFO  [PoolSizeGatherer] accountId=DS_INITIAL.user
 is not monitored,not setting up its PoolSizeGatherer

register-config:
[registerconfig] Property file C:\BIS6\software/register-config.properties loade
d.
[registerconfig] Import content of C:\BIS6\conf/SeeConfig

BUILD SUCCESSFUL
Total time: 0 seconds



===============================================================================
Register
--------

Register successful!

PRESS <ENTER> TO CONTINUE:
```

1. The various BIS modules will now be registered on the application server and the configurations will be created, according to the settings from the files *profile.properties, register.properties*, *vm.properties* and *ports.properties* from the *<BIS6_HOME>/software/* directory.
   For the upgrade procedure, the required database modifications are detected and displayed. The tables will be created with the authorization rights of the *dbo user* and the data will be saved.
2. Press Enter to continue.

Database Initialization

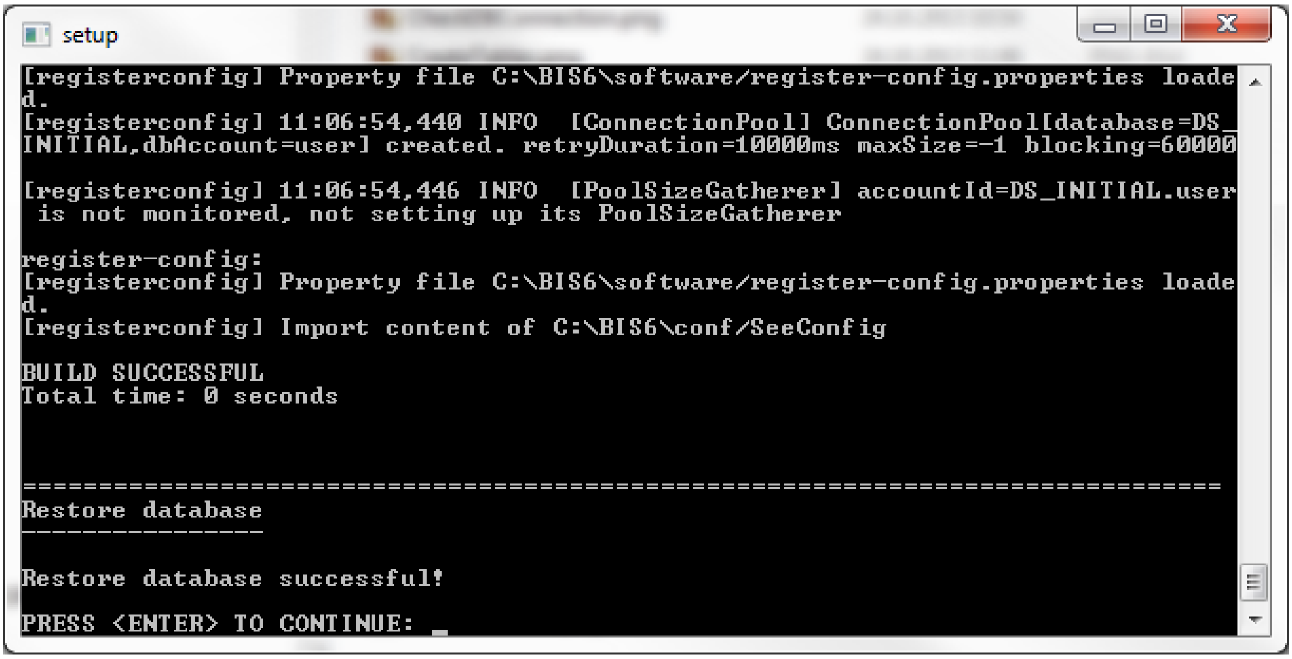
This installation step performs automatically. Database-specific scripts for generating tables and saving the system master data are executed in this step. After each partial step has been carried out, a log file will be displayed.



```
[registerconfig] Property file C:\BIS6\software/register-config.properties loade
d.
[registerconfig] 11:06:06,279 INFO  [ConnectionPool] ConnectionPool[database=DS_
INITIAL,dbAccount=user] created. retryDuration=10000ms maxSize=-1 blocking=60000

[registerconfig] 11:06:06,285 INFO  [PoolSizeGatherer] accountId=DS_INITIAL.user
 is not monitored, not setting up its PoolSizeGatherer

register-config:
[registerconfig] Property file C:\BIS6\software/register-config.properties loade
d.
[registerconfig] Import content of C:\BIS6\conf/SeeConfig

BUILD SUCCESSFUL
Total time: 0 seconds



===============================================================================
Create Tables
-------------

Creation of tables successful!

PRESS <ENTER> TO CONTINUE: _
```

1. Press Enter to continue.

If the first step has problems (for example missing authorization), it will be retried. You can fix the error condition in the background and try the step again. Fixing the problem includes modifying the register.properties file, or actually modifying or configuring objects in the SQL server.



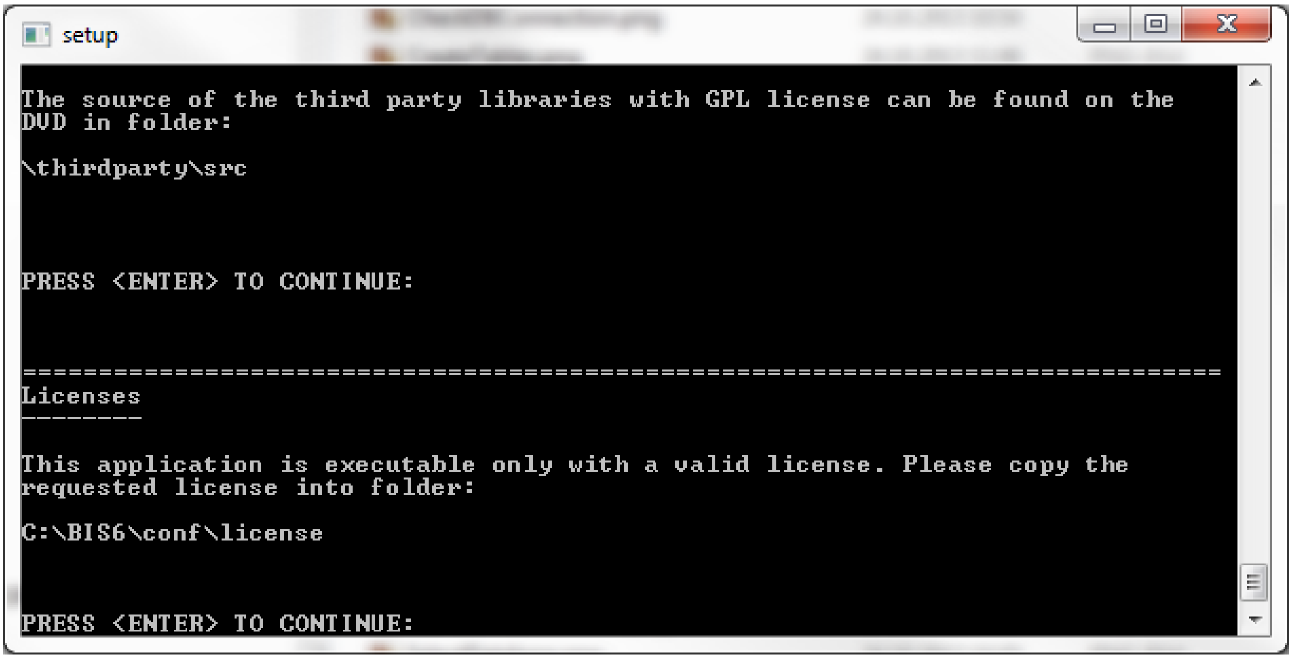
```
[registerconfig] Property file C:\BIS6\software/register-config.properties loade
d.
[registerconfig] 11:06:54,440 INFO  [ConnectionPool] ConnectionPool[database=DS_
INITIAL,dbAccount=user] created. retryDuration=10000ms maxSize=-1 blocking=60000

[registerconfig] 11:06:54,446 INFO  [PoolSizeGatherer] accountId=DS_INITIAL.user
 is not monitored, not setting up its PoolSizeGatherer

register-config:
[registerconfig] Property file C:\BIS6\software/register-config.properties loade
d.
[registerconfig] Import content of C:\BIS6\conf/SeeConfig

BUILD SUCCESSFUL
Total time: 0 seconds



===============================================================================
Restore database
----------------

Restore database successful!

PRESS <ENTER> TO CONTINUE: _
```

The default values will be written to the corresponding database tables.

If you have deselected the option *automatic SQL Import*, you are prompted to execute the SQL scripts. These scripts have to be executed before the installation is continued.

1. Press Enter to continue.

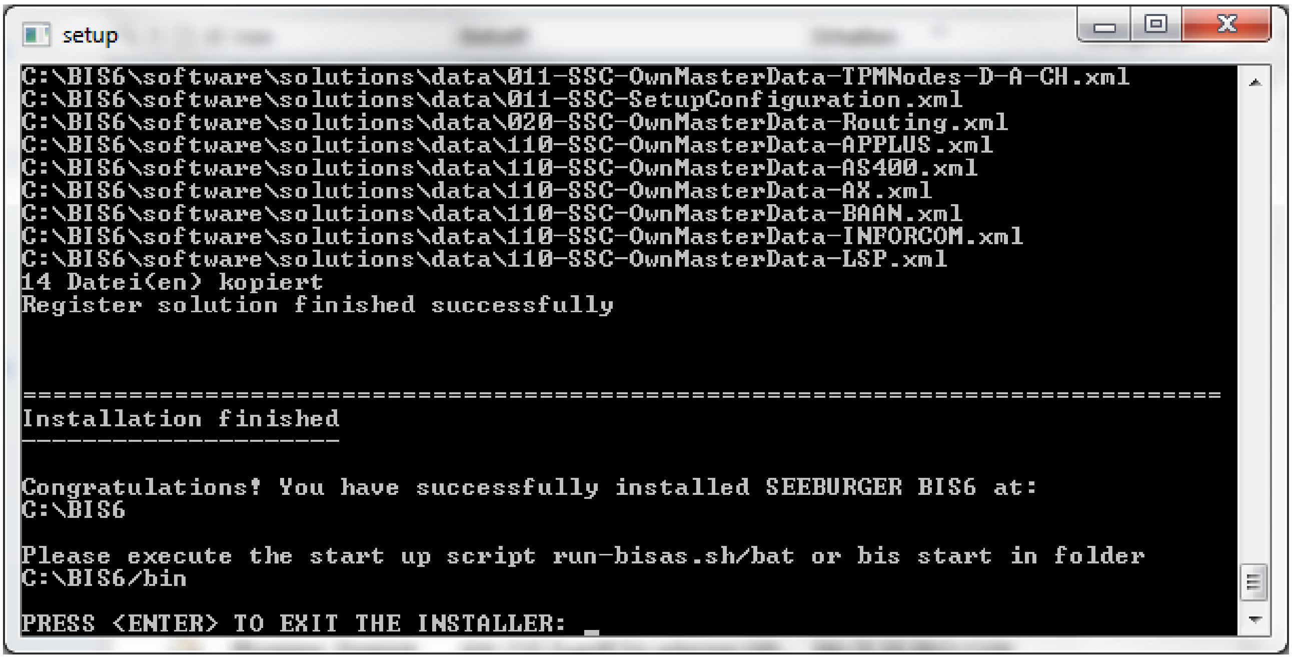
Licensing



```
The source of the third party libraries with GPL license can be found on the
DVD in folder:

\thirdparty\src



PRESS <ENTER> TO CONTINUE:



===============================================================================
Licenses
--------

This application is executable only with a valid license. Please copy the
requested license into folder:

C:\BIS6\conf\license



PRESS <ENTER> TO CONTINUE:
```

1. Please copy the requested license into the given folder.
2. Press Enter to continue.

Register Solution



```
C:\BIS6\software\solutions\data\011-SSC-OwnMasterData-TPMNodes-D-A-CH.xml
C:\BIS6\software\solutions\data\011-SSC-SetupConfiguration.xml
C:\BIS6\software\solutions\data\020-SSC-OwnMasterData-Routing.xml
C:\BIS6\software\solutions\data\110-SSC-OwnMasterData-APPLUS.xml
C:\BIS6\software\solutions\data\110-SSC-OwnMasterData-AS400.xml
C:\BIS6\software\solutions\data\110-SSC-OwnMasterData-AX.xml
C:\BIS6\software\solutions\data\110-SSC-OwnMasterData-BAAN.xml
C:\BIS6\software\solutions\data\110-SSC-OwnMasterData-INFORCOM.xml
C:\BIS6\software\solutions\data\110-SSC-OwnMasterData-LSP.xml
14 Datei(en) kopiert
Register solution finished successfully



===============================================================================
Installation finished
---------------------

Congratulations! You have successfully installed SEEBURGER BIS6 at:
C:\BIS6

Please execute the start up script run-bisas.sh/bat or bis start in folder
C:\BIS6/bin

PRESS <ENTER> TO EXIT THE INSTALLER: _
```

1. In this step, installed solutions will be registered and the installation will be finished..
2. Press enter to exit the setup..

10.3 Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files

The Java Cryptography Extension is used by TLS client, -server and other cryptographic modules. The strength of cryptographic primitives can be controlled by policy settings. This is needed in order to comply with local laws and import restrictions in certain countries. This affects algorithms and key lengths which are allowed to be used. Especially AES is limited to 128bit keys if the "unlimited" strength policy is not enabled. Further details can be found in the official JCA documentation.

The Oracle Java runtime is provided by SEEBURGER for Windows and Linux, and it should also be used on Solaris machines for BIS installations. For this Java version (starting with Java 8u152 delivered with BIS 6.5.2 SP52) there is no longer a need to download and install policy files.

The policy is instead selected with a Java security property `crypto.policy` (in `<BIS_HOME>/runtime/jvm64/jre/lib/securiry/java.security`). This property can have the values "`limited`" or "`unlimited`". In order to make changes to the `java.security` file persistent (it will be overwritten by Java runtime updates); you must request the use of the unlimited policy in the `<BIS_HOME>/software/vm.properties` file with the `vmoptions.useUnlimitedStrength=true` option. The BIS register process will use this setting to edit the JVM file.

The vm.properties option can be set with the installer and upgrade GUI.

⚠ **WARNING**: Only when using installation, update/upgrade or repair with user interaction you can see the policy option in the installer. If you use a different mode you can change the flag after installation and run register. When patch updating a version which did not have the new property before, the default is determined based on the existence of the unlimited strength policy files (which get deleted after this update if you have the updated Oracle JVM installed).

When updating BIS on Windows and Linux while using the SEEBURGER provided JVM, you normally do not manually have to remove the manually installed policy files. This happens on update automatically. However, if you maintained your JVM manually, you might need to clear the files.

The legacy policy files have been located in `<BIS_HOME>/runtime/jvm64/jre/lib/security/{US_export_policy.jar and local_policy.jar}`

For Java runtimes which do not (yet) support the policy mechanism, you need to provide the policy files (after downloading them from the JVM vendor). This is especially true for IBM JDK on AIX and HP JDK on HP/UX.

To install the policy files for the JDK which requires it, follow the following procedure:

- Download the policy files from Vendor
- Extract the Archive file, find the two JAR files
- Stop the BIS instance, make sure no Java process is running
- Replace the two files in `<BIS_HOME>/runtime/jvm64/jre/lib/security/` with the new JAR files
- If you update the JVM you need to replace those files again

Download Sources:

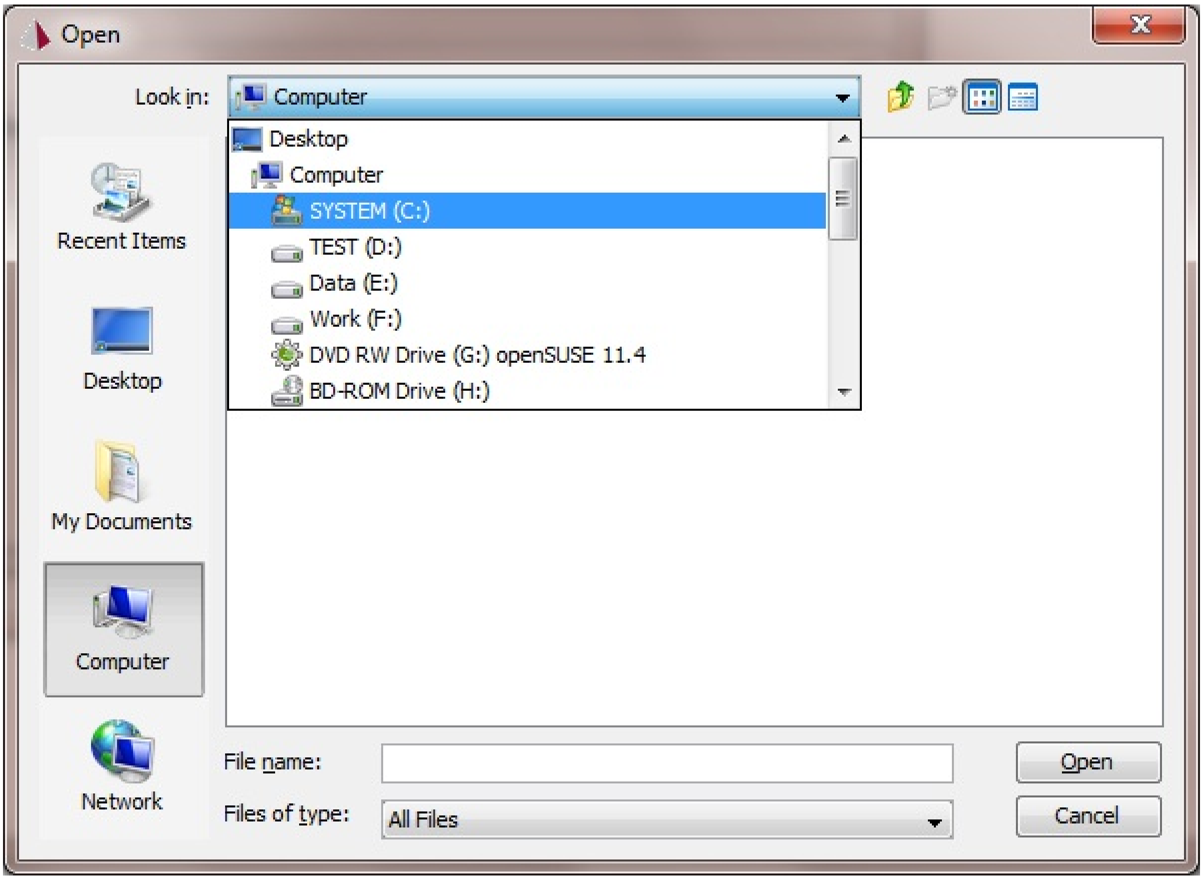
- IBM https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk (IBM.com requires login)
  - IBM Manual (IBM.com) - we do not test jurisdictionPolicyDir mechanism

The BIS Adapters will check the used JCE policy on startup and show or resolve a warning in the Error Monitor.

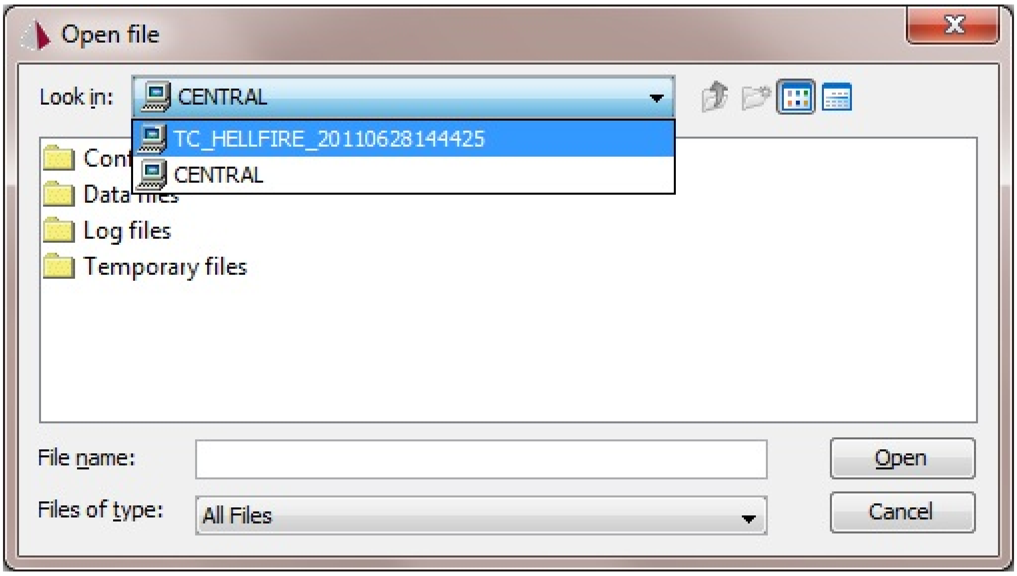
10.4 Restricting Remote Filesystem Browser

Some modules in BIS Front-end use the *RemoteFileChooser* dialog to access files on different instances (AdminServer at least and others if there are available). There is a option to allow or deny the access to specific files and directories. The AdminServer Instance and all other instances have their own configuration with access restriction.

The common *FileChooser* dialog shows all root devices on the local machine (hard disks, CD-s, network mapped folders etc.):



The *RemoteFileChooser* lists only the root items defined in the configuration file, denying access to all other files and directories. This is safer and more flexible. The *RemoteFileChooser* can access all available instances, not just the AdminServer instance:



This is the content of the default configuration (FileSystemRoots-config.xml):

```
<?xml version="1.0" encoding="UTF-8"?>
<config>
    <node name="root - Log files">
        <property name="name">Log files</property>
        <property name="path">{$bisas.log}</property>
        <property name="readonly" type="java.lang.Boolean">false</property>
        <node name="FileFilters">
            <node name="TXT Files">
                <property name="RegExp">^.+$</property>
                <property name="Mode">ALLOW</property>
                <property name="Permissions">FAA_CONNECTION_RO;FAA_CONNECTION_EDIT</
property>
            </node>
        </node>
        <node name="DirectoryFilters">
            <node name="All Directories">
                <property name="RegExp">^.+$</property>
                <property name="Mode">ALLOW</property>
                <property name="Permissions">FAA_CONNECTION_RO;FAA_CONNECTION_EDIT</
property>
            </node>
        </node>
    </node>
    <node name="root - Configuration files">
        <property name="name">Configuration files</property>
        <property name="path">{$bisas.conf}</property>
        <property name="readonly" type="java.lang.Boolean">false</property>
        <node name="FileFilters">
            <node name="TXT Files">
                <property name="RegExp">^.+$</property>
                <property name="Mode">ALLOW</property>
                <property name="Permissions">FAA_CONNECTION_RO;FAA_CONNECTION_EDIT</
property>
            </node>
        </node>
        <node name="DirectoryFilters">
            <node name="All Directories">
                <property name="RegExp">^.+$</property>
                <property name="Mode">ALLOW</property>
                <property name="Permissions">FAA_CONNECTION_RO;FAA_CONNECTION_EDIT</
property>
            </node>
        </node>
    </node>
    <node name="root - Data files">
```

```
        <property name="name">Data files</property>
        <property name="path">{$bisas.data}</property>
        <property name="readonly" type="java.lang.Boolean">false</property>
        <node name="FileFilters">
            <node name="TXT Files">
                <property name="RegExp">^.+$</property>
                <property name="Mode">ALLOW</property>
                <property name="Permissions">FAA_CONNECTION_RO;FAA_CONNECTION_EDIT</
property>
            </node>
        </node>
        <node name="DirectoryFilters">
            <node name="All Directories">
                <property name="RegExp">^.+$</property>
                <property name="Mode">ALLOW</property>
                <property name="Permissions">FAA_CONNECTION_RO;FAA_CONNECTION_EDIT</
property>
            </node>
        </node>
    </node>
    <node name="root - Temporary files">
        <property name="name">Temporary files</property>
        <property name="path">{$bisas.temp}</property>
        <property name="readonly" type="java.lang.Boolean">false</property>
        <node name="FileFilters">
            <node name="TXT Files">
                <property name="RegExp">^.+$</property>
                <property name="Mode">ALLOW</property>
                <property name="Permissions">FAA_CONNECTION_RO;FAA_CONNECTION_EDIT</
property>
            </node>
        </node>
        <node name="DirectoryFilters">
            <node name="All Directories">
                <property name="RegExp">^.+$</property>
                <property name="Mode">ALLOW</property>
                <property name="Permissions">FAA_CONNECTION_RO;FAA_CONNECTION_EDIT</
property>
            </node>
        </node>
    </node>
</config>
```

The configuration file is placed in the *SeeConfig\{com.seeburger.conf.user=BISAS}\{com.seeburger.fileaccess=FileAccessSystem}* directory.

The configuration file may contain any number of root definitions. This is the layout of each root definition:

```
1 <node name="root - Log files">
2     <property name="name">Log files</property>
3     <property name="path">{$bisas.log}</property>
4     <property name="readonly" type="java.lang.Boolean">false</property>
5     <node name="FileFilters">
6         <node name="TXT Files">
7             <property name="RegExp">^.+$</property>
8             <property name="Mode">ALLOW</property>
9             <property name="Permissions">FAA_CONNECTION_RO;FAA_CONNECTION_EDIT</property>
10        </node>
11    </node>
12    <node name="DirectoryFilters">
13        <node name="All Directories">
14            <property name="RegExp">^.+$</property>
15            <property name="Mode">ALLOW</property>
16            <property name="Permissions">FAA_CONNECTION_RO;FAA_CONNECTION_EDIT</property>
17        </node>
18    </node>
19 </node>
```

1 - The logical name (free text) of the root definition.

2 - The display name of root node (visible in RemoteFileChooser).

3 - The absolute path that logical root must point to.

4 - The read only flag.

5 - The file filters section. Each section should contain at least one filter. Each filter definition should have:

6 - The logical name (free text) of the filter.

7 - The regular expression that should match the browsing files.

8 - The mode - ALLOW (include) or DENY (exclude) the matched files.

9 - The permissions that the user has to own (to match the filter). The user has to own at least one permission (logical "OR" combination).

12 - The directory filters section. Each section should contain at least one filter. Each definition is the same as the file filter definition described above.

Note: The file and directory filter sections may contain many filters in many combinations - to include some group of files/directories and exclude others.

The current root configuration may be exported from the database to the *BIS/temp* directory by running the export-config script placed in the *BIS/software* directory. After modification of the configuration file, the changes should be imported to the database again by running the import-config script.

10.5 Startup Phase

When restarting the BIS system, you may notice that start up phase sometimes requires more time. One reason could be, that you have deployed a new process solution during BIS downtime which gets deployed to the runtime system. Another reason could be, that you have open transactions (processes in state running, recovery jobs) that are now prepared for continuation.

Check if the startup of BIS was successful by opening a new BIS FrontEnd session and checking if the BIS system starts processing and finishes processes. Check the control center in the BIS FrontEnd if the activated BIS adapters are in state READY. Search for ERROR's in the BIS log files, if you think that the startup phase was not successful. See the next topic if you find Oracle specific error messages about in-doubt transactions (Oracle error code: ORA-01591). You have to shutdown all of your BIS instances and to keep them offline until you have cleared the in-doubt transactions.

Simultaneous Starting of Multiple Instances

The simultaneous start of multiple instances can cause problems. Therefore, until it is improved upon in an upcoming version, when you want to start multiple instances it is advisable to use the following procedure:

1. Start the Adminserver.
2. After a short waiting period of 60-90 seconds, start the next instance. The wait time is system dependent, and in individual cases may require the wait time to be increased further.
3. For each instance thereafter, please wait approximately 30 seconds.

Oracle In-doubt-Transactions (when running the BIS with Oracle database):

A transaction in Oracle can acquire the state in-doubt after a system application or Oracle crashes, or network error occurs. Oracle will in most cases automatically resolve in-doubt transactions, but in some cases a manual solution is needed. A transaction which is not fully finished (in-doubt) can hold locks on tables (records, index, pages) that prevents accessing them. In a worst case scenario an application may stop working until the in-doubt transaction is resolved.

SEEBURGER recommends to automate the rollback of in-doubt transactions. Please refer to the manual *BIS with Oracle [Resolving In-Doubt Transactions]* for details.

in addition, please check prior to starting BIS for In-doubt-Transactions. The following SQL statements assist to localize and solve the problem.

(We recommend executing the commands for every start up procedure automatically over a script.)

- SQL statement which queries in-doubt transactions:

```
SELECT local_tran_id from dba_2pc_pending where state= 'prepared';
```

- SQL statement which rolls back an in-doubt transaction:

```
ROLLBACK FORCE 'transaction_id';
```

Before attempting to roll back the in-doubt distributed transaction, ensure that you have the proper privileges. Note the following requirements:

User who commits the transaction	Required privilege
You	FORCE TRANSACTION
Another user	FORCE ANY TRANSACTION

An example of an error message is shown below.

```
@LGW800     2008-10-10T13:09:08.356+0200 org.jboss.jms.asf.StdServerSession
JB21:04:24,28     JMS SessionPool

Worker-358  LOCALHOST  ERROR                         failed to commit/rollback

org.jboss.tm.JBossRollbackException:         Unable         to         commit,
tx=TransactionImpl:XidImpl[FormatId=257,           GlobalId=s088a8510/113219,
BranchQual=, localId=113219] status=STATUS_NO_TRANSACTION; - nested throwable:
(javax.ejb.EJBException: Store failed)

at org.jboss.tm.TransactionImpl.commit(TransactionImpl.java:372)
at org.jboss.tm.TxManager.commit(TxManager.java:240)
at org.jboss.jms.asf.StdServerSession.onMessage(StdServerSession.java:351)
at
org.jboss.mq.SpyMessageConsumer.sessionConsumerProcessMessage(SpyMessageConsumer.
java:902)
at org.jboss.mq.SpyMessageConsumer.addMessage(SpyMessageConsumer.java:170)
at org.jboss.mq.SpySession.run(SpySession.java:323)
at org.jboss.jms.asf.StdServerSession.run(StdServerSession.java:194)
at                        EDU.oswego.cs.dl.util.concurrent.PooledExecutor
$Worker.run(PooledExecutor.java:748)
at java.lang.Thread.run(Thread.java:595)
Caused by: javax.ejb.EJBException: Store failed
at
org.jboss.ejb.plugins.cmp.jdbc.JDBCStoreEntityCommand.execute(JDBCStoreEntityCom
mand.java:158)
at
org.jboss.ejb.plugins.cmp.jdbc.JDBCStoreManager.storeEntity(JDBCStoreManager.java
:666)
at
org.jboss.ejb.plugins.CMPPersistenceManager.storeEntity(CMPPersistenceManager.jav
a:428)
at
org.jboss.resource.connectionmanager.CachedConnectionInterceptor.storeEntity(Cach
edConnectionInterceptor.java:273)
at org.jboss.ejb.EntityContainer.storeEntity(EntityContainer.java:749)
at org.jboss.ejb.GlobalTxEntityMap$2.synchronize(GlobalTxEntityMap.java:149)
at                                         org.jboss.ejb.GlobalTxEntityMap
$GlobalTxSynchronization.synchronize(GlobalTxEntityMap.java:295)
at                                         org.jboss.ejb.GlobalTxEntityMap
$GlobalTxSynchronization.beforeCompletion(GlobalTxEntityMap.java:345)
at org.jboss.tm.TransactionImpl.doBeforeCompletion(TransactionImpl.java:1491)
at org.jboss.tm.TransactionImpl.beforePrepare(TransactionImpl.java:1110)
at org.jboss.tm.TransactionImpl.commit(TransactionImpl.java:324)
... 8 more

Caused by: java.sql.SQLException: ORA-01591: Sperre wird von unterbrochener,
verteilter Transaktion 21.33.224760 aufrecht gehalten.
```

Note: For further information, refer to: *http://download.oracle.com/docs/cd/B28359_01/server.111/b28310/ds_txnman005.htm*

10.6 Securing Connections Between BIS Components

Up to version BIS 6.5.1 there was an option ("DMZ Security") to secure the communication between the Node and the CI using an SSH tunnel. With version BIS 6.5.2 this option is removed. A redesign of your landscape, adding the BIS Secure Proxy, will make securing these connections obsolete.

Instances with communication adapters (Role Adapter Engine, formerly called Nodes) now can be moved to the internal network zone next to the instance with the Admin Server (formerly CI) role.

The external communication then can be secured and tunneled through the firewall using the BIS Secure Proxy. For details about how to integrate BIS with the BIS Secure Guide, see the BIS Secure Proxy guide.

10.6.1 Introduction

SEEBURGER BIS Secure Proxy (formerly known as SEEBURGER Secure Edge) is SEEBURGER's proxy and reverse proxy product, which secures the customers EDI, B2B and MFT communication. It provides a high level of data protection between external connections and your internal network.

Secure Proxy is able to secure

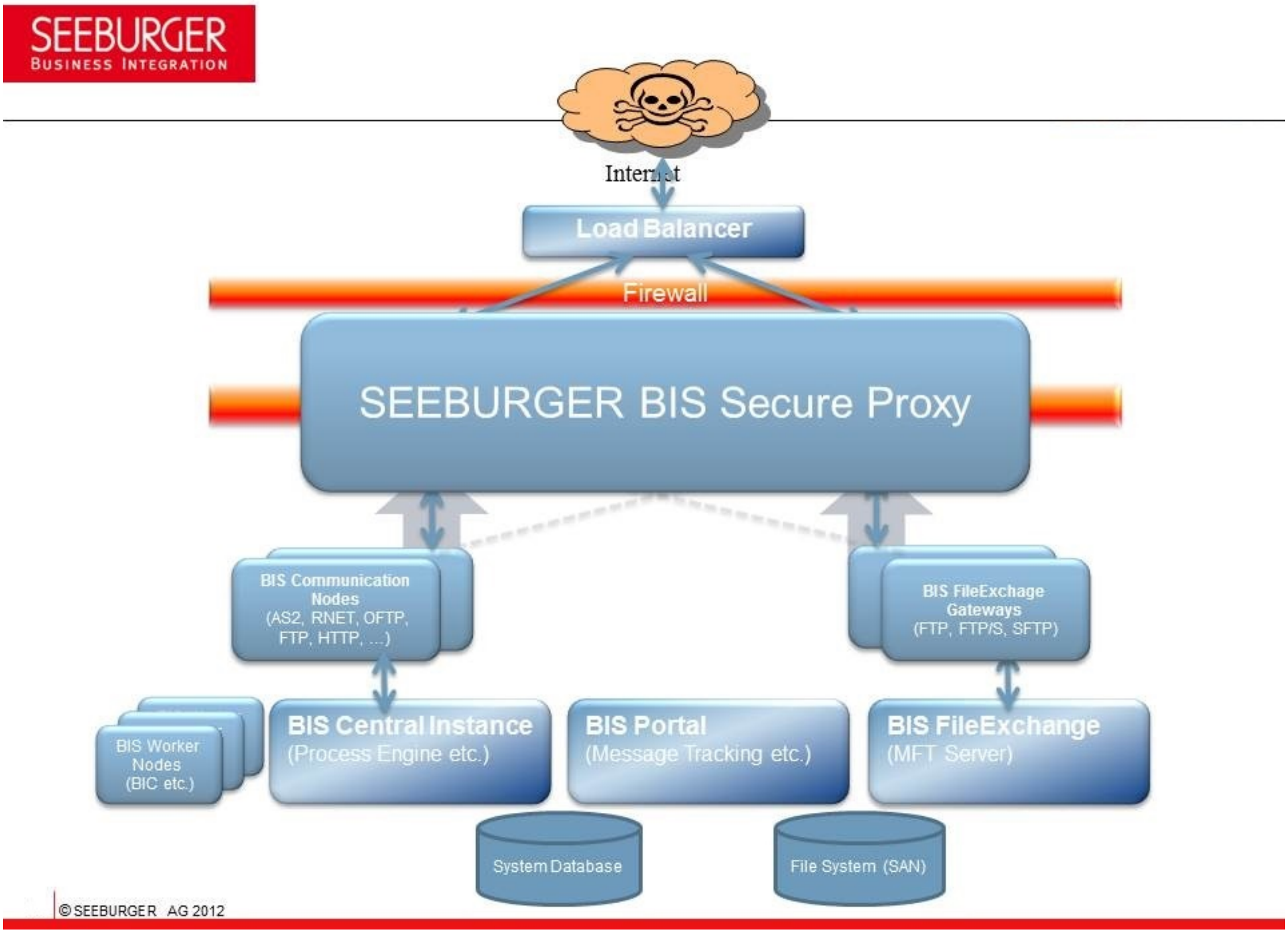
- the communication between BIS and the communication partner (for in- and outgoing transaction)
- the BIS FileExchange infrastructure
- the BIS Link Manager infrastructure

For BIS6 communication adapters, there are 2 options for integrating Secure Proxy.

- The preferred option is: Use the Secure Proxy Integration.
  - This option works for client and server adapters (e.g. HTTP client adapter and HTTP controller adapter)
  - How do I configure this? Select/activate the BIS Secure Proxy in the adapters connection configuration master data.

- The other option is: Configure and use the SOCKS Proxy Server Plugin of BIS Secure Proxy .
  - This option works only for client adapters which are able to connect to a SOCKSv5 proxy (e.g. OFTP Client)
  - How do I configure this? Select the configured SOCKS proxy in the adapters connection configuration master data

- If an adapter supports both options, always use the Secure Proxy Integration.


SEEBURGER
Business Integration
Internet
Load Balancer
Firewall
SEEBURGER BIS Secure Proxy
BIS Communication Nodes (AS2, RNET, OFTP, FTP, HTTP, ...)
BIS FileExchage Gateways (FTP, FTP/S, SFTP)
BIS Worker Nodes (BIC etc.)
BIS Central Instance (Process Engine etc.)
BIS Portal (Message Tracking etc.)
BIS FileExchange (MFT Server)
System Database
File System (SAN)
© SEEBURGER AG 2012

Securing the Connection Between the BIS AdminServer and the BIS Portal/Front-End

In order to secure access to the Admin Server instance (for the Front-End, Mapping Designer or Developer Studio) the HTTPS listener must be enabled. The steps for enabling the listener, and then securely accessing the Portal/Front-End are as follows:

1. Log into the Portal/Front-End insecurely.
2. In Front-End go to Configuration -> System settings -> HTTP services and start the HTTPS listener.
3. Optionally you can use the Key Store Manager to generate/upload a specific X.509 certificate for this listener.
4. Close the Front-End and log out from Portal
5. Log back into the Portal using the secure port (8443 by default).
   Accessing the Front-End via a secure Portal will automatically create a secure connection to the Front-End.

Note: HTTP and HTTPS services are provided by the BIS 6 server on different ports. If *HTTPS* is chosen, the port for the secure connection must be specified. The default port is *8443* for secure connections, and *10000* for normal connections. These ports are specified in the *ports.properties* file of the Admin Server instance.

Securing the Connection Between the BIS AdminServer and BIC Mapping Designer

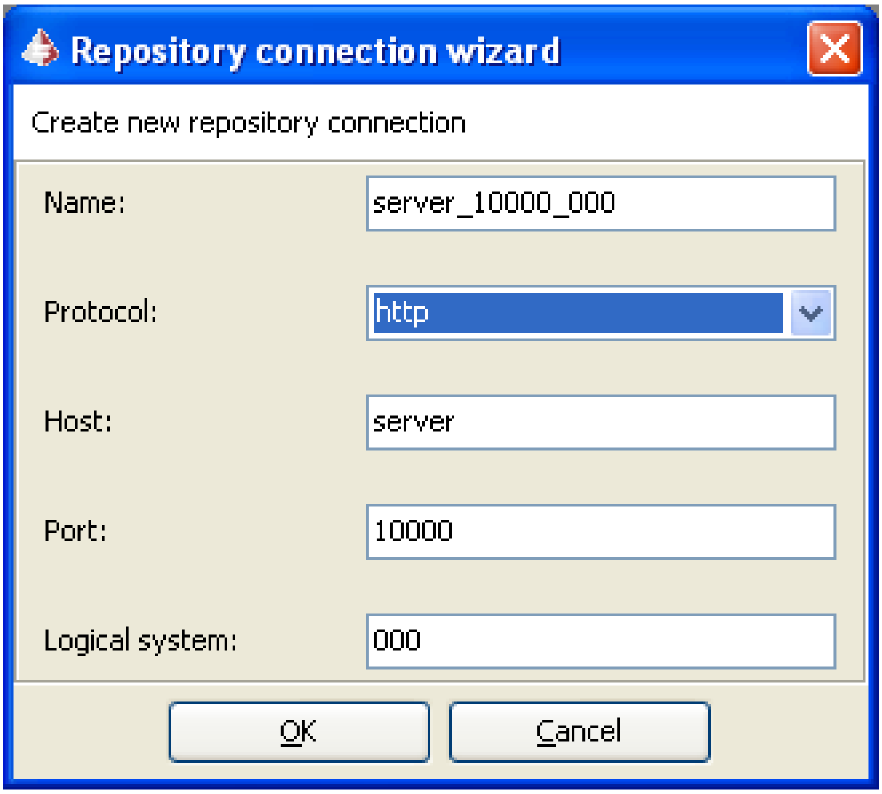
10.7 Creating a Repository Connection

Note: You need the following permissions: *SOURCE_REPOSITORY_VIEW* or *SOURCE_REPOSITORY_ACCESS.*

For use of the repository, it is required to specify the location of the server. The location has to be created by a right-mouse-click on the BIC Mapping Designer's Explorer tree (*Context menu* | *Repository* | *Manage repository connections*). The name, protocol, host address, port and logical system must be entered here.

In the *Repository Connection Wizard* dialog, you have to define the host, port, protocol, logical system and an alias name for that connection. The alias name is *host_port_ls,* if you do not change it. If a combination of *host port* and *logical system ID,* or the alias name already exists, you cannot click on the button *OK*. The wrong field is highlighted in red.

With the click on *add* the follwoing dioloag is open, to create a new repository connection:



Repository connection wizard

Create new repository connection

Name: server_10000_000

Protocol: http

Host: server

Port: 10000

Logical system: 000

After clicking on the button *OK*, you have to authenticate against the server you entered (please refer to the topic *Authentication*). If you authenticated successfully, the connection is saved, otherwise you will receive an error message that the connection test failed, and the connection is not saved. The same happens, if you click on the button *Cancel*.

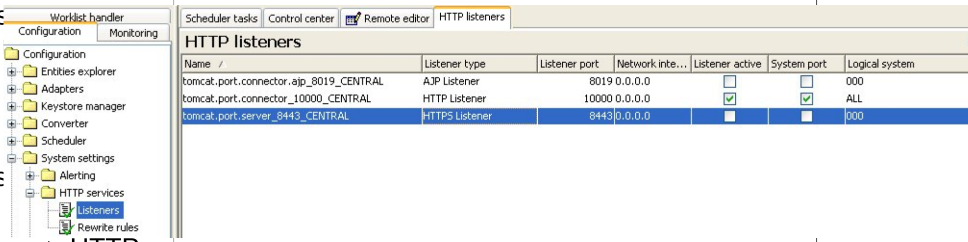
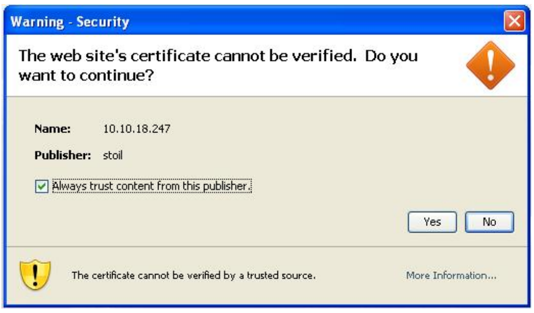
The repository connection between the Mapping Designer and the BIS server is not secure/encrypted by default. If the information travels along insecure channels, but security is required, it is possible to switch to a secure SSL connection. In order to use a secure connection, you need to:

- Choose *HTTPS* as a connection protocol.
- Choose the port the BIS Server uses for SSL connections (normally 8443).

With these two steps an https connection is configured.

Securing the Connection Between the BIS AdminServer and Process Designer

Besides the normal connection, a secure connection (HTTPS) to the back-end is supported as well. The HTTPS connection can be chosen by checking the *Use HTTPS* check box from the *Connection Preferences* screen.

Instruction	Illustration
By default, an insecure connection is us you can use a HTTPS connection, you start the HTTPS listener of the BIS and download the SSL Server Certificate to computer: 1. Log-in to the BIS back-end using ins (HTTP) and start the *Front-end*. 2. Goto Configuration -> System settings -> HTTP services and start the HTTPS listener. 3. Log-in to the BIS back-end using HTTPS and start the *Front-end*. The certificate has to be accepted and the check box *Always trust content from this publisher* has to be checked (this is needed and used by the Process Designer to create a HTTPS connection). 4. Choose *HTTPS* as connection type from the connection preference page.	 Worklist handler Configuration Monitoring Configuration Entities explorer Adapters Keystore manager Converter Scheduler System settings Alerting HTTP services Listeners Rewrite rules Scheduler tasks Control center Remote editor HTTP listeners HTTP listeners Name / Listener type / Listener port / Network inte... / Listener active / System port / Logical system tomcat.port.connector.ajp_8019_CENTRAL / AJP Listener / 8019 / 0.0.0.0 / □ / □ / 000 tomcat.port.connector_10000_CENTRAL / HTTP Listener / 10000 / 0.0.0.0 / ☑ / ☑ / ALL tomcat.port.server_8443_CENTRAL / HTTPS Listener / 8443 / 0.0.0.0 / □ / □ / 000  Warning - Security The web site's certificate cannot be verified. Do you want to continue? Name: 10.10.18.247 Publisher: stoil ☑ Always trust content from this publisher. The certificate cannot be verified by a trusted source.

10.8 Maintenance Procedures

10.8.1 Rollback to an older version

If a rollback to an older service pack release becomes necessary, the following procedure needs to be followed: Please note that such a rollback should only be done in a serious emergency and should be tested beforehand in a test environment.

All steps need to be executed on all instances in a system, starting with the AdminServer:

1. Use the installation media of the target version (older Service Pack) and execute **Upgrade** installation. The downgrade warning in the setup needs to be ignored.
2. Use the same installation media and repeat the installation, this time in **Repair** mode.
3. Install all needed hotfixes.

Note: Rolling back the installation is most reliable if the BIS was not running with the new version and no modifications to persistent database data has been done. A later roll back is still possible in the same manner, however, it can not be guaranteed that no incompatible changes to database content where applied. This might lead to processes that can not be processed completely.

Note: In any case, in order to prevent and avoid data loss, a manual check for missing, stuck or failed transactions is necessary.

10.8.2 Modifying Database Password/User/Location via the bisadm-db script

You can use the `<BIS6_HOME>/software/bisadm-db.(bat,sh)` command line tool to change how BIS connects to its system databases. After starting the script, you will be asked to choose from several commands:

list - provides a list of systems databases (System DB Accounts) used by BIS.

change - starts a step-by-step procedure which will change how ALL BIS instances in the system create their runtime connections to that particular database. On each step, you will be asked for part of the connection information (URL, password, username). If a blank value is entered, the old one will be used.

local-change - a step-by-step procedure which will change how this particular BIS instance connects to the main BIS database (for scripts and start up) As with the "change" command, you will be asked for parts of the connection information in several steps. Providing a blank value means the old value will be used.

help - prints help about each command.

If you want to change your database user/password/location, you can follow those steps:

1. Gracefully shut down all BIS instances that use the affected database (if it is the main BIS database, this means ALL instances).
2. Optional if re-using the runtime user: change the password of the database login via the appropriate 3rd party DB management tool.
3. Use the "local-change" command to adjust the connection settings on all instances of the system. Make sure to run the register script on each.
4. Use the "change" command to apply the changes to the affected DB account on the admin server.

Note: If the schema user of a database has the same name as the runtime user, make sure you change both passwords – the runtime password and the schema password - to the same value.

10.8.3 Modifying Database Password/User/Location via manual steps

You should use the guided `bisadm-db` script as described above, however the following description details the manual steps needed to adjust parameters of the system database. The procedure applies to AdminServer and all other instances and requires a shutdown:

1. On each BIS instance change the database password of the runtime and/or owner user the file `<BIS6_HOME>/software/register.properties` file. It is recommended to use the `<BIS6_HOME>/software/propedit.{bat,sh}` application which does the modification and encoding of the password.

Note: If you have a system without a GUI, you need to change the password manually in the file `<BIS6_HOME>/software/register.properties`. This file should be modified on each instance. Remember the password needs to be encoded before putting into register.properties. To encode a password use `<BIS6_HOME>/software/encode-password.{bat,sh}`.

2. Safe-Shutdown all BIS Process and Adapter Engine instances

3. Stop Scheduler Service on Admin Server

a. From the http portal (<host>:10000) navigate to *JMX Console.*

b. Find quartz entry in the left pane (usually the last one in the list)

c. Click on the link instance=ADMIN,name=InstanceScheduler,type=QuartzScheduler on the right

d. Scroll down to the *shutdown* operation and press button *Invoke*

5. In Front-End Change System Settings / System DB Accounts / MASTER_ACCOUNT. Make sure to modify all other accounts which need to be changed as well.

6. Shut down the complete BIS installation (the remaining AdminServer).

7. Optional if re-using the runtime user: change the password of the database login via the appropriate 3rd party DB management tool.

8. Execute `<BIS6_HOME>/software/register.{bat,sh}` on each instance of the Landscape.

9. Start BIS AdminServer and instances.

Tip: In order to decouple the time dependency between shutdown, change in the database and reconfiguration, you can ask your database administrator to create a new runtime user with the new password. This way you can use olduser+oldpassword and newuser+newpassword in the transition period in parallel. You can drop the old user once the changes have been completed. This works specifically well for a Microsoft SQL Server, where a single database can have multiple log-ins assigned. Make sure the new user has all corresponding permissions and the same default database assigned. For Oracle this especially means the login trigger is available and the user has granted access to all tables and views.

If you cannot use the Front-End to modify the database settings (step 5) you can also use a database management/query tool to modify the settings directly in the table `tDSAccounts`. Make sure to use the encoded password for the `cPassword` column. You need to specify the runtime user with the associated password.

Depending on your installation, there might be other places where the database configuration is stored. This includes:

1. BIS user database sources (configured in the Front-end and stored in SeeConfig).
2. Hard-coded in BIC mapping code, BIC code files or Java. (This is not recommended; use BIS 6 data sources URLs for BIC instead.)

Note: If you miss to update the database configuration in some places (especially the instances), the system might continue to work. However, you may experience problems like the system not reacting to changed master data, or missing recovery information.

10.8.4 Instance Upgrade after Switching Off the HTTP Ports

If, after installing another instance, you disable the http port via the http port and only allow communication via https,You must modify the <BISAS_HOME> /software/spm-repository.properties file on the instances for an update after the change.
After the installation via http port, there are 3 properties in this file:

```
...
spm.repository.type=http
...
spm.repository.host=<hostname
...
spm.repository.port=10000
```

The port must be adapted for the update via https.

The following properties must also be added:

```
                #@IASTART=spm.repository.encrypted
#@IATYPE=textfield
#@IALONGDESC_EN=SPM Repository TLS encryption indicator
#@IALONGDESC_DE=SPM Repository TLS encryption indicator
#@IASHORTDESC_EN=SPM Repository TLS encryption
#@IASHORTDESC_DE=SPM Repository TLS encryption
spm.repository.encrypted=true
#@IAEND=spm.repository.encrypted
```

```
                #@IASTART=spm.repository.trusted
#@IATYPE=textfield
#@IALONGDESC_EN=SPM Repository TLS trusted indicator
#@IALONGDESC_DE=SPM Repository TLS trusted indicator
#@IASHORTDESC_EN=SPM Repository TLS trusted
#@IASHORTDESC_DE=SPM Repository TLS trusted
spm.repository.trusted=true
#@IAEND=spm.repository.trusted
```

When spm.repository.trusted=false, Then the path to the Certificate must also be added:

```
                #@IASTART=spm.repository.certpath
#@IATYPE=textfield
@IALONGDESC_EN=SPM Repository certificate path
#@IALONGDESC_DE=SPM Repository certificate path
#@IASHORTDESC_EN=SPM Repository certificate path
#@IASHORTDESC_DE=SPM Repository certificate path
spm.repository.certpath=<Path to certificate>
#@IAEND=spm.repository.certpath
```

10.8.5 Copy System Database Content

If you want to move/copy the content of a BIS system database you can use the following procedure. This uses BIS im/export tools and might therefore not be the fastest option. It is recommended to use database native tools if possible.

1. Shut down the complete BIS installation (instances and AdminServer).
2. Execute `<BIS6_HOME>/software/db/backupDB.{bat,sh} -nolist ALL`

This will produce a new back folder named `<BIS6_HOME>/software/db/backup.YYYYMMDDhhmmssfff` which contains one `*.dat` file per table.

The following procedure applies to restore this data into a new empty schema:

1. Change the register.properties to point to the new schema (bisadm-db local-change).
2. Make sure the tables are created (empty): <BIS6_HOME>/software/installdb/installdb.{bat,sh}
3. Clean all files from <BIS6_HOME>/software/db/data/ and move content from backup folder into it
4. Run *<BIS6_HOME>/software/restoreDB.{bat,sh} -nolist ALL*

Modifying the Installation Directory (Moving, Cloning, Restoring)

There are multiple reasons to change the installation directory of an existing BIS 6 system:

- You want to move the installation to a better location (naming conventions or file storage).
- You have restored a backup or copied (cloned) to an intermediate location, and want to start this instance.
- You have copied an existing instance installation to a new location and want to use it as an additional instance.

All of the cases above are described in the following sections. Please remember that you also need to use a new system database, if you want to start up a new installation independent from the existing. Modify the database parameters (as described in *Modifying Database Password* or *Parameters*) to point to a new system database instance/schema user. The new database has to contain the same tables as the original installation.

After you copy or move the instance with Admin Server role you need to check the following files for the old path:

```
<NEWBIS6_HOME>/software/keystore.properties
<NEWBIS6_HOME>/software/register.properties
```

Then you need to run `<NEWBIS6_HOME>/software/register.{bat,sh}`, followed by `<NEWBIS6_HOME>/software/update-config.{bat|sh}`, which will update all locations where the fully qualified path name is stored. This is especially the file `<NEWBIS6_HOME>/bin/bis-env.{bat,sh}`. You also need to re-install the BIS 6 Service. (using Windows Service Setup).

For the mapping repository, the `com.seeburger.repository-config.xml` file has to be checked for an old path:

1. Run `<BIS6_HOME>/software/export-config.{bat,sh}`
2. Change the old JvmPath in file `<BIS6_HOME>/temp/SeeConfig/{com.seeburger.conf.user=BISAS}/com.seeburger.repository-config.xml`
3. Execute `<BIS6_HOME>/software/import-config.{bat,sh}`

Tip: To be on the safe side, you can search in all text files (especially **.xml* and **.properties*) of the new installation for the old path name, and verify if all locations are updated correctly.

Most places in the BIS 6 master data and configuration of the AdminServer can use the system variable `${bisas.data}` and therefore are independent of the actual installation location. This especially includes the hotfolder location configuration in the BIS 6 GUI as well as any file path in the TPM. However, if you do not use this convention, you need to check all the possible file related master data settings for the old path.

Note: If you clone an instance installation in order to add one more instance to an existing BIS 6 configuration, you do not need to modify the database settings, however in this case you have to modify the `INSTANCE_ID` and (optionally) `instance.group` stored in `<NEWINSTANCE_HOME>/software/profile.properties` before running the `register` script.

Note: If you create a new adapter engine instance (by cloning) the adapters of this instance may not be assigned to queues automatically.

If you want to have a **clean installation** (instead of moving an existing system) it is recommended to also delete the following files and directories:

<NEWBIS6_HOME>/
  temp/
  log/
  data/dt/

data/<instance-ID>
data/FileAccessAdapter/
data/bismt/
data/hotfolder/
data/webdav/seediaf/ (not WEB-INF/)*
domain/servers/<instance-ID>/

The above directories will not contain configuration, customization, mappings or processes. But it will remove all open and finished transactions. This means you should additionally clean out the following database tables:

tBPInstances
tBPAttach
tBPAttachProc
tBPRestartPoints
tBPRestartPointsOpt
tBPTimeout
tBPTimers
tBPWaitMsgs
tBPWaitInst
tBPFault
tMonitorErrors
*tMsgIDStore**
*tWLHOrder**
tJMSFailures
tJMSExceptions tInboxTasks tStoredMessages

tMessageHistory

The **DIAF data source pool** is special. In the default configuration instances are configured to use HTTP to the AdminServer, and the AdminServer is configured to use the local file system. This configuration includes system variables `${bisas.data}`. So this means if you did not make any changes to this constellation, you do not have to do additional steps to move the shared data store. However, if you have modified this (typically if you change the instances to use the `<NEWBIS6_HOME>/data` directory via file system, or if you have moved the DIAF store to a shared file system (NFS or Cluster), you might want to review and correct the path settings for the AdminServer and for the instances.

The AdminServer used the DIAF settings from the database. So you need to run `export-config.{bat,sh}`, modify the file

```
<NEWBIS6_HOME>/temp/SeeConfig/{com.seeburger.conf.user=BISAS}/
  {com.seeburger.diaf=ResourceProviders}/com.seeburger.diaf-config.xml
```

and run `import-config.{bat,sh}` after that. This will update the configuration of the AdminServer in the database. If the instances are not usingWebDAV/HTTP, they need a new version of this file as well. It can be the same content as the file you just modified, or it might be different, depending on the file system layout on the instances. It is important to note that you cannot use `${bisas.data}` in the instances copy of this file (since it will be relative to the remote instance and not to the admin server).

Depending on your installation you might need to modify the installation path to your BIS AdminServer or instance (especially startup- and stop scripts as well as log directory or PID file) in additional places like cluster manager scripts and config; system monitoring and management; system startup (init) scripts (especially the file you created based on `<BIS6_HOME>/bin/bis`) or (Windows) service. The same is true for eventual copies of the `run-bisas.{bat,sh}` file.

⚠ **Warning:** All changes to the file system of the AdminServer have to be done to all possible installations. This is especially important if you have a fail-over cluster setup, where you have installed BIS 6 AdminServer multiple times on the local file system. Because otherwise your modifications might not be in effect if the cluster fails over. (This is not a problem, if you make the modifications on a shared file system like NFS, Clustered or Fail-over).

10.8.6 Modifying IP Addresses or Ports of AdminServer or instance

If you want to change the IP Address of a computer running a BIS 6 instance or the AdminServer you only need to touch the configuration, if you have specified this IP Address anywhere in the config. The typical case for this is Master Data for DT Listeners (OFTP TCP/IP, FTP Server, HTTP Listener). If you stick with the same host names, you do not need to make any changes to the other system configuration.

If you want to change the **Host name, or the BIS 6 Instance running on a computer, or some configured ports**, you need to change the following configuration on the AdminServer: All networking related settings can be found in the file:<BIS6_HOME>/software/ports.properties. Replace the old host name or port with the new one, and run register.{bat,sh}. In addition to that, you need to replace one database configuration with a modified version. To do that follow these steps:

1. Stop BIS
2. Run <BISAS_HOME>/software/propedit (cmd/sh)
3. Adjust the port and save.
4. Run <BISAS_HOME>/software/register (bat/sh)
5. Start BIS

Note: If you move an AdminServer instance to a machine with a new host name, you most likely invalidate the license file. Make sure to request a temporary and permanent new license for the new host name, otherwise you cannot log into the Front-End after the move.

If the configuration of the AdminServer changes, you need to update the instances as well. This can be done by following these steps:

1. Adapt `<INSTANCE_HOME>/software/ports.properties`.
2. Run `<INSTANCE_HOME>/software/register.{bat,sh}`.

Note: If you change the HTTP port of AdminServer Instance, it is needed to change the port manually on each instance.
The easiest way to do that is to run an update on each instance. Note to select the "update" option and not the "patch" option. During the installation course you need to change the repository URL, as well as the http port in the properties file editor screen later on.

10.8.7 Installation of Additional Modules/Articles

If you need to install additional modules in an existing BIS 6 installation, you need to follow the setup wizard as during an upgrade installation. To add additional modules you need to start the setup routine from within the installation home directory:

```
<BIS6_HOME>/software/spm-repository/installer/<platform>/setup.bin
<BIS6_HOME>\software\spm-repository\installer\win64\setup.exe
```

In the Repair/Upgrade screen you should select *Upgrade* as the installation mode. Extending an already existing installation does not modify existing binaries. But the register process will touch and rebuild some configuration data, and in some cases the connected database. Therefore a backup of the file system and database is strongly recommended. Make sure to shutdown each instance before using the installer on it. It is recommended to exercise the extension on the QA environment.

⚠ **Attention:** After installing additional modules you must reinstall the previously applied hotfixes to the system.

10.8.8 Restoring Files from a Backup after an Upgrade

⚠ **Warning:** The following topic is for expert usage only. It is highly recommended to contact SEEBURGER before you are restoring data from a back-up. Furthermore you should ensure that you have a full back-up of your system and database before you follow the instructions of this topic.

Each upgrade performed with the BIS setup routine is writing a back-up of all upgraded files. The back-up of the files can be located in a directory with a 13 digit time stamp in the directory:

```
<BIS6_HOME>/software/backup
```

The higher the number of the time stamp, the newer the back-up.

For each technical article you will find a sub directory named like the technical article itself. In those folders you will find the back-ups of the files that have been overwritten during the setup routine. Files are stored in the same folder structure like they have been stored in the original installation folder.

If you need to rollback changes done during an upgrade, you will have to copy the contents of the technical articles into the installation folder.

⚠ **Warning**: Files that have been newly introduced in an upgrade scenario are not deleted by this kind of restore. You will have to delete them manually if required.

⚠ **Warning**: Database changes that have been introduced in an upgrade scenario are not rolled back by this kind of restore. You will have to roll back the database changes manually if required.

Besides the files that are extracted during the setup routine, the setup also modifies so called property files. Namely those are:

- `<BIS6_HOME>/software/register.properties`
- `<BIS6_HOME>/software/vm.properties`
- `<BIS6_HOME>/software/ports.properties`
- `<BIS6_HOME>/software/cache.properties`

You can find back-ups of the property files in the same folder with the extension ".bak"

To compare the changes made in files during upgrades, you can use a common file comparison utility. Most Unix and Linux systems do have an installed tool called *diff* which can be used for such a task.

10.8.9 Modifying Maximum Size of Inspector Queries

The Inspector is by default restricted to a maximum of 10000 items for a single query. Standard views like *All processes* are restricted to 1000 items which cannot be changed. For filters the amount of items to be returned at most are configurable up to a limit of 10000.

⚠ **Warning:** Changing the limit can have a serious impact on the performance of the BIS system.

1. To change the limit the inspector had to be open at least once. Then execute the script: *<BIS6_HOME>/software/export-config.{bat,sh}*

2. Modify the file `<BIS6_HOME>/temp/SeeConfig/CENTRAL/{com.seeburger.conf.user=BISAS}`*`/com.seeburger.inspector-config.xml`*
   The file contains a property `maxResultsetRows` which defines the maximum number of items to be returned by a query.

3. Save the changed file and run the script to import it: `<BIS6_HOME>/software/import-config.{bat,sh}`

10.8.10 Undeploy Roles from an Instance

You can remove ("undeploy") roles from an existing instance. This is especially useful after updating a BIS 6.3 "Central Instance" because you might not want to run processing on the resulting Admin Server. You can do this with an Update Installation (supported since 6.5.2 Q6):

- Shutdown Instance with Admin Server and other Roles
- Start Installer from `software/spm-repository/installer/<OS>/setup.{exe,bin}`
- The instance home directory is automatically selected, press next.
- On the "Installation Found" screen select the "Upgrade/Extend" method.
- On the roles screen deselect the Process Engine and/or Adapter Engine roles.
- Continue with the upgrade tool (do not modify any settings or article selections).
- After finishing the installer, start the instance again.

Note: if you use the Admin Server as (DIAF) file storage all instances need to be shutdown first.

10.8.11 Moving an Admin Server instance to another host

If you want to relocate the instance with the Admin Server role you can use the following procedure. This is typically done after an upgrade when you have undeployed Process Engines from the former central instance. In this case you typically want to move the installation to a smaller system.

It is important to keep the Hostname of the previous machine. If you use virtual machines it is recommended to re-size the VM and not move the installation instead.

1. Shutdown AdminServer instance
2. Move the Instance home (the whole BIS installation folder) to a new (smaller) server.
3. Shutdown or rename the old machine, rename the new machine to the existing host name.
4. If you cannot move the IP Addresses reconfigure them like described above.
5. After finishing the move, start the instance again. (You might need to re-do the operating system service startup procedure)

Note: if you used the Admin Server as (DIAF) file storage, you will have to shutdown all instances first. Also keep in mind that in this case you will have to move all archived process payloads to the new server. It is recommended to setup and use an external distributed file store before you move the admin server to avoid this.

10.8.12 Changing database connection retry duration (PersistenceLayer)

In case the database connection has been lost the PersistenceLayer tries to re-establish the connection for a certain amount of time before throwing an exception. The default value is 10 seconds. It can be configured in two ways: Either by setting the VM parameter *-Dcom.seeburger.pl.retrysec* or changing the value in the corresponding configuration file which is used for all instances. If the VM parameter is set, it overwrites the value read from the configuration file. In order to change the value in the configuration value the following steps needs to be be executed:

1. Execute the following script on the instance with role admin server: `<BIS6_HOME>/software/export-config.{bat,sh}`
2. Modify the file `<BIS6_HOME>/temp/SeeConfig/{com.seeburger.conf.user=BISAS}/{com.seeburger.conf=PLConfig}/com.seeburger.database-config.xml`
3. Save the changed file and run the script to import it: `<BIS6_HOME>/software/import-config.{bat,sh}`
4. Restart all instances.

10.8.13 Modifing InstanceID on upgrade

If it is needed to modify the InstanceId, you must not do this before upgrade procedure from 6.3.5 to 6.5.2. You can do it in the follow way:

1. Upgrade the 6.3.5 without any manual changes on properties files.
2. If upgrade is finished, change the instance.id property in the file `<BIS6_HOME>/software/profile.properties`
3. Run `<BIS6_HOME>/software/register.{bat,sh}`

10.8.14 Removing Instances from System

In case there are instances in the system, that were taken out of service for good, you may want to remove them from the list of known instances to clean-up, e.g. dashboard's landscape view.

To do so, you can use JMX-console, by navigating to MBean `com.seeburger.landscape.impl.jmx:service=LandscapeManagement` and invoking method `deleteInstanceFromDB` with the instanceID of the instance that should be removed. Note that this is only possible for instances that are in state "Out-Of-Service" to prevent the accidentally removal of running instances.

An alternative approach is to do the same via database query, like: `DELETE FROM tLandscape where cInstanceID='<insert ID here>';`

Please keep in mind that there might be master data referencing such a removed instance, which should be cleaned-up as well.

10.8.15 Allow user to keep changes made in domain.xml

BIS `domain.xml` is created each time register is executed by merging xml files in `<BIS6_HOME>/software/deployer/domain/pieces` and its subfolders. After an update, all files and subfolders in there, **except the user-input** folder, are replaced with the new ones provided with the new BIS installation. So, if the user needs to keep changes made to the domain.xml, it should place its own xml snippets in `<BIS6_HOME>/software/deployer/domain/pieces/user-input`. They will not be overwritten by an upgrade.

10.9 DMZ Encryption

To encrypt all locally stored files on any AdapterEngine, you need to edit the *com.seeburger.security-config.xml*. You have to export this configuration file with the *software\export-config.bat/.sh.* Edit the file *temp\SeeConfig\<instanceID>/{com.seeburger.conf.user=BISAS}\com.seeburger.security-config.xml* and set the *useEncryption* parameter to *TRUE*.
After that you need to import the configuration file with *software\import-config.bat/.sh* again.

The default encryption algorithm is AES with 128 bit key length.
This can be changed with the algorithm and keysize property.

Supported algorithms are AES with keysize of 128, 192 and 256. DES is also a supported algorithm.

Note: Ensure that there are no recover jobs or stored files before changing the encryption settings.

Note: Per default the used key for encryption will be found as *USERS/DMZSECURITY/fileencryption*. You have to save this key. If the key is lost, there is no possibility to read any encrypted content.

10.10 Starting Instance with Operating System

10.10.1 Installation as Unix/Linux daemon

In order to have a BIS instance started at system start use the generated <BIS6_HOME>/bin/bis script, which supports the typical *sysvinit* style start/stop usage.

Consider adjusting the startup and shutdown sequence of the BIS6 service if you have related services like a database system that must be started and stopped in relation (before/afterwards) to the BIS6 service. Modification of the start and stop priority can be done within the BIS script by changing the values of '# chkconfig: 35 20 80' if your system supports chkconfig. See your Linux manual for details.

10.10.2 Installation as Windows Service

On Windows servers, BIS 6 should be installed as a Windows service to automate the startup and shutdown, independent of the currently logged in user.

Note: There is a new method to start the instance as a Windows service. This is based on the Apache P*rocrun* tool. For descriptions of the deprecated AppCenter based service start, refer to the older versions of this documentation. Settings for re-starting a failed service and notifications about it are now done with the normal Windows Service Control Manager properties (restart service).

Warning: If you do not use the service option the BIS application server will run as a console window on your desktop. If you close this window the server will be aborted and not cleanly shut down. To avoid this you can shut-down the console by pressing Ctrl+C instead or use the `shutdown-bisas.{bat,sh}` or "`bis stop`" command instead.

After the installation of the BIS 6 instance, you need to manually register the installation with the Windows service registry. This is done with the *service.bat* command by specifying the service parameter. The following options are available:

Options	Description
-remove	Stops and removes the installed service from Windows services registry.
-amd64	Installs the service as 64-bit process for x64 Windows.
-32	Not supported: Installs the service as 32-bit process
-start	Starts the installed service.
-stop	Stops the installed service.
-monitor	Starts service monitor (tray icon application) to manage the registered service.
-help	Online reference of the service commands.

The Apache Procrun tool provides binaries for different system architectures. The AMD64 is used for x64 Windows systems. Example command to register an existing BIS 6 instance with the Windows service registry on Windows platform x64 bits:

```
> cd \BIS6_HOME\bin
> .\service.bat  -amd64
> .\service.bat  -start
```

Example command to stop and remove existing BIS 6 instance:

```
> cd \BIS6_HOME\bin
> .\service.bat -stop
> .\service.bat -remove
```

You can set more than one parameter after the *'service'* command. E.g**.** '*service.bat -remove -amd64 -start - monitor*' will remove, install, and start the service and the GUI monitor. Use -help for short reference.

10.10.2.1 Upgrade and Configuration Changes

Unlike a normal command line start (via *service.bat*) of the process, the Procrun tool remembers the Java settings in the Windows registry. If you change parameters in vm.properties manually, or because of a BIS software update, you need to write the most recent parameters to the registry. This is done by first running register.bat to upgrade the *service.bat* file with the correct parameters, and then to re-install the service:

```
> cd \BIS6_HOME\software
> .\register.bat
# this will update the parameters in set-env.bat and service.bat
> cd \BIS6_HOME\bin
> .\service.bat -stop
> .\service.bat -remove
# make sure this suceeds, if not, reboot before installing
> .\service.bat -amd64
# this will register new service definition with updated parameters
```

You can use the Windows Registry Tool or the Service Monitor to check the parameters in the registry.

10.10.2.2 Administrative Privileges

In order to invoke the commands for managing the BIS 6 Windows service, you need to have administrative privileges. Since Windows 7 or Windows Server 2008 R2 enables the administrator approval mode (enable LUA) even members of the local administrative group require additional steps to execute the service management commands with elevated permission.

The recommended method is to use the *Run as administrator...* function of the Windows Explorer in order to start a command prompt from the *Start* menu: click on *Start* **|** *command prompt* menu entry with the right mouse button (context menu) and select *Run as administrator...* Ensure this was successful before proceeding. You will notice that the title of such an privileged command prompt window will have the *Administrator:* prefix.

If you cannot use the graphical method of enabling an unrestricted administrative shell, you can try to use the built-in *Administrator* account, which is not subject to administration approval mode in most installations (depends on the *FilterAdministratorToken* group policy setting). This is done by using the *runas.exe* tool:

```
runas /env /savecred /user:Administrator "service ......."
```

⚠ **Attention**: The ***/*** *savecred* option means that the execution of *runas* will use credentials previously saved by the user. If no such credentials exist, the command prompt will ask for administrator's password. For more information on the subject please execute '*runas /?'*

10.10.2.3 Troubleshooting

In some cases of installing/starting service the error reporting is not quite clear. Please verify the following situations:

- The service was installed with 32-bits *procrun.exe,* but currently the JVM DLL is 64bits or vice versa.
- Some of the *JVM* or P*rocrun* properties have been set incorrectly, or they cannot be parsed properly in the ANT. To verify this, please open the service monitor GUI and check the service configuration.
- If BIS is installed under a Microsoft server 2008, and the service is started under the default *System* user, the following error may occur in some situations (e.g. deploying a process): *Could not get shell folder ID list.*
  The situation can be prevented when installing the service under any other user (administrator or a standard user). For more information configure the *serviceUser* property in *bis-service.properties.* You might need to re-install the service if you change this user.
- There is an option to get a Thread Dump from the GUI Monitor context menu, use this operation with care, because it is unsafe and leads to a service shutdown due to the Java *jvm -Xrs* option. If you want to safely execute a BIS 6 Application Thread dump, remove this Java option from the *Java* tab | *Java* option section and restart the service. This Java option is needed and should be removed only in case of debugging purposes or other extreme cases.
- Occasionally during a service stop the error *"error 1053:The service did not respond to the start or control request in a timely fashion"* occurs. It may lead to problems if BIS 6 runs under a MS Cluster. We recommend increasing the stopping service timeout to 90 secs (the default setting is 20 secs). Create the following entry in Windows registry:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ServicesPipeTimeout
  Type: DWORD
  Value: Decimal: 90000 (This value is in milliseconds)
  ```

⚠ **Attention**: This registry change will affect all services, and it requires the server to be re-started to become active.

10.10.2.4 Notes for Cluster Installation

If you want to use a Microsoft Cluster server (fail-over) you need to repeat the BIS_SERVICE installation on all cluster instances. The startup type of the service is set to *manual*, and you configure a *Generic Service* resource in the Cluster Manager.

If you specified cluster setup in the Installer, in the *ports.properties* the installer configures the following properties with the virtual host name (instead of *localhost*):

- *instance.host*
- *bic.src.repository.host*
- *rmi.host*
- *webdav.host*

In addition to that, you need to enter the virtual host name to all physical host names in the license request form.

BIS instances are typically installed active/active and will not be installed as a resource in the failover cluster manager.

10.10.2.5 Behind the Scene

Note: Due to the change from SEEBURGER AppCenter to Apache Procrun, the running BIS 6 instance no longer show up as *java.exe* in the Task Manager. Instead look for the *procrun.exe*.

For more information on the Procrun Service Wrapper, visit the website of the Apache Project: *http://commons.apache.org/daemon/procrun.html*

The *Procrun* tool registers the *procrun.exe* wrapper as a Windows service which will load a JVM dynamic library and start the configured Java Class. The configuration for JVM, parameters and class is stored in the Windows registry under *HKLM\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\BIS6Service.* The service itself is registered in the Windows Service Control Manager. The Procrun tool has functions to register/de-register and update settings:

The BIS specific functionality is delivered in an ANT script file (*bis-service.xml*) and a properties file (*bis-service.properties*). Both files are located in the *${BIS_HOME}\bin* directory and they are started when *service.bat* detects the parameter. The P*rocrun* application files (for different architectures) are located in the directory *${BIS_HOME}\bin.*

The properties file (*bis-service.properties*) defines the following properties:

Property	**Description**
serviceUser'	Sets the domain\user under which the service will run. The back slash is escaped with double backslash , e.g. '.\\John'. If this property is not set, the default one ('SYSTEM') will be used; otherwise you need to set the password for the given user during the service installation. ⚠ **Attention:** The user that is meant to be used for our service should have "*Log on as a service*" rights. It is recommended you set the user with the Windows system control panel, since it will check password and permissions. This user account should also be accessible at all times by the system. If access to the user's home directory is not available, the service will not run properly.
jboss.SRV	Defines name of the service that will be installed for the instance.
serviceStopTimeoutSecs	It defines the timeout for stopping the service (in secs). Default value is 180 (3 minutes).
LogPath	Defines the path for logging. Creates the directory if necessary.
PidFile	Defines the file name for storing the running process ID. The actual file is created in the *LogPath* directory.
LogLevel	Defines the logging level and can be either *Error*, *Info*, *Warn* or *Debug.*
StdOutput	Redirected *stdout* file name. If named, the auto file is created inside the *LogPath* with the name *service-stdout.YEAR-MONTH-DAY.log.*
StdError	Redirected *stderr* file name. If named, the auto file is created in the *LogPath* directory with the name *service-stderr.YEAR-MONTH-DAY.log*.
LogJniMessages	Sets this non-zero (e.g. 1) to capture *JVM jni* debug messages in the *Procrun* log file. It is not needed if the *stdout/stderr* redirection is used.
AdditionalJVMProps	Sets additional jvm properties (starting with -X or -D) for service mode. Multiple options are separated by '#'.

10.10.3 Service like starting BIS on windows

In order to start a BIS instance use the generated <BIS6_HOME>/bin/bis.bat script, which supports the start/stop/restart/kill/status style usage.

Note: Starting bis with <BIS6_HOME>/bin/bis.bat will not install it as service. It will only start/stop bis in its own process. If you close the cmd in which you have started the BIS, BIS will remain running.

Options	Description
start	Starts the installed bis service like.
stop	Stops the installed bis.
status	Returns the status of bis [running / stopped]. Also appropriate exitcode is returned: • ERRORCODE 0 - bis is running • ERRORCODE 1 - bis is not running
kill	Tries to kill started bis if there is one.
restart	Restart bis and start it service like.

Example command to start BIS 6 instance:

```
> cd \BIS6_HOME\bin
> .\bis.bat start
```

Example command to stop BIS 6 instance:

```
> cd \BIS6_HOME\bin
> .\bis.bat stop
```

10.11 Configuring Attachment Store

The attachment store for a BIS system is used to store files and attachments with a certain size. It provides storage, compression and reorganization for all instances in a BIS system. For a general introduction into designing the attachment store, please refer to the BIS *Concepts and Installation Planning* manual.

By default, an all-in-one (single instance) installation uses the local filesystem for attachment storage. If you add distributed instances they will access this local directory on the Admin Server instance via the WebDAV server embedded in the AS. You are currently limited to only one instance of role AdminServer, so if you have to shut down this instance in order to apply software updates, the still running instances fail to store or retrieve the payload.

BIS 6.5.2 comes with special support for rolling updates (page 57). A rolling update is a methodology where you update the instances of a BIS 6.5.2 environment one by one without stopping the whole system. You can configure the system to use an external shared file system or WebDAV server. Shutting down the AdminServer will then no longer impact still running instances trying to store a payload.

In addition to the external attachment store the BIS system will also store smaller attachments in memory and as large binary objects (LOBs) in the `tBPAttachments` table of the system database. This is faster for smaller attachments and integrated into HA, DR and backup/restore of the system database. A size limit restricts what compressed attachments are stored in RAM and DB. This is controlled with the MAX_BUFFER_SIZE system property (in bytes, default is 1000 kB). If you lower this limit more files will be stored in the (slower) external storage.

The following sections describes alternative methods for storing the larger attachments and files. The Data Instance Access Framework (DIAF) is used to select the methods:

Data Store

The SEEBURGER Data Store is a distributed storage solution for attachments. Please see the *Data Store* manual for installation and operation details. It replaces all other storage options as described below.

Shared File System

This scenario is easy to set up, and depending on the actual file system used it is fast and reliable. In this case, a shared file system is accessed on all instances via the FileResourceProvider of DIAF (in addition to storing very small messages in the database). Supported file systems:

- NFS (provided by an appliance, HA-NFS from a server cluster or a NFS failover server)
  This can be used if all Instances are installed on Linux/Unix machines (it is not supported to use Windows as NFS Server or Client!)
- Cluster file system
  We have good experiences with clustered *Veritas File System* (available for different Unix and Linux flavors). The cluster file system must provide the semantics as defined in the *Concepts and Planning* manual (especially: visible immediately by all nodes after the file is closed and renamed: this rules out a number of replicated solutions).

If you introduce DR and long distance replication, make sure the replication product either guarantees the same “session consistency” guarantees or you do not access the replicas in normal operation. Most replicated file systems (like DFS Replication for Microsoft Windows Server, Microsoft FRS or Dropbox) cannot be used in this scenario. Due to the limited requirements of “session consistency”, it is however theoretically possible to use file replication products if they offer synchronous modes.

HTTP Server

Instead of using a shared file system, the HTTP access is more firewall friendly, but the overhead is bigger. You also need to maintain the additional http servers. This is resulting in higher latency in some scenarios. It is therefore recommended to use the shared file system if possible.

By default, the Admin Server offers a WebDAV server which is used to store some administrative objects, but also a dedicated listener to provide WebDAV access to the DIAF file pool. If DIAF is not configured it will inherit the settings for this server. If you want to deploy an external HTTP server, the DIAF store should be configured to use the separate server, but the Admin Server repository will remain on the Admin Server and its data/ directory.

In case of parallel use of an external WebDav and the AS as WebDav provider (not recommended) take into account that the AS will always use its own data/webdav/seediaf path as store. In order to have both the external WebDav and the AS Webdav providing the same filepools it is needed to either use a symlink linking the data/webdav/seediaf directory of the AS to the external WebDav folder or setting the root of the external WebDav to the AS data/webdav directory.

Apache Configuration for WebDAV

The following is a configuration sample to provide a WebDAV repository for use as a BIS attachment (DIAF) datastore. The example assumes a dedicated file system `/shared/bisdata` (which is shared between all Apache servers). This directory needs to be owned by the Apache httpd runtime user.

BIS does not require you to share the WebDAV locking database between multiple Apache httpd servers, so you should put it on a local file system. The password file for access control is created with the `htpasswd` command (see below). Make sure the password file is not reachable by remote clients (store it outside the document roots).

For RHEL, you put this configuration into `/etc/httpd/conf.d/seewebdav.conf` and restart Apache with `/etc/init.d/httpd restart`. For SLES, the configuration is placed into `/etc/apache2/conf.d/seewebdav.conf` and the restart is done with `/usr/sbin/rcapache2 restart`.

Example Apache httpd server configuration (V 2.4.10):

```
#
```

```
# Configure /webdav for SEEBURGER BIS DIAF
#
<IfModule mod_dav_fs.c>
    DAVLockDB /var/lib/dav/lockdb

    Alias /webdav /shared/bisdata/webdav

    # file system for data storage, possibly shared
    <Directory /shared/bisdata/webdav/>
        Options None
        AllowOverride None
        ForceType application/binary

        # limit access to servers
        Order allow,deny
        Allow from 198.51.100

        Dav filesystem
        DavDepthInfinity on

        <LimitExcept GET HEAD PUT DELETE MKCOL MOVE PROPFIND>
            Deny from ALL
        </LimitExcept>

        require user seeburger
        AuthType basic
        AuthName "webdav"
        AuthUserFile /shared/bisdata/passwd.dav
    </Directory>

</IfModule>
```

Note: Since Apache does not allow for creating directories by putting files into them, you need to create the whole DIAF directory structure.

Creating DIAF Structure

With the following shell commands you can create the empty directories used by DIAF to store a larger number of files (it assumes httpd is running as user and group `apache`):

Linux:

```
            mdkir -p
            /shared/bisdata/webdav/seediaf/filepool1/temp

            cd /shared/bisdata/webdav/seediaf/filepool1
hex="0 1 2 3 4 5 6 7 8 9 a b c d e f"

            for a in $hex; do echo "$a";mkdir "$a";for b1 in $hex;do for b2 in $hex;do for
 b3 in $hex;\

                 do mkdir "$a/$b1$b2$b3";done;done;done;done

            chown -R apache:apache /shared/bisdata
```

This will create 65536 directories named `/shared/bisdata/webdav/seediaf/pool1/[0-9a-f]/[0-9a-f] [0-9a-f] [0-9a-f]/`.

eg.: `/shared/bisdata/webdav/seediaf/filepool1/5/fff /`

Windows:

```
            FOR %%G IN (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f) DO (
  FOR %%H IN (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f) DO (
    FOR %%I IN (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f) DO (
      FOR %%J IN (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f) DO (
        mkdir D:\filepool\%%G\%%H%%I%%J
      )
    )
  )
)
```

This will create 65536 directories named `D:\filepool\[0-9a-f]\[0-9a-f][0-9a-f]  [0-9a-f]\`.

eg.: `D:\Filepool\5\fff\`

Using DIAF with external HTTP Servers

Besides the data storage for attachments, WebDAV is also used for internal Admin Server specific files. It is therefore not recommended to move the whole content to the data store (via ports.properties webdav.host). You should only reconfigure the WebDavProviders for DIAF. By having an external HTTP server, you ensure processing can continue, even if you shut down the Admin Server for maintenance or a rolling update.

It is best to use a highly available NAS appliance which supports HTTP access, because then you do not have to deal with clustering and sharing the file system. However if you want to set up your own HTTP server cluster, you need to make sure to have a shared file system between the HTTP servers (or set up only one HTTP server in a failover configuration). Setting up Apache in this scenario is described above.

The following is a sample configuration for DIAF to use two external HTTP servers. The request will be issued round-robin to both servers, and if one is not reachable, it will use the remaining. The sample lists only one pool (WebdavPool1), you will need to modify all of the pools to use WebdavResourceProvider with the given properties:

```
<?xml version="1.0" encoding="UTF-8"?>
<config>
  <node name="client">
    <node name="core">
      <node name="common-properties">
        <property name="backup-output-dir">%bisas.temp%</property>
      </node>
      <node name="resource-providers">
 ...
        <node name="provider5">
          <property name="name">WebdavPool1</property>
          <property name="code">com.seeburger.diaf.client.core.WebdavResourceProvider</
property>
          <node name="config-properties">
            <node name="cp5">
              <property name="name">BasePath</property>
              <property name="value">webdav/seediaf/filepool1</property>
              <property name="type">java.lang.String</property>
            </node>
            <node name="cp6">
              <property name="name">TempBasePath</property>
              <property name="value">webdav/seediaf/filepool1/temp</property>
              <property name="type">java.lang.String</property>
            </node>
          </node>
          <node name="additional-servers">
            <property name="useOnlyAdditionalServers" type="java.lang.Boolean">
            true
            </property>
            <node name="additional-server">
              <property name="port" type="java.lang.Integer">12000</property>
              <property name="enabled" type="java.lang.Boolean">true</property>
              <property name="host">web1.example.com</property>
              <property name="scheme">http</property>
              <property name="username">seeburger</property>
              <property name="password">-5d5e847e5290c57737549ec3c3fb6daa</property>
            </node>
            <node name="additional-server">
              <property name="port" type="java.lang.Integer">12000</property>
              <property name="enabled" type="java.lang.Boolean">true</property>
              <property name="host">web2.example.com</property>
              <property name="scheme">http</property>
              <property name="username">seeburger</property>
              <property name="password">-5d5e847e5290c57737549ec3c3fb6daa</property>
            </node>
          </node> <!-- additional-servers -->
        </node> <!-- provider name=WebdavPool1 -->
        ...
      </code>
    </code>
  </code>
</config>
```

The username and password optional properties can be used to provide basic authentication for the specified server. See the section **Creating Credentials** for creating the encrypted version of the password for BIS as well as Apache httpd.

Be aware that you have to repeat the provider configuration for each pool. The name “FilePool1” and “WebdavPool1” does not mean they are specific to a protocol, those are simply commonly used (sample) pool names. All have to be switched to code=WebdavResourceProvider.

Using HTTP/S for additional-servers

It is possible to use HTTP/S (TLS protection) to access the external WebDAV servers. This will protect the data and credentials but also will put additional load on the endpoints and add some additional latency. If you want to use this, you need to import the servers certificates into a system keystore file, and add it to the configuration. You also need to use scheme=https. In this case the external WebDAV servers need to be TLS enabled and you need to specify the secure port number.

It is a good idea to decide for each distributed BIS instance if you want to use SSL or nor. This way you could configure DMZ instances to use TLS but still connect from Process Engine instances (in the same network segment than the WebDAV server) with the more efficient HTTP protocol.

Importing certificate to a truststore file is done with:

```
runtime/jvm64/bin/keytool -import -alias server1 -keystore conf/keys/webdav-truststore.jks
 -file certificate.der
```

All WebdavResourceProvider need to be configured to point to this trust store:

```
...
<node name="provider5">
  <property name="name">WebdavPool1</property>
  <property name="code">com.seeburger.diaf.client.core.WebdavResourceProvider</property>
  <node name="config-properties">
    ...
  </node>
  <node name="additional-servers">
    <property name="useOnlyAdditionalServers" type="java.lang.Boolean">true</property>
    <node name="additional-server">
      <property name="port" type="java.lang.Integer">443</property>
      <property name="enabled" type="java.lang.Boolean">true</property>
      <property name="host">myAdditionalHost.example.com</property>
      <property name="scheme">https</property>
      <property name="sslTrustStore">/seeburger/bis/conf/keys/webdav-truststore.jks</
property>
      <property name="sslTrustStorePass">TRUST_STORE_PASSWORD</property>
    </node>
    ...
  </node>
</node>
```

The trust store has a password for integrity protection. The keytool will ask for this if you want to modify the file. You also need to specify it in SeeConfig. It is not used for authentication and therefore not encrypted. See the next section on how to implement and activate the changes in SeeConfig.

DIAF SeeConfig

The Data Instance Access Framework (DIAF) in BIS uses a SeeConfig file to configure the settings accessing the files. This could be a file system (`code=com.seeburger.diaf.client.core.FileResourceProvider`) provider or a webdav (`code=com.seeburger.diaf.client.core.WebdavResourceProvider`) resource provider.

For each BIS instance in a distributed installation you have to configure this separate (this allows a mixed configuration where the Admin Server uses the file system and all other remote instances uses WebDAV to access the directory).

In BIS 6.5 the configurations are centrally maintained on the Admin Server (distributed via the system database).

In order to make modifications to the configuration, you need to call `software/export-config.{sh,bat}` to create an up-to-date export version in the temporary directory:

```
<BIS6_HOME>/temp/SeeConfig/
  <instance.id>/{com.seeburger.conf.user=BISAS}/{com.seeburger.diaf=ResourceProviders}/
    com.seeburger.diaf-config.xml
```

After modifying the files, you need to run `import-config.{bat,sh}` to overwrite the database version with the modified temporary files.

The following lists a sample template for a (shared) file system based DIAF store. "FilePool1" in this case is reachable over "FileResourceProvider", which basically uses the local file system API. This can be used to access direct attached storage, SAN or NAS. It also works with certain clustered file systems:

```
<?xml version="1.0" encoding="UTF-8"?>
<config>
  <node name="client">
    <node name="core">
      <node name="common-properties">
        <property name="backup-output-dir">%bisas.temp%</property>
      </node>
      <node name="resource-providers">
        <node name="provider1">
          <property name="name">FilePool1</property>
          <property name="code">com.seeburger.diaf.client.core.FileResourceProvider</
property>
          <node name="config-properties">
            <node name="cp1">
              <property name="name">BasePath</property>
              <property name="value">%bisas.data%/webdav/seediaf/filepool1</property>
              <property name="type">java.lang.String</property>
            </node>
            <node name="cp2">
              <property name="name">TempBasePath</property>
              <property name="value">%bisas.data%/webdav/seediaf/filepool1/temp</property>
              <property name="type">java.lang.String</property>
            </node>
          </node> <!-- config-properties -->
        </node>  <!-- provider name=FilePool1 -->
               ...
      </node> <!-- resource-providers -->
    </node>
  </node>
</config>
```

The following lists a sample entry for the same "FilePool1", but with a Webdav based DIAF store (only host and port for additional servers are properties with no default value):

```
<?xml version="1.0" encoding="UTF-8"?>
<config>
  <node name="client">
    <node name="core">
      <node name="common-properties">
        <property name="backup-output-dir">%bisas.temp%</property>
      </node>
      <node name="resource-providers">
     ...
        <node name="provider1">
          <property name="name">FilePool1</property>
          <property name="code">com.seeburger.diaf.client.core.WebdavResourceProvider</
property>
          <node name="config-properties">
            <node name="cp5">
              <property name="name">BasePath</property>
              <property name="value">webdav/seediaf/filepool1</property>
              <property name="type">java.lang.String</property>
            </node>
            <node name="cp6">
              <property name="name">TempBasePath</property>
              <property name="value">webdav/seediaf/filepool1/temp</property>
              <property name="type">java.lang.String</property>
            </node>
            <node name="cp7">
              <property name="name">CreateWebdavFolders</property>
              <property name="value">false</property>
              <property name="type">java.lang.Boolean</property>
            </node>
          </node>
          <node name="additional-servers">
            <property name="useOnlyAdditionalServers" type="java.lang.Boolean">false</
property>
            <node name="additional-server">
              <property name="port" type="java.lang.Integer">12000</property>
              <property name="enabled" type="java.lang.Boolean">true</property>
              <property name="host">web1.example.com</property>
              <property name="scheme">http</property>
              <property name="createFolders" type="java.lang.Boolean">false</property>
              <property name="basePath">webdav/seediaf/pool1</property>
              <property name="tempPath">webdav/seediaf/pool1/temp</property>
              <property name="username">remoteEjbCaller</property>
              <property name="password">-5d5e847e5290c57737549ec3c3fb6daa</property> <!--
 seeburger -->
              <property name="sslTrustStore">/seeburger/bis/conf/keys/webdav-
truststore.jks</property>
              <property name="sslTrustStorePass">TRUST_STORE_PASSWORD</property>
            </node>
            <node name="server2">...</node>
          </node>
        </node> <!-- provider name=FilePool1 -->
      </node> <!-- resource-providers -->
    </node>
  </node>
</config>
```

Note: the pools have names like "FilePool1" or "WebdavPool1". Those names are used internally by BIS components, but they don't have to be of type file or webdav. The only requirement is, that all files stored in a pool with a given name are stored on the same place (no matter which BIS instance uses the pool). So typically you configure all pools to point to the same place with any protocol you define in your landscape planning.

The node names "providerX", "cpX" and "serverX" can be any name, they just have to be unique. On the other hand "client", "core", "common-properties", "resource-providers", "additional-servers" and "config-properties" are expected names.

The `CreateWebdavFolders/createFolder=true` property tells the WebDAV provider to issue MKCOL commands before storing files. This allows to work with Webdav servers where the directories are not created by default on access. This however slows down store operations, so it is better to have this option off. createFolder on a server level overwrites the `CreateWebdavFolders` default for the pool.

While the system is running, you can actually modify some of the configuration. If you switch enabled to disabled the specific external server will no longer be contacted. This way you can pause requests to this server to restart it for maintenance. Make sure you always have at least one server enabled and reachable.

Creating Credentials

In order to allow the WebdavResourceProvider of BIS instances to log into the external HTTP server, you need to configure the password to use in BIS as well as the same password to check on the HTTP server side. On the BIS side, the encode-password tool (with algorithm "des") is used to create an encoded string.

Creating an encrypted password String on Linux/Unix for BIS:

```
$ cd software/
$ ./encode-password.sh secret des
[echo] Encoded password: 75146172de950338
```

Creating a encrypted password String on Windows for BIS:

```
> cd software\
> .\encode-password.bat secret des
[echo] Encoded password: 75146172de950338
```

Both commands will print the encrypted password (it is a big number, possibly negative) to the console. You need to copy and paste it to the SeeConfig file.

On the external HTTP server side, you use the password tool of the server vendor. Most servers (like Apache httpd) typically provide a tool "htpasswd" which is used to add user entries to a specified password file:

Creating a password file for Apache httpd on Unix/Linux:

```
$ htpasswd -csb /shared/bisdata/passwd.dav seeburger secret
```

This will create the password file and add the user "seeburger" with the SHA-1 hashed password "secret".

10.12 Security Enhanced Linux (SELinux)

Security-Enhanced Linux (SELinux) adds Mandatory Access Control (MAC) to the Linux kernel, and is enabled by default in Red Hat and Oracle Enterprise Linux 6 or 7. Running BIS with such a configuration is supported, however this requires that the BIS user is **unconfined** and the **targeted security policy** is in use (only *selinux-policy-targeted* and *selinux-policy* packages are installed, especially not the optional MLS policy).

The configuration is read from `/etc/selinux/config` at boot. You can use the `sestatus` command to verify:

```
# sudo yum install policycoreutils setools-console
# sudo sestatus
SELinux status: enabled
SELinuxfs mount: /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policyname: targeted
Current mode: permissive
Mode from config file: permissive
Policy MLS status: enabled
Policy deny_unknown status: allowed
Max kernel policy version: 28
```

In the above example output, you can see "Loaded policyname: targeted".

The system is in **permissive** mode (In case of policy violations, it requires `auditd` and will log to `/var/log/audit/audit.log` but does not deny any access). This is the default setting and should not cause problems.

If you switch the SELinux mode to **enforcing,** all alerts will cause an access denied. With the targeted policy, this will not affect BIS in normal situations.

Keep in mind that some system admin tasks might be affected when SELinux is in use, especially for topics like maintaining system services, monitoring system log files or attaching storage and file systems. SEEBURGER does not provide help for navigating on a restrictively configured environment.

With the `id` command you can query the current users access context, the „unconfined“ is the expected user, role and type and s0 is the default security label. Run this command as the BIS owner:

```
$ id -Z
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

If your user login is not unconfined, you can use the semanage command (as root) to view a list of mappings between SELinux and Linux user accounts. For this to work you need to have the `policycoreutils-python` package installed:

```
$ sudo yum install policycoreutils-python
$ sudo semanage login -l
Login Name      SELinux User      MLS/MCS Range  Service
__default__       unconfined_u    s0-s0:c0.c1023 *
Root              unconfined_u    s0-s0:c0.c1023 *
system_u          system_u        s0-s0:c0.c1023 *
```

The above example output is the expected default: there is no specific rule, so the BIS application user will use the `__default__` entry and is mapped to the `unconfined_u` SELinux user. If you created the BIS owner user with "`adduser ... -Z unconfined_u`", then the list will show a more specific entry, which is also fine:

```
seeasown unconfined_u s0-s0:c0.c1023 *
```

We do not provide support for running BIS as a confined user. (If you would want to create your own policy to allow this, you need to look at the installation and runtime procedure. Using SELinux user `user_u` would allow BIS to be installed in the home directory of the user only. You probably would have to create a role and policy to loosen these restrictions. As this is not supported by SEEBURGER, we do not recommend to do this.)

Summary

SEEBURGER BIS can be used on RHEL or OEL with enabled SELinux with the **targeted** policy activated in **permissive or enforcing mode** with the BIS runtime user as SELinux user **unconfined_u**. We do not provide support for creating and running BIS with confined users or policies different from targeted. We recommend special training for system administrators dealing with restricted systems, as we cannot provide support for system maintenance tasks in this case.

See also

The following resources can be used to learn more about SELinux and the default settings.

- RedHat Linux Enterprise 7 SELinux User’s and Administrator’s Guide: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/SELinux_Users_and_Administrators_Guide/index.html
- NSA founded SELinux project page https://www.nsa.gov/research/selinux/index.shtml
- SELinux Reference Policy (Tresys Technology) https://github.com/TresysTechnology/refpolicy/wiki

10.13 Configuring Landscape URI Discovery

If multiple SEEBURGER Systems (see manual "Concepts and Planning" for a definition of the terms "Landscape" and "System") need to be connected to each other this can be done in multiple ways. One way is to put a dedicated LoadBalancer between all systems which handles the case when single instances are taken out of service for maintenance. In addition to that, it is also possible to use client side load balancing in several SEEBURGER components. This section describes the general configuration for those components. Refer to the individual components manual for further details and / or considerations.

10.13.1 Overview

The general idea is to describe logical services which are bound to instances (which in term belong to a single system). Logical services have a type and a name and consist of at least one concrete URI per instance they run on. This URI uniquely identifies the endpoint for that service. The URI is a way for the client component to reach or address the server component. So for example if one component needs to access the web service interface of another component the URI would be the URL to the web service endpoint on the server side component.

From a configuration point of view the client component will not be configured with a direct URL to the web service endpoint of the server side component, but rather a logical URI (the landscape discovery URI) will be used instead. With that abstraction the connections between systems can be maintained on a central place for each system and is not spread over the various components. Also if multiple client components need to reach the same server endpoint in another system, the URIs are only configured once and can be reused.

10.13.2 General configuration

As mentioned above the Landscape URI discovery works with logical services consisting of a type and a name. A service can live on one or more instances of a system and can have one or more URIs per instance. Each URI has a logical network assigned to it, which means that if a service is reachable via different URIs depending on the client location, they can be configured here. Then the client can lookup the URI for the network he is placed in.

Currently each system has to maintain it's own configuration about all other systems it needs to connect to. This is only necessary for services you actually want to discover.

10.13.2.1 XML based configuration

To modify the available services or to add new systems, call

```
<BIS_HOME>/software/export-config[.bat|.sh]
```

After that navigate to

```
<BIS_HOME>/temp/SeeConfig/{com.seeburger.conf.user=BISAS}/com.seeburger.landscape.api-
config.xml
```

Note: This configuration is shared between all instances of a system but can only be modified on the AdminServer.

Initially the configuration contains some sample configuration, which will be ignored by the software. It is up to you to either copy that part and leave the sample in or to modify the existing to fit your needs. Below is a (minimal) sample configuration (based on a BIS FX Active-Active counterpart which consists of three instances, where one is currently down for maintenance purposes). It only contains the absolute minimum. The sample provided upon first start is a bit more verbose and includes for example a second network with a different URL to the BIS FX WebService.

```
<?xml version="1.0" encoding="UTF-8"?>
<config>
    <node name="bisfx-prod">
        <property name="comment">Sample BIS FX production system</property>
        <node name="sample-instance1">
            <property name="enabled">true</property>
            <node name="bisfx">
                <node name="default">
                    <property name="iternal">http://sample-instance1:8080/portal-seefx</
property>
                </node>
            </node>
        </node>
        <node name="sample-instance2">
            <property name="enabled">true</property>
            <node name="bisfx">
                <node name="default">
                    <property name="internal">http://sample-instance2:8080/portal-seefx</
property>
                </node>
            </node>
        </node>
        <node name="sample-instance3">
            <property name="enabled">false</property>
            <node name="bisfx">
                <node name="default">
                    <property name="internal">http://sample-instance3:8080/portal-seefx</
property>
                </node>
            </node>
        </node>
    </node>
</config>
```

The configuration defines one system with the ID "bisfx-prod". The system consists of three instances with the instance IDs "sample-instance1", "sample-instance2" and "sample-instance3". Each instance has a service with type "bisfx" and name "default" defined. "sample-instance3" is currently not available due to maintenance (e.g. update) and is therefore disabled (property "enabled" set to "false").

Warning: Two system IDs are ignored when the configuration is parsed:
1. "sample-system" (which is the sample delivered when the BIS is started the first time)
2. Our own system ID (the system ID of this BIS, which can be seen in `<BIS_HOME>/software/profile.properties` with the key `system.id`

After finishing the configuration you need to call

```
<BIS_HOME>/software/import-config[.bat|.sh]
```

Note: The configuration is automatically loaded even when the BIS is running. It may take up to 30 seconds until the new configuration is live.

10.13.3 Usage

In case you have a component which needs to connect to a service on another system (e.g. the BIS FTP Server Adapter with a server of type "BIS FileExchange Listener" needs to connect to BIS FX), instead of specifying one concrete URI to one instance, you can rather point the adapter to the logical service defined above. The adapter then will do a round-robin load balancing between all available instances (in the above example alternate between instance1 and instance2, but not instance3 as it is supposed to be down). This logical URI is called the Landscape Discovery URI.

10.13.3.1 Landscape Discovery URI

The landscape discovery URI is basically a way to filter the configuration down to a list of concrete URIs which are then used in a round robin based fashion. The full URI schema is as followed, though you typically need only very few informations:

```
discovery://<service-type>/[<service-name>]?[system=<system-id|default:own>]&[group=<group|
default:any>]&[instance=<instance-id|default:any>]&[network=<internal|external|
default:internal>]
```

So regarding the above example if you just need to reach the BIS FX service, a minimal working example would be

```
discovery://bisfx?system=bisfx-prod
```

Hypothetically if you want a specific FTP server listener to only connect to a specific BIS FX instance, you could also configure the following discovery URI

```
discovery://bisfx?system=bisfx-prod&instance=sample-instance1
```

which would always resolve to the URI `http://sample-instance1:8080/portal-seefx`

For further information, please refer to the respective components documentations.

10.14 Oracle JDBC Driver update

The Oracle Thin JDBC driver (ojdbcX.jar) is used by the BIS instances to connect to the system database in case you have installed BIS with the Oracle setting. This driver is externally provided at initial installation time. The setup will ask for an external folder which contains the extracted instant client (in the basic-lite variant). See the Database Driver section in the **System Database** manual for more details.

After checking the source, the setup will copy the whole user specified folder to `<BIS6_HOME>/runtime/instanctclient`. After this the register process is responsible for distributing the actual JAR files to different places in the BIS installation. This especially includes `<BIS6_HOME>/lib/ext/ojdbc.jar` for scripts and tools as well as `<BIS6_HOME>/modules/oracle/jdbc/main/ojdbc.jar` for the application server. It will also include a version of this file into the archive used to install additional instances. This is why you need to provide the driver only to the initial installation of the Admin Server or B2B Portal, but not to additional instances. At runtime the files in the instantclient directory are only accessed by register script.

Generally you should only use supported driver versions. Information on supported driver can be read in the respective Release Notes *Supported Systems* section.
If you need to update, the following procedure is recommended:

a) extract a new instant client archive into an empty folder. Make sure to use the download matching your target operating system (also this is not strictly needed, as we use only the `ojdbcX.jar` which is platform neutral, this is not a strict requirement. However for support reasons it is good to have a working native installation.

b) replace `<BIS6_HOME>/runtime/instantclient/` with the content from your archive. Since different versions might contain different number of files and sub-directories it is strongly recommended to delete the complete content before copying the new version.

Note: make sure there is no intermediate sub-directory after expanding the archive. The `ojdbcX.jar` must located be directly at `runtime/instantclient/ojdbcX.jar`

c) Make sure to specify `bisas.driver.jar=${bisas_home}/runtime/instantclient/ojdbc.jar` (i.e. without a number in the file name) in `<BIS6_HOME>/software/register.properties` then make sure to copy the driver JAR from the Java-release specific file (like `ojdbc8.jar`) to the neutral name `<BIS6_HOME>/runtime/instantclient/ojdbc.jar`. If your property files mentions older `ojdbcX.jar` you need to adjust this, as the recommended driver no longer provides it.

Note: the Oracle instant client archive does not contain the neutral named ojdbc.jar. When using the setup it will copy the latest ojdbcX.jar to this name. When manually installing an update, you will have to do this step yourself.

d) Verify the version of the driver and make sure the archive is not corrupt. You can do this with the following command line (since the Oracle driver by default prints some version information and exits):

On Linux/Unix:

```
cd BIS6_HOME
runtime/jvm64/bin/java -jar runtime/instantclient/ojdbc.jar
```

On Windows:

```
cd /d BIS6_HOME
runtime\jvm64\bin\java -jar runtime\instantclient\ojdbc.jar
```

If this prints the desired driver version you can begin with the register step (you can also do that after the update installer while the instance is still down):

1. Drain the instance with the script (if present) `bin/prepareShutdown.{bat,sh}` or from the Front-end Dashboard.
2. shut down the instance. On a Windows service use the service manager, for Linux/Unix use the `/etc/init.d/bis stop` command or run `bis/shutdown-bisas.{bat,sh}`
3. run `software/register.{bat,sh}`
4. Verify there are no errors or unexplained warnings in `log/install/register.lgw`
5. Start the instance and wait until it shows up as running in the Dashboard before you continue.

The process needs to be repeated for all instances of the same system.

11 Contact

If you have questions or need assistance for installing or using SEEBURGER solutions, please do not hesitate to contact the SEEBURGER Customer Service and Support.

To accelerate processing of your request, please ensure you have the exact version number of the product as well as your customer ID available. If case you encountered an error condition, please provide a screen shot or log file. Collecting and packaging diagnostic information should be done using the SEEBURGER Support Agent (SSA) with the 'SI' (Support Incident) profile.

SEEBURGER AG Edisonstr. 1 D-75015 Bretten Germany URL: http://www.seeburger.de Tel: +49 (0)7252 96-1443	SEEBURGER, Inc. 1230 Peachtree Street Suite 1020 Atlanta, GA 30309, USA URL: http://www.seeburger.com Phone: +1 678-638-4894
Support URL: https://servicedesk.seeburger.de Mail: servicedesk@seeburger.de	Support URL: https://servicedesk.seeburger.de Mail: servicedesk@seeburger.com

In addition to the official ways to contact SEEBURGER Support we also provide the Customer Community, a private social network. You can discuss in the forum with peers, share your experience or monitor other contributions. This is a free service for SEEBURGER customers. It is not covered by SEEBURGER support terms and gurantees.
Sign up to today with your business e-mail and do not forget to mention your customer number or service desk account: https://community.seeburger.com.