



# Ellucian Solution Manager Installation and Configuration Guide

Release 1.6  
March 2016

---

## Notices

Without limitation: Ellucian®, Banner®, Colleague®, and Luminis® are trademarks of the Ellucian group of companies that are registered in the U.S. and certain other countries; and Ellucian Advance™, Ellucian Course Signals™, Ellucian Degree Works™, Ellucian PowerCampus™, Ellucian Recruiter™, Ellucian SmartCall™, are also trademarks of the Ellucian group of companies. Other names may be trademarks of their respective owners.

© 2016 Ellucian.

Contains confidential and proprietary information of Ellucian and its subsidiaries. Use of these materials is limited to Ellucian licensees, and is subject to the terms and conditions of one or more written license agreements between Ellucian and the licensee in question.

In preparing and providing this publication, Ellucian is not rendering legal, accounting, or other similar professional services. Ellucian makes no claims that an institution's use of this publication or the software for which it is provided will guarantee compliance with applicable federal or state laws, rules, or regulations. Each organization should seek legal, accounting, and other similar professional services from competent providers of the organization's own choosing.

Ellucian  
4375 Fair Lakes Court  
Fairfax, VA 22033  
United States of America

---

# Contents

<b>Ellucian Solution Manager overview.....</b>	<b>5</b>
<b>Install Ellucian Solution Manager.....</b>	<b>6</b>
Create an esmadmin user.....	6
Set up Ellucian Solution Manager root directories.....	7
Activate the rngd service for the admin console.....	7
Create a deployment files directory.....	8
Download the installation deployment files.....	8
Install Java.....	9
Configure access to Java for the admin console.....	9
Install and configure Apache Tomcat.....	10
Install and configure a Groovy interpreter.....	11
Create an Ellucian Solution Manager configuration database encryption key.....	11
Create the Ellucian Solution Manager application data directory.....	12
Start and access the Ellucian Solution Manager application.....	13
Enter system settings.....	14
Upgrade to 1.6.....	15
<b>Manage Solution Manager.....</b>	<b>16</b>
Restart Solution Manager.....	16
Back up Solution Manager configuration database.....	16
<b>Upgrade to Solution Manager 1.6.....</b>	<b>18</b>
Upgrade to Solution Manager 1.6.....	18
Upgrading from release 1.1 or 1.2.....	19
<b>Manage Banner environments overview.....</b>	<b>21</b>
Update existing Banner environments.....	21
Provision new Banner environments.....	22
<b>Install and secure Jenkins.....</b>	<b>23</b>
Install and start Jenkins.....	23
Secure Jenkins.....	24
Configure Solution Manager for Jenkins.....	25
<b>Install upgrade communication agent into Banner environment.....</b>	<b>27</b>
Install Jenkins slave on Jobsub machine and set up agent environment.....	27
Install Jenkins slave on Windows Jobsub machine.....	28
Add a Windows service.....	29
<b>Create deployment agents.....</b>	<b>30</b>

---

---

Define a Jenkins slave on the Solution Manager Jenkins server.....	30
Install Jenkins slave on an application server / set up agent environment.....	32
Install Jenkins slave on Windows application server.....	33
Add a Windows service.....	34
<b>Set up SSH keys authentication.....</b>	<b>35</b>
SSH key based connections.....	35
Prerequisites for Solution Manager to use SSH keys.....	35
Configure Solution Manager settings.....	35
Set up SSH keys authentication.....	36
SSH connections in ESM.....	36
<b>Set up Windows machines in managed Banner environments.....</b>	<b>39</b>
Install Cygwin (download package).....	39
Install Cygwin (local directory).....	44
Configure Solution Manager Settings.....	49
<b>Configure Solution Manager for Banner environment provisioning.....</b>	<b>51</b>
Install required OS infrastructure packages.....	51
Download provisioning template.....	52
Acquire provisioning content.....	52
Configure permissions for SELinux.....	53
Set up directories for provisioning environments.....	54
Restart the inet daemon and configure DHCP.....	54
Verify TFTP service.....	55
<b>Appendix: Solution Manager worksheets.....</b>	<b>58</b>
Developer worksheets.....	58
Tomcat application server.....	58
WebLogic application server.....	59
Banner credentials database.....	61
Banner credentials installer.....	61
Admin server private network environment settings.....	62
Admin server public network environment settings.....	63
Environment configuration settings.....	63
Environment settings worksheets.....	65
INB application worksheets.....	68
INB compiler server properties.....	70
Jobsub BXE application worksheets.....	73
SSB application properties.....	74
SSB application worksheets.....	75
Machine DB Jobsub app server.....	76

## Ellucian Solution Manager overview

Ellucian Solution Manager is a software system that allows for the download, installation, configuration, and management of Ellucian products.

Ellucian Solution Manager is installed as a web application and equips system administrators with the ability to:

- install upgrades and deployments to existing Banner environments.
- provision new Banner environments.
- provision new applications into existing Banner environments.
- self-update Solution Manager (upgrade the application and manage the Solution Manager database).

**Note:**

- Ellucian Solution Manager features can be used independently of one another.
- Ellucian recommends using either Google Chrome or Mozilla Firefox to access Solution Manager. Internet Explorer is not supported.

In order to provide Banner environment upgrade and provisioning capabilities, Ellucian Solution Manager must be installed on a server (referred to as the "admin server") connected to an institution's managed Banner environments.

To install the Solution Manager 1.6 release, choose one of the following options:

- If an earlier release of Solution Manager (version 1.1 or higher) is already installed, upgrade directly to the 1.6 release using the automated self-update feature described in the online help and User Guide for the currently installed version. Please review [Upgrade to Solution Manager 1.6](#) on page 18 for special upgrade instructions for your current version.
- If Solution Manager has not been installed, install the release following the instructions in [Install Ellucian Solution Manager](#).

---

# Install Ellucian Solution Manager

Install Ellucian Solution Manager to run as a web application on the designated admin server.

**Note:** If you already have an earlier release of Solution Manager installed, you can upgrade directly to the 1.6 release using the automated self-update feature described in the online help and User Guide for the currently installed version. Please review [Upgrade to Solution Manager 1.6](#) on page 18 for special upgrade instructions for your current version.

These instructions are for installing Ellucian Solution Manager on a dedicated admin server running Oracle Enterprise Linux 6 (OEL6) or Red Hat Enterprise Linux 6 (RHEL6) configured with the minimum hardware requirements (see the *Ellucian Solution Manager 1.6 Prerequisites* document for hardware and software requirements).

These instructions assume that Solution Manager is installed using /u01 and /u02 directories for the application and associated content files. To use a different directory, the file paths must be adjusted accordingly throughout the installation process. This includes making customizations to the `prep_services_for_provision.sh` script delivered with the Solution Manager deployment zip file.

**Note:** Portions of the procedure require login to the admin server as `root` (designated by `[ROOT]`).

## Create an esmadmin user

Create a user on the Admin Server to run the Ellucian Solution Manager application. This user will also own all of the files associated with the Ellucian Solution Manager application.

### Procedure

1. `[ROOT]` Log on to the Admin Server as `root` and enter the following command:

```
# useradd -c "Ellucian Solution Manager" -U esmadmin
```

This will create a user and a group named `esmadmin`.

2. Enter the following command, followed by a unique password for the `esmadmin` user when prompted.

```
# passwd esmadmin
```

---

## Set up Ellucian Solution Manager root directories

Follow the steps to set up the root directories.

### Procedure

1. [ROOT] Create a /u01 directory on the 30GB partition on which the operating system is installed.
2. Create a /u02 directory on the second partition.
3. Change the ownership of the directories to specify `esmadmin` as the owner and group.

```
# chown esmadmin:esmadmin /u01
# chown esmadmin:esmadmin /u02
```

**Note:** These instructions assume that Solution Manager is set up using /u01 and /u02 root directories for installing the application and associated content files. If you choose not to use /u01 and /u02 root directories for installing Solution Manager, you will need to change any examples in the installation instructions to the directories you are using as substitutes.

## Activate the rngd service for the admin console

Solution Manager uses OJDBC functionality to communicate with the Banner database to determine which upgrades and patches are already installed in the environment. To support a secure communications channel, the operating system must be able to provide sufficient randomness (entropy) from the `/dev/random` device.

### About this task

The Linux operating system running the admin console may not generate sufficient randomness to support the secure communications channel. This will cause the Solution Manager version checking functionality either to hang or fail to return valid results. Installing the `rngd` service will allow the operating system to generate sufficient randomness for the version checking functionality to operate properly.

### Procedure

1. [ROOT] Check if `rngd` is already installed by logging on to the Solution Manager admin server as `root`. Run the command

```
$ service rngd status
```

This command reports whether or not `rngd` is running. If the response reads `rngd: unrecognized service` then `rngd` is not installed, in which case continue with the `yum` command described in step 2. Otherwise, continue to step 3.

2. Ensure that `rngd` is installed by running the following command:

```
$ yum install rng-tools
```

**Note:** If the above command does not find the rng-tools package, you may have to setup a new yum repository that contains the package. Add the following to a new or existing `.repo` file under `/etc/yum.repos.d`.

```
[ol6_latest]
name=Oracle Linux $releasever Latest ($basearch)
baseurl=http://public-yum.oracle.com/repo/OracleLinux/OL6/latest/$basearch/
gpgkey=http://public-yum.oracle.com/RPM-GPG-KEY-oracle-ol6
gpgcheck=1
enabled=1
```

3. Ensure that rngd service is active after the rngd tools have been installed. The service should restart automatically when the system reboots. This can be accomplished by running the following two commands:

```
$ /sbin/chkconfig rngd on
```

```
$ service rngd start
```

4. Edit the `/etc/sysconfig/rngd` file and add the following line if the rngd service will not start on the Linux server:

```
EXTRAOPTIONS="-r /dev/urandom"
```

## Create a deployment files directory

Create a directory to store Solution Manager installation files.

### Procedure

1. Log on to the admin server as `esmadmin`.
2. Run the following commands to create a directory named `/u02/esmdeploy`.

```
$ cd /u02
```

```
$ mkdir esmdeploy
```

## Download the installation deployment files

Download the file used to install the Ellucian Solution Manager application. You will download the installation file for the 1.5 version of Ellucian Solution Manager. After installing the 1.5 version, you will use Solution Manager's self-update feature to directly upgrade to release 1.6.

### Procedure

1. Download the software by logging into the Ellucian Hub at <https://www.ellucian.com/Solutions/Ellucian-Client-Support/>.



2. Navigate to either **Ellucian Download Center** or **Ellucian Support Center** to access the Software Downloads center.
3. Select the Ellucian Solution Manager product, and select **All** for the "Show Files Posted Within These Days" option under **Filters**.
4. Download the file named `ESM_1.5_DEPLOY.ZIP` under Ellucian Solution Manager 1.X into the `/u02/esmdeploy` deployment files directory.

Log on to the admin server as `esmadmin` when storing the file in the deployment files directory. If the files are put there using another login, change ownership of the file to `esmadmin:esmadmin` after storing the file in the directory.

5. Log on to the admin server as `esmadmin`. Extract and delete the downloaded file by entering the following commands:

```
$ cd /u02/esmdeploy
$ unzip ESM_1.5_DEPLOY.ZIP
```

## Install Java

Install the Java development kit that is used to support the Ellucian Solution Manager application.

### Procedure

1. To install Java into the `/u01` directory, log on to the admin server as `esmadmin`.
2. Run the following commands:

```
$ cd /u01
$ tar xvf /u02/esmdeploy/java.tar
```

You should now have a directory named `/u01/jdk1.7.0_71` containing the files for Java

## Configure access to Java for the admin console

For the Solution Manager admin console to function properly, a Java Runtime Environment (JRE) must be accessible by the admin console application.

### About this task

Modify the profile for the `esmadmin` user to set an environment variable `JAVA_HOME` that contains the path to the Java JDK that you installed in the previous step.

### Procedure

1. Modify the profile for the `esmadmin` user to set environment variable `JAVA_HOME` to contain the path to the Java JDK that you installed in the previous step. For example, if you installed Java into the `/u01/jdk1.7.0_71` directory in the previous step, the `JAVA_HOME` environment variable should contain that directory path.

2. Log off and back on as user `esmadmin` to set the `JAVA_HOME` environment variable for the rest of the installation procedure.
3. Verify that the `JAVA_HOME` variable is set correctly after logging back on as `sysadmin` and running the following command:

```
$ echo $JAVA_HOME
```

## Install and configure Apache Tomcat

Install the Apache Tomcat software used to host the Ellucian Solution Manager application.

### Procedure

1. Install Apache Tomcat on to the `/u01` directory by logging on to the admin server as `esmadmin`. Run the following commands:

```
$ cd /u01
```

```
$ unzip /u02/esmdeploy/apache-tomcat-7.0.56.zip
```

The directory (named `/u01/apache-tomcat-7.0.56`) now contains the Apache Tomcat files.

2. Run the following commands to secure the Tomcat installation:

```
$ cd /u01/apache-tomcat-7.0.56
```

```
$ rm -rf webapps/*
```

3. The Ellucian Solution Manager application uses both Apache Tomcat and Jenkins. Both applications cannot have a default port of 8080, so it is recommended that Tomcat be moved to port 8081.

Edit the delivered Tomcat server configuration file.

```
$ vi /u01/apache-tomcat-7.0.56/conf/server.xml
```

Change all port number references from 8080 to 8081 and save the modified file.

4. Modify Tomcat's startup parameters file to explicitly specify your JDK location and Java parameters.

Edit the delivered file `/u01/apache-tomcat-7.0.56/bin/catalina.sh` and insert the following two lines immediately after the opening comments and before any executable content. Ensure that the `JAVA_HOME` variable reflects the location of your installed JDK if you installed a different version of Java or installed Java in a different directory.

```
export JAVA_HOME=/u01/jdk1.7.0_71
```

```
JAVA_OPTS="-Djava.awt.headless=true -Dfile.encoding=UTF-8  
-server -Xms1536m -Xmx1536m -XX:NewSize=512m  
-XX:MaxNewSize=512m -XX:PermSize=512m -XX:MaxPermSize=512m  
-XX:+DisableExplicitGC"
```

**Note:** If the Java memory parameters for Tomcat allocate less memory than those indicated above, the Ellucian Solution Manager application may not function properly.

5. Execute the following command to ensure that all of the scripts in Tomcat's bin folder are executable:

```
$ chmod +x /u01/apache-tomcat-7.0.56/bin/*.sh
```

6. Copy the Ellucian Solution Manager application executable files into Tomcat.  
Log on to the admin server as `esmadmin`. Copy the delivered `admin.war` file containing the Solution Manager 1.5 executable files into Tomcat's `webapps` folder using the following command:

```
$ cp -p /u02/esmdeploy/admin.war /u01/apache-tomcat-7.0.56/webapps/
```

## Install and configure a Groovy interpreter

Install a Groovy interpreter to support the Solution Manager application.

### Procedure

1. Log onto the admin server as `esmadmin` and create a directory for groovy.

```
$ mkdir /u01/groovy
```

2. Install Groovy in the `/u01/groovy` directory by running the following commands:

```
$ cd /u01/groovy
```

```
$ unzip /u02/esmdeploy/groovy-binary-2.0.5.zip
```

## Create an Ellucian Solution Manager configuration database encryption key

Specify passwords to be used to generate an encryption key for the Ellucian Solution Manager configuration database. Store the encryption key so that it is available to the Ellucian Solution Manager application whenever it starts up. The generated encryption key is used to encrypt the Solution Manager configuration database.

### Before you begin

You will need to specify the following:

- A database file password
- A database user password
- A database user name

**Note:** It is important that you remember and record what you specify for these parameters, as they are not stored on disk and cannot be retrieved from the generated encryption key. They will be needed to use the database console to review the contents of the Ellucian Solution Manager application configuration database if necessary for diagnostic or troubleshooting purposes.

## Procedure

1. To create and store a database encryption key, log on to the admin server as `esmadmin` and run the following commands:

```
$ cd ~
$ mkdir .grails
$ cd /u02/esmdeploy
$ /u01/jdk1.7.0_71/bin/java -classpath
"/adminutils.jar:./commons-codex-1.5.jar"
adminutils.codec.AdminCodecUtils
```

2. Enter the appropriate information when prompted.
  - DB File Password: `<your-database-file-password>`
  - DB User Password: `<your-database-user-password>`
  - DB User Name: `<your-database-user-name>`
  - Persistence Directory: `/u01/adminApp`

The system will generate the following message:

```
Successfully created ESM config file at: /home/esmadmin/.grails/admin-
config.properties
```

3. Enter the following command to display the contents of the Ellucian Solution Manager config file:

```
$ cat /home/esmadmin/.grails/admin-config.properties
```

The `dataSource.password` property displays the encryption key generated from inputs to the program prompt. The `dataSource.username` property displays the user name:

```
#ESM config file
#Tue Nov 26 15:20:13 CST 2015
dataSource.password=9UphkPQ43PH1/hPSHgqbCsOVcd+dK0SL
persistenceDir=/u01/adminApp
dataSource.username=dbuser
```

## Create the Ellucian Solution Manager application data directory

Create the Ellucian Solution Manager application data directory (known as the persistence directory) and the initial configuration files for that directory.

### About this task

**Note:** If you have chosen to use a different content directory than `/u02`, you must edit `config.properties` and add a `contentDir=``<your-location>` value to the file.

**Procedure**

1. Log on to your admin server as `esadmin` and run the following commands:

```
$ cd /u01
$ mkdir adminApp
$ cd adminApp
$ cp /u02/esmdeploy/config.properties .
$ chmod 600 config.properties
$ cp /u02/esmdeploy/ProdCodeMap.txt .
$ chmod 600 ProdCodeMap.txt
```

2. Edit the `/u01/adminApp/config.properties` file to ensure that the correct URL is specified for downloading releases and provisioning content from the Ellucian Solution Manager Release Services.

Find the `downloadRootUrl` property. If the value of that property does not match the line below, edit the file to match the following.

```
downloadRootUrl=https://esmsvc.ellucian.com:8443
```

3. If you chose to install the Groovy interpreter in a different location than what is recommended in the installation instructions above, edit the `groovyLocalRuntimePath` property to specify the actual path to the Groovy interpreter.

```
groovyLocalRuntimePath=/u01/groovy/groovy-2.0.5/bin/groovy
```

4. If you chose to use a folder for the Solution Manager content folder other than `/u02`, edit the `contentDir` property with a value that matches your Solution Manager content folder.
5. Save your edits.

## Start and access the Ellucian Solution Manager application

Start up the Ellucian Solution Manager application and access the application for the first time.

**Procedure**

1. Log on to the admin server as `esadmin` and run the following commands:

```
$ cd /u01/apache-tomcat-7.0.56
$ bin/startup.sh
```

Tomcat will display messages similar to the following:

```
Using CATALINA_BASE: /u01/apache-tomcat-7.0.56
Using CATALINA_HOME: /u01/apache-tomcat-7.0.56
Using CATALINA_TMPDIR: /u01/apache-tomcat-7.0.56/temp
Using JRE_HOME: /u01/jdk1.7.0_71
Using CLASSPATH: /u01/apache-tomcat-7.0.56/bin/bootstrap.jar
```

2. Access the Ellucian Solution Manager application from a browser using the following URL:  
`http://<your-admin-server-hostname>:8081/admin/adminMain`
3. Enter `admin` in the **Username** field and `esadmin` in the **Password** field.

4. Click **Login**. Ellucian Solution Manager displays the empty **Environments** page.
5. Solution Manager will prompt you to change your password. Complete the following fields:
  - **Current Password:** `esadmin`
  - **New Password:** *<your new password>*
  - **Confirm New Password:** *<your new password>*
6. Click **Update**.

Log out of the Ellucian Solution Manager application by selecting **Sign Out** to return to the **Login** page. To log back into the Ellucian Solution Manager application, you will need to use your new password.

Additional information about managing Ellucian Solution Manager users is available in the *Ellucian Solution Manager User Guide*.

## Enter system settings

Complete the information to configure the Solution Manager system settings.

### Procedure

1. Log on to the Ellucian Solution Manager application.
2. Select the **System Settings** tab from the left navigation pane. The **System Settings** page will appear.
3. Complete the following fields on the System Settings page:
  - **Institution Name:** *<your institution name>*
  - **Download Center Login:** *<Login used to access Ellucian Software Download Center through Ellucian Hub>*
  - **Password:** *<Password used to access Ellucian Software Download through Ellucian Hub>*

**Note:** The login entered must be authorized to access the Ellucian Software Download center with code download privileges. The login and password will be used to connect to the Ellucian Solution Manager Release Services to automatically download provisioning content and available Banner releases, Solution Manager templates, and provisioning content.

- **Send on Downloads:** This field controls whether Ellucian Solution Manager uploads configuration information for your environments to Ellucian whenever you download new releases from the Ellucian Solution Manager Release Services. The configuration information is uploaded to a database that can be accessed by Ellucian customer support to verify configuration information when processing a support request.
4. Click **Save**.

When you save, Solution Manager will validate the Download Center Login and Password that you entered by connecting to the Ellucian Solution Manager Release Services. You will not be able to save the page contents without valid credentials. Note that you can save the page with

a blank Download Center Login and Password if you need to update the other information but don't have valid Download Center credentials available.

Ensure that the information has been saved before opting to **Send Now** or else the fields on the **System Settings** page will be cleared.

- To upload configuration information immediately, click **Send Now**.
- To see what information is uploaded, click **View Info**.

Select **Environments** on the left side of the page, the institution name will appear at the top of the **Environments** page.

## Upgrade to 1.6

The installation of Solution Manager 1.5 is complete and you can now upgrade directly to Solution Manager 1.6 as described in [Upgrade to Solution Manager 1.6](#).

Following the upgrade to version 1.6, you can proceed to set up Solution Manager for managing Banner environments as described in [Manage Banner Environments Overview](#).

You should also review the procedures for stopping and starting Solution Manager and making backups of Solution Manager's configuration database in [Manage Solution Manager](#).

---

# Manage Solution Manager

Restart the Solution Manager application and create a backup of the database file.

## Restart Solution Manager

Use the following procedure to stop and restart the Ellucian Solution Manager application.

### Procedure

1. Shut down Solution Manager.

Log on to the admin server as `esmadmin` and run the following commands:

```
$ cd /u01/apache-tomcat-7.0.56
$ bin/shutdown.sh
```

2. Start up Solution Manager.

Log on to the admin server as `esmadmin` and run the following commands:

```
$ cd /u01/apache-tomcat-7.0.56
$ bin/startup.sh
```

**Note:** Messages similar to the following will be displayed by Tomcat upon shutdown and startup:

```
Using CATALINA_BASE:/u01/apache-tomcat-7.0.56
Using CATALINA_HOME:/u01/apache-tomcat-7.0.56
Using CATALINA_TMPDIR:/u01/apache-tomcat-7.0.56/temp
Using JRE_HOME:/u01/jdk1.7.0_71
Using CLASSPATH:/u01/apache-tomcat-7.0.56/bin/bootstrap.jar
```

## Back up Solution Manager configuration database

After installing Solution Manager, you should back up the Solution Manager configuration database periodically.

### Procedure

1. Stop the Solution Manager admin application, as described in [Restart the Ellucian Solution Manager](#) application.
2. Make a copy of the Solution Manager configuration database file, `/u01/adminApp/ESMAdminProdDb.h2.db`.



3. Restart the Solution Manager admin application, as described in [Restart the Ellucian Solution Manager](#).

---

## Upgrade to Solution Manager 1.6

If you just completed the installation of Solution Manager 1.5 or have an existing installation of Solution Manager at version 1.1 through 1.5, you can directly upgrade to the 1.6 version.

After completing the following procedure,

- If you are installing Solution Manager for the first time, go to [Manage Banner Environments Overview](#) to complete setting up Solution Manager to manage existing Banner environments or provision new environments.
- If you are upgrading an existing Solution Manager installation, follow the instructions included in [Upgrading from release 1.1 or 1.2](#), if applicable. After you've completed that section, you will have completed the upgrade to Solution Manager 1.6 and are ready to continue using Solution Manager to manage your Banner environments.

## Upgrade to Solution Manager 1.6

Upgrade to Solution Manager 1.6 to maintain and upgrade Banner environments.

### Procedure

1. Log on to Solution Manager and click **Get New Releases** on the **Environments** page to download available releases.  
Solution Manager will download all releases available to your current Solution Manager version, including the upgrade to Solution Manager 1.6. At the completion of the download you should be notified that a system update is available.
2. Select the **System Updates** tab to see the available updates. The table will display the Solution Manager updates that are available to be installed. Select the 1.6 version, and click **Perform Update**.
3. The Solution Manager application will shut down temporarily while the update is performed. A wait spinner graphic and "Upgrade in Progress" notification will be displayed during the update. At the completion of the update, the application will restart and display the login page.
4. Log on to Solution Manager. Click **Get New Releases** to download additional releases that are only available to the Solution Manager 1.6 version, including templates that control some of the Solution Manager 1.6 functionality.
5. Select the **Templates** tab. Find the row in the Templates table for the highest version number that appears in the table for a template named `ProdType-BannerERP-<version>` (for example, `ProdType-BannerERP-1_4_3`, which is the 1.4.3 version of that template).  
This template installs a plug-in for Solution Manager that provides the latest version checking logic for any Banner environments that you want to manage with Solution Manager. You must activate the template to ensure that Solution Manager is using the latest available logic for checking installed versions of products in your Banner environments.
6. Click anywhere (except for the **View XML** icon) in the row for the `ProdType_BannerERP` template to display the content items for the template.

- a) On the Content Items page for that template select each row in the **Get From Ellucian** column.
  - b) Click **Get From Ellucian** to download the associated content items (there may be only one content item to download).
7. Following the content items download, some of the items may show a status of `Post Acquire Pending`.
    - a) For those items, click on the icon in the item row in the **Post Inst** column.
    - b) Read and follow the information that displays on the post installation instructions page, and click **Mark Complete** when you have completed those instructions.
  8. When all the content items for the template have a status of `Ready`, click **Mark Active** to activate the template.

## Upgrading from release 1.1 or 1.2

If you are upgrading directly to Solution Manager version 1.6 from version 1.1 or 1.2 and have already configured existing environments or provisioned new environments in your current version of Solution Manager, perform the following procedure to make sure the configuration information for your environments is correct for release 1.6.

### About this task

Disregard this section if you are upgrading from Solution Manager 1.3 or higher.

### Procedure

1. Go to the **Applications** and **App Servers** pages to verify that all applications are linked to the correct app server or machine, and that all app servers are linked to the correct machine instance.
2. Correct any linkage issues to ensure that the configuration information in the Solution Manager configuration database is accurate for each managed environment.
3. Access the **Credentials** page for each environment, then confirm that the **Install User Login Sequence** is correct. Repeat this step for the **Compile Login Sequence** for the forms compilation INB application. The default setting for the two login sequences in earlier Solution Manager releases contains the following fields:
  - a) **Credentials** page: **Install User Login Sequence** field:

```
Wait password:  
RC (banner.target.user.password)
```
  - b) **Forms Compiler INB Application** page: **Compile Login Sequence** field:

```
Wait password:  
RC (banner.form.compile.host.user.password)
```

---

For Solution Manager versions 1.2 and earlier, the Banner Upgrade Installer ignored the first two lines of the login sequence, but required that they be present. These lines should be removed from all login sequences.

Review the login sequence values to ensure that these lines are not contained in the login sequence. Ensure that the remainder of the sequence is correct before attempting to install Banner upgrades through Solution Manager 1.6.

Environments created or added to Solution Manager using release 1.3 or later have the correct login sequence, meaning that the lines listed above do not need to be removed.

4. Alter the **Compile Login Sequence** for the INB application to set the `ORACLE_INSTANCE` environment variable for forms compilation.

In earlier releases of Solution Manager, the Banner Upgrade Installer forms compilation process set the `ORACLE_INSTANCE` variable automatically, but the manner in which it was setting the variable was not correct for all client installations. When upgrading to Solution Manager 1.6 from those earlier releases, you must add lines to the **Compile Login Sequence** to set the appropriate value for `ORACLE_INSTANCE` for your forms compiler machine.

Example (specify the path that is appropriate for your forms compiler machine):

```
RC export ORACLE_INSTANCE=$ORACLE_BASE/ASINST_1
Wait $
```

---

## Manage Banner environments overview

Manage Banner upgrade downloads and automated installation of Banner releases.

When you have completed installation of Solution Manager you are ready to begin using Solution Manager to update existing Banner environments and to provision new Banner environments.

In order to update existing Banner environments or provision new Banner environments, Solution Manager uses the open-source Jenkins tool to remotely execute processes on machines in your Banner environments. So the first thing you need to do is install Jenkins on your Solution Manager admin server, as described in [Install and secure Jenkins](#).

After Jenkins has been installed, you can proceed to update existing Banner environments or provision new Banner environments.

## Update existing Banner environments

Use Solution Manager to update a Banner environment by selecting and automatically installing and deploying available Banner upgrade releases.

In order to update an existing Banner environment, you must first add the environment to Solution Manager and enter configuration information for the environment. See *Manage Banner Environments with Solution Manager* in the *Ellucian Solution Manager User Guide*.

Also, to support automated upgrades and deployments to the environment, you will need to install Jenkins remote execution agents, referred to as “upgrade communication agent” and “deployment agents”, on some machines in your Banner environment, as described in the *Solution Manager User Guide*. See [Install upgrade communication agent into Banner environment](#) and [Create deployment agents](#) in this manual for the procedures for installing the required Jenkins agents.

The Solution Manager automated upgrade process uses SSH and SFTP to make connections between machines in your Banner environment during upgrade process. By default those connections are made using a password-authenticated connection between the machines. If you do not want the system accounts used for those connections to allow password-authenticated logins, you can choose to set up SSH keys authentication for those connections, as described in [SSH connections in Solution Manager](#).

If any of the machines in your Banner environment are Windows machines, you will need to perform additional setup on those machines as described in [Setup Windows machines in managed Banner environments](#) to allow Solution Manager to access those machines for automated upgrades and deployments.

In order to provision new applications into existing environments, in addition to entering the configuration information for the environment into Solution Manager you will need to download a template and associated content items that supports provisioning of the new application. Documentation accompanying the template will explain what applications are provisioned by the template and hardware and software requirements for provisioning those applications. For available application provisioning templates, see the documents available under Ellucian Solution Manager in the Documentation Libraries section of the Ellucian Support Center.

## Provision new Banner environments

Provisioning a new Banner environment installs a complete Banner environment onto hardware resources (physical or virtual machines) that you provide.

For more information, see *Provision Banner Environments* in the *Ellucian Solution Manager User Guide*.

In order to provision new Banner environments, you must prepare Solution Manager for provisioning, as described in [Configure Solution Manager for Banner environment provisioning](#).

---

## Install and secure Jenkins

Jenkins must be installed to use Ellucian Solution Manager to install Banner upgrades into Banner environments, to provision Banner environments, and to provision new applications into existing Banner environments. This installation process installs Jenkins 1.645.

Solution Manager uses Jenkins for remote execution of processes on the machines in your Banner environments to facilitate automated installation and deployment of upgrades and provisioning of new software.

After installing and starting Jenkins, you should secure Jenkins. It will also be necessary to configure the Jenkins URL for Solution Manager.

## Install and start Jenkins

Jenkins is the infrastructure software used by the Ellucian Solution Manager application for Banner upgrade installation and provisioning of applications and environments.

### Procedure

1. Log on to the admin server as `esmadmin` and run the following scripts:

```
$ cd /u01
$ mkdir jenkins
$ cd jenkins
$ cp /u02/esmdeploy/jenkins.war .
```

2. Create a script for starting Jenkins.

```
$ cd /u01/jenkins
$ vi start.sh
```

The `start.sh` script should contain the following lines:

```
export JENKINS_HOME=/u01/jenkins
nohup /u01/jdk1.7.0_71/bin/java -jar jenkins.war &
```

3. After saving `start.sh`, enter the following command to make the file executable:

```
$ chmod +x start.sh
```

4. Start Jenkins by running the following scripts:

```
$ cd /u01/jenkins
$ ./start.sh
```

**Note:** Press **Enter** a second time after executing the last command displayed above to get back to the OS prompt.

5. After Jenkins starts, enter the following URL in a web browser: `http://<your-admin-server-hostname>:8080`

The Jenkins dashboard page appears.

The default Jenkins installation is unsecured. Ellucian recommends securing Jenkins so that it is not open to all who have network access to the admin server. To secure access to Jenkins, follow the instructions in the [Secure Jenkins](#) section.

## Secure Jenkins

Secure Jenkins so that credentials are required to access the console.

### Procedure

1. Access the Jenkins console through a browser using the following URL: `http://<your-admin-server-hostname>:8080`
2. Navigate to the Jenkins configuration page by clicking **Manage Jenkins > Configure Global Security**.
3. Find and select the **Enable Security** check box on the Jenkins security and configuration page. The page displays the available security options.
4. To limit the port number used for Jenkins remote execution agents to connect to the Jenkins master, select **Fixed** and specify the port number for the **TCP port for JNLP slave agents** option.

**Note:** Ellucian recommends using port 8082, but you can choose whichever port you prefer.

5. Select **Jenkins' own user database** from the Security Realm section.

**Note:** You MUST leave the **Allow users to sign up** check box selected until after a Jenkins administrator account is created. Otherwise, you will lock yourself out of the system.

When a functional Jenkins instance with an administrative user is defined, re-visit this form to clear the checkbox. This will prevent others from attempting to sign up. In the interim, people may be able to create their own account, but the account would have no permissions defined in the application.

6. In the Authorization section, select **Matrix-based security**. A permissions matrix appears. Clear all options for the Anonymous user, including Read permissions.
7. Define the permissions for the admin user that you will soon create by typing the username `admin` into the **User/group to add** box and selecting **Add**. After that user appears as a row in the security matrix, select all of the check boxes to ensure that this admin user has complete authority within Jenkins.
8. Click **Save**.



9. Restart Jenkins by killing the existing Jenkins process and then restarting it. To restart Jenkins, log on to your admin server as `esmadmin`. Use the `ps` command to find the process ID of the existing Jenkins process and kill it, similar to the following sequence of commands:

```
$ ps -ef | grep jenkins
esmadmin 5458 1 85 15:39 pts/0 00:00:11 /u01/jdk1.6.0_31/bin/java -
jar jenkins.war
esmadmin 5490 4793 0 15:40 pts/0 00:00:00 grep jenkins
$ kill -9 5458
$ ps -ef | grep jenkins
esmadmin 5498 4793 0 15:40 pts/0 00:00:00 grep Jenkins
```

10. Start Jenkins. See [Install and Start Jenkins](#) for details.
11. After restarting, access Jenkins again through the web console. Use the **Create an account** link to create your admin account. Enter `admin` for the Username field and complete the remaining fields. After adding the admin user to Jenkins, you should revisit the Jenkins security configuration and clear the check box that enables new users to sign up.
12. Access the Jenkins security token to authorize the Ellucian Solution Manager admin console to control Jenkins.
  - a) Click on the login information in the upper-right corner (adjacent to the **Log out** link).
  - b) Select **Configure** from the options presented on the user page.
  - c) Select **Show API token**.
  - d) Select **Change API token** to generate a new token value as recommended. Copy the displayed token value, then click **Save**.

You will use the new API token to update the Solution Manager configuration file so it can use the token for secure access to Jenkins (see [Configure Solution Manager for Jenkins](#)). Periodically updating the Ellucian Solution Manager config properties will enhance the security of the Ellucian Solution Manager console's Jenkins instance. Ellucian Solution Manager application will be able to control Jenkins with Jenkins security turned on.

## Configure Solution Manager for Jenkins

After installing Jenkins, modify the Ellucian Solution Manager configuration file to provide the URL and secure credentials to access Jenkins, then restart the Ellucian Solution Manager application.

### Procedure

1. Log on to the admin server as `esmadmin` to edit the Solution Manager configuration file for the Jenkins URL using the following commands:

```
$ cd /u01/adminApp
$ vi config.properties
```

2. Using the editor, find the line that reads `jenkinsUrl` and set it to

```
jenkinsUrl=http://<your-admin-server-hostname>:8080
```
3. Find or add the following properties and enter the corresponding values:

---

```
jenkinsUsername=admin
```

```
jenkinsToken=<your-generated-Jenkins-API-token>
```

4. Save the edited file and [restart the Solution Manager application](#) so it will read the updated configuration file. Periodically updating the Solution Manager config properties file with a new API token, as described in the preceding steps will enhance the security of Solution Manager's Jenkins instance.

## Install upgrade communication agent into Banner environment

For Ellucian Solution Manager to automate the installation of upgrades into the managed Banner environment, the environment must have an upgrade communications agent installed.

The upgrade communications agent is a Jenkins remote execution agent that communicates with the Jenkins server software that is installed on your admin server.

## Install Jenkins slave on Jobsub machine and set up agent environment

Log on to the Jobsub machine in the managed Banner environment as the Install User to set up the upgrade agent.

### About this task

If your Jobsub machine is a Windows machine, see [Install Jenkins slave on Windows Jobsub machine](#).

### Procedure

1. Verify Java JDK is installed on the Jobsub machine. If a Java JDK is not installed on the application server, install one now.  
Ellucian recommends using Java 1.7.
2. Verify that the `JAVA_HOME` environment variable is set.  
The deployment agent uses the `JAVA_HOME` variable in order for the deployment job to locate the java run time and work properly.
3. Create the folder where the Jenkins slave will be installed and then make that your current directory by entering the following commands:

```
# mkdir /u01/bmui_jenkins
# cd /u01/bmui_jenkins
```

4. Load the Jenkins slave software into the new directory by entering the following command:

**Note:** Make sure to substitute the IP address of the Ellucian Solution Manager admin server on the network connecting the Jobsub machine to the admin server for `<SolutionManagerIPAddress>`.

```
# wget http://<SolutionManagerIPAddress>:8080/jnlpJars/slave.jar
```

5. Create a `start.sh` script in the `/u01/bmui_jenkins` directory containing the following two lines (where `<EsmlpAddress>` is the IP address or host name of the Ellucian Solution Manager admin server on the network that connects the admin server to the Jobsub machine

and *<environment-id>* is the ID you specified for the managed environment in Ellucian Solution Manager).

Ensure that the correct Java runtime path is used in the command lines below. Insert the exact "-secret xxxxxxxxxxxxxxxx" text that was previously saved. This results in a startup command like the following:

```
cd /u01/bmui_jenkins
/usr/bin/nohup/u01/jdk/bin/java -jar slave.jar -jnlpUrl http://
<EsmIpAddress>:8080/computer/<environment-id>_BMUI_AGENT/slave-
agent.jnlp -secret XXXXXXXXXXXX >>jslave.log 2>&1 &
```

6. Change permissions on the "start.sh" script to make it executable by entering the following command:

```
# chmod +x start.sh
```

7. Change ownership of the /u01/bmui\_jenkins directory and its contents to the user ID and group that will be used to run the upgrade installation script by entering the following command.

In the example, *banner* is the Install User and *banner* is the group to which that the install user belongs).

```
# chown -R banner:banner /u01/bmui_jenkins
```

8. Start up the Jenkins slave by logging on to the Jobsub application as the install user and entering the following commands.

```
$ cd /u01/bmui_jenkins
$ ./start.sh
```

For security reasons, you should not start the Jenkins slave as "root".

9. Enable automatic restart when the Jobsub machine is rebooted by adding the appropriate configuration for your Jobsub machine operating system to automatically start the Jenkins slave as the install user when the system is booted.

## Install Jenkins slave on Windows Jobsub machine

Log on to the Jobsub machine in the managed Banner environment as the local administrator account to perform the steps required by the Solution Manager communications agent.

### Before you begin

- Verify Java JDK
- Verify JAVA\_HOME
- Verify Powershell

### Procedure

1. Verify Java JDK is installed on the Windows Jobsub machine.

If you do not have a Java JDK on the Jobsub machine, then install one. Ellucian recommends using Java 1.7. To check the Java version on a Windows server, use the Start menu to access **Java** and select **About Java**.

2. Verify JAVA\_HOME.  
Set the JAVA\_HOME variable in order for the Deployment Agents to work properly. Environment variables are found under **System Properties > Advanced > Environment Variables**.
3. Verify PowerShell.  
Deployment agents need PowerShell Version 2.0.
  - a) In order to verify that PowerShell is installed (and the version), launch the `Run` command from the Start menu and enter `PowerShell`.
  - b) In the PowerShell command prompt, enter `$PSVersionTable`.
4. In the Jenkins console, locate the slave created for deployments.
5. Copy the URL that points to the newly created agent page.  
`http://m019101.sungardhe.com:8080/computer/SERVERNAME_BMUI_AGENT/`
6. Open the link in a web browser. The **Launch** button will appear.
7. Click **Launch** to start the installation process.
8. Click **Next** and **Continue** on all subsequent screens until installation is complete.  
Java security may block the installation application. It may necessary to add an exception to allow the program to execute.

## Add a Windows service

After the installation is complete, it will start up the agent in a small Java window. Add a Windows service so that Jenkins will start each time the system starts up.

### Procedure

1. In the slave agent window, click **File > Install as Windows Service**.  
Next, configure the Jenkins service to run as the administrator account so that the scripts will run properly.
2. On the **Start** menu, select **Administrative Tools** and **Services**.
3. In the **Services** window, locate and double-click on the Jenkins Slave service.
4. Select the **Logon** tab.
5. Select **This Account** and enter the credentials for the administrator account and click **OK** to save your settings.
6. Right-click on the Jenkins Slave service and click **Restart**.  
This starts the Jenkins slave on the Windows machine as the administrator account.

## Create deployment agents

The deployment agent is a Jenkins agent that will facilitate the communication between Solution Manager and application server machines and orchestrate the deployment steps.

For more information regarding automated deployments, see *Deployment Jobs* in the *Ellucian Solution Manager User Guide*.

It is necessary to define and install an agent on the Jobsub application machine and each application server machine that contains a deployment target app server in the managed environment. This will allow Solution Manager to automatically run deployment jobs. Environments provisioned with Solution Manager 1.1 and later should have the necessary agents already in place.

You should have already defined and installed an upgrade agent on the Jobsub machine. Use that same agent when entering configuration information for the Jobsub machine for deployments (see the **Env Settings** page in the admin console to find the upgrade agent name). You will need to create additional agents that run on the application server machines, and they need to run as the same user that is used to run the application server (typically "oracle" for a Weblogic application server).

**Note:** If you have not yet defined and installed an agent on your Jobsub machine, see [Install upgrade communication agent into Banner environment](#). To create the agents on the application servers, execute the following steps, one time for each application server machine for each environment.

## Define a Jenkins slave on the Solution Manager Jenkins server

Define a deployment communications agent in the managed Banner environment.

### About this task

**Note:** For each application server machine in each managed Banner environment in Solution Manager, you must define a unique Jenkins deployment agent. If you have multiple environments sharing the same machine as an application server, you should define a separate deployment agent for each environment.

When defining the Jenkins deployment agent, the agent name should reflect the environment, the server role, and the application server host name. This will make it easy to determine which environment is currently executing a deployment.

Each agent should be defined with a unique root directory, referred to as the Remote FS Root when creating the agent in Jenkins. This will ensure that the Jenkins workspaces for each environment are kept separate.

## Procedure

1. Log on to the Jenkins server on your admin server (as described in "Install and Start Jenkins" in *Ellucian Solution Manager Installation and Configuration*).
2. Select **Manage Jenkins > Manage Nodes**.
3. On the **Manage Nodes** page, select **New Node**.

- a) On **Node Name**, enter a unique name.

Ellucian recommends the following naming convention for deployment agents:

`<environment-name> appserver <application-host-name>`

where `<environment-name>` is the name of the environment in Solution Manager, and `<application-host-name>` is the host name specified in the targeted app machine within the environment.

- b) Select the **Dumb Slave** option and then click **OK**.

- c) On **Description**, enter the agent name again.

- d) On **# of executors:**, enter 1.

- e) On **Remote FS Root:** Enter the path where the agent will be installed on the application server in the managed Banner environment.

Ellucian recommends using the path `/u01/deployment_jenkins_<environment-name>`. On Windows servers, use `c:\deployment_jenkins<environment-name>` or similar (where `<environment-name>` is the name of the environment for which the Jenkins agent will be used). Ensure that a directory is created if one does not already exist.

- f) On **Labels:** Enter `<environment-name> appserver <application-host-name>` where `<environment-name>` is the name of the environment in Solution Manager, and `<application-host-name>` is the host name specified in the targeted app machine within the environment.

- g) On **Usage:** Select the **Leave this machine for tied jobs only** option.

- h) On **Launch Method:** Select the **Launch slave agents via Java Web Start** option.

4. Click **Save**.

**Note:** If Jenkins is left unsecured (not recommended), the value for the "secret" tag will not appear and can be omitted.

5. Click on the agent in the resulting dialog. In the center of the screen for secured Jenkins instances, the following will appear (run from the slave command line):

```
java -jar slave.jar -jnlpUrl
http://nn.nn.nn.nn:8080/computer/XXXXX/slave-agent.jnlp -secret
3f191c1f83126b161e7956a757fb5ae9adf7bd9103792482f229e9aaacf67631
```

The `-secret xxxxxxxxxxxxxxxx` text is the secret key that permits an agent to be launched. This secret value authenticates the startup of that node only. It cannot be used to login to Jenkins for other operations.

6. Record the `-secret xxxxxxxxxxxxxxxx` text for use when putting the deployment agent on your application server.

---

## Install Jenkins slave on an application server / set up agent environment

### About this task

Log on to the application server machine in your managed Banner environment as "root" to set up mount points required by the Solution Manager communications agent, as specified in *Deployment Jobs* in the *Ellucian Solution Manager User Guide*. If your application server machine is a Windows machine, see [Install Jenkins slave on Windows Application Server](#) instead of following the procedure in this section.

### Procedure

1. Log on to the application server machine as the user that we used to run the application server (Weblogic or Tomcat) that Solution Manager will deploy applications to.
2. Create a link named `/u01/jdk` to a Java JDK installed on the application server machine by entering a command similar to the following (with the actual path to the Java JDK on your Job Sub application substituted for `/usr/java/jdk1.7.0_71` in the example).

```
# ln -s /usr/java/jdk1.7.0_71 /u01/jdk
```

If you do not have a Java JDK on the Job Sub application already, then you need to install one first. Ellucian recommends using Java 1.7.

3. Create the folder where the Jenkins slave will be installed and make that your current directory by entering the following commands.

```
# mkdir /u01/deployment_jenkins
# cd /u01/deployment_jenkins
```

4. Load the Jenkins slave software into the directory you just created by entering the following command.

```
# wget http://EsmIpAddress:8080/jnlpJars/slave.jar
```

Make sure to substitute the IP address of the Solution Manager admin server on the network connecting the Job Sub application to the admin server for *EsmIpAddress*.

5. Create a "start.sh" script in the `/u01/deployment_jenkins` directory containing the following two lines (where *EsmIpAddress* is the IP address of your Solution Manager admin server on the network that connects the admin server to the Job Sub application and *environment-id* is the ID you specified for the managed environment in Solution Manager).

Insert the exact "-secret xxxxxxxxxxxxxxxx" text that was previously saved. This results in a startup command like the following:

```
cd /u01/deployment_jenkins
/usr/bin/nohup /u01/jdk/bin/java -jar slave.jar -
jnlpUrl http://EsmIpAddress:8080/computer/<environment-
name>_appserver_<application-host-name>/slave-agent.jnlp -secret
XXXXXXXXXXXX >>jslave.log 2>&1 &
```



6. Change permissions on the "start.sh" script to make it executable by entering the following command:

```
# chmod +x start.sh
```

7. Change ownership of the /u01/deployment\_jenkins directory and its contents to the user ID and group that you will use to run the upgrade installation script (see Enter upgrade-related credentials information) by entering the following command. In the example, "banner" is the Install User and "banner" is the group to which that the Install User belongs).

```
# chown -R banner:banner /u01/deployment_jenkins
```

8. Start up the Jenkins slave by logging on to your Job Sub application as the Install User and entering the following commands. For security reasons, you should not start the Jenkins slave as "root".

```
$ cd /u01/deployment_jenkins  
$ ./start.sh
```

9. If you want the Jenkins slave to restart automatically when your Job Sub application is rebooted, add an appropriate script to /etc/init.d to start the Jenkins slave as the Install User. For security reasons, you should not start the Jenkins slave as "root".

## Install Jenkins slave on Windows application server

Log on to the Windows application server machine in the managed Banner environment as the local administrator account to install and set up the Solution Manager communications agent.

### Before you begin

- Verify Java JDK
- Verify JAVA\_HOME
- Verify Powershell

### Procedure

1. Verify Java JDK is installed on the Windows Jobsub machine.  
If you do not have a Java JDK on the Jobsub machine, then install one. Ellucian recommends using Java 1.7. To check the Java version on a Windows server, use the Start menu to access **Java** and select **About Java**.
2. Verify JAVA\_HOME.  
Set the JAVA\_HOME variable in order for the Deployment Agents to work properly. Environment variables are found under **System Properties > Advanced > Environment Variables**.
3. Verify PowerShell.  
Deployment agents need PowerShell Version 2.0.

- a) In order to verify that PowerShell is installed (and the version), launch the `Run` command from the Start menu and enter `PowerShell`.
- b) In the PowerShell command prompt, enter `$PSVersionTable`.
4. In the Jenkins console, locate the slave created for deployments.
5. Copy the URL that points to the newly created agent page.  
`http://m019101.sungardhe.com:8080/computer/SERVERNAME_BMUI_AGENT/`
6. Open the link in a web browser. The **Launch** button will appear.
7. Click **Launch** to start the installation process.
8. Click **Next** and **Continue** on all subsequent screens until installation is complete.  
Java security may block the installation application. It may necessary to add an exception to allow the program to execute.

## Add a Windows service

After the installation is complete, it will start up the agent in a small Java window. Add a Windows service so that Jenkins will start each time the system starts up.

### Procedure

1. In the slave agent window, click **File > Install as Windows Service**.  
Next, configure the Jenkins service to run as the administrator account so that the scripts will run properly.
2. On the **Start** menu, select **Administrative Tools** and **Services**.
3. In the **Services** window, locate and double-click on the Jenkins Slave service.
4. Select the **Logon** tab.
5. Select **This Account** and enter the credentials for the administrator account and click **OK** to save your settings.
6. Right-click on the Jenkins Slave service and click **Restart**.  
This starts the Jenkins slave on the Windows machine as the administrator account.

---

# Set up SSH keys authentication

## SSH key based connections

Machines can be configured such that User-A on Server-A can connect to Server-B as User-B without passwords being required.

This is achieved through the use of SSH keys. For example, Server-A and Server-B will communicate that User-A can connect to Server-B as User-B without having to provide the password for User-B. This is possible under the following conditions:

- User-A has placed their private key on Server-A in the `<HOME_DIRECTORY_OF_USER_A>/ .ssh` folder
- User-A has published their public key to User-B on Server-B through the `<HOME_DIRECTORY_OF_USER_B>/ .ssh/authorized_keys` file

## Prerequisites for Solution Manager to use SSH keys

Ensure that the following steps are completed so that Ellucian Solution Manager is equipped to accommodate a SSH connection using SSH keys instead of password authentication.

If two servers Server-A and Server-B are configured such that User-A from Server-A can create a SSH connection to Server-B as User-B using SSH keys instead of passwords, the following steps must be performed so that Ellucian Solution Manager can recognize and use such a setup.

## Configure Solution Manager settings

Ensure that Solution Manager is equipped to handle a connection using SSH keys.

### Procedure

1. Log in as `User A` to Server A.
2. Navigate to the `<HOME_DIRECTORY_OF_USER_A>`.  
If the `.ssh_esm` folder does not exist in `<HOME_DIRECTORY_OF_USER_A>`, create one now.
3. Create a file titled `ssh_<USER_B>_<SERVER_B>.nopassword`.  
If SSH key-based communication has been setup between `banner@192.111.222.333` and `oracle@192.111.222.444`, create a file titled `ssh_oracle_192.111.222.444.nopassword` in the `/home/banner` folder on `192.111.222.333`.

If SSH key-based communication has been setup between `oracle@192.111.222.333` and `oracle@192.111.222.333`, create a file titled `ssh_oracle_192.111.222.333.nopassword` in the `/home/oracle` folder on `192.111.222.333`.

**Note:** Replace all server names, user names and user home locations with the corresponding values for the environment.

## Set up SSH keys authentication

### SSH connections in ESM

Review the prerequisites to ensure that SSH key-based communication is enabled for the combination.

Number	User A on Server A	User B on Server B	Description
1	UserA: OS user meant to run the BMUI Jenkins agent on the Jobsub machine (usually the same as the Install User specified on the Env Credentials configuration page)  ServerA: Jobsub machine	UserB: Install User (specified on Env Credentials configuration page in Solution Manager, usually 'banner')  ServerB: Jobsub machine	BMUI is started by the Jenkins job and must log into the Jobsub machine through SSH as the Install User to execute the steps for installing the upgrade.
2	UserA: Install User (specified on Env Credentials configuration page, usually as 'banner')  ServerA: Jobsub machine	UserB: Install User (specified on Env Credentials configuration page, usually 'banner')  ServerB: Jobsub machine	After logging into the Jobsub machine, BMUI uses SFTP to retrieve the SQL script for checking versions of software installed in the environment and to update the <code>login.sql</code> script.
3	UserA: OS user used to run the BMUI Jenkins agent on the Jobsub machine (usually the same as the Install User specified on the	UserB: Compile Host User (specified on the Application configuration page for the INB application that is designated as the forms compiler)	BMUI logs from the Jobsub server into the INB forms compiler server through SSH to compile forms that need to be compiled for each upgrade.

Number	User A on Server A	User B on Server B	Description
	Env Credentials configuration page) ServerA: Jobsub machine	ServerB: Forms compilation host machine (machine that is selected on the Application configuration page for the INB application that is designated as the forms compiler)	
4	UserA: Compile Host User (specified on the Application configuration page for the INB application that is designated as the forms compiler) ServerA: Forms compilation host machine (machine that is selected on the Application configuration page for the INB application that is designated as the forms compiler)	UserB: Install User (specified on Env Credentials tab for the environment in Solution Manager, usually 'banner') ServerB : Jobsub machine	After logging into the forms compiler server, BMUI uses SFTP to log back into the Jobsub server to get the forms source files from the Banner code tree and copy them to the forms compiler server to compile the forms.
5	UserA: Compile Host User (specified on the Application configuration page for the INB application that is designated as the forms compiler) ServerA: Forms compiler machine (machine that is selected on the Application configuration page for the INB application that is designated as the forms compiler)	UserB: INB Host User (specified on each INB application) ServerB: INB application host machine (specified on the Application configuration page for each INB application)	After successfully compiling forms, BMUI uses SFTP to connect to each specified INB server to push the newly compiled executables to the INB executables directory on each INB server.
6	UserA: OS user used to run the BMUI Jenkins agent on the Jobsub machine	UserB: User ID (specified in the Application Properties section of the	If there are SSB objects delivered on an upgrade, BMUI connects to the SSB

---

Number	User A on Server A	User B on Server B	Description
	(usually the same as the Install User specified on the Env Credentials configuration page)  ServerA: Jobsub machine	SSB Application configuration page)  ServerB: SSB machine (machine specified on the SSB Application configuration page)	server through SFTP to copy the SSB objects to the SSB staging area (the WebServer Doc Root Path and the Banner SSB Cascade EAR File Staging Path fields on the SSB Application configuration page)

---

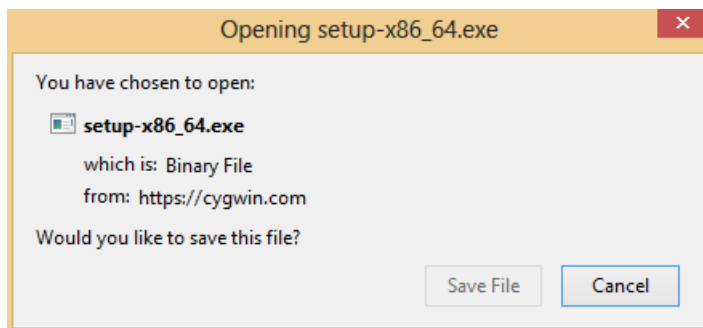
# Set up Windows machines in managed Banner environments

## Install Cygwin (download package)

All of the Windows Server 2008 R2 or later servers that are managed by Solution Manager require that Cygwin version 1.7.35 or later is installed. This includes the Jobsub machine and any application server machines on which Solution Manager will need to run automated deployments

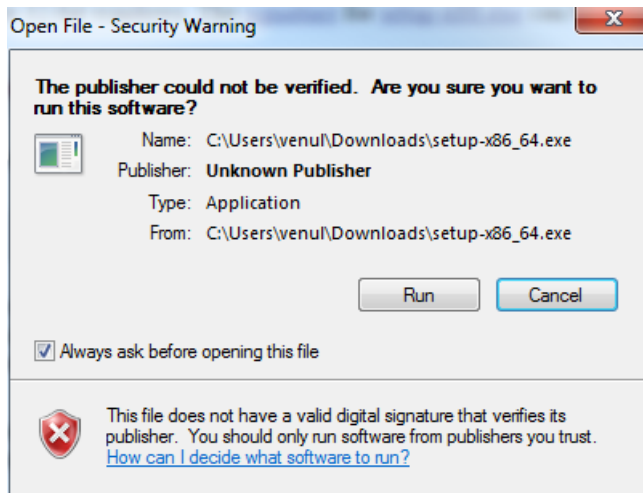
### Procedure

1. Go to <https://cygwin.com/>. Under **Cygwin**, select **Install Cygwin**.
2. Select Cygwin for 32/64-bit version of Windows.

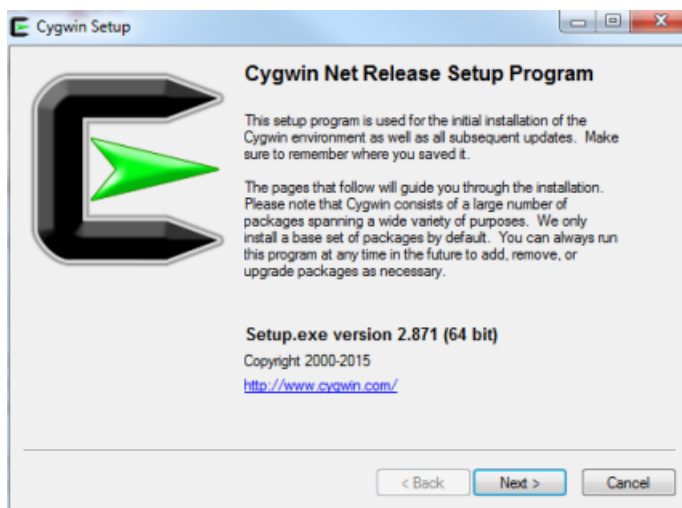


Save the file.

3. Access the directory where the file is saved. Right-click and select **Run as administrator**. Click on **Run**.



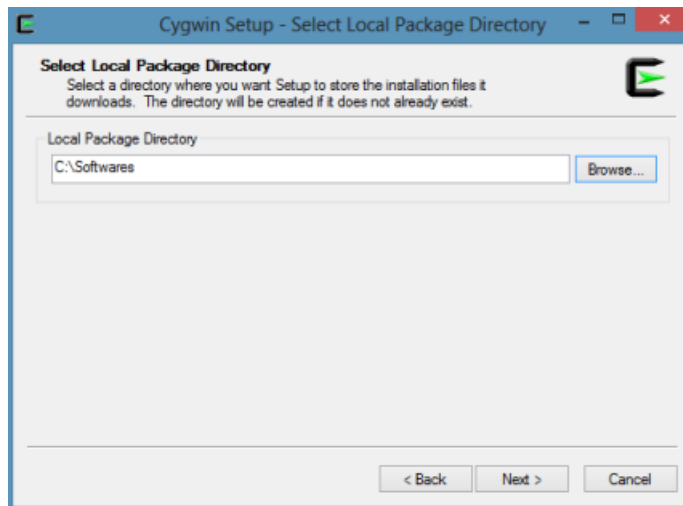
4. The Cygwin Net Release Setup Program installation will start.



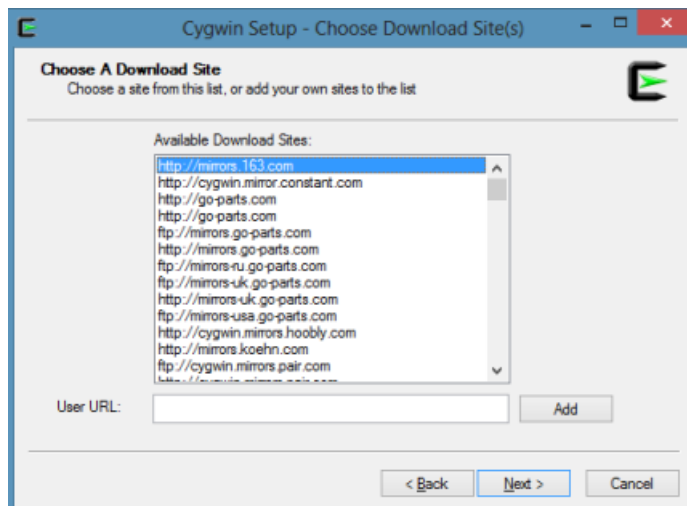
Click **Next**.

- a) Select the **Download Without Installing** option and **Next**.
- b) Select a local directory where you want to download the software and **Next**.

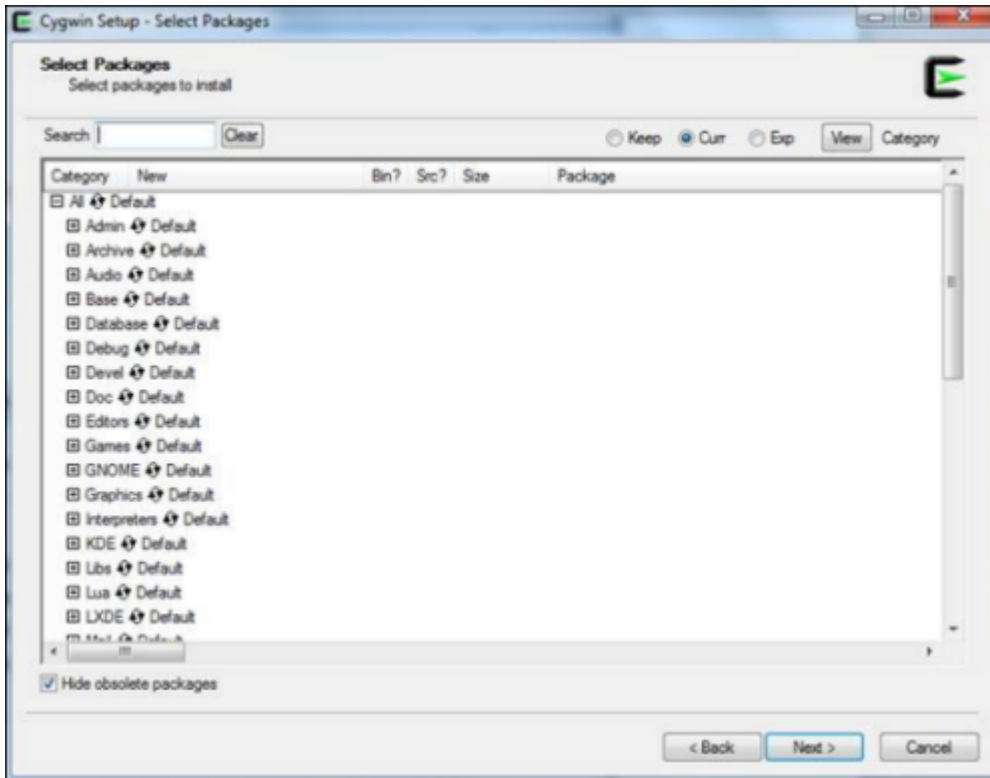




- c) Select the **Direct Connection** option and click **Next**.
- d) Select a download site and click **Next**.



The package download will begin. After the downloading is complete, the following screen will appear.



- Under **Category**, expand the **Admin** option.

Category	New	Bin?	Src?	Size	Package
[-] All	Default				
[-] Admin	Default				
[-] Admin	Skip	n/a	n/a	49k	attr: Utilities for managing filesystem extended attributes
[-] Admin	Skip	n/a	n/a	53k	cron: Vixie's cron.
[-] Admin	Skip	n/a	n/a	62k	cygrunsrv: NT/W2K service initiator
[-] Admin	Skip	n/a	n/a	7k	libattr1: Shared lib for managing filesystem extended attributes
[-] Admin	Skip	n/a	n/a	20k	shutdown: Shutdown, reboot, hibernate or suspend the machine
[-] Admin	Skip	n/a	n/a	267k	stow: Manage local software installations
[-] Admin	Skip	n/a	n/a	338k	syslog-ng: Next generation system logging daemon

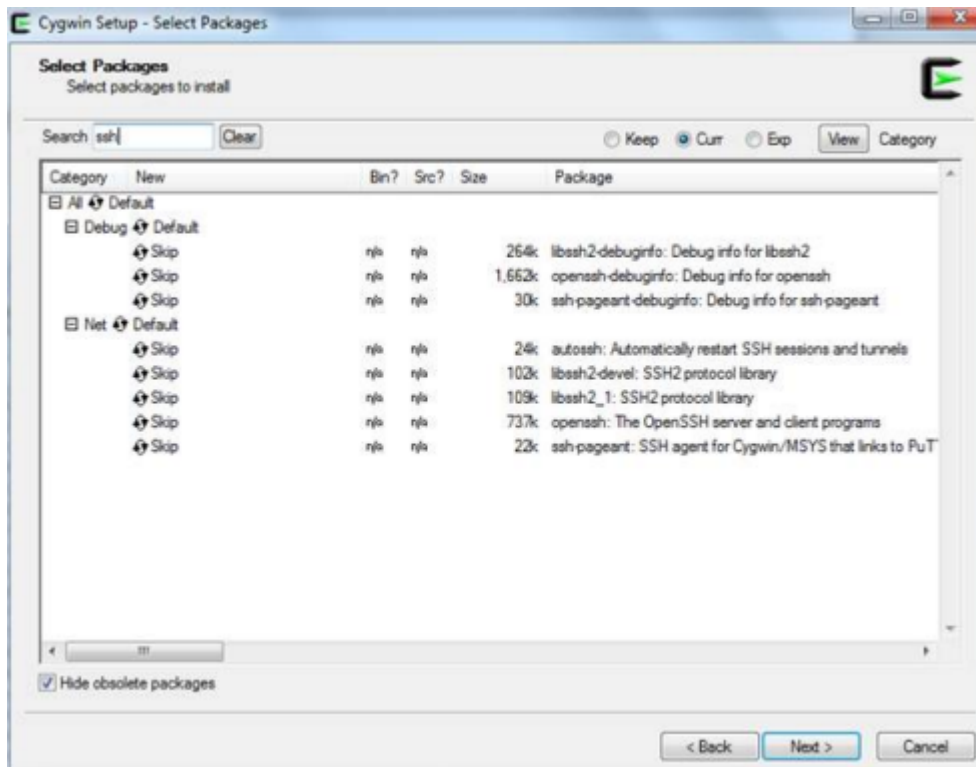
The `cygrunsrv` package will be in "Skip" mode.

- Click on **Skip** in the `cygrunsrv` row to install it.

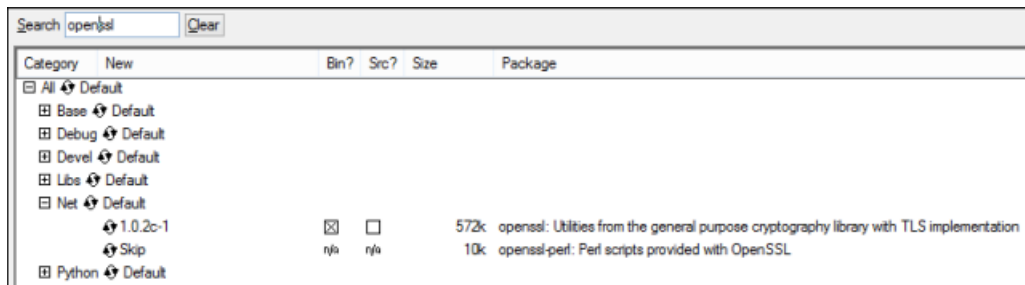
The screen should resemble following:

Category	New	Bin?	Src?	Size	Package
[-] All	Default				
[-] Admin	Default				
[-] Admin	Skip	n/a	n/a	49k	attr: Utilities for managing filesystem extended attributes
[-] Admin	Skip	n/a	n/a	53k	cron: Vixie's cron.
[-] Admin	1.62-1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	62k	cygrunsrv: NT/W2K service initiator
[-] Admin	Skip	n/a	n/a	7k	libattr1: Shared lib for managing filesystem extended attributes
[-] Admin	Skip	n/a	n/a	20k	shutdown: Shutdown, reboot, hibernate or suspend the machine
[-] Admin	Skip	n/a	n/a	267k	stow: Manage local software installations
[-] Admin	Skip	n/a	n/a	338k	syslog-ng: Next generation system logging daemon

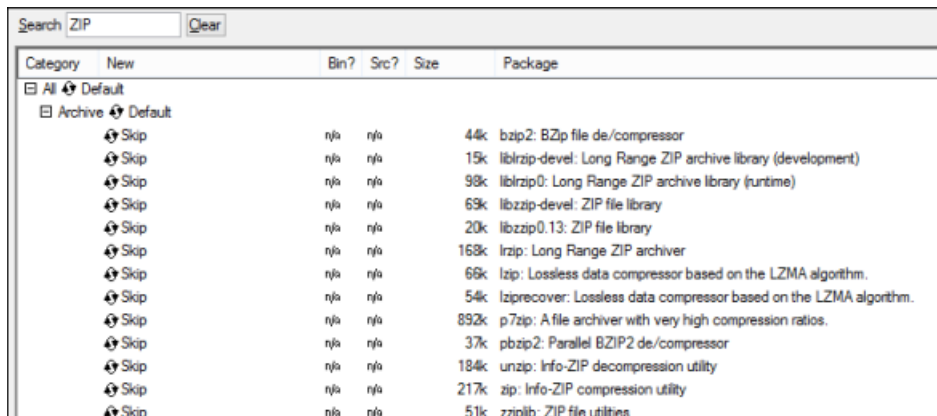
7. Enter `ssh` in the Search window. Under **Category**, expand the **Debug** and the **Net** options. By default, `openssh`, may be in "Skip" mode. Click on the `openssh` row under each to install it.



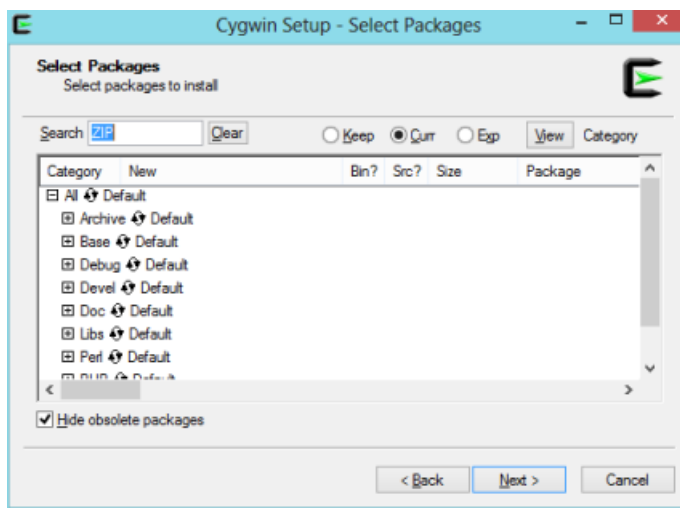
8. Enter `openssl` in the Search window. Under **Category**, expand the **Net** option. By default, "openssh" might be in Skip mode. Click on the `openssh` row under each to install it.



9. Enter `ZIP` in the Search window. Under **Category**, expand the **Archive** option. By default, the **Unzip** and **Zip** may be in Skip mode. Click on the appropriate rows to install them.



10. After the required packages are selected, click **Next**.



11. Select the **Select required packages (RECOMMENDED)** check box and **Next**.

12. After the download completes, click **Finish**.

To install the package, see [Install Cygwin \(local directory\)](#) on page 44.

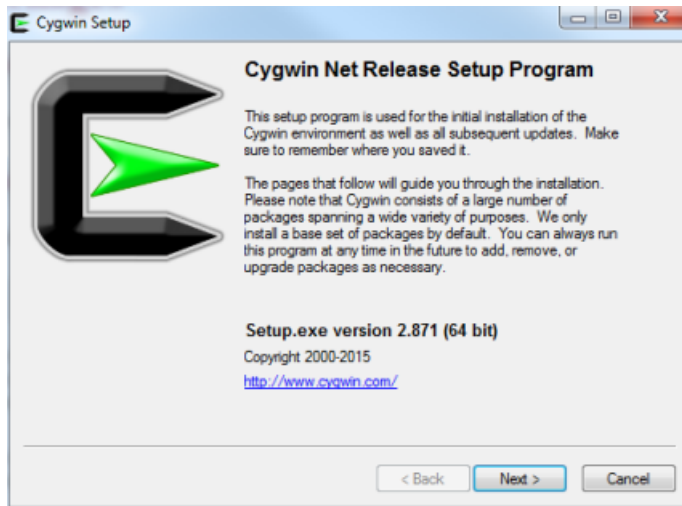
## Install Cygwin (local directory)

All Windows Server 2008 R2 or later servers managed by Solution Manager must have Cygwin version 1.7.35 or later installed.

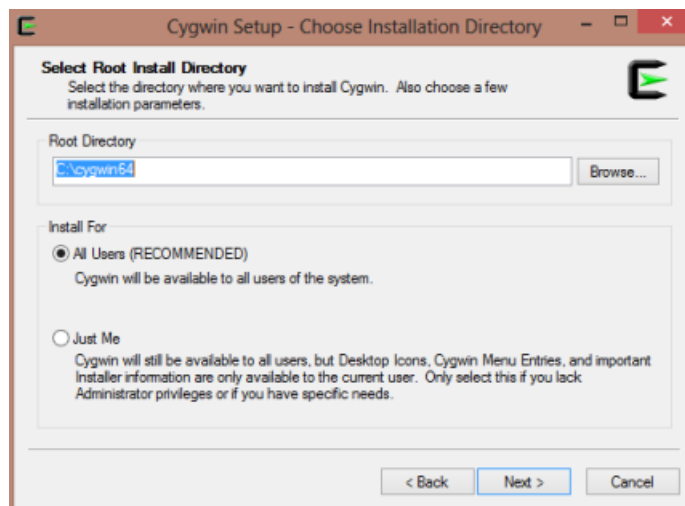
### Procedure

1. Copy the `setup.exe` and the downloaded package using [Install Cygwin \(download package\)](#) on page 39.

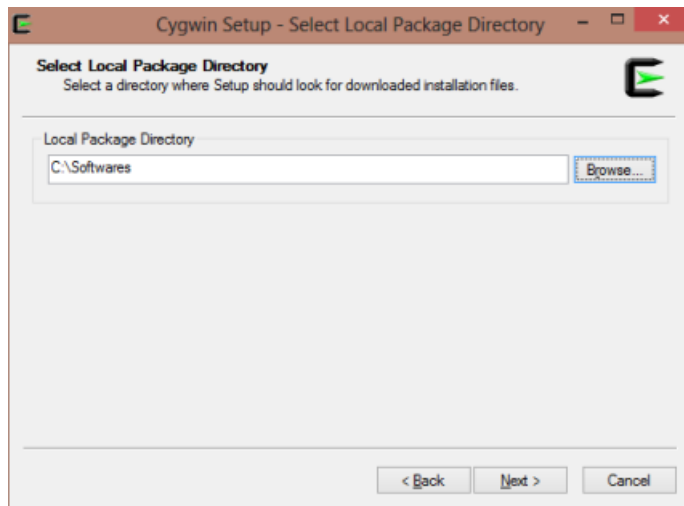
2. Run the `Setup.exe` file and click **Next**.



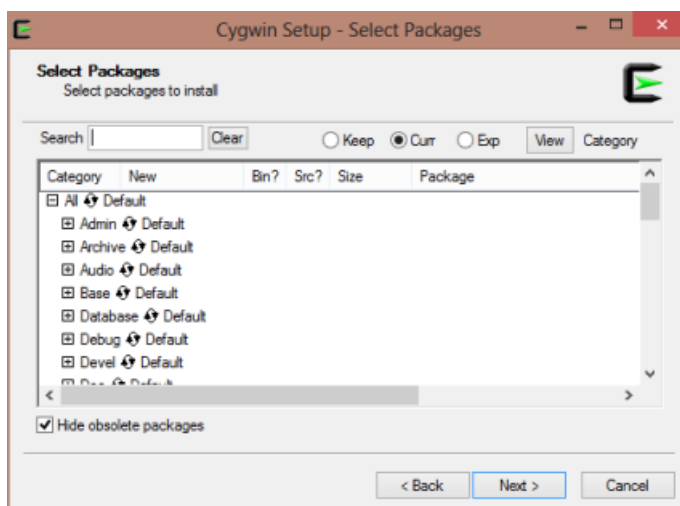
3.
  - a) Select the **Install from Local Directory** option and click **Next**.
  - b) Select the directory where the installation will be done and click **Next**.



- c) Select the local directory where the CYGWIN package is placed.



The installation will begin. Select which packages to install after the following screen appears:



- Under **Category**, expand the **Admin** option.  
The "cygrunsrv" package is about to be in Skip mode.

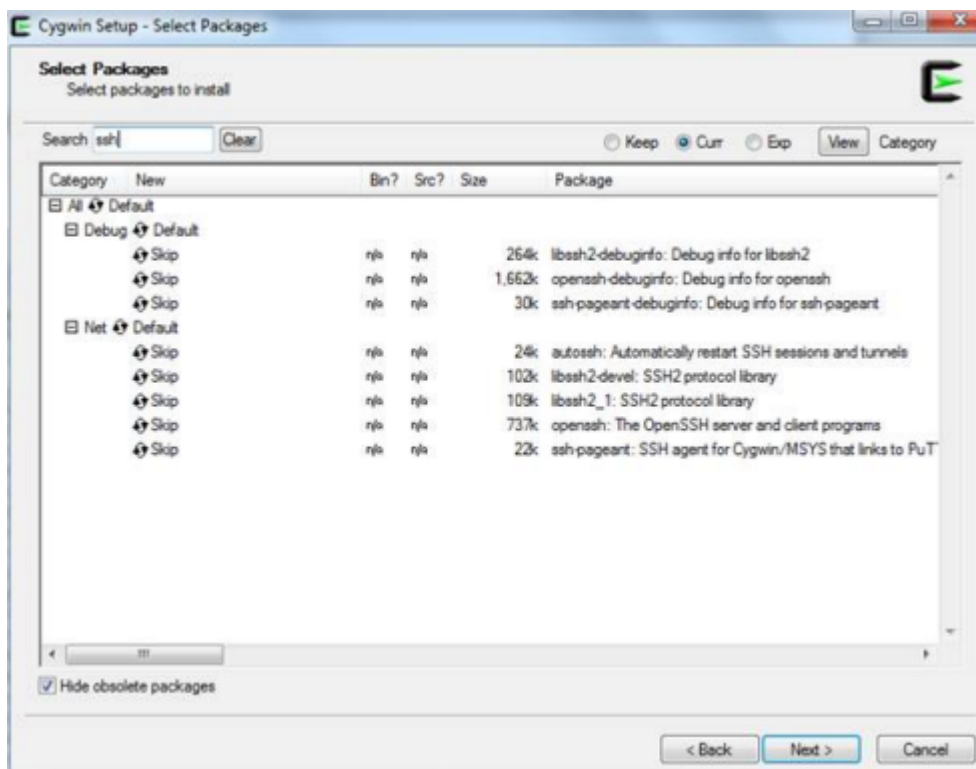
Category	New	Bin?	Src?	Size	Package
Admin	Skip	n/a	n/a	49k	attr: Utilities for managing filesystem extended attributes
	Skip	n/a	n/a	53k	cron: Vixie's cron.
	Skip	n/a	n/a	62k	cygrunsrv: NT/W2K service initiator
	Skip	n/a	n/a	7k	libattr1: Shared lib for managing filesystem extended attributes
	Skip	n/a	n/a	20k	shutdown: Shutdown, reboot, hibernate or suspend the machine
	Skip	n/a	n/a	267k	stow: Manage local software installations
	Skip	n/a	n/a	338k	syslog-ng: Next generation system logging daemon

- Click on **Skip** in the "cygrunsrv" row to install it.

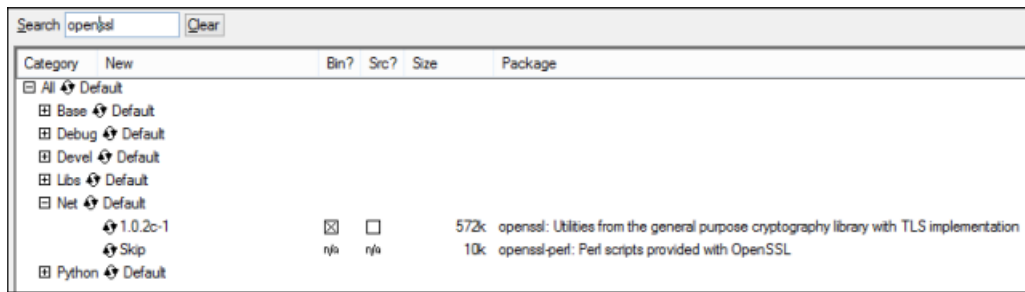
The screen should resemble the following:

Admin	Default						
	Skip	n/a	n/a	49k	attr: Utilities for managing filesystem extended attributes		
	Skip	n/a	n/a	53k	cron: Vixie's cron.		
	1.62-1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	62k	cygrunsrv: NT/W2K service initiator		
	Skip	n/a	n/a	7k	libattr1: Shared lib for managing filesystem extended attributes		
	Skip	n/a	n/a	20k	shutdown: Shutdown, reboot, hibernate or suspend the machine		
	Skip	n/a	n/a	267k	stow: Manage local software installations		
	Skip	n/a	n/a	338k	syslog-ng: Next generation system logging daemon		

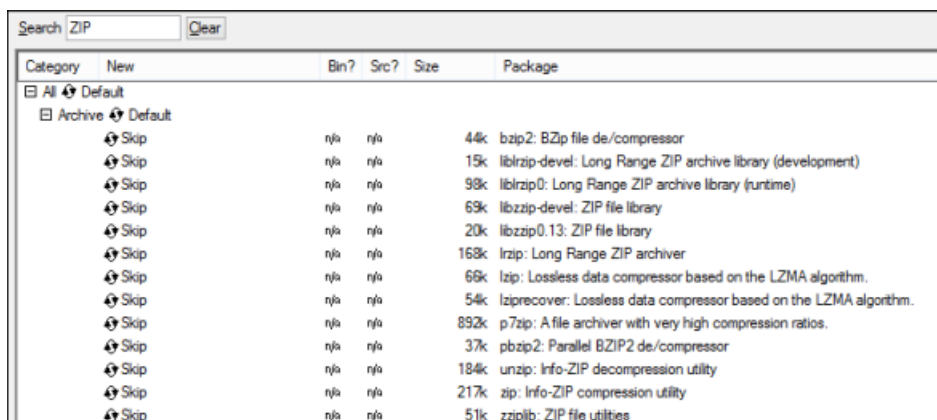
- Enter `ssh` in the Search window. Under **Category**, expand the **Debug** and the **Net** options. By default, "openssh" might be in Skip mode. Click on the "openssh" row under each to install it.



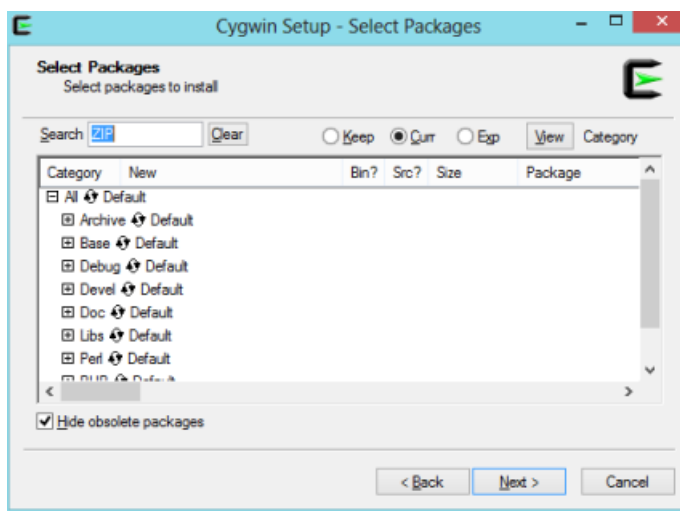
- Enter `openssh` in the Search window. Under **Category**, expand the **Net** option. By default, "openssh" might be in Skip mode. Click on the "openssh" row under each to install it.



- Enter ZIP in the Search window. Under **Category**, expand the **Archive** option. By default, "Unzip" and "Zip" might be in Skip mode. Click on the appropriate rows to install them.



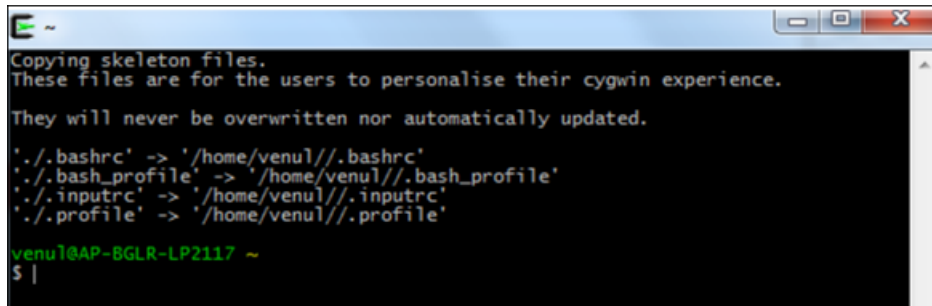
When the required packages are selected, click **Next**.



- Select the **Select required packages (RECOMMENDED)** check box and **Next**.



10. Select the **Create icon on Desktop** check box to create a shortcut for Cygwin terminal. After the download completes, click **Finish**.
11. Go to the desktop and double-click on the **Cygwin Terminal** icon. After this window appears, Cygwin installation will be complete.



```

E ~
Copying skeleton files.
These files are for the users to personalise their cygwin experience.

They will never be overwritten nor automatically updated.

'./.bashrc' -> '/home/venu1//.bashrc'
'./.bash_profile' -> '/home/venu1//.bash_profile'
'./.inputrc' -> '/home/venu1//.inputrc'
'./.profile' -> '/home/venu1//.profile'

venu1@AP-BGLR-LP2117 ~
$ |

```

Close the window.

12. Navigate to the Cygwin installation directory (for example, C:\cygwin64).
  - a) Open the `Cygwin.bat` file in edit mode using any editor.
  - b) Add the following line before invoking the bash shell: `set CYGWIN=ntsec`

```

C:
chdir C:\cygwin64\bin
set CYGWIN=ntsec
bash --login -i

```
13. To verify that Cygwin (`cygrunsrv`) is installed properly, run `C:\cygwin\Cygwin.bat`
14. Run the following command: `cygrunsrv -h`  
If Cygwin is installed properly, then all of the Cygwin help options will display on the screen.

## Configure Solution Manager Settings

Ensure that Solution Manager is equipped to handle a connection using SSH keys.

### Procedure

1. Log in as `User A` to `Server A`.
2. Navigate to the `<HOME_DIRECTORY_OF_USER_A>`.  
If the `.ssh_esm` folder does not exist in `<HOME_DIRECTORY_OF_USER_A>`, create one now.
3. Create a file titled `<USER_B>_<SERVER_B>.nopassword`.  
If SSH key-based communication has been set up between `banner@192.111.222.333` and `oracle@192.111.222.444`, create a file titled `ssh oracle 192.111.222.444.nopassword` in the `/home/banner` folder on `192.111.222.333`.

If SSH key-based communication has been set up between `oracle@192.111.222.333` and `oracle@192.111.222.333`, create a file titled `ssh oracle 192.111.222.333.nopassword` in the `/home/oracle` folder on `192.111.222.333`.

**Note:** Replace all server names, user names and user home locations with the corresponding values for the environment.

---

## Configure Solution Manager for Banner environment provisioning

Configure the admin server and Ellucian Solution Manager to provision new Banner environments.

You can configure the Admin Server and Ellucian Solution Manager for provisioning new Banner environments. This includes setting up the admin server and downloading files from the Ellucian Solution Manager Release Services that contain the provisioning template and associated content files.

**Note:** You only need to perform the instructions in this section if you want to provision new Banner environments using the environment provisioning templates available for Solution Manager. It is not necessary to perform any of the steps in this section to use Solution Manager to download, install, and deploy upgrades and patches into your existing Banner environments.

### Install required OS infrastructure packages

Before provisioning new Banner environments, first install the required infrastructure packages into the operating system.

#### Procedure

1. [ROOT] Log on to your admin server as root.

To install the required infrastructure packages, use the yum directory. It might be necessary to add a line similar to the following to the configuration file `/etc/yum.conf` (this will allow yum to acquire packages from the Internet):

```
Proxy = http://www-proxy.<your-institution-domain>:8080
```

2. Run the following scripts to install the required infrastructure packages:

```
# yum install createrepo
# yum install httpd
# yum install xinetd.x86_64
# yum install tftp-server
# yum install dhcp.x86_64
# yum install expect
```

## Download provisioning template

To download the template, access the Ellucian Solution Manager application from a web browser.

### Procedure

1. Sign in and click on the **Environments** tab.
2. Click **Get New Releases** at the bottom right of the **Environments** page:

After you click on the button, Ellucian Solution Manager displays the **Download Monitor** page, which displays download progress.

- You can set the automatic refresh rate on the page by typing the number of seconds between each desired refresh in the **Auto Refresh (secs)** field and then clicking **Refresh**.
- You can also manually refresh the display at any time by clicking **Refresh**. You can scroll through the rest of the display to see what is happening during the download.

The **Get New Releases** function contacts the Ellucian Solution Manager Release Services, then downloads available templates and upgrade releases for licensed Banner products. Also included are releases that have been updated since they were last downloaded.

## Acquire provisioning content

Acquire the content associated with downloaded provisioning templates.

### About this task

Access the Ellucian Solution Manager application from the web browser.

### Procedure

1. Log in and select **Templates** from the menu on the left. Ellucian Solution Manager displays a list of templates that you have downloaded.

If the **Templates** table does not display any rows, click on **Refresh Templates**.

2. Navigate to the **Template Contents** page to acquire the content files associated with the provisioning template. To do so, click anywhere except in the View column on the row for the template in the **Templates** table.

Ellucian Solution Manager displays the **Template Contents** page.

If you scroll through the page, you will see a number of content items. For each item, the Status column should be blank and the check box should be cleared in the Get From Ellucian column. To download the content files associated with the template, select the check box for each item in the Get From Ellucian column and then click on the **Get From Ellucian** button at the bottom of the page.

When you click the **Get From Ellucian** button, Ellucian Solution Manager will contact the Ellucian Solution Manager Release Services and begin downloading the content files for the

content items that are selected in the Get From Ellucian column. Either download all of the items at one time by selecting all of the check boxes in the Get From Ellucian column before clicking on the **Get From Ellucian** button, or select one or more specific items to download separately.

The Size column gives an approximate size in megabytes for each file. Ellucian Solution Manager is capable of downloading all of the files at once, but due to the size of some files and varying transfer rates, download times may be considerable. If files are downloaded in batches, you monitoring may be made easier. (If a download fails, simply select the item and download it again).

After clicking on the **Get From Ellucian** button, a `Download in Progress` message is displayed at the top of the page. When the download is complete, the downloaded item will display a status of either `Ready` or `Post Acquire Instructions`.

3. Complete the content acquisition for each item with the status of `Post Acquire Instructions` by clicking on the icon in the last column of that row.

This will display the associated post-acquisition completion instructions page.

Follow the instructions on the page and click **Mark Completed**. Ellucian Solution Manager will display the **Template Contents** page, where the status of the content item should be `Ready`.

**Warning!** After all the content has been acquired and the post-acquire instructions are marked complete for any content containing such post acquire instructions, a **Mark Active** button will appear at the bottom of the template's content page.

4. Click on the **Mark Active** button to set the template status to `Active` so that it can be used during provisioning.

## Configure permissions for SELinux

If the admin server has SELinux capabilities turned on you might encounter permission issues with HTTP and other required services (for example, TFTP) serving files.

### Procedure

1. [ROOT] Log on to the admin server as `root`.
2. Enter the `sestatus` command to see if SELinux capabilities are available.
  - If the response is `command not found`, then SELinux is not installed.
  - If the response indicates that SELinux status is disabled, then SELinux controls are turned off.
    - a) If the `sestatus` command indicates that SELinux status is enabled, turn SELinux controls on or off using the `setenforce` command:

```
setenforce permissive to turn controls off
setenforce enforcing to leave controls on
```
3. To leave SELinux enabled, you will need to alter some permissions to allow the Apache HTTP daemon to serve files from your repository folder during environment provisioning.

```
# chcon -t httpd_sys_content_t /u02
```

## Set up directories for provisioning environments

Set up the directories that will be used to kick start provisioned servers, for HTTP, and for the BannerUpgradeRepository. This is used for storing Banner upgrades so that Solution Manager can be used to view and install Banner upgrade releases.

### Before you begin

This task includes exporting several required shares using NFS. Before completing this procedure, first acquire the content as described in the [Acquire Provisioning Content](#) section.

### Procedure

1. [ROOT] Log on to the admin server as root and run the following command to set up the directories for provisioning environments:

```
# sh /u02/esmdeploy/prep_services_for_provision.sh
# chown -R esmadmin:esmadmin /u01
```

2. The NFS exports that are set up by this script are available as read-only to any host. To view the exports, enter the following command:

```
# cat /etc/exports
```

In response to the command, a system message similar to the one listed below will appear:

```
/u01/ks/ksCmds *(ro)
/u02/installs *(ro)
```

You can edit the `prep_services_for_provision.sh` script before you run it to comment out the lines that set up the `BannerUpgradeRepository` exports.

**Tip:** If any of the lines are duplicated, edit the file and remove the duplicate lines.

3. Restrict access to these shares by modifying the export parameters.  
Shares must be available to the VMs in any environment provisioned with Ellucian Solution.

## Restart the inet daemon and configure DHCP

Restart the inet daemon to implement network changes.

### Procedure

1. [ROOT] Log on to the admin server as `root` and run the following command to restart the inet daemon:

```
# service xinetd restart
```

The environment provisioning process uses the admin server as a DHCP server on the private network connecting the admin server to the environment VMs.

2. [ROOT] Log on to the admin server as root and run the following commands to properly configure your admin server as a DHCP server for environment provisioning.
3. Enable the Ellucian Solution Manager application to modify the `dhcpd.conf` file by executing the following commands:

```
# chgrp esmadmin /etc/dhcp
# chgrp esmadmin /etc/dhcp/dhcpd.conf
# chmod g+w /etc/dhcp
# chmod g+w /etc/dhcp/dhcpd.conf
```

4. Enable the Ellucian Solution Manager application to restart DHCP by adding the following lines to the bottom of the `/etc/sudoers` file. Use the `visudo` command to add the following lines to the file:

```
Defaults!/sbin/service !requiretty
esmadmin ALL = NOPASSWD: /sbin/service dhcpd restart
```

5. Ensure that the DHCP server will broadcast on the correct Ethernet interface for the system. Edit the `/etc/sysconfig/dhcpd` file to set the correct Ethernet interface for your Ellucian Solution Manager admin network.

The result should look similar to the following:

```
DHCPDARGS="eth1";
```

Use the `ifconfig` command to determine which network interface is connected to the private admin network between the admin server and the environment to be provisioned.

## Verify TFTP service

During provisioning the servers in the environment must use TFTP to access kick start files from the admin server. Verify that the TFTP service is running on the admin server.

### Procedure

1. [ROOT] Log on to the admin server as root and run the following commands:

Note that `192.168.x.x` is replaced by the IP address of the admin server on the private administration network that connects the admin server to VMs in the environment to be provisioned.

```
# cd /tmp
# tftp 192.168.x.x
# tftp> get pxelinux.0
# tftp> quit
# ls -l pxelinux.0
```

`tftp>` in the command list above represents the prompt that follows executing the `tftp 192.168.x.x` command.

If the `tftp>` prompt does not appear after the `tftp 192.168.x.x` command is executed, then TFTP services are not running. Proceed to the next step to start up the TFTP service.

If the commands are successful, there will be a response to the last command similar to the following:

```
-rw-r--r-- 1 root root 16662 Jun 2 22:24 pxelinux.0
```

If the commands in this section are successful, the TFTP service is running. No further action is required.

If the commands in this step (to verify that the TFTP service is functioning correctly) are not successful, then continue with the procedure to get the service running.

2. [ROOT] Log on to the admin server as `root` to run the commands in this step. Ensure that TFTP is installed. If a `command not found` error message appears after running the `tftp` command listed in the previous step, TFTP is likely not installed. To install TFTP, enter the following command:

```
# yum install tftp
```

If a `command not found` error message does not appear after entering the `tftp` command, but were not successful in retrieving the `pxelinux.0` file. Ensure that TFTP is enabled.

3. [ROOT] Log on to the admin server as `root` to run the commands in this step. To verify that TFTP is enabled enter the following command:

```
# cat /etc/xinetd.d/tftp
```

In response to this command, an input similar to the following should appear:

```
# default: off
# description: The tftp server serves files using the trivial file
  transfer \
#       protocol.   The tftp protocol is often used to boot diskless
  \
#       workstations, download configuration files to network-aware
  printers, \
#       and to start the installation process for some operating
  systems.
Service tftp
{
    socket_type           = dgram
    protocol              = udp
    wait                  = yes
    user                   = root
    server                 = /usr/sbin/in.tftpd
    server_args            = -s /u01/tftp
    disable                = no
    per_source             = 11
    cps                    = 100 2
    flags                  = Ipv4
}
```

4. Verify that the `disable` parameter is set to `no`. If not, edit the `/etc/xinetd.d/tftp` file and change that parameter to `no`.



- Verify that the contents of `/u01/tftp` are correct and are readable by entering the following command:

```
# ls -al /u01/tftp
```

In response to that command, a list of the contents of the `/u01/tftp` directory will appear:

```
total 47844
drwxr-xr-x  3 esmadmin esmadmin    4096 Sep 10  2012 .
drwxr-xr-x.  9 esmadmin esmadmin    4096 May 23 16:42 .
-rw-r--r--  1 esmadmin esmadmin 12366480 Sep 10  2012
  initrd_oel5.img
-rw-r--r--  1 esmadmin esmadmin    16662 Aug 24  2012 pxelinux.0
drwxr-xr-x  2 esmadmin esmadmin    4096 May 10 19:31 pxelinux.cfg
-rwxr-xr-x  1 esmadmin esmadmin   21.6644 Sep 10  2012 vmlinuz_oel5
```

The files should be owned by `esmadmin` and read permission should be set for owner, group, and world for the directory and all the files in the directory.

- If read permissions are not set, enter the following command to grant read permissions on the files:

```
# chmod -R +r /u01/tftp
```

- If the file ownership is not correct, enter the following command to reset file ownership:

```
# chown -R esmadmin:esmadmin /u01/tftp
```

- Check to ensure that there are no IP restrictions that can prevent the environment VMs from connecting to the admin server and accessing the TFTP files. Check for IP restrictions by entering the following command:

```
# iptables -L
```

If the response is a command not found message or output similar to the following, then no IP restrictions exist:

```
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

If the output from the `iptables` command differs from that shown above, enlist someone with experience setting up IP restrictions in a Linux environment review the rules and modify them so that they do not restrict the environment VMs from connecting to the admin server.

- Restart the TFTP service to ensure that all the changes are recognized by entering the following command:

```
# service xinetd restart
```

The restart command should generate the following message:

```
Stopping xinetd:          [ OK ]
Starting xinetd:         [ OK ]
```

## Appendix: Solution Manager worksheets

Developer worksheets can be filled out either electronically or manually.

### Developer worksheets

The Solution Manager developer worksheets should be completed in conjunction with the procedures included in the *Ellucian Solution Manager User Guide*. Consult the user guide for information on provisioning new environments, managing existing ones, and performing updates within Solution Manager.

### Tomcat application server

Enter the appropriate information when configuring the Tomcat server.

Name	Value	Default	Banner Source	Responsibility	Record Your Value
App Server	Enter a name for this Tomcat App Server.		The name specified for the Tomcat app server has no impact.		
Type	Tomcat				
Admin Port Number	Note that this field is not used for Tomcat app servers.				n/a
Application Port Number	Enter the port number that will be used when	8080	This field can be left blank if the		

Name	Value	Default	Banner Source	Responsibility	Record Your Value
	deploying applications to this app server.		client is using the default of 8080.		
Use SSL	Indicate whether this is an SSL port.				
Admin User/pw	Note that this field is not used for Tomcat app servers.		n/a		
Catalina WebApps Path	Enter full Tomcat webapps directory path.		Specifically the path to the webapps directory located under \$CATALINA_HOME		

## WebLogic application server

Enter the appropriate information when configuring the WebLogic server.

Name	Value	Default	Banner Source	Responsibility	Record Your Value
App Server	Enter your choice of name for this WebLogic App Server	None specified	Currently this App Server name must match the WebLogic managed server name.		
Type	WebLogic		This name will need to match exactly.		

Name	Value	Default	Banner Source	Responsibility	Record Your Value
Admin Port Number	This field is not used for Tomcat app servers		This is the port number used to access the WebLogic Admin console. It is not the WebLogic app server port.		
Application Port Number	This field is not used for Tomcat app servers.		This is the port number that you defined when you created the server in the WebLogic admin console.		
Use SSL	Indicate whether this is an SSL port.	admin/password1			
Admin User/pw	Not used for Tomcat app servers.				
Catalina WebApps Path	Enter the full Tomcat webapps directory path.	e.g., /setDomainEnv.sh	This is simply the machine name.		

## Banner credentials database

Set up credentials for the Banner database.

Name	Value	Default	Banner Source	Responsibility	Record Value
System and SYS passwords	Enter the chosen password.	manager	The database administrator should provide this information.	Database administrator	

## Banner credentials installer

Install credentials for the Banner database.

Name	Value	Default	Banner Source	Responsibility	Record Value
Upgrade Owner User Password		upgrade1/u_pick_it	This is the Oracle user that is set up to own the modification tables. No need to change if the default is used.		
Install User Password		banner or Administrator (for Windows)/u_pick_it	This is the login that the upgrade installation process should use to log into the application containing the Banner code tree to install the		

Name	Value	Default	Banner Source	Responsibility	Record Value
			upgrades. No need to change if the default selection is used.		
Install User Login Sequence	Enter the commands to execute after the login of the install user on to the server containing the Banner code free.		This field allows users to customize the login. The <i>User Guide</i> describes the syntax and variables that can be used here.		
Banner Schema Passwords	Enter the passwords for each user schema for the Banner DB.				

## Admin server private network environment settings

Configure environment settings for the admin server private network.

Name	Value	Default	Responsibility	Record Your Value
Subnet	Subnet where the Solution Manager resides.		Network Administrator	
Network IP	Network IP address of the Solution Manager server.		Network Administrator	
Gateway IP	Gateway IP address of the Solution Manager server.		Network Administrator	

## Admin server public network environment settings

Configure environment settings for the admin server public network.

Name	Value	Default	Responsibility	Record Your Value
Domain	The domain and suffix where Solution Manager and the managed Banner environments reside.  Example: ellucian.com		Network Administrator	
Subnet	Subnet of the net where the Solution Manager DB is located.		Network Administrator	
Gateway IP	Gateway IP address of network where the Solution Manager server is located.		Network Administrator	

## Environment configuration settings

Enter the appropriate environment settings for Banner DB configuration.

Name	Value	Default	Responsibility	Record Your Value
Identity Services URL	For Banner Pages deployments: Enter the URL of the user		Network Administrator	

Name	Value	Default	Responsibility	Record Your Value
	<p>authentication service used with the Banner pages deployment, such as Ellucian Identity Services (EIS) or Central Authentication Service (CAS).</p> <p>For additional information, see the Installation Guide for a Banner Pages release, such as the Human Resources 9.0 release.</p> <p>For example: <code>https://m03420.ellucian.com:8443/cas</code></p>			
Application Navigator URL	<p>For Banner Pages deployments: Enter the base URL for accessing the Application Navigator instance that is used to access the Banner pages deployment.</p> <p>For additional information, see the Installation Guide for a Banner Pages release, such as the Human Resources 9.0 release.</p>		Network Administrator	



Name	Value	Default	Responsibility	Record Your Value
	For example: https:// m034197.ellucian.com:8888			

## Environment settings worksheets

Enter the appropriate information when configuring the environment settings.

Name	Value	Default	LINUX Source	Responsibility	Record Your Value
DB SID	Enter the Oracle database SID for the Banner environment	SEED	Prerequisites: <ul style="list-style-type: none"> <li>Name/connection info for the server hosting your database</li> <li>Basic LINUX commands</li> <li>Location of your \$ORACLE_HOME</li> </ul> <ol style="list-style-type: none"> <li>Log into the database server.</li> <li>Navigate to the etc directory and open the oratab file.</li> </ol> <p><b>Note:</b></p>	DBA	

Name	Value	Default	LINUX Source	Responsibility	Record Your Value
			<p>Only one of multiple entries will be marked with a Y against a given \$ORACLE_HOME. If multiple \$ORACLE_HOME entries exist, verify with the DBA which one points to the BANNER instance. The DBSID is also included in this file.</p>		
Database Port	Enter the Oracle Communications Port for the Database.	1521	<p>This information is located in the <code>tnsname.ora</code> file.</p> <p>The <code>tnsnames.ora</code> file is located in the <code>ORACLE_HOME</code> directory (see DBSID on how to get this information) in the network directory.</p> <p><b>Note:</b> Multiple <code>tnsnames.ora</code> files may exist.</p>	Banner Administrator/ Network Admin/DBA	

Name	Value	Default	LINUX Source	Responsibility	Record Your Value
			<p>If uncertain of the correct file, navigate to the \$ORACLE_HOME directory and open the listener.log file. This will show which port the database is listening on.</p>		
Upgrade Agent Name	Enter the name of the Jenkins agent created for the upgrades.	<env_name>_BMUI_AGENT	<p>Used for upgrades only.</p> <p>It will be necessary to create and start this Jenkins agent on the Jobsub machine before specifying its name here.</p> <p>See the appropriate section of the <i>User Guide</i> for instructions on creating this agent.</p>		
Banner XE Shared Config Dir	No need to change this from the default unless otherwise specified.	shared_configuration	<p>This value should be the text: shared_configuration</p> <p>No need to change the default, unless otherwise specified.</p>		

Name	Value	Default	LINUX Source	Responsibility	Record Your Value
Banner Wait For (secs)	3600	3600			
Banner Wait for Forms (secs)	3600	3600			
Banner Wait for Forms	7200	7200			
Wait for Display	Cleared	Cleared			

## INB application worksheets

Use the following information when adding the INB application to the Banner environment.

Name	Value	Default	Banner Source	Responsibility	Record Value
Solution Manager Local Deployment Root	Optional configuration item that allows an administrator to specify a local path for Solution Manager to copy large files.				
Banner Staging Paths (Help only)	Enter the full paths to each of the staging areas on the server associated with a Banner Application.  There are separate paths for Banner 8 online help, Banner	Example: /u02/ banapp/staging/ ban8help			

Name	Value	Default	Banner Source	Responsibility	Record Value
	9 online help, and Banner 9 WAR deployments (General Event Management, Faculty Grade Entry, etc.).				
INB Host Forms Path	This is where the compiled version of the forms (*.fmx) are located along with the source files (*.fmb).		The path on the INB application to the directory where the forms executables (*.fmx" and associated file types) are stored.		
INB Host Reports Path	This is where the compiled version of the reports (*.rep) are located along with the source files ().		The path on the INB application to the directory where the reports executables (*.rep" and associated file types) are stored.		
INB Host User/PW	This is the user account that will log into the INB server and compile the forms and reports.  The forms and reports compiling process will run under this user account.	Oracle/u_pick_it	The user login that should be used by the automated upgrade installation process when logging on to the INB application to update the forms or reports executables.		

## INB compiler server properties

Enter the appropriate information when configuring the INB server.

Name	Value	Default	Banner Source	Responsibility	Record Your Value
Host SID Name	This is the local Oracle SID on the INB server and can be found in the oratab file.	as_1	<p>What you need to know beforehand:</p> <ul style="list-style-type: none"> <li>• Password for the Oracle user</li> <li>• Basic LINUX commands</li> </ul> <ol style="list-style-type: none"> <li>1. Login to the INB server using the Oracle user.</li> <li>2. Navigate to the etc directory and open the oratab file. There should only be one oracle home specified in this file.</li> </ol>		
Host TNSADMIN Path			The path to the Oracle admin directory in the Oracle instance on the INB forms compiler application that is		

Name	Value	Default	Banner Source	Responsibility	Record Your Value
Host FMB Path			set up for forms and reports compilation.		
Host RDF Path			The path on the INB forms compiler application to the directory where the ".fmb" files (and associated file types) are stored for forms compilation.		
Banner Links			The path on the Banner code tree server (usually the job sub or database application) for the environment to the "links" directory in the Banner code tree. (The automated upgrade installation process uses this directory to access the forms and reports source files to		

Name	Value	Default	Banner Source	Responsibility	Record Your Value
			transfer them to the INB forms compiler application to do the forms and reports compilations).		
Compile Host Oracle Home Path			The path to the Oracle home directory for the Oracle instance on the INB forms compiler application that is set up for forms and reports compilation.		
Compile Host User/PW			The user login that should be used by the automated upgrade installation process to log on to the INB forms compiler application to do forms and reports compilation.		
Compile Login Sequence		Wait \$ RC source /usr/local/bin/oraenv Wait ORACLE_SID = [oracle] ? RC DFLT	A series of instructions for the automated upgrade installation process of use when logging on to the INB forms compiler for forms and report compilation.		



Name	Value	Default	Banner Source	Responsibility	Record Your Value
		Wait \$ RC export ORACLE_INSTANCE= \$ORACLE_BASE_asinst_1	This login instruction sequence must be set up to recognize any prompts that occur during the login sequence and to provide appropriate responses to those prompts.		
		Wait \$ ADDPROP banner.form.compile.two	The login sequence must also set the Oracle environment for doing the forms and reports compilation.		

## Jobsub BXE application worksheets

Enter the appropriate information when adding the Jobsub BXE application to the Banner environment.

Name	Value	Default	Banner Source	Responsibility	Record Your Value
Solution Manager Local Deployment Root	Optional configuration item that allows an administrator to specify a local path for Solution Manager to copy large files.		Only applies to deployments on WebLogic hosted on Windows.		

Name	Value	Default	Banner Source	Responsibility	Record Your Value
Banner Staging Paths	Enter the full paths to each of the staging areas on the server associated with a Banner Application.  There are separate paths for Banner 8 online help, Banner 9 online help, and Banner 9 WAR deployments (General Event Management, Faculty Grade Entry, etc.).				

## SSB application properties

Enter the appropriate information when adding the SSB application to the Banner environment.

Name	Value	Default	Banner Source	Responsibility	Record Your Value
UserID/PW			Only applies to Deployments on WebLogic hosted on Windows.		
WebServer Doc Root Path			The path to the folder on the SSB application server where the upgrade		

Name	Value	Default	Banner Source	Responsibility	Record Your Value
			process will place images, CSS, and its files.		
Banner SSB Cascade EAR File Staging Path			The path to the folder on the SSB application server where EAR files needing SSB deployment will be placed by BMUI.		
Host SID Name					

## SSB application worksheets

Enter the appropriate information when adding the SSB application to the Banner environment.

Name	Value	Default	Banner Source	Responsibility	Record Your Value
Solution Manager Local Deployment Root	Optional configuration item that allows an administrator to specify a local path for Solution Manager to copy large files.		Only applies to Deployments on WebLogic hosted on Windows		
Banner Staging Paths (Help only)	Enter the full paths to each of the staging areas on the server associated with a Banner Application.		The staging areas are directories (manually created by the client) into which the upgrade process		

Name	Value	Default	Banner Source	Responsibility	Record Your Value
	There are separate paths for Banner8 online help and Banner 9 online help.  Example: /u02/ banapp/staging/ ban8help		will place new application files that need to be deployed. Typically this is for the Online Help, but these are also used for the Banner XE application deployments.		

## Machine DB Jobsub app server

Enter the following information when configuring the Jobsub server.

Name	Value	Default	Banner Source	Responsibility	Record Your Value
Role	This is one of three values: DB, App or Job Sub. These roles will be defined before the Solution Manager installation.			Network Administrator/CAS Administrator	
Network Type		Internal			
Machine Status	Will be ready for existing environments.	Ready			
Machine OS	Will be UNIX or Windows.				
Host Name	Will be previously defined for existing environments.				

Name	Value	Default	Banner Source	Responsibility	Record Your Value
IP	Will be previously defined for existing environments.				
Root Password	Will be previously defined for existing environments.				
Deployment Agent Name	Enter the name of the Jenkins agent created for deployments.	<env_name>_DEPLOYMENT_AGENT	Used for	Used for deployments only. It will be necessary to create and start this Jenkins agent on this machine before specifying its name here.  See the appropriate section of the <i>User Guide</i> for instructions on creating this agent.	
Bash Shell Path	Specify the path to bash on this machine.	/bin/sh		Specify the path to bash on this machine. Only needed if the default (/bin/sh) does NOT point to bash.	

---

Name	Value	Default	Banner Source	Responsibility	Record Your Value
Public Network (App Servers Only)					
Host and IP					