

Configuring a secured Precise system

This section includes the following topics:

- [About secured Precise systems](#)
- [Installing new servers](#)
- [Configuring a secured Precise system](#)
- [Verifying Precise login credentials using an external password repository](#)
- [Running Precise services on Windows with a non-Administrative user](#)
- [Configuring the Single Sign On feature for Precise](#)
- [Configuring LDAP to authenticate Precise users](#)

About secured Precise systems

Precise systems can provide a high level of protection against external and internal intruders, restricting access to the sensitive information that Precise uses and monitors.

This information includes the following:

- Passwords used by Precise to access the monitored instances
- Data sent between the various Precise agents on the different servers
- Data sent between the Web-based Precise user interface client and the various Precise agents

Installing new servers

When installing a new server, a communication security key is transferred to the new server. To ensure secure transfer of the key, see [Securing communication key transfer to a new server](#).

Configuring a secured Precise system

Configuring a secured Precise systems involves setting file permissions and enabling Precise security mechanisms, such as the Advanced Encryption Standard (AES) and password encryption.

The communication encryption mechanism and the password encryption mechanism support Advanced Encryption Standard (AES) which is used by default. For higher security, it is recommended to use the Precise Web-based user interface client using the Secure Socket Layer (SSL) protocol.

In general, it is recommended to update all the mechanism encryption keys (including SSL) every so often.

Setting file permissions

Verify that only the Precise users and group have access to files under the Precise root folder. You can change the entire files permissions to have 770 permissions.



Some monitored instances also require access to the file, so the Precise user should be part of these monitored instances user groups as well.

To set file permissions on Windows

- Verify that the Precise installation folder is not shared and grants access to required users only.

About configuring AES communication

By default, Precise communicates using a symmetric key encryption algorithm called Advanced Encryption Standard (AES).

Replacing the encryption key on the Precise FocalPoint server

To replace the communication AES key

1. Log in to the Main Precise FocalPoint.
2. Run the following command from the `<Precise_root>` folder:
 - **Windows**

```
infra\bin\psin_cli.bat
-i3-user<user_name>
{-i3-encrypted-password<encrypted_password>|-i3-clear-password<clear_password>}
-action communication-key-change
-type aes
```
 - **UNIX**

```
./infra/bin/psin_cli.sh
-i3-user<user_name>
{-i3-encrypted-password<encrypted_password>|-i3-clear-password<clear_password>}
```

```
-action communication-key-change
-type aes
```

Distributing the new encryption settings to all servers

For the new encryption settings to take effect, you must distribute them to all servers, completing no later than 24 hours after you changed the encryption configuration on the Precise FocalPoint server.

The new encryption settings will be effective within 48 hours. If a server does not receive the new settings within 48 hours, it is no longer able to communicate with the Precise system. In this case, you need to perform an additional step to reestablish the communication.

 At the exact moment of key replacement, communication errors may occur in some of the active communication connections. You may encounter these errors in the user interface or in the log files. If they do not persist, ignore them.

To distribute the new encryption settings to all servers

1. Run the following command from the `<Precise_root>` folder on the Main Precise FocalPoint server:

- **Windows**

```
infra\bin\psin_cli.bat
-i3-user<user_name>
{-i3-encrypted-password<encrypted_password>|-i3-clear-password<clear_password>}
-action communication-key-distribute
{-servers "<comma_separated_servers_list>" | -all-servers true}
[-manual true]
[-secure true -user-name<user_name>-password<password>]
[-user-name<user_name>]
[-password<password>]
```

- **UNIX**

```
./infra/bin/psin_cli.sh
-i3-user<user_name>
{-i3-encrypted-password<encrypted_password>|-i3-clear-password<clear_password>}
-action communication-key-distribute
{-servers "<comma_separated_servers_list>" | -all-servers true}
[-manual true]
[-secure true -user-name<user_name>-password<password>]
[-user-name<user_name>]
[-password<password>]
```

Specify one: `-servers` and a comma separated list of specific servers to distribute the key to, or `-all-servers true` to distribute the key to all installed servers.

To use the secured mode transfer of the key, you need to specify `-secure true`, and supply the user name and password to use in SSH to connect to the servers.

Alternatively, specify `-secure true` and `-manual true` to use the manual mode to send the secured mode transfer of key. Note that this manual mode requires you to run the script manually on the related servers.

If you selected automatic distribution to servers, only servers with SSH or SCP protocols are supported.

2. If a server does not receive the new settings within 48 hours, do the following:
 - a. Copy all files from the `<precise_root>/infra/listener/etc/crypt` folder on the Precise FocalPoint server to the server that did not receive the new settings.
 - b. Restart all agents on that server.

Verifying encryption configuration on a server (optional)

You can verify that the encryption configuration has been updated on all servers. This procedure scans all of your Precise servers and checks if the server were successfully updated with the new encryption.

If one of the server reports an error, you need to redistribute the encryption settings. If you still encounter an error after redistributing the settings, contact Precise Customer Support.

 Run the verify command at least 48 hours after creating the new AES key. This will ensure that the protocol is secured with the new key.

See [Distributing the new encryption settings to all servers](#).

If the new encryption settings were successfully received on all servers, the scan results in an output like the following:

```
Server (aix1) ok
Server (aix2) ok
Server (aix3) ok
server scan done
```

If errors occurred on at least one of the servers, the scan results in an output like the following:

```
Server (aix1) ok
error on server (aix 2), see log file for details.
Server (aix3) ok
servers scan done
```

The encryption log is written to the following trace file:

```
<Precise_root>/logs/infra.i3fp.crypt.log
```

To verify encryption configuration on all servers

1. Run the following command from the <Precise_root> folder on the Main Precise FocalPoint server:

- **Windows**

```
infra\bin\psin_cli.bat
-i3-user<user_name>
{-i3-encrypted-password<encrypted_password>|-i3-clear-password<clear_password>}
-action communication-key-verify
{-servers "<comma_separated_servers_list>" | -all-servers true}
```
- **UNIX**

```
./infra/bin/psin_cli.sh
-i3-user<user_name>
{-i3-encrypted-password<encrypted_password>|-i3-clear-password<clear_password>}
-action communication-key-verify
{-servers "<comma_separated_servers_list>" | -all-servers true}
```

Specify one: `-servers` and a comma separated list of specific servers to distribute the key to, or `-all-servers true` to distribute the key to all installed servers.

About encrypting passwords

Precise uses an Advanced Encryption Standard (AES) to encrypt the passwords that its different components require to access the monitored instances (such as passwords for databases or Java application servers). These passwords are then saved in internal configuration files.

By default the password encryption is AES.

Replacing the password encryption key on the Precise FocalPoint server

You can replace the password encryption key on the Precise FocalPoint server by using the Precise Command Line Interface (CLI) installation utility. For information on how to deploy this utility, see the [Precise CLI Utility Reference Guide](#).

To replace the password encryption key on the Precise FocalPoint server

1. Verify that the CLI installation utility is deployed.
2. Run the following command from the <Precise_root> folder on the Precise FocalPoint server:

- **Windows**

```
infra\bin\psin_cli.bat
-i3-user<user_name>
{-i3-password encrypted-password
 | -i3-clear-password clear-password}
-action encrypt-update
-type [aes-key]
```
- **UNIX**

```
./infra/bin/psin_cli.sh
-i3-user user-name
{-i3-password encrypted-password
 | -i3-clear-password clear-password}
-action encrypt-update
-type [aes-key]
```

Table 1 Configuring password encryption type elements on the Precise FocalPoint server

Element	Description
-i3-user	See Authenticate to CLI Utility .
-i3-encrypted-password	See Authenticate to CLI Utility .
-action	Always: encrypt-update Mandatory: Yes
-type	Always: aes-key Mandatory: Yes AES-based encryption that uses a random symmetric key. It is recommended to update this key once a year. Security level: high

For example:

```
./infra/bin/psin_cli.sh
-i3-user user-name
{-i3-password encrypted-password
| -i3-clear-password clear-password}
-action encrypt-update
-type aes-key
```

Distributing the new password encryption settings to all servers

For the new password encryption settings to take effect, you must distribute them to all servers by using the Precise CLI installation utility. This procedure depends on the Precise Listener being up and running on all servers; otherwise, the agents on the servers will not be able to function.

To distribute the new encryption settings to all servers

1. In AdminPoint, verify that the Precise Listener is up and running on all servers.
2. Run the following command from the <Precise_root> folder on the Precise FocalPoint server:

- **Windows**

```
infra\bin\psin_cli.bat
-i3-user user-name
{-i3-password encrypted-password
| -i3-clear-password clear-password}
-action encrypt-distribute
```
- **UNIX**

```
./infra/bin/psin_cli.sh
-i3-user user-name
{-i3-password encrypted-password
| -i3-clear-password clear-password}
-action encrypt-distribute
```

Table 2 Distributing new password encryption element settings to all servers

Element	Description
-i3-user	See Authenticate to CLI Utility .
-i3-encrypted-password	See Authenticate to CLI Utility .
-action	Always: encrypt-distribute Mandatory: Yes

Configuring the Precise Apache Tomcat to work in HTTPS mode (SSL)

The Precise user interface is based on an Apache Tomcat server. You can configure it to work in HTTPS mode. This mode uses the Secure Socket Layer (SSL) protocol to encrypt the data that is sent from the Web browser to the Tomcat server.

To configure Precise Apache Tomcat to work in HTTPS mode

1. Create a certificate keystore on the Apache Tomcat server. This file is saved in the folder <Precise_root>\products\gui\website as a certificate .keystore file.
 - a. Before you create the .keystore file, delete the alias Tomcat if it already exists. To delete the alias Tomcat, run the following command from the <Precise_root> folder on the Precise FocalPoint:

- **Windows**

```
java\JRE\bin\keytool -delete -alias tomcat -keystore products\gui\website\keystore
```

 For the password, use "changeit." For the question "What is your first and last name," provide the server name used in the URL for the Precise GUI as the answer.

- **UNIX**

```
java/JRE/bin/keytool -delete -alias tomcat -keystore products/gui/website/.keystore
```
- b. To create your own certificate, run the following command from the <Precise_root> folder on the Precise FocalPoint:
 - **Windows**

```
java\JRE\bin\keytool -genkey -alias tomcat -keyalg RSA -keystore products\gui\website\keystore -validity 3000
```
 - **UNIX**

```
java/JRE/bin/keytool -genkey -alias tomcat -keyalg RSA -keystore products/gui/website/.keystore -validity 3000
```

 For the password, use "changeit." Also, use the host as displayed in the url for the name.

2. In the file <Precise_root>\products\gui\website\conf\server.xml

- a. Add comment tags around the non-SSL <Connector> tag, where the preliminary remark is "<!-- Define a non-SSL HTTP/1.1 ...-->."
 - b. Remove the comment tags around the SSL <Connector> tag, where the preliminary remark is "<!-- Define a SSL Coyote HTTP /1.1 ...-->."
3. Restart the Precise FocalPoint process on the UNIX server. Restart the Precise FocalPoint service and the Precise user interface service on the Windows server.
 4. Open the Precise application using HTTPS.
For example:
https://<host>:<port>

 After restarting the Precise FocalPoint, the SSL port changes to the default port added by the user during installation. If you want to use a different port, you can change the port as described in the Change GUI server port section in the [Precise CLI Utility](#).

When first launching Precise in a client, a security alert is displayed with the certificate details. You should sign your certificate with a trusted root authority (such as VeriSign). Alternatively you can install the certificate on each client server that uses the Precise GUI.

5. In AdminPoint, click the Setup tab and click on **Nodes** in the drop-down menu
6. In the Nodes tab, click **Edit** to update the URL of the node for which you configured the SSL, according to step 4. In addition, if you are working with the Precise Custom Portal, the following configuration must be performed.

To configure Precise Apache Tomcat to work in HTTPS mode with the Precise Custom Portal

1. Export the certificate:
<i3>java\jre\bin\keytool -export -alias tomcat -file <file_name>.crt
-keystore <i3>products\gui\website\keystore
2. Import the certificate:
<i3>java\jre\bin\keytool -import -file <file_name>.crt -alias tomcat
-storepass <changeit> -keystore <i3>\java\JRE\lib\security\cacerts

 Verify that the same <file_name>.crt is used for exporting and importing the certificate.

 For the password, use "changeit."

To install a certificate

1. When you get the certificate warning, click **View certificate**.
2. Click **Install certificate**.
3. Click **Next**.
4. Select **Place all certificates in the following store**.
5. Click **Browse**.
6. Check **Show physical store**.
7. Select **Local Computer** under Trusted root certification Authorities.
8. Click **OK, Next**, and then **Finish**.
9. Close and restart the Precise GUI, and verify that the warning for the certificate does not re-appear.

For general information regarding configuring HTTPS mode, see Apache Tomcat server instructions found at this site: <http://tomcat.apache.org/tomcat-4.1-doc/ssl-howto.html>

For information regarding configuring J2EE to work in HTTPS mode, see the [Precise for J2EE User Guide](#).

Changing the session timeout for an Apache Tomcat server

For an Apache Tomcat server, you can configure the Tomcat session timeout.

To change the session timeout for an Apache Tomcat server

1. Open the following file in a text editor:
<Precise_root>\products\gui\website\webapps\i3\web.xml
2. Change the default session timeout (180) to the required minutes. For example:
<session-config>
 <session-timeout>180</session-timeout>
</session-config>
3. Restart the Precise FocalPoint server.

Verifying Precise login credentials using an external password repository

 Configuring the Precise login mechanism is not required to secure a Precise system.

Precise FocalPoint confirms the Precise authentication credentials by using the Java Authentication and Authorization Service (JAAS). The JAAS runs a login module that authenticates the password according to an internal Precise roles' table.

Because the JAAS is a common Application Programming Interface (API), you can also configure it to run a custom login module that authenticates a role's password against an external, centralized password repository. To do so, you must first define the respective role in AdminPoint. For more information on managing roles in AdminPoint, see the [Precise Administration Guide](#).

The login module is a Java class that implements the login module interface of the JAAS API. This API exists for the Java Runtime Application (JRE) version 1.4.2 and later. It is part of the `javax.security.auth.*` package.

When your own login module is ready for use, configuring the external password authentication involves the following tasks:

- Updating the Precise configuration to work with the new login module
- Adding the class of the new login module to the Precise CLASSPATH

To update the Precise configuration

1. Log in to the Precise FocalPoint.
2. Back up the following file:
`<Precise_root>/products/i3fp/login/jaas.config`
3. In the original file, do the following:
 - a. **Change the line.** `StartPoint{com.precise.infra.login.InfraDbLdapSupportLoginModule required};`
 - b. **To.** `StartPoint{new login module class required};`
where new login module class is the class name of your custom login module.
4. Save and close the file.

To add the new login module class to the Precise classpath

1. Log in to the Precise FocalPoint.
2. Back up the following file:
`<Precise_root>/products/i3fp/bin/psin_i3fp_init.xml`
3. In the original file, append the path of the class of the new login module to the classpath section.
4. Save and close the file.
5. Restart Precise FocalPoint.

Running Precise services on Windows with a non-Administrative user

After you have finished installing all Precise components on a server, you may remove the user (used by the Precise services) from the Administrators group and either assigns it to the Power Users group or Users group. In both cases the user should be set to have Login as service authorization. If the user is set to the Users group, you also need to grant access permissions to authenticated users for each Precise service on the machine. To do this, use the SC.exe utility from the Microsoft Resource Kit.

For example:

```
E:\Program Files\Resource Kit\sc.exe sdset psin_sentry_8.7
D: (A;;CCLCSWRPWPDTLOCRRC;;;SY) (A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA) (A;;CCLCSWRPWPDTLOCRRC;;;AU) (A;;CCLCSWRPWPDTLOCRRC;;;PU)
E:\Program Files\Resource Kit\sc.exe sdset psin_i3fp_8.7
D: (A;;CCLCSWRPWPDTLOCRRC;;;SY) (A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA) (A;;CCLCSWRPWPDTLOCRRC;;;AU) (A;;CCLCSWRPWPDTLOCRRC;;;PU)
E:\Program Files\Resource Kit\sc.exe sdset psin_gui_8.7
D: (A;;CCLCSWRPWPDTLOCRRC;;;SY) (A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA) (A;;CCLCSWRPWPDTLOCRRC;;;AU) (A;;CCLCSWRPWPDTLOCRRC;;;PU)
```



This is only an example. Do not copy and paste it in your application. The commands may be different in different Windows versions. The general idea is to use `sdshow` to show the service permissions and then to use `sdset` to copy the Power User group permissions (represented as PU) to the Authenticated Users group permissions (represented as AU). For more details, see the `sc.exe` help file in the Microsoft Resource Kit.

Configuring the Single Sign On feature for Precise

Support of the Single Sign On feature means adding the capability to Precise to be an integrated part of an enterprise application. It also allows the enterprise application users to log in to their systems only once, remembering the credentials and authorization used by the user, and then removing the need to log in again to each of the enterprise systems.

The prerequisites, installation, and configuration of this feature is described in the following sections:

- [About prerequisites](#)
- [Configuring the Apache Web server](#)
- [Installing the SiteMinder Web agent](#)
- [Configuring the SiteMinder Policy server](#)
- [Changing the Precise configuration](#)
- [Disabling the Precise integration with SiteMinder](#)

About prerequisites

Before you configure the Single Sign On feature it is best to define at least one user in Precise who also appears in the SiteMinder folder. This is important for security reasons.

To configure Precise and to enable it to operate using a Single Sign On feature, install and configure the following products:

- Apache Web server version 2.2.3 or higher
- SiteMinder Web agent version 6.00 Hotfix 05.03 or higher*



Precise does not sell or provide CA SiteMinder®. This product should be acquired from Computer Associates.

- Precise version 8.2 and up.

*At the moment of creation of this text, the Web agent for the following platforms could be downloaded:

- Web-Agent 6QMR5 CR002 certified with ASF Apache 2.2.3 Web server on the SPARC based Solaris 8/9/10 platforms.
- Web-Agent 6QMR5 CR002 certified with ASF Apache 2.2.3 Web server on the RHAS 3.0 platform.
- Web-Agent 6QMR5 CR002 certified with ASF Apache 2.2.3 Web server on the RHAS 4.0 platform.
- Web-Agent 6QMR5 CR002 certified with ASF Apache 2.2.3 Web server on the Windows 2000 SP4 platform.
- Web-Agent 6QMR5 CR002 certified with ASF Apache 2.2.3 Web server on the Windows 2003 SP1 and Windows 2003 R2 platforms.
- Web-Agent 6QMR5 CR002 certified with ASF Apache 2.2.3 Web server on the AIX 5.2 and AIX 5.3 platforms.

Configuring the Apache Web server

The Precise Single Sign On feature works with Apache Web server v2.2.3 or higher. The Apache Web server should be configured to work as a reverse proxy server, which is installed using the Tomcat port of Precise.

To configure the Apache Web server for Windows

1. Open the \conf\httpd.conf file in the Apache installation folder.
2. Change the line with the Listen and port number to the GUI port of Precise (The port that the Precise Tomcat Web server listens to, in this example 20760). The information will become: Listen 20760
3. Change the line with the *ServerName* and port number (in this example 20760) to the required server and GUI port.
ServerName GUI-TEST-INST.precise.com:20760
4. Look for the following three lines with the proxy modules and remove the pound/hash marks (# sign) from them:
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_http_module modules/mod_proxy_http.so
5. Change the port the Precise Tomcat Web server will listen to, for example to 20761 by adding the following entries at the end of the file, where the new port of the Tomcat is used (In this case 20761, see the following section about this port):
<Proxy *>
 Order deny,allow
 Allow from all
</Proxy> ProxyRequests Off ProxyPreserveHost On
ProxyPass / http://gui-test-inst.precise.com:20761/
ProxyPassReverse / http://gui-test-inst.precise.com:20761/
Verify that http://gui-test-inst.precise.com:20761 is replaced with the fully qualified domain name and port of your Precise installation.
6. Open the <Precise_root>/infra/setup.xml file and edit the <tomcat-port> tag.
7. Change the port of the Precise Tomcat Web server to a port that is not open to the outside world, or is behind a firewall, to prevent direct access to it. In this example, the Tomcat port will be 20761.
8. Restart first the Tomcat service and then the Apache service.

The restart order is important because the Tomcat server has to release the port that the Apache server is configured to listen to.

To configure the Apache Web server for Linux

1. Change the port of the Precise Tomcat Web server to a port that is not open to the outside world, or is behind a firewall, to prevent direct access to it. In this example, the Tomcat port will be 20761.
Remember to make the change in the Precise setup.xml file
2. Enable the mod_proxy feature in the Apache Web server. For example, on a Debian server it is done by symlinking some files:
symsrv:/etc/apache2/mods-enabled# ls
cgid.conf cgid.load userdir.conf userdir.load
symsrv:/etc/apache2/mods-enabled# ln -s ../mods-available/proxy.* . symsrv:/etc/apache2/mods-enabled# ln -s
../mods-available/proxy_http.* .
symsrv:/etc/apache2/mods-enabled# ls
cgid.conf cgid.load proxy.conf proxy.load proxy_http.conf proxy_http.load userdir.conf userdir.load
3. Configure the mod_proxy feature by creating a configuration file snippet, conf.d/symi3, as described in the following code:
symsrv:/etc/apache2/mods-enabled# cd ../conf.d
symsrv:/etc/apache2/conf.d# cat > symi3
<Proxy *>
 Order deny,allow
 Allow from all
</Proxy>
</Proxy>
ProxyRequests Off
ProxyPreserveHost On

ProxyPass / http://gui-test-inst.precise.com:20761/ ProxyPassReverse / http://gui-test-inst.precise.com:20761/
teacup:/etc/apache2/conf.d#
Verify that http://gui-test-inst.precise.com:20761 is replaced with the fully qualified domain name and port of your Precise installation.

Installing the SiteMinder Web agent

For installing the SiteMinder Web agent you need to have SiteMinder installed on your application and a user name and password for access to the SiteMinder support site to download the SiteMinder Web agent.

To install the SiteMinder Web agent

1. Before downloading and installing the SiteMinder Web agent, perform the steps described in the procedure, [To make changes on the System tab in Configuring the SiteMinder Policy server](#).
2. Download and install the latest SiteMinder Web agent for Apache Web servers.
Verify that the version you download supports the Apache Web server version that we support – in this case, version 2.2.3 and that you download the file for the platform on which your Apache Web server is installed.
 - a. Download the agent from <https://support.netegrity.com>.
 - b. Insert your user name and password.
 - c. Select **Tools** in the left pane.
 - d. Choose **Download Manager**.
 - e. Select **SiteMinder Web Agent** in the Download a product drop-down menu.
 - f. Choose **SiteMinder 6.x QMR's**.
 - g. Choose the agent to be downloaded.
3. After installing the SiteMinder Web agent, configure it according to the SiteMinder's *Web agent Installation and Configuration guide*.
4. Open the WebAgent.conf file in the \Program Files\Apache Software Foundation\Apache2.2\conf folder, and then set EnableWebAgent="YES".
5. Add the Apache Web server as a protected resource to the SiteMinder's protected resources.
6. Restart the machine after you have installed the Web Agent.

Configuring the SiteMinder Policy server

The SiteMinder Policy server is used to configure the policy server to protect Precise.

To configure the Policy server

1. Log in to the Policy server management application.
2. Define the protection on the Precise application by performing steps on two of the three main tabs (System, Domains, Global Policies) on the main window of the Policy server management application as described in separate procedures.

To make changes on the System tab

1. Define a new Web agent under the Agents item.
2. Define a new Host Configuration Object under the Host Conf Objects item.
3. Duplicate the DefaultHostSettings object, give it a name, and replace the complete <IPAddress> with the Policy Server IP address.
4. Define a new Agent Configuration Object under the Agent Conf Objects item.
5. Duplicate the ApacheDefaultSettings configuration object, give it a name, and configure the following items so that they have the values as described in the table:
 - **PersistentCookies.** Yes
 - **IgnoreExt.** Add the following extensions: .xml and .css
 - **ForceFQHost.** Yes
 - **DefaultAgentName.** Verify that this contains the name of the new Web agent defined in the Agents item.
 - **AgentName.** Verify that this contains the name of the new Web agent defined in the Agents item.
 - **CookieDomain.** Add the domain the agent is working in. For example: .precise.com

To make changes on the Domains tab

1. In the domain tab, add a domain and give it a name, such as precise.
2. Add the user directories to the related Precise domain. See the SiteMinder documentation for further instructions.
3. Under the Precise domain, add a realm and give it a name, such as precise-Realm. This realm will protect Precise.
4. Configure the Precise-Realm in the realms subfolder.
5. Under the Precise-Realm, create a rule and give it a name, such as Precise-rule.
6. Add a new response under the Precise/Responses entry.
7. Add a new policy under the Precise/Policies entry:

To configure the Precise-Realm

1. Open the Realms subfolder by clicking the + icon next to the Realms folder under the Precise domain
2. Double click the Precise-Realm folder.
3. On the Resource tab, verify that the following items have the following values:
 - **Agent.** Add the Web agent that is installed on the Precise Web server.
 - **Resource filter.** /i3/Login
 - **Authentication scheme.** Basic authentication
 - **Default resource protection.** Protected
4. On the Session tab, verify that the following items have the following values:
 - **Maximum Time Out Enabled.** Check 2 hours, 0 minutes Idle.
 - **Time Out Enabled.** Check 2 hours, 0 minutes.
 - **Persistent Session.** Choose No Persistent Session.
 - **Synchronous Auditing.** Should be unchecked.

5. On the Advanced tab, perform the following steps:
 - a. Configure the Directory Mapping to the location of the user folder.
 - b. Select the Process Authentication Events checkbox.
 - c. Select the Process Authorization Events checkbox.
6. Click **Apply**, and then click **OK**.

To create and name a rule under the Precise-Realm

1. Right-click in the tree on the Precise-Realm and choose **Create Rule** under Realm.
2. In the Rules Properties dialog box provide a name for the rule, such as Precise-Rule.
3. Clear the Perform Regular Expression checkbox.
4. Under the Action group, select the Web Agent actions and Get and Post.
5. Under the Allow/Deny and Enable/Disable group, select the Allow Access radio button.
6. Under the Allow/Deny and Enable/Disable group, select the Enabled checkbox.

To add a new response under the Precise/Responses entry

1. Give a name to the response, such as Precise-response.
2. Select SiteMinder's Web agent response type option.
3. Click **Create** and create the response attribute.
4. Select the User Attribute radio button.
5. Create a cookie called Precise-SiteMinderUser. That returns the FullName if it is the NT domain name. If you are working with a different folder, choose the property in the folder that holds the user name.
This user name should be defined also in the Precise application in the Precise AdminPoint.
6. Select the Recalculate value every xx seconds checkbox and give it a value of 15.

To add a new policy under the Precise/Policies entry

1. Give a name to the policy, such as Precise-policy.
2. Verify that the policy is enabled.
3. In the Rules tab, insert the Precise-rule and the Precise-response with the values you set in the previous procedures.
4. In the Users tab, define the relevant users.

Changing the Precise configuration

The Precise configuration needs to be changed to connect it to SiteMinder and activate the Single Sign On feature. To connect SiteMinder and activate the Single Sign On feature to Precise.

1. Edit the SiteMinder.htm file located in:
`<Precise_root>\products\gui\website\webapps\i3\Login`
2. Set the bSiteMinderActive variable to True (bSiteMinderActive = true;).
3. Save the file.
4. Edit the `products\i3fp\login\jaas.config` file so that its content looks like:
`StartPoint{com.precise.infra.login.SiteMinderLoginModule required};`
5. Stop and then restart the Precise FocalPoint.

Disabling the Precise integration with SiteMinder

To disable the integration between SiteMinder and Precise, two procedures need to be performed: one to roll back the Precise configuration changes and one to roll back the Apache Web agent configuration changes.

To roll back the Precise configuration changes

1. Edit the siteMinder.htm file located in:
`<Precise_root>\products\gui\website\webapps\i3\Login`
2. Set the bSiteMinderActive variable to False (bSiteMinderActive = false;).
3. Edit the `products\i3fp\login\jaas.config` file so that its content looks like:
`StartPoint{com.precise.infra.login.InfraDbLoginModule required};`
4. Stop and then restart the Precise FocalPoint.

To rollback the SiteMinder configuration changes

1. Shut down the Web Agent installed on Precise Web server machine. For more information on how to shut down the Web agent, see the SiteMinder documentation.
2. In the Apache installation folder, open the WebAgent.conf file which is located in:
 - **Windows.** `\Program Files\Apache Software Foundation\Apache2.2\conf`
 - **Linux.** `web_server_home/conf`
 where `web_server_home` is the location of the installed Web server.
3. Change EnableWebAgent to No (EnableWebAgent="NO").
4. Restart the Apache service.

Configuring LDAP to authenticate Precise users

Precise can integrate with Lightweight Directory Access Protocol (LDAP). LDAP is a better option than JAAS. The following section describes how to configure LDAP.

Best practices for LDAP configuration

Once integrated with LDAP, Precise gets all users and groups from the LDAP and synchronizes them into its own database. Login passwords are authorized by LDAP, thus preventing the need to keep (and verify) the users' passwords within Precise.

LDAP provides access for management and browser applications that provide read/write interactive access to the X500 folder. Setting up an LDAP configuration will reduce Users/Roles management in Precise; it also uses the already managed LDAP repository for Precise.

Pay close attention to your organizational structure in the LDAP repository before setting up the LDAP configuration for Precise. You must understand the current LDAP structure to determine the data needed from existing LDAP repository entities for Precise.

Map a set of users and roles to a Precise domain. While synchronizing the LDAP data to Precise, the relevant users/roles will be identified by the given domain. For login, the domain name will be the user.



It is preferable to set the domain name as the enterprise domain, and the Users/Roles root as the relevant LDAP branch which contains the domain users.

Setting up the Precise system to work with LDAP blocks all user/role management operations in the Precise system, except for permissions management. The LDAP synchronization process deletes all Precise users and roles from the Precise system which are not also found in the LDAP repository, except for user "admin" and role "Precise manager."

Map a set of users and roles to the Precise domain. After synchronizing the LDAP data to the Precise system, the domain will identify relevant users or roles. The domain name will be user-defined for login purposes. Set the domain name as the enterprise domain, and the users/roles root as the relevant LDAP branch that holds domain users.

To enable synchronization of Users and Roles from the LDAP repository into the Precise database, configure the LDAP as described below.

To configure LDAP

1. Update the ldap file (as specified below) in the main Precise FocalPoint machine under:
`<precise_root>\products\i3fp\registry\products\infrastructure\login\ldap.xml`
2. Delete the ldap.xml.status file (in the same folder as ldap.xml)
3. Update the roles file in the main Precise FocalPoint server under:
`<precise_root>\products\i3fp\registry\products\infrastructure\roles\settings.xml` by updating ignore-last-role-on-delete to true:
`<ignore-last-role-on-delete>true</ignore-last-role-on-delete>`
4. Delete the settings.xml.status file (in the same folder as settings.xml)
5. Restart the Precise FocalPoint.

Connection details

Enter the following connection information:

- `<host>` to specify the host name/IP of the LDAP repository server
- `<port>` to specify the port on which the LDAP repository server is listening on
- `<bind-user>` to specify the LDAP user name for binding in the synchronization process
- `<bind-password>` to specify the password of the bind user



The `<bind-password>` will be supplied encrypted. Use the "encrypt" CLI action to encrypt. If `<use-ldap-authentication>` is "false," the password setting must be an encrypted empty string. For more details on how to encrypt a password, see the [Precise CLI Utility Reference Guide](#).

Mapping information

The domain element holds information for the domains that are required to synchronize. You can specify one or more domain elements. Enter the following mapping information:

- `<domain-name>` A unique name for the domain, to be concatenated to the imported users or roles name. The user name of such user is: `domain-name\user-name`.
- `<root-group>` To specify an LDAP group DN. The import process will take all members (users and groups) of this group. (Use this when `<domain-in-root-method>` is 'single'.)
- `<users-root>` To specify an LDAP object DN. The import process will take all users under this object. (Use this when `<domain-root-method>` is 'multiple'.)
- `<groups-root>` To specify an LDAP object DN. The import process will take all groups under this object. (Use this when `<domain-root-method>` is 'multiple'.)



The names `<root-group>`, `<users-root>`, and `<groups-root>` may have multiple entries under each domain entry.

General information

Enter the following general information:

- `<user-object-class>` Indicates the object class name in the LDAP for the user entity.
- `<group-object-class>` Indicates the object class name in LDAP for the group entity.
- `<user-name-attribute>` Indicates the attribute name in the LDAP for the user name.
- `<group-name-attribute>` Indicates the attribute name in the LDAP for the group name.
- `<user-dn-attribute>` Indicates the attribute name in the LDAP for the user entity DN.
- `<user-login-attribute>` Indicates the attribute name in the LDAP for the user login ID.
- `<group-members-attribute>` Indicates the attribute name in the LDAP for the group members list.
- `<max-users>` Indicates the maximum number of users allowed to import into Precise.
- `<max-groups>` Indicates the maximum number of groups allowed to import into Precise.
- `<domain-root-method>` Indicates whether to use the `<root-group>` or the `<users-root>/<groups-root>` configuration for the entities mapping. Specify single or multiple.
- `<paging-size>` Indicates the number of entities per page in the result set from the LDAP. If zero (0) is specified, the paging mechanism is not used.
- `<use-ldap-authentication>` Indicates whether the LDAP authentication mechanism is used. Specify true or false.
- `<use-ldap-management>` If `<use-ldap-authentication>` is set to true, this parameter specifies whether users/roles management is by LDAP or by the Precise user interface. Specify true or false.
- `<use-case-sensitive>` If `<use-case-sensitive>` is set to true, the LDAP sync user will be set to case sensitive.

Example of a registry entry

Below is a registry entry example for the ldap.xml file.

```

</ldap>
  <!-- Indicator for using Ldap authentication true/false -->
  <use-ldap-authentication>true</use-ldap-authentication>
  <!-- Indicator for using Ldap for managing users/roles, true will block I3 GUI operations -->
  <use-ldap-managment>true</use-ldap-managment>
  <!-- Ldap server host name -->
  <host>pss-dc01</host>
  <!-- Ldap server port -->
  <port>389</port>
  <!-- Ldap paging size -->
  <paging-size>500</paging-size>
  <!-- Ldap bind user name -->
  <bind-user>CN=i4dcf,OU=APM Service Users & Groups,DC=precise,DC=com</bind-user>
  <!-- Ldap bind user password, encrypted!! -->
  <bind-password>_EncryptI3_A_1_F10EEB2FC3B6F88E</bind-password>
  <!-- in case there is only on domain the user can configure not to type the domain in the login -->
  <use-domain-in-login>>false</use-domain-in-login>
  <domains>
    <domain>
      <domain-name>development</domain-name>
      <!-- Ldap group to import its members -->
      <root-group>CN=BU_RnD,OU=R&D,OU=APM,DC=precise,DC=com</root-group>
      <!-- Ldap group to import its members -->
      <root-group>CN=GRP_Integration,OU=Unknown users & groups,OU=APM Service Users & Groups,DC=precise,DC=com</root-
group>
    </domain>
    <domain>
      <domain-name>QA</domain-name>
      <!-- Ldap group to import its members -->
      <root-group>CN=BU_RnD,OU=R&D,OU=APM,DC=precise,DC=com</root-group>
    </domain>
  </domains>
  <!-- Ldap objectClass of the Users to sync -->
  <user-object-class>person</user-object-class>
  <!-- Ldap objectClass of the Roles to sync -->
  <group-object-class>group</group-object-class>
  <!-- Ldap attribute name of the User name -->
  <user-name-attribute>name</user-name-attribute>
  <!-- Ldap attribute name of the User distinguished name -->
  <user-dn-attribute>distinguishedName</user-dn-attribute>
  <!-- Ldap attribute name of the User login name -->
  <user-login-attribute>sAMAccountName</user-login-attribute>
  <!-- Ldap attribute name of the Role member list -->
  <group-members-attribute>member</group-members-attribute>
  <!-- Ldap attribute name of the Role name -->
  <group-name-attribute>name</group-name-attribute>
  <!-- I3 max users -->
  <max-users>500</max-users>
  <!-- I3 max roles -->
  <max-roles>500</max-roles>
  <!-- Parameters handling method: single/multiple -->
  <domain-root-method>single</domain-root-method>
  <!-- Ldap sync user set as case sensitive -->
  <use-case-sensitive>>false</use-case-sensitive>
</ldap>

```

For more information on running LDAP-sync command, see the [Precise CLI Utility Reference Guide](#).