Password Policy Enforcer/Web

V3.5

Administrator’s Guide

Contents

Introducing PPE/Web

PPE/Web is a web server extension that allows users to change their Windows NT/2000 passwords using a web browser. All processing takes place on the web server, so there are no applets, components or scripts to deploy.

PPE/Web enhances security by ensuring that user passwords comply with the organization's password policy. A password policy defines the rules that users must follow when choosing a new password. Password policies are important because they ensure that users choose passwords that are:

- Difficult to guess or crack.
- Compatible with other networks or applications.

PPE/Web is not a standalone product; it works in conjunction with Password Policy Enforcer. It is assumed that the reader is familiar with PPE's concepts and features. More information about Password Policy Enforcer is available at www.anixis.com

Organizations that do not want to deploy Password Policy Enforcer across their internal network can configure PPE to only enforce the password policy for passwords that are changed via PPE/Web. Refer to the Installation section for more information.

Installation

System requirements

- Windows NT [1], 2000 or XP
- A web server capable of calling Internet Server API (ISAPI) extensions
- Password Policy Enforcer V3.0 or later
- 1 Megabyte free disk space
- 32 Megabytes RAM
- A forms capable web browser

[1] Windows NT V4 with Service Pack 3 or higher required

Upgrading from PPE/Web V3.0

Follow these steps to upgrade from PPE/Web V3.0 to V3.5:

1. Replace the existing PPEcWEB.DLL and ClntIns.EXE files with the updated files included in the PPE/Web V3.5 distribution.
2. Run the PPE/Web V3.5 ClntIns utility to configure PPE/Web.

Upgrading from PPE/Web V1.0

Follow these steps to upgrade from PPE/Web V1.0 to V3.5:

3. Install, configure and test PPE V3.5.
4. Edit the Client Configuration File
5. Run the Client Installer
6. Replace the existing PPEcWEB.DLL with the updated PPEcWEB.DLL included in the PPE/Web V3.5 distribution.
7. Extract Rejected.htm from the PPE/Web V3.5 distribution and copy it into the PPE/Web folder.

Installing Password Policy Enforcer

The Password Policy Server (PPS) included with PPE V3.x is responsible for distributing the password policy to PPE/Web. Proceed to the Installing PPE/Web section if you have already installed and configured a Password Policy Server.

Refer to the PPE Administrator's Guide for detailed instructions on installing and configuring a Password Policy Server.

Visit www.anixis.com to download Password Policy Enforcer.

The Choosing Password Policy Server(s) section of the PPE Administrator's Guide explains which computer(s) should be used as Password Policy Servers when enforcing the password policy:

- for an entire domain
- for a standalone workstation or member server
- for part of a domain
- without a domain controller

PPE/Web is compatible with all these configurations. The PPS uses very few system resources, so it can be installed onto a server that is also running PPE/Web.

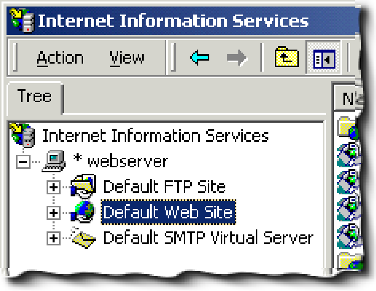
Some sections of the PPE Administrator's Guide specify that the Password Policy Client must be installed for certain features to work. Most of these features will also work with PPE/Web.

Installing PPE/Web

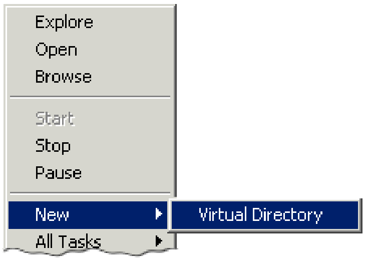
PPE/Web should work with any web server that supports Internet Server API (ISAPI) extensions. This section demonstrates the installation procedure for Microsoft Internet Information Server 5.0. The installation procedure is very similar for other versions of IIS. Refer to your web server's documentation if you are not using IIS.

Do not proceed until you have installed and configured at least one Password Policy Server. Refer to the Installing Password Policy Enforcer section for more information.

1. Extract the contents of PPEWeb35.zip into a new folder.
2. Select **| Start | Programs | Administrative Tools | Internet Services Manager |**
3. Select the web site that will host PPE/Web.

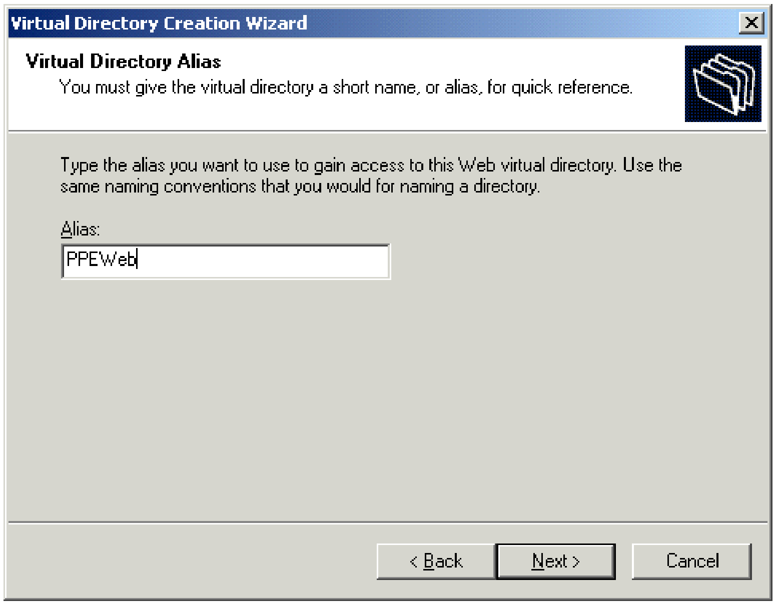

Internet Information Services
Action
View
Tree
Na
Internet Information Services
* webserver
Default FTP Site
Default Web Site
Default SMTP Virtual Server

4. Click the right mouse button and select **| New | Virtual Directory |**



5. The Virtual Directory Creation Wizard will start. Click the **Next** button to continue.

6. You will be prompted to enter an Alias for this virtual directory. Enter an Alias name and click **Next** to continue.



Virtual Directory Creation Wizard

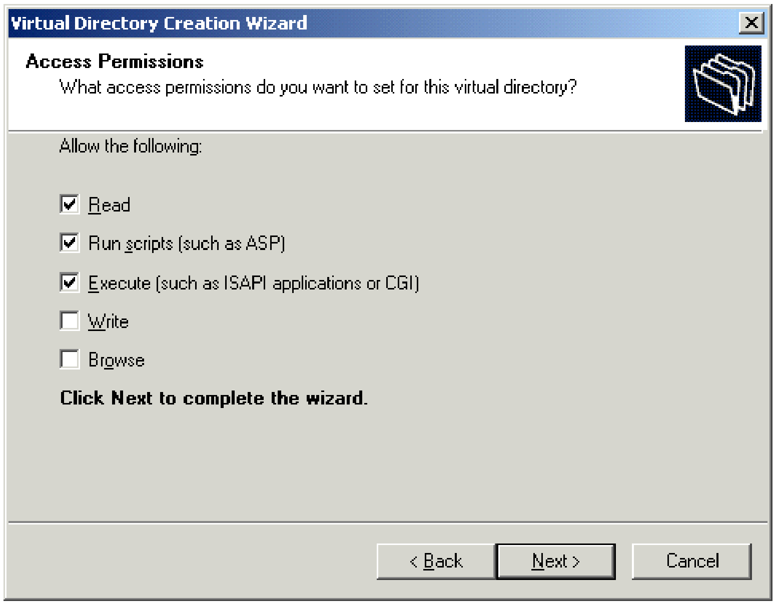
Virtual Directory Alias

You must give the virtual directory a short name, or alias, for quick reference.

Type the alias you want to use to gain access to this Web virtual directory. Use the same naming conventions that you would for naming a directory.

Alias: PPEWeb

7. The Virtual Directory Creation Wizard will prompt you to enter a path. Enter the path to the folder that you created in Step 1. Click **Next** to continue.
8. You will be prompted to select the desired access permissions for the PPE/Web virtual directory. Ensure that **Read**, **Run** and **Execute** are all enabled. Click **Next** to continue.



Virtual Directory Creation Wizard

Access Permissions

What access permissions do you want to set for this virtual directory?

Allow the following:

☑ Read

☑ Run scripts (such as ASP)

☑ Execute (such as ISAPI applications or CGI)

☐ Write

☐ Browse

Click Next to complete the wizard.

9. Click the **Finish** button to complete the installation.

Configuration

PPE/Web must be configured before it is used to change passwords. This section will guide you through the various configuration tasks.

Editing ChangePw.htm

ChangePw.htm is in the PPE/Web folder that was created during installation. Open this file with a HTML or text editor.

Use Notepad if you don't have a HTML editor.

ChangePw.htm contains HTML comment tags to help you identify the various sections of the file. HTML comment tags look like this:

```
<!-- This is a comment -->
```

Entering the password policy rules

PPE/Web does not retrieve the password policy message from the PPS. The password policy message is hard coded into ChangePw.htm.

Search for the comment tag shown below to find the rules section.

```
<!-- START RULES SECTION -->
```

The rules section looks like this:

```
<!-- START RULES SECTION -->
<!-- Enter your Password Policy rules below this line -->
<!-- End each line with a <br> (break) tag          -->
                    [Enter your rules here]<br>
                    [Enter your rules here]<br>
                    [Enter your rules here]<br>
                    [Enter your rules here]<br>
                    [Enter your rules here]<br>
                    [Enter your rules here]<br>
                    [Enter your rules here]<br>
                    [Enter your rules here]<br>
<!-- END RULES SECTION -->
```

Use the editor to modify this text so that it describes the rules that users must comply with when changing their password. For example:

```
<!-- START RULES SECTION -->
<!-- Enter your Password Policy rules below this line -->
<!-- End each line with a <br> (break) tag          -->
                    - Contain a Uppercase Alpha character<br>
                    - Contain a Lowercase Alpha character<br>
                    - Contain a Numeric character<br>
                    <br><br><br><br><br>
<!-- END RULES SECTION -->
```

Note that the extra <br> tags have been kept in this example to preserve the page formatting of the original file.

Entering domain names

The second change that must be made to ChangePw.htm is in the domain names section. Search for this comment tag to find the domain names section:

```
<!-- START DOMAIN NAMES SECTION -->
```

The domain names section is used to display a dropdown list of domain names. One line is needed for each domain that users will be changing passwords on. The format for each line is:

```
<option value="[Domain name]">[Display name]</option>
```

Replace `[Domain name]` with the name of the Windows NT/2000 domain. Replace `[Display name]` with the text that will be shown in the dropdown list. For example:

```
<option value="Finance">Finance</option>
```

The `[Domain name]` and `[Display name]` do not have to be the same. This example is also valid:

```
<option value="Admin">Admin network</option>
```

The modified HTML should look similar to this:

```
<!-- START DOMAIN NAMES SECTION -->
<!-- Refer to the PPE/Web Administrator's Guide for more -->
<!-- information about this block of HTML                -->
                  <option value="Admin">Admin network</option>
                  <option value="Finance">Finance</option>
<!-- END DOMAIN NAMES SECTION -->
```

The domain name list can be hidden if users will be changing passwords for a single domain. Refer to a HTML reference for information on hidden form fields.

PPE/Web will not work if the domain name list is deleted.

Save the changes that you have made to ChangePw.htm.

Editing the Client Configuration File

The Client Configuration File (PPEClnt.cfg) is also in the PPE/Web folder that you created during installation. Edit this file with a text editor such as Notepad.

The PPE/Web Client Configuration File is identical to the PPE Client Configuration File. If you have already created a PPE configuration file, copy it into the PPE/Web folder and proceed to Using the Client Installer.

PPEClnt.cfg contains the PPE/Web configuration settings. These settings are explained below. Lines in PPEClnt.cfg starting with a # are ignored by the installer.

Domain/Server list

PPE/Web uses this list to locate the Password Policy Server(s). PPE/Web cannot communicate with a PPS if the Domain/Server list is empty. The format for each entry in the list is:

```
DOM [Domain Name] [Hostname or IP Address]
```

Multiple servers can be defined for a domain, but only one server is permitted per line. Servers are queried in sequence starting at the top of the list. For example, your Domain/Server list may look like this:

```
DOM Finance 192.168.10.12
DOM Finance srv01.finance.company.com
DOM Research 192.168.20.20
```

When a user tries to change their Finance domain password, PPE/Web will query the PPS with the IP address 192.168.10.12. If this server fails to respond, PPE/Web will query the PPS on the srv01.finance.company.com computer.

The Research domain only has one PPS in the example above. It has the IP address 192.168.20.20. This server is queried when a user tries to change their password for the Research domain.

At least one DOM entry must exist for every domain name defined in ChangePw.htm.

Set the IP address to 127.0.0.1 if PPE/Web and the PPS are installed on the same computer.

Timeout

The Timeout setting specifies how long PPE/Web will wait (in milliseconds) for a response from a PPS. The default timeout of two seconds is suitable for most networks.

Retries

The Retries setting specifies how many times PPE/Web will try to resend a request that has timed out. The default value of two should be suitable for most networks.

PPE/Web will retry a request before querying the next PPS in the Domain/Server list. This may lead to long delays if one of the Password Policy Servers stops responding. If this is the case, either reduce the Retries setting or remove the problem server from the Domain/Server list.

PPS_Port

The PPS_Port setting specifies the UDP Port that PPE/Web uses to communicate with the PPS. This value should be set to match the **Password Policy Server port** property in the PPS properties page.

Port 1333 has been assigned by IANA to the Password Policy Protocol.

Using the Client Installer

The Client Installer (ClntIns.exe) reads the configuration settings from the Client Configuration File and stores them in the registry. Execute this command in the PPE/Web folder to configure PPE/Web:

```
ClntIns INSTALLWEB PPEClnt.cfg
```

ClntIns.exe should respond with:

```
PPE/Web Client Configured.
```

Execute the `ClntIns INSTALLWEB PPEClnt.cfg` command every time that changes are made to PPEClnt.cfg.

Execute the following command to remove the client configuration settings from the registry:

```
ClntIns UNINSTALL
```

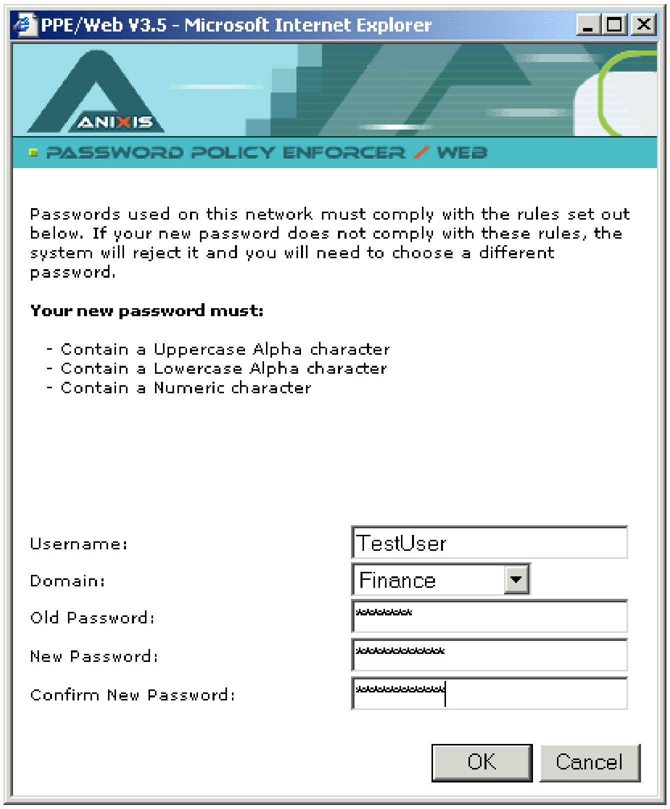
PPE/Web is now installed and configured.

Testing

Use a web browser to open the PPE/Web welcome page in the PPE/Web virtual directory. For example:

http://www.mywebserver.com/PPEWeb/default.htm

Display the password change form by clicking the **Change Password with PPE/Web** button at the bottom of the welcome page.


PPE/Web V3.5 - Microsoft Internet Explorer
ANIXIS
PASSWORD POLICY ENFORCER / WEB
OK
Cancel

Passwords used on this network must comply with the rules set out below. If your new password does not comply with these rules, the system will reject it and you will need to choose a different password.

Your new password must:

- Contain a Uppercase Alpha character
- Contain a Lowercase Alpha character
- Contain a Numeric character

Username: TestUser
Domain: Finance
Old Password: ********
New Password: ************
Confirm New Password: ************

Enter the required information into the relevant fields and click the **OK** button.

PPE/Web displays a Password Changed message if the password was successfully changed.

PPE/Web displays a Password Rejected message if the new password does not comply with the password policy. Click the **OK** button to try a different password.

Refer to the Troubleshooting section if PPE/Web displays an error message.

Resetting passwords

Administrators can use PPE/Web to reset a user's password without knowing the current password.

Create a new PPE/Web virtual directory for administrators to reset user passwords. The required configuration changes may stop users from changing their own passwords.

Administrators will have to authenticate themselves to the web server before they can reset a password. Disable anonymous access to the PPE/Web folder and enable one of the web server's authentication methods.

Edit ChangePw.htm and replace the domain names with computer names in UNC format. Use the name of the Primary Domain Controller for domain accounts. For example:

```
<!-- START DOMAIN NAMES SECTION -->
<!-- Refer to the PPE/Web Administrator's Guide for more -->
<!-- information about this block of HTML                -->
        <option value="\\ADMDC01">Admin (reset)</option>
        <option value="\\FINDC01">Finance (reset)</option>
<!-- END DOMAIN NAMES SECTION -->
```

Edit PPEClnt.cfg and replace the domain names in the Domain/Server list with the computer names used in ChangePw.htm. For example:

```
DOM \\ADMDC01 192.168.40.9
DOM \\FINDC01 srv01.finance.company.com
```

The IP Address / Hostname points to the PPS, not the computer that the user account resides on. For example, in the first line above, PPE/Web would reset the user password on the ADMDC01 computer, but it would get the password policy off the PPS at 192.168.40.9.

Execute the command shown below to store the updated Domain/Server list in the registry:

```
ClntIns INSTALLWEB PPEClnt.cfg
```

PPE/Web can now be used to reset account passwords. PPE/Web will only reset a password if the Old Password field is blank. The Old Password field can be hidden, but not deleted.

PPE/Web only allows authorized users to reset account passwords. All other users will receive an Access Denied error. Refer to the Windows NT/2000 documentation for information on which groups are permitted to reset account passwords.

If one web server will be used for both password changes and password resets, then the Domain/Server list should contain both sets of entries. For example:

```
DOM Finance 192.168.10.12
DOM Finance srv01.finance.company.com
DOM Research 192.168.20.20
DOM \\ADMDC01 192.168.40.9
DOM \\FINDC01 srv01.finance.company.com
```

Customizing the user interface

You can modify PPE/Web's user interface so that it integrates seamlessly with your other HTML forms and documents. There are five HTML files that define PPE/Web's user interface:

ChangePw.htm (can be renamed)

This file contains the password change form. The form must call PPEcWeb.dll with the POST method and must contain Username, Domain, OldPassword, NewPassword and ConfirmPassword fields.

If PPE is enforcing multiple password policies, you can create one password change form for each policy and direct users to the appropriate form.

Default.htm (can be renamed)

This file contains the welcome page and should have a button or link that opens ChangePw.htm (or equivalent).

Error.htm (do not rename)

This file is used to display user error messages and must contain the [ERROR] placeholder (including square brackets). PPE/Web replaces the [ERROR] placeholder with the error message.

Rejected.htm (do not rename)

This file is used to display the rejection reason message and must contain the [REJECTION_MESSAGE] placeholder. PPE/Web replaces this placeholder with the rejection reason returned by the PPS.

Success.htm (do not rename)

This file is used to notify the user that their password was successfully changed.

Securing PPE/Web

Consider the following issues before allowing users to access the PPE/Web virtual directory:

Use a secure protocol

The HTTP protocol does not encrypt user details (including passwords) before sending them to the web server. HTTPS is a secure version of the HTTP protocol that does encrypt details before transmitting them. Refer to your web server's documentation for information on HTTPS and SSL.

Disable Anonymous Access

By default, web servers do not require users to authenticate themselves to view a web page. This is not recommended for PPE/Web. Disable anonymous access to the PPE/Web folder.

Restrict access to the PPE/Web folder

Access to the PPE/Web folder should be restricted so that PPEc32.DLL cannot be deleted, modified or replaced.

Remove unnecessary files

The PPE/Web folder should only contain required files. The Client Installer and Client Configuration File are not needed after PPE/Web has been configured. Remove these and any other unnecessary files.

Consider removing the domain list

If it is undesirable to publicly expose your Windows domain names, replace the dropdown list in ChangePw.htm with an edit field.

Purchasing a license

PPE/Web is licensed on a per-user basis. One license is required for each person that will be changing his or her password with PPE/Web. Visit the ANIXIS web site for the latest pricing and purchase information: www.anixis.com

PPE/Web can be used for evaluation purposes without having to purchase a license. PPE/Web will randomly display a license reminder until a license is purchased. The license reminder is displayed approximately once in every ten password changes. PPE/Web does not change the user's password if it displays a license reminder.

You are permitted to evaluate PPE/Web for up to 21 days. After this time, you must either remove all copies or purchase a license for it.

Troubleshooting

HTTP Error 405: Method Not Allowed

Internet Information Server displays this error message if the PPE/Web virtual directory does not have execute permissions. Use the Internet Services Manager console to enable the execute permission for the PPE/Web virtual directory.

PPE/Web Error 000: Evaluation reminder

PPE/Web periodically displays this message if it cannot find a license file. Refer to the licensing section for more information.

PPE/Web Error 100: Invalid Method

This error is displayed if the change password form is not using the POST method. Always use the POST method with PPE/Web.

PPE/Web Error 200: Missing Form Field

This error indicates that at least one required field is missing from ChangePw.htm. The form must contain all these fields: Username, Domain, OldPassword, NewPassword and ConfirmPassword. Fields can be hidden, but they cannot be removed.

PPE/Web Error 300: File Open Failed

This error is displayed when PPE/Web cannot open Error.htm, Rejected.htm or Success.htm. Make sure that all three files are in the PPE/Web folder.

PPE/Web Error 400: No Response

This error indicates that a PPS did not respond. Check the PPS and verify that the PPE/Web configuration settings are correct.

Check the support section of the ANIXIS web site www.anixis.com/products/ppeweb/support.htm if you cannot resolve a PPE/Web problem.

Technical support

Several technical support options are available for PPE/Web users.

Technical Documents

PPE/Web Technical Documents contain answers to frequently asked questions. PPE/Web Technical Documents are available online at www.anixis.com/products/ppeweb/tdindex.htm

Email support

Email support is available to registered customers as well as organizations that are evaluating PPE/Web. Questions are normally answered within 24 hours. Send questions to support@anixis.com

Telephone support

Telephone support is only available to customers that have pre-purchased telephone support incidents. If you call while the office is unattended, please leave a message. Your message will be sent to a pager and your call will be returned as soon as possible.

Australian Customers: (02) 4733 0500
International Customers: +61 2 4733 0500

Support is available in English.

License Agreement

If you agree to these terms and conditions, ANIXIS grants you a nonexclusive license to use the accompanying software (the "Software") and documentation. The Software and the documentation are referred to in this Agreement as "Licensed Materials".

BY INSTALLING AND USING THE LICENSED MATERIALS, YOU ARE CONFIRMING ACCEPTANCE OF THIS LICENSE AGREEMENT AND AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT WISH TO DO SO, DO NOT COMPLETE THE INSTALLATION PROCESS. CONTACT ANIXIS PROMPTLY FOR A FULL REFUND.

1. Ownership
The Licensed Materials are the sole and exclusive property of ANIXIS. By paying the license fee, you do not become the owner of the Licensed Materials, but are entitled solely to use the Licensed Materials according to the terms of this Agreement.

2. License
The license granted to you by ANIXIS in this Agreement authorizes you to use the Software on any number of computers, as long as the total number of user licenses is not exceeded. YOU MAY NOT USE, COPY OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT.

3. Term
This Agreement is effective from the date on which you install the Software. This Agreement may be terminated by you at any time by destroying the Licensed Materials, together with all copies, modifications, and merged portions in any form. It will also terminate automatically if you fail to comply with any term or condition of this Agreement.

4. Restrictions on Transfer
You may permanently transfer the Licensed Materials to any other party if the other party agrees to the terms and conditions of this Agreement, and you transfer all copies of the Licensed Materials to that party or destroy those not transferred. By such transfer, you terminate the license granted to you in this Agreement. You may not sublicense, assign, share, rent, lease, or otherwise transfer your right to use the Licensed Materials, nor any rights granted to you under this Agreement, except as stated in this paragraph.

5. Restrictions against copying or modifying the Licensed Materials
The Licensed Materials are copyrighted © by ANIXIS or third parties. Except as expressly permitted in this Agreement, you may not copy or otherwise reproduce the Licensed Materials. In no event does the limited copying or reproduction permitted under this Agreement include the right to decompile or disassemble the Software, or to translate the Software into another computer language.

You agree to include the copyright notice set forth on the label of the media embodying the Software on any copy of the Software in any form, in whole or in part, or of any modification of the Software or any updated work containing the Software or any part thereof. You also agree not to remove any existing copyright notice from any of the Licensed Materials.

6. Protection and Security
You agree to use your best efforts and to take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized person has access to them and that no unauthorized copy, publication, disclosure or distribution of any of the Licensed Materials is made. You acknowledge that the Licensed Materials contain valuable, confidential information and trade secrets and that unauthorized use and copying are harmful to ANIXIS, and that you have a confidential obligation with respect to such valuable information and trade secrets.

7. Upgrades
If this copy of the Licensed Materials is an upgrade from an earlier version of the Licensed Materials, it is provided to you on a license exchange basis. You agree by your installation and use of this copy of the Software to voluntarily terminate your earlier license and that you will not continue to use the earlier version of the Licensed Materials nor transfer it to another.

8. Trial Version
If this copy of the Licensed Materials is a Trial Version, you are permitted to use the Licensed Materials without charge for up to 21 days. After 21 days, you must either destroy all copies of the Licensed Materials or pay the required license fee.

Use of the Licensed Materials after the 21 day trial period without paying the license fee is in violation of Australian and international copyright laws.

9. Limited Warranty

ANIXIS warrants that the media on which the Software is recorded will be free from defects in workmanship and materials for a period of 90 days from the date of payment of the license fee. If the media and dated proof of purchase are returned to ANIXIS within 90 days of the date of payment of the license fee, and if ANIXIS determines the media to be defective and provided the media was not subject to misuse, abuse or use in defective equipment, ANIXIS will, at its option, (1) replace the media, or (2) refund the license fee paid by you, upon your return to ANIXIS of the Licensed Materials, including all copies or any portions thereof, and the dated proof of payment of the license fee.

ALL IMPLIED WARRANTIES ON THIS MEDIA, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE LIMITED TO THE DURATION OF THE EXPRESS WARRANTY SET FORTH ABOVE.

IN NO EVENT WILL ANIXIS OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF PROFITS OR INABILITY TO USE THE LICENSED MATERIALS, EVEN IF ANIXIS OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL ANIXIS'S OR SUCH OTHER PARTY'S LIABILITY FOR ANY OTHER DAMAGES OR LOSS TO YOU OR ANY OTHER PARTY EXCEED THE LICENSE FEES PAID FOR THE LICENSED MATERIALS.

10. General

If any provision or portion of a provision of this Agreement is determined to be invalid under any applicable law, it shall be deemed omitted and the remaining provisions and partial provisions of this Agreement shall continue in full force and effect.

This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements, and undertakings are hereby expressly cancelled.