



ANIXIS Password Reset

Administrator's Guide

V2.1



© Copyright 2003 - 2011 ANIXIS. All rights reserved.

ANIXIS, ANIXIS Password Reset, ANIXIS Password Reset Client and Password Policy Enforcer are trademarks of ANIXIS. Microsoft, Microsoft Office Excel, Windows, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 and Windows 7 are either registered trademarks or trademarks of Microsoft Corporation. Other product and company names may be the trademarks of their respective owners.

Table of Contents

Introduction	1
What's New	2
Installing APR.....	3
System Components.....	3
Preparing IIS (Windows 2008 and 2008 R2 only)	4
Installation Types	6
Single Server Installation	7
Multiple Server Installation	8
Upgrading From APR V2.x.....	10
Upgrading From APR V1.x.....	11
Using APR	13
Enroll.....	14
Reset.....	15
Unlock	16
Change.....	17
Error Messages.....	18
Configuring APR	19
General Tab	19
Enroll Tab.....	21
E-mail Tab.....	23
Triggers	24
Security Tab	25
Permissions Tab	27
About Tab.....	28
Using the Data Console	29
Filtering Data.....	31
The Filter Row.....	31
Filtering by Column Values	32
Custom Filters	33
The Filter Editor.....	34
The Filter and Status Bars	35
Exporting Data	35
Deleting Users.....	35
Backing up the Database	36
Securing APR.....	37
Installing and Using an SSL Certificate.....	37
Delegating Permissions to the APR Server Service	38
Using Delegated Permissions with Protected Groups.....	39

Editing the HTML Templates.....	40
Examples	41
Replace the ANIXIS Logo	41
Edit Page Instructions	42
Edit Validation Error Messages.....	42
Edit Critical Error Messages.....	43
Edit Finished Messages	43
Replace Enroll Question Lists with Text Boxes.....	44
Change Font Sizes and Colors	44
The Password Reset Client.....	45
Installing the PRC	46
Configuring the PRC	49
Licensing the PRC	52
License Agreement	53

Introduction

ANIXIS Password Reset is a self-service password management system that helps organizations to reduce the number of password related help desk calls. APR allows users to securely change their password and unlock their account, even if they have forgotten their current password. The benefits of using APR include:

Reduced Costs

Studies into the costs of password management show that between 20% and 40% of help desk calls are password related. ANIXIS Password Reset helps you to reduce the number of these calls.

Increased Productivity

Employee productivity plummets while they wait in the help desk queue to have their password reset. With ANIXIS Password Reset, users can reset their own password in less than two minutes. Users can even reset their password from the Windows [logon screen](#). This frees the help desk to handle more important issues.

Improved Security

Identifying staff over the phone can be difficult, especially in large organizations. ANIXIS Password Reset identifies users by asking them to answer up to ten questions about themselves. Incorrect answers are logged, and you can configure APR to automatically [lock out](#) users who give too many incorrect answers.

Higher Availability

ANIXIS Password Reset is ready to respond to password management requests at any hour of the day. It takes only minutes to install, and can handle thousands of requests every hour.

The [APR Evaluator's Guide](#) contains step-by-step instructions to help you quickly install, configure, and evaluate ANIXIS Password Reset. Read the Evaluator's Guide if you are using APR for the first time.

What's New

Web Interface

- Compatible with Windows 2008 and 2008 R2.
- Updated HTML templates allow [customization](#) of all user interface elements, including error messages.
- Accepts [user-created](#) enrollment questions.
- Displays the [Password Policy Enforcer](#) policy message during password resets and changes.
- Works without a firewall rule for Password Policy Enforcer Integration when the web server is in a DMZ.
- Gets user and domain names from [URL parameters](#).

APR Server

- Compatible with Windows 2008 and 2008 R2.
- Hashes answers with the SHA-256 algorithm for added security.
- Sends [e-mail alerts](#) to notify users when their account is used.
- Uses a Microsoft SQL Server Compact Edition database. SQL Server Compact is free to use. The database engine is installed by the APR Setup Wizard. No configuration or maintenance needed.
- Can use a service account that is [not a member of Domain Admins](#).
- More detailed auditing with events stored in a database.
- Optimized for multi-CPU and multi-core servers.
- Configurable [inactivity timeout](#), [minimum answer length](#), and [minimum password age](#).
- Works with DNS, UPN, and NetBIOS names.

Password Reset Client

- Included free. The [Password Reset Client](#) allows users to access APR from the Windows Logon and Unlock Computer screens.

Data Console

- The [Data Console](#) is a viewer for the audit log and users database.
- Uses [filters](#) to quickly find relevant information.
- Displays a [recent activity](#) chart with drill-down to daily events.
- [Exports](#) users and logs to Microsoft Excel, HTML, and Text files.
- Displays last enroll, reset, unlock, and password change times.
- Permits manual [deletion](#) of users.

Installing APR

ANIXIS Password Reset V2.1 is designed to run on Windows 2003 and Windows 2008. Users access APR from a web browser, or from the [Password Reset Client](#).

System Requirements

- Windows 2003, 2003 R2, 2008, or 2008 R2 (x86 and x64 editions).
- 20 Megabytes free disk space.
- 20 Megabytes free RAM.

System Components

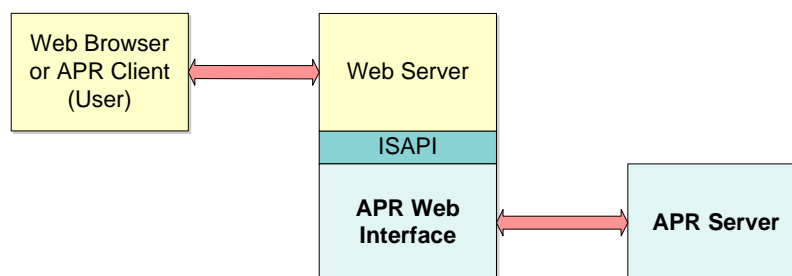
ANIXIS Password Reset has two server components, and an optional [client](#). Both server components can be installed on one server, or they may be installed on separate servers if your web server is in a DMZ.

The Web Interface

The Web Interface is the component that users interact with. It accepts user requests, encrypts them, and sends them to the APR Server. The Web Interface must be installed on a server running IIS 6 or later.

The APR Server

The APR Server is the component that performs requests on behalf of users. It receives requests from the Web Interface, checks the user's credentials, and performs the requested task if the credentials are valid.



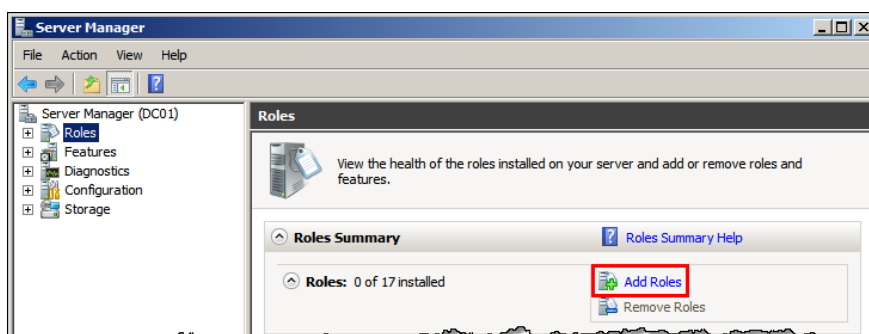
Microsoft SQL Server Compact Edition is installed with the APR Server. SQL Server Compact is free to use and should not be removed. Go to <http://www.microsoft.com/sqlserver/2005/en/us/compact.aspx> for more information. SQL Server Compact is an embedded database. Unlike the full SQL Server, you do not need to configure or manage it.

Preparing IIS (Windows 2008 and 2008 R2 only)

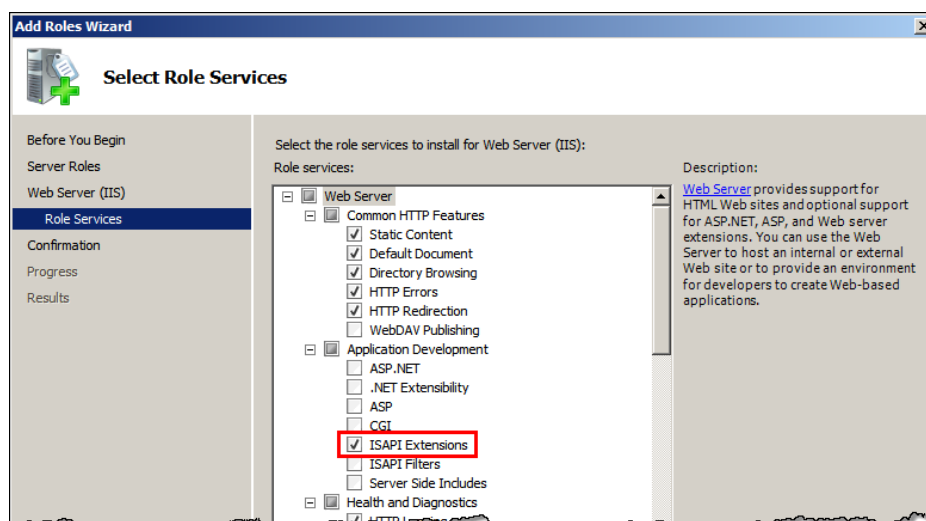
Windows 2008 and 2008 R2 include a modular version of IIS that only has a small set of core features enabled by default. The Web Interface is an ISAPI (Internet Server Application Programming Interface) extension, so you must enable ISAPI extensions on the server that will host the Web Interface.

If IIS is not Installed on the Server

1. Start the Server Manager console (ServerManager.msc).
2. Click the **Roles** item in the left pane.



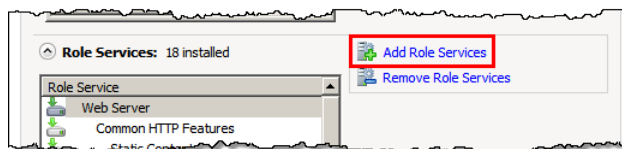
3. Click **Add Roles** in the right pane.
4. Click **Next** if you see the “Before You Begin” page.
5. Select the **Web Server (IIS)** role, and then click **Next** twice.



6. Select **ISAPI Extensions** in the **Application Development** group.
7. Click **Next**, and then click **Install**.
8. Wait for IIS to install, and then click **Close**.

If IIS is Already Installed on the Server

1. Start the Server Manager console (ServerManager.msc).
2. Expand the **Roles** item in the left pane, then click **Web Server (IIS)**.
3. Scroll down to the **Role Services** section in the right pane.



4. Click **Add Role Services**.
5. Select **ISAPI Extensions** in the **Application Development** group.
6. Click **Next**, and then click **Install**.
7. Wait for the role service to install, and then click **Close**.

Installation Types

A single server installation is recommended where users will only access APR from a trusted network, including a VPN. In this installation type, the Web Interface and APR Server are both installed on the same server. The server must have IIS installed, and it must have access to a domain controller in each managed domain.

If ANIXIS Password Reset will be accessible from the Internet without a VPN, then it is likely that you will want to run the Web Interface in a DMZ. A multiple server installation is recommended for this scenario. In this installation type, the Web Interface is installed on an IIS server in the DMZ and the APR Server is installed on another server in the internal network. A firewall rule allows the two servers to communicate.

You must choose the installation type when installing APR, but you can change it later.

An APR Server can accept requests from more than one Web Interface. Having multiple Web Interfaces allows for load balancing and failover, but you should only consider this option if you already have redundant web servers. Most organizations only need one Web Interface.

ANIXIS Password Reset can share server resources with other applications. It is normally not necessary to dedicate a server exclusively to APR. The Web Interface can be installed on an existing web server as long as it is well secured and not overloaded. The APR Server can run on an existing member server or domain controller.

Install the hotfix from Microsoft KB [954896](#) on any Windows 2003 server that will be used as an APR Server. This hotfix is not needed on the Web Interface server in a multiple server installation.

Single Server Installation

To install the Web Interface and APR Server on a single server:

1. Start the APR Setup Wizard (APR21.exe).
2. The Setup Wizard may ask you to backup some files if an older version of APR is detected. Backup the files, and then click **Next**.
3. Click **Next**.
4. Read the [license agreement](#). Click **I accept the terms of the license agreement**, and then click **Next** if you accept all the terms.
5. Select the **All Components** option, and then click **Next**.
6. Type a **User Name**, **Domain**, and **Password** for the APR Server service account. The account will be created and added to the Domain Admins group if it does not exist. You can [remove](#) the account from the Domain Admins group later. If using an existing account, make sure that it has the [required permissions](#).
7. Click **Next**.
8. Select an **IIS Web Site** from the drop-down list, and optionally change the default **Virtual Directory** for the Web Interface. The Web Interface should be installed in its own virtual directory.
9. Click **Next** twice.
10. Wait for ANIXIS Password Reset to install, and then click **Finish**.

The APR Setup Wizard installs the APR Server and associated files into the \Program Files [(x86)]\ANIXIS Password Reset\ folder by default. Use the SERVERDIR parameter to install the APR Server to a different folder. For example, APR21.exe SERVERDIR="D:\Programs\APR\"

Multiple Server Installation

In a multiple server installation you will most likely have a DMZ firewall between the Web Interface and APR Server. Create a firewall rule to allow these components to communicate. The Web Interface initiates a request by sending a datagram with the following properties:

Protocol	UDP
Source address	Web Interface server's IP address
Source port	Any
Destination address	APR Server's IP address
Destination port	5100

The APR Server responds with a datagram that has these properties:

Protocol	UDP
Source address	APR Server's IP address
Source port	5100
Destination address	Web Interface server's IP address
Destination port	Any

Firewalls that perform Stateful Packet Inspection should only need a rule for the request datagram as the response will be allowed automatically.

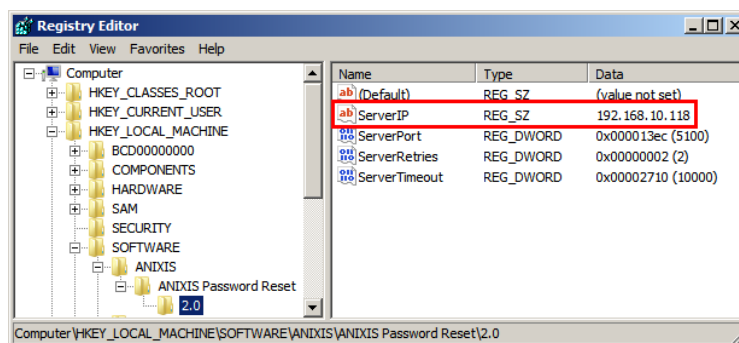
To install the APR Server on a server in the internal network:

1. Start the APR Setup Wizard (APR21.exe).
2. The Setup Wizard may ask you to backup some files if an older version of APR is detected. Backup the files, and then click **Next**.
3. Click **Next**.
4. Read the [license agreement](#). Click **I accept the terms of the license agreement**, and then click **Next** if you accept all the terms.
5. Select the **Server Only** option, and then click **Next**.
6. Type a **User Name**, **Domain**, and **Password** for the APR Server service account. The account will be created and added to the Domain Admins group if it does not exist. You can [remove](#) the account from the Domain Admins group later. If using an existing account, make sure that it has the [required permissions](#).
7. Make sure the **Create Windows Firewall Exception for the APR Server service** check box is selected.
8. Click **Next** twice.
9. Wait for the APR Server to install, and then click **Finish**.

Manually create a firewall exception for UDP port 5100 if a host-based firewall other than the Windows Firewall is installed on the APR Server computer. This does not replace the DMZ firewall exception mentioned above. Both are needed in a multiple server installation.

To install the Web Interface on a server in the DMZ:

1. Start the APR Setup Wizard (APR21.exe).
2. The Setup Wizard may ask you to backup some files if an older version of APR is detected. Backup the files, and then click **Next**.
3. Click **Next**.
4. Read the [license agreement](#). Click **I accept the terms of the license agreement**, and then click **Next** if you accept all the terms.
5. Select the **Web Interface Only** option, and then click **Next**.
6. Select an **IIS Web Site** from the drop-down list, and optionally change the default **Virtual Directory** for the Web Interface. The Web Interface should be installed in its own virtual directory.
7. Click **Next** twice.
8. Wait for the Web Interface to install, and then click **Finish**.
9. Start the Registry Editor (regedit.exe).
10. Expand the **HKEY_LOCAL_MACHINE, SOFTWARE, ANIXIS, ANIXIS Password Reset, and 2.0** registry keys.
11. Set the **ServerIP** registry value to the IP address of the computer that you installed the APR Server onto.



The APR Setup Wizard only installs one Web Interface on each server, but you can copy the files to another directory and publish several Web Interfaces from one server. This allows you to present different user interfaces from each directory. The Web Interfaces all communicate with the same APR Server because there is only one ServerIP value. If you want the Web Interfaces to communicate with different APR Servers:

1. Start the Registry Editor (regedit.exe).
2. Expand the **HKEY_LOCAL_MACHINE, SOFTWARE, ANIXIS, ANIXIS Password Reset, and 2.0** registry keys.
3. Clear the data in the **ServerIP** registry value.
4. Create a REG_SZ value for each Web Interface called ServerIP_PATH where PATH is the last component of the path to APR.DLL (normally the name of the virtual directory).
5. Set each ServerIP_PATH value to the IP address of the APR Server.

Upgrading From APR V2.x

Some planning is needed to ensure a smooth upgrade from APR V2.x. A trial run on a lab network is recommended.

Before You Begin

The database files are not overwritten during an upgrade, but you should still create a backup before upgrading. Follow the instructions in the [Backing up the Database](#) section to backup the database files.

The Web Interface files are overwritten during an upgrade. You must backup any customized Web Interface files before upgrading. The Web Interface files are installed in the \inetpub\wwwroot\pwreset\ folder by default.

A full backup of the APR server(s) is recommended. This allows you to roll back to the previous version if the upgrade cannot be completed.

If APR was originally installed by someone else and you do not have their installation notes, then read the [Installing APR](#) section before you begin. Also make sure you know the password for the APR Server service as you will need it during the upgrade.

Upgrading to V2.1

Start the APR Setup Wizard (APR21.exe) and follow the prompts. The Setup Wizard uninstalls the previous version, so there is no need to manually uninstall it first.

If the APR Server and Web Interface are installed on different servers, then upgrade all servers before using the new version. The APR Server and Web Interface are only tested with matching versions.

Restore any customized Web Interface files after upgrading. Do not restore APR.dll from the backup as it belongs to the previous version.

You may need to restart Windows after upgrading.

Upgrading From APR V1.x

As this is a major upgrade with many changes, some planning is needed to ensure a smooth upgrade. A trial run on a lab network is recommended, especially if you will [customize the user interface](#).

The APREnroll and APRDump utilities from APR V1.x are incompatible with APR V2.1. If you have scripts that rely on these utilities, then send an e-mail to support@anixis.com before upgrading.

Before You Begin

1. Backup the APR V1.x server(s).
2. Take screenshots of all settings in the APR Configuration Program.
3. Close the APR Configuration Program.
4. Stop the “ANIXIS Password Reset” service and backup APRSVC.DAT.

Upgrading to V2.1

1. Follow the steps in the [Installing APR](#) section. If the Web Interface is on a different server, then upgrade it as well.
2. Open [https://\[server\]/pwreset/](https://[server]/pwreset/) in a web browser and check that APR can enroll users and reset passwords. APR’s database will be empty as the data from V1.x has not been imported yet.
3. Open the [Configuration Console](#) and configure APR.
4. Install your new [license key](#).

Importing the V1.x Data

1. If you installed the APR Server into a different folder to the previous version, then copy the APR V1.x data store (APRSVC.DAT) into the APR V2.1 installation folder. The APR Server is installed into the \Program Files [(x86)]\ANIXIS Password Reset\ folder by default.
2. Extract the files from <http://www.anixis.com/ftp/apr/APRImport2.zip> into the APR installation folder. The files in this folder should now include APRImport.exe, APRImport.dll, APRSVC.DAT, and apr.sdf.
3. Run APRImport.exe from a command prompt.
4. Open APRImport.log with Notepad and check it for errors.

APR V2.1 hashes user answers with the SHA-256 algorithm, but imported records are hashed with the SHA-1 algorithm from APR V1.x. If maximum security is required, then phase out the V1.x enrollments by asking users with imported records to re-enroll after upgrading. You can use the [Filter Editor](#) in the Data Console to search for V1.x records.

Other Tasks

1. Update the [backup script](#) to backup the new database files.
2. If you are using the [Password Reset Client](#) and it is configured to take users directly to the Reset page, then update the **Start address** and **Restricted path** settings in the [PRC Configuration](#). The new URL format is: `https://[server]/pwreset/apr.dll?cmd=reset`
3. Set up an account with [delegated permissions](#) for the APR Server.
4. Delete APR.LIC, APRSVC.DAT, APRSVC.BAK (if it exists), APRImport.exe, APRImport.dll, and APRImport.log from the installation folder. Keep a backup copy of APRSVC.DAT elsewhere.
5. If Password Policy Enforcer integration was enabled in APR V1.x, and the Web Interface is in a DMZ, then the DMZ firewall will have a rule to allow connections from the web server to a domain controller on UDP port 1333. Delete this rule as it is no longer needed.

Using APR

ANIXIS Password Reset is a web application. Users access it from their web browser, and from the [Password Reset Client](#). The default URL for the Web Interface is:

`http://[server]/pwreset/`

Where [server] is the name or IP address of the server hosting the Web Interface.



Users access the [Enroll](#), [Reset](#), [Unlock](#), and [Change](#) features from the menu. These features are explained in the following pages.

ANIXIS Password Reset encrypts the connection between the Web Interface and APR Server, but the web server is responsible for encrypting the connection between itself and the user's web browser. You should [install an SSL certificate](#) on the web server and use the HTTPS protocol if APR will be used on an unencrypted network.

Enroll

Users must enroll into APR before they can use it to reset their password or unlock their account. Users only need to enroll once, but they can enroll again if they are [locked out](#) of APR, or if they want to change their questions or answers. To enroll into APR:

1. Click the **Enroll** item in the menu.

Enroll

Enter your username, domain and password to confirm your identity. You cannot enroll if you have forgotten your password, or if your account is locked.

Select some questions and enter your answers to these questions. Try to choose questions that only you know the answers to. You will need to enter the same answers whenever you need to reset your password or unlock your account.

Username:

Domain:

Password:

Question 1:

Answer:

Question 2:

Answer:

Question 3:

Answer:

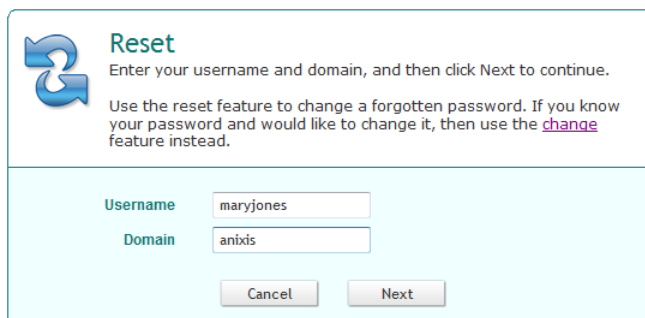
2. Type a **Username**, **Domain**, and **Password**.
3. Type an e-mail address if the **E-mail** text box is [visible](#).
4. Select a question from each of the **Question** drop-down lists, and type an answer to each question in the **Answer** text boxes.
5. Click **Next**.

Windows increments the bad password count in Active Directory every time a user tries to enroll with an incorrect password. This may trigger a lockout if the Windows account lockout policy is enabled.

Reset

Users should use the Reset feature if they have forgotten their password. Resetting a password also unlocks the account if it is locked.

1. Click the **Reset** item in the menu.



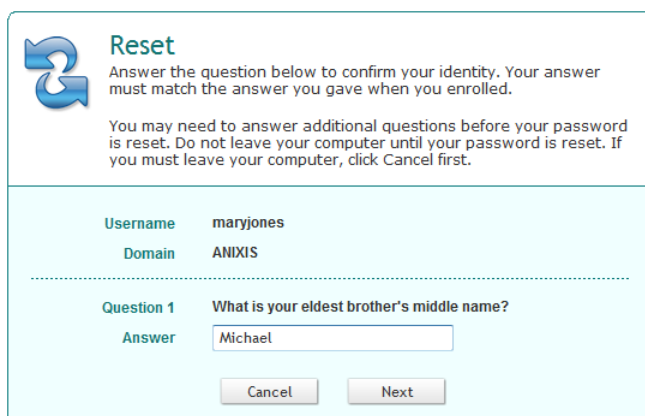
Reset
Enter your username and domain, and then click Next to continue.

Use the reset feature to change a forgotten password. If you know your password and would like to change it, then use the [change](#) feature instead.

Username

Domain

2. Type a **Username** and **Domain**, and then click **Next**.



Reset
Answer the question below to confirm your identity. Your answer must match the answer you gave when you enrolled.

You may need to answer additional questions before your password is reset. Do not leave your computer until your password is reset. If you must leave your computer, click Cancel first.

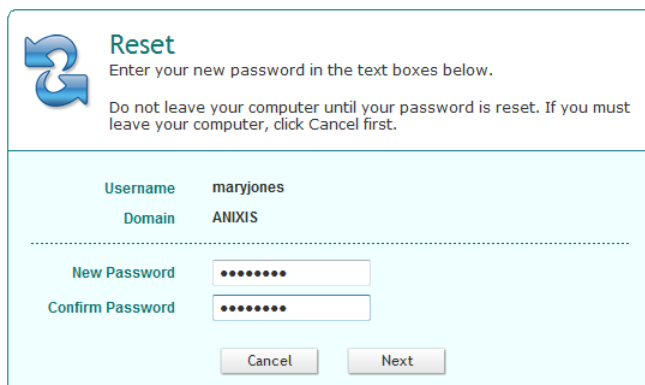
Username

Domain

Question 1

Answer

3. Type the **Answer** to the first question, and then click **Next**. Repeat until all questions are answered correctly.



Reset
Enter your new password in the text boxes below.

Do not leave your computer until your password is reset. If you must leave your computer, click Cancel first.

Username

Domain

New Password

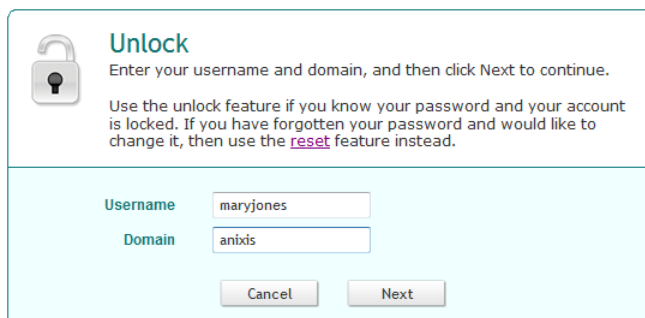
Confirm Password

4. Type the new **Password** into both text boxes, and then click **Next**.

Unlock

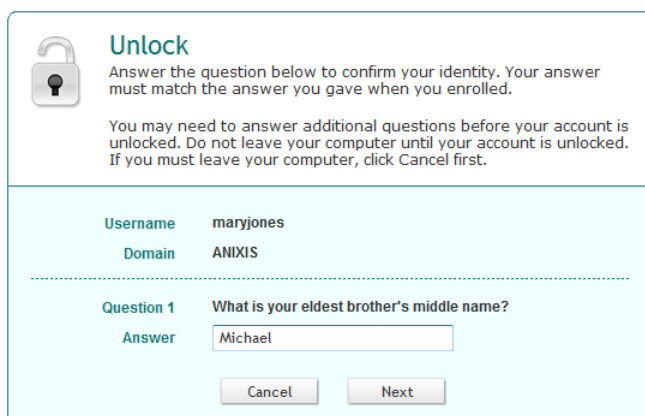
Users should use the Unlock feature if they know their password, but have entered it incorrectly too many times and locked out their account.

1. Click the **Unlock** item in the menu.



The screenshot shows a light blue 'Unlock' form. At the top left is a padlock icon. The title 'Unlock' is in bold. Below the title is the instruction: 'Enter your username and domain, and then click Next to continue.' A second instruction reads: 'Use the unlock feature if you know your password and your account is locked. If you have forgotten your password and would like to change it, then use the [reset](#) feature instead.' Below this are two input fields: 'Username' with the value 'maryjones' and 'Domain' with the value 'anixis'. At the bottom are 'Cancel' and 'Next' buttons.

2. Type a **Username** and **Domain**, and then click **Next**.



The screenshot shows the same 'Unlock' form, but now with the 'Next' button disabled. The 'Username' field is now 'maryjones' and the 'Domain' is 'ANIXIS'. A horizontal dashed line separates this from the next section. Below the line, 'Question 1' is 'What is your eldest brother's middle name?'. The 'Answer' field contains '.Michael'. 'Cancel' and 'Next' buttons are at the bottom.

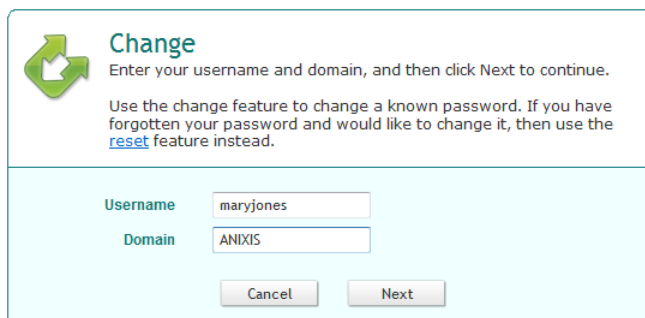
3. Type the **Answer** to the first question, and then click **Next**. Repeat until all questions are answered correctly.

The Unlock feature unlocks accounts in Active Directory. Users who are [locked out](#) of APR should [re-enroll](#) to gain access to APR.

Change

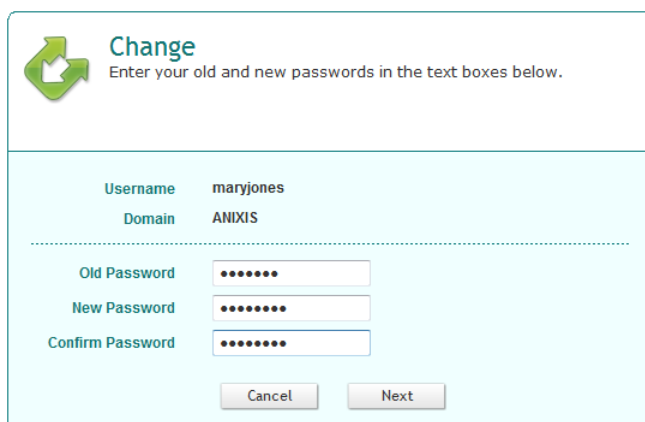
Users should use the Change feature if they know their password and would like to change it.

1. Click the **Change** item in the menu.



The screenshot shows a light blue box with a green circular arrow icon on the left. The title is "Change" in blue. Below the title, there is a sub-header "Change" and a paragraph: "Enter your username and domain, and then click Next to continue. Use the change feature to change a known password. If you have forgotten your password and would like to change it, then use the [reset](#) feature instead." Below this text are two input fields: "Username" with the value "maryjones" and "Domain" with the value "ANIXIS". At the bottom are two buttons: "Cancel" and "Next".

2. Type a **Username** and **Domain**, and then click **Next**.



The screenshot shows the same light blue box with the green circular arrow icon. The title is "Change" in blue. Below the title, there is a sub-header "Change" and a paragraph: "Enter your old and new passwords in the text boxes below." Below this text, the "Username" and "Domain" fields are pre-filled with "maryjones" and "ANIXIS" respectively. Below these fields is a horizontal dashed line. Under the dashed line are three password input fields: "Old Password", "New Password", and "Confirm Password", each containing seven dots. At the bottom are two buttons: "Cancel" and "Next".

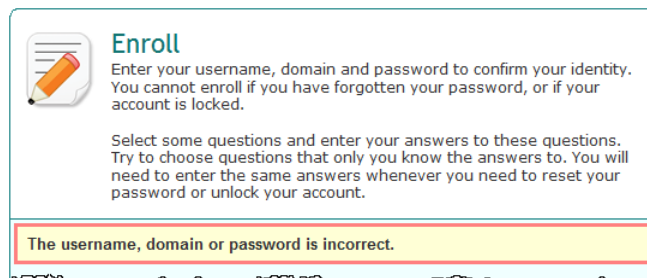
3. Type the **Old Password**, **New Password**, and **Confirm Password**, and then click **Next**.

You can send users a URL that takes them directly to the Enroll, Reset, Unlock, or Change page. The URL can also include the username and/or domain so users won't have to type them. For example:

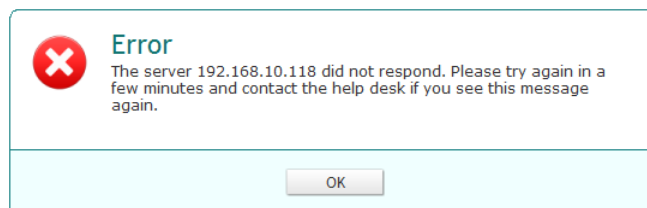
```
https://[server]/pwreset/apr.dll?cmd=enroll&username=maryjones&domain=ANIXIS
```

Error Messages

Validation messages are shown in a yellow box below the page instructions. Validation errors are normally caused by invalid user input. They can often be overcome by changing the value of one or more input fields and resubmitting the form.



Critical errors are shown on their own page. These errors are mostly a result of configuration or system errors. An event may be written to the Application event log on the APR Server computer when a critical error occurs. Users can sometimes overcome a critical error by following the instructions in the error message, but most critical errors are beyond the user's control.



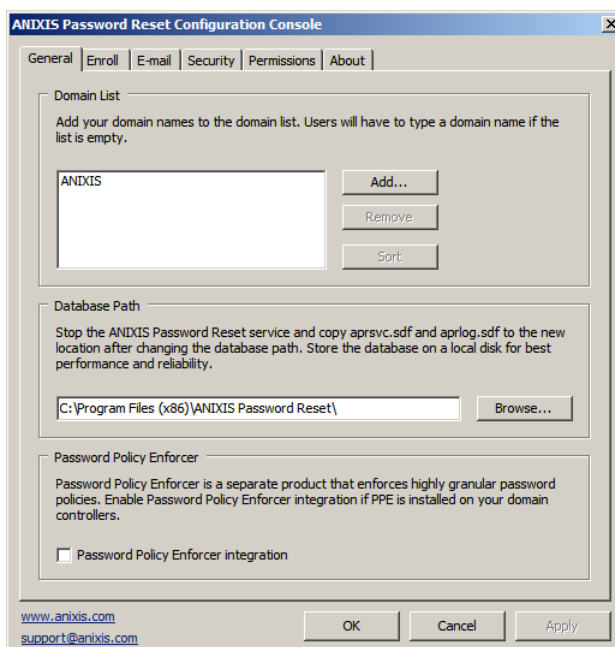
Validation and critical error messages are stored in the HTML templates. You can modify the default messages by [editing the templates](#).

Configuring APR

The APR Configuration Console is installed with the APR Server. Click **Start > [All] Programs > ANIXIS Password Reset > APR Configuration Console** to open the console.

General Tab

Use the **General** tab to maintain the list of managed domains, set the database path, and enable [Password Policy Enforcer](#) integration.



Domain List

When APR is first installed, the Domain List is empty and users must type their domain name. You can configure APR to display a list of domains instead of an empty text box. To add a domain to the list:

1. Click **Add...**
2. Type a NetBIOS (NT Compatible) or DNS domain name.
3. Click **OK**, and then click **Apply**.

The most frequently used domain should be first in the list as it will be the default. You can rearrange the domains by dragging them to another position. You can also click **Sort** to sort them alphabetically.

To remove a domain from the list:

1. Select the domain name in the Domain List.
2. Click **Remove**, and then click **Yes** when asked to confirm.
3. Click **Apply**.

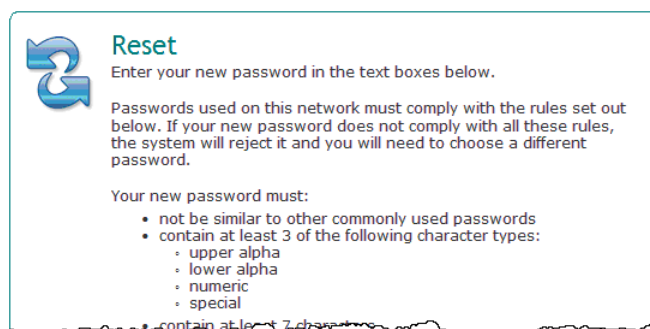
Database Path

The APR Server creates two database files (apr.sdf and aprlog.sdf) in the APR installation folder. To move these files to another folder:

1. Stop the “ANIXIS Password Reset” service.
2. Move apr.sdf and aprlog.sdf from the current **Database Path** to their new location. The database files should remain on a local disk.
3. Give the APR service account read and write permissions to the database files in their new location.
4. Click **Browse...** in the APR Configuration Console.
5. Select the new database path, and then click **OK** and **Apply**.
6. Start the “ANIXIS Password Reset” service.

Password Policy Enforcer

Password Policy Enforcer is a configurable password filter that enforces granular password policies with many advanced features. ANIXIS Password Reset can integrate with Password Policy Enforcer to help users choose a compliant password.

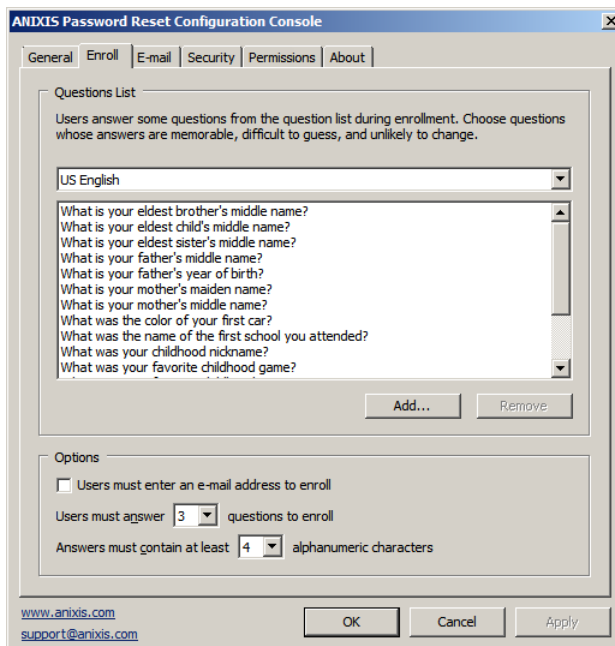


APR displays the PPE password policy message when a user is prompted for their new password, and the PPE rejection message if the new password does not comply with the password policy. Select the **Password Policy Enforcer integration** check box if you have installed and configured Password Policy Enforcer on your domain controllers.

An APR license does not include a Password Policy Enforcer license. Go to www.anixis.com/products/ppe/ to learn more about PPE.

Enroll Tab

Use the **Enroll** tab to maintain the list of enrollment questions and to configure the enrollment options.



Question List

Users must answer some questions about themselves when they enroll into APR. They choose their questions from the Question List. To add a question to the list:

1. Select a language from the drop-down list above the Question List.
2. Click **Add...**
3. Type the new question, including the question mark.
4. Click **OK**, and then click **Apply**.

To remove a question from the list:

1. Select a language from the drop-down list above the Question List.
2. Select the question in the Question List.
3. Click **Remove**, and then click **Yes** when asked to confirm.
4. Click **Apply**.

You can rearrange questions by dragging them to another position. You can also [replace some of the question lists](#) on the Enroll page with text boxes so users can enter their own questions during enrollment.

Options

ANIXIS Password Reset can send [e-mail alerts](#) to users when a request is submitted for their account. These alerts can be sent to the user's Active Directory e-mail address and/or to an e-mail address in APR's database. Select the **Users must enter an e-mail address to enroll** check box if users should enter an e-mail address during enrollment.

The number of questions that users must answer to enroll is configurable, and is set to three by default. Select the desired number of questions from the **Users must answer...** drop-down list.

You can also set a minimum length for each answer. Only alphanumeric characters are counted because APR only checks alphanumeric characters. Select the minimum number of alphanumeric characters in each answer from the **Answers must contain at least...** drop-down list.

E-mail Tab

Use the **E-mail** tab to configure how e-mail is sent to users, when it is sent, and also to edit the e-mail templates.

The screenshot shows the 'ANIXIS Password Reset Configuration Console' with the 'E-mail' tab selected. The 'E-mail Delivery' section has three radio button options: 'Disable e-mail alerts' (unselected), 'Send e-mail to an SMTP server' (selected), and 'Save e-mail to a pickup folder' (unselected). Under 'Send e-mail to an SMTP server', the 'Server' text box contains 'smtp1.anixis.net' and the 'Port' text box contains '25'. Under 'Save e-mail to a pickup folder', there is an empty 'Path' text box and a 'Browse...' button. The 'Triggers' section has a heading and a description, followed by a grid of checkboxes for 'Enroll', 'Unlock', 'Reset', and 'Change' events. The 'Enroll' section has 'Incorrect password' and 'After enroll' (both unselected). The 'Unlock' section has 'Incorrect answer' and 'After unlock' (both selected). The 'Reset' section has 'Incorrect answer' and 'After reset' (both selected). The 'Change' section has 'Incorrect password' and 'After change' (both unselected). At the bottom, there are 'OK', 'Cancel', and 'Apply' buttons, and contact information for 'www.anixis.com' and 'support@anixis.com'.

E-mail Delivery

APR can deliver e-mail alerts directly to an SMTP server, or save them to a pickup folder. Select the **Send e-mail to an SMTP server** option if APR should send e-mails directly to an SMTP server. Type the name or IP address of an SMTP server in the **Server** text box, and the SMTP port number in the **Port** text box.

Select the **Save e-mail to a pickup folder** option if APR should save e-mails to a folder for delivery by a mail server. Click **Browse...** to select a folder. The mail server must monitor this folder for new e-mail.

Saving e-mail to a pickup folder is the fastest and most reliable delivery method. Use this option if your mail server supports pickup folders.

Triggers

Triggers define when e-mail alerts are sent. If the trigger for an event is enabled, then APR sends an e-mail whenever the event occurs. Enabled triggers are shown in blue and underlined. Click the name of an enabled trigger to edit the trigger's e-mail template.

Type the name and e-mail address you wish to appear in the e-mail's **From** field in the **From** text box. The correct format is "Display Name" <mailbox@domain.com>

Type the recipient's e-mail address in the **To** text box. The correct format is "Display Name" <mailbox@domain.com>. Separate multiple recipients with a semicolon. You can also use these macros.

Macro	Replaced with
[AD_EMAIL]	The e-mail address in Active Directory
[APR_EMAIL]	The e-mail address in APR's database
[AD_OR_APR_EMAIL]	The e-mail address in AD, or the e-mail address in APR if the AD address is blank
[APR_OR_AD_EMAIL]	The e-mail address in APR, or the e-mail address in AD if the APR address is blank

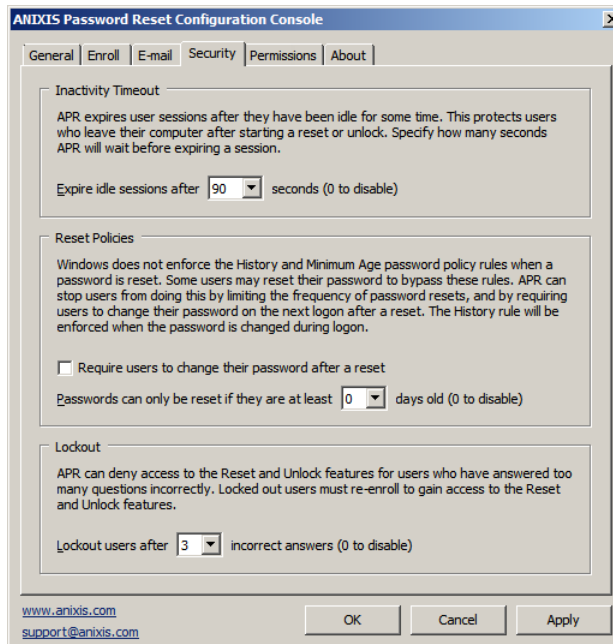
Use [APR_OR_AD_EMAIL] with caution as APR does not check the validity of e-mail addresses. If the e-mail address in APR's database is no longer valid and an alert is sent to [APR_OR_AD_EMAIL], then the alert is only sent to the invalid address.

Type the e-mail's Subject in the **Subject** text box.

Type the body of the e-mail in the large text box. The e-mail is sent as plain text unless the body includes the <html> tag. If sending e-mail as HTML, you must include the complete HTML document starting with <html> and ending with </html>.

Security Tab

Use the **Security** tab to configure the inactivity timeout, password reset policies, and the lockout threshold.



Inactivity Timeout

Users should remain at their computer while resetting their password or unlocking their account. Their account could be compromised if they leave their computer after answering the first question. APR protects user accounts by expiring sessions if users take too long to respond. Select the inactivity timeout from the **Expire idle sessions after...** drop-down list. Set it to 0 seconds to disable the inactivity timeout.

Reset Policies

APR can set the “User must change password at next logon” flag in Active Directory after users reset their password. This is useful if you are using the Windows password history rule as Windows does not enforce this rule during a password reset.

Select the **Require users to change their password after a reset** check box to enable this feature. Users will have to comply with the Windows history rule when they change their password during their next logon. Users whose passwords are set to never expire in Active Directory will not be forced to change their password during logon.

The [Password Policy Enforcer](#) History rule is enforced for password resets if the **Do not check admin/helpdesk password resets** check box is not selected in the PPS properties page, and if the **Enforce this rule when a password is reset** check box is selected in the History rule's properties page.

Windows and PPE do not enforce their minimum age rules during a password reset. If a user resets their password several times in quick succession, they could bypass the password history rule by “pushing” their old password off the end of the history list. Select a value from the **Passwords can only be reset if they are at least...** drop-down list to stop users from doing this. Set it to 0 days to disable this feature.

Lockout

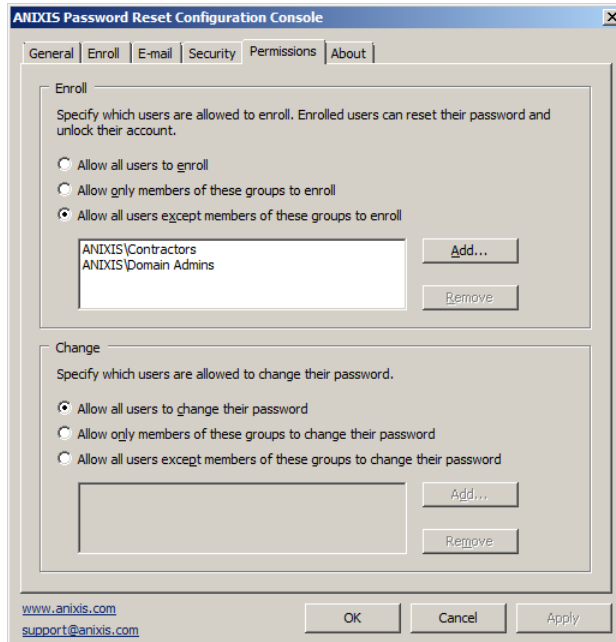
APR's lockout should not be confused with the Windows lockout policy. A Windows lockout stops users from logging on, whereas an APR lockout stops users from resetting their password and unlocking their account. Windows locks out users when they enter too many incorrect passwords. APR locks out users when they enter too many incorrect answers.

Select a value from the **Lockout user after...** drop-down list to specify how many incorrect answers APR will accept before locking out a user. Set it to 0 incorrect answers to disable the lockout feature.

Locked out users must re-enroll before they can use APR to reset their password or unlock their account. The incorrect answer count is reset when a user enrolls, or answers all questions during a reset or unlock.

Permissions Tab

Use the **Permissions** tab to control which users can enroll and change their password.



Enroll

Select the **Allow all users to enroll** option if all users are permitted to enroll. Only enrolled users can reset passwords and unlock accounts.

Select the **Allow only members of these groups to enroll** option if users are permitted to enroll only if they belong to a specified group. Click **Add...** to choose which groups are permitted to enroll.

Select the **Allow all users except members of these groups to enroll** option if users are permitted to enroll unless they belong to a specified group. Click **Add...** to choose which groups are not permitted to enroll.

To remove a group from the list, select it and then click **Remove**.

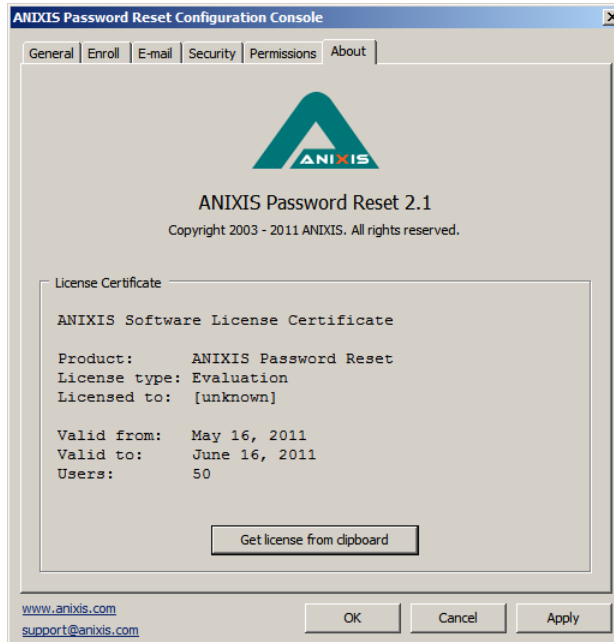
An enrolled user can continue to reset their password and unlock their account even if they are no longer permitted to enroll.

Change

These settings specify which users can change their password. Users do not have to enroll to change their password with APR.

About Tab

Use the **About** tab to check the version and license information, and to install a new license key.



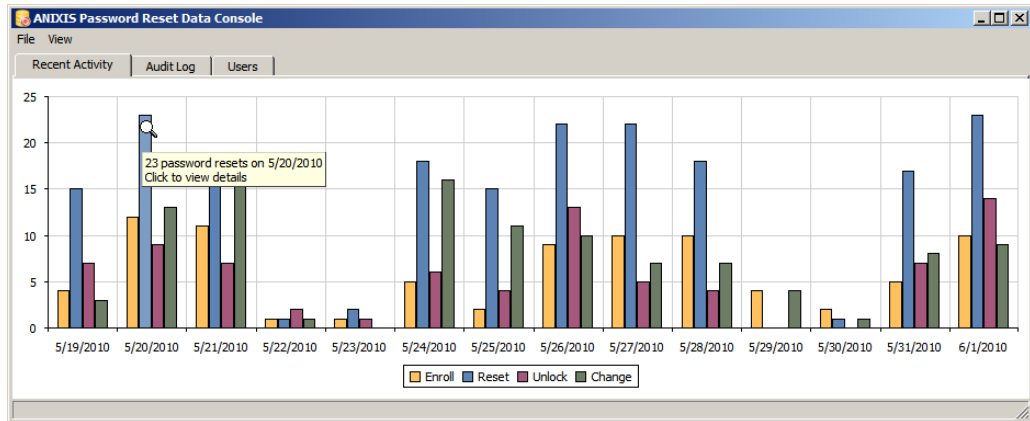
The **About** tab contains version and license key information. To install a new license key, copy the entire license e-mail to the clipboard, and then click **Get license from clipboard**.

ANIXIS Password Reset includes a 30-day evaluation license for up to 50 users. Send an e-mail to support@anixis.com if you would like to evaluate APR with more than 50 users.

Using the Data Console

The Data Console allows you to view and [export](#) data collected by APR. Click **Start > [All] Programs > ANIXIS Password Reset > APR Data Console** to open the console.

The Data Console has three tabs. The **Recent Activity** tab shows a chart of recent requests. The chart is empty when APR is first installed, but it will populate itself as the system is used.



The bars in the chart show how many successful enrollments, resets, unlocks, and changes occurred every day. You can click the bars to see a filtered view of the events for that day. For example, you could click the blue bar on 5/20/2010 to see all the password resets for that day.

The Audit Log tab displays a list of events. The following table shows the 23 successful password resets on 5/20/2010.

Type	Date	Time	Source	User	Domain	Event	Source IP	Source User
Success	5/20/2010	08:12:44 PM	Reset	rgalloway	ANIXIS	Password reset	192.168.118.147	
Success	5/20/2010	06:43:38 PM	Reset	emoore	ANIXIS	Password reset	192.168.109.185	
Success	5/20/2010	05:13:06 PM	Reset	ahendrix	ANIXIS	Password reset	192.168.119.66	
Success	5/20/2010	02:35:12 PM	Reset	jdavenport	ANIXIS	Password reset	192.168.115.110	
Success	5/20/2010	01:38:19 PM	Reset	kharvey	ANIXIS	Password reset	192.168.119.230	
Success	5/20/2010	01:03:07 PM	Reset	rmacias	ANIXIS	Password reset	192.168.109.231	
Success	5/20/2010	11:13:54 AM	Reset	mirwin	ANIXIS	Password reset	192.168.105.98	
Success	5/20/2010	10:55:22 AM	Reset	zstone	ANIXIS	Password reset	192.168.115.58	
Success	5/20/2010	10:08:05 AM	Reset	dtucker	ANIXIS	Password reset	192.168.116.150	
Success	5/20/2010	10:07:20 AM	Reset	abowers	ANIXIS	Password reset	192.168.113.16	
Success	5/20/2010	09:32:18 AM	Reset	rfarrell	ANIXIS	Password reset	192.168.117.69	
Success	5/20/2010	09:16:46 AM	Reset	amcmillan	ANIXIS	Password reset	192.168.109.237	

Showing 23 of 1,314 records

The resulting view shows only the 23 successful password resets on 5/20/2010. These are shown in the **Audit Log** tab. You can create your own [filters](#) to find events in this tab.

The **Audit Log** tab has nine columns. You can drag a column's header to rearrange the columns, or click a column header to sort the records.

Column	Information
Type	Event type (Success or Failure)
Date	Event date
Time	Event time
Source	Event source (Reset, Unlock, etc.)
User	User's Active Directory username
Domain	User's Active Directory domain
Event	A description of the event
Source IP	The request's source IP address
Source User	The request's source username (blank if anonymous access is enabled)

The **Users** tab contains information about each user. All users are shown by default, but you can create [filters](#) to find specific users.

User	Domain	E-mail	Last Enroll	Last Reset	Last Unlock	Last Change
abooker	ANIXIS	abooker@anixis.net	4/15/2010 9:15:32 AM		5/9/2010 9:00:14 AM	
abowers	ANIXIS	abowers@anixis.net	3/22/2010 12:47:18 PM	5/20/2010 10:07:20 AM		
adaugherty	ANIXIS	adaugherty@anixis.net	5/24/2010 8:59:19 AM	5/30/2010 9:12:48 AM		
adavidson	ANIXIS	adavidson@anixis.net	5/18/2010 3:26:53 PM			
aguerrero	ANIXIS	aguerrero@anixis.net				5/30/2010 4:12:11 PM
aharper	ANIXIS	aharper@anixis.net	3/30/2010 1:44:28 PM	4/16/2010 2:26:13 PM	5/23/2010 6:48:04 PM	
ahendrix	ANIXIS	ahendrix@anixis.net	4/17/2010 10:10:48 AM	5/20/2010 5:13:06 PM		
aholmes	ANIXIS	aholmes@anixis.net	5/14/2010 9:41:32 AM			
ajenkins	ANIXIS	ajenkins@anixis.net	4/29/2010 9:01:51 AM			
akauffman	ANIXIS	akauffman@anixis.net	5/10/2010 11:18:54 AM			
akoch	ANIXIS	akoch@anixis.net	4/1/2010 2:39:25 PM	5/30/2010 10:27:18 AM		
alester	ANIXIS	alester@anixis.net	4/19/2010 8:27:11 AM			
alindsey	ANIXIS	alindsey@anixis.net	5/5/2010 11:55:03 AM			4/9/2010 10:19:41 AM

The **Users** tab has seven columns.

Column	Information
User	User's Active Directory username
Domain	User's Active Directory domain
E-mail	E-mail address entered during enrollment
Last Enroll	Date and time of last successful enroll
Last Reset	Date and time of last successful password reset
Last Unlock	Date and time of last successful account unlock
Last Change	Date and time of last successful password change

The Data Console does not automatically display new information as it is added to the database. Press F5 to refresh the view.

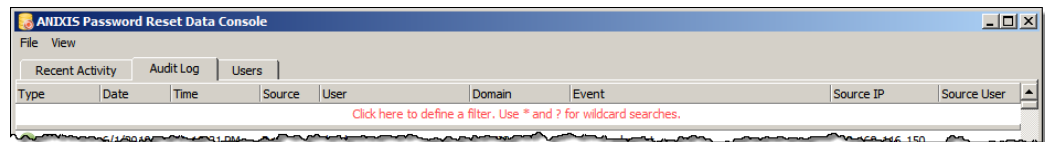
Filtering Data

The Data Console can show thousands of records, but only some of them will be of interest to you at any time. Filters let you hide the unimportant information.

You can create simple filters by typing values directly into the [Filter Row](#), or by selecting values from [column headers](#). More complex filters are created with the [Custom Filter](#) and [Filter Editor](#) windows.

The Filter Row

The top row in the **Audit Log** and **Users** tabs is called the Filter Row. You can type filter values directly into this row.



The Filter Row is empty when you first open the Data Console. To create a filter, click the Filter Row in the column you wish to filter. A cursor will appear. Type a value, and then press ENTER or TAB.

You may see a button to the right of the cursor. Click the button to show an editor or selector that will help you enter a value. Values can include the ? and * wildcard characters. Use a ? to match any single character, or a * to match more than one character.

Type	Date	Time	Source	User	Domain	Event	Source IP	Source User
	5/20/2010		Reset				192.168.115.*	
Success	5/20/2010	02:35:12 PM	Reset	jdavenport	ANIXIS	Password reset	192.168.115.110	
Success	5/20/2010	10:55:22 AM	Reset	zstone	ANIXIS	Password reset	192.168.115.58	

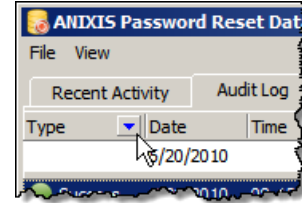
The image above shows a filter on the Date, Source, and Source IP columns. Only password reset events on 5/20/2010 originating from IP addresses starting with 192.168.115 will be shown.

Rows are shown only if they match all filter values (logical AND). Use the [Custom Filter](#) or the [Filter Editor](#) windows for a logical OR filter.

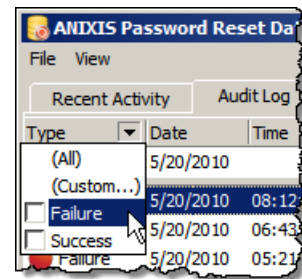
Filtering by Column Values

You can also create a filter by selecting values from a list in each column's header.

Hover the mouse pointer over a column header until a small button appears.



Click the button to show a list of visible values in the column.

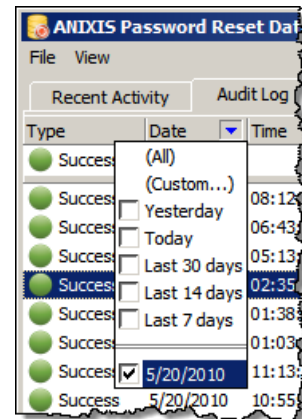


Select one or more values from the list. Rows that do not match one of the selected values are hidden.

The list of values for date and date/time columns also includes date ranges such as **Last 7 days**, **Today**, **Yesterday**, etc.

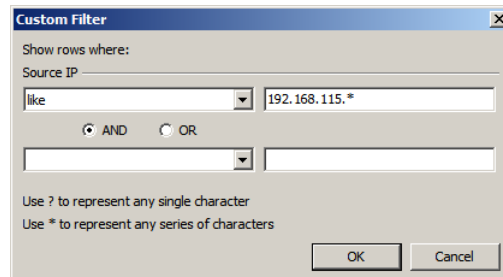
Click **(All)** to clear the filter and display all values for the column.

Click **(Custom...)** to create a [custom filter](#) for the column.



Custom Filters

Use custom filters to search for partial matches, find a range of values, or to create more complex filters. Click **(Custom...)** in a column header's value list to create a custom filter.



Custom filters can contain one or two conditions for each column. Select an operator for the first condition from the drop-down list below the column name. Only relevant operators are shown for each column.

Type a value for the condition in the text box beside the operator. The text box may have a button on the right. Click the button to show an editor or selector that will help you enter a value. Values can include the ? and * wildcard characters. Use a ? to match any single character, or a * to match more than one character.

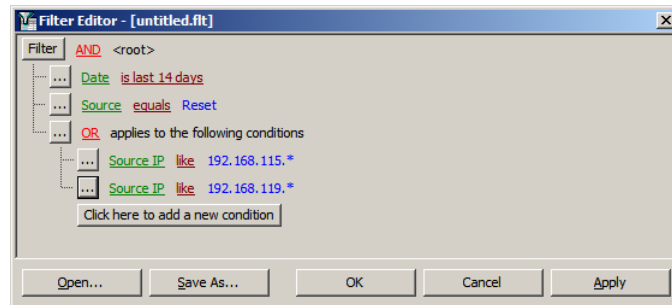
Select the **AND** or **OR** operator if the filter will have two conditions. Select **AND** if the filter should only show rows that meet both conditions. Select **OR** if the filter should show rows that meet either condition.

Select an operator and value for the second condition, or leave them blank if your filter only has one condition. Click **OK** to close the Custom Filter window and apply the filter.

The [Filter Editor](#) is shown instead of the Custom Filter window if the current filter is too complex for the Custom Filter window.

The Filter Editor

Use the Filter Editor to create complex filters, filters for hidden columns, or to save and open regularly used filters. Press CTRL + F to open the Filter Editor, or click the **Filter Editor** button in the lower right corner of the Data Console.



A filter may contain several conditions. Conditions start with a column name, followed by an operator, and sometimes a value. Column names are shown in green, operators in maroon, and values in blue.

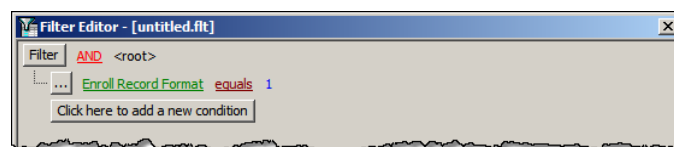
A filter also contains a root node and optionally one or more groups. These are used to include Boolean operators in the filter. Boolean operators are shown in red. Grouped conditions are indented.

The filter in the image above contains the root node, one group, and four conditions. It will show all reset requests in the last fourteen days originating from IP addresses starting with 192.168.115 or 192.168.119.

Click the **Click here to add a new condition** button to add a new condition to the filter. Click the button to the left of each line to add or remove conditions and groups. Click column names, operators, and values to edit them. Most can be selected from a list. Values can also contain the ? and * wildcard characters.

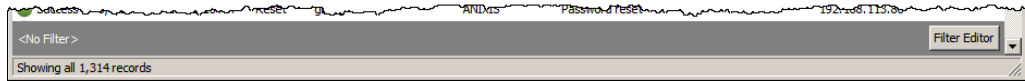
Click **Save As...** to save a filter to a file, or **Open...** to use a saved filter. Click **OK** to close the Filter Editor and apply the filter.

Some columns are hidden in the Data Console. You can use the Filter Editor to create filters for these columns. For example, the filter in the image below shows all users with an APR v1 enrollment record.



The Filter and Status Bars

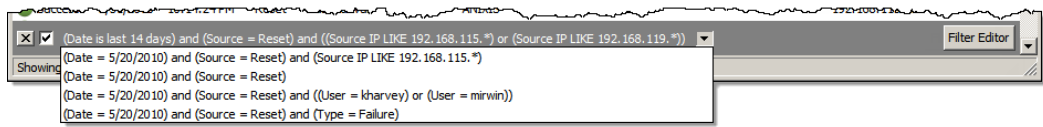
The Status Bar appears at the very bottom of the Data Console. It shows the number of visible records and the total record count. The Filter Bar appears above the Status Bar, and it shows the active filter. The button on the right side of the Filter Bar opens the [Filter Editor](#).



A button and a check box appear on the left side of the Filter Bar when a filter is active. Click the button to clear the filter. Toggle the check box to disable or enable the filter.



Another button appears to the right of the filter. Click this button to select a recently used filter.



Exporting Data

You can export the visible rows to Microsoft Excel, HTML, and text formats. To export the visible rows:

1. Click the **Audit Log** or **Users** tab.
2. Click **File | Export to Excel**, **Export to HTML**, or **Export to Text**.
3. Type a filename, and then click **Save**.

Deleting Users

To delete a user from the Data Console:

1. Click the **Users** tab.
2. Select the user(s) you wish to delete.
3. Press the DELETE key, and then click **OK**.

Deleting a user does not delete the user's events in the Audit Log.

Backing up the Database

The ANIXIS Password Reset database should be backed up regularly. The database files are in the APR Server's installation folder by default, but the location is [configurable](#). Ensure that you backup the correct files, otherwise your backup may contain outdated data.

The APR Server service should be stopped, and Data Console closed during the backup. The recommended backup procedure is:

1. Close the Data Console.
2. Stop the "ANIXIS Password Reset" service.
3. Copy the database files to a local or network disk.
4. Start the "ANIXIS Password Reset" service.
5. Copy the database files to another device.

The database files are called apr.sdf and aprlog.sdf. The following commands create copies of these files with a .bak extension. You should copy the .bak files to another device. These commands should be added to a script that runs daily.

```
net stop "ANIXIS Password Reset"

copy /Y "c:\program files\anixis password reset\apr.sdf"
        "c:\program files\anixis password reset\apr.bak"

copy /Y "c:\program files\anixis password reset\aprlog.sdf"
        "c:\program files\anixis password reset\aprlog.bak"

net start "ANIXIS Password Reset"
```

Change the paths above if the APR Server is running on Windows x64, or if it is configured to store the database files in a [different folder](#).

To restore the database files from a backup:

1. Restore apr.bak and aprlog.bak from the backup device.
2. Close the Data Console.
3. Stop the "ANIXIS Password Reset" service.
4. Copy apr.bak over apr.sdf, and aprlog.bak over aprlog.sdf.
5. Start the "ANIXIS Password Reset" service.

apr.sdf contains hashes of the user answers. The hashes are salted and encrypted to protect them from attack, but you should still ensure that this file and all backup copies are stored securely.

Securing APR

APR has many inbuilt security features, but there are some changes you can make to improve security. The most important of these is to install an [SSL certificate](#) for the Web Interface. You can also set up a standard user account with [delegated permissions](#) for the APR Server.

Installing and Using an SSL Certificate

The Web Interface and APR Server always communicate over a secure channel. You do not have to configure the encryption for this connection, but you do need to set up SSL (Secure Sockets Layer) encryption for the connection between the web browser (or [Password Reset Client](#)) and the web server.

Do not use ANIXIS Password Reset on a production network without SSL encryption.

You can use a self-signed certificate with APR, but most organizations purchase certificates from a certificate authority. This is a recurring cost, and you will need to complete forms for the certificate authority to verify your identity. You can install the Web Interface on a server that already has an SSL certificate if you would rather not purchase another one.

The IIS documentation explains how request, install, and use SSL certificates. Refer to the documentation for more information:

Windows 2008: Configuring Server Certificates in IIS 7
[http://technet.microsoft.com/en-us/library/cc732230\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc732230(WS.10).aspx)

Windows 2003: Certificates (IIS 6.0)
<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/89c7ef2f-f7d6-483c-8b08-ae0c6584dd4d.mspx>

Ensure that users only access APR over an encrypted connection after the SSL certificate is installed. The **Start address** and **Restricted path** in the [Password Reset Client configuration](#) should start with https://. Web browsers can be redirected to the secure URL.

Delegating Permissions to the APR Server Service

When the Setup Wizard creates a service account for the APR Server, it adds the account to the Domain Admins group. This allows ANIXIS Password Reset to start working without additional configuration, but it also gives the service excessive permissions. You can improve security by removing the service account from the Domain Admins group and granting only the required permissions.

You can grant Active Directory permissions from the command-line with `dsacls.exe`, or with a graphical user interface. The examples below use the command-line, but you can use either method.

`dsacls.exe` is included with Windows 2008. On Windows 2003, it is installed with the Windows Support Tools. Microsoft article [281146](#) explains how to install and use `dsacls.exe`.

The commands you need to execute are:

```
dsacls "[object]" /I:S /G "[account]":CA;"Reset Password";user
dsacls "[object]" /I:S /G "[account]":RPWP;lockoutTime;user
dsacls "[object]" /I:S /G "[account]":RPWP;pwdLastSet;user
```

Where `[object]` is the distinguished name of the domain or OU containing the user accounts, and `[account]` is the name of the service account in `user@domain` or `domain\user` format.

The first two commands allow APR to reset passwords and unlock accounts on behalf of users. The third command allows APR to set the “User must change password at next logon” flag in Active Directory if the **Require users to change their password after a reset** option is enabled in the Configuration Console’s [Security](#) tab.

For example, the following command grants the `axs\apr` account permission to reset passwords for users in the `axs.net` domain:

```
dsacls "dc=axs,dc=net" /I:S /G "axs\apr":CA;"Reset Password";user
```

Remove the service account from the Domain Admins group and restart the “ANIXIS Password Reset” service after executing these commands.

Using Delegated Permissions with Protected Groups

When you delegate permissions for the APR service account, the delegated permissions are initially applied to all users in the domain or OU. After some time, Windows restores the original permissions for some important user accounts. This stops these users from resetting their password and unlocking their account with APR.

The accounts protected by this feature vary by Windows version, and include members of the Domain Admins, Enterprise Admins, and Schema Admins groups. The list of protected groups is configurable, so it may differ from the defaults in the Windows documentation.

If you are using an APR service account with delegated permissions and do not want these privileged accounts to reset their password or unlock their account with APR, then there is no need to make any configuration changes. Windows automatically restores the original permissions for these accounts. This is done every hour by default.

If you want to allow these users to reset their password and unlock their account with APR, then you need to change the permissions for the AdminSDHolder container. The commands you need to execute are:

```
dscls "[AdminSDHolder]" /G "[account]":CA;"Reset Password"  
dscls "[AdminSDHolder]" /G "[account]":RPWP;lockoutTime  
dscls "[AdminSDHolder]" /G "[account]":RPWP;pwdLastSet
```

Where [AdminSDHolder] is the distinguished name of the AdminSDHolder container, and [account] is the name of the service account in user@domain or domain\user format.

The DN of the AdminSDHolder container for the anixis.net domain is CN=AdminSDHolder,CN=System,DC=anixis,DC=net

Changes to the AdminSDHolder container are not applied to accounts immediately. You may need to wait up to an hour for Windows to update the DACL for these accounts. You can also start the process manually. Search for runProtectAdminGroupsTask or FixUpInheritance in Microsoft's documentation or more information.

Editing the HTML Templates

APR's user interface is built with customizable templates. You can easily modify the user interface by editing the templates.

User Interface Files

APR installs seven .htm files for every language. Each filename starts with a language code. The files for the US English language are:

Filename	Content
en_default.htm	Static HTML for the menu page
en_enroll.htm	Template for the Enroll page
en_reset.htm	Template for the Reset pages
en_unlock.htm	Template for the Unlock pages
en_change.htm	Template for the Change pages
en_finished.htm	Template for the Finished page
en_error.htm	Template for the Critical Error page

The other user interface files are language independent. Most of the formatting is in apr.css, and some additional CSS for Internet Explorer is in apr_ie.css. The image files are in the images folder. These files are installed into the \inetpub\wwwroot\pwreset\ folder by default.

Always backup the user interface files before and after editing them. Your changes may be overwritten when APR is upgraded, and some changes could stop APR from working correctly. Having a backup allows you to quickly revert to a working setup.

en_default.htm contains static HTML, but the other .htm files contain special comment tags that are used to prepare the pages. Some of these comments define ranges. A range looks like this:

```
<!--RANGE_NAME-->Some text or HTML<!--/RANGE_NAME-->
```

The Web Interface deletes ranges (and the text inside them) when they are not needed. Some ranges span only one word, while others span several lines. The other type of comment tag is called a field.

```
<!--USERNAME-->
```

Fields are replaced by some other information. For example, the field above is replaced with a username.

Resource Strings

Each template ends with a resource string section.

```
<!--RESOURCE_STRINGS--><!--
@RES_EMPTY_FIELD_USERNAME:  Enter your username in the Username bo...
@RES_EMPTY_FIELD_DOMAIN:    Enter your domain name in the Domain b...
--><!--/RESOURCE_STRINGS-->
```

Resource strings are mostly [validation error messages](#), but they can contain any text APR may need to build the page. Do not modify the identifiers on the left, only edit the text on the right. Resource strings are always inside a range called RESOURCE_STRINGS. APR deletes this range before sending the page to the user's web browser.

You may rebrand the APR user interface, but it is a violation of the [License Agreement](#) to remove or obscure any copyright notices.

Examples

This section contains examples of common customizations. Use these examples to gain a better understanding of APR's templates. You don't need to be an expert in HTML to follow these examples, but a basic understanding of HTML will help. Work through them carefully, and backup files before you edit them. The examples in this section are from the US English files, but the format is the same for all languages.

Replace the ANIXIS Logo

The ANIXIS logo is shown in the top left corner of the menu page. The logo is installed into the \inetpub\wwwroot\pwreset\images\ folder by default, and it is called logo.gif. You can replace this file with one containing your organization's logo.

Your logo may appear distorted if it is not the same size as the ANIXIS logo. You can fix this by opening en_default.htm in a text editor such as Notepad. Search for the line shown below, and replace the width (116) and height (69) with the dimensions of your logo in pixels.

```

```

Edit Page Instructions

Instructions appear at the top of each page in the white section above the input fields. You can edit these instructions by opening the relevant .htm file and searching for the text you wish to modify.

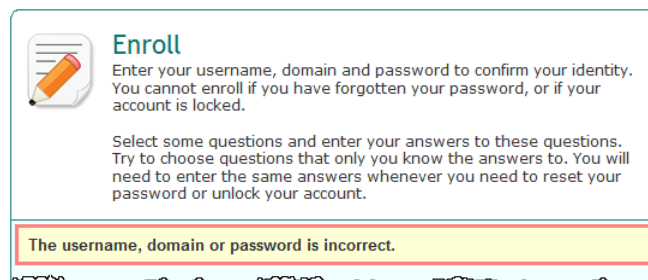
Instructions are sometimes inside a range called SECTION_A, SECTION_B, or SECTION_C. Each section contains instructions for the different pages in the template. Make sure you edit the instructions in the correct section, or they may be displayed on the wrong page.

```
<!--SECTION_A-->
    <p>Enter your username and domain, and then click Next to con...
    <p>Use the reset feature to change a forgotten password. If y...
<!--/SECTION_A-->

<!--SECTION_B-->
    <p>Answer the question below to confirm your identity. Your a...
    <p>You may need to answer additional questions before your pa...
<!--/SECTION_B-->
```

Edit Validation Error Messages

Validation error messages are shown in a yellow box below the page instructions. Validation errors are normally caused by invalid user input.



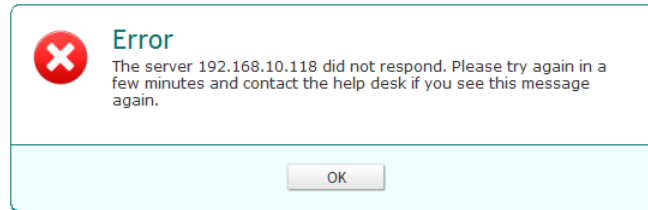
Validation error messages are defined in the relevant template (en_enroll.htm, en_reset.htm, en_unlock.htm, or en_change.htm). The error messages are in the [resource strings](#) section near the end of the file. Some messages are in more than one file, so you may need to edit several files to change all instances of a message.

You may see placeholders like %1 and %2 in some error messages. These are replaced with more information about the error. You should keep these as they provide important information about the error, but you can delete them if you do not want them.

```
@RES_EMPTY_FIELD_EMAIL:      Enter your e-mail address in the E-mail...
@RES_IDENTICAL_QUESTIONS:    Question %1 and %2 are the same. Select...
@RES_IDENTICAL_ANSWERS:      The answers to question %1 and %2 are t...
```

Edit Critical Error Messages

All the critical error messages are defined in `en_error.htm`. The messages are in the [resource strings](#) section near the end of the file.



You may see placeholders like `%1` and `%2` in some error messages. These are replaced with more information about the error. You should keep these as they provide important information about the error, but you can delete them if you do not want them.

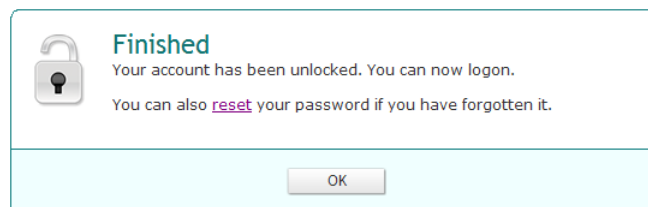
```
@RES_LOCKED_OUT_AD: Your account is locked because an incorrect p...
@RES_NO_RESPONSE: The server %1 did not respond. Please try aga...
@RES_NOT_ENROLLED: You are not enrolled to use this feature. <a ...
```

If you want to display some text for all error messages, then insert your text above or below the “`<p><!--ERROR--></p>`” line. For example:

```
<p><!--ERROR--></p>
<p>The help desk phone number is 555-555-5555.</p>
```

Edit Finished Messages

Finished messages are shown after users successfully complete an enroll, reset, unlock, or change. These messages are defined in the [resource strings](#) section near the end of `en_finished.htm`.



`en_finished.htm` has two resource strings for password changes (`RES_FINISHED_CHANGE` and `RES_FINISHED_CHANGE_INVITE`). The first is shown when a user who has enrolled into APR changes their password. The second is shown when a user who has not enrolled changes their password. The second message invites the user to enroll so they can also use the reset and unlock features in future.

Replace Enroll Question Lists with Text Boxes

When users enroll into APR, they must choose their questions from the [Question List](#). You can replace some or all of the question lists with text boxes so users can enter their own questions.

The lines you need to edit in en_enroll.htm look like this:

```
<select class="question" id="q1" name="q1"><!--QL1--></select>
```

There are ten of these lines in en_enroll.htm, each with their own question number (the number after the “q”). You do not have to edit all ten lines. If users will be allowed to enter two questions, then only edit the q1 and q2 lines. Replace these lines with a line like this:

```
<input class="question" id="q1" name="q1" value="<!--Q1-->"
maxlength="64" />
```

Remember to change the three question numbers on each line so they match the original numbers, otherwise APR will not work correctly. You should also [edit the validation error messages](#) in en_enroll.htm as some of them make reference to “selecting” questions from a list.

Users may not choose appropriate security questions, so it is advisable to leave the question lists for some of the enrollment questions.

Change Font Sizes and Colors

apr.css contains most of the user interface formatting information. You can easily change font sizes and colors by editing this file. You can even reposition and resize items, but you will need some understanding of CSS to do this. For example, this is the CSS for the [validation error](#) box:

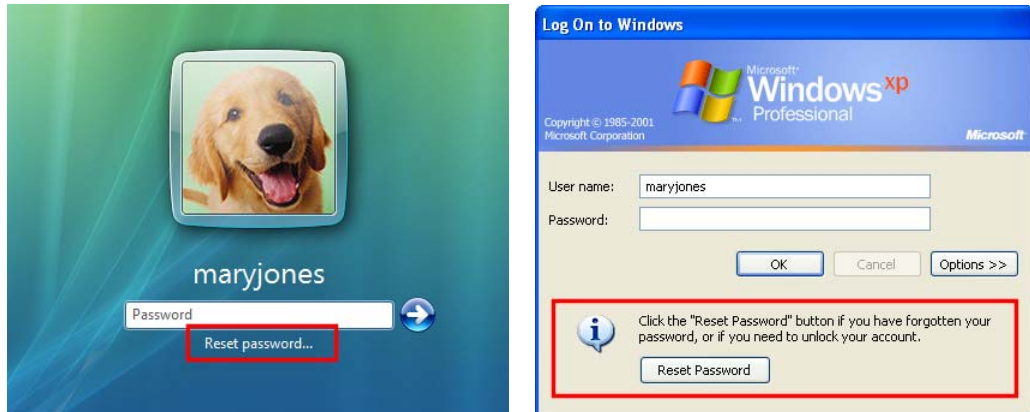
```
.error {
    background-color: #ffffd6;
    border: 3px solid #ff8080;
    color: #333333;
    font: bold 1.3em/1.2em Arial, sans-serif;
    margin: 3px 0 0 4px;
    padding: 6px 22px 6px 8px;
    width: 499px;
}
```

Edit these properties to change the appearance of the error box. You may need to clear your web browser’s cache to see the changes.

Different web browsers render style sheets differently, so test your changes with the most popular browsers to ensure compatibility.

The Password Reset Client

The Password Reset Client allows users to securely reset their password from the Windows Logon and Unlock Computer screens. Users simply click the **Reset Password** button or command link to access the ANIXIS Password Reset system.



The Password Reset Client does not install a new GINA DLL or modify any Windows system files.

Installing the PRC

The Password Reset Client is designed to run on Windows 2000, XP, 2003, Vista, 2008, and 7. The PRC is also compatible with Windows Terminal Services and Remote Desktop Connection on these operating systems.

System Requirements

- Windows 2000, XP, 2003, 2003 R2, Vista, 2008, 2008 R2, or 7 (x86 and x64 editions).
- 1 Megabyte free disk space.
- 128 Kilobytes free RAM (per session if using Terminal Services).

You can install the PRC manually if you only have a few computers, but it is easier to perform an automated installation if you have many computers. Follow the instructions below to perform an automated installation with Group Policy.

Create a Distribution Point

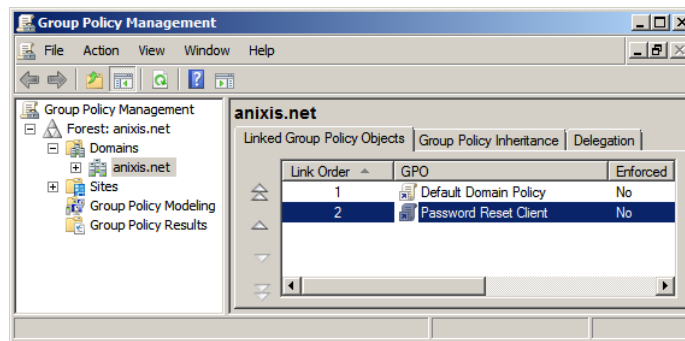
A distribution point can either be a UNC path to a server share, or a DFS (Distributed File System) path. Organizations with large, multi-site networks should use DFS as it offers fault tolerance and load sharing. To create a PRC distribution point:

1. Log on to a server as an administrator.
2. Create a shared network folder to distribute the files from.
3. Give the "Domain Computers" security group read access to the share, and limit write access to authorized personnel only.
4. Copy APRCIt27.msi into the distribution point folder. APRCIt27.msi is in the "Client" folder below the APR Server's installation folder. (\Program Files [(x86)]\ANIXIS Password Reset\ by default).
5. Give the "Domain Computers" security group read access to the APRCIt27.msi file in the distribution point.

Create a Group Policy Object

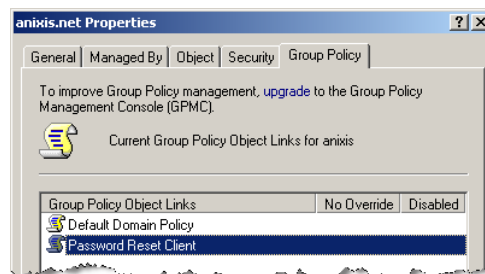
If you are using the Group Policy Management Console:

1. Start the Group Policy Management Console (gpmc.msc).
2. Expand the forest and domain items in the left pane.
3. Right-click the domain root node in the left pane, and then click **Create a GPO in this domain, and Link it here...** or **Create and Link a GPO Here...**
4. Type "Password Reset Client", and then press ENTER.



If you are not using the Group Policy Management Console:

1. Start the Active Directory Users and Computers Console (dsa.msc).
2. Right-click the domain object in the left pane, and then click **Properties**.
3. Click the **Group Policy** tab, and then click **New**.
4. Type "Password Reset Client", and then press ENTER.



Edit the Group Policy Object

1. Right-click the **Password Reset Client** GPO, and then click **Edit**.
2. Expand the **Computer Configuration, Policies** (if visible), and **Software Settings** items.
3. Right-click the **Software installation** item, and then select **New > Package**.
4. Type the full UNC path to APRCIt27.msi in the Open dialog box. You must enter a UNC path so that other computers can access this file over the network. For example,
\\file server\distribution point share\APRCIt27.msi
5. Click **Open**.
6. Select the **Assigned** deployment method, and then click **OK**.
7. Close the Group Policy Object Editor.

Complete the Installation

Restart each computer to complete the installation. Windows installs the Password Reset Client during startup, and then immediately restarts the computer a second time to complete the installation.

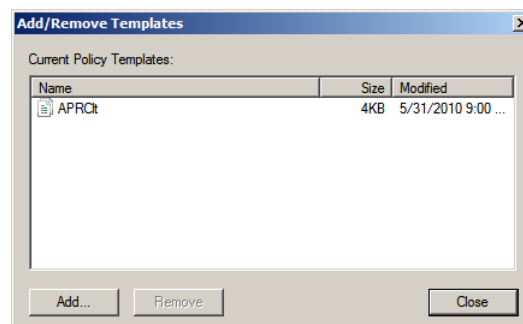


Computers with Fast Logon Optimization enabled may not install the Password Reset Client during the first restart. These computers perform a background refresh of Group Policy, and will install the client on the first restart after the refresh. Microsoft article [305293](#) has more information about the Fast Logon Optimization feature.

Configuring the PRC

You must install an Active Directory administrative template to configure the Password Reset Client. The administrative template only has to be installed once. To install the PRC administrative template:

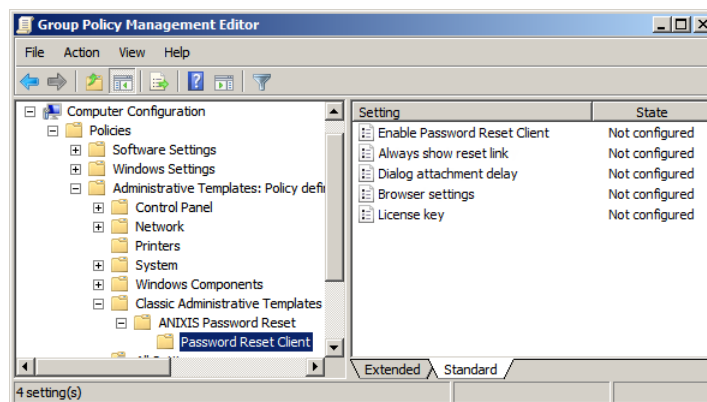
1. Use the Group Policy Management Console, or Active Directory Users and Computers Console to display the GPOs linked at the domain level.
2. Right-click the **Password Reset Client** GPO, and then click **Edit**.
3. Expand the **Computer Configuration** item.
4. Expand the **Policies** item if it is visible.
5. Right-click the **Administrative Templates** item, and then click **Add/Remove Templates...**
6. Click **Add...** and then browse to the “Client” folder below the APR Server’s installation folder.
(\Program Files [(x86)]\ANIXIS Password Reset\ by default).
7. Select APRCIt.adm, and then click **Open**.



8. Click **Close**.

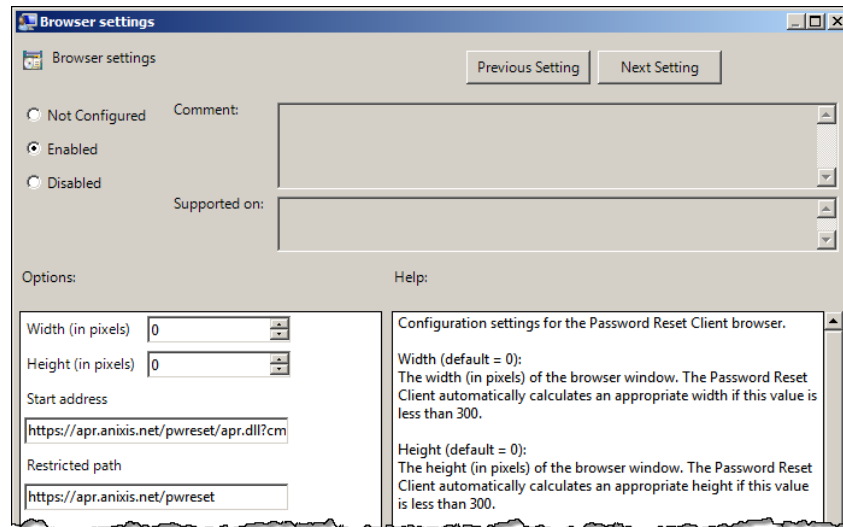
To configure the Password Reset Client:

1. Use the Group Policy Management Console, or Active Directory Users and Computers Console to display the GPOs linked at the domain level.
2. Right-click the **Password Reset Client** GPO, and then click **Edit**.
3. Expand the **Computer Configuration, Policies** (if visible), **Administrative Templates, Classic Administrative Templates** (if visible), **ANIXIS Password Reset**, and **Password Reset Client** items.
4. Double-click the **Browser settings** item in the right pane of the Group Policy Object Editor.



The **Enable Password Reset Client**, **Always show reset link**, and **Dialog attachment delay** are automatically set by the Password Reset Client, and are normally left in their default (Not configured) state.

The administrative template contains detailed information about all the PRC configuration settings. This information is shown on the **Help** panel in recent Windows versions, and on the **Explain** tab in earlier versions. The Help panel and Explain tab are shown after you double-click one of the configuration settings in the right pane.

5. Select the **Enabled** option.

6. Type the desired **Width** and **Height** of the PRC browser window, or set them to 0 to have the PRC calculate an appropriate size.
7. Type the **Start address** (URL) of the ANIXIS Password Reset system. The URL can point to the APR menu, or directly to the reset page. See the **Help** panel or **Explain** tab for more information.
8. Type a **Restricted path** (URL) to stop users from following links to other sites from the Password Reset Client browser.
9. Click **OK**.
10. Close the Group Policy Object Editor.

The new PRC configuration is applied to all computers in the domain. This does not happen immediately, as Windows takes some time to apply the changes to Group Policy. You can force an immediate refresh of Group Policy on the local computer with the following command:

Windows 2000: `secedit /refreshpolicy machine_policy`

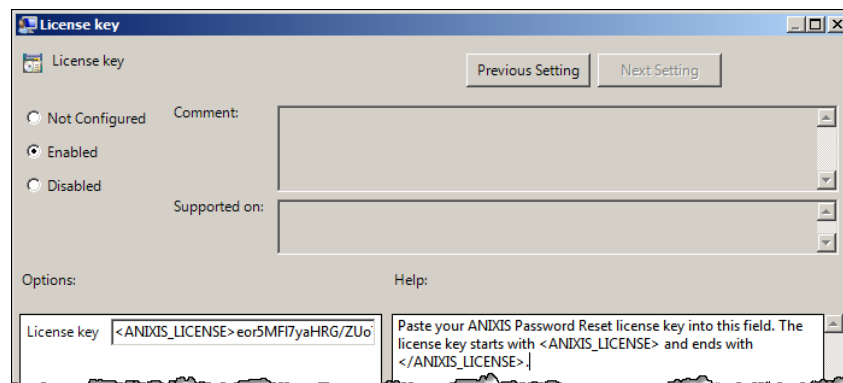
Windows XP and later: `gpupdate /target:computer`

Users may follow links to untrusted sites if the APR user interface or server error pages contain external links. This is a security risk because the Password Reset Client runs under the context of the local system account. Specify a restricted path to stop users from following links to other sites from the Password Reset Client.

Licensing the PRC

To add a license key to the PRC configuration:

1. Start the APR [Configuration Console](#) and [install your license key](#).
2. Start the Registry Editor (regedit.exe).
3. Expand the **HKEY_LOCAL_MACHINE, SOFTWARE, ANIXIS, ANIXIS Password Reset, and 2.0** registry keys.
4. Double-click the LicenseKey value, and then copy the entire license key to the clipboard by selecting it and pressing CTRL + C.
5. Use the Group Policy Management Console, or Active Directory Users and Computers Console to display the GPOs linked at the domain level.
6. Right-click the **Password Reset Client** GPO, and then click **Edit**.
7. Expand the **Computer Configuration, Policies** (if visible), **Administrative Templates, Classic Administrative Templates** (if visible), **ANIXIS Password Reset, and Password Reset Client** items.
8. Double-click the **License key** item in the right pane of the Group Policy Object Editor.
9. Select the **Enabled** option.
10. Click inside the **License key** text box, and then press CTRL + V to paste the license key.



11. Click **OK**.
12. Close the Group Policy Object Editor.

The license key is applied to all computers in the domain. This does not happen immediately, as Windows takes some time to apply the changes to Group Policy. You can force an immediate refresh of Group Policy on the local computer with the following command:

Windows 2000: `secedit /refreshpolicy machine_policy`

Windows XP and later: `gpupdate /target:computer`

License Agreement

ANIXIS IS WILLING TO LICENSE THIS SOFTWARE ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS SOFTWARE LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY. IF YOU DO NOT AGREE WITH THESE TERMS, THEN ANIXIS IS UNWILLING TO LICENSE THE SOFTWARE TO YOU.

ANIXIS SOFTWARE LICENSE AGREEMENT AND WARRANTY STATEMENT

(End-User Trial Use License With Option For Extended Use/Redistribution Prohibited)

1. The Software.

The Software licensed under this Agreement consists of computer programs, data compilation(s), and documentation referred to as ANIXIS Password Reset V2.x (the "Software").

2. Trial Use.

You are authorized to use the Software for evaluation purposes during a trial use term of thirty (30) days, unless prior to the expiration of the trial use term this license is terminated by You for convenience or terminated by either party for material breach. You have the option to register for full use of the Software at any time by paying the required license fee. Registration will authorize You to use an unlocking key which will convert the Software to full use, subject to the terms and conditions of this agreement. Your use of the Software under this trial use license for any purpose after the expiration of the initial trial use term is not authorized without the prior written consent of ANIXIS. Upon expiration of the limited trial use term, the Software may automatically disable itself. Immediately upon expiration of the limited trial use term, You shall either register for full use of the Software, or destroy all copies of the Software and documentation.

3. Perpetual Term.

If You purchase a perpetual license, then the term of the license granted herein shall be perpetual unless terminated by You for convenience or terminated by either party for material breach. Immediately upon termination of this license for any reason, You shall destroy all copies of the Software and documentation.

4. Subscription Term(s).

If You purchase a subscription license, then the term of this license is on a subscription basis with an initial term of one (1) year, and optional renewal terms of one (1) year each, unless prior to renewal this license is terminated by You for convenience or terminated by either party for material breach. Renewal procedures are available from ANIXIS, and unless such procedures are strictly satisfied, including the payment of any required license fee, Your use of the Software for any purpose after the expiration of the subscription term is not authorized. Upon expiration of the subscription term, the Software may automatically disable itself. Immediately upon expiration or termination of this license for any reason, You shall destroy all copies of the Software and documentation.

5. License Grant.

You are granted non-exclusive rights to install and use the Software on any computer and/or transmit the Software over a computer network, provided that You acquire and dedicate a licensed copy of the Software for each user who may access the Software. A license for the Software may not be shared or used concurrently by different users. You may purchase additional licenses for the Software from time to time. This Agreement shall take precedence over any purchase order for additional licenses, and any conflicting, inconsistent, or additional terms in such purchase orders shall be null and void. You may copy the Software for archival purposes, provided that all copies must contain the original Software's proprietary notices in unaltered form.

6. Restrictions.

You may not: (i) permit others to use the Software, except as expressly provided above for authorized network use; (ii) modify or translate the Software, except the HTML, CSS, and image files; (iii) reverse engineer, decompile, or disassemble the Software, except to the extent this restriction is expressly prohibited by applicable law; (iv) create derivative works based on the Software; (v) merge the Software with another product; (vi) copy the Software, except as expressly provided above; or (vii) remove or obscure any proprietary rights notices or labels on the Software.

7. Transfers.

You may not transfer the Software or any rights under this Agreement without the prior written consent of ANIXIS, which consent shall not be unreasonably withheld. A condition to any transfer or assignment shall be that the recipient agrees to the terms of this Agreement. Any attempted transfer or assignment in violation of this provision shall be null and void.

8. Ownership.

ANIXIS and its suppliers own the Software and all intellectual property rights embodied therein, including copyrights and valuable trade secrets embodied in the Software's design and coding methodology. The Software is protected by Australian copyright laws and international treaty provisions. This Agreement provides You only a limited use license, and no ownership of any intellectual property.

LIMITED WARRANTY STATEMENT; LIMITATION OF LIABILITY. ANIXIS warrants only to You that the Software shall, in unmodified form, perform substantially in accordance with accompanying documentation under normal use for a period of thirty (30) days from the purchase date. The entire and exclusive liability and remedy for breach of this Limited Warranty shall be, at ANIXIS's option, either (i) return of the amount received by ANIXIS for the Software, or (ii) replacement of defective Software and/or documentation. ANIXIS AND ITS SUPPLIERS AND RESELLERS SPECIFICALLY DISCLAIM THE IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SYSTEM INTEGRATION, AND DATA ACCURACY. THERE IS NO WARRANTY OR GUARANTEE THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT THE SOFTWARE WILL MEET ANY PARTICULAR CRITERIA OF PERFORMANCE, QUALITY, ACCURACY, PURPOSE, OR NEED, EXCEPT AS EXPRESSLY PROVIDED IN THE LIMITED WARRANTY. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS AGREEMENT. NO USE OF THE SOFTWARE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER. No action for the above Limited Warranty may be commenced after one (1) year following the expiration date of the warranty. To the extent that this Warranty Statement is inconsistent with the jurisdiction where You use the Software, the Warranty Statement shall be deemed to be modified consistent with such local law. Under such local law, certain limitations may not apply, and You may have additional rights which vary from jurisdiction to jurisdiction. For example, some states in the United States and some jurisdictions outside the United States may: (i)

preclude the disclaimers and limitations of this Warranty Statement from limiting the rights of a consumer; (ii) otherwise restrict the ability of a manufacturer to make such disclaimers or to impose such limitations; or (iii) grant the consumer additional legal rights, specify the duration of implied warranties which the manufacturer cannot disclaim, or prohibit limitations on how long an implied warranty lasts.

INDEPENDENT OF THE FORGOING PROVISIONS, IN NO EVENT AND UNDER NO LEGAL THEORY, INCLUDING WITHOUT LIMITATION, TORT, CONTRACT, OR STRICT PRODUCTS LIABILITY, SHALL ANIXIS OR ANY OF ITS SUPPLIERS BE LIABLE TO YOU OR ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND, INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER MALFUNCTION, OR ANY OTHER KIND OF COMMERCIAL DAMAGE, EVEN IF ANIXIS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT PROHIBITED BY APPLICABLE LAW.

IN NO EVENT SHALL ANIXIS'S LIABILITY FOR ACTUAL DAMAGES FOR ANY CAUSE WHATSOEVER, AND REGARDLESS OF THE FORM OF ACTION, EXCEED THE AMOUNT OF THE PURCHASE PRICE PAID, IF ANY, FOR THE SOFTWARE LICENSE.

EXPORT CONTROLS. You agree to comply with all local laws in Your jurisdiction which might impact Your right to import, export or use the Software, and You represent that You have complied with any regulations or registration procedures required by applicable law to make this license enforceable.

MISCELLANEOUS. This Agreement constitutes the entire understanding of the parties with respect to the subject matter of this Agreement and merges all prior communications, representations, and agreements. This Agreement may be modified only by a written agreement signed by the parties. If any provision of this Agreement is held to be unenforceable for any reason, such provision shall be reformed only to the extent necessary to make it enforceable. This Agreement shall be construed under the laws of the State of New South Wales, Australia, excluding rules regarding conflicts of law. This Agreement will not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. The parties have requested that this Agreement and all documents contemplated hereby be drawn up in English. Les parties aux presentes ont exige que cette entente et tous autres documents envisages par les presentes soient rediges en anglais.

U.S. GOVERNMENT END USERS: If the Software and documentation is acquired by or for the United States Government then it is provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, or subparagraphs (c)(1) and (2) of the Commercial Computer Software-Restricted Rights at 48 CFR 52.227-19 or clause 18-52.227-86(d) of the NASA supplement to the FAR, as applicable. Manufacturer is ANIXIS, 9 Monterey Terrace, Glenmore Park, NSW 2745 Australia.