ANIXIS Password Reset

Administrator’s Guide

V3.23

Table of Contents

Introduction

ANIXIS Password Reset is a self-service password management system that helps you 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 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 reset their password from the Windows logon screen, or a mobile device. 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 some questions about themselves, and optionally by sending a verification code to their mobile phone. 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 and night. 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

APR Server

- Random verification codes can be sent to users by e-mail and SMS. Users must enter the code to reset their password or unlock their account. Verification codes can be used for two-factor authentication, or to authenticate users that have not enrolled (automatic enrollment).
- The database can be moved to SQL Server for better security, fault tolerance, and accessibility.
- Users are automatically deleted from the database approximately one week after they are deleted from Active Directory.
- Can enforce the Active Directory password history and minimum age policies for password resets.
- Improved handling of password changes across domains and forests.
- More secure enrollment record format. APR V2 records are upgraded to the new format when the system maintenance task runs at 1:00 AM.
- More secure communication protocol. The updated protocol uses 2048-bit RSA keys, has better error detection, and uses fewer CPU cycles.
- E-mail alerts are sent in the user's preferred language if possible. The preferred language is set after a successful enroll, reset, unlock, or change.
- Can send all PPE queries to a specific Password Policy Server.
- Default database updated to SQL Server Compact 4.0 SP1.
- Improved multithreading performance when querying the database.
- Replaced the 32-bit APR Server service with a 64-bit version.

Web Interface

- REST API to remind (or require) users to enroll.
- Page content and layout changes for small mobile phone screens.
- Icons are in Scalable Vector Graphics (SVG) format. These look sharper when resized, and make it easy to change the color scheme.
- Improved encryption of temporary data.
- Improved handling of e-mail addresses with unusual characters.
- Updated response headers to improve compatibility with some browsers, and to reduce the likelihood of user-submitted information being cached.
- Answer fields are masked during Reset and Unlock.
- Performance improvements to the page generator and request parser.

Password Reset Client

- Displays HTML in Internet Explorer 11 mode for improved compatibility with the latest web standards.
- Improved compatibility with third-party credential providers.
- Updated window sizing algorithm to suit the APR V3 page templates.
- Client window closes with the JavaScript window.close() method.
- Displays messages after the page finishes loading to avoid display problems.

Data Console

- Can run remotely after the database is moved to SQL Server.
- .xlsx and .xml export file formats.
- Filter icons shown in column headers.
- Improved performance when reading, sorting, and filtering data.

Configuration Console

- Can create e-mail alerts in different languages.
- Added Bcc address to e-mail template editor.
- Increased Question List capacity.

Installer

- Offers to silently install IIS before installing the Web Interface.
- Automatically installs required IIS Role Services for the Web Interface.
- Sets the APR application pool to 64-bit.
- Installs SQL Server Compact 4.0 SP1.

Installing APR

ANIXIS Password Reset V3.23 is designed to run on Windows 2008 to 2019. Users access APR from a web browser, or from the Password Reset Client.

System Requirements

- Windows 2008*, 2008 R2, 2012, 2012 R2, 2016, or 2019.
  * x64 only for APR Server and Web Interface.
- 20 Megabytes free disk space.
- 20 Megabytes free RAM.

System Components

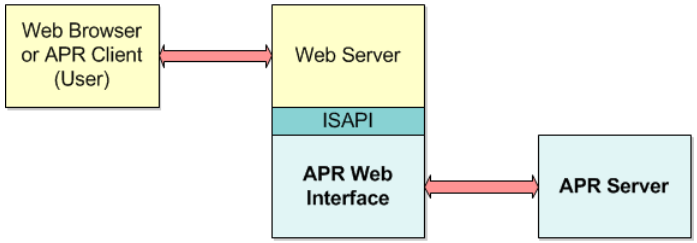
ANIXIS Password Reset has two server components, and an optional client. Both server components can be installed on one server, or they may be installed on separate servers if your web server is in a DMZ.

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 7 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 is installed with the APR Server. SQL Server Compact is free to use, and should only be removed if you move the database to SQL Server. SQL Server Compact is an embedded database. Unlike SQL Server, you do not need to configure or manage it.

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 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 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 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.

Single Server Installation

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

1. Start the APR Setup wizard (APR323.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. The Setup wizard may offer to install IIS. Click **OK** to install IIS.
7. Type a **User Name**, **Domain**, and **Password** for the APR 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 it has the required permissions.
8. Click **Next**.
9. 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.
10. Click **Next** twice.
11. 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\ANIXIS Password Reset\ folder by default. Use the SERVERDIR parameter to install the APR Server to a different folder. For example, APR323.exe SERVERDIR="D:\Programs\APR\"

Multiple Server Installation

Create firewall rules to allow the Web Interface and APR Server to communicate if there is a DMZ firewall between them. 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

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

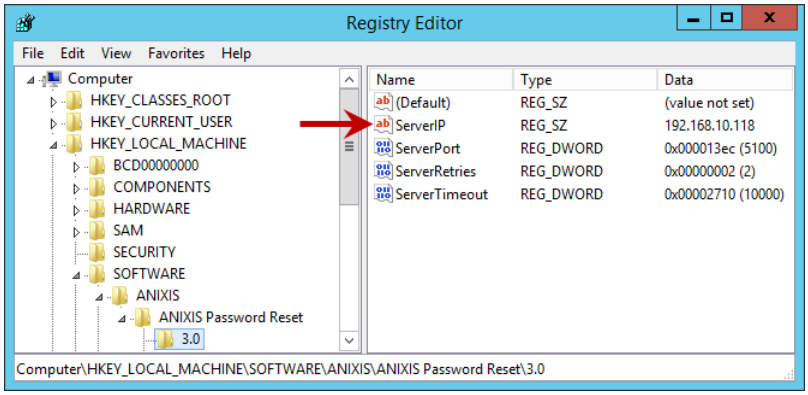
1. Start the APR Setup wizard (APR323.exe).
2. The Setup wizard may ask you to backup some files if an older version of APR is detected. Backup the files, and then click **Next**.
3. Click **Next**.
4. Read the license agreement. Click **I accept the terms of the license agreement**, and then click **Next** 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 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 it has the required permissions.
7. Make sure the **Create Windows Firewall Exception for the APR Server service** check box is selected, and then click **Next** twice.
8. Wait for the APR Server to install, and then click **Finish**.

Open UDP port 5100 on the APR Server computer if a host-based firewall other than the Windows Firewall is installed. This is needed in addition to the DMZ firewall rules above.

The APR Setup wizard installs the APR Server and associated files into the \Program Files\ANIXIS Password Reset\ folder by default. Use the SERVERDIR parameter to install the APR Server to a different folder. For example, APR323.exe SERVERDIR="D:\Programs\APR\"

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

1. Start the APR Setup wizard (APR323.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. The Setup wizard may offer to install IIS. Click **OK** to install IIS.
7. 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.
8. Click **Next** twice.
9. Wait for the Web Interface to install, and then click **Finish**.
10. Start the Registry Editor (regedit.exe).
11. Expand the **HKEY_LOCAL_MACHINE**, **SOFTWARE**, **ANIXIS**, **ANIXIS Password Reset**, and **3.0** registry keys.
12. 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 **3.0** registry keys.
3. Clear the data in the **ServerIP** registry value.
4. Create a REG_SZ value for each Web Interface called ServerIP_VDIR where VDIR is the name of the virtual directory. For example, if the virtual directory is called Finance, then the registry value should be called ServerIP_Finance.
5. Set each ServerIP_VDIR value to the IP address of the APR Server.

Upgrading From APR V3.x

Some planning is needed to ensure a smooth upgrade from APR V3.x. A trial run on a lab network is recommended if you have not installed APR before.

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.

You may need to restart Windows after upgrading.

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 account as you will need it during the upgrade.

Upgrading to V3.23

Start the APR Setup wizard (APR323.exe) and follow the prompts. The Setup wizard uninstalls the previous version, so there is no need to manually uninstall it.

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 should keep a copy of the original Web Interface files and compare them with the files from the previous version using a file comparison tool. Any changes between versions should be merged into your customized files.

The APR V3.23 Data Console does not read the VerificationCode or EnrollRecord columns from the Usr table on SQL Server. Access to these columns can be denied for Data Console users after upgrading all instances of the Data Console.

Upgrading From APR V2.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.

APR V3.23 is only compatible with Password Policy Enforcer V7.0 and later. Upgrade PPE to a compatible version if you have enabled Password Policy Enforcer integration.

APR V3.23 does not include a 32-bit APR Server or Web Interface. The computer(s) running the APR server components must be running Windows 64-bit. This does not apply to the client computers.

APR V3.23 uses HTML5 and CSS3 features that are not supported by Internet Explorer 8 and earlier. The Password Reset Client uses Internet Explorer for page rendering, so the default HTML templates do not display correctly in the Password Reset Client on Windows XP and Server 2003. Send an e-mail to support@anixis.com before upgrading if you still have computers running Internet Explorer 8.

APR V3.23 server components have not been tested on, and are not supported on Windows 2003.

Before You Begin

1. Backup the APR V2.x server(s).
2. Close the Data Console if it is open.
3. Stop the "ANIXIS Password Reset" service and backup the database.

Upgrading to V3.23

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 the Data Console, and check the **Audit Log** and **User** tabs to make sure the data was imported.
3. Open APR in a web browser and test the Enroll, Reset, and Change features.
4. Install your new license key if you have a perpetual license.
5. Update the Client license key if you have a perpetual license.

Other Tasks

The database files are created in the installation folder when APR is first installed. The default installation folder for APR V2.x was below the "Program Files (x86)" folder, but in APR V3.23 it is below the "Program Files" folder. The database files are not moved automatically during an upgrade, so you should move them to the new installation folder (or a different folder) after upgrading. To move the database files to the \Program Files\ANIXIS Password Reset\ folder:

1. Close the Data Console if it is open.
2. Stop the "ANIXIS Password Reset" service.
3. Move apr.sdf and aprlog.sdf from the \Program Files (x86)\ANIXIS Password Reset\ folder to the \Program Files\ANIXIS Password Reset\ folder.
4. Open the Configuration Console.
5. Click the **General** tab.
6. Click **Change...**
7. Click **Browse...** and then browse to the \Program Files\ANIXIS Password Reset\ folder.
8. Click **OK** twice, and then click **Apply**.
9. Start the "ANIXIS Password Reset" service.
10. Update the backup script to copy from the new folder.

Older versions of the Password Reset Client display pages in Internet Explorer 7 emulation mode. This mode cannot display the new HTML templates correctly. You can upgrade the Password Reset Client to the latest version, or configure existing installations to use IE 11 mode. This only works on Windows Vista and later with IE 9 or later. To configure the Password Reset Client to use IE 11 mode:

1. Start the Registry Editor (regedit.exe).
2. Expand the **HKEY_LOCAL_MACHINE**, **SOFTWARE**, **Microsoft**, **Internet Explorer**, **MAIN**, **FeatureControl**, and **FEATURE_BROWSER_EMULATION** registry keys.
3. Create a new DWORD value called **LogonUI.exe**, and set it to 2AF8 (hex).

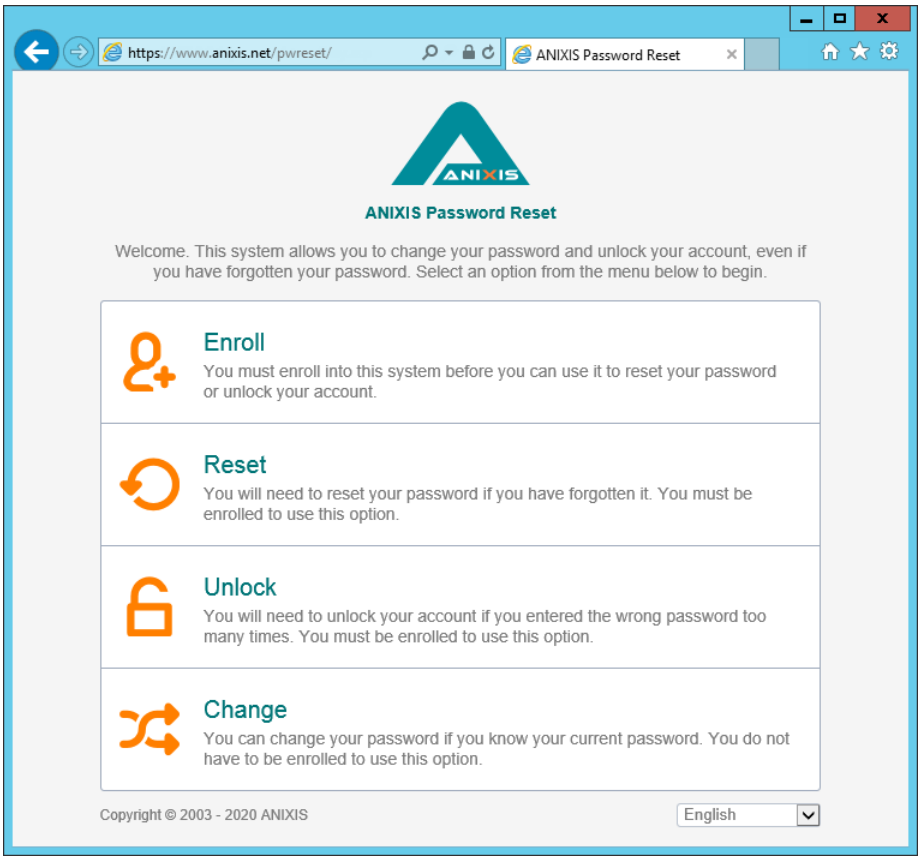
Create this registry value on all the Password Reset Client computers. IE 11 mode can be requested even if the computer is running an older version of IE.

Using APR

ANIXIS Password Reset is a web application. Users can access it from a web browser, or from the Password Reset Client. The default URL for the Web Interface is: `http://[server]/pwreset/`

You can use URL parameters to open a specific page, and to set the user and domain names. For example: `http://[server]/pwreset/apr.dll?cmd=enroll&username=maryjones&domain=ANIXIS`

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



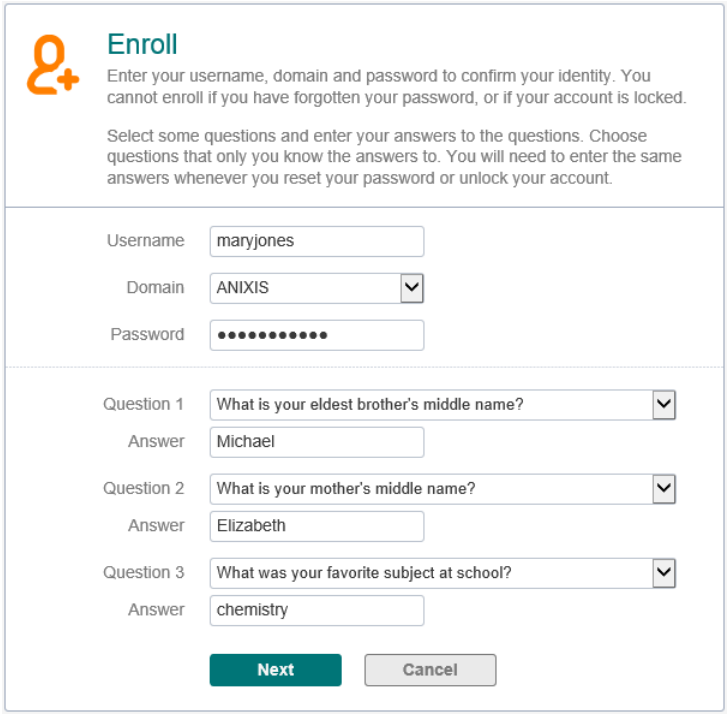
Users access the Enroll, Reset, Unlock, and Change features from the menu. These features are explained on the following pages.

The connection between the Web Interface and APR Server is always encrypted. Install an SSL certificate on the web server and use HTTPS to encrypt connections from the browser to the web server.

Enroll

Only enrolled users can reset their password and unlock their account. Users can enroll manually by answering some questions about themselves, or they can be enrolled automatically if automatic enrollment is enabled. 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 manually enroll into APR:

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



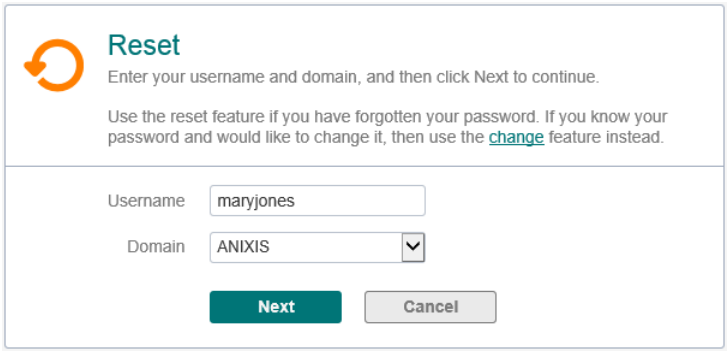
2. Type a **Username**, **Domain**, and **Password**.
3. Type an e-mail address if the **E-mail** text box is visible.
4. Select a question from each of the **Question** drop-down lists, and type an answer to each question in the **Answer** text boxes.
5. Click **Next**, and then click **OK** to return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

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

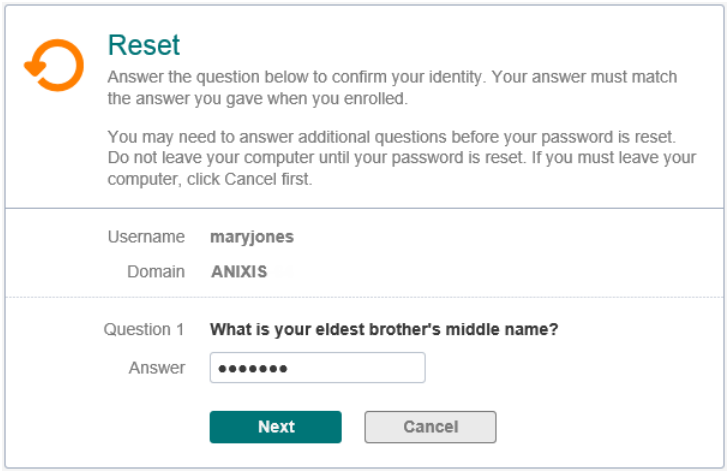
Reset

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

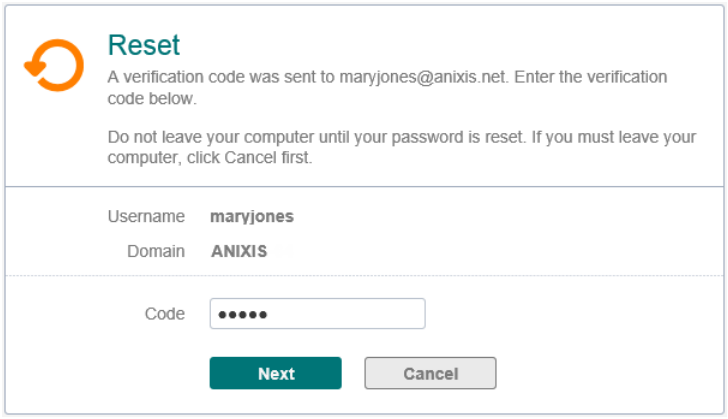
1. Click the **Reset** item in the menu.



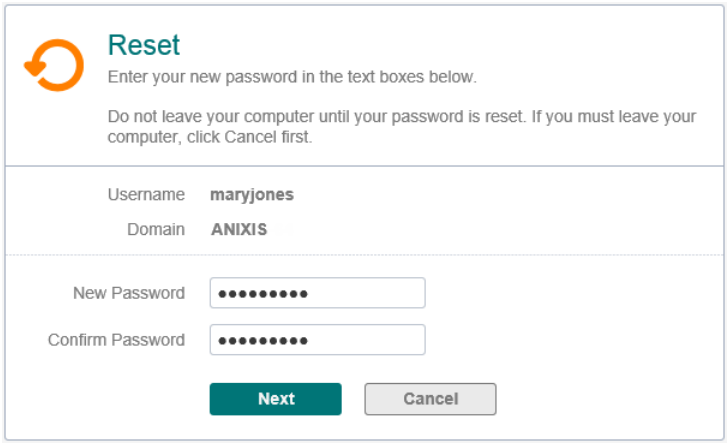
2. Type a **Username** and **Domain**, and then click **Next**.



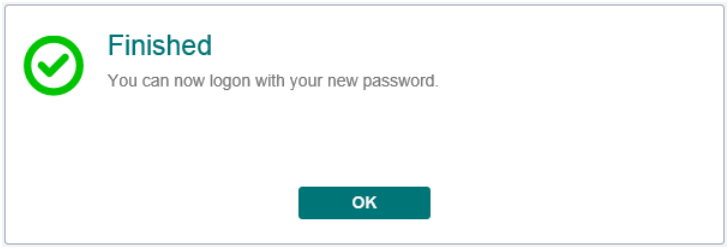
3. Type the **Answer** to the first question, and then click **Next**. Repeat until all questions are answered correctly.



4. You may be asked to enter a verification code. The verification code is sent to your phone by e-mail or SMS. Type the **Code**, and then click **Next**.



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

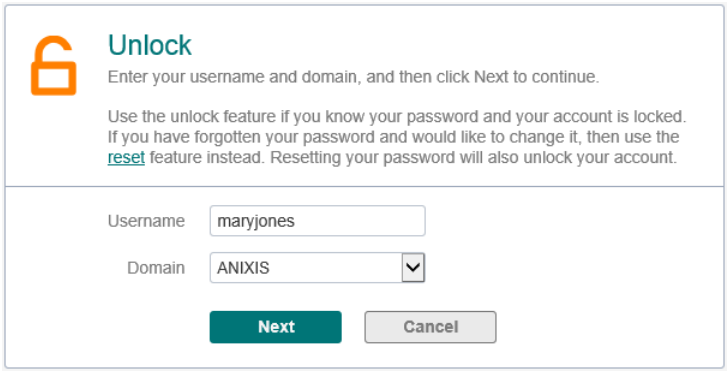


6. Click **OK** to return to the menu.

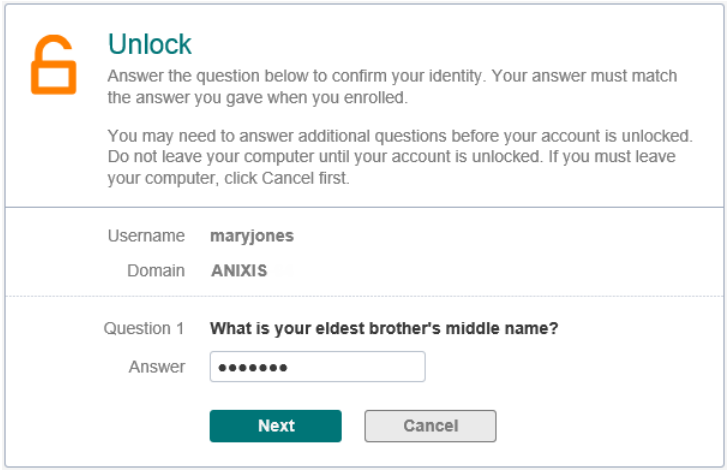
Unlock

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

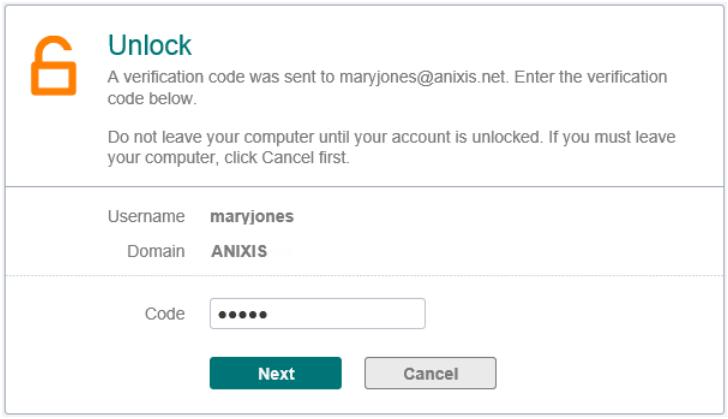
1. Click the **Unlock** item in the menu.



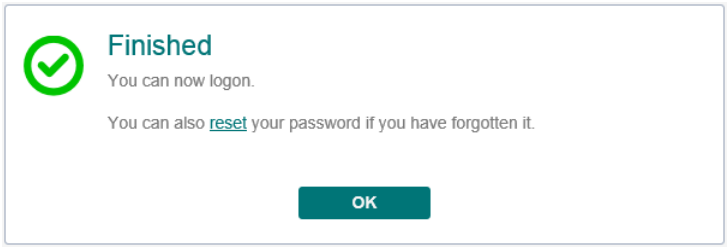
2. Type a **Username** and **Domain**, and then click **Next**.



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



4. You may be asked to enter a verification code. The verification code is sent to your phone by e-mail or SMS. Type the **Code**, and then click **Next**.



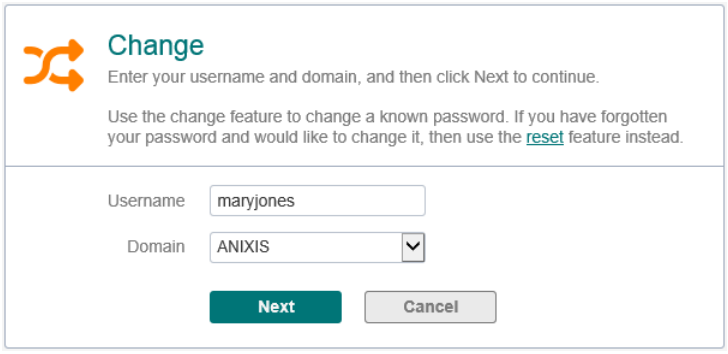
5. Click **OK** to return to the menu.

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

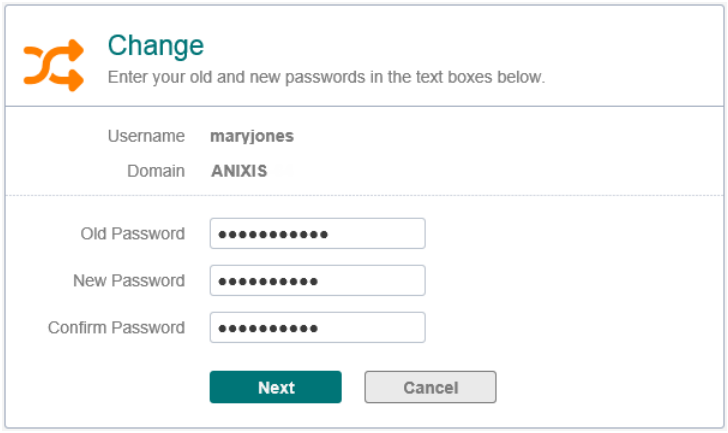
Change

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.



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

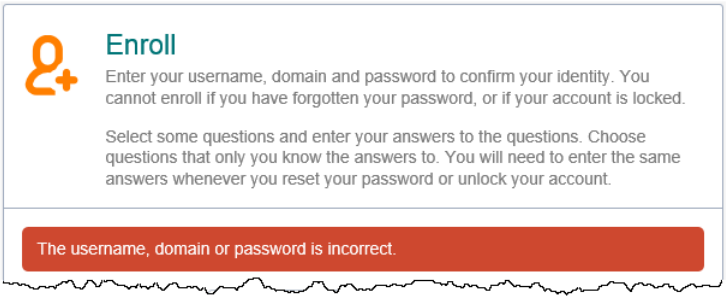


3. Type the **Old Password**, **New Password**, and **Confirm Password**, and then click **Next**.
4. Click **OK** to return to the menu.

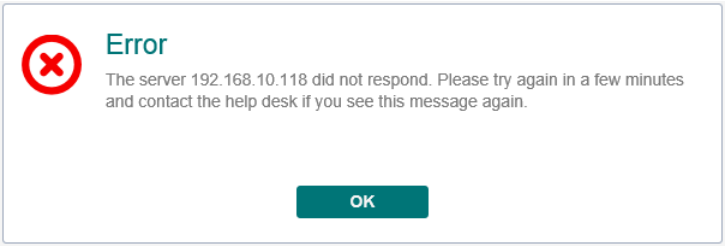
Windows increments the bad password count in Active Directory when a user tries to change their password with an incorrect password. This may trigger a lockout if the Windows account lockout policy is enabled.

Error Messages

Validation errors are shown in a red 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 Windows 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.



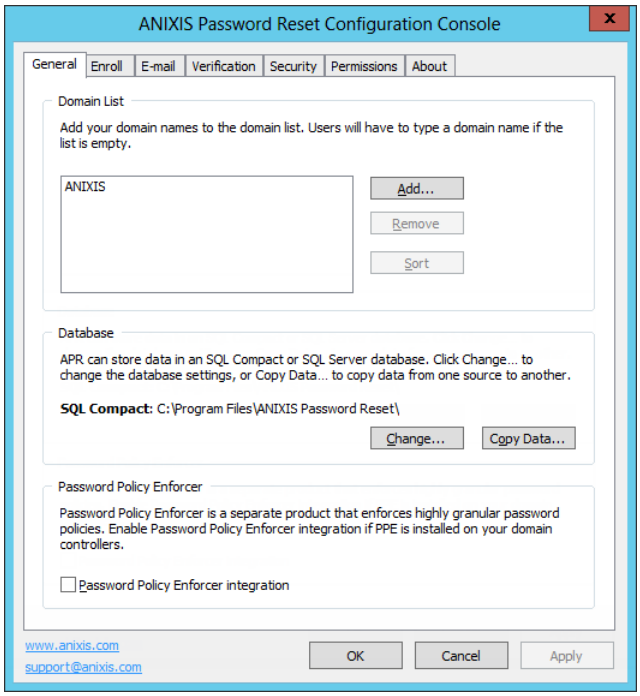
Validation and critical error messages are stored in the HTML templates. You can modify the default messages by editing the templates.

Configuring APR

Click **Start > ANIXIS Password Reset > APR Configuration Console** on the APR Server computer to open the Configuration Console.

General Tab

Use the **General** tab to maintain the list of managed domains, set the database options, and enable Password Policy Enforcer integration.



Domain List

The Domain List is empty when APR is first installed, 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

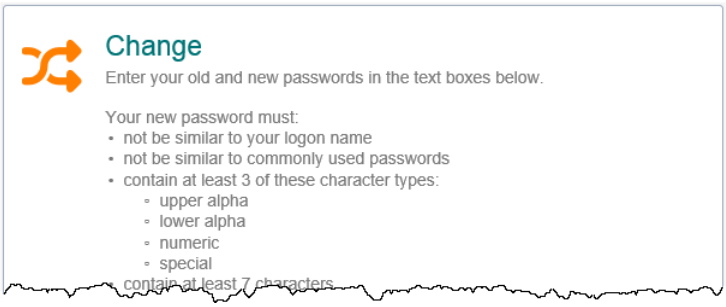
APR uses an SQL Server Compact database by default. It creates two database files (apr.sdf and aprlog.sdf) in the APR installation folder. To move these files to another folder:

1. Close the Data Console if it is open.
2. Stop the "ANIXIS Password Reset" service.
3. Move apr.sdf and aprlog.sdf to their new location. The database files should remain on a local disk.
4. Give the APR service account read and write permissions to the database files in their new location.
5. Open the APR Configuration Console, and click **Change...** in the **General** tab.
6. Click **Browse...** and select the new database path.
7. Click **OK** twice, and then click **Apply**.
8. Start the "ANIXIS Password Reset" service.
9. Update the backup script to copy from the new folder.

You can also move the database from SQL Server Compact to SQL Server. See the Moving to SQL Server section for more information.

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 PPE to help users choose a compliant password.



APR displays the PPE policy message when users are 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 PPE on your domain controllers.

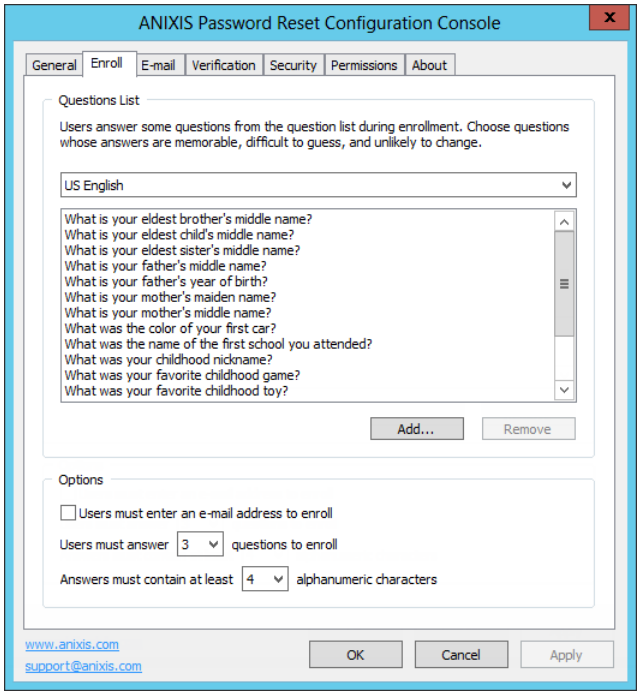
APR locates and queries a domain controller in the user's domain when Password Policy Enforcer integration is enabled. You can override this behavior and send all PPE queries to a specific IP address by setting the **PPEIPAddress** registry value to the IP address of a Password Policy Server. The **PPEIPAddress** value is in **HKEY_LOCAL_MACHINE\SOFTWARE\ANIXIS\ANIXIS Password Reset\3.0**. Users are more likely to see the PPE Generic Rejection message rather than the more detailed Rejection message when this registry value is set. Users may also have the wrong policy, or no policy enforced if the queried server is not a domain controller in the user's domain.

Queries to the Password Policy Server are sent to UDP port 1333 by default. You may need to create firewall rules to open this port. See the "Creating Firewall Rules for the PPC" section of the PPE Administrator's Guide for more information.

Password Policy Enforcer is not included with APR. 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 options.



Question List

Users must answer some questions about themselves when they manually enroll. 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. You can also replace question lists with text boxes so users can enter their own questions.

Options

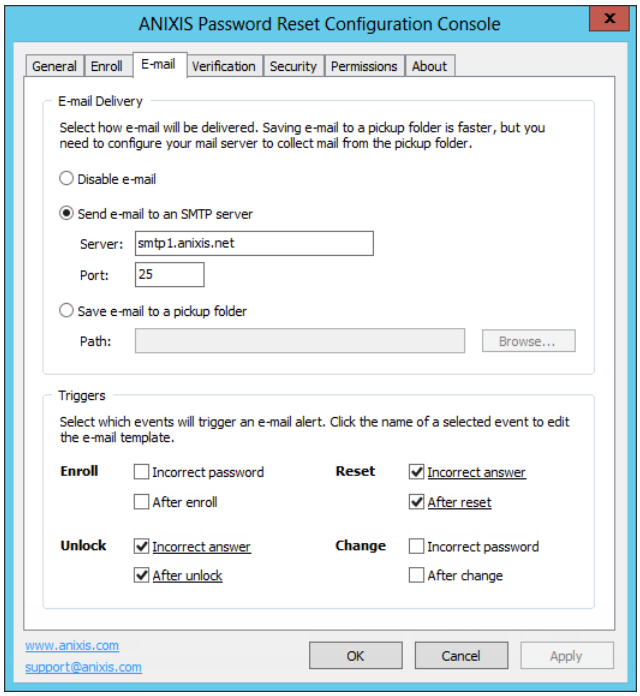
ANIXIS Password Reset can send e-mail alerts to users when a request is submitted for their account. These alerts can be sent to the user's Active Directory e-mail address and/or to an e-mail address in APR's database. Select the **Users must enter an e-mail address to enroll** check box if users should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



E-mail Delivery

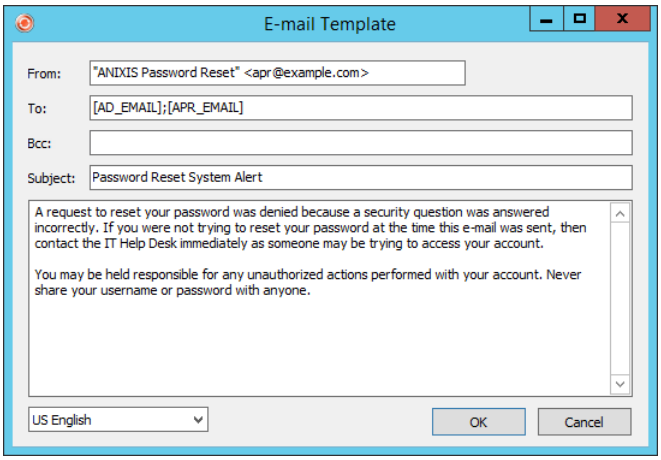
APR can send e-mail alerts directly to an SMTP server, or save them to a pickup folder. Select the **Send e-mail to an SMTP server** option if APR should send e-mails directly to an SMTP server. Type the name or IP address of an SMTP server in the **Server** text box, and the SMTP port number in the **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-mails are sent. If the trigger for an event is enabled, then APR sends an e-mail when the event occurs. Enabled triggers are 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, then the alert is only sent to the invalid address.

Type additional recipient e-mail addresses in the **Bcc** text box if you want to send any blind carbon copies. Separate multiple recipients with a semicolon.

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

Type the e-mail's body in the large text box. The e-mail is sent as plain text unless the body contains the <html> tag. Include the entire HTML document when sending e-mail as HTML. You can also use these macros.

Macro	Replaced with
[AD_DOMAIN]	The user's Active Directory domain name
[AD_USER]	The user's Active Directory logon name

APR stores the user's preferred language every time they successfully complete an Enroll, Reset, Unlock, or Change. E-mail alerts are sent in the user's preferred language, or in the current Web Interface language if the user's preferred language is not known. If an e-mail template is not defined for the user's preferred language, then the alert is sent in English.

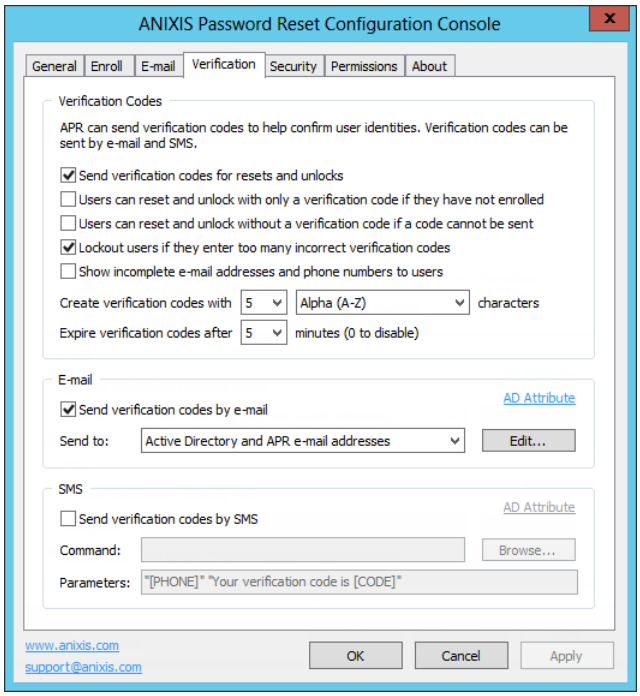
Use the drop-down list at the bottom of the E-mail template editor to switch between template languages. Changes are preserved as you switch between languages. The **From**, **To**, and **Bcc** are the same for all languages.

A warning icon is shown beside the language drop-down list if an e-mail template is not defined for every language. You should define an e-mail template for every language to ensure that users can understand their e-mail alerts.

An attacker may choose a specific language to avoid detection. E-mail alerts are sent in the Web Interface language chosen by the attacker if the target user has not enrolled or changed their password with APR. The target user will receive the e-mail alerts, but they may not understand them. Use the REST API to remind new users to enroll so their preferred language is known to APR.

Verification Tab

Use the **Verification** tab to enable verification codes for resets and unlocks. Verification codes are used for two-factor authentication, and to authenticate users that have not manually enrolled. A verification code is sent to the user's mobile phone by e-mail and/or SMS, and the user enters the verification code to continue.



Verification Codes

Select the **Send verification codes for resets and unlocks** check box to enable verification codes.

Select the **Users can reset and unlock with only a verification code if they have not enrolled** check box to enable automatic enrollment. Automatic enrollment allows users to reset their password and unlock their account even if they have not previously enrolled. APR enrolls the users when they request a reset or unlock, and sends them a verification code for authentication. Users that are automatically enrolled can also manually enroll with questions later. Users that are only automatically enrolled cannot continue to reset their password and unlock their account if this option is subsequently disabled. Automatic enrollment should only be used with secure devices connected to a secure network, otherwise a stolen or lost device could be used to reset a user's password.

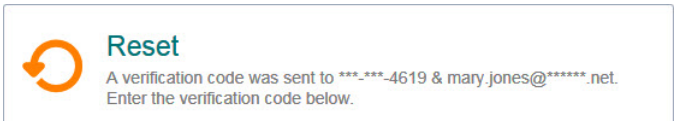
Automatically enrolled users:

- Do not have an APR e-mail address, so verification codes are only sent to the user's Active Directory e-mail address and/or phone number.
- Must be authenticated with a verification code, so their reset or unlock request will be denied even if the **Users can reset and unlock without a verification code if a code cannot be sent** check box is selected.
- Need to manually enroll if the sending of verification codes, or automatic enrollments are disabled after they are automatically enrolled.
- Can manually enroll at any time. Authenticating users with questions and verification codes is more secure than using only verification codes.
- Are not sent the After Enroll e-mail alert.

Select the **Users can reset and unlock without a verification code if a code cannot be sent** check box if users should be allowed to continue when a verification code cannot be sent. Verification codes can only be sent to users that have a mobile phone number or e-mail address in Active Directory, or an e-mail address in APR's database. Even if this information is present, an error could stop the verification code from being sent. If this check box is not selected, then users will need to contact the help desk if a verification code cannot be sent.

Select the **Lockout users if they enter too many incorrect verification codes** check box if the incorrect answer count should be incremented when users submit an incorrect verification code. A user's APR record can be locked out if they enter too many incorrect answers or verification codes. The lockout threshold is set on the **Security** tab.

Select the **Show incomplete e-mail addresses and phone numbers to users** check box if APR should hide parts of the e-mail address and phone number when requesting a verification code. This is especially important if automatic enrollment is enabled, as it stops an attacker from discovering information about the user.



Verification codes are of a specified length, and may contain both alpha and numeric characters. Select the desired options from the **Create verification codes with...** drop-down lists. Longer, more complex (alphanumeric) verification codes are harder to guess, but also harder to enter. Verification codes do not need to be very long or complex if the verification code lockout and expiry features are enabled.

Select a value from the **Expire verification codes after...** drop-down list to limit how long users have to enter their verification code. Set it to 0 minutes if the verification code should not expire. A new verification code is sent for every reset and unlock. This setting limits how long a user has to enter their verification code, it does not allow old verification codes to be reused.

E-mail

Select the **Send verification codes by e-mail** check box to send verification codes to users via e-mail. You must configure the e-mail delivery options in the **E-mail** tab to send verification codes by e-mail.

Verification codes can be sent to the Active Directory e-mail address and/or the APR e-mail address. Select the desired option from the **Send to** drop-down list.

Click **Edit...** to edit the e-mail template for verification codes. The [CODE] macro is replaced with the verification code, so include the [CODE] macro in the e-mail subject or body.

The user's Active Directory e-mail address is read from the "mail" attribute by default. Click **AD Attribute** if you want to use an e-mail address from a different attribute. Type the name of the attribute, and then click **OK**.

SMS

Select the **Send verification codes by SMS** check box to send verification codes to users via SMS. Any SMS provider with a Windows command-line interface (CLI) can be used.

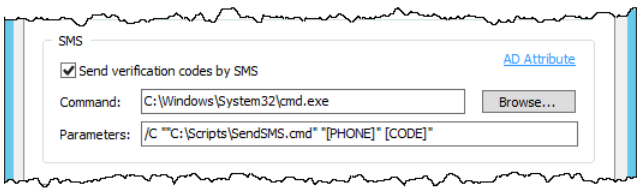
Click **Browse...** to select the executable that sends the SMS. The executable is supplied by your SMS provider.

Type the command-line parameters in the **Parameters** text box. Refer to your SMS provider's documentation for the expected parameters. You can also use the macros in the table below. Use quotes around parameters and macros that may contain space characters.

Macro	Replaced with
[CODE]	Verification code
[PHONE]	User's Active Directory phone number
[USERNAME]	User's Active Directory user logon name
[DOMAIN]	User's Active Directory domain name
[LANG]	Current Web Interface language code

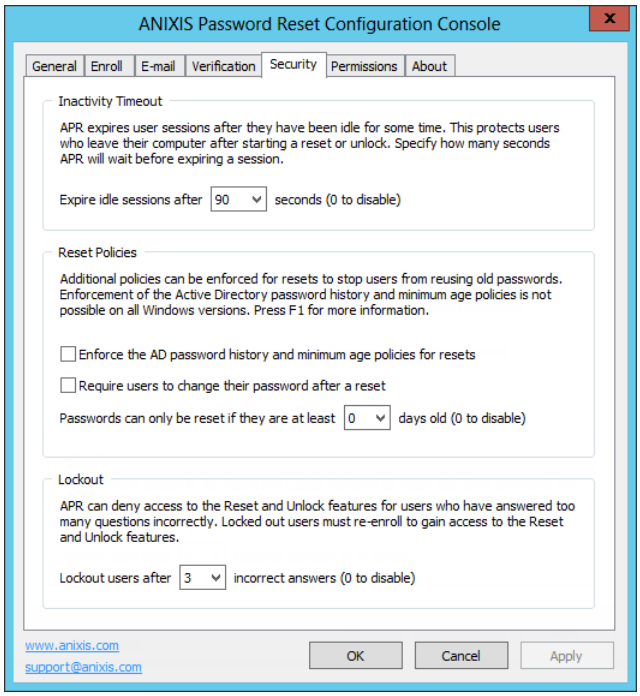
The user's Active Directory mobile phone number is read from the "mobile" attribute by default. Click **AD Attribute** if you want to use a phone number from a different attribute. Type the name of the attribute, and then click **OK**.

Use a script to perform additional processing before sending the SMS. For example, a script could read the user's phone number from a database, or send a language-specific SMS based on the value of the [LANG] macro. Put the path of the scripting engine executable in the **Command** text box, and the path to the script file and other parameters in the **Parameters** text box.



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

Select the **Enforce the AD password history and minimum age policies for resets** check box to enforce these Active Directory password policies during a reset. Older Windows versions cannot enforce these policies for password resets. This capability was added as a hotfix for Windows 2008 and 2008 R2 (see Microsoft KB 2386717). The hotfix is included with SP1 for Windows 2008 R2, and is a standard feature on later Windows versions.

Users are more likely to forget a password shortly after changing it. Enforcing a minimum age for password resets may increase the number of help desk calls

because users won't be able to reset recently changed passwords. One solution is to clear the check box above, and select the **Require users to change their password after a reset** check box instead. The Active Directory password history policy won't be enforced for the password reset, but it will be enforced for the password change when the user logs on. This stops users from reusing a recent password, but it won't stop them from resetting a recently changed password. Users whose passwords are set to never expire in Active Directory will not be forced to change their password during logon, even if this check box is selected.

Password Policy Enforcer's History rule is enforced for password resets if the **Enforce policy when password is reset** check box is 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. PPE does not enforce the Minimum Age rule for password resets.

Users may try to evade the password history policy by resetting their password several times in quick succession to "push" a password off the password 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. If the Active Directory minimum password age policy is also enforced for password resets, then the effective minimum age is the greater of the AD and APR minimum ages.

Lockout

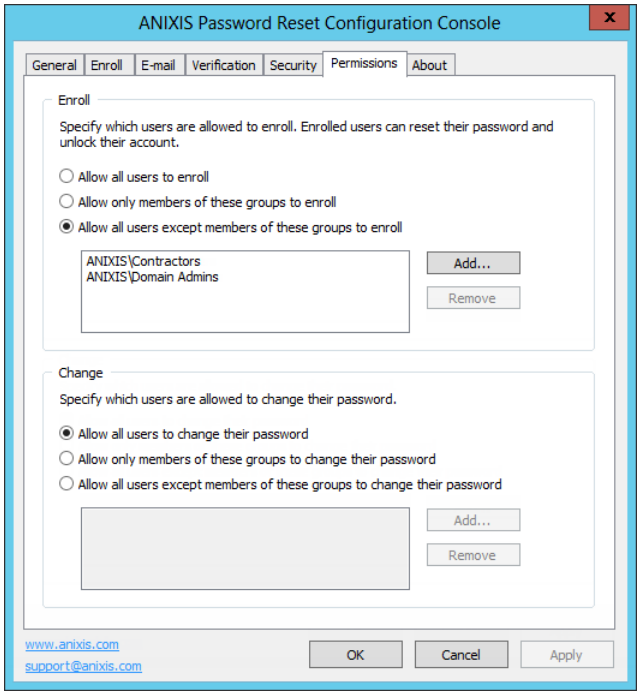
APR's lockout should not be confused with the Windows lockout policy. A Windows lockout stops users from logging on, whereas an APR lockout stops users from resetting their password and unlocking their account. Windows locks out users when they enter too many incorrect passwords. APR locks out users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

Select a value from the **Lockout user after...** drop-down list to specify how many incorrect answers APR accepts before locking out a user. Set it to 0 incorrect answers to disable the lockout feature. Incorrect verification codes are counted as incorrect answers if the **Lockout users if they enter too many incorrect verification codes** check box is selected on the **Verification** tab.

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 use APR.



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.

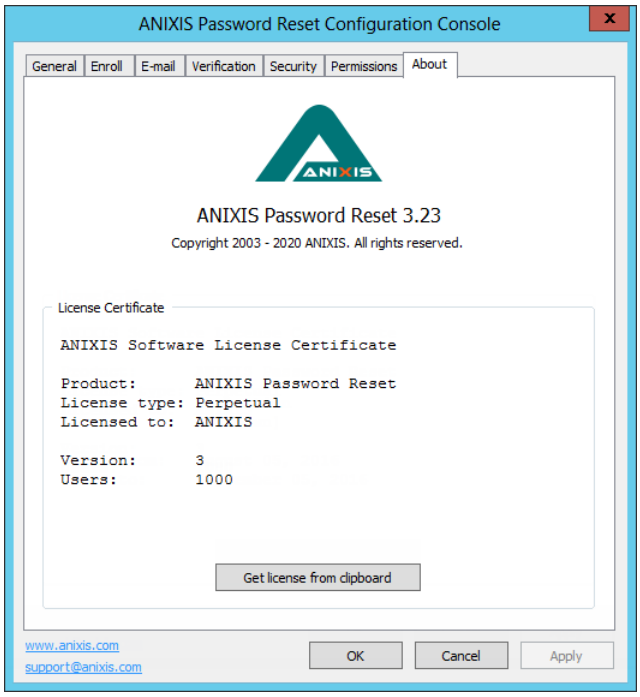
To remove a group from the list, select it and then click **Remove**. Enrolled users can continue to reset their passwords and unlock their accounts even if they are no longer allowed to enroll.

Change

These settings specify which users can 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.



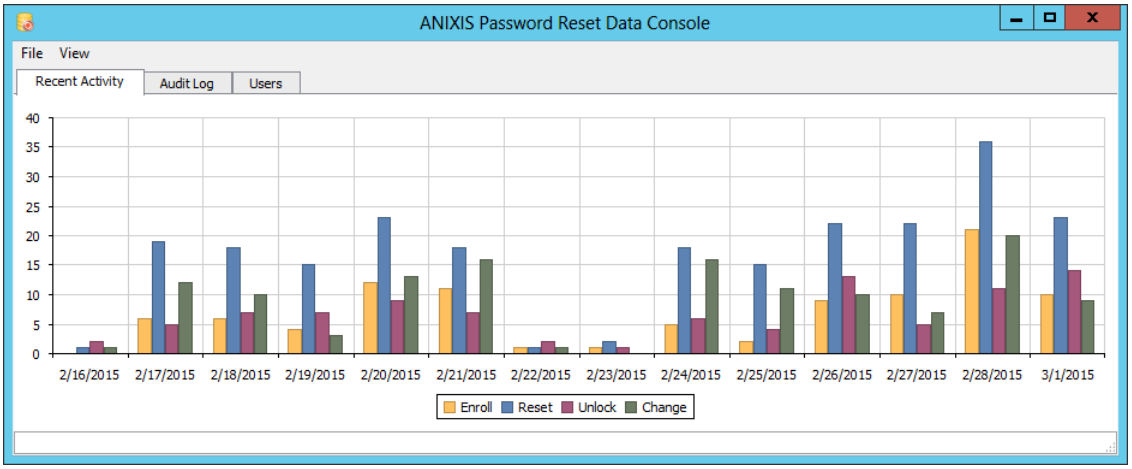
To install a new license key, copy the entire license e-mail to the clipboard, and then click **Get license from clipboard**.

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.

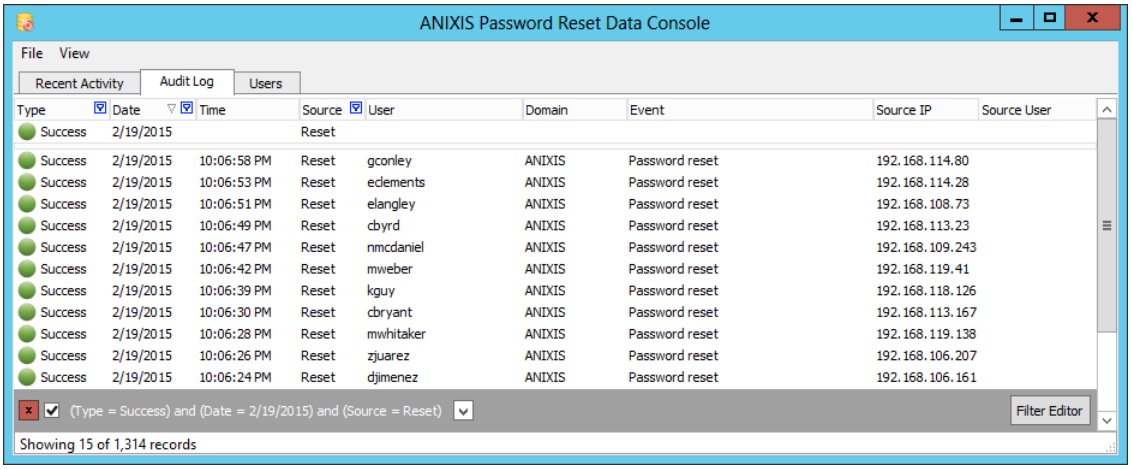
Using the Data Console

The Data Console allows you to view and export data collected by APR. Click **Start > 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 2/19/2015 to see all the password resets for that day.

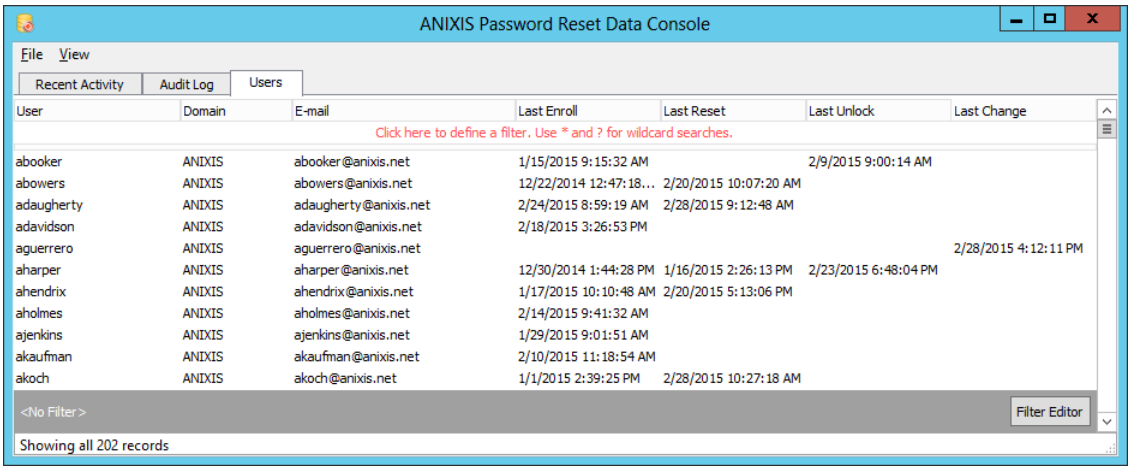


The resulting view shows only the 15 successful password resets on 2/19/2015. These are shown in the **Audit Log** tab. You can create your own filters to find events in this tab.

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 user logon name
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.



The **Users** tab has seven columns.

Column	Information
User	User's Active Directory user logon name
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.

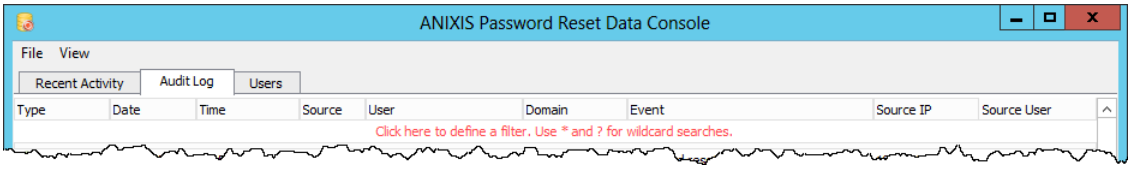
Filtering Data

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 focus on the important 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.

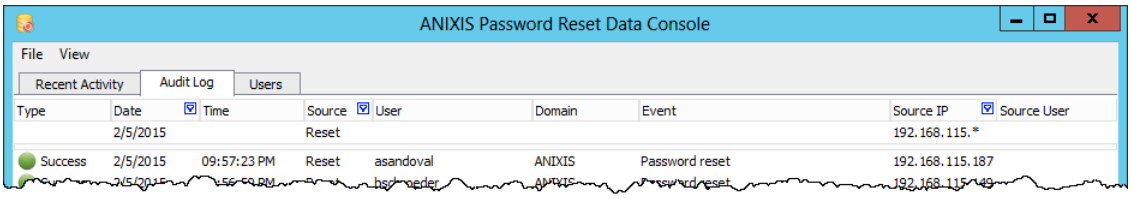
The Filter Row

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 shown an editor or selector that helps you enter a value. Values can include wildcard characters. Use a ? to match any single character, or a * to match more than one character.



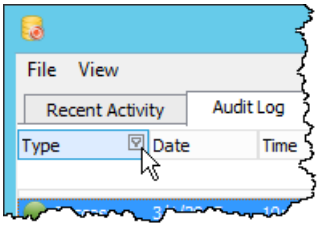
The image above shows a filter on the Date, Source, and Source IP columns. Only password reset events on 2/5/2015 originating from IP addresses starting with 192.168.115 are shown. The small blue icons in the column headers show which columns have active filters.

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

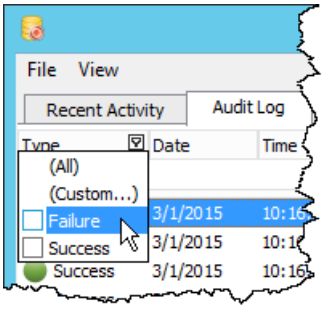
You can also create a filter by selecting values from a list in the column headers.

Hover the mouse pointer over a column header until a small button appears on the right side of the header.



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

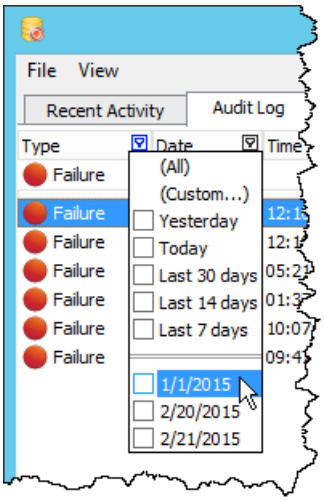
Select one or more values from the list. Rows that do not match one of the selected values are hidden.



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

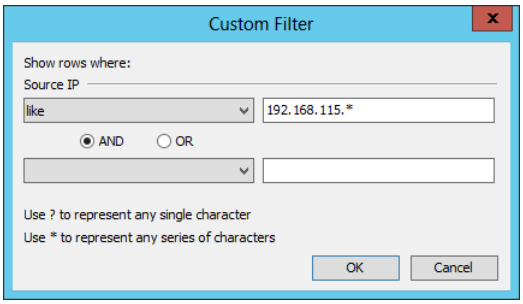
Click **(All)** to clear the filter and display all values.

Click **(Custom...)** to create a custom filter.



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 shown an editor or selector that will help you enter a value. Values can include wildcard characters. Use a ? to match any single character, or a * to match more than one character.

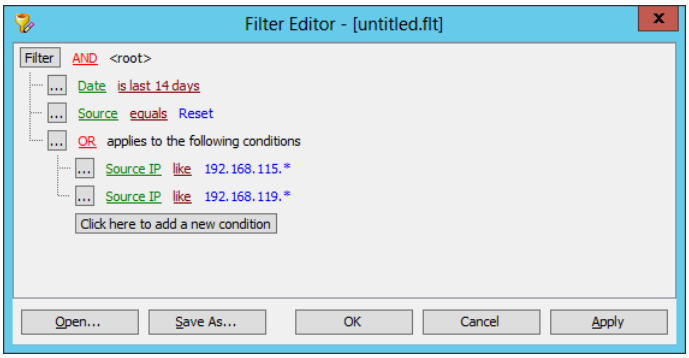
Select the **AND** or **OR** operator if the filter will have two conditions. Select **AND** if the filter should only show rows that meet both conditions. Select **OR** if the filter should show rows that meet either condition.

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.

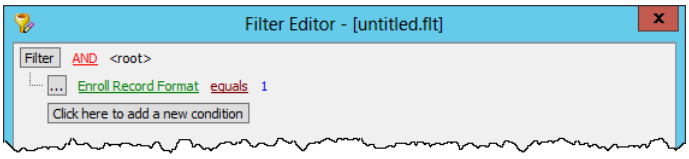
A filter also contains a root node and optionally one or more groups. These are used to include Boolean operators in the filter. Boolean operators are shown in red. Grouped conditions are indented.

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 ellipsis button on 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.

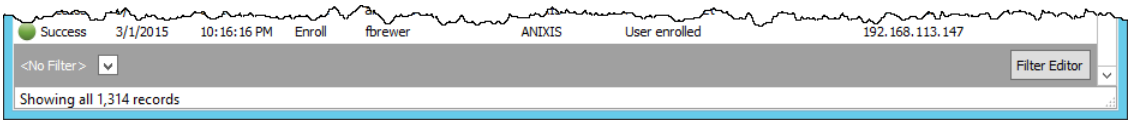
Click **Save As...** to save a filter to a file, or **Open...** to use a saved filter. Click **OK** to close the Filter Editor and apply the filter.

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.

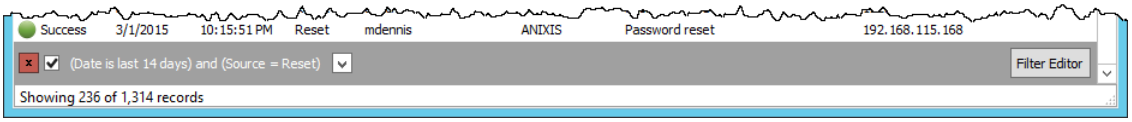


The Filter and Status Bars

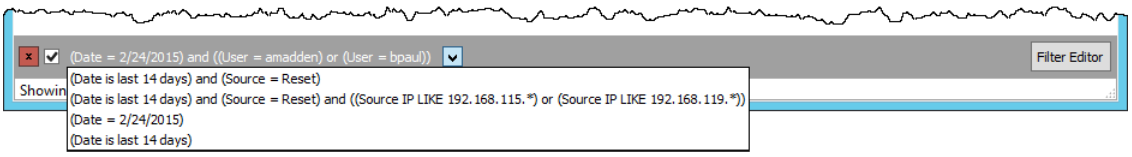
The Status Bar appears at the very bottom of the Data Console. It shows the number of visible records and the total record count. The Filter Bar appears above the Status Bar, and it shows the active filter. The button on the right side of the Filter Bar opens the Filter Editor.



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.



A drop-down button appears to the right of the filter. Click it to select a recently used filter.



Exporting Data

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

1. Click the **Audit Log** or **Users** tab.
2. Click the **File** menu, and then click one of the export menu items.
3. Type a filename, and then click **Save**.

When exporting to Excel, you can choose the file type from the **Export to Excel** window. The default file type is .xlsx.

Deleting Users

Users are automatically deleted from APR's database approximately one week after they are deleted from Active Directory. You can also manually delete users from the Data Console. To delete a user:

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

You can still view a user's event history in the **Audit Log** tab after they are deleted from the **Users** tab.

Working with the Database

The APR Server stores user and event information in a database. The default database is Microsoft SQL Server Compact, an embedded version of SQL Server. The benefits of using SQL Server Compact include:

- No manual installation or configuration required.
- No maintenance apart from database backups.
- Fast and lightweight.
- Free to use.

Despite these benefits, there are some disadvantages to using an embedded database. These can be overcome by moving the database to Microsoft SQL Server. The benefits of using SQL Server include:

- Remote access to the database from the Data Console and other applications.
- Improved availability if SQL Server is configured for high availability.
- Increased security.

Backing up the Database

The database should be backed up regularly. The instructions below are for an SQL Server Compact database. If using SQL Server, then use your backup software to backup the database. The recommended backup procedure is:

1. Close the Data Console if it is open.
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 (apr.sdf and aprlog.sdf) are in the APR Server's installation folder by default, but the location is configurable. The following commands create copies of the files with a .bak extension. Copy the .bak files to another device, and run the backup script 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 database files are 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 if it is open.
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.

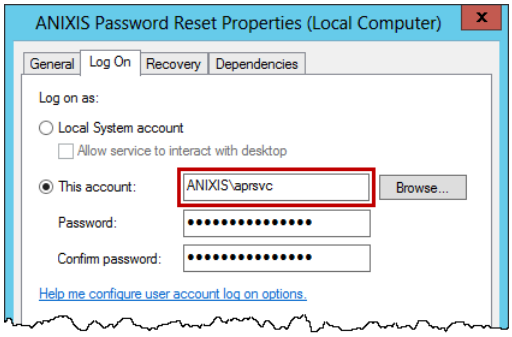
Moving to SQL Server

Some planning is needed before moving the database to SQL Server. A trial run on a lab network is recommended. You can run the Data Copy wizard more than once if you cannot complete the move on the first attempt. A move back to SQL Server Compact is also possible.

Create the Database

Your database administrator needs to set up the SQL Server database. The instructions below are an overview of the procedure, they are not step-by-step instructions. APR V3.23 has been tested with SQL Server 2012 to 2019.

1. Create an SQL Server database.
2. Create an SQL Server login for the APR service account, and configure it for Windows authentication. To identify the service account, open services.msc, double-click the **ANIXIS Password Reset** service, and then click the **Log On** tab. APR logs on to SQL Server with this account.



3. Create an SQL Server user, and map it to the service account login.
4. Add the SQL Server user to the db_datareader, db_datawriter, and db_ddladmin server roles for the database.

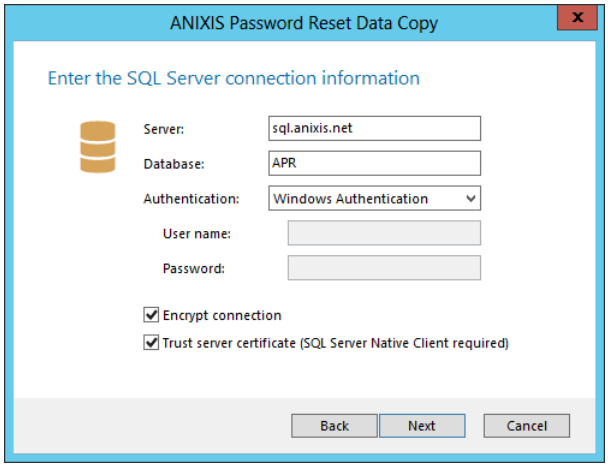
Your database administrator also needs to grant access to the users that will use the Data Console. These users only need to be added to the db_datareader server role, and they can be denied access to the VerificationCode and EnrollRecord columns in the Usr table. The user running the Data Copy wizard also needs to be added to the db_datawriter and db_ddladmin server roles.

Additional permissions can be set for users of the Data Console after the tables are created. Grant the DELETE privilege on the Usr table to users who are allowed to delete user records. Deny all privileges on the VerificationCode and EnrollRecord columns in the Usr table as they are not used by the Data Console.

Create the Tables and Copy the Data

The Data Copy wizard creates the database tables and copies the data to SQL Server. You must run the wizard even if the SQL Server Compact database is empty. Data in the destination database is deleted before it is copied from the source database. To create the tables and copy the data:

1. Open the Configuration Console.
2. Click the **General** tab.
3. Click **Copy Data...** to open the Data Copy wizard.
4. Click **Copy from SQL Compact to SQL Server**.
5. Check the path to the SQL Server Compact database files. If the default path is incorrect, then click **Browse...**, choose a path, and then click **OK**.
6. Click **Next**.
7. Set the SQL Server connection settings for the Data Copy wizard. You can set different connection settings for the service account later. The **User name** and **Password** are only needed if **SQL Server Authentication** is selected. The user must be in the db_datareader, db_datawriter, and db_ddladmin SQL Server roles. **Encrypt connection** should be selected to protect user information, and **Trust server certificate** must be selected if SQL Server is using a self-signed certificate. SQL Server uses a self-signed certificate if a trusted certificate is not installed. The SQL Server Native Client must be installed if **Trust server certificate** is selected.



8. Click **Next**.
9. Check the summary information, and then click **Start**.
10. Wait for the wizard to finish, and then click **Close**.

Configure APR to Connect to SQL Server

Configure APR to connect to SQL Server immediately after copying the data. If the cutover is delayed, then run the Data Copy wizard again to update the SQL Server database with the latest data. To configure APR to connect to SQL Server:

1. Open the Configuration Console.
2. Click the **General** tab.
3. Click **Change...**
4. Select the **SQL Server** option.
5. Type the server name in the **Server** text box. Use [server]\[instance] to connect to a named instance.
6. Type the database name in the **Database** text box.
7. Select the **Encrypt connection** option to encrypt the connection to SQL Server. This option should be selected to protect user information.
8. Select the **Trust server certificate** option if SQL Server is using a self-signed certificate. SQL Server uses a self-signed certificate if a trusted certificate is not installed. APR cannot connect to SQL Server with a self-signed certificate if this option is not selected. The SQL Server Native Client must be installed if **Trust server certificate** is selected.
9. Click **OK**, and then click **Apply**.
10. Restart the "ANIXIS Password Reset" service. If the service does not start, then check the database connection options and the SQL Server login, user, and server roles configured earlier. You can change the database back to SQL Server Compact while you troubleshoot the issue.

Other Tasks

Open the Data Console and set your SQL Server connection options. You will need to enter a password every time you open the Data Console if **SQL Server Authentication** is selected. The Data Console executable and help file (APRDC.exe and APR.chm) can be copied to the computers of other users who will use the Data Console.

Delete the two SQL Server Compact database files (apr.sdf and aprlog.sdf) after cutting over to SQL Server. These files will soon contain outdated information, and leaving them on the server is an unnecessary security risk. Also ensure that the SQL Server database is backed up regularly.

Securing APR

APR has many inbuilt security features, but there are some things you should do to secure APR. 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. You can install the Web Interface on a server that already has an SSL certificate if you would rather not purchase another one.

Your certificate authority will have instructions to guide you through the certificate request and installation process. You can also learn more about using SSL certificates with IIS on these two pages:
http://www.iis.net/learn/manage/configuring-security/how-to-set-up-ssl-on-iis
http://technet.microsoft.com/en-us/library/cc732230(WS.10).aspx

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 the graphical user interface. The examples below use the command-line, but you can use either method. 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. Both commands are required even if the Unlock item is hidden from the menu because APR automatically unlocks an account when its password is reset. The third command allows APR to set "User must change password at next logon" 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"
```

If APR is configured to use an SQL Server Compact database, then give the service account read and write permissions to the database files.

Remove the service account from the Domain Admins group and restart the "ANIXIS Password Reset" service after executing these commands. Check the Windows Application event log if the service does not start.

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. The restored permissions do not allow APR to reset passwords or unlock accounts for these users.

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:

```
dsacls "[AdminSDHolder]" /G "[account]:CA;Reset Password"
dsacls "[AdminSDHolder]" /G "[account]:RPWP;lockoutTime"
dsacls "[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. The templates are written in HTML5 and formatted with CSS3, so they work with all modern web browsers. Older browsers such as Internet Explorer 8 may work, but the pages may be badly formatted. Send an e-mail to support@anixis.com if you need to use APR with older web browsers.

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 formatting information is in apr.css, and 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.

Web browsers display pages differently, so test your changes with several versions of the most popular browsers to ensure compatibility.

Ranges and Fields

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 box.
@RES_EMPTY_FIELD_DOMAIN:    Enter your domain name in the Domain box.

--><!--/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.

Responsive Content

APR's templates are responsive. The page layout and content changes to suit the user's screen size. The layout is defined in the CSS file, and the content in the HTML files. The text_short and text_long classes are used to display different content depending on the screen size. text_short elements are shown on small screens (up to 420 pixels wide). text_long elements are shown on larger screens.

You may rebrand the APR user interface, but it is a violation of the License Agreement to modify, remove or obscure any copyright notice.

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 at the top of the page. The logo is installed into the \Inetpub\wwwroot\pwreset\images\ folder by default, and it is called logo.svg. You can replace this file with one containing your organization's logo.

You will also need to edit the HTML files if your logo is not in SVG format, or if it has a different aspect ratio to the ANIXIS logo. Open every HTML file in a text editor such as Notepad, and search for the line shown below. Change the filename (logo.svg), height (70 pixels) and width (116 pixels) to suit your logo.

```
<img class="logo" src="images/logo.svg" height="70" width="116"
alt="ANIXIS" onerror="this.style.display='none';">
```

Edit Page Instructions

Instructions appear at the top of each page. You can edit the instructions by opening the relevant .htm file and searching for the text you wish to modify.

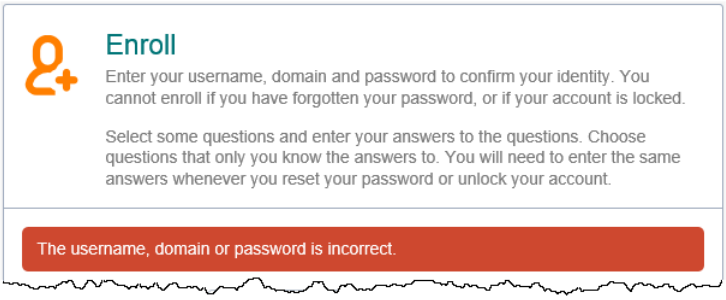
Instructions are often inside a range called SECTION_A, SECTION_B, SECTION_C, or SECTION_D. Each section contains instructions for the different pages in the template. Make sure you edit the instructions in the correct section, or they may be displayed on the wrong page. The text_long and text_short classes are used in page instructions to tailor content to the screen size.

```
<!--SECTION_A-->
     <p>Enter your username and domain, and then click Next to continue…
     <p class="text_long">Use the reset feature if you have forgotten y…
<!--/SECTION_A-->

<!--SECTION_B-->
     <p>Answer the question below to confirm your identity. Your answer…
     <p class="text_long">You may need to answer additional questions b…
<!--/SECTION_B-->
```

Edit Validation Error Messages

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



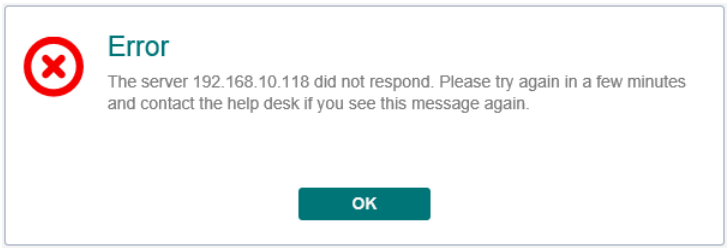
Validation error messages are defined in the relevant template (en_enroll.htm, en_reset.htm, en_unlock.htm, or en_change.htm). The error messages are in the resource strings section near the end of the file. Some messages are defined in more than one file, so you may need to edit several files to change 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, but you can delete them if you do not want them.

```
@RES_EMPTY_FIELD_EMAIL:    Enter your e-mail address in the E-mail box.
@RES_EMPTY_FIELD_QUESTION: Select a question from the Question %1 list.
@RES_IDENTICAL_QUESTIONS:  Question %1 and %2 are the same. Select a di…
```

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, but you can delete them if you do not want them.

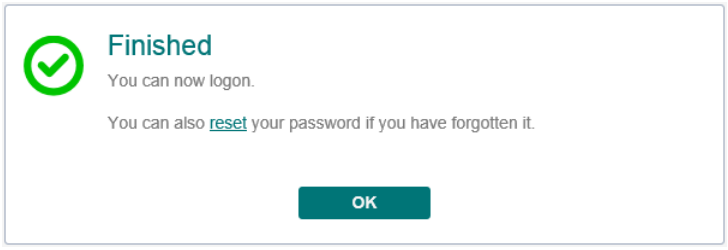
```
@RES_LOCKED_OUT:     This feature has been disabled because too many qu…
@RES_LOCKED_OUT_AD:  Your account is locked because an incorrect passwo…
@RES_REQUEST_FAILED: The server %1 could not handle your request. Pleas…
```

If you want to display some text for all error messages, then insert your text above or below the " <!--ERROR--> " 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 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="field_question_list" name="q1" id="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="field_question" name="q1" id="q1" value="<!--Q1-->"
maxlength="64">
```

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 the user interface formatting information. You can 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:

```
.apr_form .error {
     background-color: #CE482F;
     border-radius: 5px;
     color: #FFF;
     margin: 0 15px 15px;
     padding: 10px 13px;
}
```

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.

Change Icon Colors

The Web Interface icons are in Scalable Vector Graphics (SVG) format. Vector graphics maintain their sharpness when resized. You can easily change the colors of the icons with a text editor. Open the SVG file with a text editor like Notepad, and edit this section of the file:

```
fill="#FF7F00"
```

Replace the hexadecimal color code with your desired color code. You can use a color picker like this one to generate the color code:
https://www.w3schools.com/colors/colors_picker.asp

Some old web browsers with basic HTML5 support cannot display SVG images. APR works with these browsers, but the SVG images are not shown. You can convert the icons to GIF or PNG format if you want them shown on these older browsers.

The Password Reset Client

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

The Password Reset Client does not modify any Windows system files.

Installing the PRC

The Password Reset Client is designed to run on Windows XP to Windows 10, and Server 2003 to Server 2019. The PRC is compatible with Remote Desktop Services on these operating systems. Support for Windows XP and Server 2003 is depreciated because the PRC uses Internet Explorer for page rendering, and Internet Explorer 8 has very limited support for HTML5. Send an e-mail to support@anixis.com if you need to use the Password Reset Client with these older operating systems.

System Requirements

- Windows Vista, 7, 8, 8.1, or 10.
  Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, or 2019.
  Windows XP, Server 2003, or 2003 R2 (depreciated).
- 1 Megabyte free disk space.
- 128 Kilobytes free RAM (per session if using Remote Desktop 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.

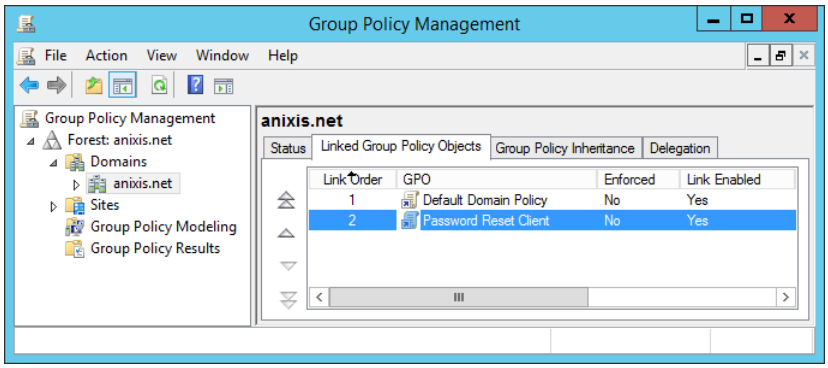
Create a Distribution Point

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 APRClt323.msi into the distribution point folder. APRClt323.msi is in the "Client" folder below the APR Server's installation folder. (\Program Files\ANIXIS Password Reset\ by default).
5. Give the "Domain Computers" security group read access to the APRClt323.msi file in the distribution point.

Create a Group Policy Object

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...**
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**, and **Software Settings** items in the left pane.
3. Right-click the **Software installation** item, and then select **New > Package...**
4. Type the full UNC path to APRClt323.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\APRClt323.msi
5. Click **Open**.
6. Select the **Assigned** deployment method, and then click **OK**.
7. Close the Group Policy Management Editor.

Complete the Installation

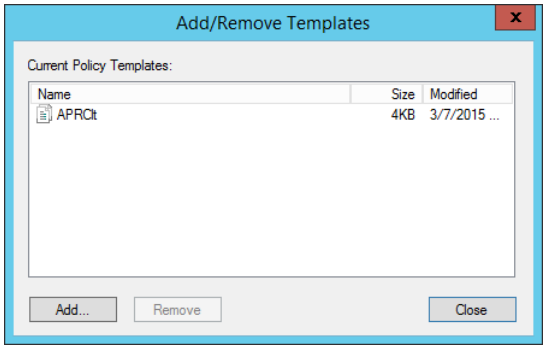
Restart each computer to complete the installation. Windows installs the Password Reset Client during startup. The computer may restart itself automatically to complete the installation.

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:

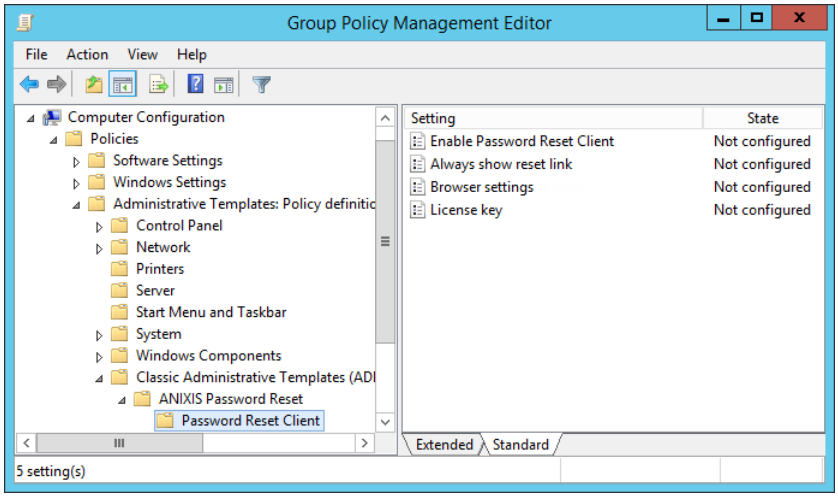
1. Use the Group Policy Management Console (gpmc.msc) to display the GPOs linked at the domain level.
2. Right-click the **Password Reset Client** GPO, and then click **Edit...**
3. Expand the **Computer Configuration** item.
4. Expand the **Policies** item if it is visible.
5. Right-click the **Administrative 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\ANIXIS Password Reset\ by default).
7. Select **APRClt.adm**, and then click **Open**.



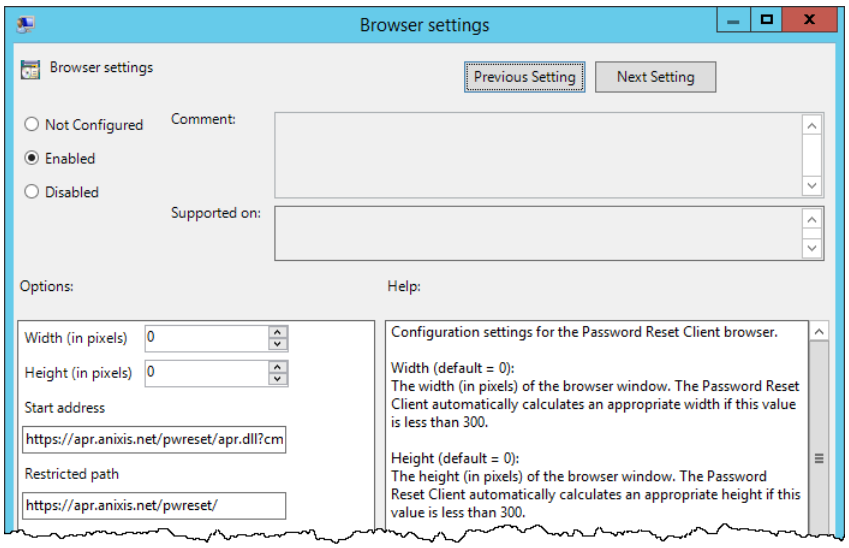
8. Click **Close**.

To configure the Password Reset Client:

1. Use the Group Policy Management Console (gpmc.msc) 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 it exists), **Administrative Templates**, **Classic Administrative Templates (ADM)**, **ANIXIS Password Reset**, and **Password Reset Client** items.
4. Double-click the **Browser settings** item in the right pane of the Group Policy Management Editor.



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 should point to the APR menu or reset page. See the **Help** box 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 Management 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: gpupdate /target:computer

The Password Reset Client only opens URLs with .dll, .htm, and .html extensions. URLs without a filename are not opened. The PRC also blocks some page content, including audio and video files, ActiveX controls and Java applets. Send an e-mail to support@anixis.com if you need to change the default filename and content restrictions.

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. The start address and restricted path should both begin with https://

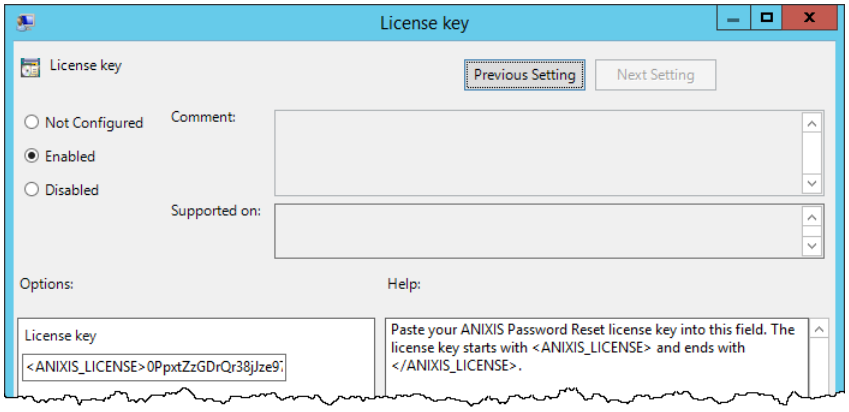
The **Enable Password Reset Client**, **Always show reset link**, and **Dialog attachment delay** are automatically set by the Password Reset Client, and are normally left in their default (Not configured) state.

The administrative template contains detailed information about all the PRC configuration settings. This information is shown on the **Help** box. The **Help** box is shown after you double-click one of the configuration settings in the right pane.

Licensing the PRC

To add a license key to the PRC configuration:

1. Open the 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 **3.0** 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 (gpmc.msc) 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 it exists), **Administrative Templates**, **Classic Administrative Templates (ADM)**, **ANIXIS Password Reset**, and **Password Reset Client** items.
8. Double-click the **License key** item in the right pane of the Group Policy Management 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 Management 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: gpupdate /target:computer

Persuading Users to Enroll

The Web Interface includes a REST API which your web sites and applications can query to determine if a user is enrolled. Your web site or application can take appropriate action to encourage the user to enroll. This could be anything from displaying a discreet message to denying access until the user enrolls.

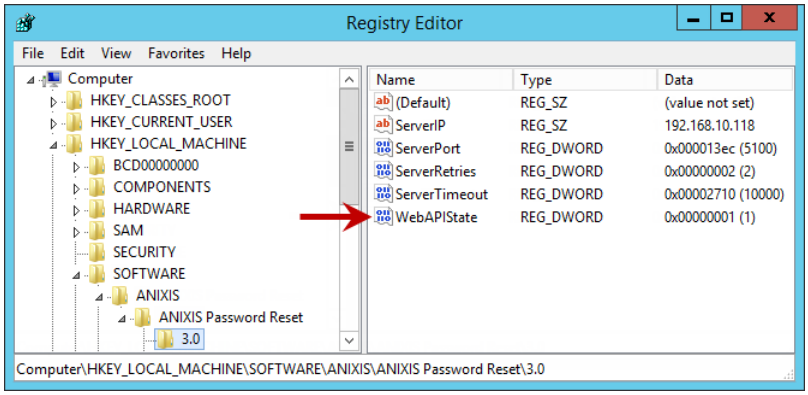
Enabling the API

The API is disabled by default. If an attacker sends many queries to the API, they could try to guess the domain and user names of enrolled users. They could get the same information by sending many requests to the Web Interface, but the API is a more attractive target because:

- The API responds faster.
- API queries are not logged to the Audit Log.

If you do not want to enable the API because your Web Interface is accessible from the Internet, then you could leave the API disabled on your Internet-facing Web Interface and set up an internal Web Interface for API queries. Use the ServerIP registry value to point both Web Interfaces to the same APR Server, and enable the API only on the internal server. To enable the API:

1. Start the Registry Editor (regedit.exe).
2. Expand the **HKEY_LOCAL_MACHINE**, **SOFTWARE**, **ANIXIS**, **ANIXIS Password Reset**, and **3.0** registry keys.
3. Create a new DWORD value called **WebAPIState**, and set it to 1.



Querying the API

Send a GET request with the user's Active Directory domain and user name like:

```
GET https://[server]/pwreset/apr.dll/api/enrollments/[domain]/[user]
```

You can also use the User Principal Name (UPN):

```
GET https://[server]/pwreset/apr.dll/api/enrollments/upn/[user@domain]
```

Interpreting the Response

There are three possible responses:

Response	Meaning
{"isEnrolled": true}	User is enrolled
{"isEnrolled": false}	User is not enrolled or does not exist
{}	System maintenance is running

The API may also return one of these HTTP errors:

Error	Reason
400 Bad Request	Invalid request path
403 Forbidden	API disabled, or cannot read configuration
500 Internal Server Error	Other error

Performance and Caching

API performance is dependent on many factors. Synchronous queries will suffice in most cases, but asynchronous queries are recommended to avoid delays. Avoid unnecessary calls to the API as they can overload the server. Try to call the API only once after users logon.

Caching improves performance and increases capacity. When the API sends a "user is enrolled" response, it requests caching for up to two weeks. The web browser should cache the response and use it for the next two weeks before querying the server again. No caching is requested for other responses.

You may get a "user is enrolled" response after deleting an enrolled user when testing the API. Clearing the browser cache may fix this, but not if other HTTP caches have cached the response.

License Agreement

ANIXIS PTY LTD ("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 V3.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) modify, remove or obscure any copyright, trademark or other 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' 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' 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 PTY LTD, 9 Monteray Terrace, Glenmore Park, NSW 2745 Australia.