



ANIXIS Password Reset

V1.0

Administrator's Guide

© Copyright 2003 ANIXIS. All rights reserved.

ANIXIS Password Reset, Password Policy Enforcer, Password Policy Server, Password Policy Client and Password Policy Protocol are trademarks of ANIXIS. Microsoft, Windows, Windows 95, Windows 98, Windows 2000, Windows 2003, Windows NT and Windows Installer are either registered trademarks or trademarks of Microsoft Corporation. RSA is a registered trademark of RSA Security Inc. Other product and company names may be the trademarks of their respective owners.

Contents

Introduction	1
Documentation	2
Evaluating ANIXIS Password Reset	2
Concepts and Planning	3
Installation types	4
Single computer installation	4
Multiple computer installation	4
Installing APR	5
System requirements	5
The APR Installation Wizard	6
Configuring IIS6 (Windows Server 2003 only)	9
Configuring the APR Server	11
Domain list	11
Password Policy Enforcer	12
Question list	13
Enroll question count	13
Auditing	14
Expire password after reset	15
Enrollment record lockout	15
Remotely configuring an APR Server	16
Configuring the Web Interface	17
Using APR	18
Enroll	19
User errors	19
System errors	19
Reset password	20
Unlock account	21
Change password	22
Backing up the data store	23

Security and Encryption	24
Securing APR	25
Enable HTTPS	25
Install the latest software updates	25
Set folder security	26
Set registry security	26
Encryption	27
Troubleshooting	28
Installation Wizard	28
Web Interface	28
System Errors	29
Technical support	30
License Agreement	31

Introduction

ANIXIS Password Reset (APR) is a self-service password management system that allows users to change their password and unlock their account, even if they have forgotten their current password. APR authenticates users who have forgotten their password by asking them to answer some questions about themselves.

The benefits of using APR over traditional password management procedures include:

Reduced costs – Various research groups have conducted studies into the costs associated with password management. The results vary, however the consensus is that between 20% and 40% of all helpdesk calls are password management issues. Organizations that implement APR can expect a very quick return on investment.

Increased productivity – Employees cannot perform their duties while waiting in the helpdesk telephone queue for their password to be reset. APR allows these users to reset their own password and carry on with their work. An additional benefit is that helpdesk waiting times are reduced when users manage their own passwords.

Improved security – Helpdesk staff are often unable to positively identify a caller, especially in large organizations with centralized helpdesks. APR uses a challenge/response system that makes it difficult to impersonate another person.

Improved manageability – Automating and centralizing password management functions ensures that corporate policies are enforced consistently. APR's integrated auditing also allows network administrators to monitor password management activity.

Improved availability – APR can handle password management requests 24 hours a day. The system scales well and can serve the needs of thousands of users.

Documentation

This Administrator's Guide contains detailed information on installing, configuring and using APR.

The [APR Evaluator's Guide](#) contains step-by-step instructions to quickly guide you through the installation and configuration process. Refer to the Evaluator's Guide if you are evaluating APR to determine if it meets your requirements.



APR is compatible with Windows NT 4, Windows 2000, Windows XP and Windows Server 2003. This document collectively refers to these operating systems as "Windows".

Evaluating ANIXIS Password Reset

The [License Agreement](#) allows organizations to evaluate APR for up to 30 days without purchasing a license. You are permitted to install APR on any number of computers during the evaluation period.

Organizations that purchase an APR license are sent a license file that activates the installed copy. There is no need to reinstall APR after purchasing a license.

APR will stop working after the 30-day evaluation period has expired. If you are still evaluating APR after 30 days, send an email to support@anixis.com requesting an extended evaluation period.

Concepts and Planning

The APR package contains two software components, the Web Interface and the APR Server.

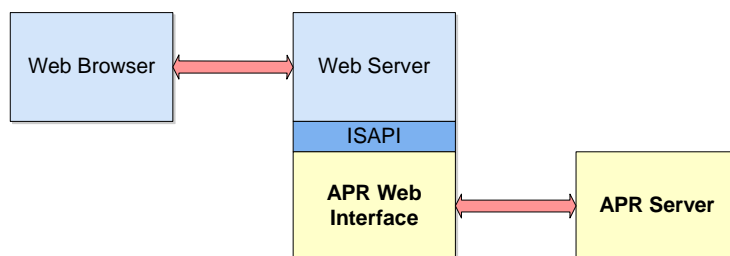
Web Interface

The Web Interface is an Internet Server API (ISAPI) extension that resides on a Web server. Users interact with the Web Interface via their Web browser. The Web Interface encrypts user requests and submits them to the APR Server for processing.

APR Server

The APR Server is a Windows service application that handles password management requests. The APR Server also maintains the data store, a repository for data collected during user enrollments.

The diagram below shows how the system components interact.



It is possible to install the APR Server onto a Windows workstation operating system. Installation of the Web Interface onto a workstation operating system is also possible, but not recommended due to the concurrent connection restrictions imposed by the operating system.

Installation types

The Web Interface and APR Server can either be installed onto a single computer, or distributed amongst several computers. Network administrators can choose the configuration that best suits their requirements.

Single computer installation

This is the preferred option for most networks. Both the Web Interface and APR Server are installed onto one computer. A single computer installation can serve the needs of several thousand users as long as the initial user enrollments are staggered.

Advantages:

- Easier to install and configure.
- Faster response (no network overhead for communication between components).

Disadvantages:

- System load placed on one computer.

Multiple computer installation

A multiple computer installation requires some additional configuration ([more information](#)), however it is a more flexible option that suits some networks better than a single computer installation. In a multiple computer installation, one or more Web Interface computers send requests to an APR Server.

Advantages:

- Handles more complex requirements. For example, the Web Interface can be installed in a DMZ while the APR Server remains safely behind the firewall.
- Greater load handling capacity.
- Improved availability (if multiple Web Interfaces are installed).

Disadvantages:

- More work to install and configure.
- Slightly slower response times due to network overhead.



The installation type can easily be changed after APR is installed. Administrators that are concerned about server load should choose a single computer installation and then convert to a multiple computer installation if necessary.

Installing APR

System requirements

- Windows NT ¹, 2000, XP or 2003 Server.
- 5 Megabytes free disk space.
- 16 Megabytes free RAM.
- Internet Information Server ², or other Web server capable of calling ISAPI extensions.

¹ Windows NT V4 with Service Pack 5 or later recommended

² IIS V4 or later recommended



Only administrators can install APR. Logon with administrative privileges before continuing.

If you are using Microsoft IIS to host the Web Interface, install and test IIS before installing APR. The APR Installation Wizard automatically configures IIS if it is detected during installation.

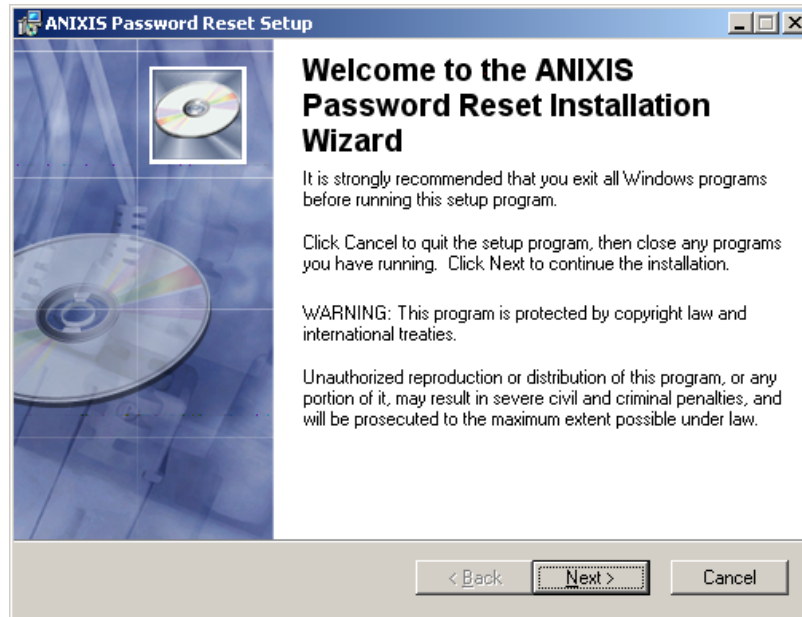
If you are not using IIS to host the Web Interface, send an email to support@anixis.com for additional information.



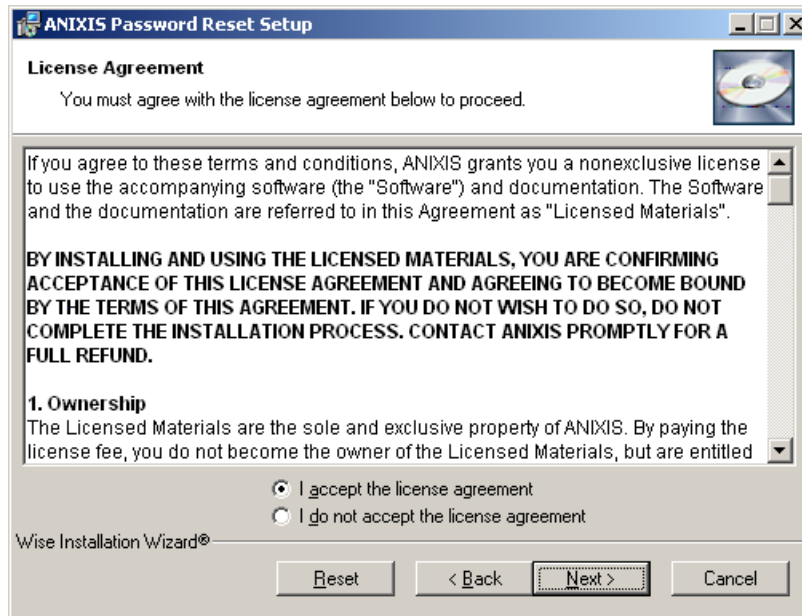
The [Security and Encryption](#) section contains important information about the HTTPS protocol. Do not use APR on a production network until you have enabled HTTPS.

The APR Installation Wizard

Start the APR Installation Wizard by running APRnn.EXE (where nn is the APR version number). Click the **Next** button to continue.

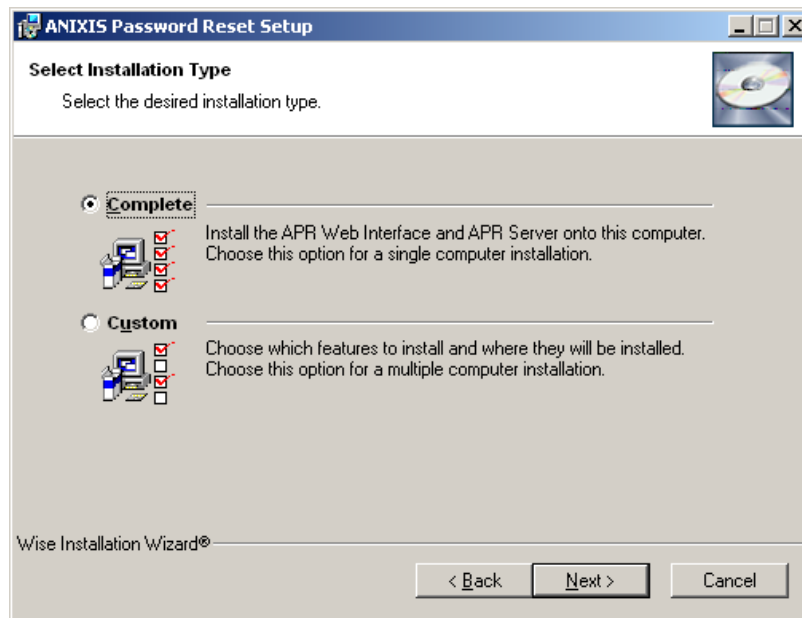


You must agree to the terms of the APR License Agreement to continue the installation.



Click the **Next** button to display the Readme page. The Readme contains the most up-to-date information about APR. Read this information carefully and click the **Next** button.

The APR Installation Wizard will ask you to choose the installation type. Select the **Complete** option for a [single computer installation](#), or the **Custom** option for a [multiple computer installation](#). Click the **Next** button to continue.



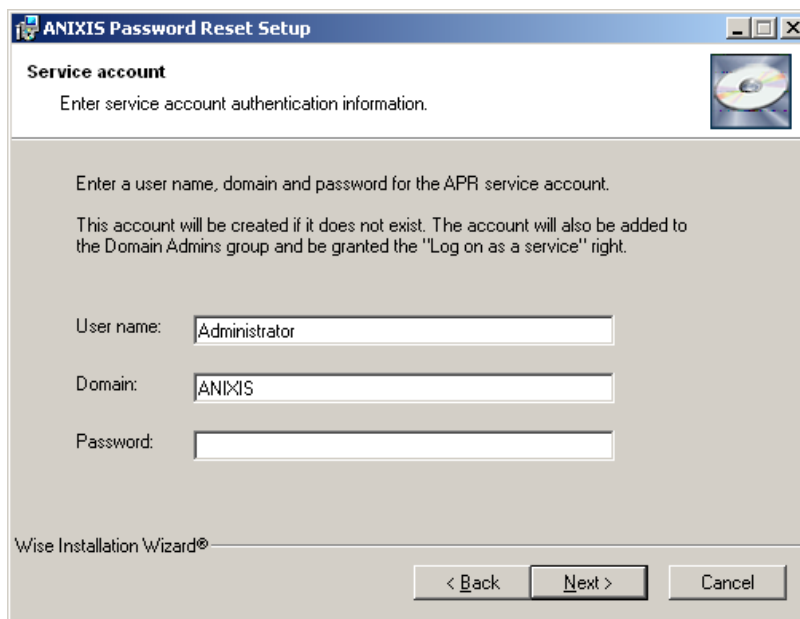
If you chose the custom installation type, the APR Installation Wizard will ask you to select the features that will be installed onto this computer. Install the **Server** feature if this computer will be an APR Server, or the **Web Interface** feature if this computer will host the Web Interface.

If the Server feature is being installed, the APR Installation Wizard will ask you to enter the **User name**, **Domain** and **Password** of the APR service account. This is the account that the APR Server uses to logon to the network.

The APR Server resets passwords on behalf of users, so it must have sufficient privileges to do this in all domains that this APR Server will service.

The APR Installation Wizard will create the service account if the specified user name does not exist in the domain. The APR Installation Wizard will also:

- Make the account a member of the Domain Admins group.
- Grant the “Log on as a service” right to the account.



ANIXIS Password Reset Setup

Service account
Enter service account authentication information.

Enter a user name, domain and password for the APR service account.
This account will be created if it does not exist. The account will also be added to the Domain Admins group and be granted the "Log on as a service" right.

User name:

Domain:

Password:

Wise Installation Wizard®

< Back Next > Cancel

Enter the authentication information for the APR service account and click the **Next** button to continue. Click the **Next** button again to start installing APR.



The APR Server creates a new data store when it starts for the first time. This process can take several minutes. Disk and CPU utilization will be high while the data store is created.

Uninstalling APR does not undo changes made to the APR service account. You should delete or modify this account manually if APR is uninstalled.

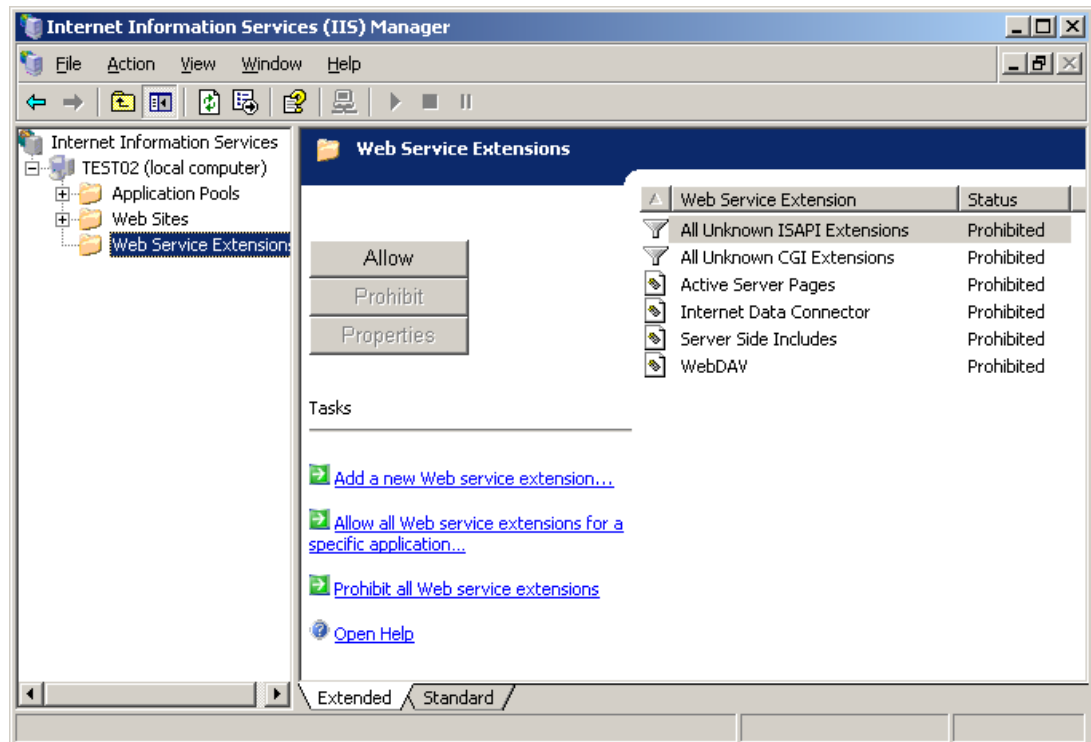
Configuring IIS6 (Windows Server 2003 only)

Windows Server 2003 includes version 6.0 of Internet Information Services (IIS6). IIS6 is installed in a secure “locked” mode by default and will not allow unknown ISAPI extensions to execute. You must manually configure IIS to allow the Web Interface to execute.



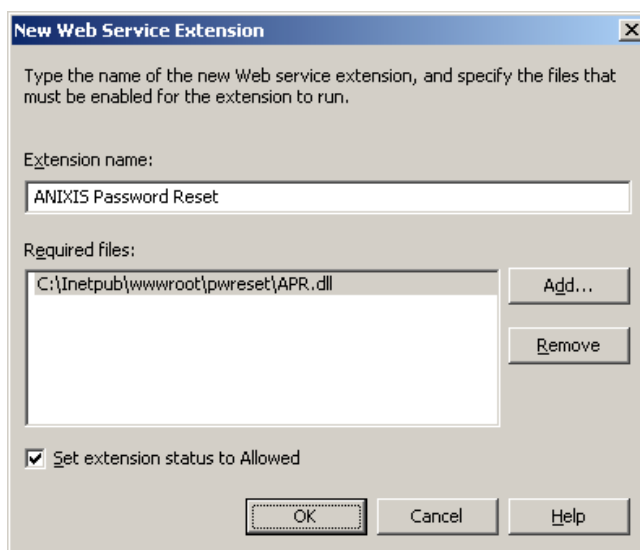
Skip this section if the computer is not running Windows Server 2003, or if the Web Interface was not installed (custom installation type with Web Interface feature disabled).

Select | **Start** | **Administrative Tools** | **Internet Information Services (IIS) Manager** | to open the IIS Manager console.



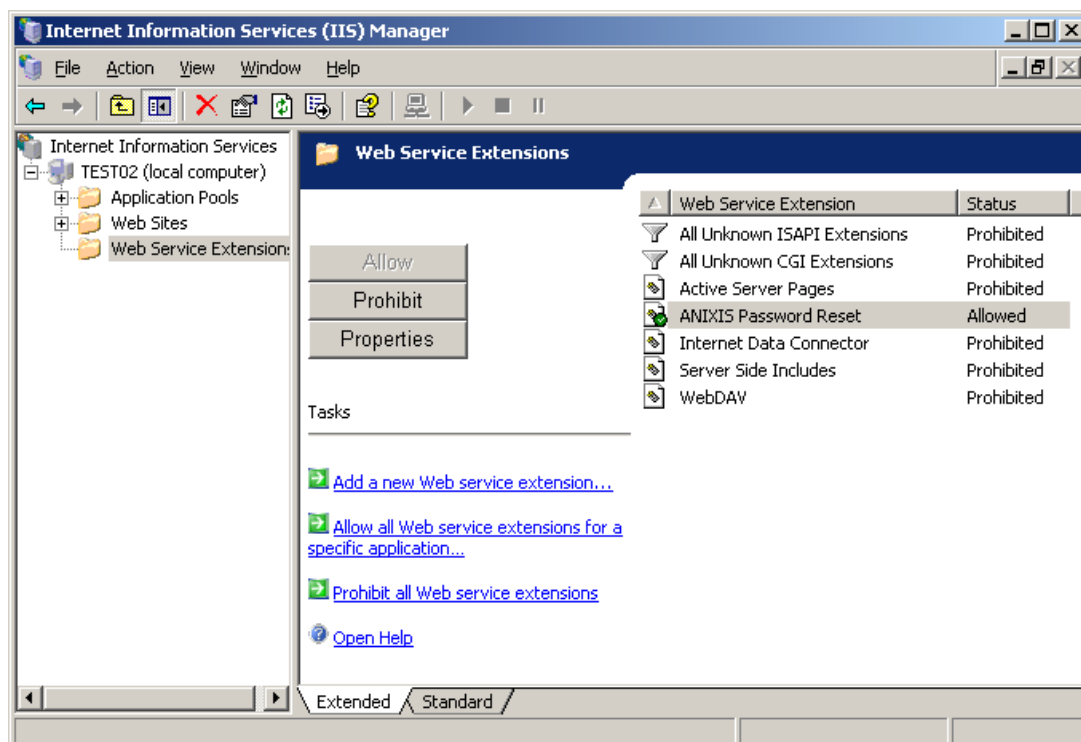
Select the **Web Service Extensions** item in the left pane of the IIS Manager console.

Click the **Add a new Web service extension...** task (right pane).



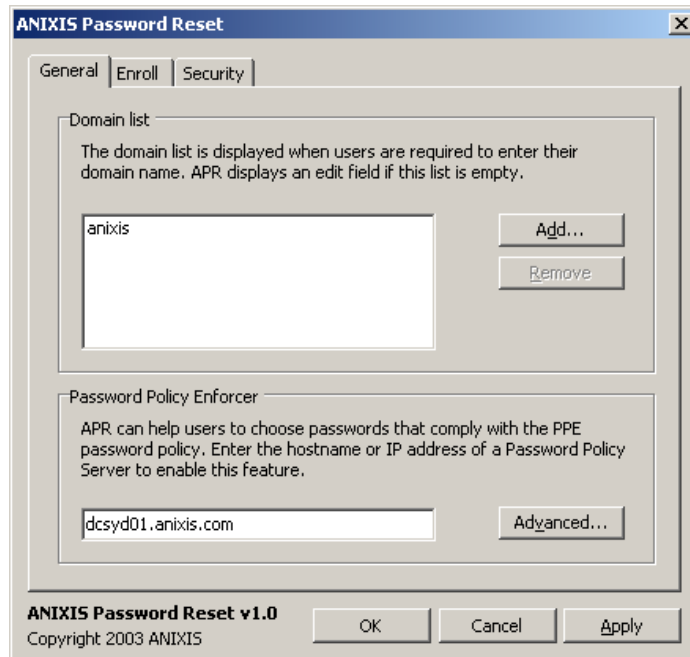
Enter “ANIXIS Password Reset” in the **Extension name** field. Click the **Add...** button and the **Browse...** button to display the open file dialog. Select APR.dll in the \inetpub\wwwroot\pwreset folder and click the **Open** button. Click the **OK** button.

Check the **Set extension status to Allowed** option and click the **OK** button to continue. The ANIXIS Password Reset extension should have its status set to “Allowed” as shown below.



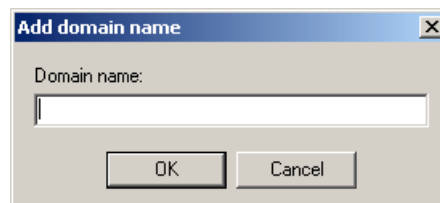
Configuring the APR Server

Select | Start | Programs | ANIXIS Password Reset | Configuration| to open the APR configuration program.



Domain list

The Web Interface displays an edit field whenever a user is required to enter their domain name. Administrators who would prefer to allow users to choose their domain from a dropdown list should add their domain names to the Domain list. Click the **Add...** button to add a new domain to the list. Enter the domain name and click **OK**.



Password Policy Enforcer

Password Policy Enforcer allows network administrators to create and enforce a password security policy. All new passwords are checked for compliance with the policy and any passwords that do not comply with the policy are rejected. Visit www.anixis.com/products/ppe/ for more information about Password Policy Enforcer.

APR can integrate with Password Policy Enforcer to make it easier for users to choose a password that complies with the password policy. APR does this by displaying the PPE Rejection Reason message when a password does not comply with the PPE policy.

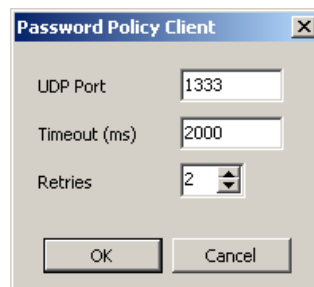
Enter the hostname or IP address of a Password Policy Server into the field provided to enable integration with Password Policy Enforcer.



Enter 127.0.0.1 if the Web Interface and Password Policy Server are both installed on the same computer.

APR is compatible with PPE V3.0 and later.

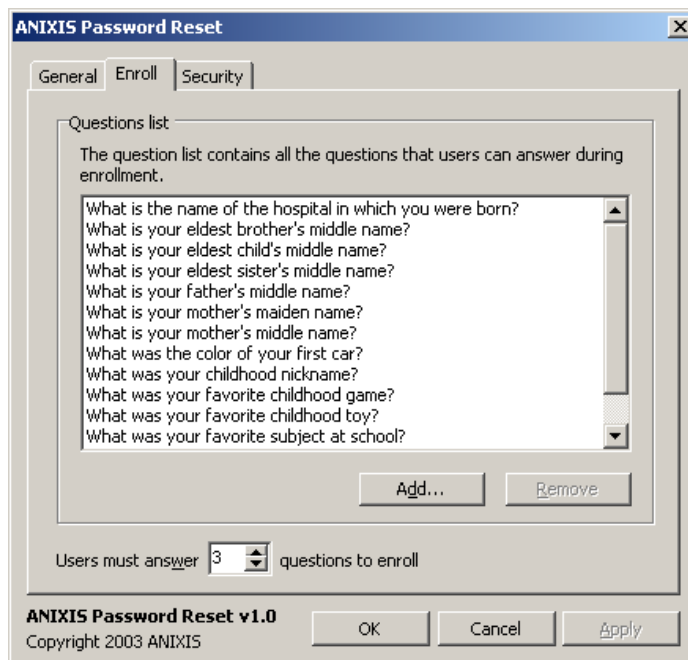
Click the **Advanced...** button to edit the Password Policy Client communications parameters. Refer to the [PPE Administrator's Guide](#) for more information about PPC communications parameters.



The Web Interface is a Password Policy Client and therefore uses the client dictionary file defined in the Dictionary rule properties page (PPE management console). Copy the client dictionary file onto the Web Interface computer if the PPE Dictionary rule is enabled.

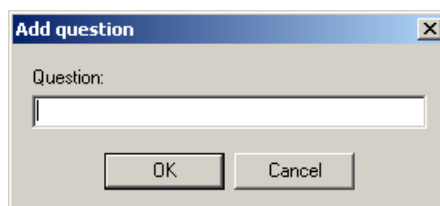
The [PPE Evaluator's Guide](#) and [PPE Administrator's Guide](#) contain more information about Password Policy Enforcer, the Password Policy Client and the client dictionary file.

Click the **Enroll** tab to display the enrollment properties page.



Question list

The Question list contains the questions that users can answer during enrollment. Click the **Add...** button to add a new question to the list. Enter the new question and click the **OK** button to continue.



To remove a question from the list, click the question to highlight it and then click the **Remove** button.

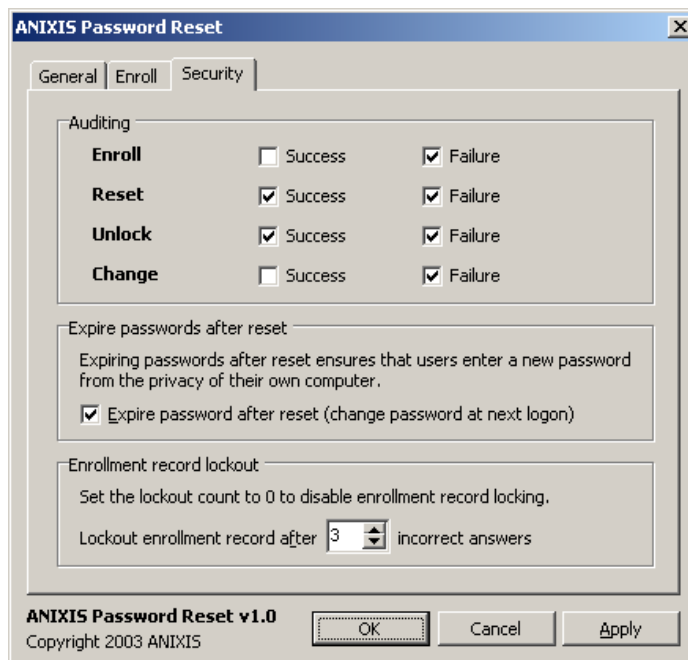


Removing a question removes it from future enrollments, but it does not have any impact on users that have already answered the question during a prior enrollment.

Enroll question count

The Enroll question count specifies how many questions a user must answer during enrollment. Specify the desired number of questions from 1 to 10. A higher question count makes it more difficult for a user to impersonate another user.

Click the **Security** tab to display the security properties page.



Auditing

The APR Server logs important events to the Windows Event Log. Check the desired options to enable auditing for an event. Both success and failure events can be logged.

For example, to write an event log entry whenever a user successfully resets their password with APR, check the **Success** option beside the **Reset** event. Check the **Failure** option to also log failed password reset attempts.



The APR Server writes audit events to the Application event log because it does not have permission to write to the Security event log. This occurs because the APR Server runs in the context of a domain account, and only the local system account has permission to write to the Security event log.

Expire password after reset

Checking the **Expire password after reset** option instructs APR to expire user passwords when they are reset. Windows will prompt users to choose a new password when they next logon to the network. Administrators may want to enable this option if users are accessing APR from a computer with limited privacy such as a colleague's computer, or a shared computer.



Passwords are not reset for accounts that have the "Password never expires" option enabled. Refer to the Windows documentation for more information about this option.

Enrollment record lockout

APR maintains an incorrect answer count for every enrollment record. The incorrect answer count is incremented whenever a user answers a question incorrectly during a password reset or account unlock.

APR locks an enrollment record if the incorrect answer count exceeds the enrollment record lockout threshold. Access to locked enrollment records is denied, so a user whose enrollment record is locked must contact the helpdesk to reset their password or unlock their account.

Specify the enrollment record lockout threshold in the field provided. A low value increases security, but also increases the likelihood of users accidentally locking themselves out due to typing errors.



Setting the enrollment record lockout threshold to 0 disables this feature. Disabling the enrollment record lockout feature is not recommended.

The incorrect answer count is reset to zero when the user answers all questions correctly (during a password reset or account unlock), or when the user re-enrolls.



The enrollment record lockout feature works independently from the Windows account lockout policy. APR does not lock a user's Windows account under any circumstances.

Remotely configuring an APR Server

The APR configuration program (APRConf.exe) can be copied onto an administrator's workstation and used to remotely configure an APR Server. To remotely configure a server, start APRConf.exe with the remote computer's UNC name as the first parameter. For example:

```
APRConf \\ServerName
```



Remotely configuring an APR Server from a Windows XP workstation

Configuring the Web Interface

The Web Interface is pre-configured for a [single computer installation](#). **Skip this page if the Web Interface and APR Server are both installed on one computer.**

Use the registry editor (regedit.exe) to open this registry key on the computer that is hosting the Web Interface:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ANIXIS\ANIXIS Password Reset\x.x
```

where x.x is the APR version number.

Double-click the **Server** registry value and enter the hostname or IP address of the computer that is running the APR Server. For example, apr.syd.anixis.com or 192.168.50.10



If the “Server” registry value does not exist, create a new value of type REG_SZ.

The APR Server can accept requests from more than one Web Interface. Configure each Web Interface computer to query the same APR Server if this type of configuration is required.

Click the **OK** button to store the updated value in the registry.

Using APR

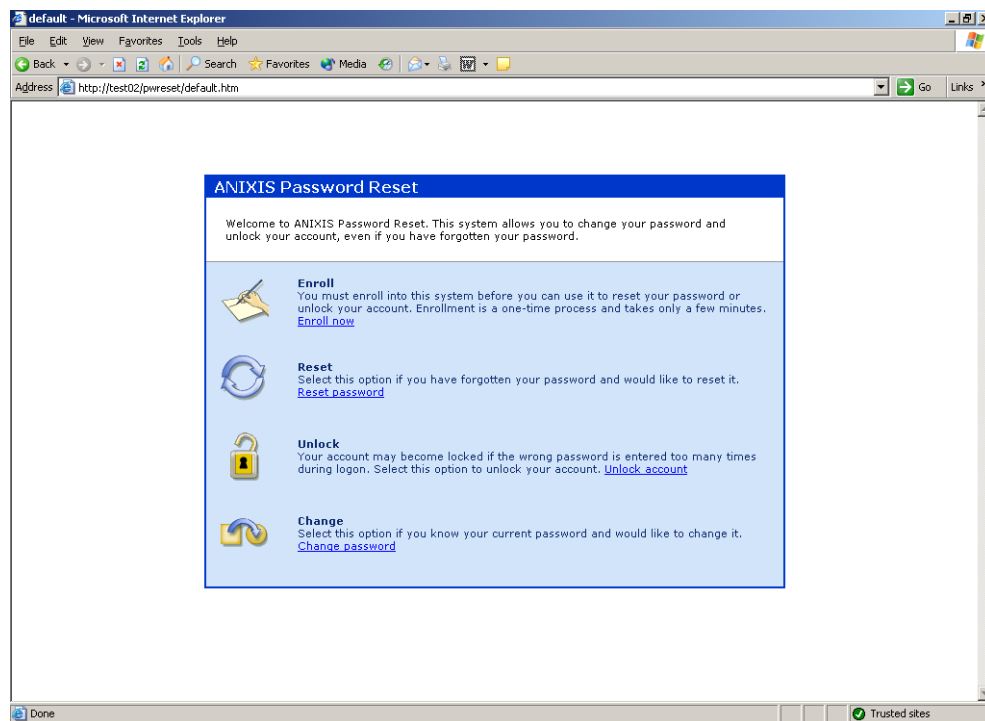
Users access the Web Interface from their Web browsers. The default URL for the Web Interface is:

`http://computer/pwreset/default.htm`

Replace `computer` in the URL above with the name or IP address of the computer that is hosting the Web Interface.



The Web Interface and APR Server both run on the same computer in a [single computer installation](#).



The APR main menu

Enroll

Users must enroll before they can use the Reset and Unlock features. Users only have to enroll once, however re-enrollment is required to:

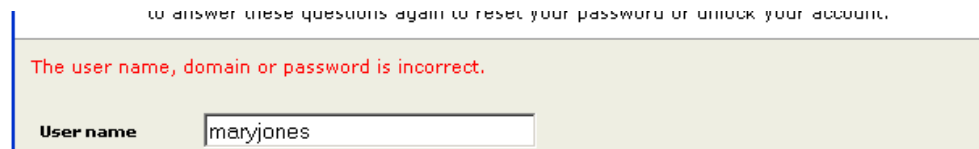
- change questions or answers.
- unlock an enrollment record (see [enrollment record lockout](#)).

Click the **Enroll** item in the main menu to enroll into APR.

Enter your **User name**, **Domain** and **Password** into the relevant fields. Select a **Question** from each of the dropdown lists and enter your **Answer** to each question in the field provided. A question cannot be selected more than once. Click the **Next** button to submit the enrollment form.

User errors

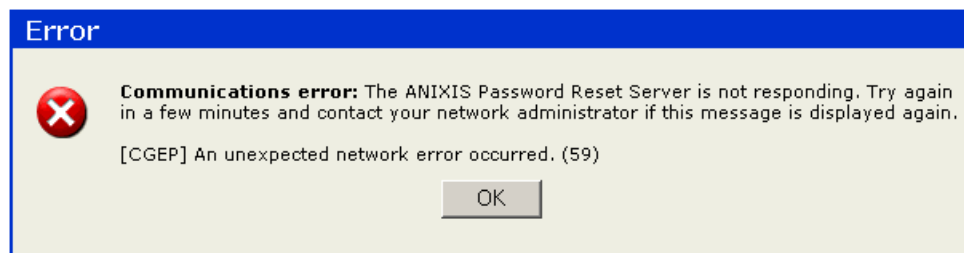
APR redisplay the enrollment form with an error message (in red) if a user error occurs. User errors are often caused by an invalid field value. If a user error occurs, correct the error and click the **Next** button to resubmit the form.



The screenshot shows a web form with a light green background. At the top, there is a small text prompt: "to answer these questions again to reset your password or unlock your account." Below this, a red error message reads: "The user name, domain or password is incorrect." Underneath the error message, there is a label "User name" followed by a text input field containing the text "maryjones".

System errors

APR displays a system error if it encounters a more serious problem. Only a network administrator can fix system errors. Refer to the [Troubleshooting](#) section for information on common system errors.



Reset password

The Reset feature allows users to reset a forgotten password. Click the **Reset** item in the main menu to reset your password.

Enter your **User name** and **Domain** into the relevant fields and click the **Next** button. APR will ask you to answer the first enrollment question. Enter the same **Answer** you entered during enrollment and click the **Next** button. Continue answering the questions until a form with two password fields is displayed.

Enter your new password into both fields and click the **Next** button to reset your password. APR displays an error message if the new password does not comply with the password policy rules.



The screenshot shows a dialog box titled "Reset" with a blue header. Below the header, there is an information icon and the text: "Enter your New password. You must enter the same password into both fields." Below this, a red error message states: "Your new password was rejected because it did not comply with the password policy." The error details are: "Your password was rejected because it: - did not contain a Uppercase Alpha character - did not contain a Numeric character - did not contain at least 7 characters". Below the error, the user's details are shown: "User name: maryjones" and "Domain: anixis". There are two input fields for "New password" and "Confirm password". At the bottom, there are "Cancel" and "Next >>" buttons.



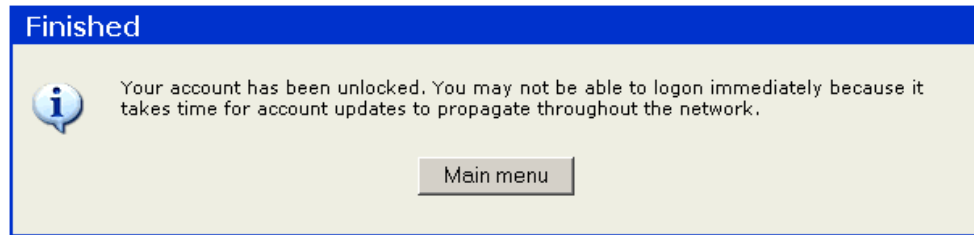
The Reset feature has a 60 second inactivity timeout. If a user takes longer than 60 seconds to answer a question, their session expires and they will have to start again.

Windows may lock out an account if the wrong password is entered too many times during logon. APR automatically unlocks an account when its password is reset.

Unlock account

The Unlock feature allows users to unlock their account. Windows may lock a user's account if the wrong password is entered too many times during logon. The Windows account lockout policy is not related to APR's [enrollment record lockout](#) feature. Click the **Unlock** item in the main menu to unlock your account.

Enter your **User name** and **Domain** into the relevant fields and click the **Next** button. APR will ask you to answer the first enrollment question. Enter the same **Answer** you entered during enrollment and click the **Next** button. Continue answering the questions until your account is unlocked.



The Unlock feature has a 60 second inactivity timeout. If a user takes longer than 60 seconds to answer a question, their session expires and they will have to start again.

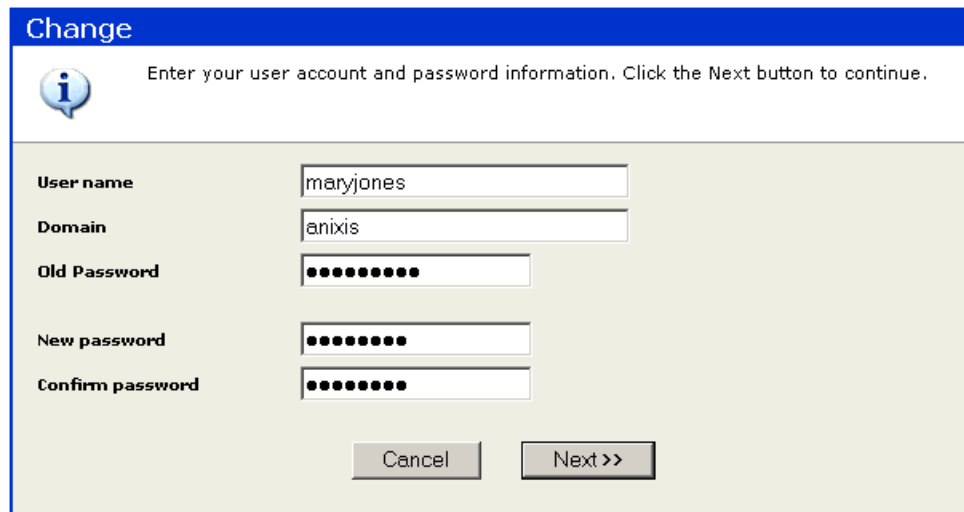
Repeatedly trying to enroll with the wrong password may also trigger the Windows account lockout policy.

Refer to your Windows documentation for information about the account lockout policy settings.

Change password

The Change feature allows users to change their password if they know their current password. Click the **Change** item in the main menu to change your password.

Enter your **User name**, **Domain** and **Old Password** into the relevant fields. Enter your new password into the **New password** and **Confirm password** fields.



Change

Enter your user account and password information. Click the Next button to continue.

User name

Domain

Old Password

New password

Confirm password

Click the **Next** button to change your password. APR displays an error message if the password does not comply with the password policy rules.

Backing up the data store

The APR Server stores user enrollment records in an encrypted database called the data store. The data store should be backed up regularly so that it can be restored after a hardware or software failure.

The APR Server exclusively locks the data store file while the service is running. Some backup programs have an open file option to backup locked files, however ANIXIS recommends the following backup procedure for the data store file:

- Stop the ANIXIS Password Reset service.
- Create a backup copy of the data store.
- Start the ANIXIS Password Reset service.
- Copy the backup data store to another device (e.g. Tape).

The following commands create a backup copy of the data store. These commands should be scheduled to run daily.



The copy command below assumes that the APR Server is installed in the "c:\program files\anixis password reset" folder. You may need to edit this path to suit your configuration.

```
net stop "ANIXIS Password Reset"  
  
copy /Y "c:\program files\anixis password reset\aprsvc.dat"  
        "c:\program files\anixis password reset\aprsvc.bak"  
  
net start "ANIXIS Password Reset"
```

The backup data store (aprsvc.bak) should be copied to another device after these commands have executed.



- To restore the data store from a backup device:
- Restore aprsvc.bak from the backup device.
 - Stop the ANIXIS Password Reset service.
 - Copy aprsvc.bak over aprsvc.dat.
 - Start the ANIXIS Password Reset service.
-

Security and Encryption

APR has many security features, some of which are transparent to the user and administrator. Four of these features are described below.

User answer hashing – User answers are the answers entered by users when they enroll, reset their password or unlock their account. APR protects user answers by converting them to a hash (an abstract representation of the answer). There is no known way to convert a hash back to the original answer. A brute force algorithm could discover the original answer, however this could take many years.

The original user answer is destroyed after the hash is calculated, so even APR has no record of the original answer. APR can still check answers though because a hash algorithm always has the same output for a given input. This allows APR to check user answers without having to store them.

Encrypted communications – Communications between the Web Interface and APR Server are encrypted with the [RSA](#) and [AES](#) encryption algorithms. Encryption keys are randomly generated at runtime, making it virtually impossible for an attacker to discover them.

Encrypted data store – The data store is encrypted with a derived AES key. Discovery of this key will not reveal user answers because only the hashes are kept in the data store, not the answers.

Limited one-way trust – Confidential information is allowed to pass from the Web Interface to the APR Server, but not in reverse. The one-way trust stops a compromised Web Interface from retrieving confidential information. It also allows the Web Interface to operate in a less secure environment such as a DMZ because all privileged operations are handled by the APR Server, not the Web Interface.

Securing APR

Despite APR's inherent security features, network administrators can modify the default configuration to further improve security.

Enable HTTPS

HTTPS is a secure version of the HTTP protocol used by Web browsers and servers. HTTPS uses public-key encryption to secure communications between the Web browser and server.

Refer to your Web server's documentation for more information about HTTPS (also known as Secure Sockets Layer or SSL). The links below contain information for users of Microsoft IIS.

About Encryption

www.microsoft.com/windows2000/en/server/iis/htm/core/iicrsc.htm

Enabling Encryption

www.microsoft.com/windows2000/en/server/iis/htm/core/iiecrsc.htm

Setting Encryption Strength

www.microsoft.com/windows2000/en/server/iis/htm/core/iistesc.htm

Obtaining a Server Certificate

www.microsoft.com/windows2000/en/server/iis/htm/core/iiocrsc.htm

Step-by-Step Guide to Setting up a Certificate Authority

www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/walkthru/casetup.asp

Install the latest software updates

Install the latest Service Packs and security patches to ensure that the Web Interface and APR Server are protected from all known operating system and Web server vulnerabilities.

Set folder security

The NTFS permissions on the Web Interface folder specify which users and groups can use APR. Set the permissions on this folder to allow only authorized users to access the Web Interface.



The Web Interface is installed into this folder if Microsoft IIS is detected during installation:

```
\inetpub\wwwroot\pwreset
```

Otherwise the Web Interface is installed into this folder:

```
\Program Files\ANIXIS Password Reset\wwwroot\pwreset
```

Set registry security

APR configuration settings are stored this registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ANIXIS\ANIXIS Password Reset
```

Only users that are authorized to configure APR should be granted write access to this registry key.

Encryption

APR uses encryption and hashing to protect confidential information. This page contains an overview of these encryption and hashing algorithms.

RSA – <http://www.rsasecurity.com/rsalabs/>

Ronald L. Rivest, Adi Shamir and Leonard Adleman created the RSA algorithm in 1977. RSA is the most widely used public-key encryption algorithm. APR uses the RSAES-OAEP scheme with randomly generated 1024-bit keys.

AES (Rijndael) – <http://csrc.nist.gov/cryptoolkit/aes/>

The U.S. National Institute of Standards and Technology ([NIST](#)) developed the Advanced Encryption Standard (AES) to replace the Data Encryption Standard (DES). After considering various submissions, NIST chose the Rijndael algorithm as the AES. The Rijndael algorithm was invented by Joan Daemen and Vincent Rijmen.

Rijndael is a Federal Information Processing Standard ([FIPS-197](#)) approved symmetric encryption algorithm that may be used by U.S. Government organizations to protect sensitive information.

APR uses both derived and randomly generated 256-bit AES keys (AES-256). This is the longest key length adopted in [FIPS-197](#).

SHA – <http://csrc.nist.gov/CryptoToolkit/tkhash.html>

The U.S. National Institute of Standards and Technology ([NIST](#)) developed the SHA algorithm using similar principles to those used by Ronald L. Rivest in the MD4 message digest algorithm.

SHA is a Federal Information Processing Standard ([FIPS-180-2](#)). APR uses the SHA-1 algorithm to create a 160-bit hash (message digest).

Troubleshooting

Installation Wizard

Could not add the [acct] account to the Domain Admins group. Add this account to the group manually after setup completes.

This error is normally caused by insufficient permissions. Add the account to the Domain Admins group and restart the ANIXIS Password Reset service.

Could not assign the "Log on as a service" right to the [acct] account. Assign this right manually after setup completes.

This error is normally caused by insufficient permissions. Assign the "Log on as a service" right to the specified account (on the APR Server computer) and start the ANIXIS Password Reset service.

Could not create a virtual directory for the Web Interface. Create the virtual directory manually after setup completes. The physical path is [path]

APR should work with any ISAPI capable Web server, however the Installation Wizard only recognizes and configures Microsoft IIS. Use your Web server's configuration tools to create a new virtual directory called pwreset. Users should have read and execute permissions in this directory. The path contains the files to be published.

Web Interface

APR Main Menu not displayed in Web browser

The Installation Wizard creates the pwreset virtual directory in the first available IIS Web site. An IIS server can host multiple Web sites, so you may need to manually create a virtual directory called pwreset in the desired Web site. Users should have read and execute permissions in this directory.

System Errors

The ANIXIS Password Reset Server is not responding. Try again in a few minutes and contact your network administrator if this message is displayed again.

This error occurs when the APR Server is busy, unavailable or unreachable. If the APR Server was recently installed, it may be busy building the data store, so try again after a few minutes.

If the ANIXIS Password Reset service has started on the APR Server computer, then the problem is most likely a configuration or network error. Check the [Web Interface configuration](#) and also ensure that UDP packets can pass between the Web Interface and APR Server computers. The APR Server listens on UDP port 5100 by default.

The ANIXIS Password Reset Server encountered an error while processing your request.

Email the complete message text to support@anixis.com

ANIXIS Password Reset cannot load the file [filename]. This file should be in the same folder as APR.DLL.

Ensure that the specified file exists in the Web Interface virtual directory and that users have permission to read the file. An incorrectly configured virtual directory can also cause this error.

An error occurred in the Password Policy Enforcer interface.

Check the [PPE configuration settings](#) and also ensure that UDP packets can pass between the Web Interface and Password Policy Server computers. The PPS listens on UDP port 1333 by default.

The path [path] is not valid.

The Web Interface (APR.DLL) was called with an invalid path. Check the URL that called the Web Interface.



Still having problems? Send an email describing the problem to support@anixis.com

Technical support

Three technical support options are available for administrators who require assistance with ANIXIS Password Reset.

Technical Documents

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

Email support

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

Telephone support

Telephone support is available to customers that have pre-purchased telephone support incidents. If your call is diverted, please leave a message and your call will be returned as soon as possible.

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



Support is available in English.

License Agreement

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

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

1. Ownership

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

2. License

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

3. Term

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

4. Restrictions on Transfer

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

5. Restrictions against copying or modifying the Licensed Materials

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

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

6. Protection and Security

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

7. Upgrades

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

8. Evaluation Version

If this copy of the Licensed Materials is an Evaluation Version, you are permitted to use the Licensed Materials without charge for up to 30 days. After 30 days, you must either destroy all copies of the Licensed Materials or pay the required license fee.

Use of the Licensed Materials after the 30 day evaluation period without paying the license fee is in violation of Australian and international copyright laws.

9. Limited Warranty

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

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

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

10. General

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

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