



# **ANIXIS Password Reset**

**V1.0**

## **Evaluator'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
Preparing the computers for the evaluation	2
Installing APR	3
Configuring IIS6 (Windows Server 2003 only)	4
Using APR for the first time	5
Configuring APR	8
Using APR with the updated configuration	9
Other features	10
Password Policy Enforcer	11

# Introduction

---

The purpose of this Evaluator's Guide is to introduce the reader to ANIXIS Password Reset. The guide highlights key features and benefits that are of interest to those who are evaluating APR, as well as those who are using APR for the first time.

Refer to the [APR Administrator's Guide](#) for more in-depth coverage of the topics in this guide.

## What is ANIXIS Password Reset?

ANIXIS Password Reset 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.

## Why use a self-service system rather than the helpdesk?

A major benefit of self-service password management systems is a reduction in operating costs. Various studies have shown that between 20% and 40% of all helpdesk calls are password management issues.

A self-service system also improves security, especially in large organizations with centralized helpdesks because helpdesk staff may find it difficult to identify callers. APR uses a challenge/response system to identify users who have forgotten their password.

## Benefits of using APR

- **Reduced operating costs:** 20% to 40% of all helpdesk calls are password management issues.
- **Increased productivity:** Users can continue to work instead of waiting in the helpdesk telephone queue.
- **Reduced helpdesk demand:** Password management issues are offloaded to APR instead of the helpdesk.
- **Improved security:** Users are securely identified and strong encryption is used to protect confidential information.
- **Improved manageability:** Centralized system ensures consistent enforcement of corporate policies. Integrated auditing allows network administrators to monitor all password management activity.
- **Improved availability:** APR is available 24 hours a day and can serve the needs of thousands of users.
- **Quick return on investment:** Competitive license terms combined with a reliable software package ensure a quick and substantial return on investment.

# Preparing the computers for the evaluation

---

Two computers are required for the evaluation, a server and a client. Prepare the evaluation computers as described below.



Send an email to [support@anixis.com](mailto:support@anixis.com) if you have any questions, or if you experience problems during the evaluation.

---

## Operating system

Install a server edition of Windows on the server computer. The screen images in this guide were taken from Windows Server 2003, however Windows NT 4 and Windows 2000 are also suitable.

## Windows domain

The evaluation computers should be members of a Windows domain. The server can be a domain controller, but it does not have to be.

## Web server

The Microsoft IIS Web server should be installed on the server computer, even if a different Web server is used on the production network. IIS is recommended for the evaluation because the APR Installation Wizard automatically creates and configures an IIS virtual directory for APR. The virtual directory must be created manually on other Web servers.

## Test account

Create a domain user account called APRTTest. Uncheck the **User must change password at next logon** option for this account.

Logon to the APRTTest account from the client computer to ensure that the computer is configured correctly. You should also be able to access the default IIS home page from the client computer's Web browser ([http://server\\_ip\\_address](http://server_ip_address)).



The [APR Administrator's Guide](#) contains important security information. Do not allow users to access APR until you have read this information and enabled the HTTPS protocol.

---

# Installing APR

---

Administrative privileges are required to install and configure APR. Use a domain administrator's account to logon to the server computer.

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



2. Select **I accept the license agreement** and click **Next**.
3. Read the Readme information carefully and click **Next**.
4. Select the **Complete** option and click **Next**.
5. Enter a **Username**, **Domain** and **Password** for the APR Server service account. The Installation Wizard will create the account if it does not exist. Click **Next**.
6. Click **Next** to copy the files onto the computer.



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.

---

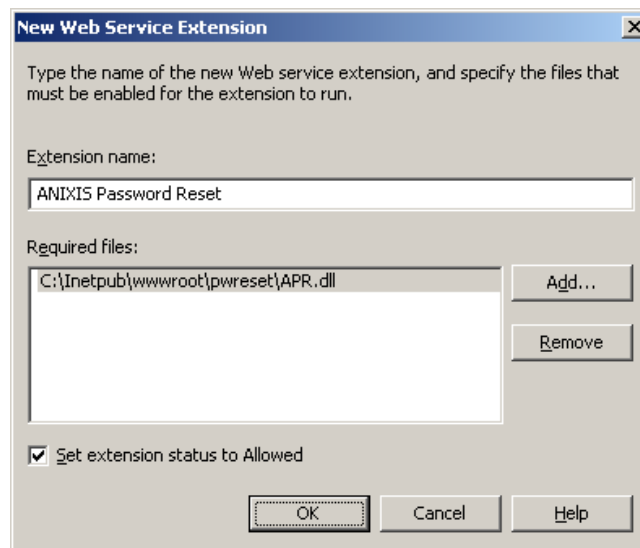
# Configuring IIS6 (Windows Server 2003 only)

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 page if the server computer is not running Windows Server 2003.

1. Select | **Start | Administrative Tools | Internet Information Services (IIS) Manager** | to open the IIS Manager console.
2. Click the **+** beside the **local computer** item to expand it (in the left pane of the IIS Manager console).
3. Select the **Web Service Extensions** item.
4. Click the **Add a new Web service extension...** task (in the right pane of the IIS Manager console).
5. Enter “ANIXIS Password Reset” in the **Extension name** field.
6. Click **Add...** and then **Browse...** Select APR.dll in the \inetpub\wwwroot\pwreset folder and click the **Open** button.
7. Click **OK**.
8. Check the **Set extension status to Allowed** option.
9. Click **OK**.



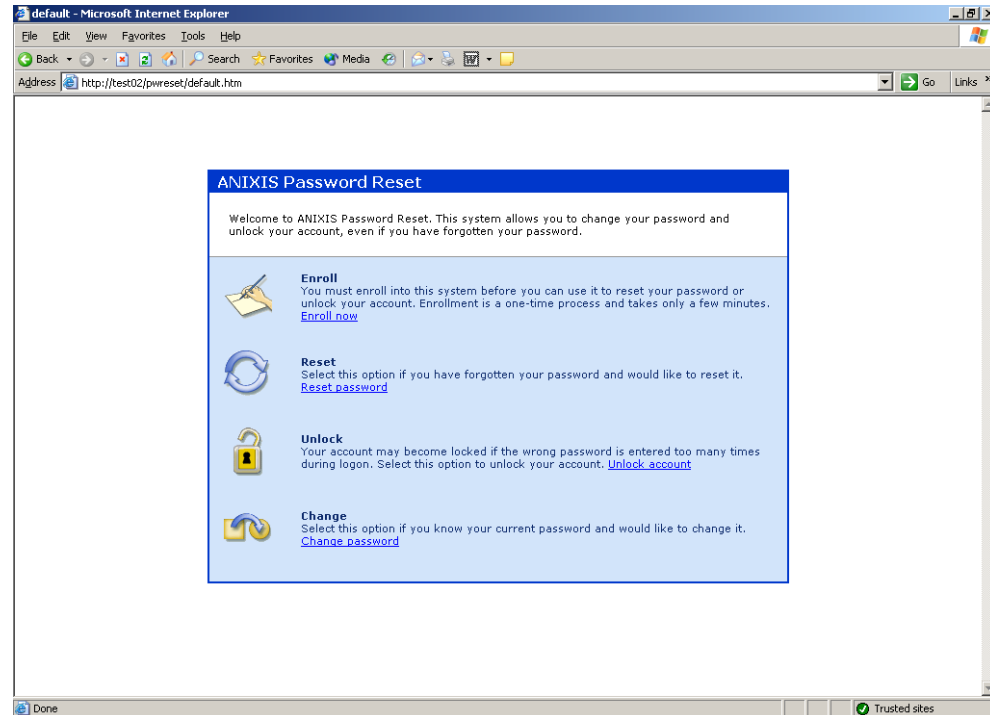
# Using APR for the first time

---

Logon to the client computer and type this URL into the **Address** field:

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

Replace `computer` with the name or IP address of the server computer. The APR main menu should appear in the Web browser.



## Enroll

1. Click the **Enroll** item in the main menu to enroll into APR.
2. Enter APRTTest in the **User name** field.
3. Enter the domain name in the **Domain** field.
4. Enter the password in the **Password** field.
5. Select a unique question from each of the **Question** lists and enter answers in the relevant **Answer** fields.
6. Click **Next**.

APR should display a message stating that your enrollment was successful. If an error message is displayed instead, correct the error and resubmit your enrollment details.

The Troubleshooting section in the [APR Administrator's Guide](#) contains information about the most common error messages.

## Reset

1. Click the **Reset** item in the main menu.
2. Enter APRTTest in the **User name** field.
3. Enter the domain name in the **Domain** field.
4. Click **Next**.
5. Enter the **Answer** to the first question and click **Next**.
6. Enter the **Answer** to the second question and click **Next**.
7. Enter the **Answer** to the third question and click **Next**.
8. Enter a new password in the **New password** and **Confirm password** fields.
9. Click **Next**.

APR should display a message stating that your password was reset. If an error message is displayed instead, correct the error and resubmit your request.

Test the Reset feature by logging off the APRTTest account and logging on with the new password.

## Unlock

1. Click the **Unlock** item in the main menu.
2. Enter APRTTest in the **User name** field.
3. Enter the domain name in the **Domain** field.
4. Click **Next**.
5. Enter the **Answer** to the first question and click **Next**.
6. Enter the **Answer** to the second question and click **Next**.
7. Enter the **Answer** to the third question and click **Next**.

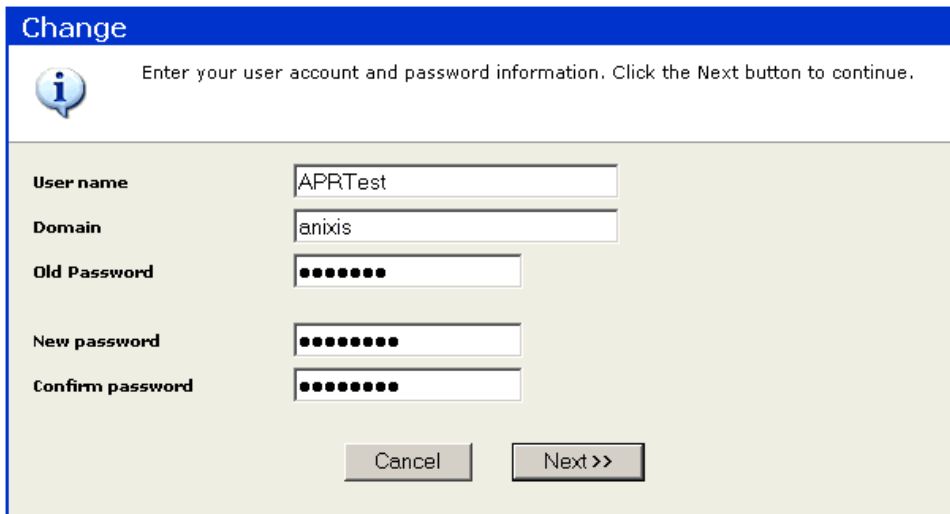


APR should display a message stating that your account was unlocked. If an error message is displayed instead, correct the error and resubmit your request.

Test the Unlock feature by intentionally locking the APRTTest account and then unlocking it from another computer.

## Change

1. Click the **Change** item in the main menu.
2. Enter APRTTest in the **User name** field.
3. Enter the domain name in the **Domain** field.
4. Enter the current password in the **Password** field.
5. Enter a new password in the **New password** and **Confirm password** fields.
6. Click **Next**.



**Change**

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

**User name**

**Domain**

**Old Password**

**New password**

**Confirm password**

APR should display a message stating that your password was changed. If an error message is displayed instead, correct the error and resubmit your request.

Test the Change feature by logging off the APRTTest account and logging on with the new password.

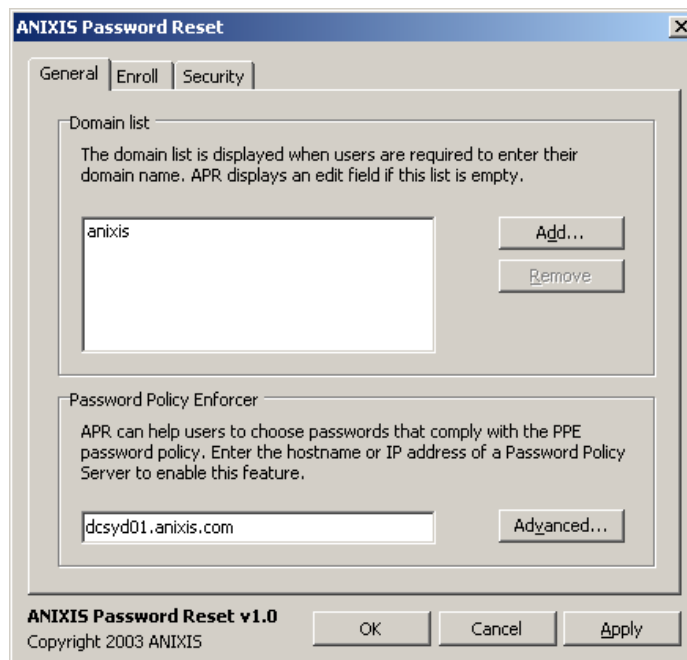
# Configuring APR

---

You will now use the APR configuration program to make these configuration changes:

- Define a default domain name.
- Enable Password Policy Enforcer integration (optional).
- Change the number of enrollment questions.
- Automatically expire passwords after they are reset.

1. Select **Start | Programs | ANIXIS Password Reset | Configuration** to open the APR configuration program.
2. Click the **Add...** button and enter the name of the domain that you are using to evaluate APR. Click **OK**.
3. If your network contains a Password Policy Server (even on another domain), enter the hostname or IP address of the PPS into the **Password Policy Enforcer** field. Enter 127.0.0.1 if PPE and APR are both installed on the same computer.



4. Click the **Enroll** tab and change the enroll question count (at the bottom of the page) to **2**.
5. Click the **Security** tab and enable the **Expire Passwords after reset** option.
6. Click **OK** to store the configuration settings.



Refer to the [Password Policy Enforcer](#) section if you would like to enforce a password policy, but do not have a Password Policy Server on your network.

---

# Using APR with the updated configuration

---

You should notice the following changes when using APR with the updated configuration settings.

## **Domain field**

The Domain edit field is replaced by a dropdown list in the Enroll, Reset, Unlock and Change forms. Use the APR configuration program to add domain names to this list.

## **PPE Integration (if enabled)**

The Reset and Change forms display the PPE Rejection Reason and Generic Rejection messages when a password does not comply with the password policy. Use the PPE management console to customize these messages.

## **Enrollment questions**

Users only have to answer two questions to enroll (previously three). Administrators can set the enrollment question count from one to ten in the APR configuration program.



The Reset and Unlock features require users to answer all their enrollment questions. Users who enrolled prior to the configuration change must still answer three questions to reset their password or unlock their account.

These users will only have to answer two questions if they re-enroll after the configuration change.

---

## **Password expiry**

Users who reset their password are prompted to choose a new password when they next logon to the network. This happens because the “Expire passwords after reset” feature is enabled.

## Other features

---

Congratulations! You have now installed, configured and used ANIXIS Password Reset. This page contains additional exercises that introduce you to some of APR's other features.



Refer to the [APR Administrator's Guide](#) for help with these exercises.

---

Add some questions to the question list. Choose questions whose answers are not publicly known and do not change over time.

Look in the Application event log for APR audit events. The APR Server writes audit events to the Application event log because it does not have permission to write to the Security event log.

Experiment with the Enrollment record lockout feature and intentionally lockout your enrollment record. You can access your enrollment record again by re-enrolling, or increasing the lockout threshold.

Remotely configure the APR Server from a client workstation.

Enable HTTPS to secure communications between the Web browser and server. The "Securing APR" section of the [Administrator's Guide](#) contains more information about HTTPS.

If you have a basic understanding of HTML, open the finished.htm file with Notepad or a HTML editor. Edit the message displayed when a user resets their password with APR.



Do not modify any of the comment tags in the APR HTML files. APR uses these tags to prepare the pages.

APR may not work correctly if an editor reformats its HTML files. Use a HTML editor that preserves formatting, or Notepad to modify the APR HTML files.

---

# Password Policy Enforcer

---

APR can integrate with Password Policy Enforcer to enforce a password policy and help users choose a compliant password. This section shows the reader how to quickly install and configure PPE during an APR evaluation.

PPE has many features that are beyond the scope of this document. Additional information about PPE is available in the [PPE Evaluator's Guide](#) and [PPE Administrator's Guide](#). Refer to these documents to learn more about PPE.



Ignore this section if PPE is already installed on your network. APR can communicate with your existing PPS.

Install PPE and APR on the same computer for the evaluation.

If you are installing PPE on Windows NT, ensure that the following components are installed before PPE:

- NT4 Service Pack 3 or later
  - Microsoft Management Console Version 1.2
- 

## Installing PPE

1. Download the latest version of PPE from [www.anixis.com](http://www.anixis.com)
2. Start the PPE Installation Wizard on the server computer by running PPEnn.EXE (where nn is the PPE version number).
3. Click **Next** to continue.
4. Select **I accept the license agreement** and click **Next**.
5. Read the Readme information carefully and click **Next**.
6. Select the **Complete** option and click **Next**.
7. Click **Next** to copy the files onto the computer.

You must restart the computer to activate the Password Policy Server. Click **Yes** when prompted to restart the computer.



PPE and APR are both installed on the same computer, so set the PPE IP address to 127.0.0.1 in the [APR configuration program](#).

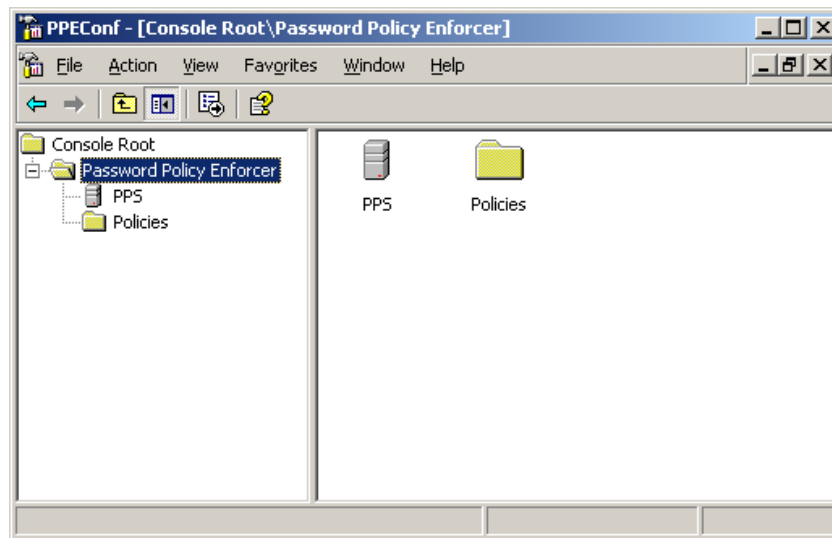
---

## Creating a password policy

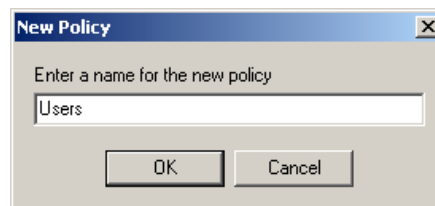
A password policy is a set of rules that evaluate every new password. You will use the PPE management console to create a password policy that enforces these rules:

- Password must contain at least seven characters.
- Password must contain at least one uppercase and one lowercase alpha character.
- Password must not be similar to the Username.
- Password must not exist in a dictionary of common passwords.

1. Select | **Start | Programs | Password Policy Enforcer | Configuration** | to open the PPE management console.

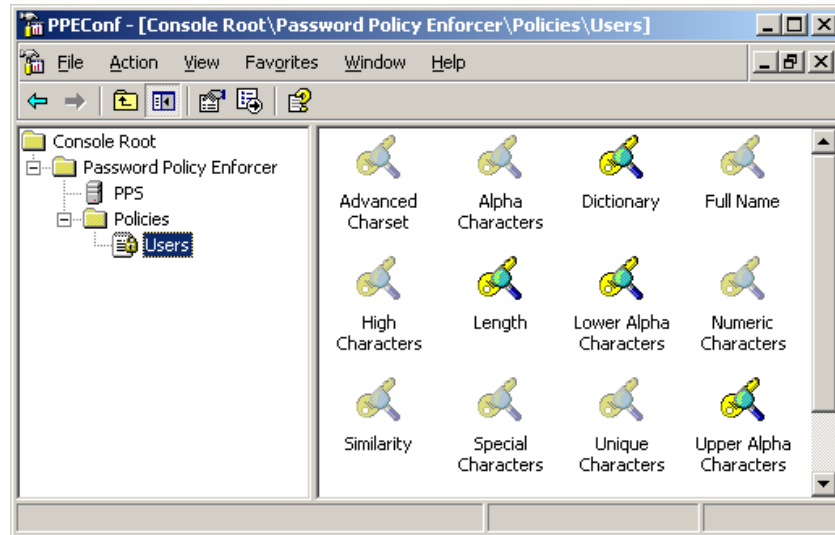


2. Right-click the **Policies** folder and select **New Policy...**
3. Type **Users** and click the **OK** button.



## Configuring password policy rules

PPE creates the new password policy in the **Policies** folder. The icons in the right pane of the management console represent the PPE rules. You will now configure these rules.



1. Double-click the **Length** icon.
2. Check the **Enabled** property.
3. Select the **at least** option and select **7** from the dropdown list.
4. Click the **OK** button.
  
5. Double-click the **Upper Alpha Characters** icon.
6. Check the **Enabled** property and click the **OK** button.
  
7. Double-click the **Lower Alpha Characters** icon.
8. Check the **Enabled** property and click the **OK** button.
  
9. Double-click the **Username** icon.
10. Check the **Enabled** property and click the **OK** button.
  
11. Double-click the **Dictionary** icon.
12. Check the **Enabled** property.
13. Click the ... button beside the **Server file** field.
14. Select the **DICT.TXT** file in the PPE installation folder.  
(Program Files\Password Policy Enforcer\)
15. Click the ... button beside the **Client file** field.
16. Select the **DICT.TXT** file in the PPE installation folder.
17. Click the **OK** button.

Remember to set the PPE IP address to 127.0.0.1 in the [APR configuration program](#).