

AUP Informant User Guide

4th September 2009

Contents

1	Introduction	3
2	Installation	4
2.1	Prerequisites	4
2.2	Server Installation	4
2.3	Client Installation: Interactive	5
2.4	Client Installation: Active Directory	5
2.5	Client Installation: RM Community Connect 3	6
2.6	Firewall Settings	7
3	Getting Started	8
3.1	Software Usage Summary	8
3.2	Starting the Server	8
4	Server Administration	9
4.1	Getting to Know the Server Window	9
4.2	Examining the Application Status	9
4.3	Adjusting Client Appearance	9
4.3.1	General Appearance	10
4.3.2	Customisation and Branding	10
4.4	Configuring Usage Policies	10
4.4.1	Policy Display	10
4.4.2	Primary Policy	11
4.4.3	Secondary Policy	11
4.4.4	Actions	12
4.5	Configuring Email Notifications	12
4.5.1	Creating the Mail Message	12
4.5.2	Notification Settings	13
4.5.3	Mail Server Settings	13
4.5.4	Authentication	13
4.6	Working with Reports	14
4.6.1	Report Viewer	14
4.6.2	Custom Reports	14

1 Introduction

Thank you for downloading AUP Informant; I hope you find it useful. This manual will guide you through the installation and configuration process as well as providing some useful tips along the way.

I'm always open to suggestions and corrections for this document and the software itself so please get in touch via paul@paulbeesley.com at any time!

Let's get started...

2 Installation

The installation process has been completely overhauled and should only take around 2 minutes on the server, after which the client program can be deployed using your usual method. Both client and server installers are standard MSI files which will work with Active Directory deployment and RM CC3 packages.

2.1 Prerequisites

Please make sure the following pieces of software are installed before installing AUP Informant.

Server

- **Microsoft .NET Framework 3.5** - a foundation for building modern applications. We recommend that you install version 3.5 SP1 if possible, the framework installer will install the full version and then update it to the latest version.
- **Microsoft SQL Server Compact 3.5** - a lightweight database. Can be installed safely alongside SQL Server and MSDE. The database server only runs when AUP Informant is active.
- Windows Server 2003 or Windows Server 2008 or Windows XP (SP2, SP3)

Client

- **Microsoft .NET Framework 2.0** - a foundation for building modern applications. Included with Windows Vista or later. AUP Informant also works with later versions such as 3.0 and 3.5.
- Windows XP (SP2, SP3) or Windows Vista or Windows 7

2.2 Server Installation

The server application has been designed to place the minimum possible load on your server and the install process should take less than one minute. Please do not deploy the client application until the server application is installed and started.

1. First, ensure that the server prerequisites above are installed before proceeding.

2 Installation

2. Check that no existing copies of AUP Informant server are running on your network.
3. Double click on the "AUP Informant Server 2.x.x.msi" file to launch the setup wizard. It will guide you through the installation process.
4. Once the server application is installed, it will launch the next time an administrator logs on. You can launch it from the "AUP Informant" entry in the Start Menu straight away if you wish.
5. That's it for now. You can safely deploy the client application before the server is configured - policies will not be displayed to users until the server configuration is complete.

2.3 Client Installation: Interactive

For small numbers of machines, the client installer can be run manually when you are logged on as an administrator. For larger numbers of machines it may be quicker to use an automated deployment tool such as those shown in later sections.

1. Ensure that the .NET Framework 2.0 or greater is installed on the computer.
2. Double click on the "AUP Informant Client 2.x.x.msi" file to launch the setup wizard. Follow the wizard to complete the installation.
3. You're done. The AUP Informant client application will launch next time a user logs on to the computer.

2.4 Client Installation: Active Directory

If your network is based on Windows Server with Active Directory then group policy provides the framework for package deployment. Packages can be installed per-machine or per-user; the first is appropriate for AUP Informant.

Note: These instructions are only applicable to Windows Server 2008. For Windows Server 2003 deployments, refer to the Microsoft article at <http://support.microsoft.com/kb/816102>.

1. Download the "AUP Informant Client 2.x.x.msi" package and place it in an accessible folder on the server you use for package deployment. The folder permissions should be set to allow your users to read and execute files in the directory.
2. Click Start -> Administrative Tools -> Group Policy Management
3. In the directory tree, expand your domain and then expand Group Policy Objects
4. Right click on Group Policy Objects and select New

2 Installation

5. Enter "AUP Informant Client" as the name of the new GPO. Ensure "Source Starter GPO" is set to None and press OK.
6. Double click on your new GPO and examine the Security Filtering section of the property page. Remove any existing groups that the policy applies to. Then, add the relevant groups that you want to deploy the client to.
7. Right click on the GPO in the list and select Edit
8. Expand Computer Configuration -> Policies -> Software Settings and click on Software Installation
9. Right click in the property page and select New -> Package
10. Browse for and select the "AUP Informant Client 2.x.x.msi" package.
11. Choose Assigned and press OK.
12. The client will be deployed to computers following a reboot.

2.5 Client Installation: RM Community Connect 3

There's no need to manually repackage AUP Informant for RM CC3 networks - you can use the RM Application Wizard to turn the MSI into a CC3 package in just a few steps.

1. Start the RM Application Wizard. This does not have to be on a clean package build station since we are not creating a package from scratch. The wizard may only be available on stations in the Package Build location.
2. Install the client application onto the workstation by running the "AUP Informant Client 2.x.x.msi" file. It can be removed after the RM package has been built.
3. From the Application Wizard, select "Add an existing Windows Installer package" and follow the steps, selecting the "AUP Informant Client 2.x.x.msi" package from the location you saved it to.
4. The wizard will now convert the MSI, prepare a CC3 package on the server and copy the files needed for deployment. The package list should be automatically updated.
5. (Optionally) Remove the client application from your workstation using Windows' Add/Remove Programs feature from Control Panel.
6. The package is now ready to deploy to workstations and can be allocated using the RM Management Console.

2.6 Firewall Settings

AUP Informant communicates over the local network and requires certain ports to be opened on the server and on client PCs. Without these ports open, the policy may not be displayed or responses may not be saved in the database.

Server Ports:

- UDP 5024 Inbound
- TCP 5025 Outbound
- TCP 5026 Inbound

Tip: If you are using Windows Server 2008, you can use the following commands in a command prompt to open the required ports:

```
netsh firewall set portopening UDP 5024 "AUPBcRec"  
netsh firewall set portopening TCP 5025 "AUPCrespSnd"  
netsh firewall set portopening TCP 5026 "AUPCrespRec"
```

Client Ports:

- UDP 5024 Outbound
- TCP 5025 Inbound
- TCP 5026 Outbound

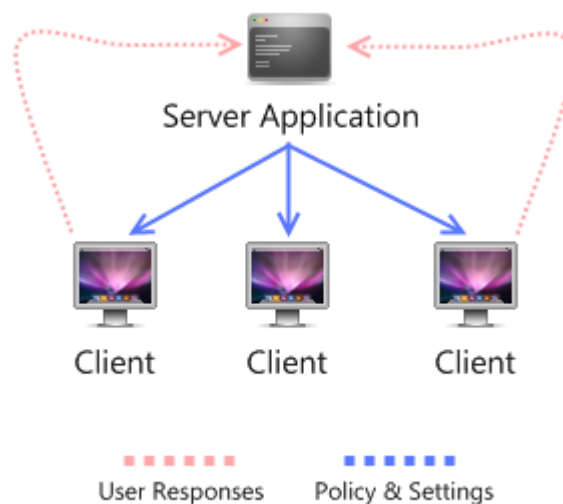
For assistance with using group policy to configure Windows Firewall on your client PCs, please refer to the Microsoft Technet documentation at: <http://technet.microsoft.com/en-us/library/bb490626.aspx>

3 Getting Started

3.1 Software Usage Summary

AUP Informant 2 is made up of two separate applications that work together to deliver your policy to users and to gather their responses. The server application controls the appearance of the client application and is responsible for pushing the usage policies out to clients. It also provides charting and reporting functions and sends email notifications.

The client application receives your usage policies from the server and displays them to users. It sends the user responses back to the server application.



3.2 Starting the Server

Once the server application has been installed on a network server it needs to be started before clients will receive any usage policies. To start the server, open the Start Menu, navigate to All Programs -> AUP Informant and choose "AUP Informant Server".

4 Server Administration

4.1 Getting to Know the Server Window

Along the top of the window is the tab bar that provides access to the various program functions. The Status tab is the first visible tab when the server starts-up. It provides an overview of the server's functionality and displays a log of user activity which updates in real time.

The second tab is the Client Appearance tab which is where you can customise the text and the logo that appear on the client window that your users see.

The third tab, Policies and Actions, lets you choose up to two policies to display and customise when they appear. You can also specify the actions that are taken when a user declines the policy.

The fourth tab manages email notifications, when they are sent and to whom.

The fifth tab shows you an overview of your policy's acceptance and also launches the Report Viewer that gives you more detailed information.

The final tab is a link to the product website and the support form.

Note: The guide follows the server window's tabs from left to right. You can complete the steps in any order, however.

4.2 Examining the Application Status

This tab displays a scrolling log of client events that updates in real time. Each time a user connects to the server and responds to a policy an event is logged here.

4.3 Adjusting Client Appearance

The appearance of the client software can be adjusted to reflect your organisation. The following settings are found on the Client Appearance tab.

4.3.1 General Appearance

Show a semi-transparent background behind the client window: Enable this option to show a partly-transparent black window behind the main client window. This window covers the entire screen preventing the user from using other programs until they have responded to the prompt.

Show the close button on the client window: Enable to display the “X” button in the top-right corner of the client window. When this is enabled users have the option of giving no response to your policy so you may wish to leave this disabled.

4.3.2 Customisation and Branding

All text on the client window can be customised to fit your organisation’s branding. Click any button to open the text editor and change the associated text. The default logo can also be changed to an image of your choice.

Window Title: The text that appears in the title bar of the client window.

Main Heading: The large text that appears in a blue font near the top of the window.

Sub-Heading: The smaller text directly beneath the main heading.

Buttons: Opens the button editor so that you can change the text on the Accept, Decline and Help buttons.

Logo: Opens a file browser so that you can select a new logo to replace the default one. The logo you choose should be 48x48 pixels (other sizes will be scaled to fit) and must be a JPEG, PNG, GIF or BMP image. It is not necessary for the image you choose to be accessible over the network because the resized image is sent to clients by the server application.

4.4 Configuring Usage Policies

4.4.1 Policy Display

This setting governs how often the client window with your policies is shown to your users.

Never: Prevents the client window from ever being shown - useful for open days.

Until User Accepts: The client window is shown at every log on until the user accepts your policy. If they decline the policy or close the window then it will appear at the next log on.

Every Logon: The client window appears every time a user logs on.

4.4.2 Primary Policy

The primary policy is your default policy that is shown to all users- the secondary policy appears instead when certain conditions are met. A common setup in schools is to use the primary policy for students and the secondary for staff.

Policy Location: This field must be set to the path of your usage policy. This can be either a website URL or the location of a saved web page on disk. E.g. “http://intranet/policies/student.html” or “\\server1\public\policies\student.html”.

Note: If you select a policy that is saved on disk, ensure that the relevant users have read access to it or the policy will not be displayed.

Note: Using mapped drives is possible but not recommended. Occasionally, AUP Informant will load before the drive has been mapped and your policy will appear to be unavailable. Use full paths with server names if you can.

4.4.3 Secondary Policy

Normally your primary policy will be shown to all users. The secondary policy can be enabled and is only displayed when certain conditions are met.

Policy Location: See notes on Primary Policy.

Show this Policy: By default this field is set to never, which means that only the primary policy will be shown. To show the secondary policy for some users, select an alternate display setting from the drop-down list and enter some words in the text field. The username of the logged on user is searched for the words that you enter and, if a match is found, the secondary policy will be shown in place of the primary policy.

The display settings are:

- **Never:** Always display the primary policy. Your secondary policy will never be shown.
- **When the username contains the following words:** If the current user’s username contains any of the specified words, the secondary policy is shown.
- **When the username does not contain...:** If the user’s username does not contain any of the specified words, the secondary policy is shown.
- **When the username starts with the following words:** Checks the username letter by letter to see if it begins with any of the specified words. If there is a match then the secondary policy is shown. Does not match words that appear in the middle of other words.
- **When the username does not start with...:** If none of the specified words are found at the beginning of the username, the secondary policy is shown.

There is no limit to the number of words that you can enter but they must be separated by commas. It doesn't matter if you add a comma to the end of the list or not. There is no need to place a space after the word and before the comma.

4.4.4 Actions

If a user does not accept your policy and presses the Decline button on the client window you can apply certain actions.

Log User Off: Logs the user off the computer they are currently using. Does not prevent them logging back in.

Restart Computer: Restarts the computer, logging the user off in the process.

4.5 Configuring Email Notifications

If you have an SMTP server available (either on your local network or accessible via the Internet) then AUP Informant can send email notifications when a user responds to your policy.

4.5.1 Creating the Mail Message

This section works similarly to a regular email program. Enter the address at which you want to receive the notifications in the To field and the subject in the Subject field; choose something that will make it obvious that the email is from AUP Informant. You will need to specify the email address that the email will appear to be from in the From field. When you receive emails, they will appear to be from "AUP Informant" regardless of what you set here.

The Message Body field can contain static text and also certain variables that are converted to text when the message is sent. These variables represent information about the user that declined the policy. For example, the variable %username% is converted to the user's actual username when the email is sent. You can use the drop-down list to select and insert variables into the Message Body field.

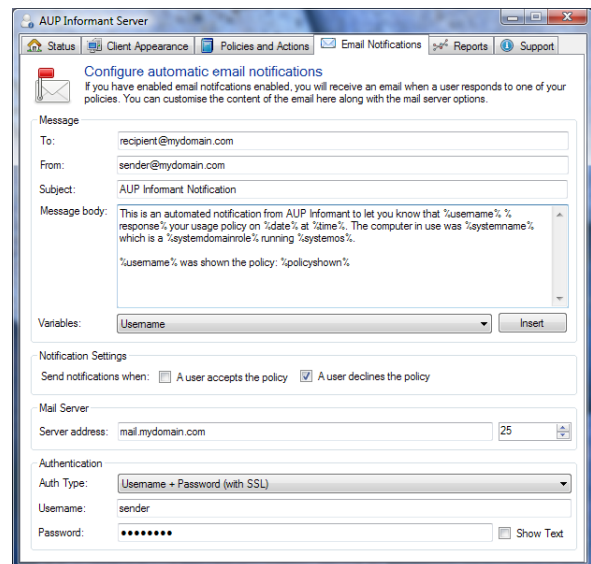


Figure 4.1: Email Notifications Tab

Tip: The subject field will also convert variables into their actual values so you can use them in the subject line as well as the body.

4.5.2 Notification Settings

You can choose to be notified by email when a user accepts the policy, declines the policy or both. Turning on notifications for accepted policies may generate a large number of messages for networks with many users.

4.5.3 Mail Server Settings

Server Address: The local or Internet address of the mail server that AUP Informant should use to send messages. This can be either a computer name (e.g. mail.mydomain.com) or an IP address (e.g. 192.168.114.101). The server must have SMTP support enabled; some servers such as Microsoft Exchange do not always have this turned on by default.

So long as the server supports SMTP, AUP Informant should work with it.

Port: The port that your SMTP server uses for incoming connections. By default this is port 25.

Enable SSL: Some SMTP servers require SSL encryption to be enabled when sending mail. If your server requires that it is turned on, check this box. You may also need to change the port to the default of 465.

4.5.4 Authentication

Some mail servers will require you to provide logon credentials in order to send mail. If this is the case then you can provide AUP Informant with a set of credentials that it will use when sending mail. The Auth Type setting specifies the type of authentication the server requires. For many servers this can be left on the default setting of None.

Authentication Type	Description
None	Attempt to send mail without providing any credentials
Username + Password	Provides the username and password you specify as the credentials
Username + Password (with SSL)	As above but also enables SSL encryption required by some servers
Domain Credentials	Sends the Windows credentials of the currently logged-on user to the server
Domain Credentials (with SSL)	As above but also enables SSL encryption required by some servers

4.6 Working with Reports

The reports tab shows an overview graph that displays your policy acceptance as it currently stands. The blue section of the graph represents users who have accepted your policy while the red section is for those who have declined. Figures on the graph represent the actual number of users that make up the slice and not a percentage.

When you first start AUP Informant, there may not be enough data to build a graph. If this is the case you will see a grey area with a message that states “There is not enough data to produce a chart”. If this is the case, simply wait until the client application is deployed and some users have responded to your policy.

The chart updates itself every minute and does not need to be refreshed.

4.6.1 Report Viewer

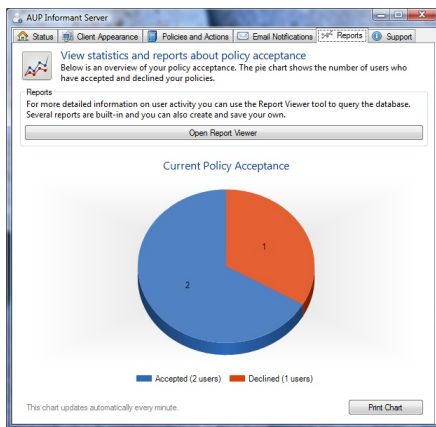


Figure 4.2: Reports Tab

The report viewer is used to store and run reports on the database. A report is a pre-packaged SQL query that filters certain information and returns it from the database to be displayed. Several reports are built into AUP Informant that you should find useful. For example, you can examine all the responses that have been made within the past day or week.

To run a report, click the “Generate Report” button on the toolbar. The results will be displayed in the grid below.

4.6.2 Custom Reports

If you are familiar with SQL queries, you can create your own reports and save them. The database schema is available

for reference. Report creation will be upgraded in a future release with a simple, graphical report builder.