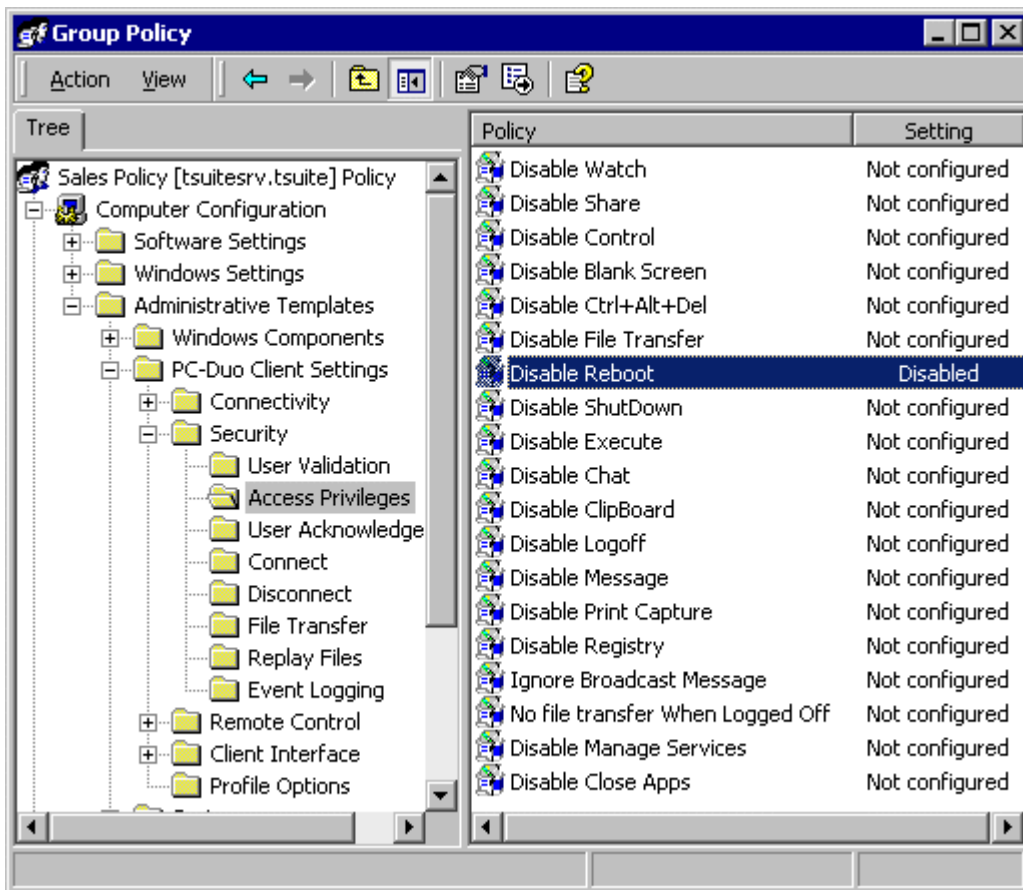


What's New in PC-Duo Enterprise Remote Control v8.5

Active directory Integration

Active Directory is a directory service that enables organizations to share and manage information about their network resources from a central Console. Remote Control 8.5 provides support for the Active Directory management of Client configuration settings using an Administrative Template.



Settings configured in the Active Directory Console are stored in the registry of the selected Clients. In Remote Control, the Client first looks for its configuration settings in the location specified by the Client parameters in the CLIENT32.INI file. However, it also looks in the local registry for Active Directory settings and these take priority over the settings specified in the configuration file.

A sample ADM script that enables you to add Remote Control settings to your Active Directory Console is installed as part of the PC-Duo Control kit.

Extended Logging Functions

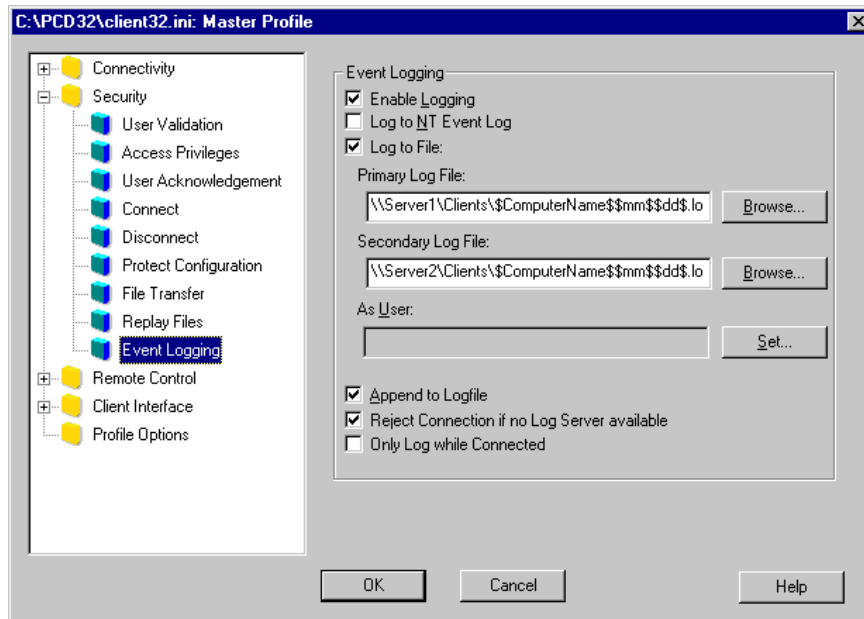
Remote Control v8.5 includes extended logging functions, which provide administrators with extra tracking information and help increase Client security:

Configurable Log-file Names You can now configure the Client application to store separate Log files for each Client and for each day by including tokens in the log file name. For example, to include the name of the Client in the log file name, append the \$ComputerName\$ token. You can also add the date to the file name using the following tokens:

Days Tokens \$d\$, \$dd\$, \$ddd\$ or \$dddd\$

Year Tokens \$y\$, \$yy\$, \$yyy\$ or \$yyyy\$

Month Tokens \$m\$, \$mm\$, \$mmm\$ or \$mmmm\$



Secondary Log Server The Client Configurator now includes the option to specify a secondary storage location for Client log files that is automatically used by Clients when the primary location is unavailable. In addition, you can configure Clients to reject connection attempts when they cannot access the specified server locations.

Extended Event Logging The Log to File and Log to NT Event Log options in the Client Configurator are now implemented as check boxes instead of radio buttons. This gives administrators the ability to configure Clients to record events in both logs simultaneously.

Record Control Details The log file and event log record the account details of the Control user when a connection is made.

Log the Reason for a Connection If the Prompt for additional information when connecting option is enabled in the Control configuration, the Client log file records the reason for the connection entered by the Control user. For example:

12-Sep-03, 14:44:42, Client32 TMBTEST1: Reason for connection from INVH093 @ >10.0.0.30:1617 (testing the new security features)

The User Acknowledgement Required option in the Client configuration must also be enabled to use this feature.

Restricted Logging When enabled, the Only Log while Connected option restricts the Client's log file entries to those related to control sessions. Other events such as startup and shutdown are not logged.

Using Screen Scrape Mode in Connection Sessions

Because Remote Control's standard method of displaying screens cannot display some applications that use advanced screen-handling techniques, Control PCs have the ability to display Client screens by reading directly from the memory of the Client PC's display adaptor. This *screen scrape* mode is slower than the standard display method, and displays in only 256 colors, but it does allow Controls to view the majority of these applications. Remote Control version 8.50 includes the following enhancements for screen scrape mode:

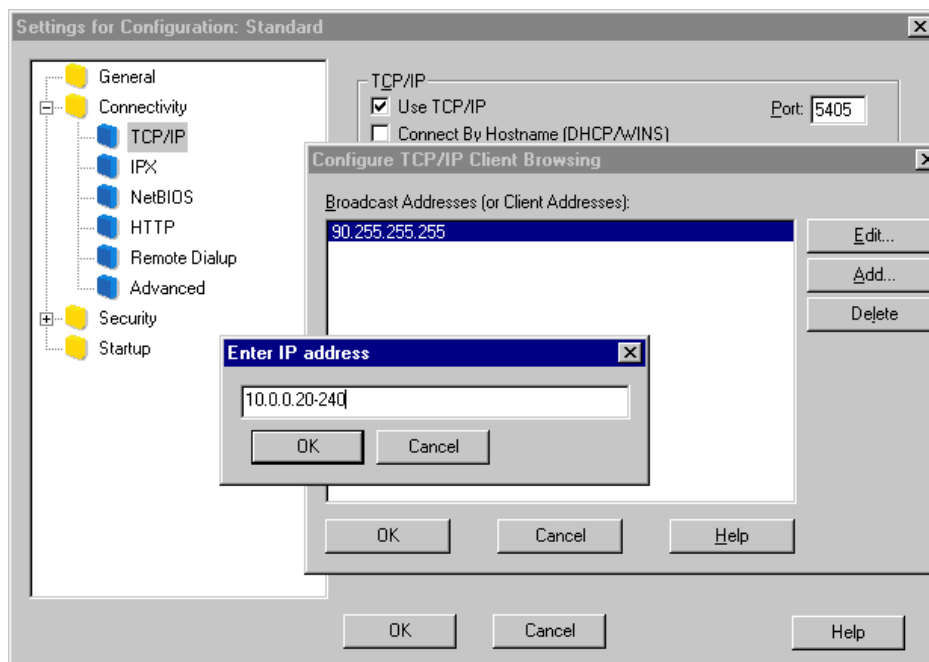
- To specify screen scrape as the default mode for all connections, select the Settings button in the Control toolbar and enable the Screen Scrape option in the Remote Control, View page. All new connections are started in screen scrape mode.
- To toggle between screen scrape and standard mode during a view session, right-click the View window toolbar and choose Customize to add the Scrape icon to Toolbar.

You can also select screen scrape as the default mode for specific Clients using the Client configuration.

Browsing for Clients on UDP-disabled Subnets

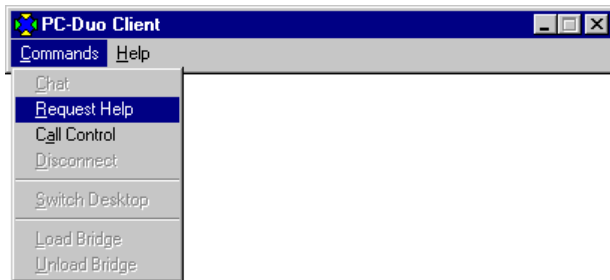
By default, Controls browse for Clients by broadcasting a UDP message on the subnet addresses specified in the TCP/IP section of their configuration settings. However, this method cannot find Clients when their subnet is located behind a router where UDP browse is disabled.

To avoid specifying an individual IP address for each Client on the browse-disabled subnet that you want to access, Remote Control v8.5 enables you to specify one or more address ranges in the last address (Class C) field. For example, to browse all Clients in the address range 10.0.0.20 to 10.0.0.240, open the Configure TCP/IP Client Browsing dialog, click Add and enter 10.0.0.20-240 in the Enter IP address dialog. The Control sends a unicast message to each Client within the range.



Improved Integration with Help Desk Systems

As an alternative to having Client users report problems directly to support staff, you can now integrate Remote Control with Web-based problem reporting systems. The Select a URL for Help Request option in the Client configuration enables administrators to customize the Request Help option of the Client's Commands menu and make Remote Control part of a formal problem-reporting system.



Note: This option disables other help request options in the Client Configurator.

Display the current Client User during a Browse

The Details View of the Control includes a new column in the browse list showing the user name of the logged on Client user.

Gateway support for Multiple Private Networks with the same IP Ranges

Remote Control v8.5 Gateways support Client connections on installations where multiple private networks are configured to use the same IP ranges. The uniqueness of each Client is provided by combining the apparent (translated) IP address of the Client connection with the Gateway and source port. The following string is displayed when the Control user moves the mouse cursor over a Client icon:

```
>gateway_name/>real_ip_address (apparent_ip_address:apparent_port)
```

for example:

```
>GATEWAY/>10.0.0.40 (182.76.34.2:4200)
```

Where 10.0.0.40 is the IP address of the Client and 182.76.34.2 is the IP address of the NAT router/firewall between Client and Gateway

Select a Network Card for use with Client

You can now specify the IP address on which you want Clients to listen for incoming Control connections. Administrators can select a specific IP address for Clients or choose to have them listen on all available IP addresses assigned to the local PC.

By default, the Client listens on all IP addresses. This is the recommended option and should only be altered in specific cases such as when using a Firewall.