Intego Remote Management Console 2 User Manual

Welcome to the User Manual for Intego Remote Management Console 2. Use the Table of Contents below to go to the different sections of the manual. You can come back to this main Table of Contents at any time by clicking the *Go to Main Table of Contents* link at the top of each page.

Table of Contents

Welcome to Remote Management Console 2

Managing Intego Software on Multiple Macs

Companies, schools and other institutions have security policies that must be applied and enforced. Intego's Internet security software provides robust protection from the many dangers of the Internet: protection from viruses and malware, network attacks, unwanted content, and much more. Institutions with large numbers of Macs using Intego software will benefit from centralized administration of software, allowing administrators to establish and deploy their security policy quickly and easily.

Intego Remote Management Console 2 is a software administration tool designed for managing Intego software on multiple Macs. Remote Management Console 2 allows administrators to create and load policies, configure individual settings and functions, and make changes to Intego programs on all managed computers quickly and easily. Policies for these programs can be managed for individual workstations or for groups of workstations.

Remote Management Console allows administrators to manage and configure Intego security software on any number of Macs over a local network or via the Internet. The administrator can contact client computers via a Remote Management Console server and set policies for the following programs:

- **VirusBarrier X6** provides comprehensive protection from malware and network threats. VirusBarrier X6 is the only antivirus program for Mac that includes full anti-malware protection together with firewall, network protection, anti-phishing, anti-spyware features and more.
- **ContentBarrier** is a content filtering program for Mac, providing functions for parents and businesses. It is designed to filter and block certain Internet content according to the needs of each school, business or institution.
- **NetUpdate** ensures that updates to Intego's programs and filters are downloaded and installed when available. NetUpdate can check for updates automatically on Intego's server, or it can check a NetUpdate proxy server set up on a computer selected by the administrator, and automatically update all of Intego's programs and their

filters.

Deploying Intego Software on Multiple Macs

If you manage a large number of Macs, it's good to know that deploying Intego software on your managed computers is simple. Intego has a white paper called Intego Enterprise Software Deployment Guide that you can download and use to prepare and manage your deployment.

Remote Management Console 2 Features

Remote Management Console 2 lets administrators:

- Manage Intego software on multiple Macs
- Organize client computers by list or group
- Apply security policies by list or group
- Access information about managed client Macs
- Perform automatic and manual updates of Intego software and filters on client Macs
- Run manual tasks, such as malware scans, on client Macs
- Monitor Intego software on client Macs, and access full logs

Installing and Setting Up Remote Management Console 2

Remote Management Console 2 consists of four components:

- **Server**: The Server component retrieves settings and logs from managed workstations and provides the workstations with updated settings.
- **Client**: The Client component is installed on managed workstations and is the bridge between the Server component and the Intego software installed on the workstation.
- **Console**: The Console component is the application which allows administrators to interact with the Server component. The Console can interact with one or more servers, and can be installed on a server where the Remote Management Console 2 Server component is installed, or on any other Mac.
- **NetUpdate proxy**: The NetUpdate proxy is an optional component that can be used to save Internet bandwidth and keep software on managed workstations up-to-date without them being directly connected to the Internet. NetUpdate is the Intego tool used to update software and filters.

Remote Management Console 2's Console, Server and NetUpdate Proxy components require Mac OS X 10.5 or later, or Mac OS X Server 10.5 or later, running on either a PowerPC or Intel-based Mac. Client components require Mac OS X 10.5 or later, on either PowerPC or Intel-based Macs, and are not supported on Mac OS X Server.

Remote Management Console works with the following versions of Intego software:

- VirusBarrier X6 10.6.5 or later
- ContentBarrier 10.6.3 or later
- NetUpdate 10.5.5 or later

Preparing for Installation

Installation of Remote Management Console involves several steps, as you install the different components mentioned above and prepare your workstations for installation of Intego software. These steps are as follows:

1. You first install the Server component. It is recommended to install the Server component on a computer that is always on and is accessible to all the managed workstations.

2. You then install the Console component on a Mac which will be used by an administrator.
3. (Optional) If you want to use a NetUpdate proxy, you can install the NetUpdate proxy component on any Mac. It can be the same computer that runs the Server component or another one. The Mac with the NetUpdate proxy component must be able to connect to the Internet to access the Intego NetUpdate server, and must be accessible to other computers running Intego software so they can access the installation packages for program and filter updates that it hosts.
4. You use the Remote Management Console 2 application to configure the Server.
5. You deploy the Client component and the appropriate Intego software on managed workstations.

Installing the Server Component

To install the Remote Management Console 2 Server component, mount the Remote Management Console 2 disk image. If you are not logged in on the server, copy the Remote Management Console Server.pkg installation package to the server. On the server, double-click on the Remote Management Console Server.pkg installation package, then follow the instructions displayed by the Installer.

You can do this using Apple Remote Desktop, or via the command line, if you wish to perform a remote installation.

Installing the NetUpdate Proxy Component

To install the NetUpdate Proxy component, mount the Remote Management Console 2 disk image. If you are not logged in on the server, copy the NetUpdateProxyServer.pkg installation package to the server. On the server, double-click on the NetUpdateProxyServer.pkg installation package, then follow the instructions displayed by the Installer.

You can do this using Apple Remote Desktop, or via the command line, if you wish to perform a remote installation.

Installing the Console Component

The Console component is an application that requires no special installation process. Open the Remote Management Console 2 disk image and drag the Remote Management Console application into the /Applications folder on the Mac where you wish to use it.

Connecting Remote Management Console 2 to Remote Servers

For Remote Management Console to be able to connect to the server, the server must be able to accept connections through port 18133 TCP. For workstations to be able to connect to the server, the server must be able to accept connections through port 18134 TCP. If servers use a firewall, including that which is part of VirusBarrier X6, these ports must be open for the different components to be able to communicate.

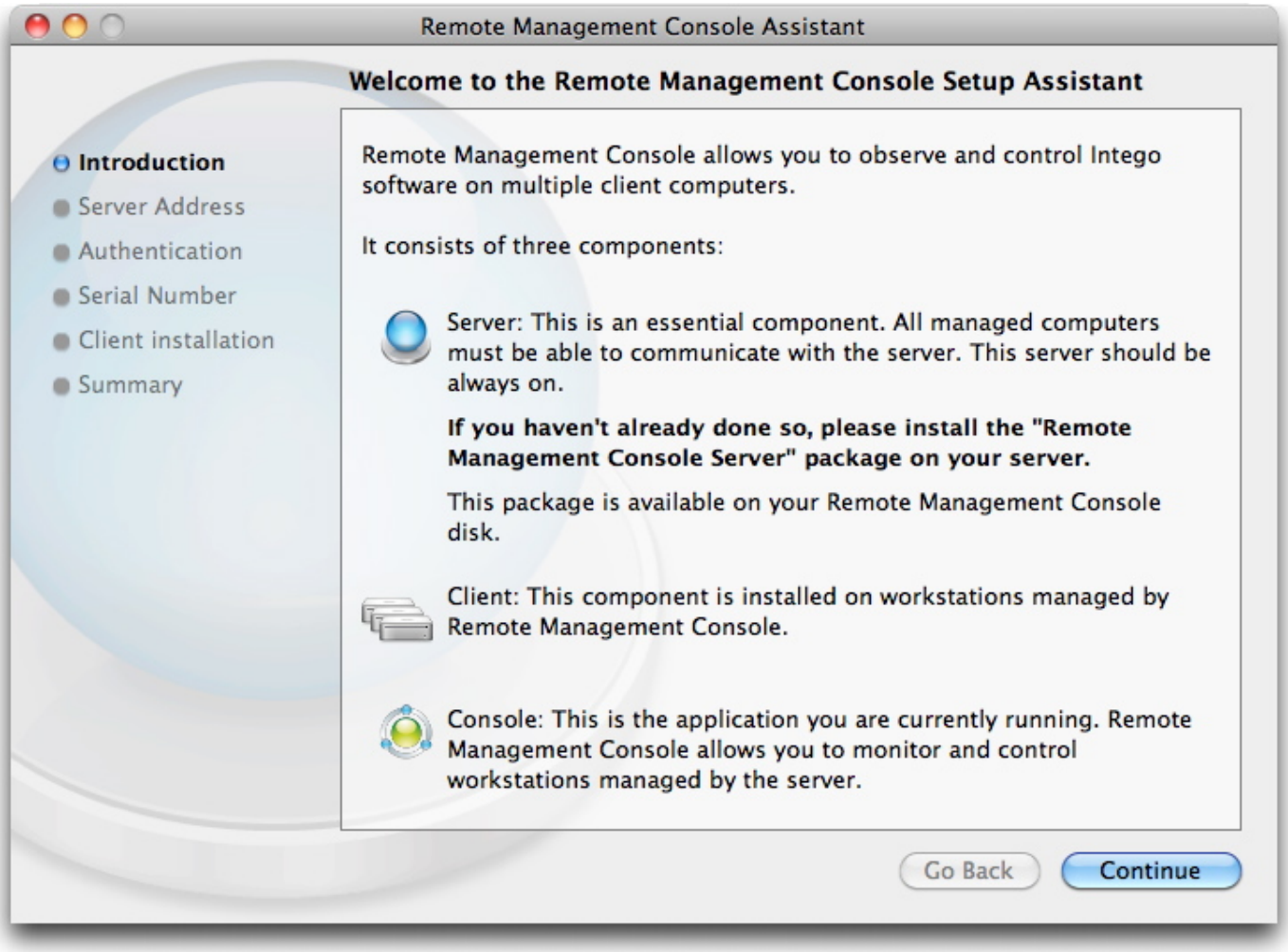
Network Ports Used by Server	
Connections from Remote Management Console	18133 TCP
Connections from workstations	18134 TCP

Deploying the Client Component

The Client component is installed on workstations that you manage using Remote Management Console. The deployment of the Client component is covered in the Using Remote Management Console section of this manual. Note that each time the Remote Management Console software is updated you must create and deploy a new version of the Client component.

Using the Remote Management Console Assistant

After you've completed the installation of the various components of Remote Management Console, you can launch the Remote Management Console application. The first time you do this, the Remote Management Console Assistant will display to help you complete your setup.



This assistant will give you some information about using Remote Management Console, and will help perform the setup necessary to enable the program. The Assistant presents six screens:

- **Introduction**
- **Server Address**
- **Authentication**
- **Serial Number**
- **Client installation**
- **Summary**

Introduction

The Introduction screen gives you an overview of the three components used by Remote Management Console. Make sure that you have installed the Remote Management Console Server component on your server before continuing. To go to the next screen, click **Continue**.

Server Address

This screen asks you to enter the name or IP address of the server on which you have installed the Remote Management Console Server component. Do this, then click **Continue** to go to the next screen. Remote Management

Console will attempt to connect to the server.

Authentication

Enter the necessary information to create the first Remote Management Console administrator account. This is different from the accounts already on the server, but you may use the same name and password if you wish. Check **Remember this password in my keychain** if you want this password stored in your keychain so you don't have to enter it manually in the future.

Enter the necessary information, then click **Continue** to go to the next screen. Note that this screen may be different from what is shown here if you have already set up a server and are connecting to it from an instance of Remote Management Console that did not set up the server.

Note: you can choose to not enter a password when creating an account in this step, or later from the Remote Management Console application, and instead use key authentication. To learn how to use this, see Appendix: Using Key Authentication at the end of this section of the user's manual.

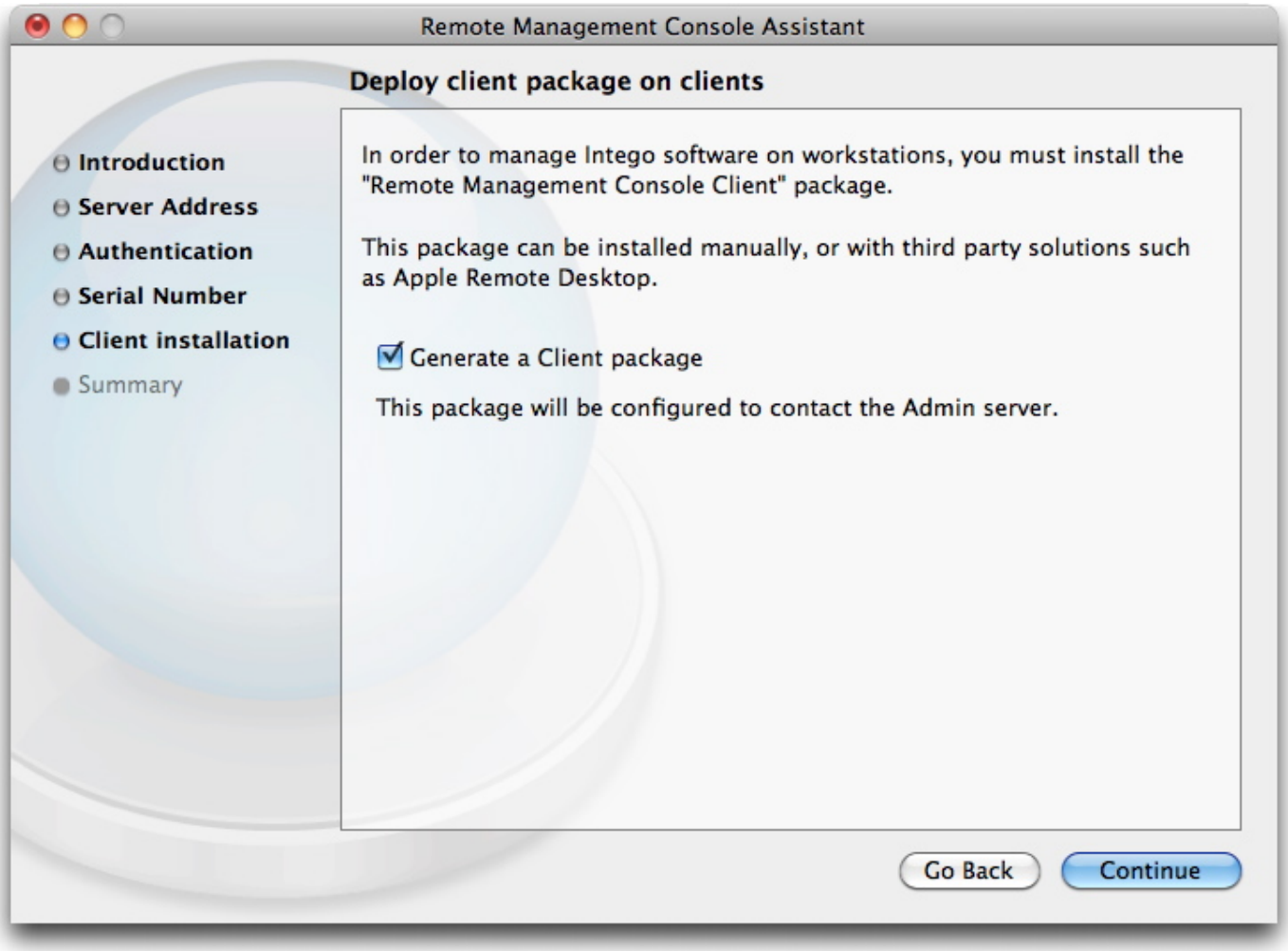
Serial Number

Enter your Remote Management Console serial number, then click **Continue**. Note that this screen will not display if you have already set up a server and serialized it.

Your serial number determines how many workstations Remote Management Console can manage. You cannot use the same serial number on more than one server; if you wish to use more servers, contact Intego for an additional license.

Client installation

The next screen lets you create a Remote Management Console Client package, that you can then install on your client computers. This package contains information allowing the clients to securely communicate with your server.



Click **Continue** to create this client package. You'll be asked to save this package.

After you have created this client package, you must install it on the client computers you are managing. You can do this in three ways:

- Copy the package to the client computers, then double-click it and use the Apple Installer application to install it.
- Use Apple Remote Desktop to install the package on your client computers.
- Install it via the command line. Connect to each client computer via `ssh`, then copy the package file, and install it using the `installer` command.

Summary

The Summary screen shows you that the configuration process has been completed. Click **Close** to quit the Assistant and use Remote Management Console.

Updating Remote Management Console 2

When updates are available to any of the components that make up Remote Management Console 2, the Console component will display an alert. In such case, the alert will display a link from which you can download a new disk

image containing the new versions of all the components. Follow the same installation instructions presented above to install the updates.

For updates, a Console > Server > Client hierarchy should be respected. When new versions are available, if it is not possible to update all clients at once, the Console should be updated first, then the Server, and finally the clients. New versions of the Console will be compatible with older versions of the Server; new versions of the Server will be compatible with older versions of the Client component.

About Your Copy of Remote Management Console

To get information about your copy of Remote Management Console 2, choose **Remote Management Console** > **About Remote Management Console**. This screen shows the version number of your copy of Remote Management Console 2.

Technical support

Technical support is available for registered purchasers of Intego products with valid subscriptions from the Intego Support page.

Appendix: Using Key Authentication

When you set up user accounts, you can choose to use passwords, but you can also use key authentication if you wish to limit access to only those users on specific computers that you have authorized. To do so, you need to perform the following operations:

1. On the Mac where the Remote Management Console application is to be used, note the contents of the ~/Library/Preferences/Remote Management Console/console_host_key.pub file.
2. On the server, create the following file: /Library/Preferences/Intego/Remote Management Console/Server/authorized_keys.plist. Administrative rights are necessary to do this. This is an XML file which contains associations between user names and keys.

3. Enter the key copied in step 1 together with the user name; the file should look like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>

<key>B2A2434293CBDC8D0E13D40ED89D93A1056C24ACE4C7BE077FFAC005B5BD7A860D3AD4FD8853E96138FFF3430E3E59E560C8D03308750DF345E53028F0763814150
BBDD9C5C464122F596A2759F29E6A5393F6551AD94EDB7DFE92DA57AE8B392C3F19ACAA0D2D1B052336699A882142E84E62E7F79BA240ED9FE833E4F8C91813F539B5D7D
D63DCA3811BBE08BAE5BB85D07CED86C2BFF42C65FD1D8D781437FC126BFF3AC973A8FD51FBE2014D86FB705D7422F4B115519C9748EFD027F48BA9E53C0D2D2B567FE709
E29D4F29B6D6B21184B160057C2FB19F7962E3F6A58A4512C27804812C5361F3B7749B78974D1A72085018F7A99AAAAFA4F10DF9C0DB</key>
    <string>alice</string>

<key>D55B15EC1C27A54800F5BD648D93BD84E9B17A4ED3F02EF490295E35D117987B500221EAF9280686F4A1687D9496257DD35E54E0F1DB0C06B8165EC6BC58546272F
131BC67E88794DF162CCF12DE9558C083308FBA51BDA9BFCC6AB5C6EAB882904A9C12321F82F131CFE44CE76FEB4E0BC4C7C6E6724B7F2663DC8AC9EBFAC00F7A6FF7F9B3
D12EF17987B47B736BB0A1DFB6B1E74965E10C5B57A307C5D0545EF1907F3DF723AF9EA2F1013E774217A5CE6E5793927EF20D023568355D461EF4A201F57BFFD83DA51B81
C267CEF05A4B4126C6F7F7747CECB41B2D3B80877388E84763F9D26A593614A9F5795F5986B72E97DBC8116AE798861DEE02B80C11</key>
    <string>bob</string>
</dict>
</plist>
```

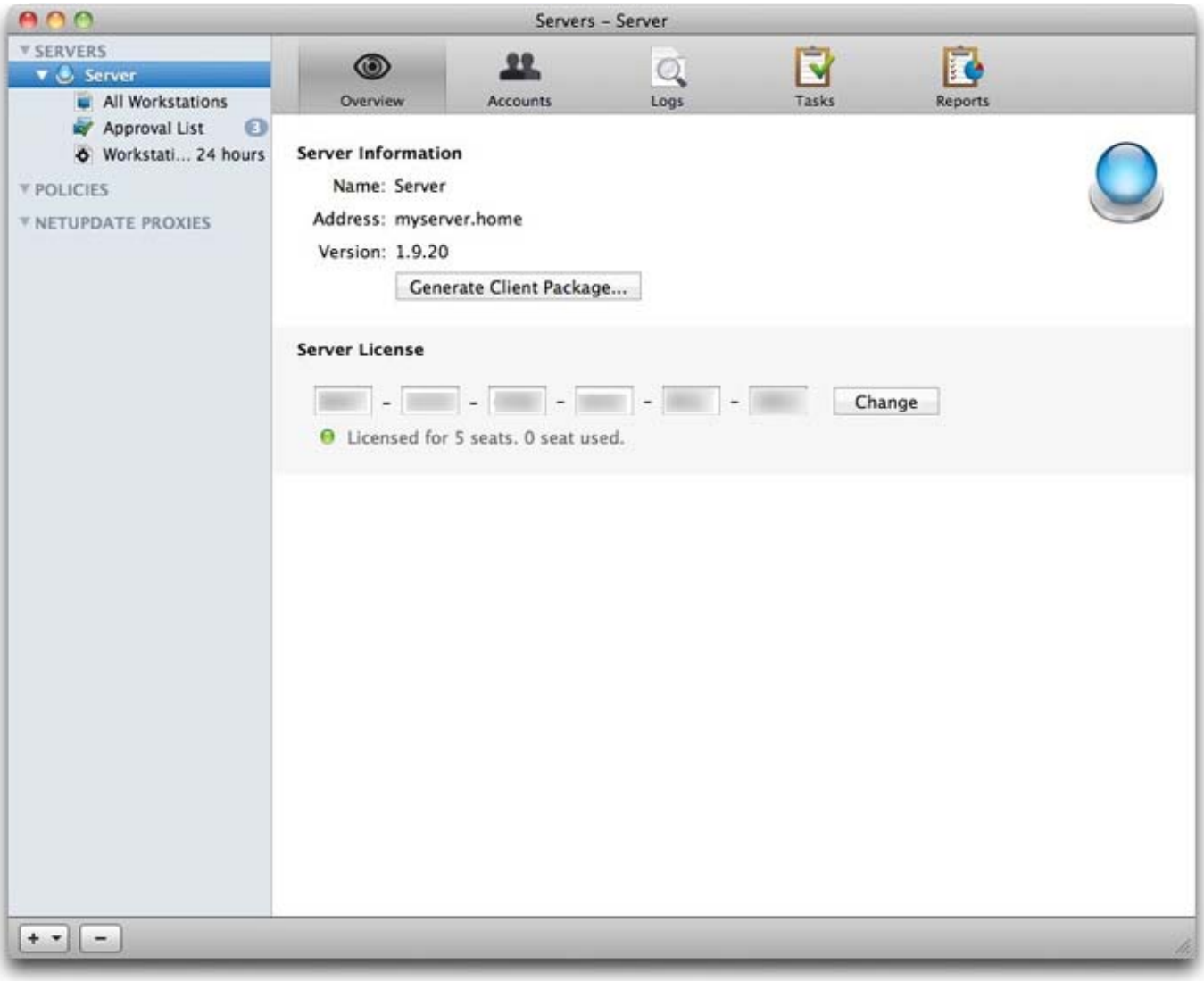
   Each key should appear only once, but the same user name can be associated with several keys, if you wish to provide access to the same user from multiple Macs.
4. Now that the key-base authentication has been set up, you can deactivate password-based authentication on the server, if you wish. To do this, edit the /Library/Preferences/Intego/Remote Management Console/Server/UsersList.plist file and delete the PasswordHash entry and its associated <data> entry for the users for whom you have set up key authentication.
5. Quit the RMCServer process on the server; you can do this from Activity Monitor or via the command line. The process will be automatically relaunched.
6. From this point on, a user need only enter their user name if they are on an authenticated Mac to connect to the server; they no longer need to enter a password.

Using Remote Management Console ››

Using Remote Management Console 2

Server Information

When you have completed the Remote Management Console 2 setup procedure, the Remote Management Console 2 application will open and your server will be visible in the sidebar. Five tabs display information about that server, or allow you to view logs, run tasks or create reports.



Overview

This displays the name and address of your server, its version number, and its serial number. You can generate a client package if you haven't already done so with the Remote Management Console 2 Assistant, or if you add workstations after initial setup.

Accounts

This is a list of user accounts set up to work with your Remote Management Console 2 server. When you configured Remote Management Console, you created a first administrator's account. You can add, remove or edit accounts by clicking the buttons below the accounts list.

Remote Management Console offers two types of accounts: Administrators and Observers. Administrators can make changes to settings, workstation lists and all other items related to managing Intego software. Observers can only view settings, lists, logs, etc. When you create an account, check **Allow user to edit settings** if you want them to be an administrator.

Logs

This tab displays logs of server activity. You can choose to display all entries or just errors. You can also choose when you want to remove logs, or do so manually.

Tasks

This shows a list of all tasks you have run using your server. You can run a new task by clicking the + button. For more on tasks see Working with Tasks.

Reports

This tab lets you create and view reports for the Macs managed by your server. For more on reports see Working with Reports.

Working with Workstation Lists

Click the disclosure triangle next to your server to see lists related to that server.

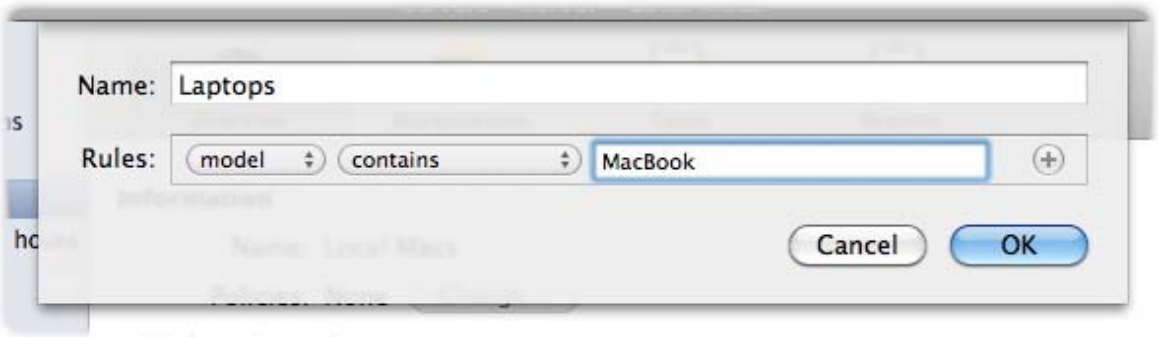
The **All Workstations** list contains all Macs that you have set up with a Remote Management Console 2 client package for that server. When you first install that package, however, computers will be in the **Approval List**. Click that list, then select the computers you wish to approve and click **Approve**. They will be added to the **All Workstations** list.

Creating Lists and Smartlists

Remote Management Console 2 lets you create two types of lists to organize the Macs that you administer. You can create lists and smartlists. The former are static lists to which you add workstations manually, and the latter populate themselves based on criteria you choose. (These lists work like playlists and smart playlists in iTunes.)

To create a list, click the + button below the sidebar and choose **New List**.... Enter a name for the list, and add any workstations you want to it by dragging them from the **All Workstations** list; you can access individual workstations from the **Workstations** tab.

To create a smartlist, click the + button below the sidebar and choose **New Smart List**.... Enter a name for the smartlist, then choose among the criteria available.

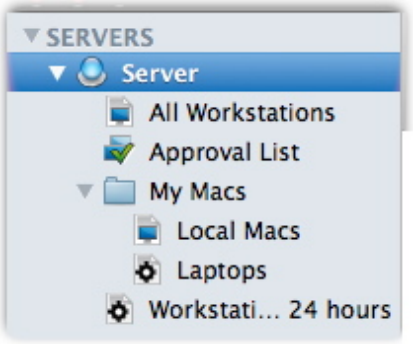


In the example above, the smartlist will find any Macs whose model names contain "MacBook," therefore finding all of the laptops being managed. Other criteria are available, such as name, system version, client version and more. Criteria can be combined by clicking the + button at the right of the **Rules:** section. An example smartlist displays in Remote Management Console 2 when you launch the program: it contains all computers that have not been connected in the past 24 hours.

Creating Groups

In addition to the two types of lists above, you can also create groups. A group is presented as a folder, and can contain lists, smartlists and/or other groups. To create a group, click the + button below the sidebar and choose **New**

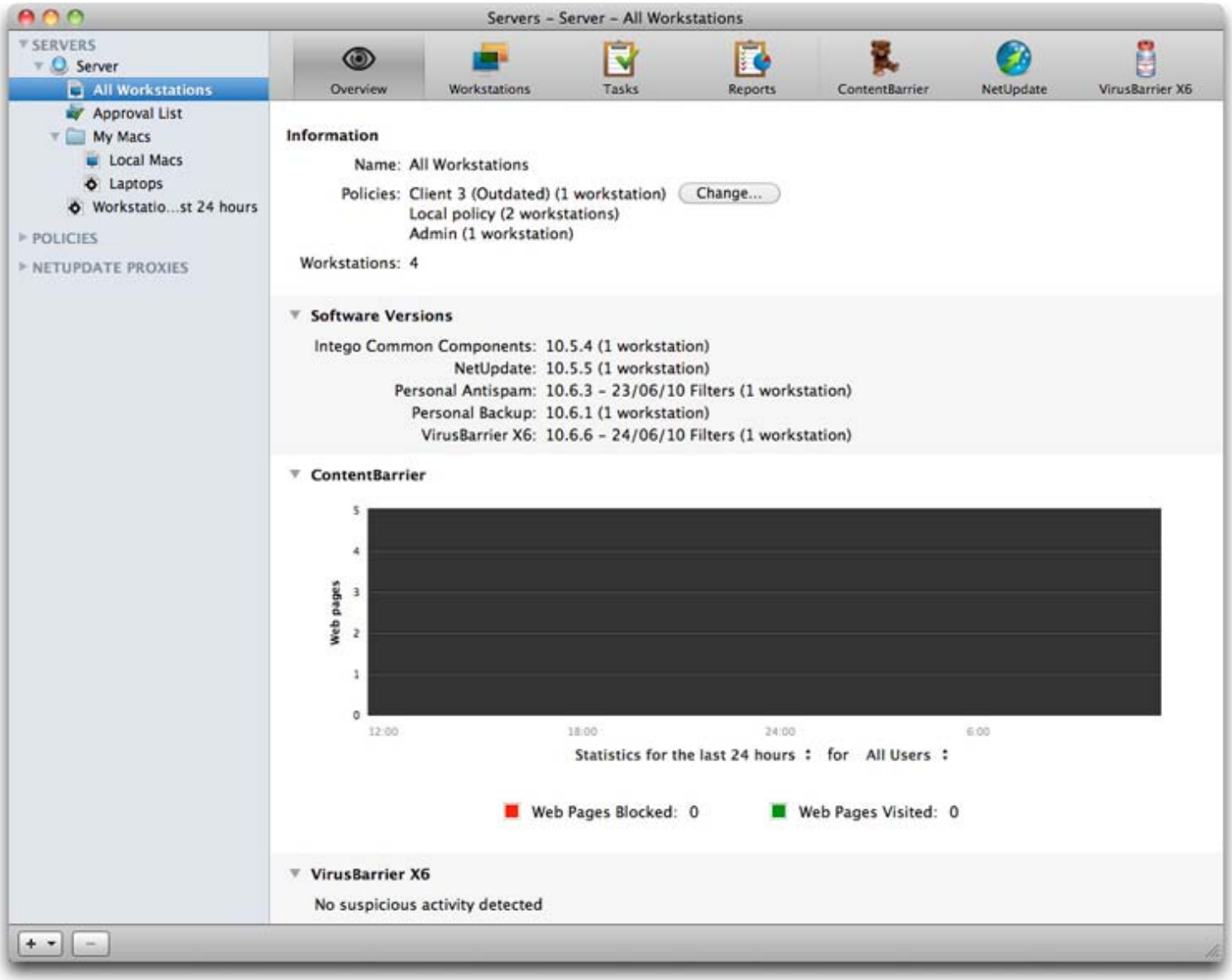
Group.... Name the group, then add lists and smartlists to it as you desire by dragging them onto the group's folder icon.



Viewing Lists and Groups

When you select a list or group, you'll see the information about the Macs in that list or group. You see **Information** about the selected item, such as its name, the policies used on the workstations it contains and the number of workstations. Below this, in the **Software Versions** section, is a list of the Intego programs and software components installed on the workstations in the selected item. This shows version numbers and the latest filter updates installed. There is also activity information for **ContentBarrier** and/or **VirusBarrier**, depending on which of these programs are installed.

The toolbar contains four tabs that provide information and access to those workstations, plus additional tabs for the Intego software you have installed on them.



- **Overview**
- **Workstations**
- **Tasks**
- **Reports**
- **ContentBarrier**
- **NetUpdate**
- **VirusBarrier**

Overview

This tab gives you an overview of the Macs in your list or group. It shows the name of the list or group, the number of workstations it contains, the policy or policies in effect, and shows some information for ContentBarrier (user statistics) and/or VirusBarrier (recent suspicious activity) if these programs are installed. Even if only one Mac in a list or group has a specific program, the section for that program will display.

Note that while Remote Management Console allows you to manage settings for VirusBarrier X6, ContentBarrier and NetUpdate, other Intego software will display in the **Software Versions** section of this pane if they are installed on client computers that you manage. This is because NetUpdate can be used to update those programs and/or their filters.

Workstations

This is a list of the Macs in the list or group. It shows the name, model, policy applied, system version, client version, last connection, and IPv4 and IPv6 addresses for each Mac. (Right-click on the column headers to choose to show or hide specific columns.) If you double-click a workstation, you can access information about that workstation. You can also change settings for that workstation's version of ContentBarrier and/or VirusBarrier from those programs' tabs.

Tasks

This tab shows tasks that have been applied to the Macs in the list or group. For more on tasks see Working with Tasks.

Reports

This tab lets you create and view reports for the Macs in the list or group. For more on reports see Working with Reports.

ContentBarrier or VirusBarrier

These tabs let you see logs for ContentBarrier or VirusBarrier. Combined logs display for all the workstations in the list or group.

NetUpdate

If you click the NetUpdate icon, you can access a list of **Software Versions** installed on the workstations in the selected item, or view a log of **Installed Updates**. From the **Software Versions** tab you can apply updates to individual programs. Click on a program, then, if updates are available, click **Update**... and follow the instructions.

Working with Policies

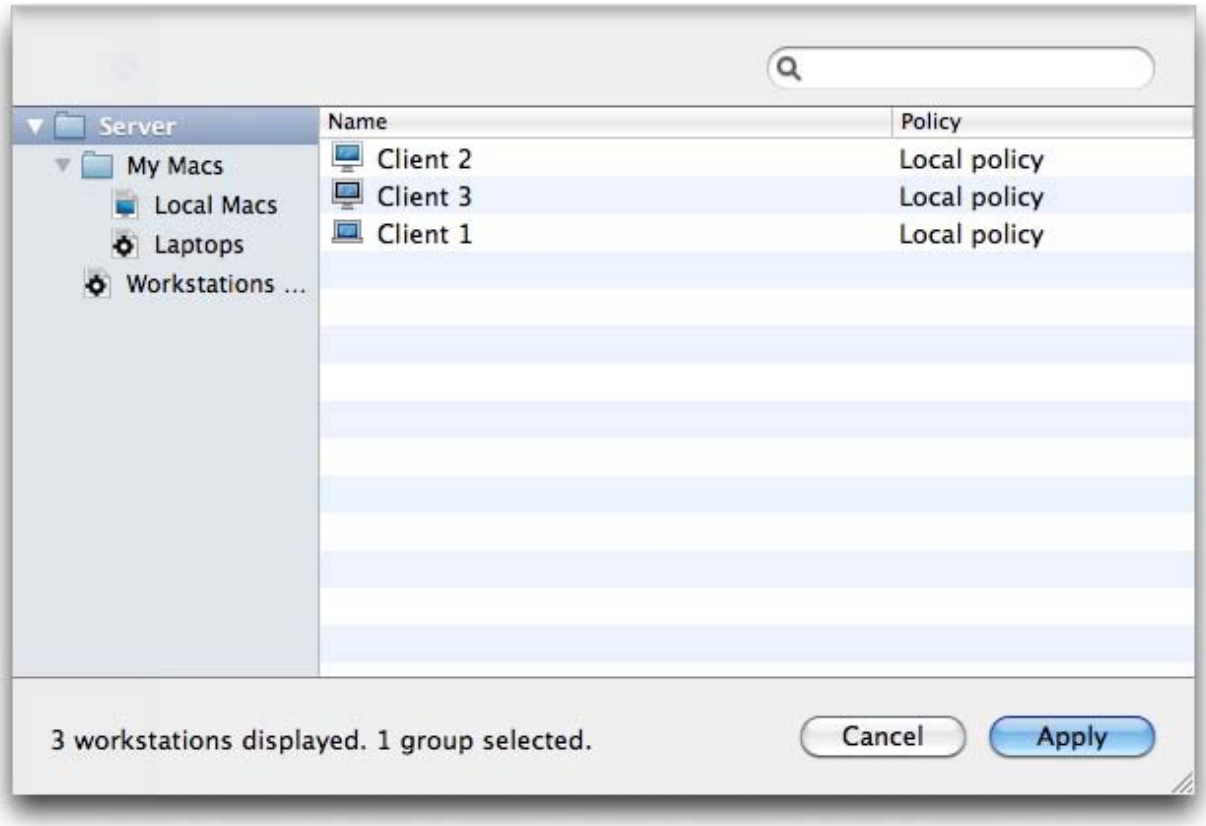
Remote Management Console 2 lets you create and apply policies to the Intego software (ContentBarrier, VirusBarrier and/or NetUpdate) on the Macs you manage. You can create as many policies as you want, and apply them to lists of Macs, groups, or even to individual computers.

Creating Policies

To create a new policy, click the + button below the sidebar and choose **New Policy**.... The new policy will display as an entry in the sidebar in the **POLICIES** section. Enter a name for the policy, then make changes to the settings of ContentBarrier, VirusBarrier and/or NetUpdate and click **Save**. When you click either the ContentBarrier, VirusBarrier or NetUpdate icon in the Remote Management Console 2 toolbar you'll have access to all of the settings of the selected program. While the actual display of the settings is slightly different from that of the individual programs, you can access all such settings. For more information on these individual settings, see the user manuals for the versions of the programs you are using on this web page.

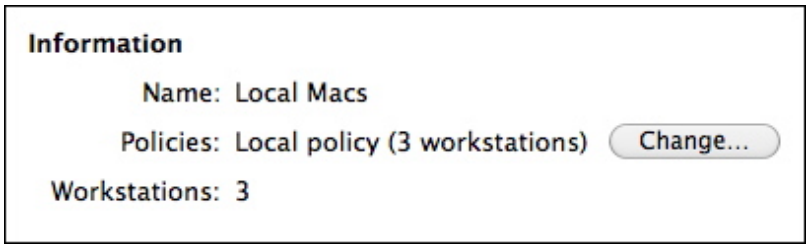
Applying Policies

When you create policies, there are two ways to apply them. If you click on the name of a policy in the sidebar, then click on **Apply to**... at the bottom of the window, the following dialog displays:

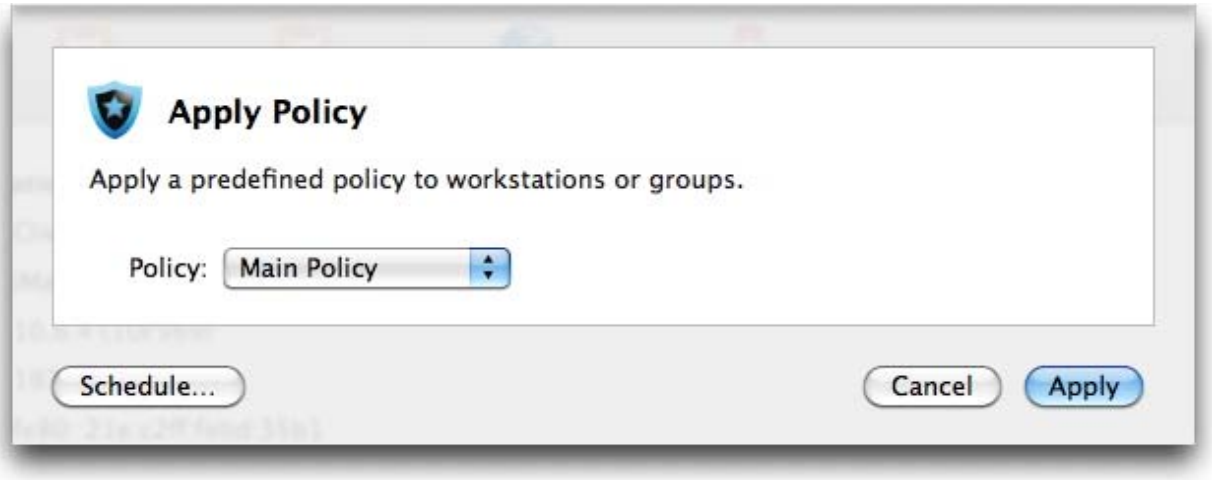


Select your server to see all the Macs it manages, or select a list or group to narrow down the list. You can also type part of a computer's name in the search field to narrow down the list. Click **Apply** to apply the policy to the selected computer.

You can also apply policies by selecting your server, a list or a group, then clicking the **Overview** button in the Remote Management Console 2 toolbar. In the **Information** section at the top of the window you'll see which policy is currently applied.



Click **Change**... to change the policy. The following dialog displays:



Choose a policy from the **Policy** pop-up menu, then click **Apply**.

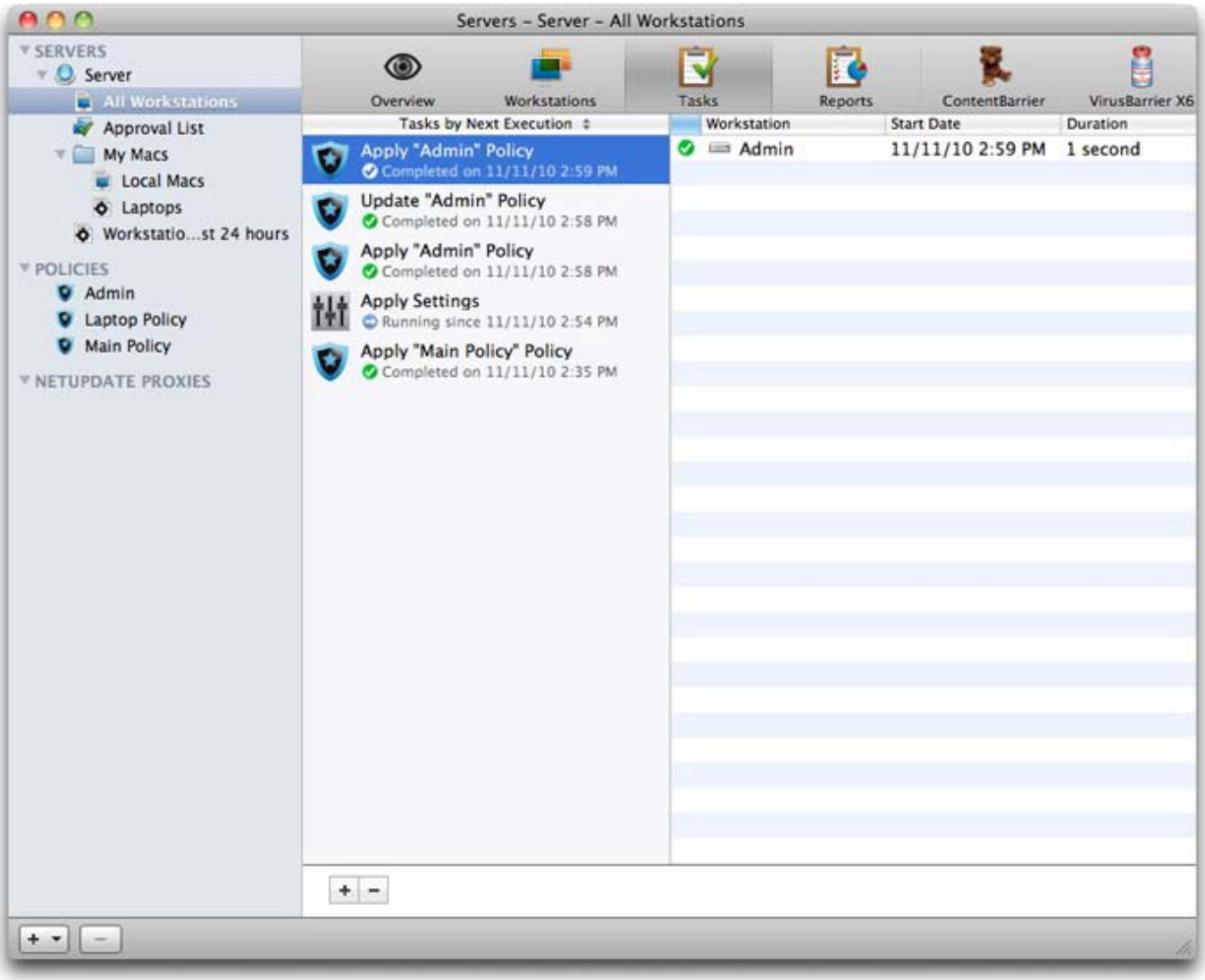
If you wish to schedule policy changes, you can do so by clicking the **Schedule**... button. When you schedule a policy, it will be applied at the time you select, and you can choose to repeat it at regular intervals of minutes, hours, days, weeks or months.

If you apply policies to computers that are not currently accessible, the change in policy will be made the next time they are on line.

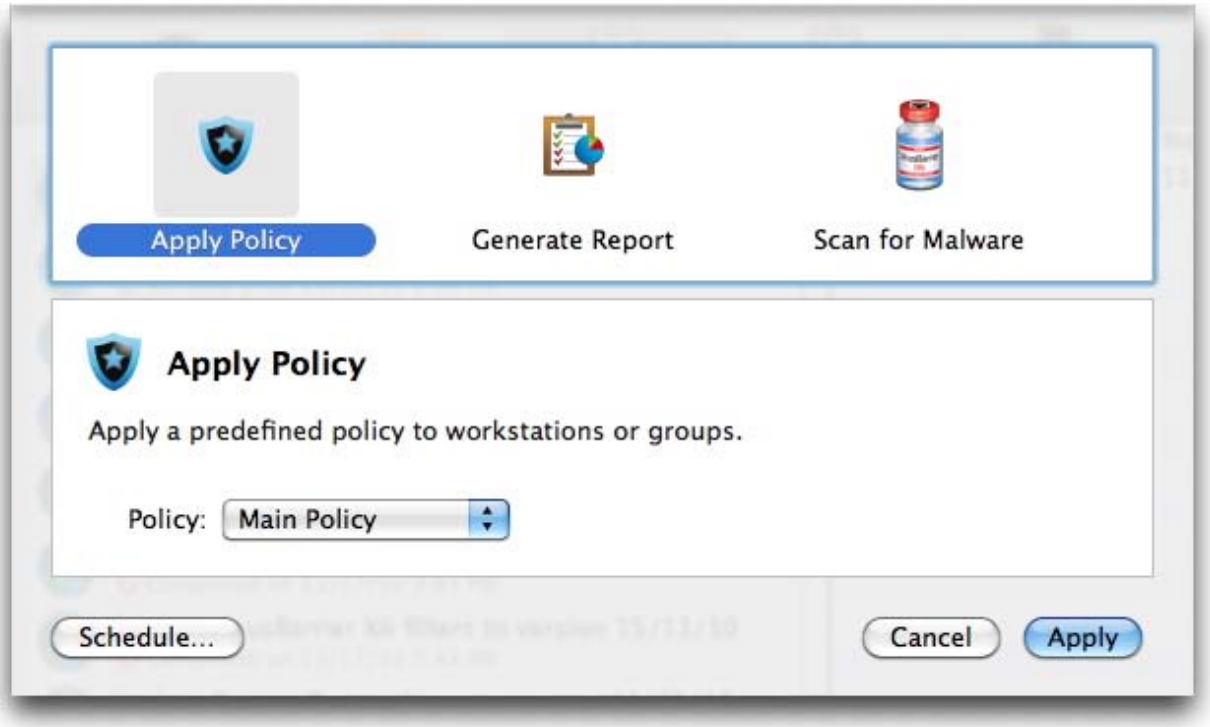
Working with Tasks

Remote Management Console 2 lets you run several types of tasks on managed computers. You can apply policies, generate reports or run malware scans with VirusBarrier. You can run tasks by selecting a server, list or group, then clicking the **Tasks** tab in the toolbar.

When you view the Tasks pane, you will first see a list of tasks. You can delete any of these by selecting them and clicking the - button below the **Tasks** list. You can select multiple items and delete them as well.



To perform a new task, select an item – your server, a list or a group – then click the + button below the **Tasks** list. The following dialog displays:



Click on the type of task you wish to run. The options for each task are different.

Applying Policies via Tasks

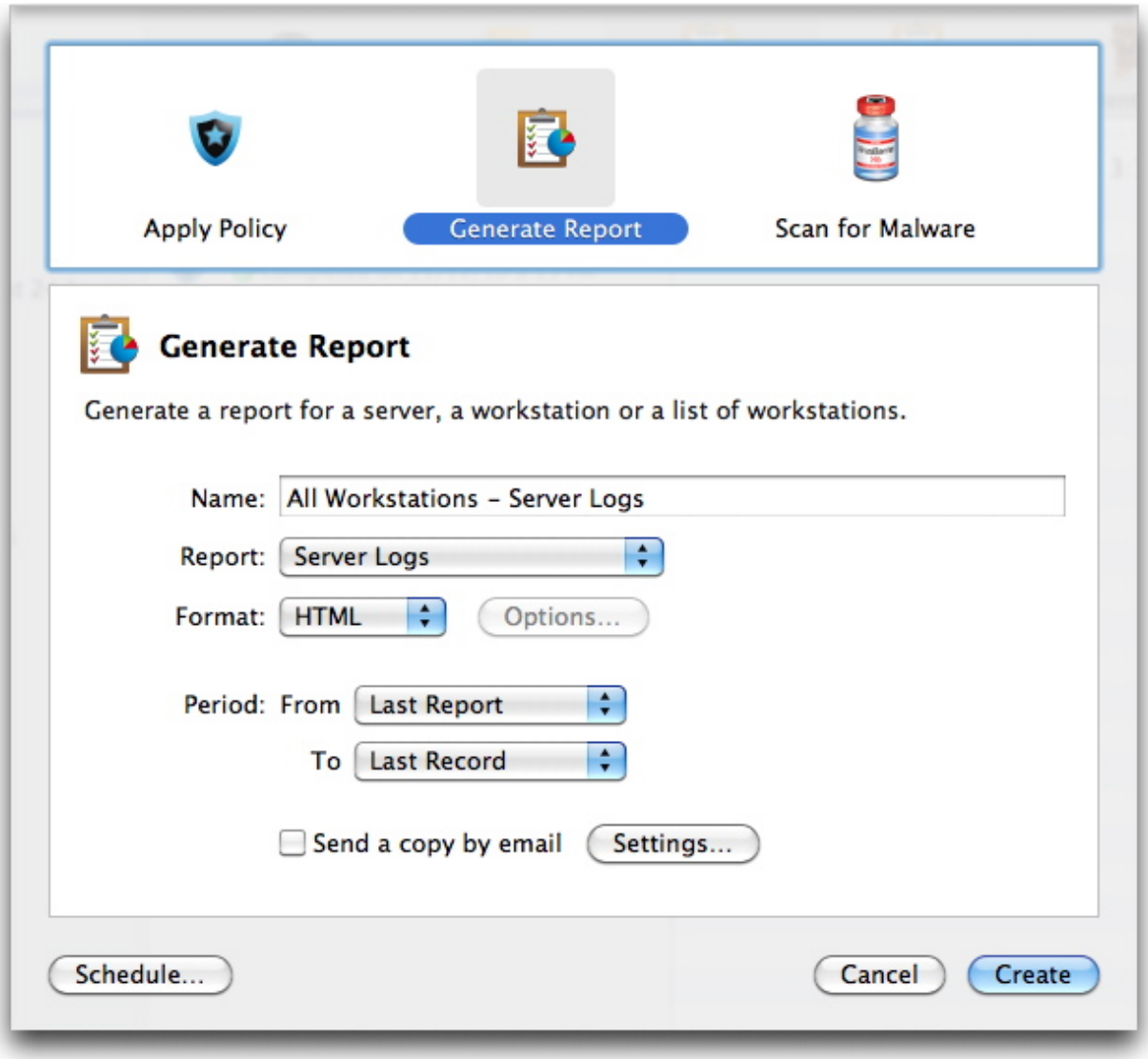
To apply a policy via Tasks, select the policy from the **Policy** pop-up menu, then click **Apply**.

If you wish to schedule policy changes, you can do so by clicking the **Schedule**... button. When you schedule a policy, it will be applied at the time you select, and you can choose to repeat it at regular intervals of minutes, hours, days, weeks or months.

If you apply policies to computers that are not currently accessible, the change in policy will be made the next time they are on line.

Generating Reports via Tasks

To generate a report via Tasks, click the Reports icon in the Tasks window. The following dialog displays:

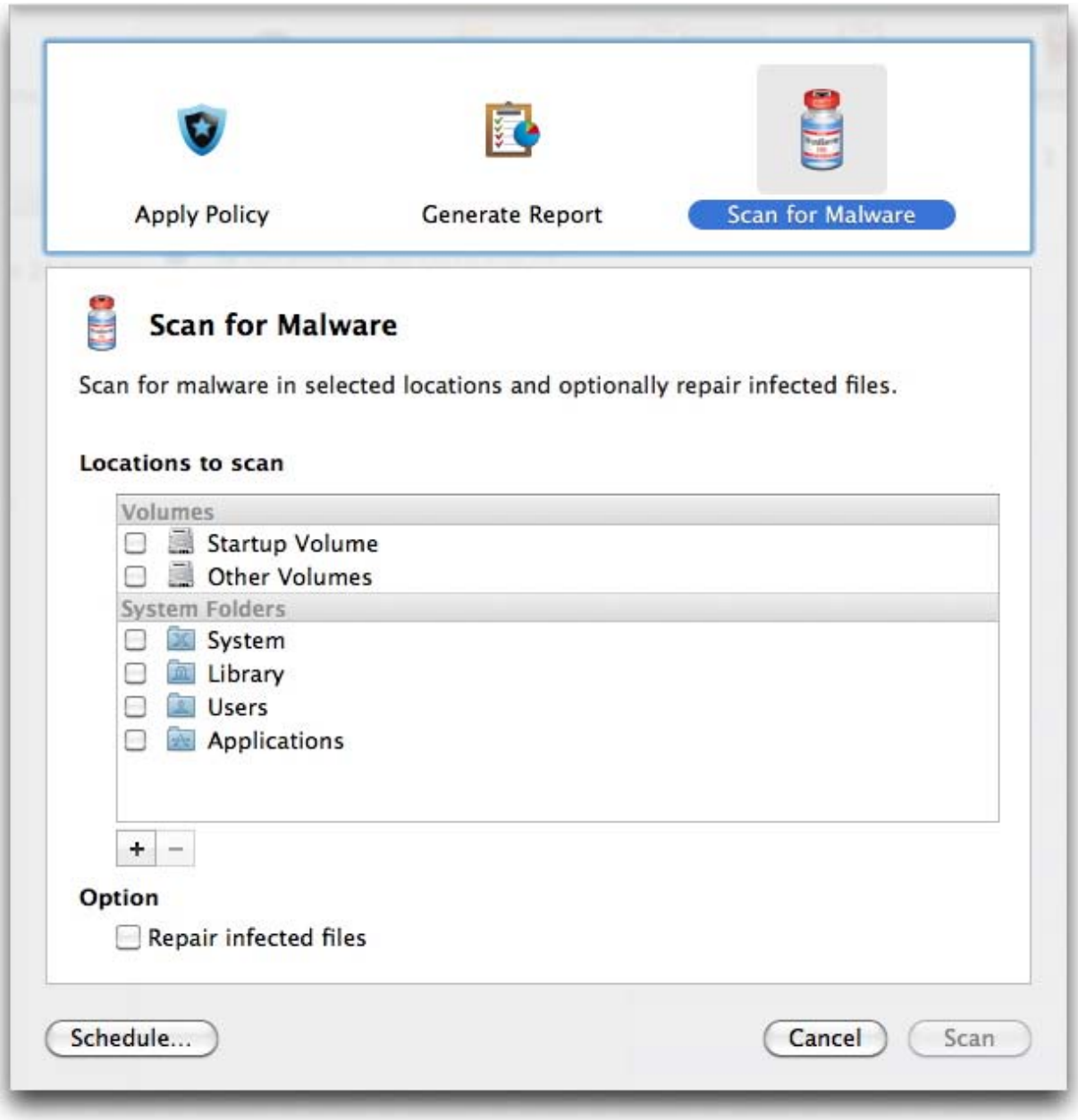


The report will be created for the item you have selected. You can choose from a number of options. See Working with Reports for more on reports and their options.

If you wish to schedule report generation, you can do so by clicking the **Schedule**... button. When you schedule a report, it will be generated at the time you select, and you can choose to repeat it at regular intervals of minutes, hours, days, weeks or months.

Running Malware Scans via Tasks

To run a malware scan with VirusBarrier via Tasks, click the Scan for Malware icon in the Tasks window. The following dialog displays:



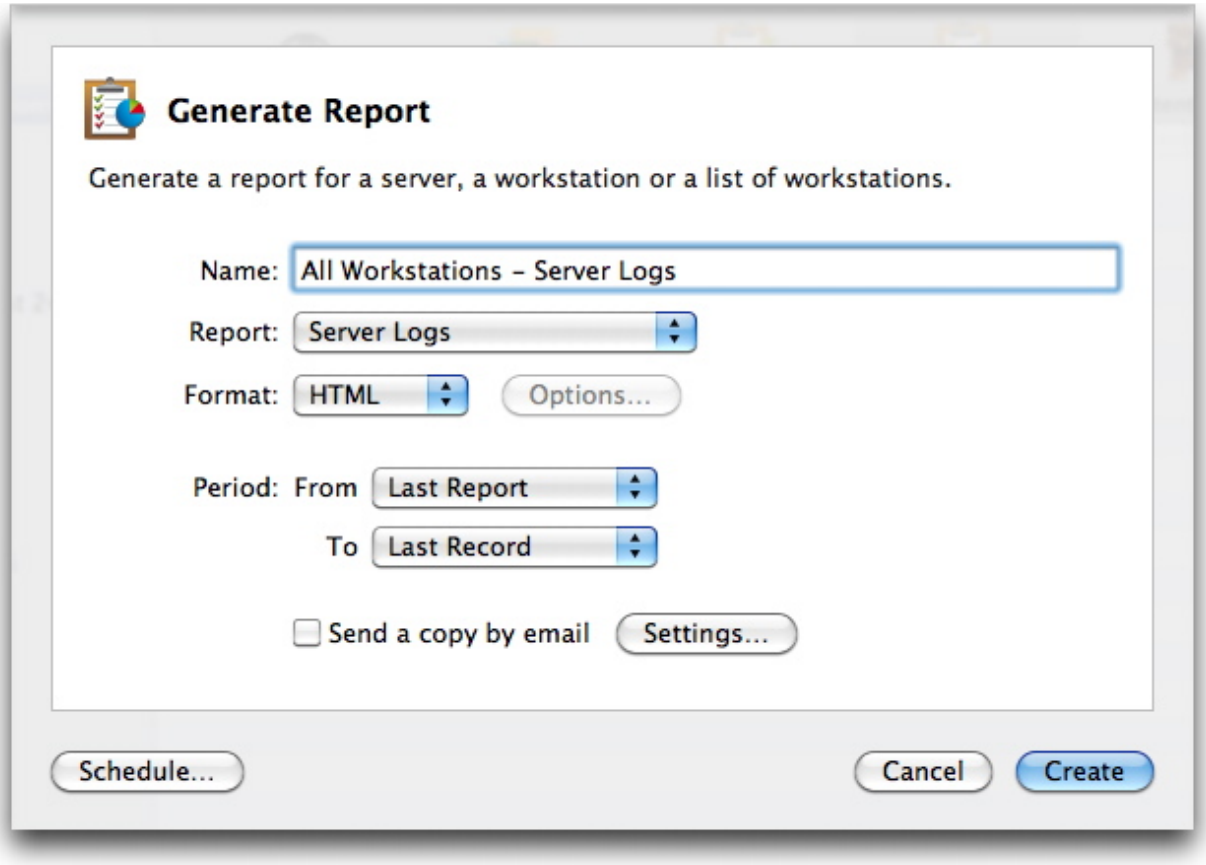
Chose the locations you wish to scan: a number of standard locations are available in the list, but you can add others by clicking the + button and entering a path in the **Additional Paths** list that displays. You can optionally choose to repair infected files during this scan.

If you wish to schedule malware scans, you can do so by clicking the **Schedule**... button. When you schedule a malware scan, it will be run at the time you select, and you can choose to repeat it at regular intervals of minutes, hours, days, weeks or months.

Working with Reports

Remote Management Console 2 lets you generate reports for individual computers, lists or groups of computers. You can view these reports in Remote Management Console, or you can export them to save them and view them in other programs.

To create a report, select a list, group or individual computer, then click the **Reports** icon in the Remote Management Console 2 toolbar. Click the + button and the following dialog displays:



Here are your options:

- **Name**: the name field is populated with the name of your selection - the list, group or computer. You can change this name if you wish.
- **Report**: choose the type of report you wish to create. You can choose from **Server Logs**, **ContentBarrier**, **VirusBarrier X6 Malware**, and **VirusBarrier X6 Network**.
- **Format**: choose HTML or PDF. If you choose the latter, you can click the **Options**... button to adjust the page setup for the resulting PDF file.
- **Period**: choose from several options available from the pop-up menus.
- **Send a copy by e-mail**: If you check this, the report will be e-mailed to one or more addresses. Click the **Settings**... button to choose e-mail settings.

When you have chosen how you wish the report to be generated, click **Create** to have Remote Management Console 2 create the report. If you wish to schedule report generation, you can do so by clicking the **Schedule**... button. When you schedule a report, it will be generated at the time you select, and you can choose to repeat it at regular intervals of minutes, hours, days, weeks or months.

Updating Client Computers

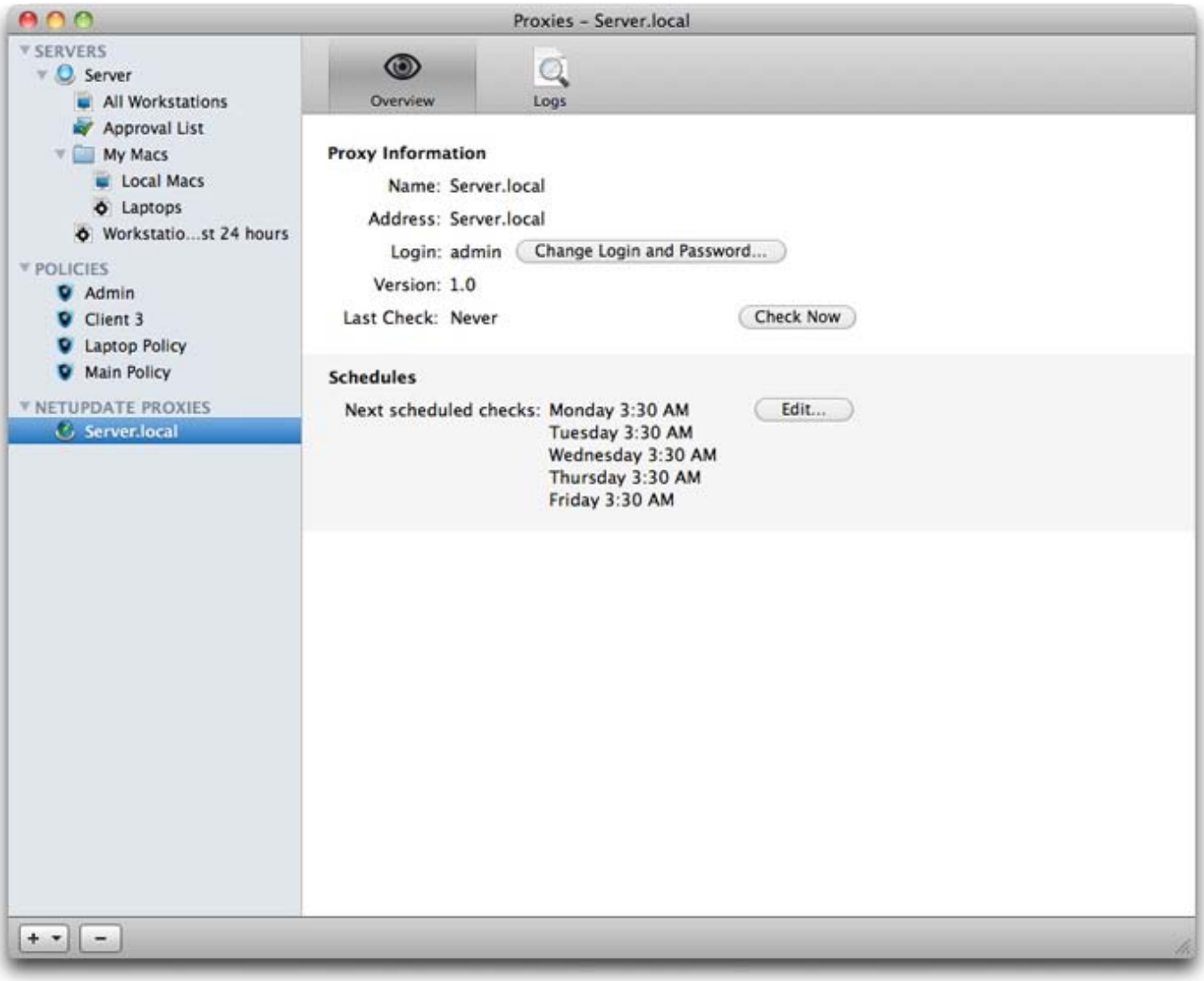
Intego software provides subscription-based updates to filters to ensure up-to-date protection from malware, for VirusBarrier, and updated content filter keywords and URLs, for ContentBarrier. Intego NetUpdate is used to provide these filter updates, as well as updates to the programs themselves. NetUpdate is installed on all client computers to ensure updates, and Remote Management Console 2 lets you use a NetUpdate Proxy, which offers centralized updating for all the Macs you manage. Rather than have each client Mac connect to the Internet to download updates, you download a single update and store it on your server, and client computers obtain the update from that location.

To use a NetUpdate Proxy, you have to add one to Remote Management Console. Click the + button below the Remote Management Console 2 sidebar and choose **Add NetUpdate Proxy**... The NetUpdate Proxy Setup Assistant displays.

In the first screen, shown above, enter the server name. You can click the triangle at the right of the field to see a list of available NetUpdate proxies. Click **Continue** to go to the next screen.

Set up your NetUpdate Proxy account by entering a user name and password, then click **Continue**. Complete the setup by clicking **Close** on the summary screen.

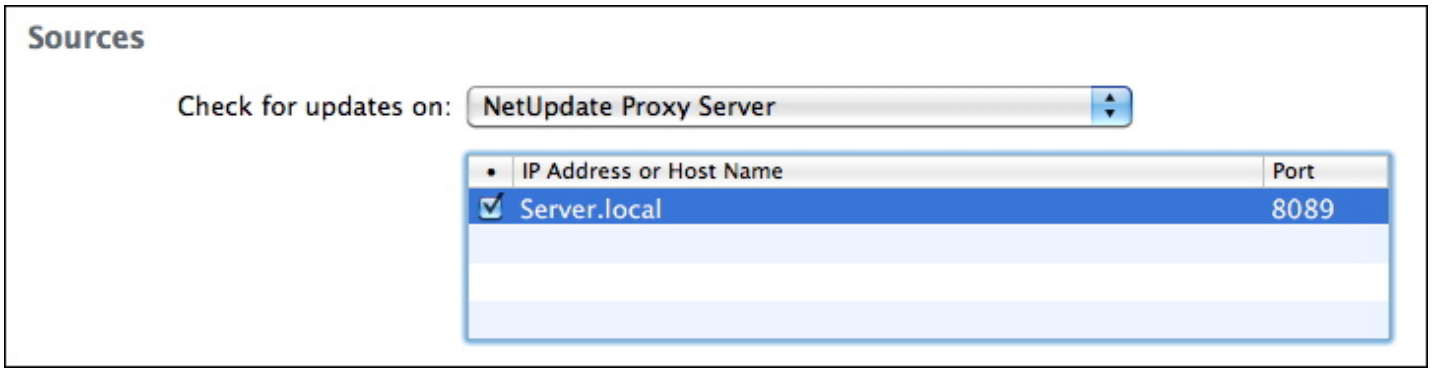
When this has finished, you'll see your NetUpdate proxy in the **NETUPDATE PROXIES** section of the Remote Management Console sidebar. If you select it, you'll see information about that NetUpdate proxy.



This pane shows you the name and address of your server, and the account that is being used. You can change the login and password for that account if you wish. It also shows the last time the server checked with Intego's NetUpdate server for updates. You can check manually by clicking **Check Now**.

In the **Schedules** section you'll see when the NetUpdate proxy is scheduled to check for updates. By default, updates are set to run once a day at a certain time. You can click the **Edit**... button and make changes in the dialog that displays: you can change the time, by double-clicking a time, or choose which days you want to check for updates, by checking or unchecking them.

To set your workstations to use the NetUpdate proxy to check for updates, click on one of your policies in the Remote Management Console sidebar, then click on the **NetUpdate** icon in the toolbar. In the **Sources** section of this screen, choose **Check for updates on: NetUpdate Proxy Server**, then check the server you want to use. (You can set up more than one NetUpdate proxy server.)

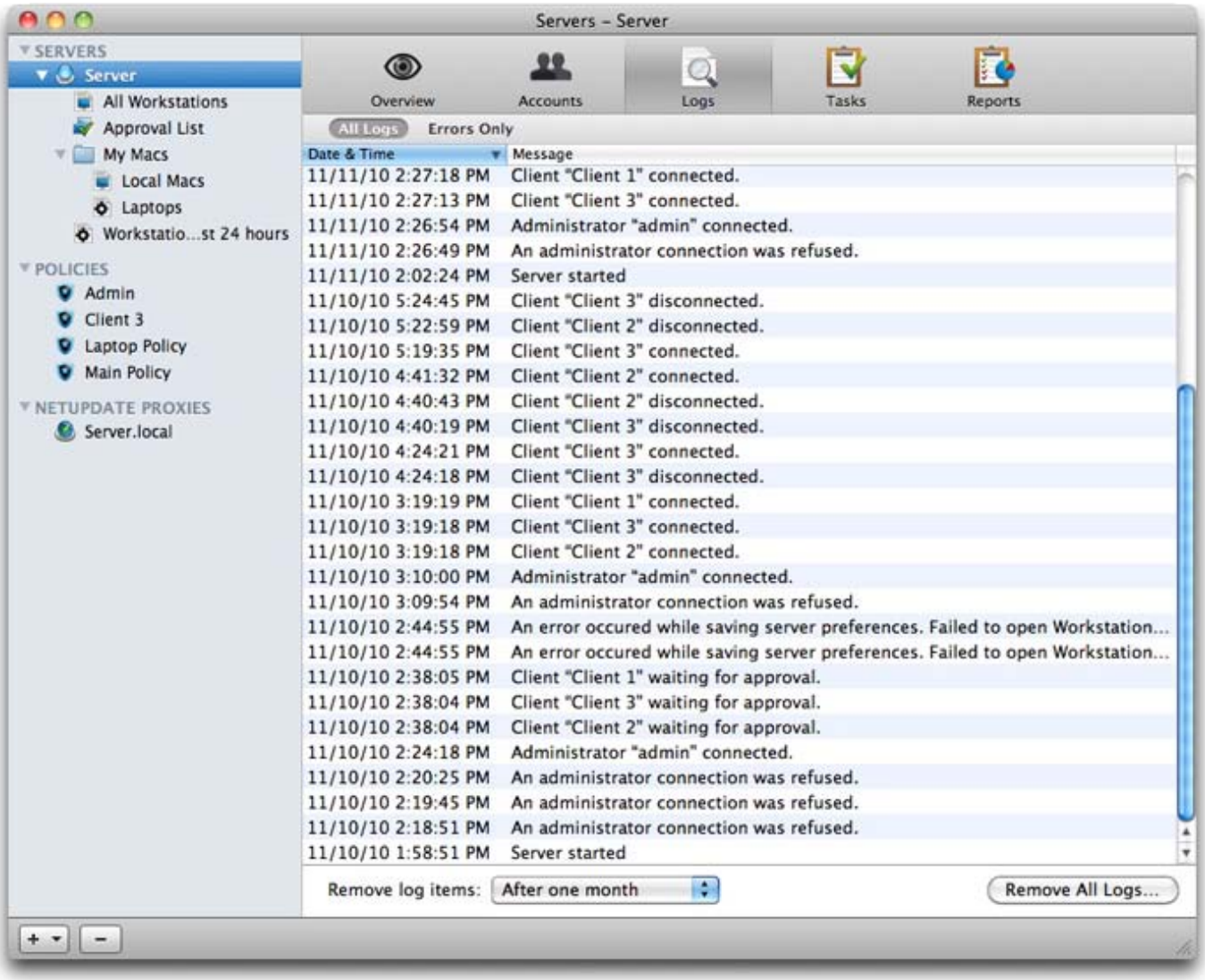


For a NetUpdate proxy to function, the computer in which it is installed must be able to accept connections through port 8089 TCP.

Viewing Logs

Remote Management Console 2 offers logs for both servers and NetUpdate proxies. Click one of these items, then click the **Logs** icon in the toolbar to see these logs.

Server logs show activity related to the server: connections and disconnections of workstations, connections by administrators, any refused connections, and any errors that occur. You can choose when to remove log entries, or you can remove all entries manually.



NetUpdate proxy logs show server activity, connections by workstations, and any errors that occur.

‹‹ Welcome to Remote Management Console 2