Netintelligence

Netintelligence Enterprise Manager Frequently Asked Questions

Version no. 1.0 (August 2007)

Contents

1 Firewall/Proxy

1.1 How do I configure my firewall/proxy for Enterprise Manager deployment?

The Netintelligence Client program requires access through your organisation's firewall/proxy server to the following IP ranges on ports 80/TCP and 443/TCP in order to function correctly:

Range	IPs	Mask
62.233.64.0/18	62.233.64.0 - 62.223.127.255	255.255.192.0
84.22.161.0/24	84.22.161.0 - 84.22.161.255	255.255.255.0
62.128.193.0/24	62.128.193.0 - 62.128.193.255	255.255.255.0
209.97.194.32/27	209.97.194.32 – 209.97.194.63	255.255.255.224
209.97.202.218/32	209.97.202.218 - 209.97.202.218	255.255.255.255

The services **LiteClient.exe**, **LiteClientAM.exe** and **NINDfltr.exe** should be given access rights through the firewall.

Please refer to the documentation for your firewall/proxy for instructions on how to configure these settings.

The above firewall/proxy configuration will allow all Netintelligence clients to pass through the firewall/proxy services unhindered.

Important: customers should provide Netintelligence Support with a list of the proxies that they use, prior to installation. Please pass these details on to support@netintelligence.com.

1.2 How do I configure a machine's personal firewall for Enterprise Manager deployment?

The services **LiteClient.exe**, **LiteClientAM.exe** and **NINDfltr.exe** should be given access rights through the personal firewall. Please refer to the documentation for your personal firewall for instructions on how to configure these settings.

2 Policies

2.1 What is the Default Policy?

Netintelligence has a special kind of policy, called the 'Default Policy', that is applied to all users of machines to which Netintelligence has been deployed. The rules of this policy will be effective wherever another policy rule applied to a user does not conflict. In other words, this policy applies to all users wherever you have not already stated a specific setting in another policy applied to any given user.

2.2 What policy is effective when I apply more than one policy to a group of users?

Having more than one policy applied to a group of users means that it is possible to have different rules set for the same policy category, for those users. In this circumstance (where rules for policy categories overlap), some rules take priority over others. The order of priority for these rules is always:

'Only allow' > 'Allow' > 'Warn' > 'Block'

For example, if you have set an 'Allow' rule for a category in one policy (not excepting the Default Policy), and 'Block' in another policy, then when both of these policies are applied to the same user group, the 'Allow' rule overrules the 'Block' rule. The combined effect of the application of these two policies to a user group is that the user will be allowed access to the category in question.

Note that the Default Policy is applied to all users, and so 'Allow' rules in your Default Policy will overrule any rules for the same category in your custom policies. When planning the application of customised policies, in general you are advised to leave the category as 'Not Set' in the Default Policy, then apply your preferred rule to the category in your customised policies.

2.3 The blocking for my Default Policy is not working. Why?

If the Default Policy has a category set to 'Block' but a user is not being blocked, then there is usually a problem with the settings you have specified. To resolve this, follow these troubleshooting steps:

1. Check the **Default Policy** as follows:

   Web Site Categories - check that the particular category is set to 'Block'.
   Times - check that appropriate times have been applied. The start time should always occur after the stop time. Also note that, to set a period of an entire day, you must use a start time of 00:00 and a stop time of 23:30, rather than 00:00 to 00:00 (the latter represents 'no elapsed time' between the start and stop times, i.e. the same time on the same day).

2. Check any **custom policies** applied to any affected user groups as follows:

   Groups - check which user groups are specified in the policy, then verify that the user in question is in fact included in one of the groups (using Group Settings).
   Web Site Categories - once you have verified the above, check that the category in question is not set to 'Only Allow', 'Allow' or 'Warn' (these settings will overrule your Default Policy settings).
   If you wish the affected user to be blocked for this category, you must make changes to either exclude

the user from the affected user group, or to prevent application of this custom policy to this user group.

2.4 What is the effect of using the 'Not Set' rule option?

The 'Not Set' rule option indicates that no action will be taken for this category. When setting up policy rules, we recommend that you use the 'Not Set' rule option in preference to the 'Allow' option. This enables normal internet use (i.e. users can visit sites as they would normally with no action from the Netintelligence Client). The 'Allow' rule option should be used if you want to 'unblock' URLs that are blocked by virtue of being included in a predefined Netintelligence category.

2.5 How do I allow access to some URLs in a 'blocked' category?

To exclude URLs from blocking, create a custom category (using Custom Web Categories) and add the URLs you want to allow into it. The custom category will now be available for you to use in your customised policies.

If you want to allow access to these URLs for *all* users, set the newly created custom category to 'Allow' in your Default Policy. Please note that it can take up to 20 minutes for the Netintelligence Client programs to update with this policy change.

If you want to allow access to these URLs for *specific* users, you can use the new custom category in the same way as existing categories, by either editing existing policies applied to existing user groups, or by creating a new user group and a new policy and applying the new policy to the new user group (using Group Settings).

3 Deployment

Important: please note that the machine on which your Netintelligence Deployer is installed should NOT be firewalled. The Netintelligence Deployer requires access to all the machines on your network on which a Netintelligence Client program is (or will be) installed, and should be set up with an administrator account.

For an initial deployment, we recommend that you deploy to a small number of machines (e.g. 1-10), over a period of one hour. For subsequent deployments, we recommend that you set up deployment jobs for small batches (e.g. up to 50 machines), and for no longer than 24 hours.

3.1 I'm getting an error when I attempt to remote deploy. What should I do?

Common deployment errors are:

- Deployment Failed. Failed to Connect to Machine. Machine Possibly Offline.
- Failed to Connect to Remote Machine. Possible reasons: Machine Offline, No Admin Share or Access Denied.
- Failed to Connect to Remote Registry.

Where remote deployment has failed with one of the above errors, you must check the individual machine involved:

1. Check that the machine is online.
2. Ping the machine by name from the Deployer machine – deployment works using machine name only, not IP.
3. Check that the Client machine's firewall allows the connection, or is switched off during deployment.
4. Check that the user account supplied to the Deployer service has the correct privileges to deploy to the Client machine. This user account must be able:
    a. to access the C$ (admin Share) of the Client machine, and to copy files.
    b. to access Remote Registry and to create registry keys.
    c. to access Remote Services and to create services.
5. Check that the Remote Registry Service is running on the Client machine.

4 Data Recording Problems

4.1 No data is being shown for a machine in my Control Centre. What should I do?

There are a number of reasons why data is not being recorded. Follow the troubleshooting steps below:

1. Check proxy/firewall settings (see 1.1 How do I configure my firewall/proxy for Enterprise Manager deployment? and 1.2 How do I configure a machine's personal firewall for Enterprise Manager deployment? on page 3).
2. Check that the client is still installed (using Windows® Add/Remove Programs).
3. Check that the Netintelligence processes in Windows® services are running (using Start menu > Control Panel > Administrative Tools > Services). The services that should be running are:
    a. Netintelligence Client
    b. Netintelligence Web Filter
    c. Service Monitor

4.2 One of my machines does not appear in the Machine Summary. Why?

A machine may not appear in the Machine Summary for a number of reasons:

1. The machine has not been restarted after installation.
2. Sufficient time has not elapsed since installing/restarting the machine (it can take up to 30 minutes after installation/restart for a machine to be added to the Machine Summary page).
3. There is no Web Sites Visited, Web Blocking or Instant Messenger data yet for the machine for the Client to send (there must be Web Sites Visited, Web Blocking or Instant Messenger data for a machine for it to be displayed in the Machine Summary).
4. The Client may not be communicating due to a network firewall/proxy issue (see 1.1 How do I configure my firewall/proxy for Enterprise Manager deployment? on page 3).
5. The Client may not be communicating due to a personal firewall issue (see 1.2 How do I configure a machine's personal firewall for Enterprise Manager deployment? on page 3).

5 Netintelligence Anti-Virus and Firewall

5.1 I'm getting a message that my licence key has expired. Why?

This message comes from the Netintelligence Anti-Virus and/or Firewall program. Note that this does not indicate the end user's Netintelligence account has expired.

The Anti-Virus and Firewall licence keys update automatically every 30 days. These programs use the Client program for their licence updates.

To allow the anti-virus/firewall licence key to update, ensure that the Netintelligence Client program is installed and running, and that the machine has an enabled internet connection.

5.2 I'm getting an error when attempting to update the virus database. What should I do?

Restart the affected machine and attempt the update again.

If you are still unable to update the virus database, then fully uninstall and then reinstall the Anti-Virus program.

6 General

6.1 Debug Logs

Some problems may require debug logs to be gathered from the affected machine(s). Netintelligence Support will instruct you on what is required from the end user, on a per case basis.

If Netintelligence Support requests these logs, the Log program can be downloaded by accessing the following URL:

http://downloads.netintelligence.com/dbgvnt.zip

Once instructed by Netintelligence Support, please ask the end user to unzip the program and run it on the affected machine(s) for 20-30 minutes (the timescale may vary depending on the problem).

The end user should then save and zip the logs for return.