nFront AD Disabler

Never worry about dormant accounts again.

Version 2.6.00

Documentation

Contents

NOTE: Please report any problems with this document to feedback@nFrontSecurity.com. Your feedback is important and we sincerely appreciate your help.

nFront AD Disabler Overview

nFront AD Disabler is a Windows application that will automatically monitor and disable dormant Windows Active Directory users.

Disabling accounts after a period of inactivity should be a standard security practice within your organization. Furthermore it is a requirement of compliance initiatives like PCI and IRS 1075.

With nFront AD Disabler you never have to worry about dormant or inactive accounts again.

Features:

- Determines last "true logon time" for all active directory accounts. In other words, it scans across all domain controllers to get the correct last logon time for each user.
- Can disable accounts even though all domain controllers are not available at the time of the query.
- Do not disabler system accounts like IUSR_<machine-name>.
- Do not disable the built-in Administrator account.
- Do not disable specific groups like a group for service accounts.
- Generates local HTML reports.
- Can email a PDF or HTML report of the dormant accounts to an Administrator.
- Builds a CSV file of disabled accounts.
- Maintains a running log of all accounts that have been disabled by nFront AD Disabler. This log does not track accounts that have been disabled outside of nFront AD Disabler.
- Smart enough to skip accounts that you created yesterday whose last logon time is "never."

Limitations of the Evaluation Version

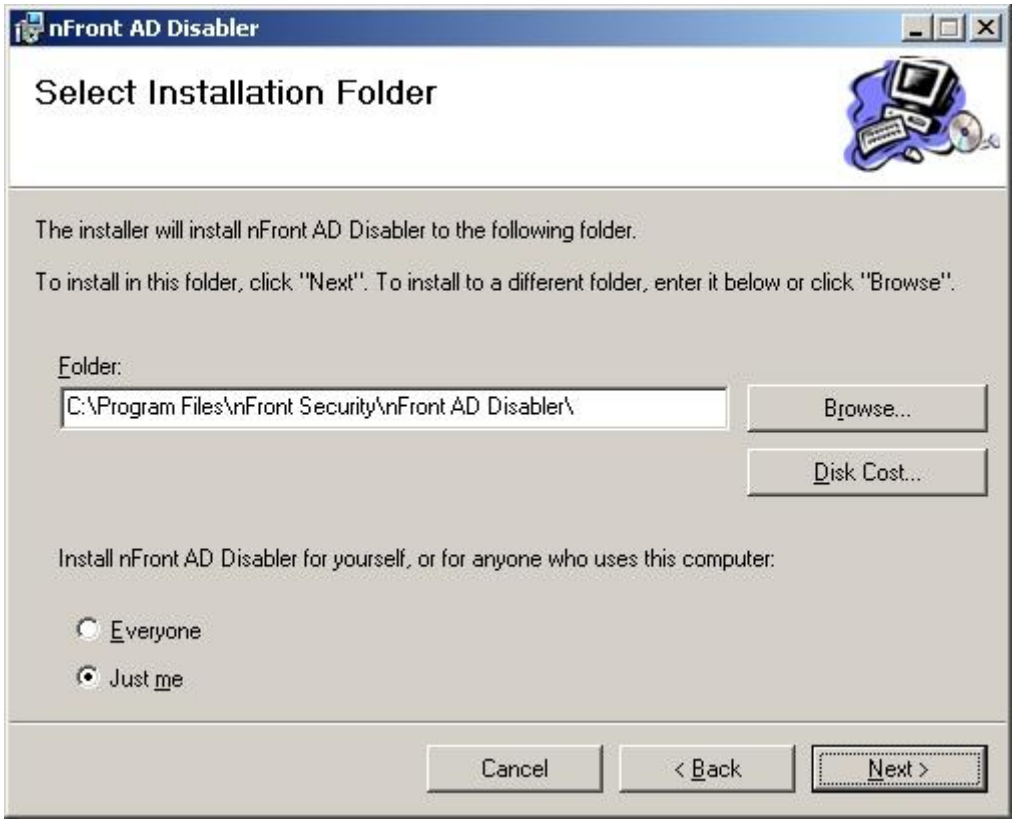
The evaluation version has the following limitations:

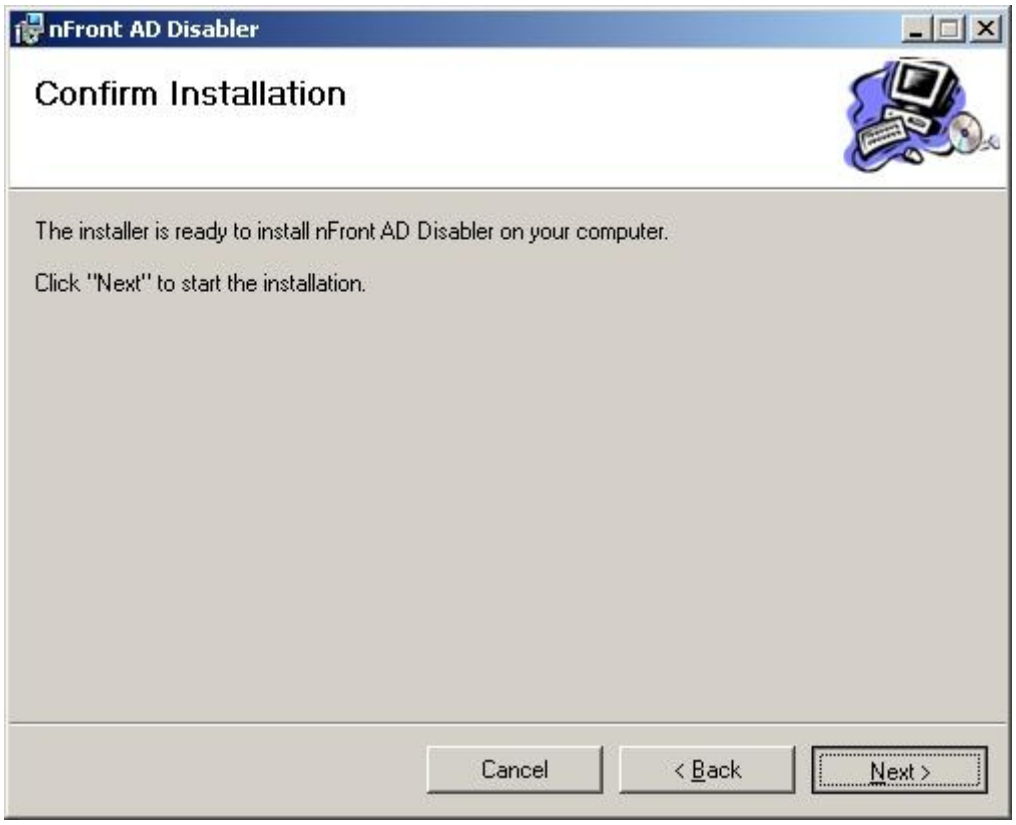
- Reports up to 3 inactive accounts
- Does not disable any dormant accounts

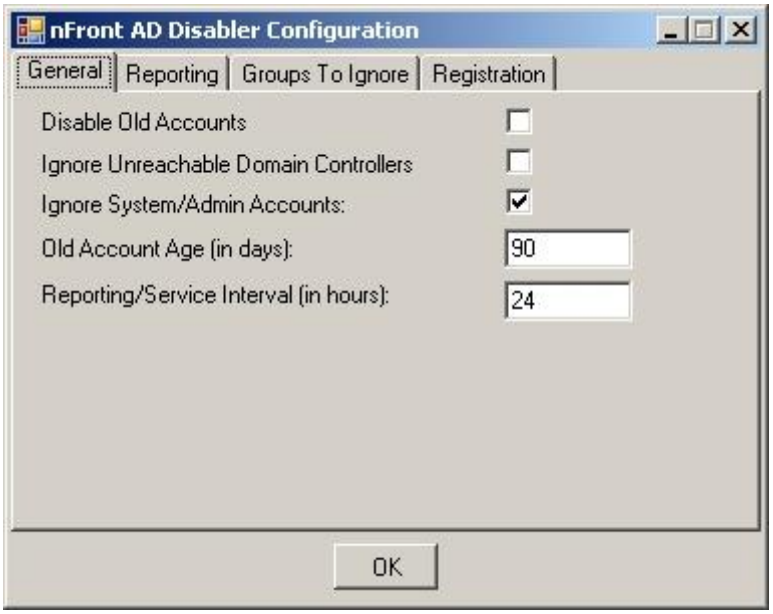
Installation

nFront AD Disabler is packaged in an MSI format. The software is installed and run on a domain controller. It will run on a Windows 2000, Windows 2003 or Windows 2008 domain controller. A Windows 2000 or Windows 2003 domain controller will require a download and install of the .NET Framework 2.0 or later. You can get more information and download the latest Microsoft .NET Framework at http://www.microsoft.com/net/.

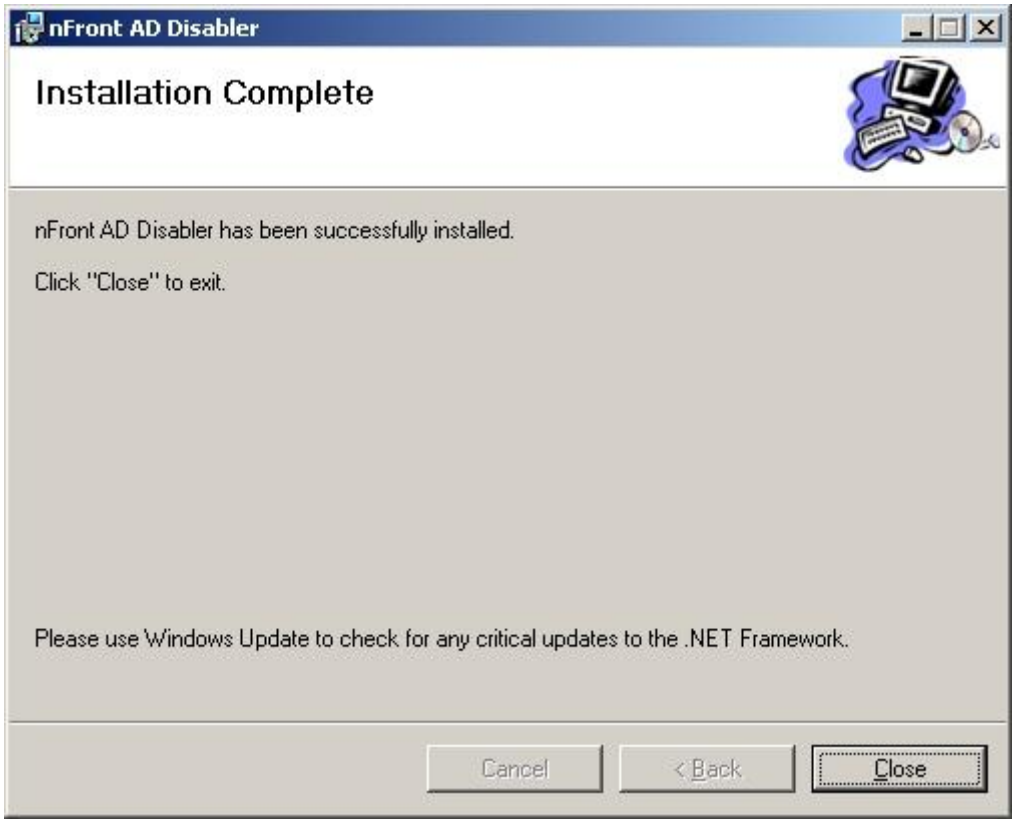
The following screenshots outline the installation process. During installation you are prompted with the configuration utility. To learn more about the configuration settings please see the section of this document titled "Configuring nFront AD Disabler."





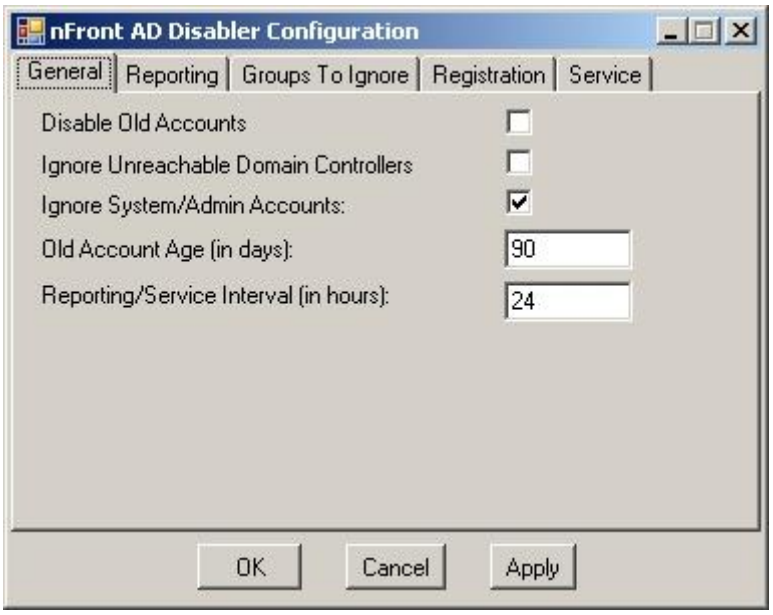


See “Configuring nFront AD Disabler” section of this document for more information on the settings in the tabbed configuration dialog.

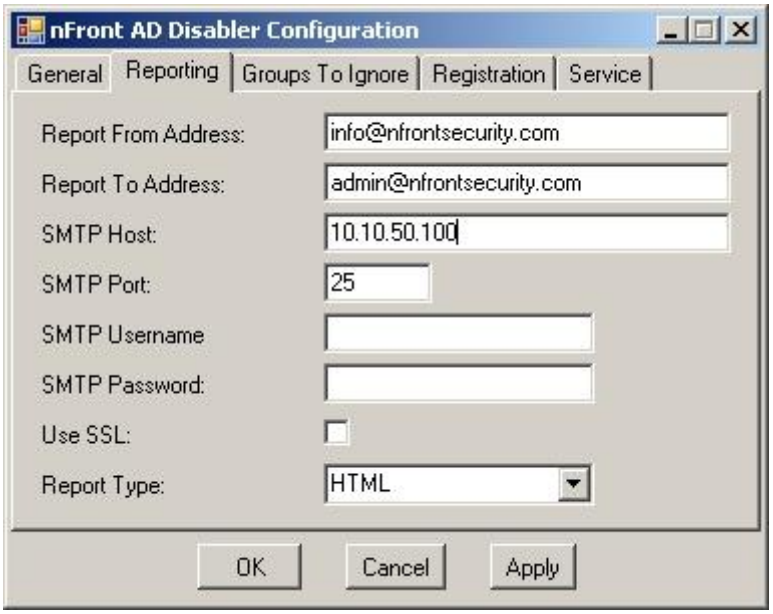


Configuring nFront AD Disabler

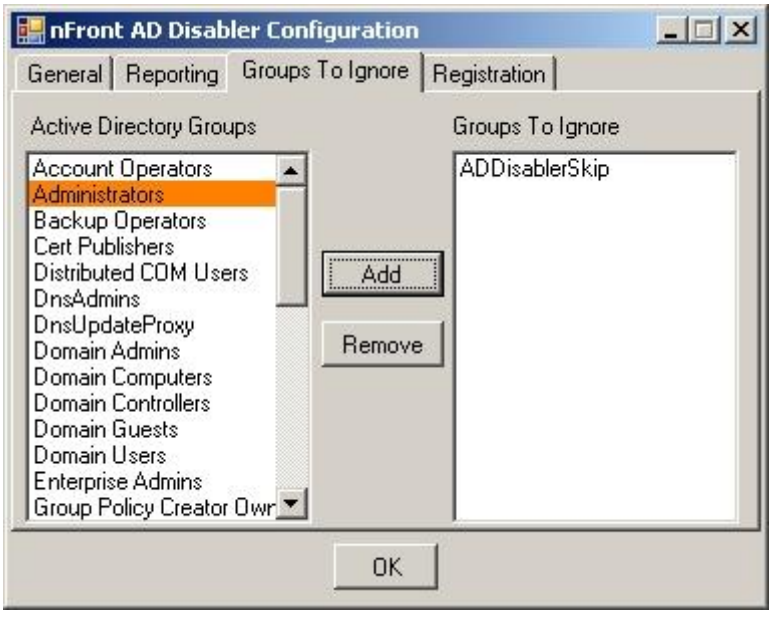
nFront AD Disabler can be configured during installation or later via a Start Menu shortcut.



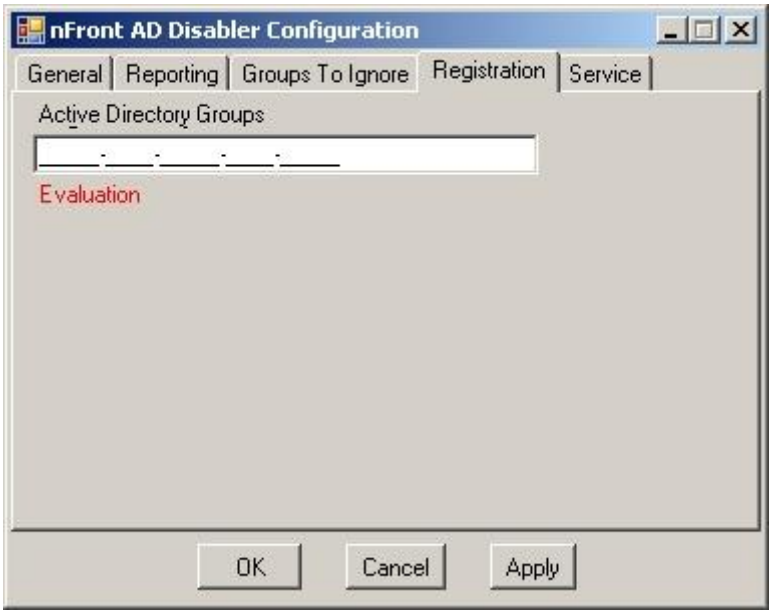
Disable Old Accounts	If this box is not checked the software runs in a "reporting only" mode. It will generate a local report and a report via email but it will not disable any dormant accounts that are identified.
Ignore Unreachable Domain Controllers	To get the "true" last logon time all domain controllers must be queried for each user account. The report will list the names of any domain controllers that were not reachable at the time of the query.
Ignore System/Admin Accounts	The built-in Administrator account is ignored. Accounts that start with username IUSR_, IWAM_, and SUPPORT_ are ignored also. The built-in Administrator account is detected based on SID so renamed built-in Administrator accounts will also be ignored.
Old Account Age (in days)	Accounts with a last logon time greater than the time specified here will be declared as dormant accounts.
Reporting/Service Interval (in hours)	By default the service runs once per day.



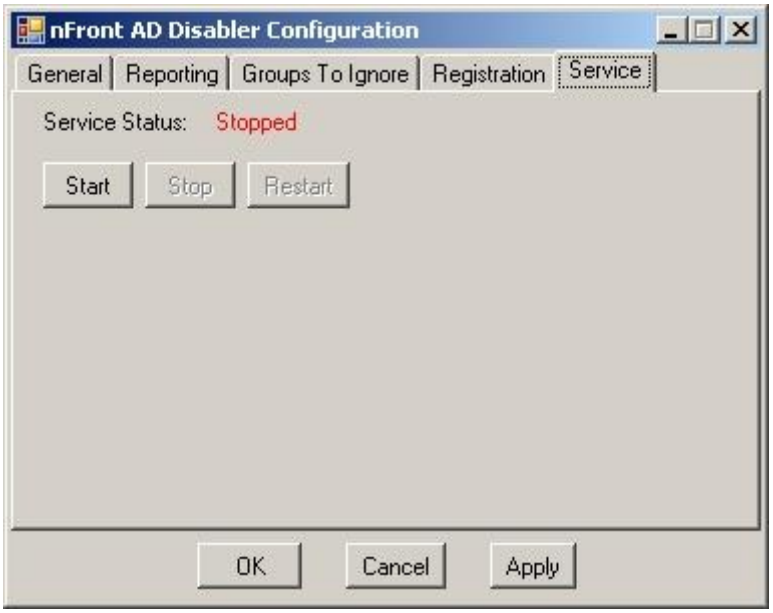
Report From Address	The email address from which you wish to receive email reports.
Report To Address	The email address to which you wish to send reports.
SMTP Host	Your email server specified with an IP address or DNS name.
SMTP Port	Default port is 25. Other ports may be used.
SMTP Username / Password	This is required only if your SMTP Host server requires authentication.
Use SSL	If enabled, the application connects to the SMTP server using SSL.
Report Type	Default reporting format is HTML. However you may also receive reports as a PDF attachment.



Groups To Ignore	You should include groups of accounts that you wish to skip here. It would be a good idea to skip accounts used for services like Microsoft Exchange, Sharepoint and SQL Server.



Registration	A valid license code will enable nFront AD Disabler to report more than 3 dormant accounts and enable the ability to disable them.



Service Tab	This gives you a convenient place to start and stop the service.

Reporting

nFront AD Disabler maintains a robust reporting system. The product can email reports to an administrator. It will also generate a local copy of the report.

Email Reporting

The system is designed to email reports to the "Report To Address" specified in the configuration. The reports may be sent in an HTML email format or a PDF format. If there is an error sending the report via email an event will be logged to the Application Log of the Event Viewer.

Example Report sent via email:

nFront AD Disabler Report

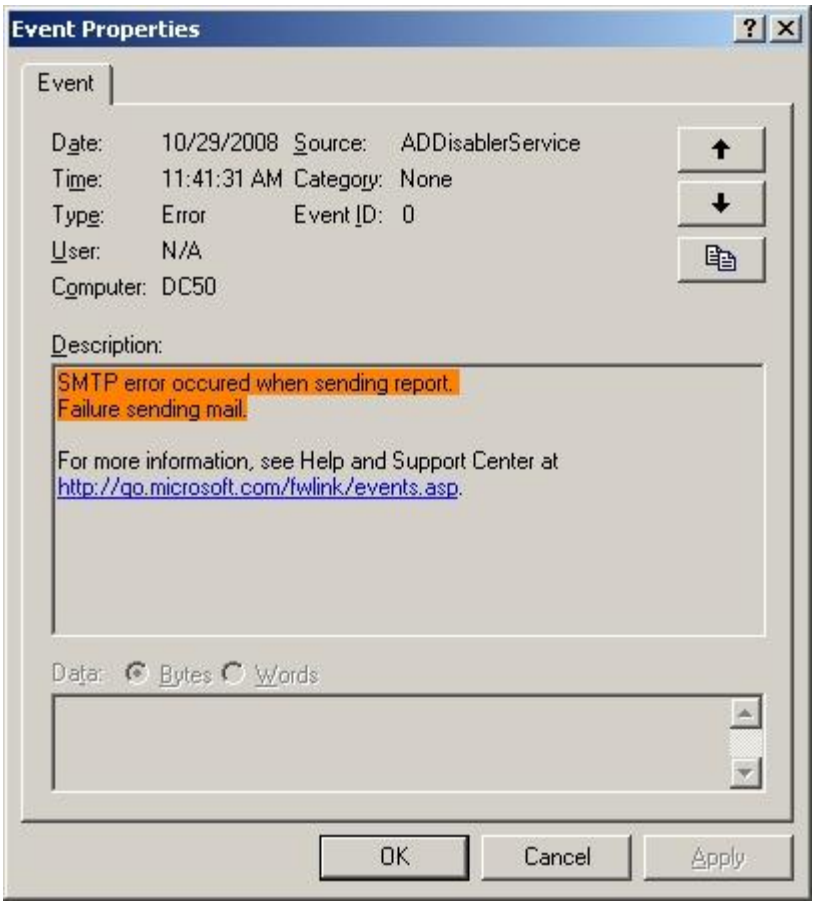
Date of Run: 10/23/2008 5:24:44 PM
Active User Accounts: 897
Settings:

Disable Old Accounts:	True
Ignore unreachable domain controllers:	False
Old Account Age (in days):	90
Reporting / Service Interval (in hours):	24
Report To Address	joeadmin@nfrontsecurity.com
Report From Address	info@nfrontsecurity.com
SMTP Server:	10.10.11.22

Users with a dormant account:

Username	Last Logon Time	Server Name	Disabled
test981	1/28/2008 4:00:00 PM	dc50.lab5.nfrontlabs.local	Yes
test982	4/17/2008 1:57:23 PM	dc50.lab5.nfrontlabs.local	Yes
test983	Never logged on	dc50.lab5.nfrontlabs.local	Yes
test984	Never logged on	dc50.lab5.nfrontlabs.local	Yes
test985	Never logged on	dc50.lab5.nfrontlabs.local	Yes
test986	Never logged on	dc50.lab5.nfrontlabs.local	Yes
test987	Never logged on	dc50.lab5.nfrontlabs.local	Yes
test988	Never logged on	dc50.lab5.nfrontlabs.local	Yes
test989	Never logged on	dc50.lab5.nfrontlabs.local	Yes
test990	Never logged on	dc50.lab5.nfrontlabs.local	Yes

Event when the mail server IP is not correct.



Local Reporting

nFront AD Disabler always generates 3 files in the c:\windows\system32\logfiles\AD Disabler directory:

1. nFront-AD-Disabler-Report.html (a local copy of the report that is emailed)
2. nfront-ad-disabler-disabled-accounts.html (a running log of all accounts disabled by NADD)
3. nfront-ad-disabler-disabled-accounts.csv (a running log of all accounts disabled by NADD in a convenient CSV format)

Here is an example of the CSV file contents:

```
"test901","AccountDisabled, NormalAccount","7/1/2008 2:33:11 AM","dc50.lab5.nfrontlabs.local","12/31/1600 7:00:00 PM"
"test902","AccountDisabled, NormalAccount","7/1/2008 2:33:11 AM","dc50.lab5.nfrontlabs.local","12/31/1600 7:00:00 PM"
"test903","AccountDisabled, NormalAccount","7/1/2008 2:33:11 AM","dc50.lab5.nfrontlabs.local","12/31/1600 7:00:00 PM"
"test904","AccountDisabled, NormalAccount","7/1/2008 2:33:11 AM","dc50.lab5.nfrontlabs.local","12/31/1600 7:00:00 PM"
"test905","AccountDisabled, NormalAccount","7/1/2008 2:33:11 AM","dc50.lab5.nfrontlabs.local","12/31/1600 7:00:00 PM"
```

The CSV file is generated to help you in a case of a mistake. Suppose you forgot to tell NADD to skip a group that contains 5000 users and now you must “re-enable” those accounts.

You can enable an account directly with the following command line syntax:

```
net user <username> /active:yes
```

To fully automate enabling accounts from the CSV file you can run the following VB script. Just copy the following text into a file with a VBS extension. If you do not wish to “re-enable” all accounts from the CSV file copy the CSV and VBS files to a new directory and edit the CSV file to remove the accounts you do not wish to “re-enable.”

```
'VBScript file to read CSV file and enable all accounts found there
dim fso,objCSVFile
const readOnly = 1, unicode = -1
set fso=CreateObject("Scripting.FileSystemObject")
set objCSVFile = fso.openTextFile("nfront-ad-disabler-disabled-
accounts.csv",readOnly,False,unicode)

Do while NOT objCSVFile.AtEndOfStream
  strLine = objCSVFile.Readline
  firstDelimiter = instr(strLine,",")
  if firstDelimiter<>0 then
    userStr=mid(strLine,2,firstDelimiter-3)
    execStr="net user " & userStr & " /active:yes"
    set objShell = CreateObject("WScript.Shell")
    set objScriptExec = objShell.Exec(execStr)
    wscript.echo userStr & " is enabled"
  end if
Loop

objCSVFile.Close
set objCSVFile = Nothing
set fso = Nothing
```

Uninstallation

nFront AD Disabler may be removed via the Add/Remove Programs applet in the Control Panel. Removing the application will remove the service and all corresponding files.

Troubleshooting

Here are some common troubleshooting steps you should consider:

- Check the Event Viewer application log on the server running the nFront AD Disabler service.
- Is the nFront AD Disabler service running?
- Look at the local report file generated in the c:\windows\system32\logfiles\AD Disabler directory.

You can have the nFront AD Disabler service generate a verbose debug file. To do so, set HKLM\Software\nFront Security\AD Disabler\debug=1. Then stop and restart the nFront AD Disabler service. The service will now build nfront-ad-disabler-debugger.txt file in the windows\system32\logfiles directory.