Getting Started

Viewfinity Local Admin Discovery

March 2011

2011

Table of Contents

1. LEGAL STUFF 2
2. INTRODUCTION 2
3. BEFORE YOU BEGIN 2
4. INSTALLATION 3
5. DISCOVERY OF LOCAL ADMINISTRATORS 4
6. GODSPEED! 12

1. LEGAL STUFF

This document contains information about installing and using Viewfinity Local Admin Discovery.

For the latest information about installing and using Viewfinity Local Admin Discovery, see "Release Documentation for Windows Home Server" at the Viewfinity Web site (http://www.viewfinity.com/support/).

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Viewfinity.

Viewfinity may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Viewfinity, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2011 Viewfinity Inc. All rights reserved.

All trademarks are property of their respective owners.

2. INTRODUCTION

The Viewfinity Local Admin Discovery is a free tool that allows you to discover user accounts and groups that are members of the local "Administrators" built-in user group on computers in your Windows domain. Being a local Administrator provides a lot of possibilities for damaging the computer either intentionally or accidentally thus causing an unnecessary headache for both end users and Help desk. Sometimes the damage (e.g. by unintentional installing of some virus) may even jeopardize other computers in your network as well. One can imagine numerous additional scenarios, including information security risks, licensing issues, and so on.

Viewfinity Local Admin Discovery makes it easy to pinpoint such potential flaws and remotely fix them on individual computers to prevent possible complications.

3. BEFORE YOU BEGIN

Prior to installing of the Viewfinity Local Admin Discovery please ensure that:

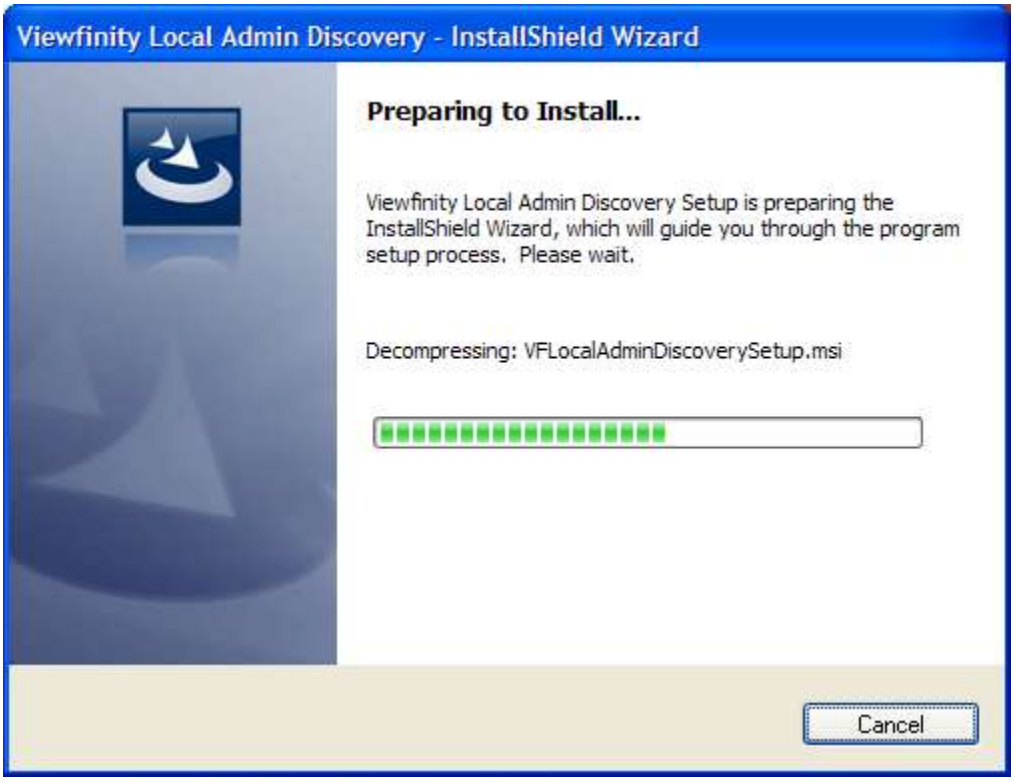
- You are going to install it on a PC that is a member of the Active Directory to be analyzed.
- Microsoft .NET Framework 3.5 Service Pack 1 is installed on the PC.

- Microsoft Report Viewer 2010 is installed on the PC.

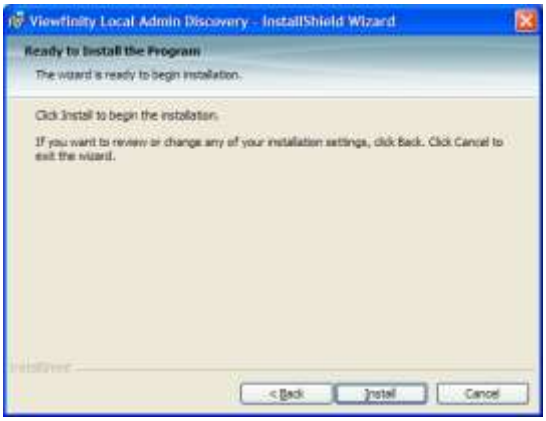
Please note that in case some prerequisites (Microsoft .NET Framework 3.5 Service Pack 1 and/or Microsoft Report Viewer 2010) are not installed on the PC you'll be prompted to download and install them in the course of the Viewfinity Local Admin Discovery installation.

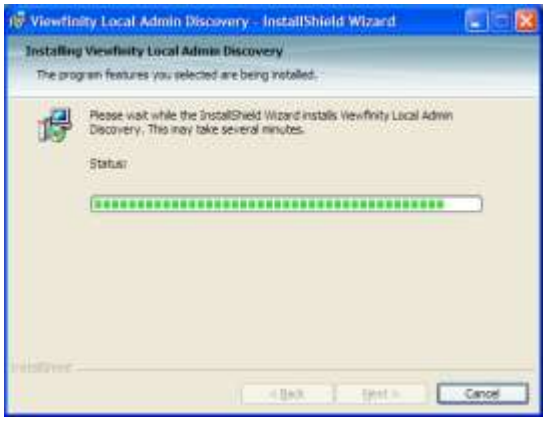
4. INSTALLATION

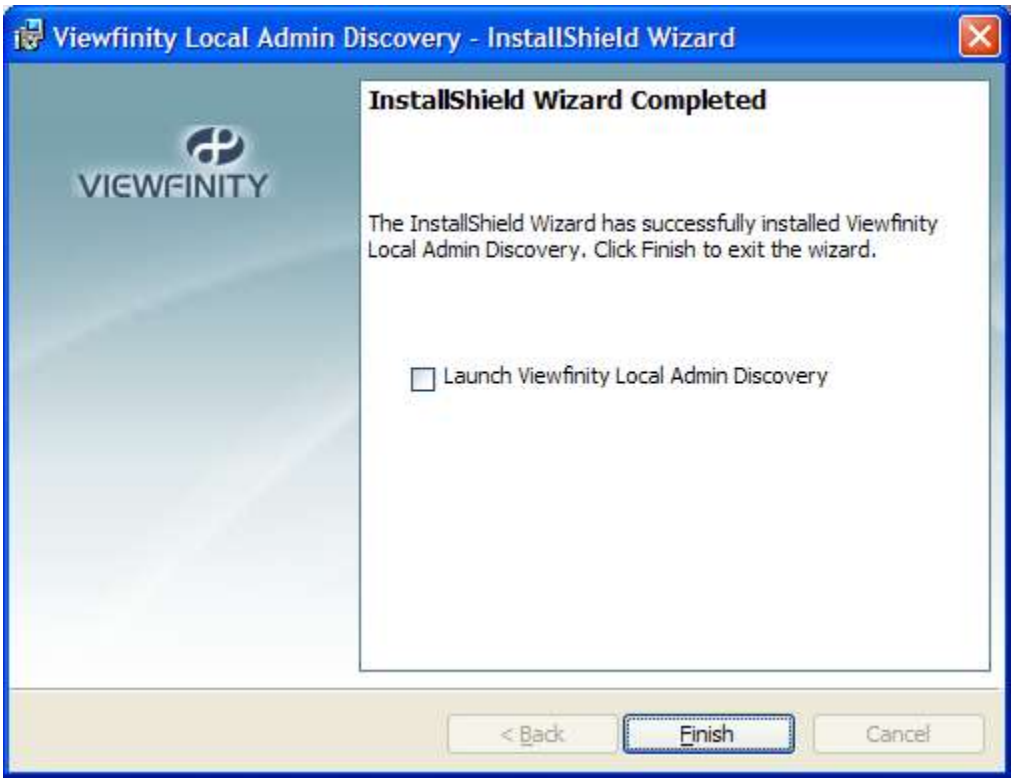
You can download the Viewfinity Local Admin Discovery installation package VFLocalAdminDiscoverySetup.exe from Viewfinity Web site at http://www.viewfinity.com. Alternatively you may obtain it on a CD or other media. Launching VFLocalAdminDiscoverySetup.exe initiates the installation of the Viewfinity Local Admin Discovery:



The installation of the Viewfinity Local Admin Discovery is simple and straightforward and should rarely require anything besides clicking on the "Next" button:



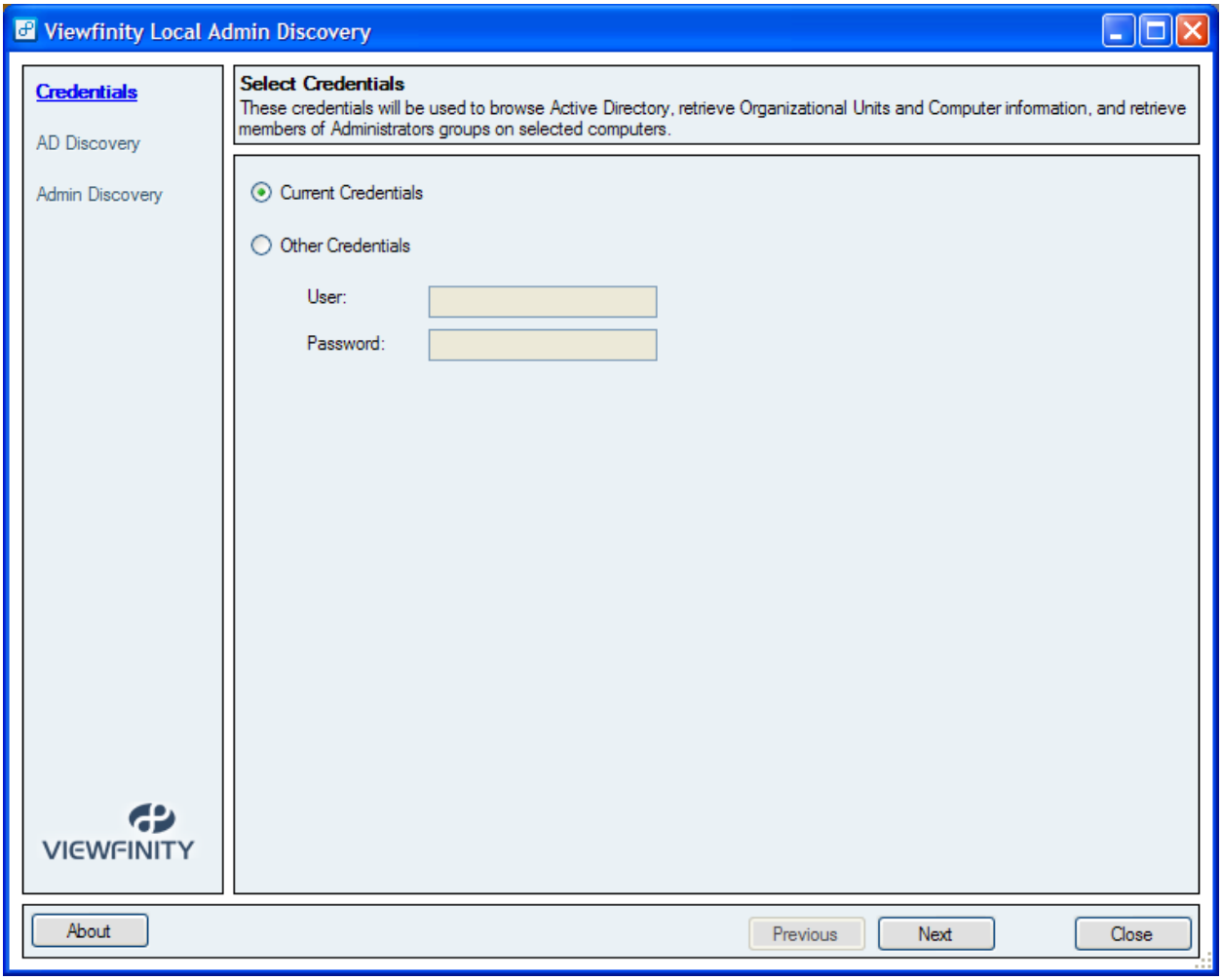




Congratulations! You have installed the Viewfinity Local Admin Discovery.

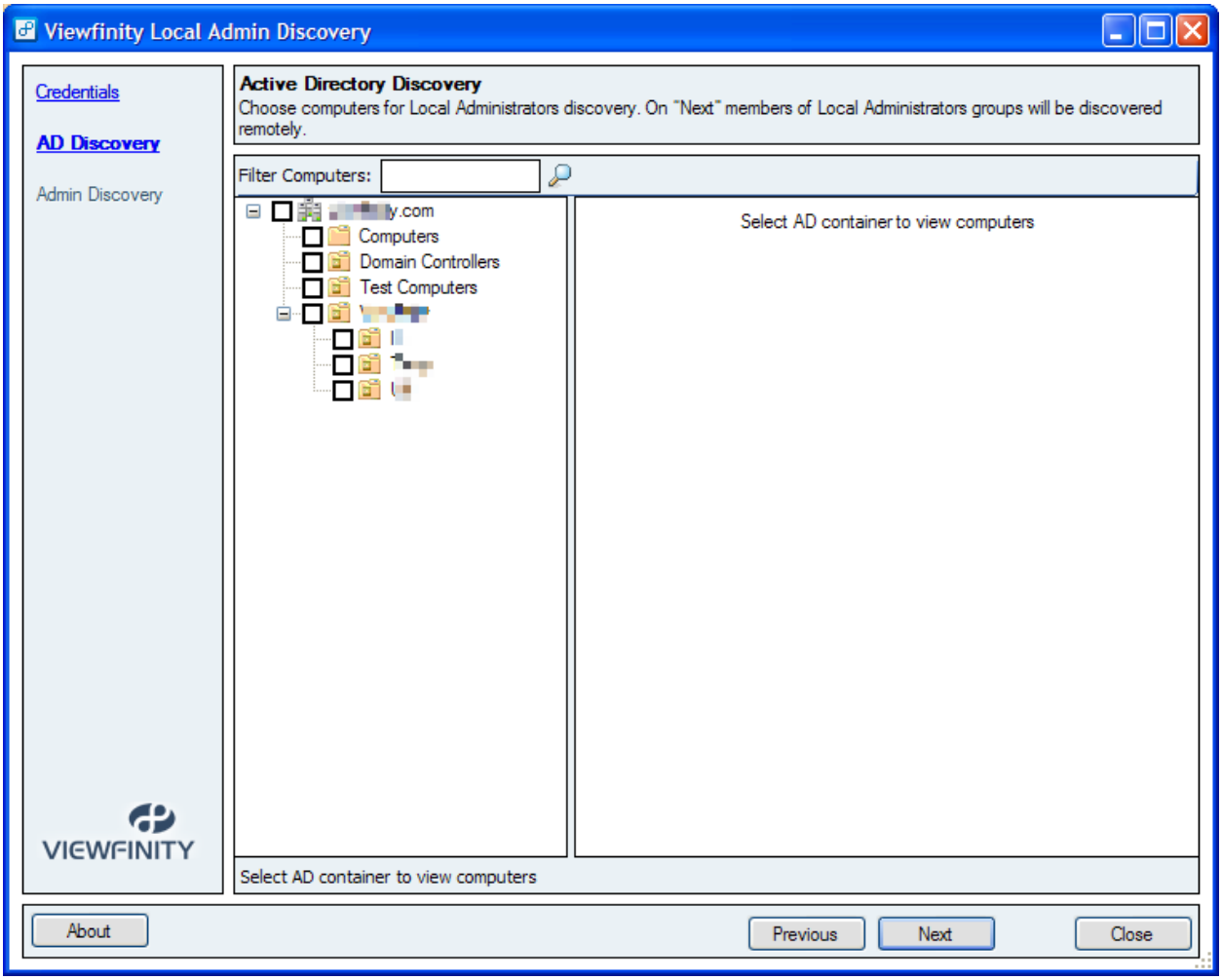
5. DISCOVERY OF LOCAL ADMINISTRATORS

Upon launching Viewfinity Local Admin Discovery, you are prompted to select credentials to be used for accessing Active Directory and selected computers:

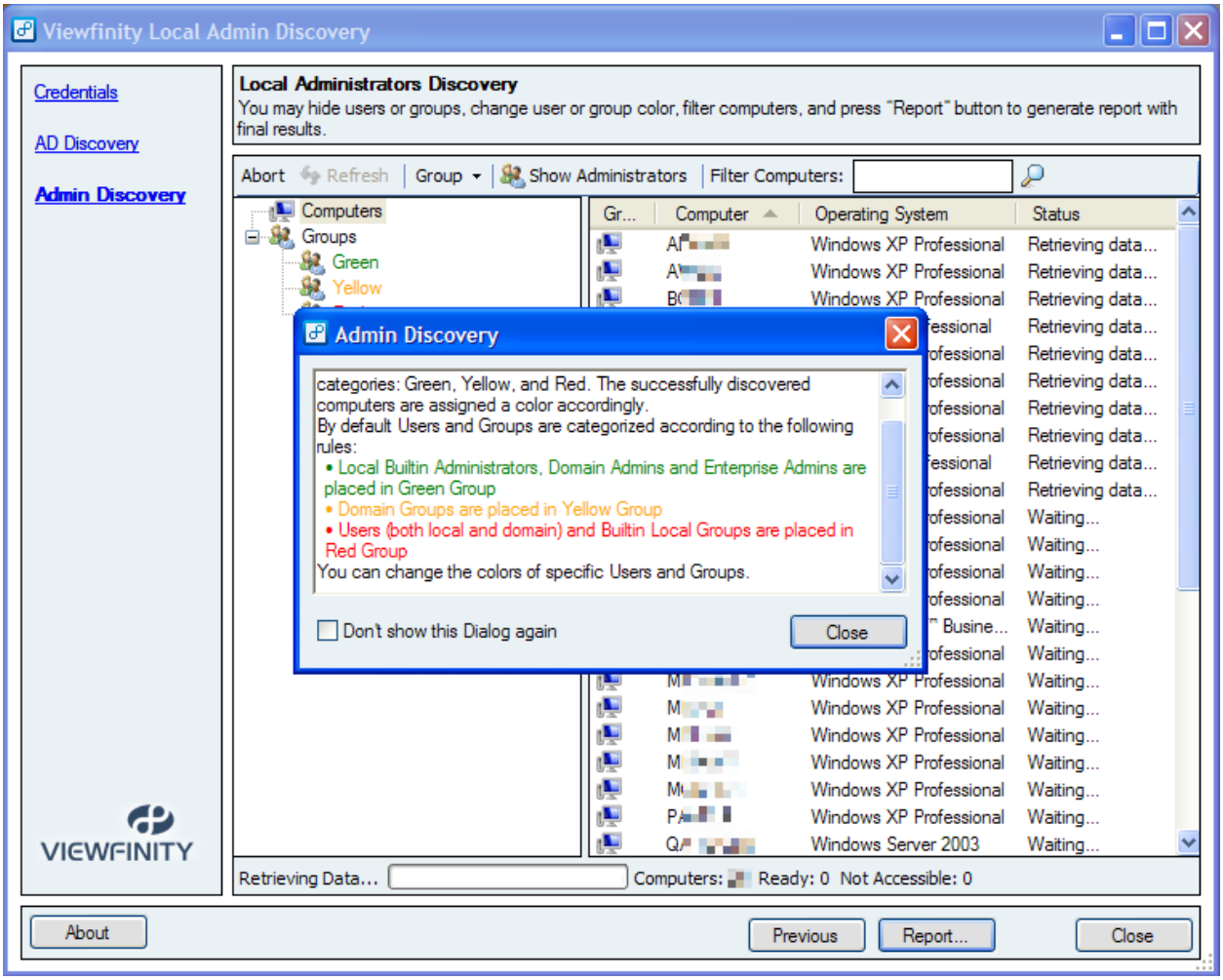


Please note that credentials of the current user may be insufficient to perform some operations (like deleting a user from local “Administrators” user group on a remote computer). In such cases you can provide credentials of another domain user with sufficient permissions.

Upon click on the “Next” button the Viewfinity Local Admin Discovery will discover the structure of your Active Directory:



When you select a specific Active Directory Container in the tree you will see computers belonging to it. Now you can select specific computers to be analyzed for members of their local "Administrators" user group, or click checkboxes in the Domain tree to select entire Domain or another Active Directory Container (please keep in mind that selecting a large number of computers may result in a long computer discovery time). Click on "Next" starts the analysis:



Each of the selected computers is connected to in order to retrieve information about members of the local "Administrators" user group. The overall progress and status of each specific computer analysis is easily observable.

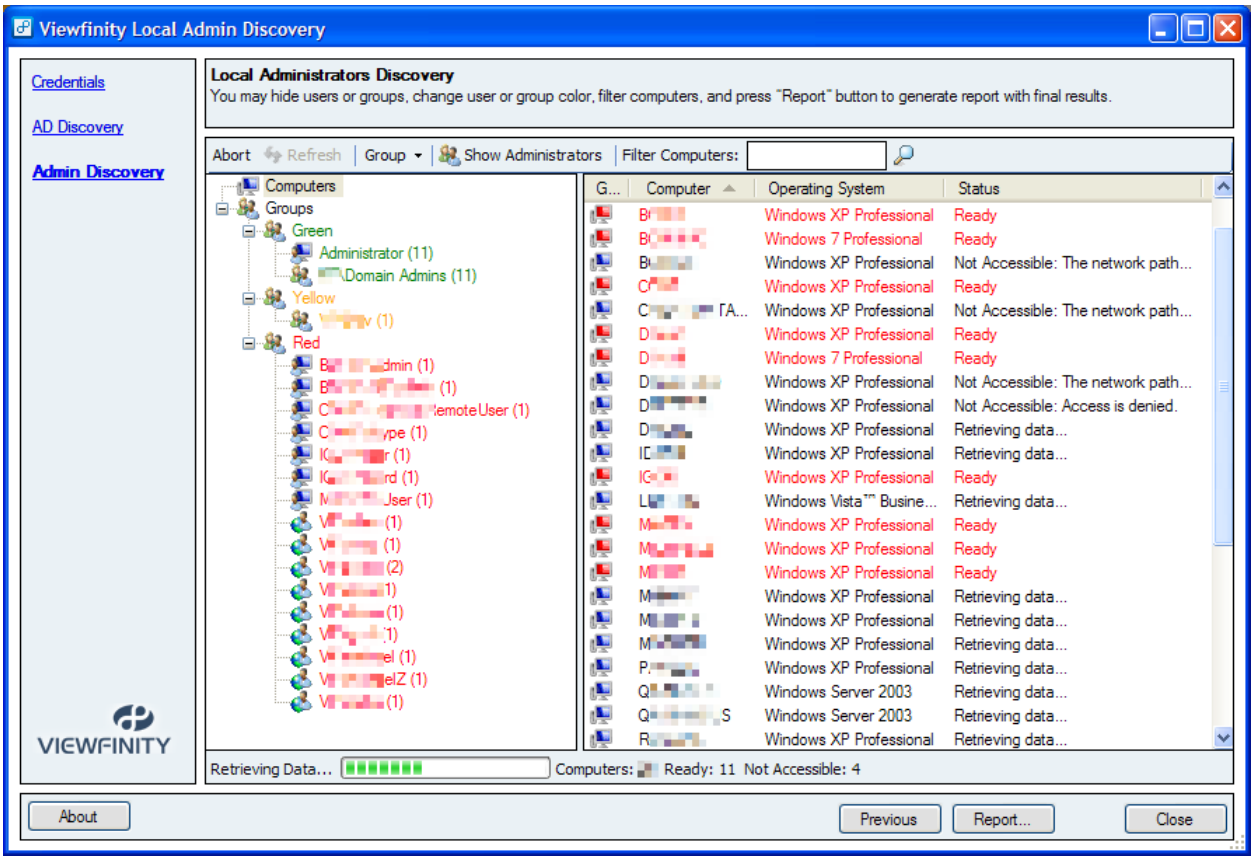
Each discovered user or user group is assigned a color according to the following color scheme of vulnerability:

green	Well-known security identifiers of default members of "Administrators" group (see more information at http://support.microsoft.com/kb/243330): built-in "Administrator" local user, and "Domain Admins" and "Enterprise Admins" Domain user groups.
yellow	Other Domain user groups (not "Domain Admins" and "Enterprise Admins").
red	Other (not local "Administrator") users (both local and domain) and any local user groups.

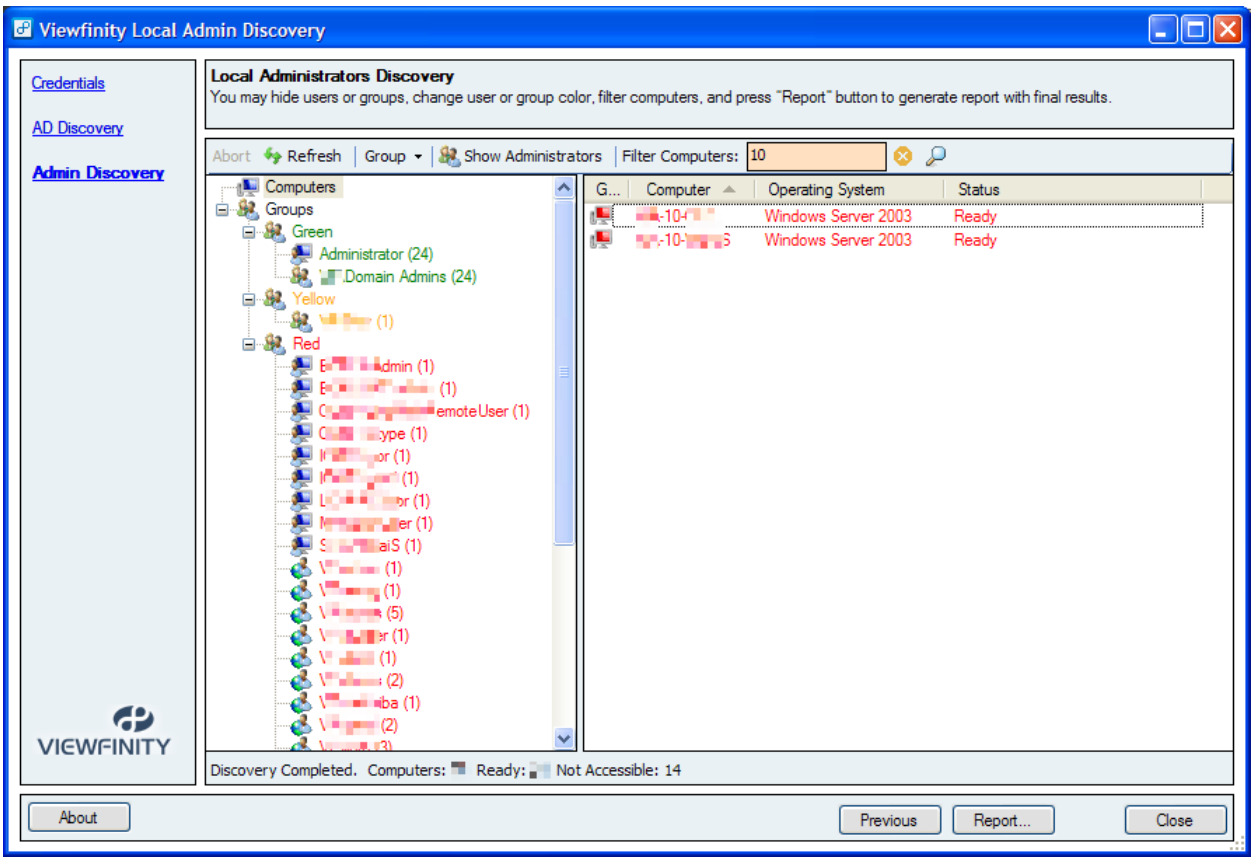
Computers are assigned a color based on the colors of the members of the local "Administrators" user group:

black	Computers which are not analyzed yet or where the analysis failed (specific error is listed in the Status field).
green	Local "Administrators" user group contains only "green" user groups and users.
yellow	Local "Administrators" user group contains only "green" and/or "yellow" user groups and users (no "red" entries).
red	Local "Administrators" user group contains at least one "red" user group or user.

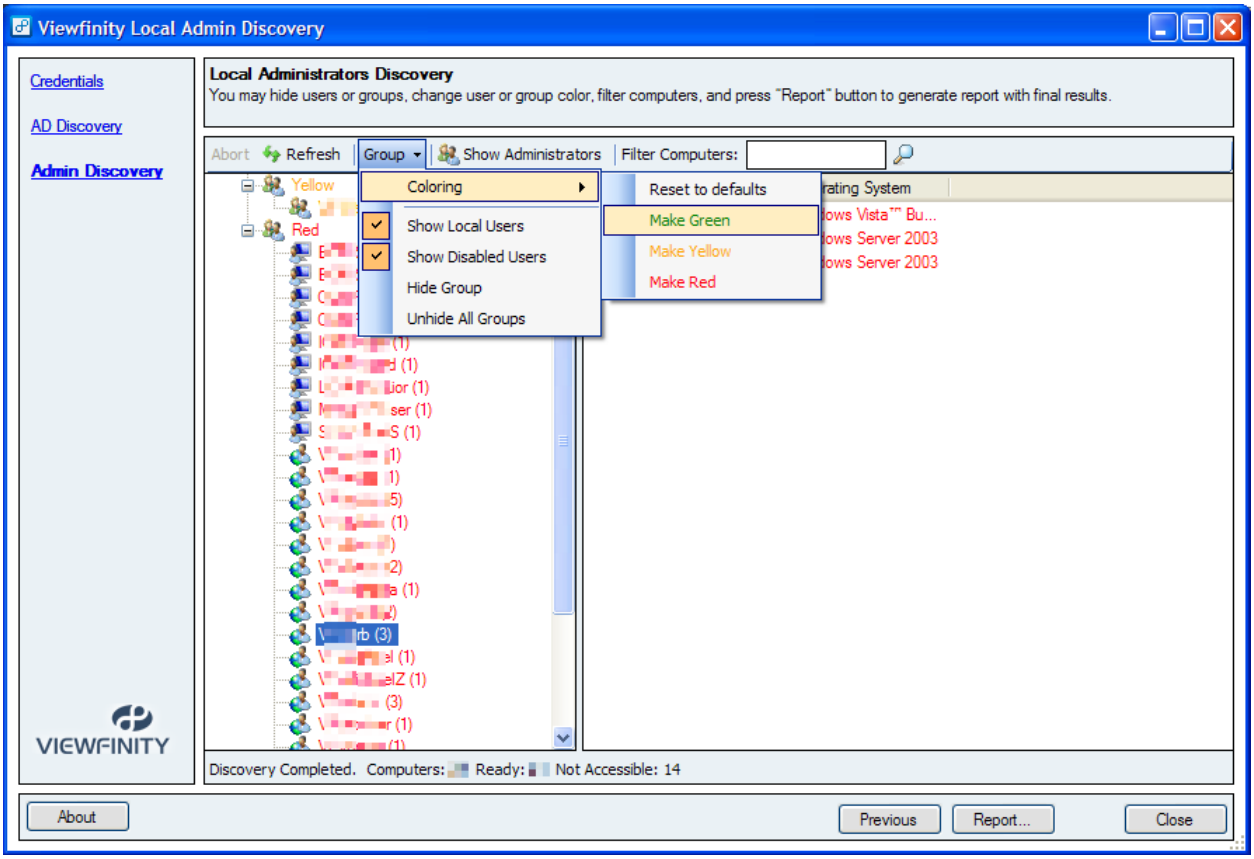
When the analysis is complete, the left pane represents all found local Administrators grouped according to vulnerability level, and the corresponding computers are shown in the right pane:



Selecting specific Group or User in the tree will display computers with this user group or user as a local Administrator. Convenient filtering by any part of computer name allows easy browsing in long lists:

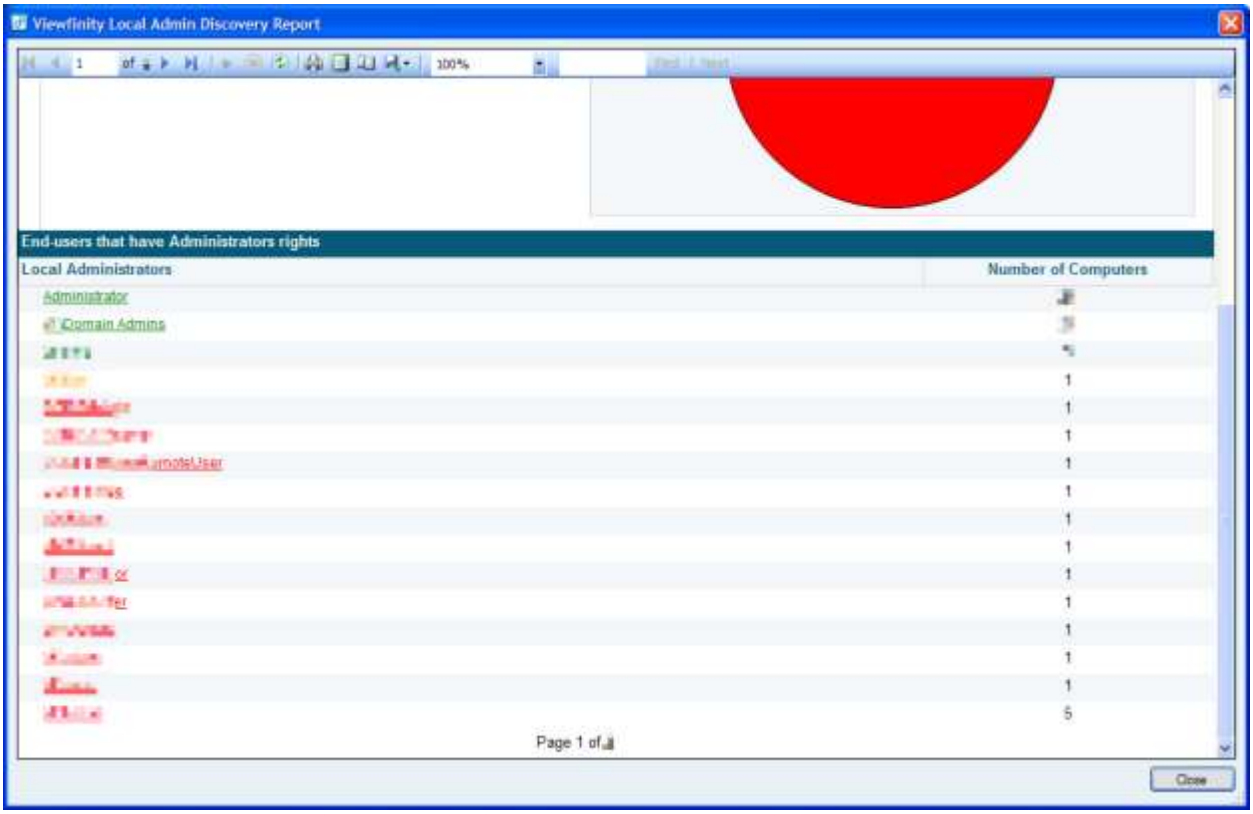


In case you know exactly that the vulnerability level of some user/group is assumed incorrectly (e.g. you have a special Domain user group "IT Staff" that should be a member of local "Administrators" according to your organization policy), you can change the coloring:

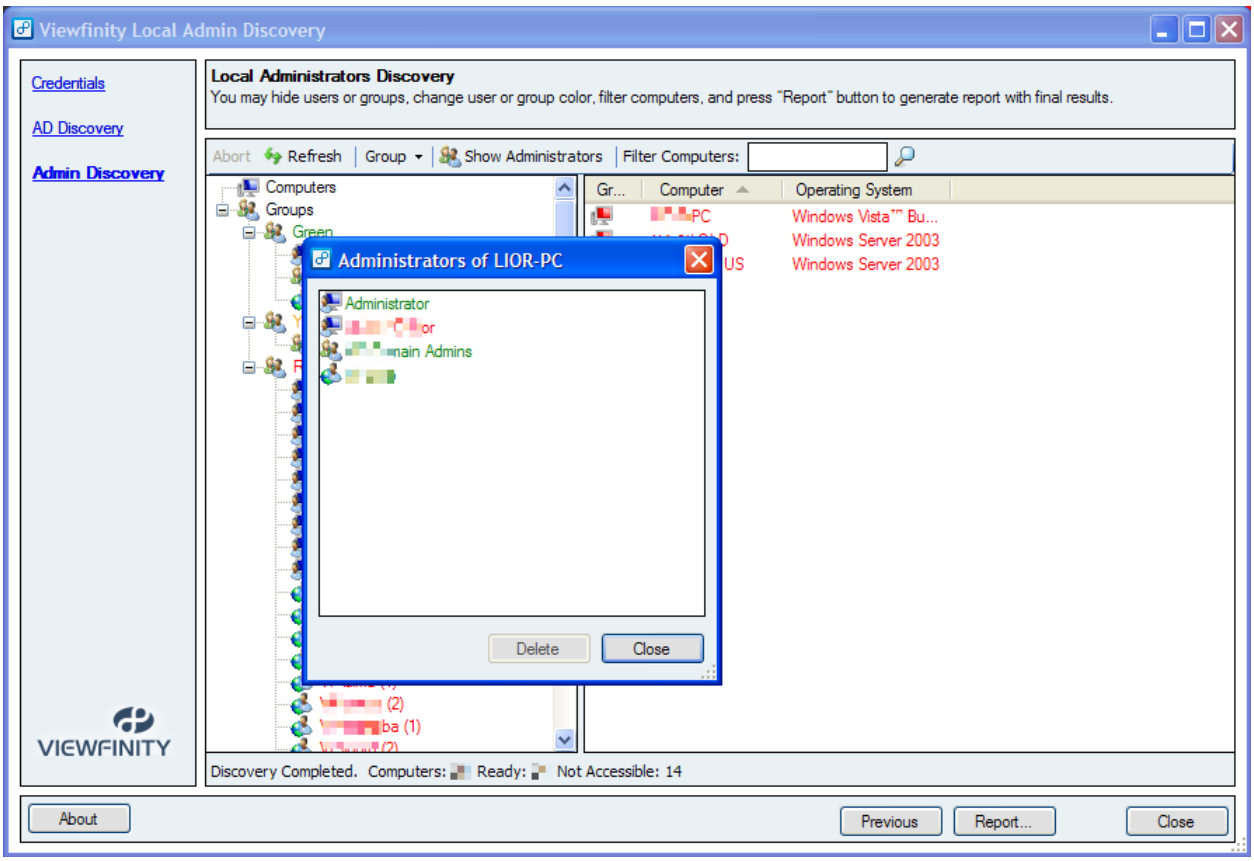


You can also choose if Local Computer Users and Disabled Users should be included in the display.

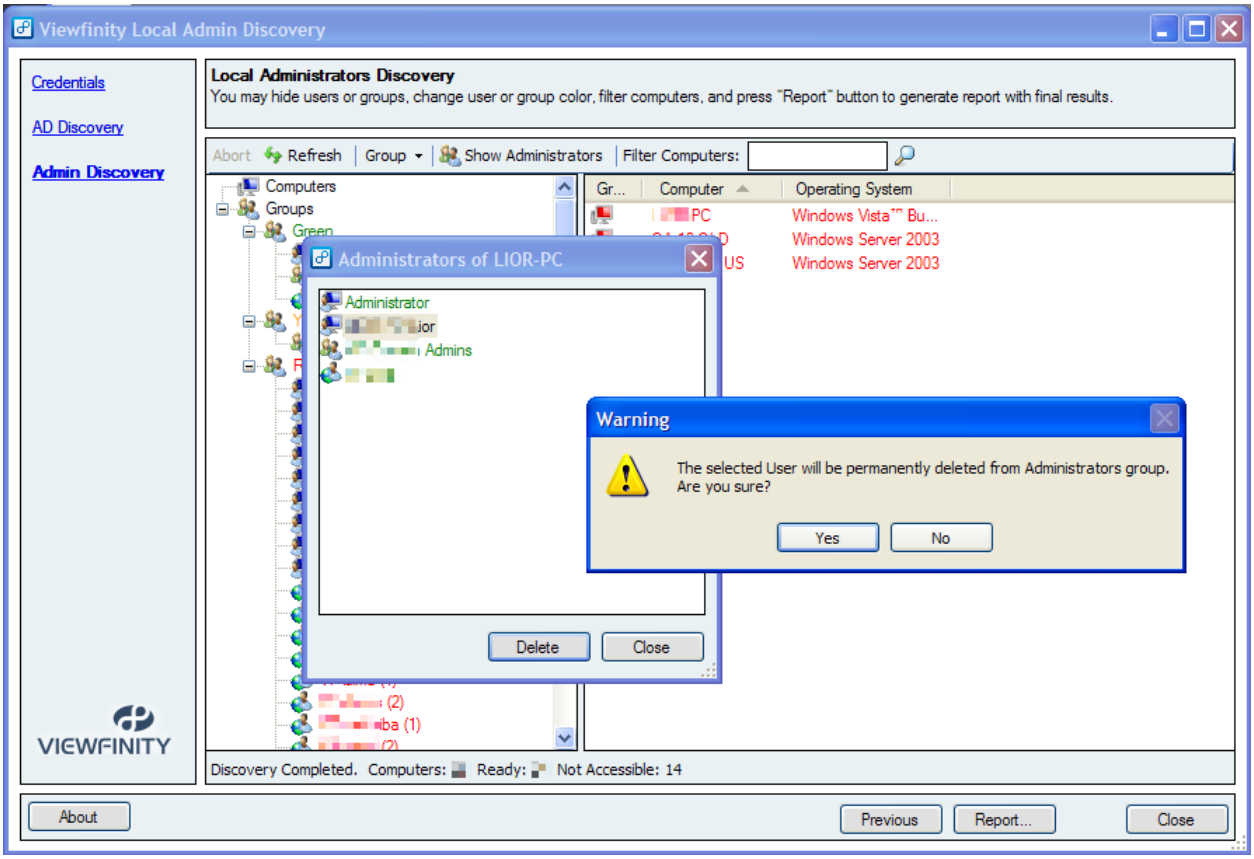
Click on "Report…" provides you with a printable representation of the discovery results according to the selected filters:



Finally, by selecting a specific computer and clicking “Show Administrators” the full list of local Administrators is displayed:



Now you can remove a user or user group from the local “Administrators” of the specific computer remotely – with just one click on “Delete” button (please note that changes to a group membership will not take effect until the next time the user logs on):



Attention: removing yourself (either directly or by removing a user group you belong to) will result in your inability to manage this computer in the future!

6. GODSPEED!

With the Viewfinity Local Admin Discovery is becomes easy to cure PCs where end users have local Administrator rights by some obsolete operational reasons.

Nevertheless in many enterprises, it is an organization policy to add end users to the local “Administrators” group on their assigned PC. The most likely reason for that is use of legacy applications, which require administrative privileges in order to work properly.

For such enterprises Viewfinity provides a comprehensive solution - Viewfinity Privilege Management.

Viewfinity Privilege Management offers IT Administrators a flexible approach for controlling its corporate desktop and laptop environment. With tighter, yet flexible control over the types of applications and privileges your distributed workforce are allowed, the more stable your desktop environment becomes. With this enhanced control over managing your environment, the number of end user support calls to the Help desk is reduced.

For more information about Viewfinity Privilege Management please visit http://www.viewfinity.com.