VIRTUAL DESKTOP MONITOR

USER MANUAL

ZAGREB, 4/26/11

acceleratio

Gradiscanskih Hrvata 24
21000 Split, Croatia
+385 21 272 413

sales@acceleratiosoftware.com
www.acceleratiosoftware.com

CONTENTS

ABOUT VIRTUAL DESKTOP MONITOR

Virtual Desktop Monitor is a VDI monitoring application that allows you to easily monitor user activities on virtual desktops on your **Microsoft Windows VDI Technology, Citrix XenDesktop, Quest vWorkspace** or **VMware View**.

Software will provide you with reports such as:

- Users Activity Monitoring
- Applications Monitoring
- Subscribe to reports via email
- License compliance monitoring
- Concurrent usage reports
- Custom reports & real-time alerts

The software supports:

- a static or persistent virtual desktop
- a dynamic or non-persistent one
- future offline VDI scenarios

The software runs in client – server scenario to minimize the impact on your environment and support all the VDI environments that we know today. The client collects data in the local database on the VDI client and then syncs with central SQL server. This way not all clients' need to be on the network as they will sync eventually when they connect to the enterprise managed network.

VIRTUAL DESKTOP MONITOR REPORTS

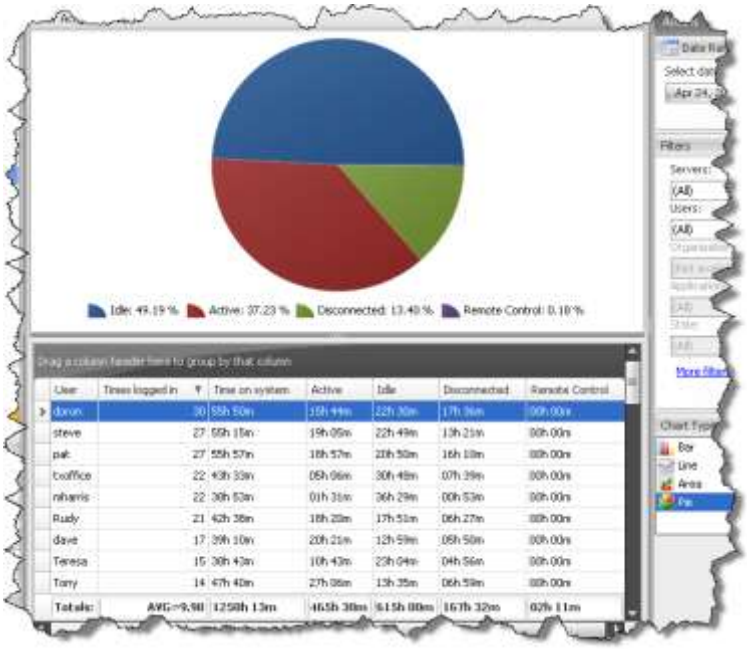
USER REPORTS

The set of Virtual Desktop Monitor User Reports provides administrators with valuable information about activities of remote users. Information displayed in these reports is based on the time users spend connected to Virtual Desktops. Data provided can be used for time tracking for billing purposes or employee auditing. You can generate reports for your Virtual Desktop usage, monitor employee log on/log off times, monitor active/idle sessions, do time tracking for each user on the server or farm and determine total active hours for subcontractors.

USER ACTIVITY BY STATE

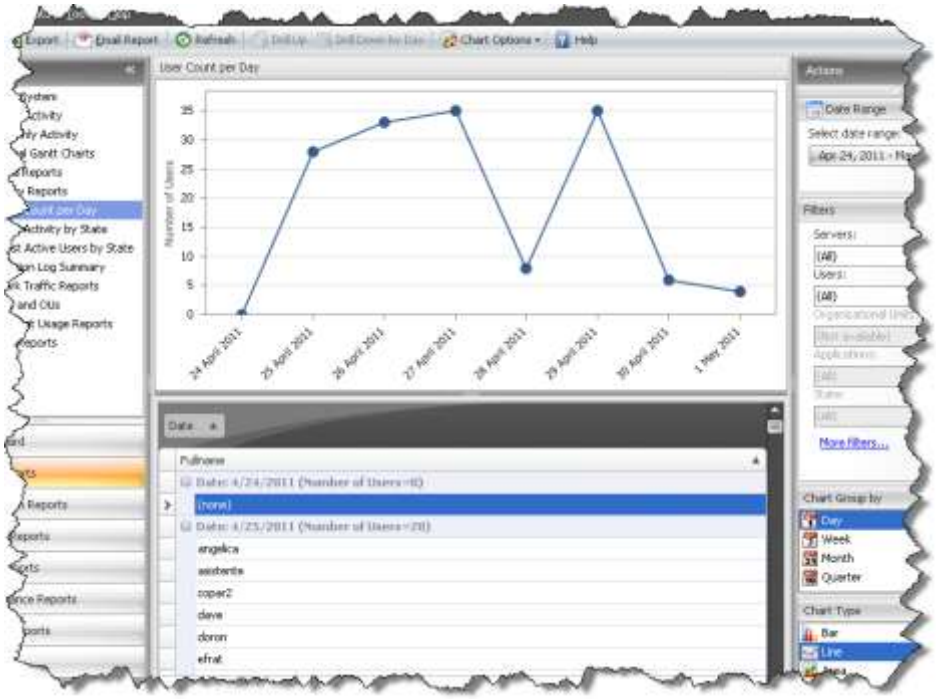
The User Activity by State Report summarizes activities for all users, displaying information about how long users were active (total time), idle, or disconnected. Use this report to determine the ratio of active / idle / disconnected activities. The report is presented as a simple pie chart and data table.

If you are paying your employees or subcontractors by the hour, you can use this report to see the total time a user was connected to your server in Active or Idle time.



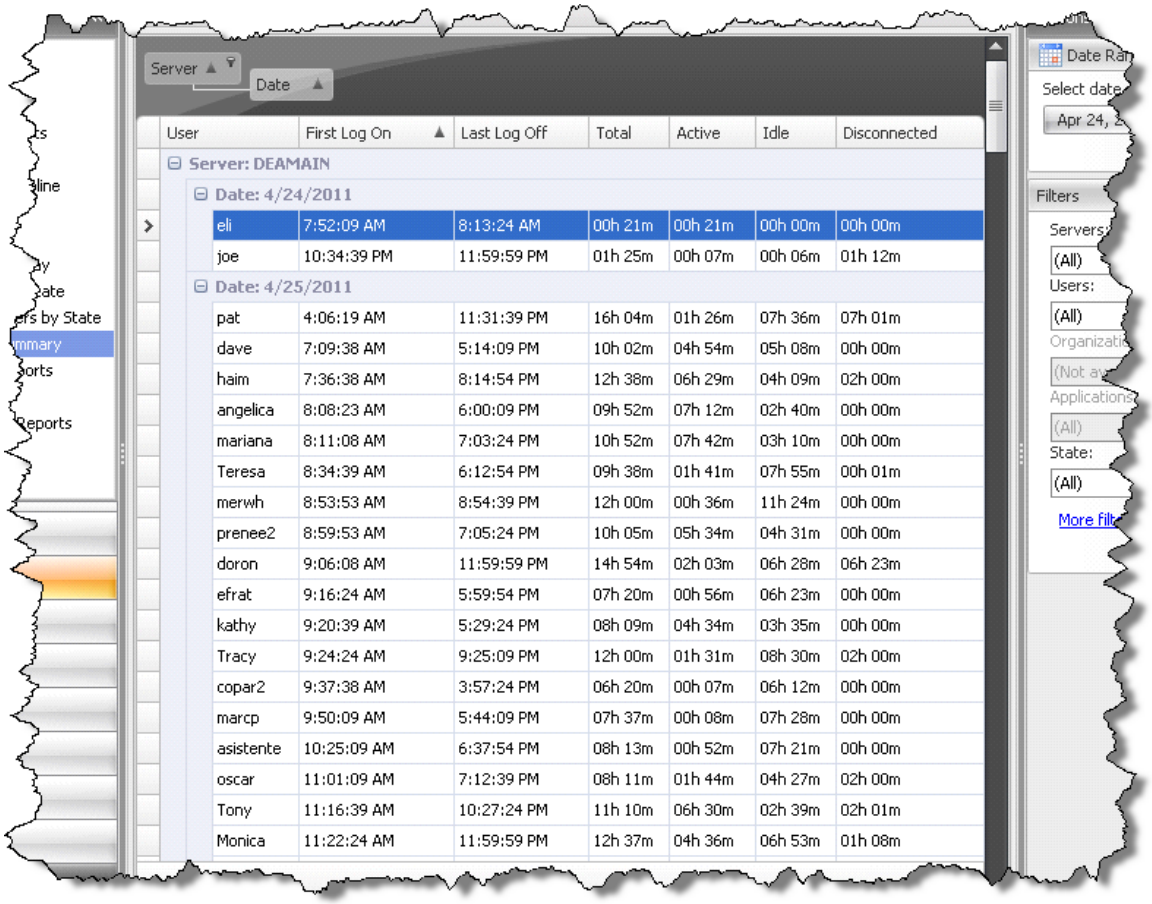
USERS COUNT PER DAY

Shows the number of unique users connected to a server in a selected time span. Use it to monitor the overall usage and utilization of your Terminal Services farm or a particular server or TS User CALs. Filters allow you to customize the report to analyze user behavior or server usage.



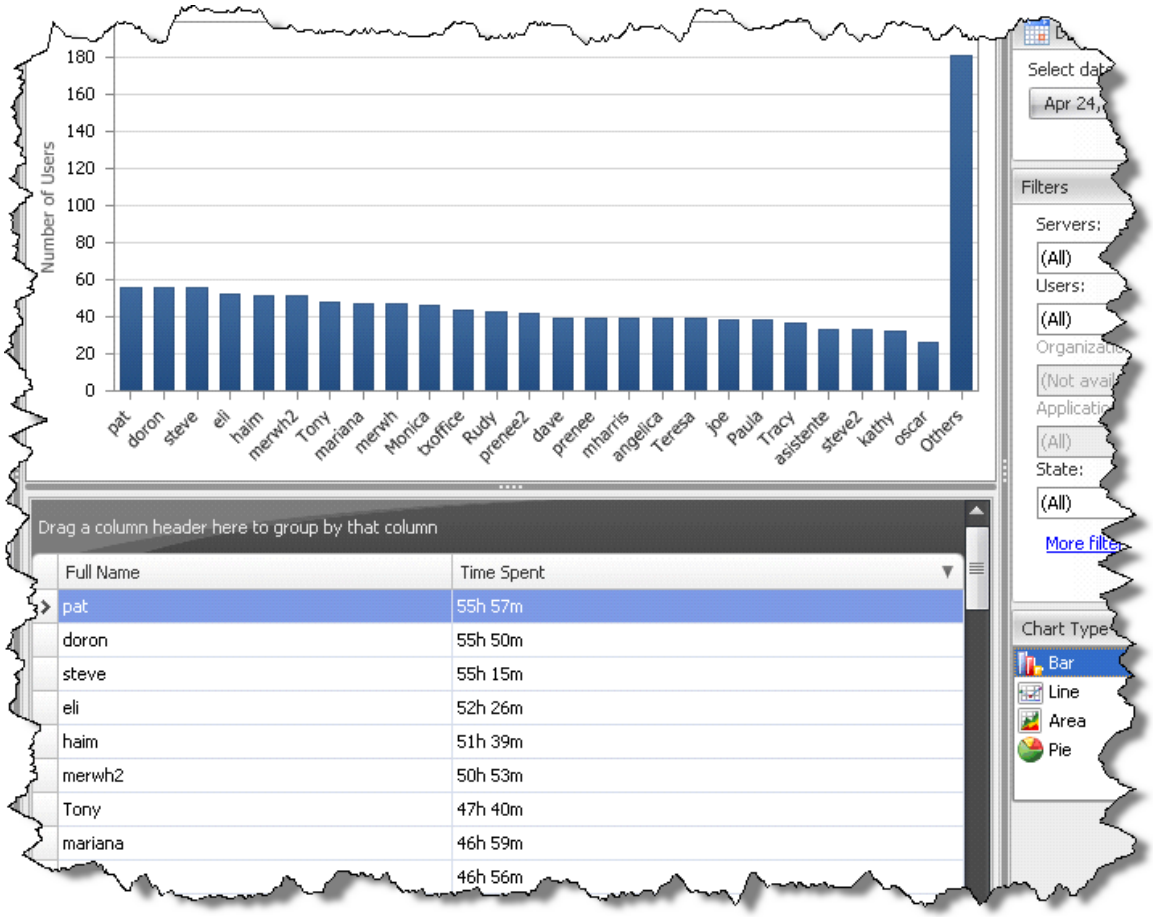
SESSION LOG ON/OFF FOR ALL THE USERS

This report gives you a list of all sessions and users that connected to your server in a selected time span. It provides you with the session name, start time, end time, and duration of each session. Duration is divided into active, idle, and disconnected time for each session. Use it to analyze user activities and session duration.



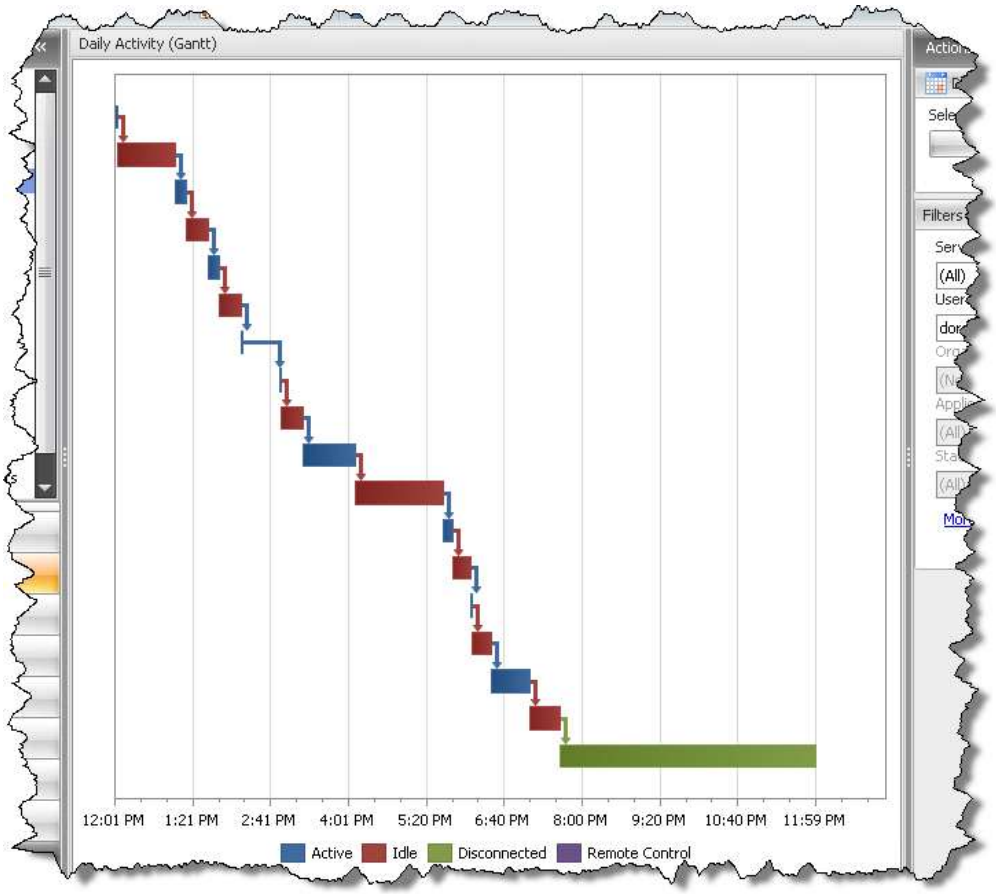
MOST ACTIVE USERS BY STATE

The Most Active Users by State Report displays the most active users by activity state (Active / Idle / Disconnected / Remote Control). The report provides you with a column chart, including a list of the most active users and a data table with all the details. Use the report to identify the most active user or a user who was idle during their entire remote desktop session.



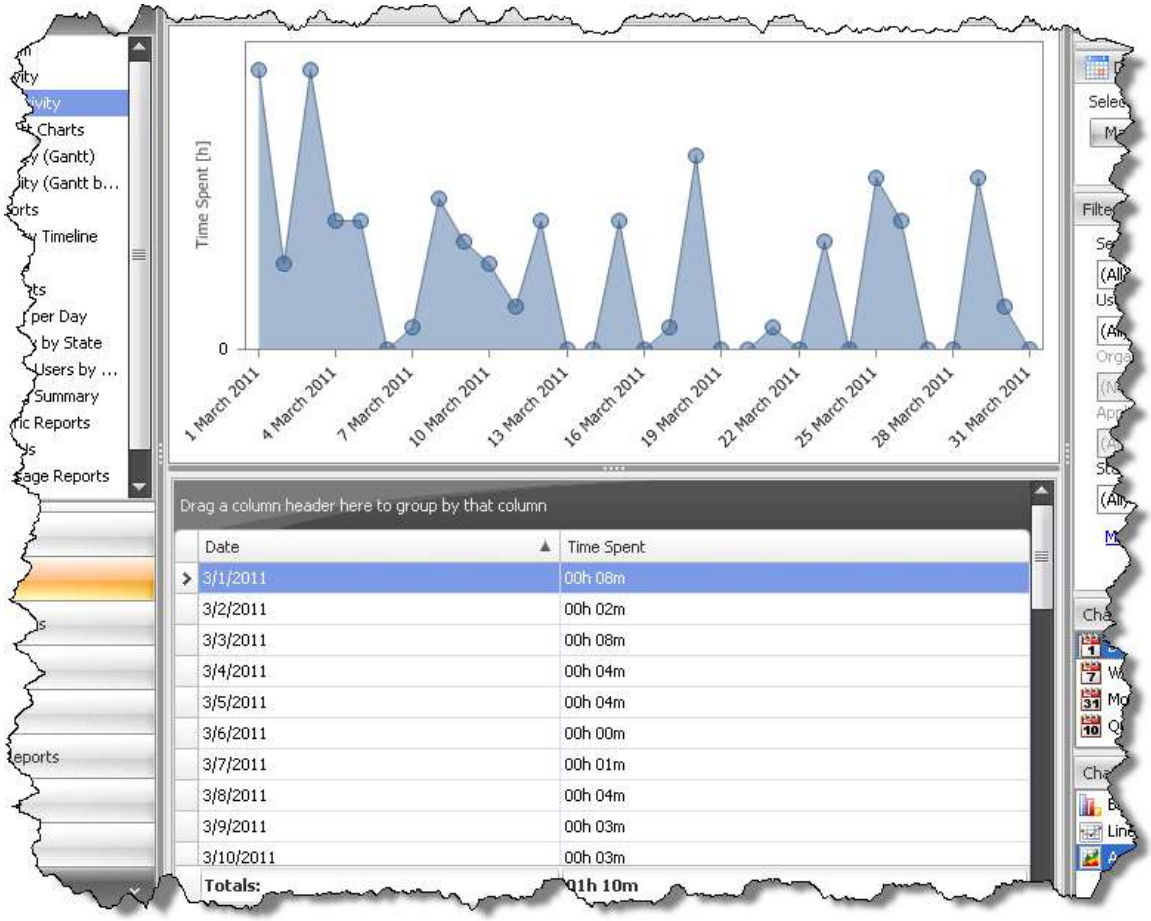
GANTT CHARTS

Two Gantt chart reports show user activities during one day as a Gantt chart. Both reports allow administrators to easily track what a user is doing during a workday. In farm environments, reports summarize activities across all servers and show a unique chart for each user, and it can be valuable to identify unexpectedly long periods of user's inactivity.



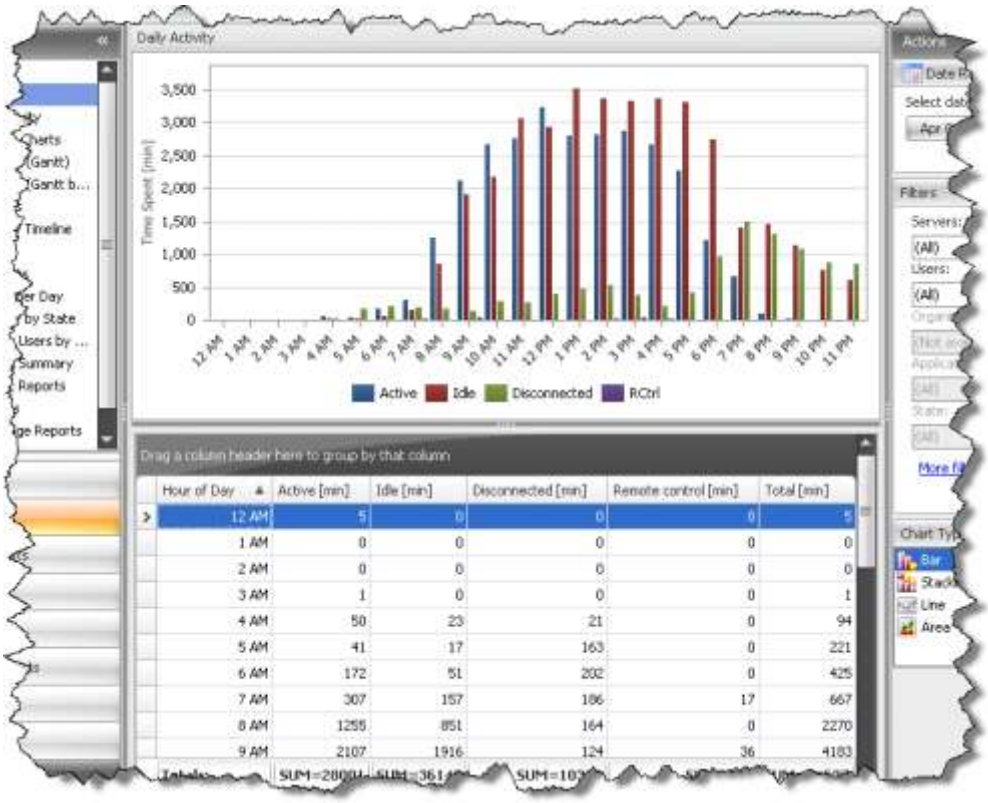
MONTHLY ACTIVITY

This report provides you with the summarized usage of your servers for one month. Use this report to check utilization for your servers day-by-day, and by applying various filters you can see activities for a particular user or server in the selected period.



DAILY ACTIVITY

In order to be able to optimize resource usage on your Terminal Services / Citrix server farm you need to identify a time frame when the server is heavily used. The Daily Activity Report provides you with valuable information about server usage during the day. All activities are broken down by the hour so you can easily configure your backups and other system activities to run while your server is idle.



APPLICATION REPORTS

Application reports provide administrators with important audit information about applications being used on a Terminal Server or Citrix server. These reports can be used to pinpoint the most heavily used applications for a given user. Administrators can use the provided data to generate various compliance reports (SOX, HIPAA, GLBA, PCI DSS, FISMA) or monitor Citrix published applications.

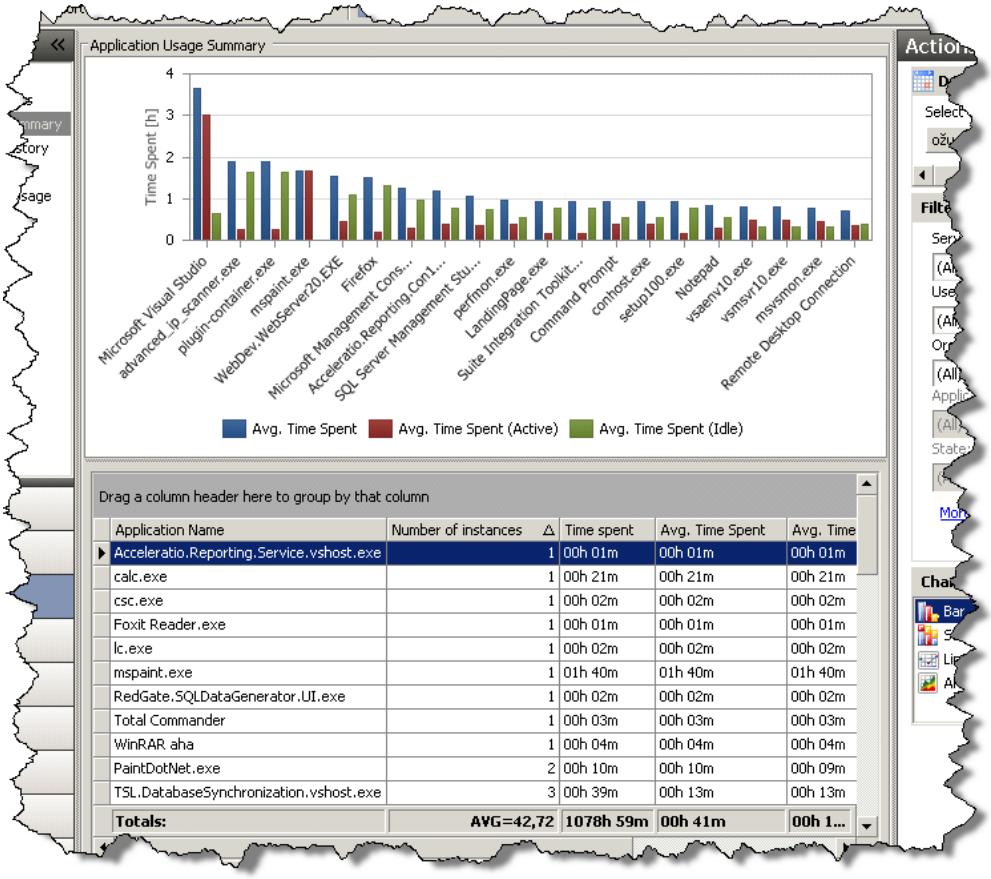
MOST USED APPLICATIONS BY USER

This report shows a list of frequently used applications on a server. It summarizes the time users have spent using each application. By using filters you can easily create custom reports to find the most used application by an individual user. You can also export or print information provided by this report.

USER - APPLICATION SUMMARY

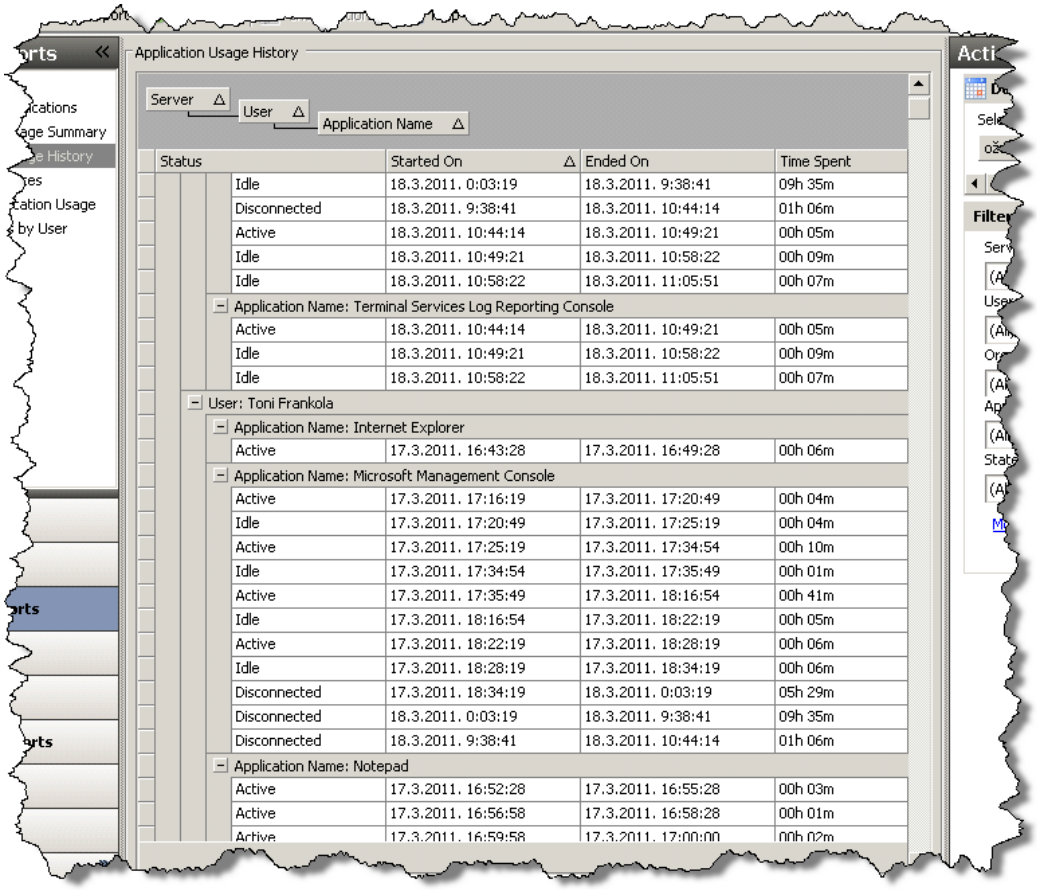
Summarizes data about applications opened on a Terminal Server. It allows you to monitor:

- Number of application instances
- Time spent (using each application)
- Average time spent (using each application)
- Average time an application was active
- Average time an application was idle



APPLICATION AUDIT

The Process Audit report provides you with valuable information about processes on your server, which allows you to comply with various compliance requirements such as SOX. It provides information about usage duration and the precise time when it was used for each user in the selected period.

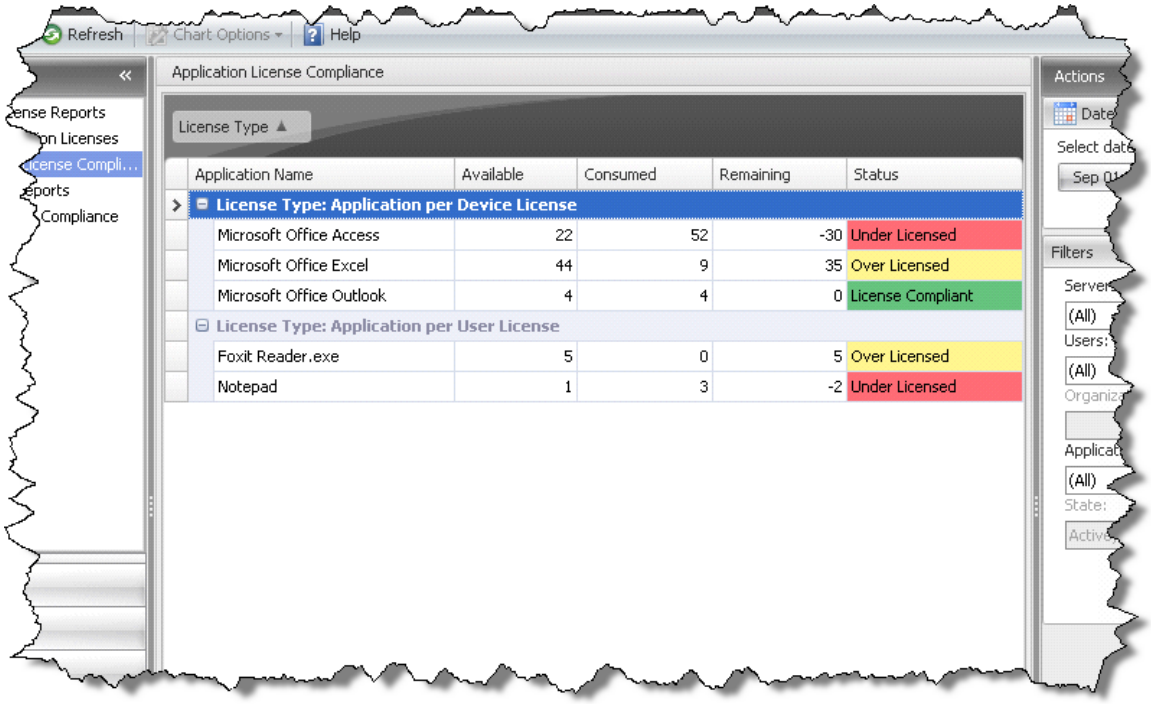


License Reports

With all the applications installed on a Remote Terminal Server or Citrix server it is hard to track all the available and used licenses. License Compliance Reports is a set of reports that helps you track all licenses being used on your server, or across all servers in your server farm. These reports help you track 5 different types of CALs (Client Access Licenses): Remote Desktop Services CALs (User and Device), Citrix Concurrent User licenses and per-user and per-device licenses for all the applications running on your server. Administrators can use these reports to check if you are license compliant and to plan further license needs and license contract renewals

APPLICATION LICENSE COMPLIANCE REPORTS

Terminal Services Log shows you the number of software licenses used on a server or in a server farm. You can use license reports to verify if you satisfy license compliance requirements or to check if you need to purchase additional licenses for published applications. This report can save you a lot of money by detecting if there are any unused software licenses. This report can also help you avoid possible penalties for using software without appropriate licenses.



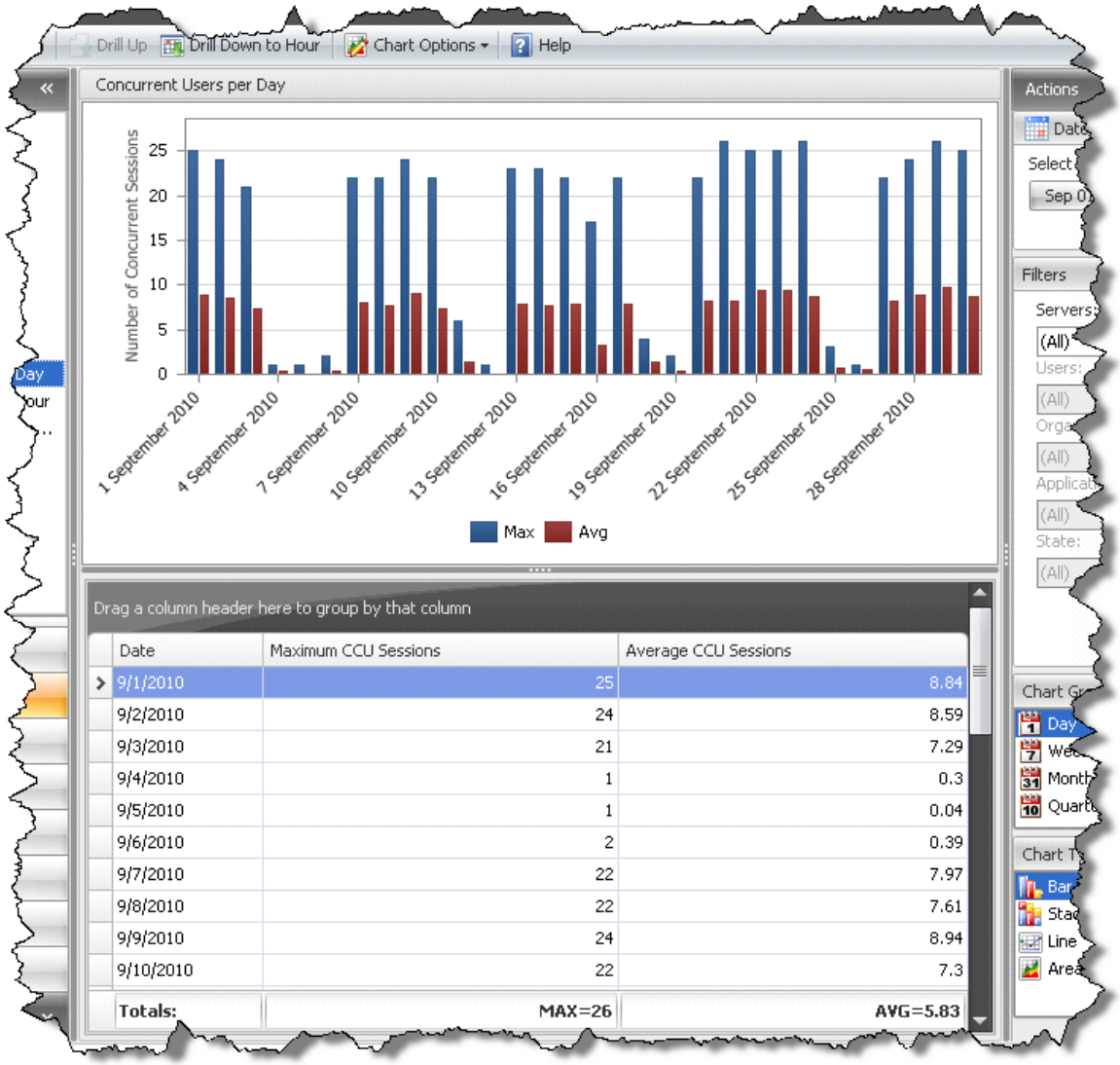
CLIENT LICENSE COMPLIANCE REPORTS

With Farm License Compliance Reports you can easily monitor the number of used Remote Desktop (Terminal Services) CALs and Citrix licenses across the entire server farm. These reports allow administrators to easily track the number of Name or Device licenses being used.

The feature was designed to help administrators determine if the number of licenses purchased matches the current usage and to optimize the costs associated with these. You can easily mix all license types.

CITRIX CONCURRENT LICENSE REPORTS

Terminal Services Log shows you the number of Citrix concurrent licenses used on a Citrix farm. Reports include monthly average use, with the ability to drill down on the per day use report and to see the particular users that are consuming your licenses.



VIRTUAL DESKTOP MONITOR INSTALLATION

PREPARING YOUR ACTIVE DIRECTORY DOMAIN

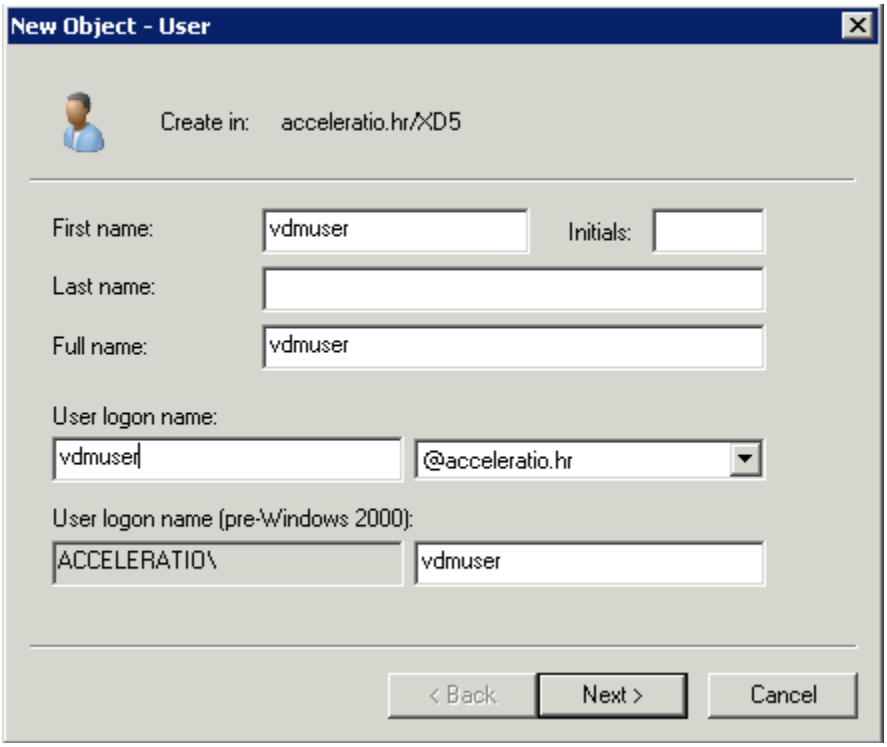
Before installing the application we need to setup a domain for VDM installation, which means creating a new user that will have local admin account on all the virtual desktops.

This user needs to be the local admin on the virtual desktops because it will be used to read all the user related data and will be used for storing data in the central SQL server database.

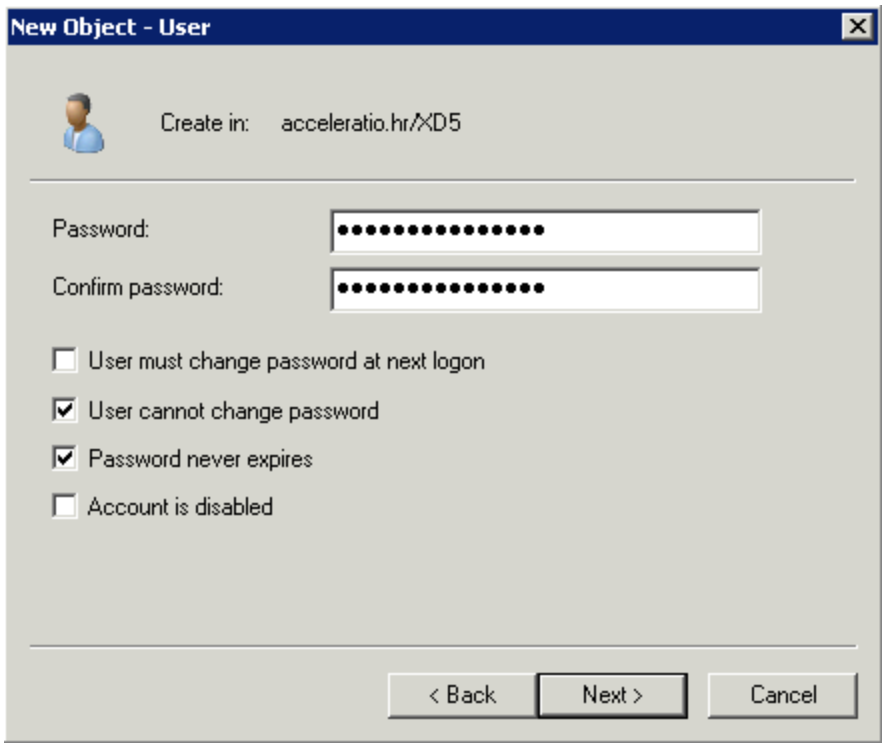
Please note: In test environments, to speed up testing, you can use Existing Domain Admin user but for production environments we strongly recommend creating dedicated service user.

CREATE A SERVICE USER

1. Virtual Desktop Monitor needs a service user that will run the VDM service.
2. Login on the domain controller and open **Active directory users and computers** in **Administrative tools**.
3. Right click on the **domain name** and select **New > User**.
4. Fill in the First name and User logon name fields with e.g. vdmuser (or another name of your choice). This user will be used as the Virtual Desktop Monitor service account.



5. In the next window type the password, and choose the User cannot change password and Password never expires options.
   Important: It is important to check Password never expires option, otherwise your password might expire causing Virtual Desktop Monitor service will stop collecting data. We recommend using a strong password! Please use 7 or more characters with letters, numbers and special characters. Service might fail to start in case of a weak password.



ADDING A SERVICE USER TO THE LOCAL ADMINISTRATORS GROUP

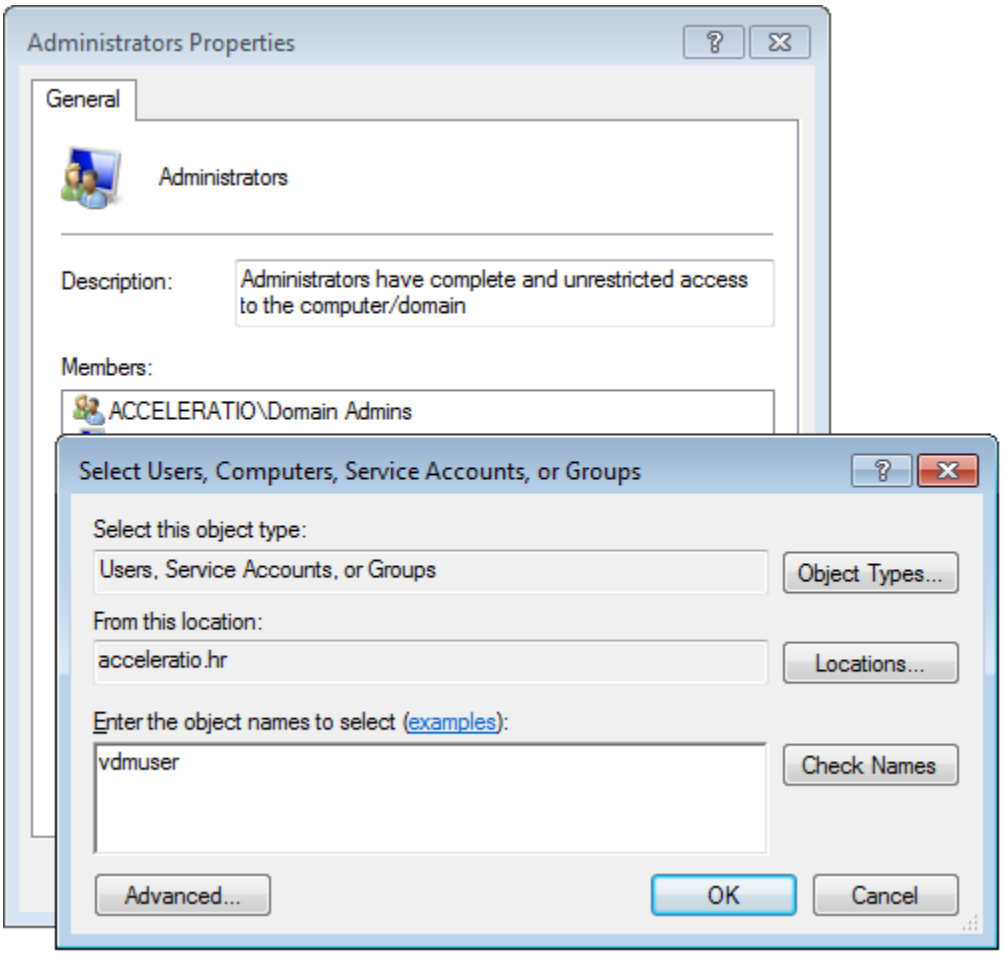
The Service user you created needs administrative privileges on each virtual desktop you plan to monitor. You will need to add the service user to the local Administrators security group. There are two ways to accomplish this:

- Adding Service User to local Administrators Group manually (recommended only for dynamic or non-persistent desktops where you can configure one golden image to be shared across all users that will share the image)
- Adding Service User to local Administrators Group via Group Policy (recommended for most environments, static or persistent virtual one-to-one desktops)

ADDING SERVICE USER TO LOCAL ADMINISTRATORS GROUP MANUALLY

Us this scenario only for dynamic or non-persistent desktops where you can configure one golden image to be shared across all users, otherwise we recommend the second way of using group policy.

1. Logon to the server you plan to monitor.
2. Open Computer management in Administrative tools.
3. Select Local user and groups and then Groups. Double click on the **Administrators** security group**.**
4. Add VDM service user by simply clicking **Add** and typing the name of your VDM service user (usually **vdmuser**).
5. Please note: You need to repeat this procedure for every golden image or desktop you plan to monitor with Virtual Desktop Monitor.

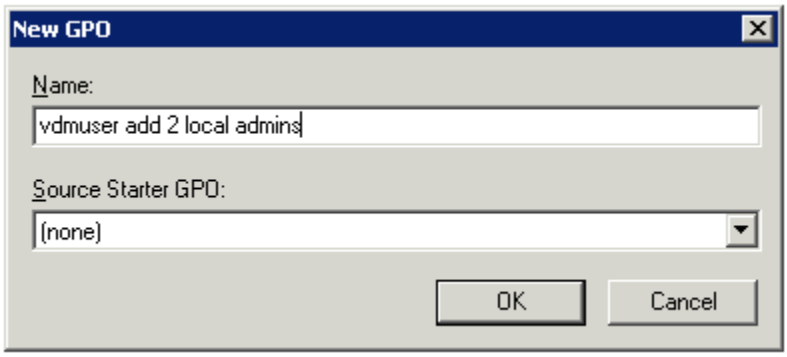


ADDING SERVICE USER TO LOCAL ADMINISTRATORS GROUP VIA GROUP POLICY

Use this to add the Virtual Desktop Monitor Service User to local Administrators group on each virtual desktop you plan to monitor via Group Policy.

In case you have many one-to-one virtual desktops you plan to monitor it is much easier to configure service user permissions via Group Policy. By adding our service user to Restricted groups, you will define his privileges across your domain. You can fine tune administrative privileges via Organizational Units.

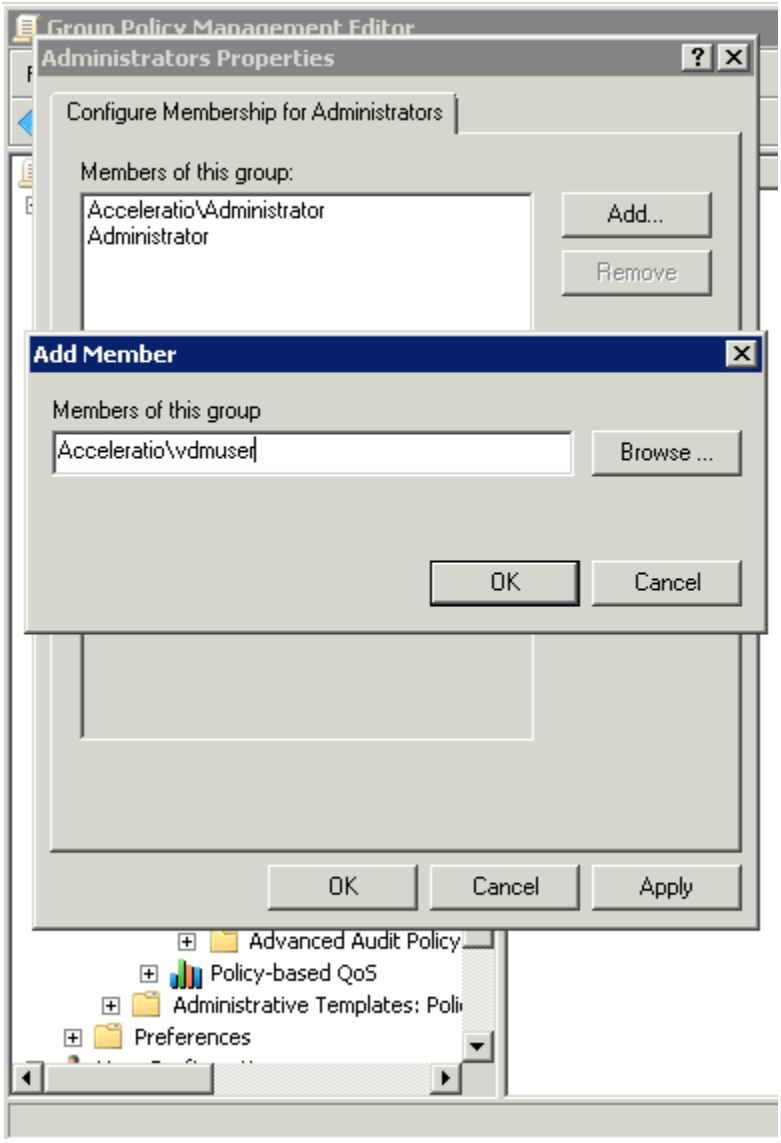
1. Open Group policy management in the Administrative tools on your domain controller.
2. Click on the OU where the virtual desktops are located and select to create a new policy.
3. Name it, for example, *vdmuser add 2 local admins.*



4. Right click on it and select to edit policy.
5. Find the policy setting **Computer Configuratio**n > **Policies** > **Windows settings** > **Security setting** > **Restricted groups**.
6. Right click on the **Restricted groups** and select **Add group**.
7. In the group name type **Administrators** (make sure you did not make a typo. In case you mistype group policy update will fail!).

8. In the members of this group type:
    - Administrator
    - YOUR_DOMAIN\Administrator
    - YOUR_DOMAIN\Domain admins
    - YOUR_DOMAIN\vdmuser

    Please note: If you have other users that you need to add to admin group please define them here as this policy will overwrite local admin group settings on each virtual desktop

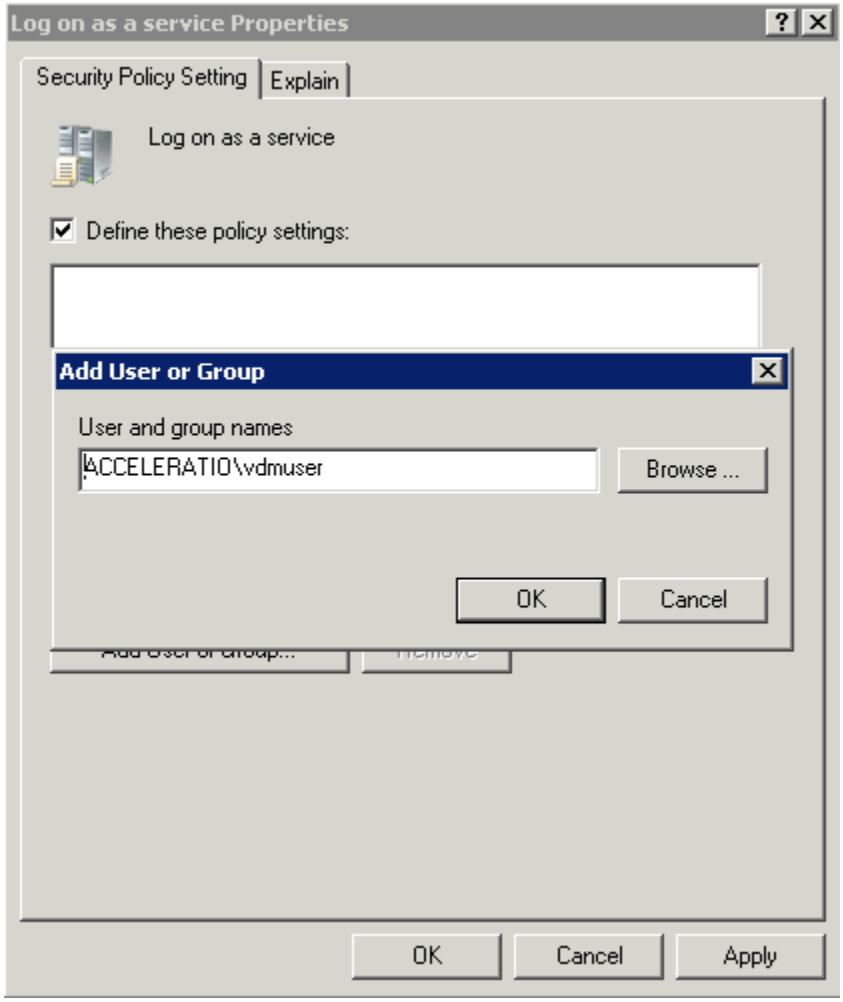


SET "LOG ON AS A SERVICE USER" FOR VIRTUAL DESKTOP MONITOR SERVICE USER

It is important to define a Domain group policy that is going to allow the service user to "Log on as a service user".

You can use the same group policy that we used before, or you can create a new one.

Find the policy setting **Computer Configuration** > **Policies** > **Windows settings** > **Security setting** > **Local Policies** > **User rights assignments** > **Logon as a service** and add the service user that you have created before.



PREPARING SQL SERVER

During installation you will be prompted to select the authentication type for SQL Server.

You can choose between:

- Windows integrated authentication or
- SQL server authentication

In case you are running Virtual Desktop Monitor in a domain environment we strongly recommend using Windows authentication. SQL Server authentication should only be used in Workgroup environments or in case of security restrictions in your domain.

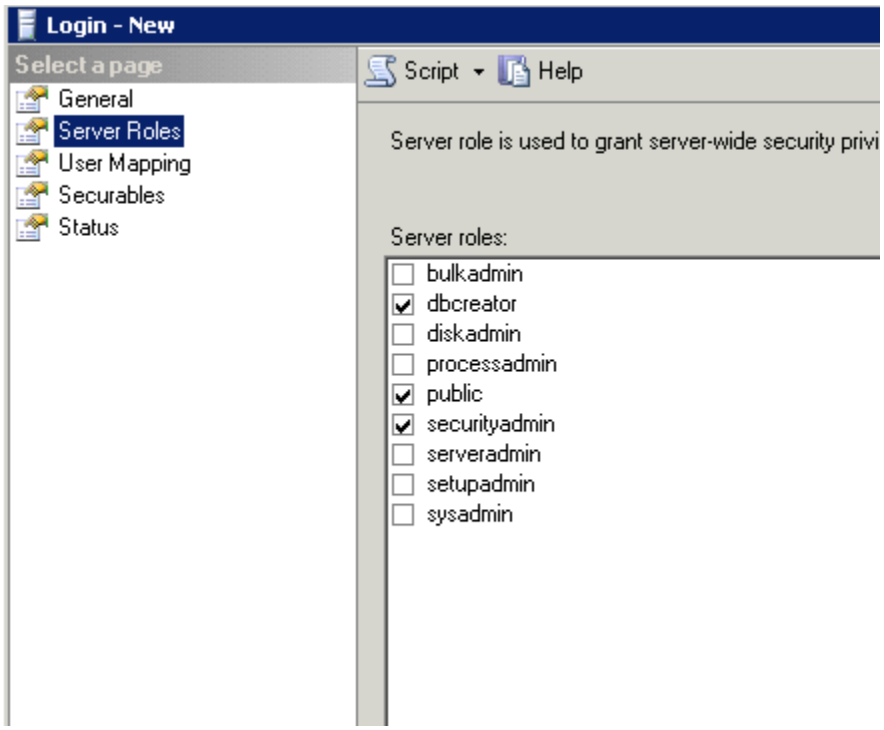
WINDOWS INTEGRATED AUTHENTICATION

In case you plan to use Windows authentication we recommend using our Configuration Wizard to create and configure the Virtual Desktop Monitor database. Service User running the configuration wizard needs to have **Security administrator** and **dbcreator** privileges on SQL Server to create and configure the database.

(Please note: In case you already have a user that you use to connect to your databases, you can skip this step)

In case you want to add an existing domain user to SQL Server follow this:

1. Open SQL Management Studio.
2. Expand Your SQLServer > Security Logins.
3. Right click on the logins and select new login.
4. Type in **your_domain\vdmuser** as the login name.
5. Open **Server Roles** tab on the left, and check **dbcreator** and **security admin** (alternatively in test environments you can use **sysadmin** role).

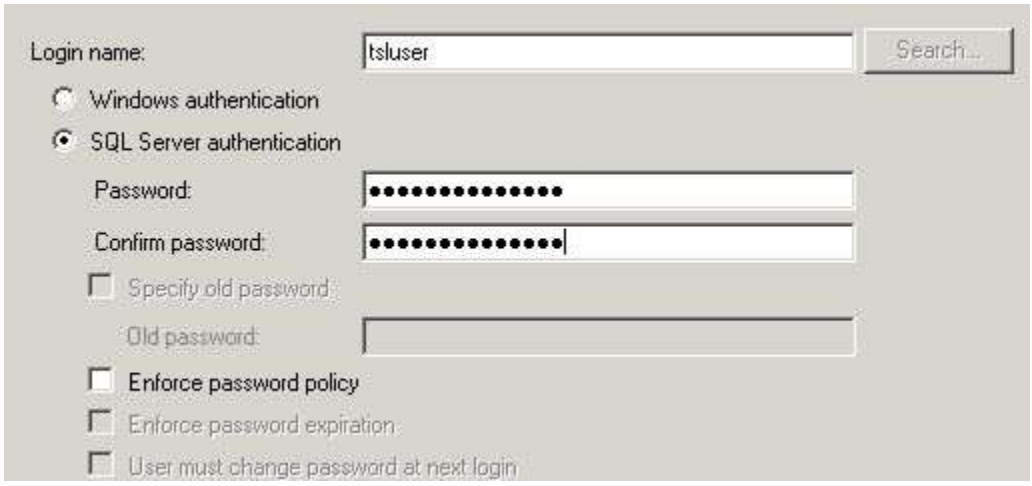


SQL SERVER AUTHENTICATION

SQL Server authentication is used in environments without Active Directory domain, or if SQL Server is outside the domain or simply if you have a security policy that requires you to use SQL Server authentication. Before installing Virtual Desktop Monitor with SQL Server authentication you need to perform additional steps and create a SQL user that will be used to connect to the database.

(Please note: In case you already have a user that you use to connect to your databases you can skip this step)

1. In **SQL Server Management Studio**, open **Object Explorer** and expand the folders of the server instance in which you plan to create a new database.
2. Right-click on the **Security** folder, point to **New**, and then click **Login**.
3. On the **General** page, enter a **Login name** (e.g. *tsluser*).



4. Select **SQL Server Authentication**.
5. Enter a **password** for the login.
6. Uncheck the **Enforce password policy**, **enforce password expiration** and **user must change password at next login**
7. Click **Server Roles** page and check **dbcreator** role (you can uncheck this option once installation is finished)
8. Click **OK** and confirm wizard

INSTALLING VIRTUAL DESKTOP MONITOR

Finally we will deploy the software in the virtual desktop and console on to the admin server.

Installation of the Virtual Desktop Monitor consists of two steps:

1. Installing software admin console
2. Deploying client service on the virtual desktops

Software admin console, the so called Virtual Desktop Monitor Console, is the application that you will use to view reports from clients, schedule email reports to be sent to managers, and control clients' installations on virtual desktops.

VDI client installation is a small footprint installation that is deployed directly on the client that collects the data to the local Microsoft SQL compact database and then syncs the local data with the central SQL server.

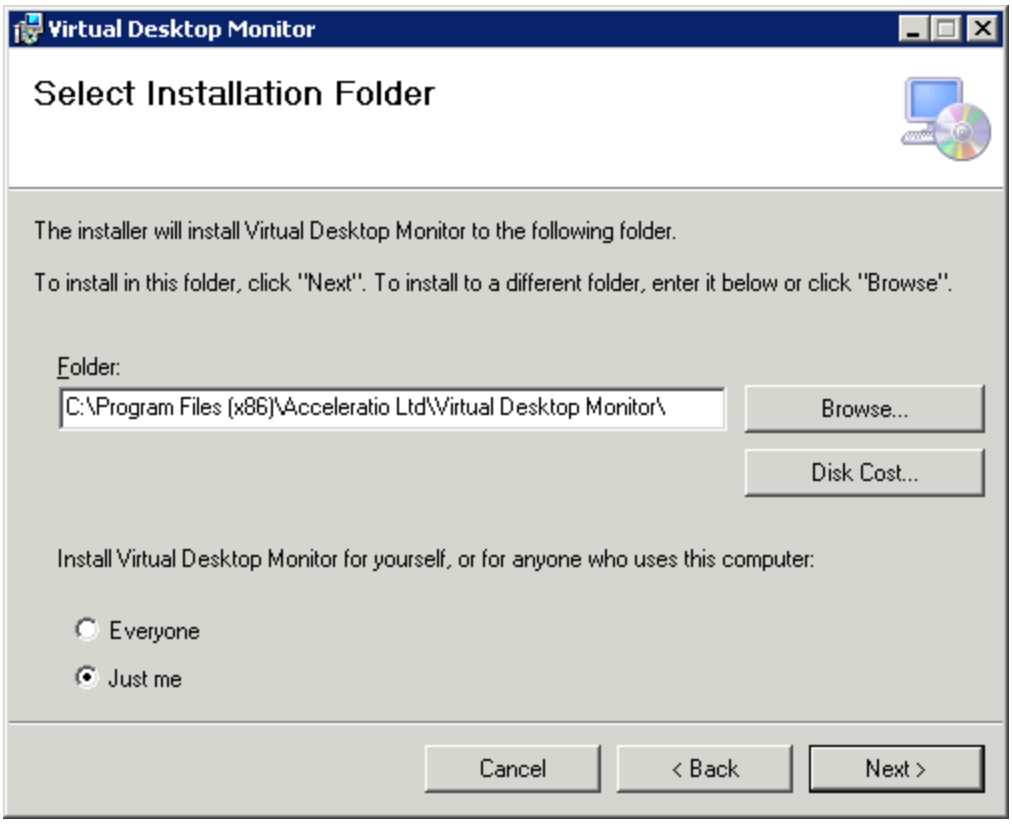
This way client is not dependent on the server and can be used in future deployments for the offline VDI clients. In other words, sync will occur only when client connects to the corporate network.

INSTALLING SOFTWARE ADMIN CONSOLE ON THE SERVER

Software admin console is used to view the reports from the clients, schedule email reports and enable/disable virtual desktops.

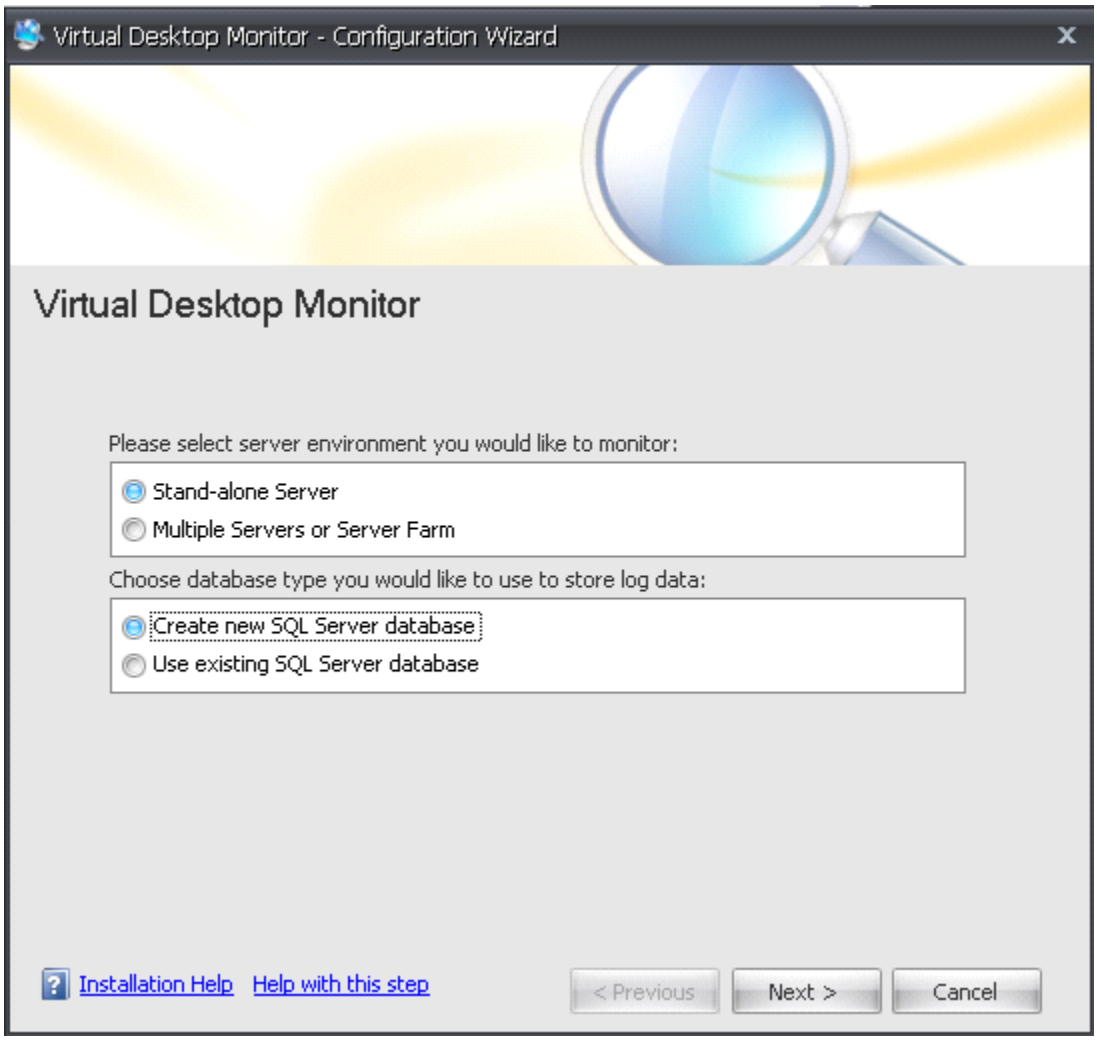
In the file you have downloaded you need to execute **SetupVDI.msi** to install the software on the server.

1. During installation you will be prompted to choose the installation **folder**. We recommend installing Virtual Desktop Monitor with the **Just me** option to prevent other users from using it. You can modify security later and delegate permissions to other users.



2. Once the installation is completed the **Virtual Desktop Monitor Configuration Wizard** will start (if the wizard does not start automatically after installation you can run it manually from: **Start** > **Programs** > **Virtual Desktop Monitor** > **Virtual Desktop Monitor Console**).

3. Choose **Environment** > **Stand-alone server** in order to deploy the software console on only one server.



4. For Database Type **Create a new SQL Server database.** This option will create a new SQL Server database for the data**.**

Please note (for SQL Server Deployments): In case you already have a Virtual Desktop Monitor database or your DBA created a database manually choose **Use existing SQL Server database.*

5. Click **Next >** to proceed.

6. You need to specify **Farm database server (SQL server)**, **database name** and **authentication** that will be used.

Once you enter correct database information click **Test Connection** to verify the information you have entered. Click **Next >** to proceed.

7. You need to enter information about the user account that will be used for running Virtual Desktop Monitor Service. This is the account that we created before that has local admin permissions on each virtual desktop.

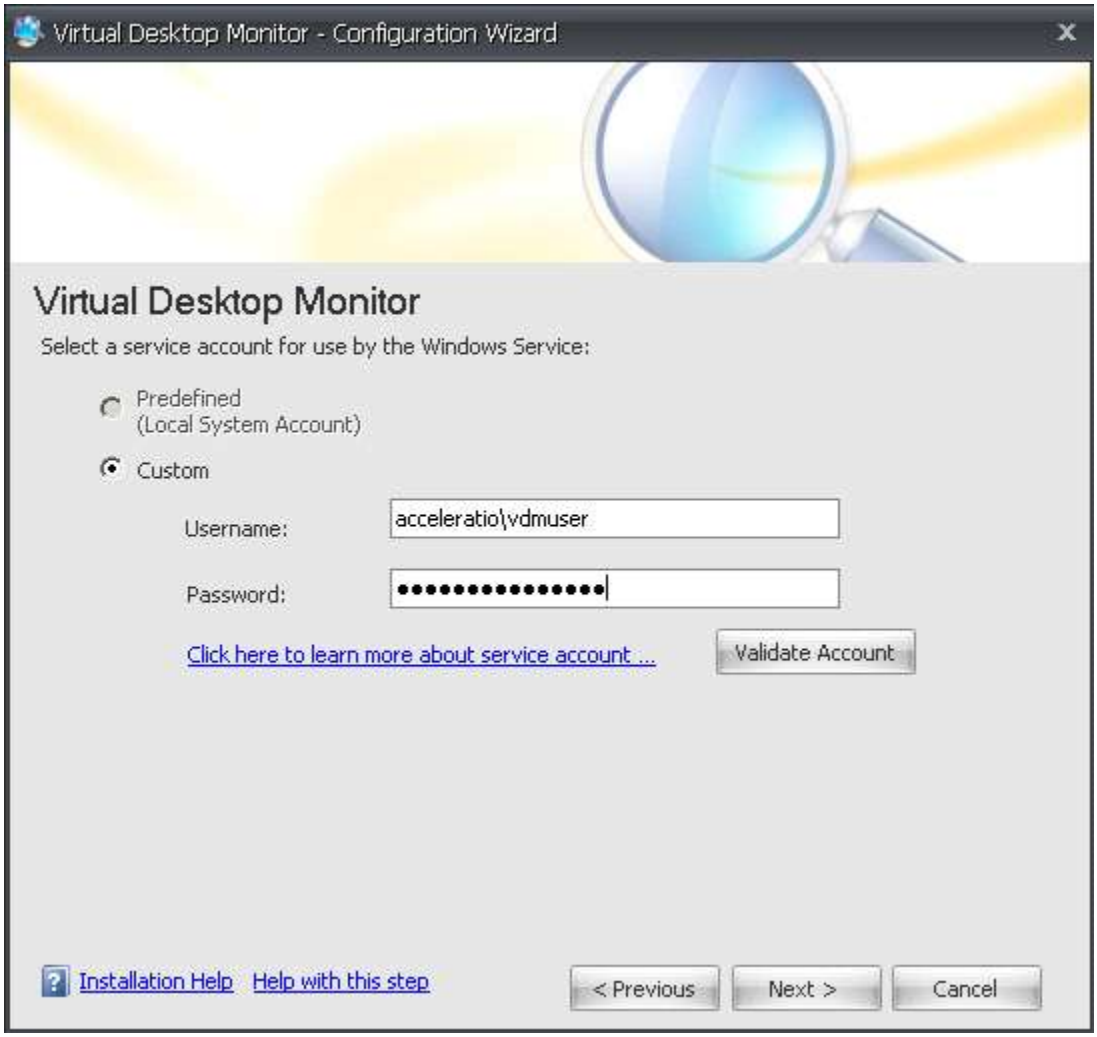
Select **Custom** account

Enter **Username** in the following format **DOMAIN\USERNAME** and password.

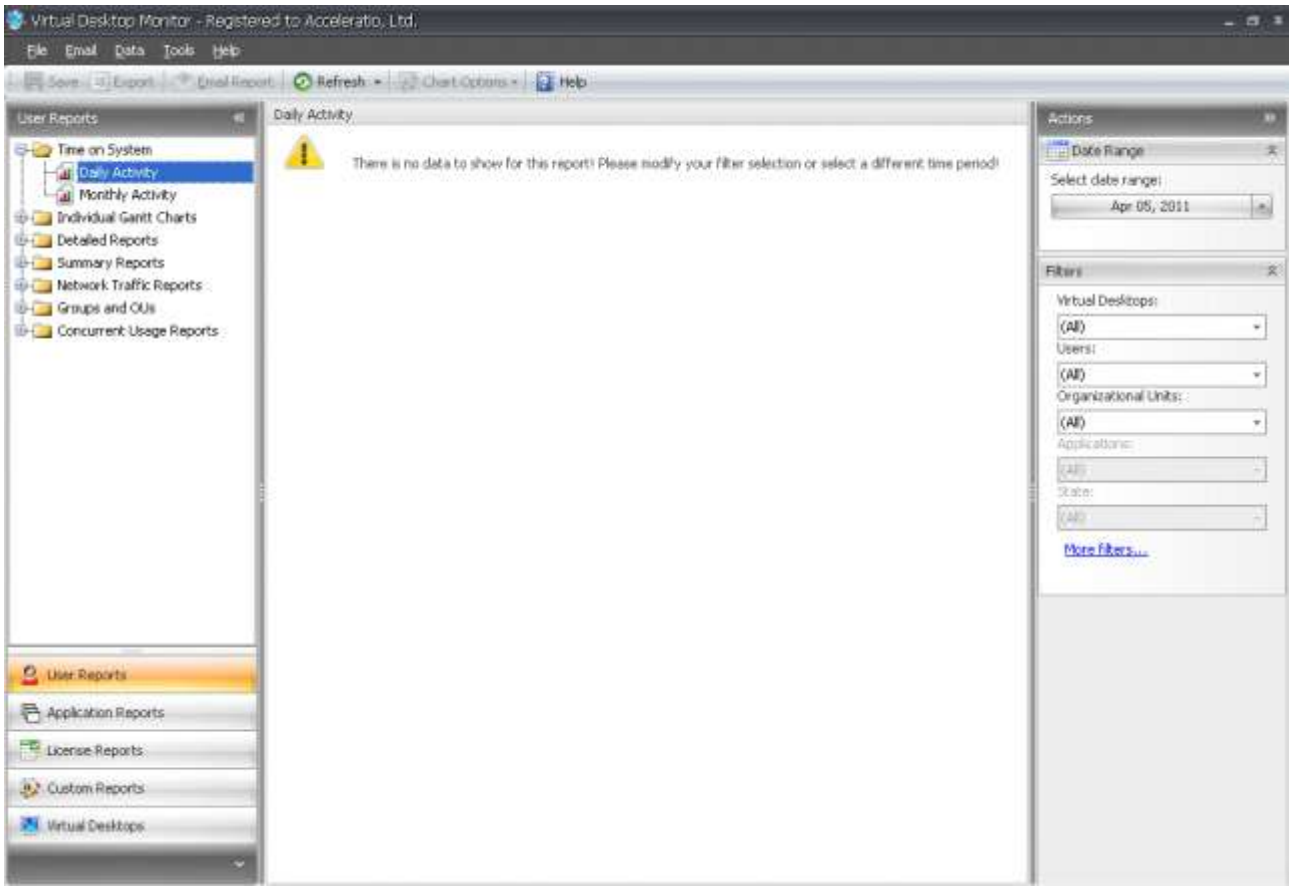
Click **Validate Account** to check the credentials

Click **Next >** to finish the Configuration Wizard.

Application now will create and initiate database on the SQL Server.



In a minute, the application will open and you will see the following interface. Please note there is no data in the database as the client service still has not been deployed.



INSTALLING SOFTWARE ADMIN CONSOLE ON CLIENTS

As mentioned before, client service can be deployed on any VDI environment.

The software supports:

- a static or persistent virtual desktop and
- a dynamic or non-persistent one
- future offline VDI scenarios

INSTALLING SOFTWARE ON STATIC OR PERSISTENT CLIENTS

In static mode, there is a one-to-one mapping of VMs to users. Each user is assigned with a designated VM.

For this scenario we need to deploy VDM service via group policy using software installation settings.

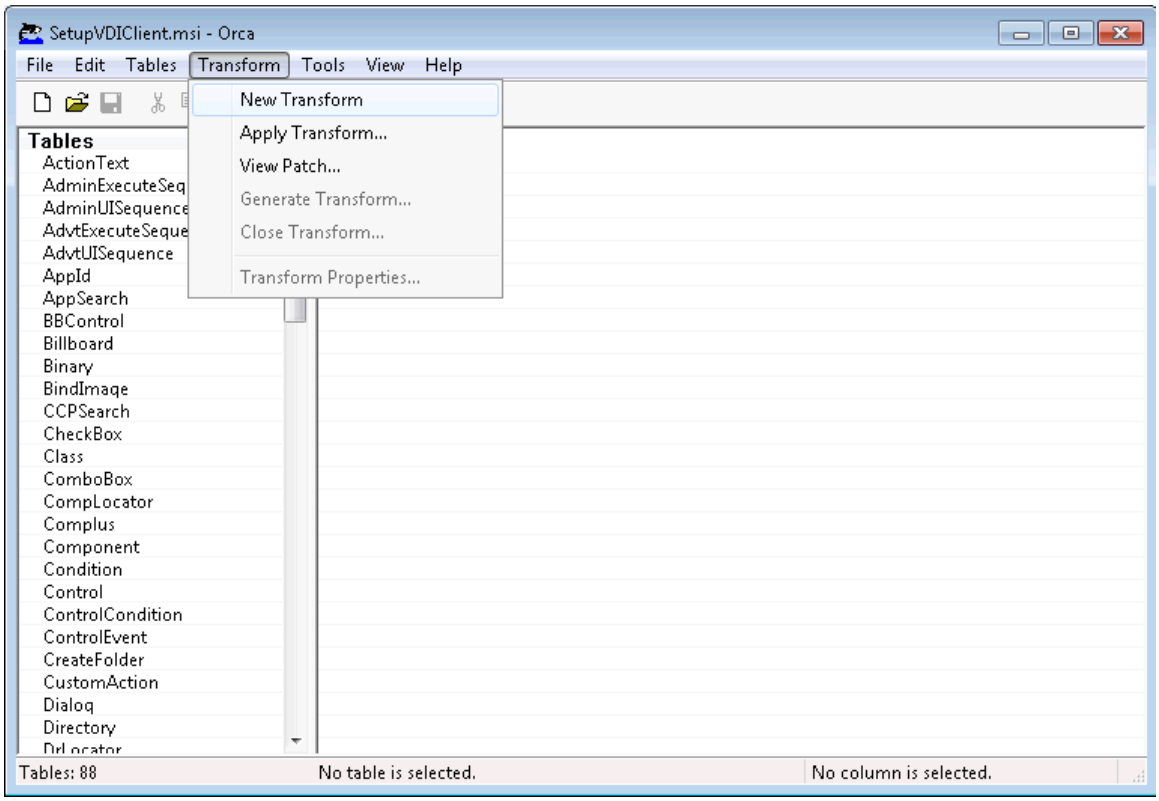
First we will prepare client installation. Client installation is in the zip file that you downloaded and is called SetupVDIClient.msi

GENERATING TRANSFORMATION FILE

Transformation file is added to client installation that specifies the service user and SQL Server database. It is required in order to connect the client installation to the central SQL Server and to specify user which will be used to connect to the database and credentials to run the service.

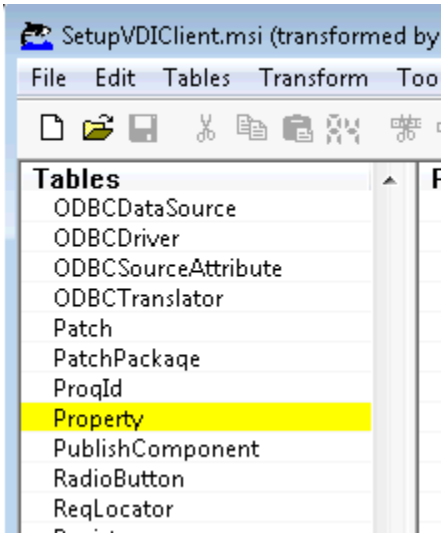
You need to download Orca Msi editior from www.acceleratiosoftware.com/downloads/orca.msi to generate the transformation file.

Once you have download the Orca and installed it somewhere, use it to open **SetupVDIClient.msi**.

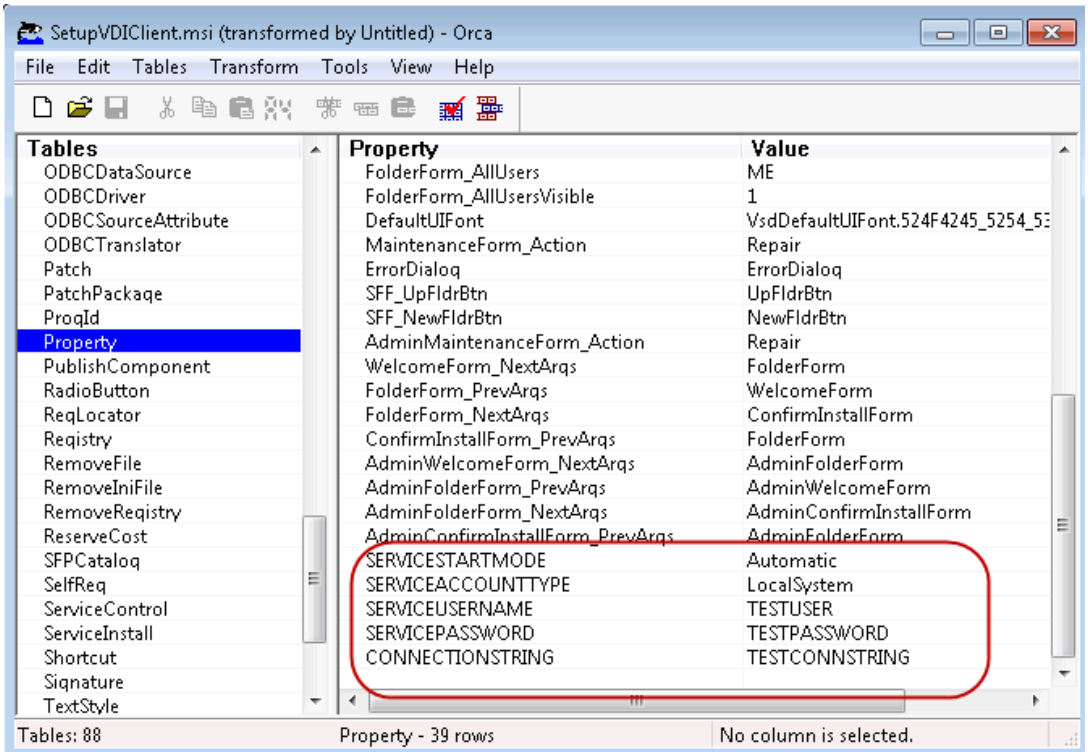


Now we will generate transformations that need to be applied to the MSI file on the installation.

1. Choose **new transform** in **transform** on menu
2. Scroll down **Tables** to find the **Property** field.



3. In the right window scroll down to 5 properties (all written with capital letters) that we need to edit.

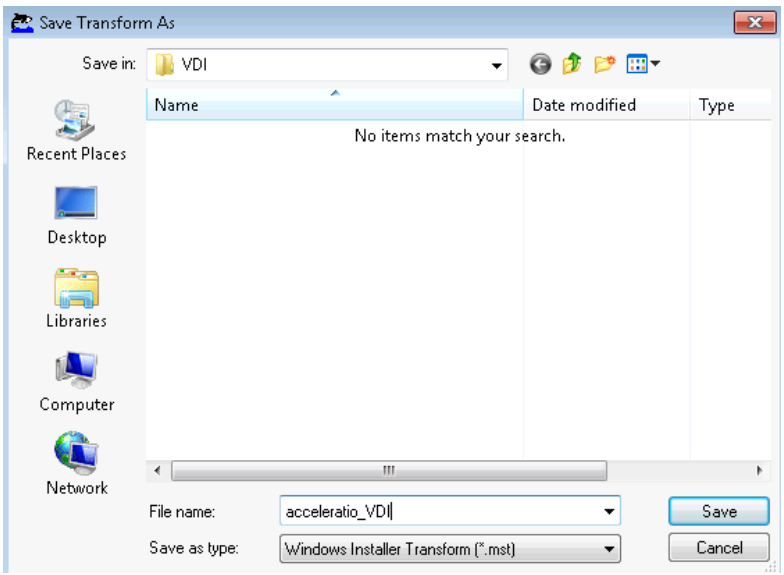


4. Properties are:
   - SERVICESTARTMODE - service start mode
   - SERVICEACCOUNTTYPE – in case you use windows authentication then we will use here service User, otherwise LocalSystem for SQL authentication will be used
   - SERVICEUSERNAME – username of the service user that we created previously vdmuser
   - SERVICEPASSWORD – password of the service user that you setup for vdmuser
   - CONNECTIONSTRING – connection string for the SQL server (using the same database that was created with Virtual Desktop Monitor console)

   Configure properties as follows for recommended Windows authentication:

   SERVICESTARTMODE - **Automatic**
   SERVICEACCOUNTTYPE – **User**
   SERVICEUSERNAME – **DOMAIN\vdmuser**
   SERVICEPASSWORD – **P4$$w0rd4VD1**
   CONNECTIONSTRING – **Server=SQLserver\SQLInstance;Database=VirtualDesktopMonitor;Trusted_Connection=yes; Asynchronous Processing=true;**

5. To generate Transform file in menu **Transform** select **Generate Transform.** Save the file as **acceleratio_VDI.mst,** for instance.

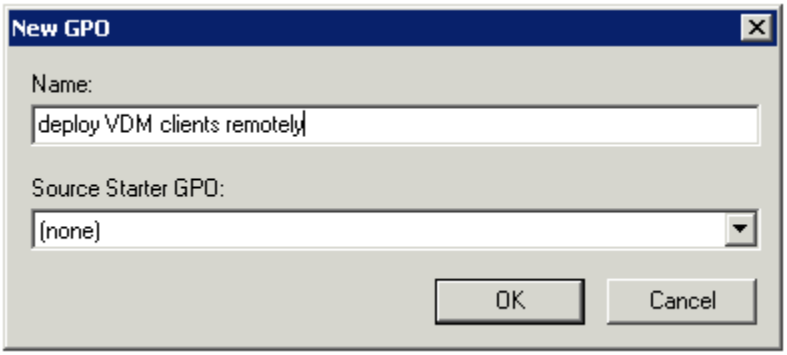


DEPLOYING CLIENT FILES USING GROUP POLICY SOFTWARE INSTALLATION

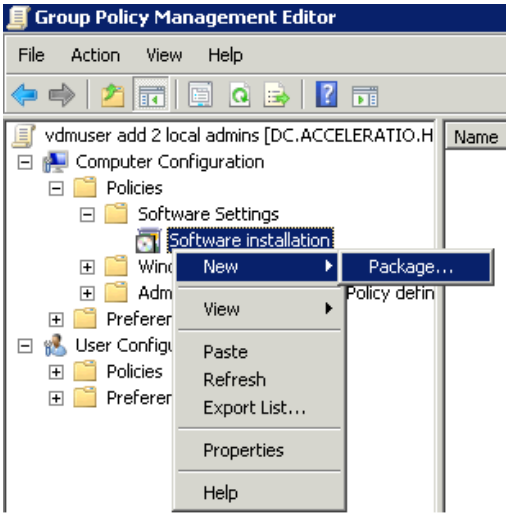
First, we need to copy msi and mst file to the network share where all the Virtual Desktops will have access. For example, we will use **\\file_server\VDMshare**

Now that we have msi and mst file for group policy, we will deploy the client to the virtual desktops. To do this we must create new group policy for the virtual desktops that will install the software.

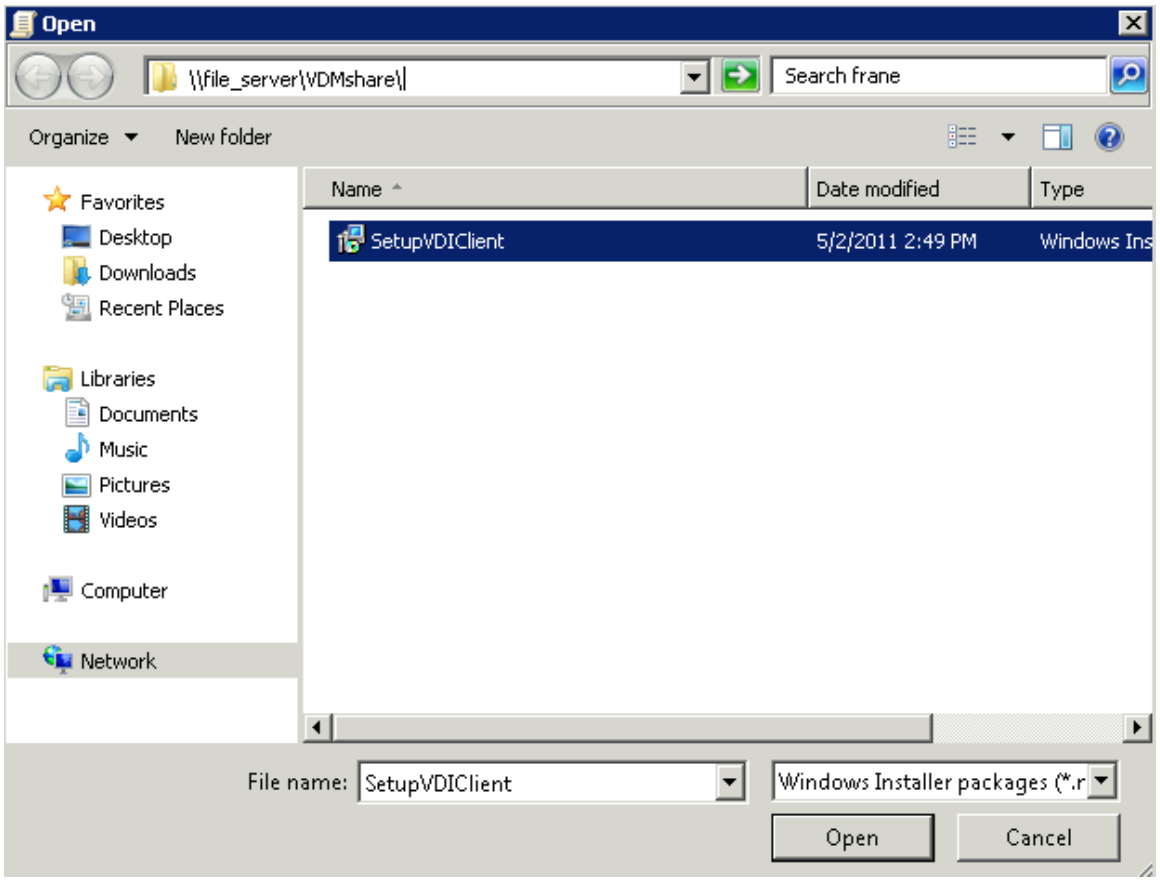
1. Logon to Domain Controller and open **Group Policy Management.**
2. Locate Organization unit where your virtual desktops are or use the same that we used before for logon as a service and restricted groups.
3. Right click on the OU and select to **create a GPO and link it here.**
4. Name the policy "deploy VDM clients remotely", for example.



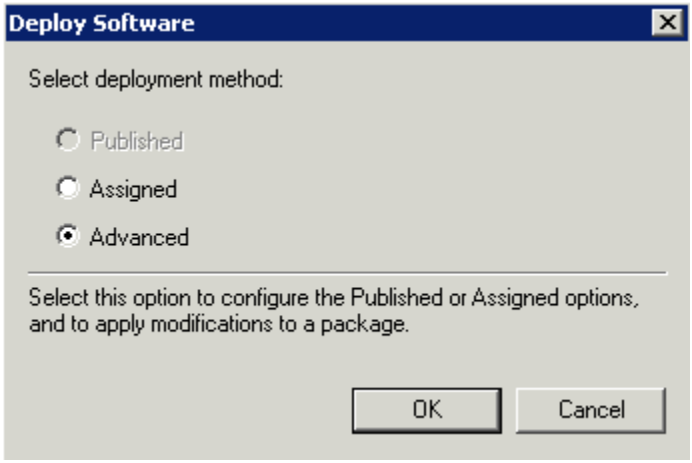
5. Right click on the newly created policy and **Edit** .
6. When the Management editor opens, expand **Computer Configuration** > **Policies** > **Software Settings** > **Software Installation.**
7. Right click on **Software Installation** and choose **New** > **Package.**



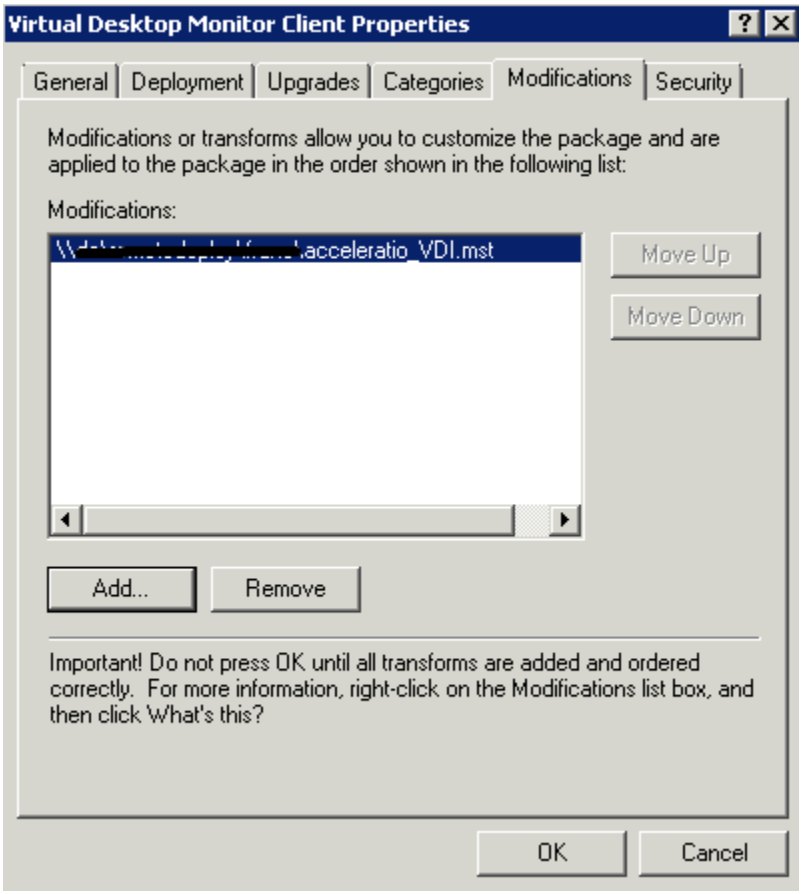
8. You need to select SetupVDIClient.msi file on the file share where we initially copied the file. In this example we will choose a file from **\\file_server\VDMshare**



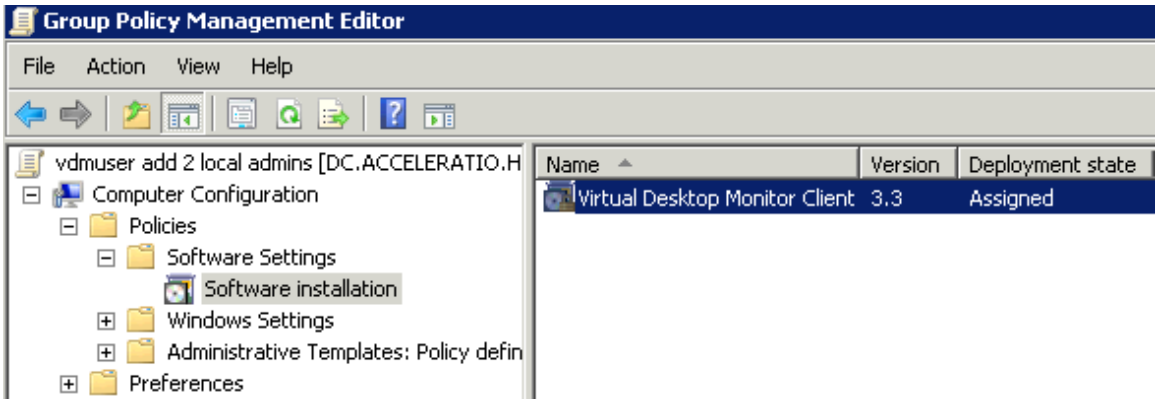
9. Click open and to deploy the software in next window choose **Advanced** because we will need to specify the transformation file.



10. Group policy will now take up to 30 seconds to locate and verify the file, let's wait for that to finish and then we will have Properties of the MSI file.
11. The tab that is interesting for us is **Modifications**, where we are going to select the previously generated transformation MST file from the same file share **\\file_server\VDMshare**



12. Click **OK** and Windows will prepare the software installation MSI file to be deployed on the remote clients.



On the next restart, the software will be deployed to all virtual desktops and slowly you will start to see data in the Virtual Desktop Monitor console that we configured before.

DEPLOYING CLIENT FILES BY INSTALLING ON THE GOLDEN IMAGE

The second way to deploy Virtual Desktop Monitor is to install the monitoring files directly on the golden image that is used for non-persistent desktops where one image is shared between numerous users.

Before moving on, take a look at the **Generating Transformation File** chapter where it is explained how to generate Transformation file, needed in order to configure clients to find the central SQL Server.

Depending on whether you are using Microsoft, Citrix, Quest or VMware solution, you need to edit the golden image and deploy the software installation directly there.

Installation is really simple as everything you need to do is to execute MSI installation with MST transformation file parameter.

The command is:

msiexec /i "SetupVDIClient.msi" TRANSFORMS="acceleratio_VDI.mst" /qn

Save the golden image and return it to the pool where is it accessible for booting. Every time a user logs on to the pooled desktop, the application will start inside the virtualized machine, log the user data and eventually it will sync with the central SQL Server.