

# IMPLEMENTING SOLARWINDS ORION

## Your SolarWinds Account

When you buy a SolarWinds product for the first time you will receive a Customerid (i.e. SW34999) and a password (i.e. tx334d). This information must be stored for future use as you will have to use them when you install the products and when you want to access your customer portal on [www.solarwinds.com](http://www.solarwinds.com). We recommend that you send these details to Draware and we will note them in our CRM system so when you call for support we are able to help you better and faster.

Using your SolarWinds account you can download the latest versions of the products, the newest MIB file and access the “Additional components” section of your account where you will find extra utilities.

## Selecting hardware for your SolarWinds installation

We recommend that you as a minimum reserve 2 servers for your SolarWinds installations – 1 for Orion and the modules (if any) and one for the Microsoft SQL database. The first server can well be virtual and a good starting point is a 2 CPU, 4Gb RAM and 40Gb Free disk space. The second server (i.e. the SQL server) should if possible be a physical server running minimum 4 disks in RAID 10 and have 2 CPUs, 8Gb RAM and approximately 200GB free disk space. Ensure that the Orion server has only ONE IP ADDRESS.

## Installing your SolarWinds Software

Please see the section “Notes about the Orion installation” before proceeding. Download the latest version of your SolarWinds products and the latest MIB file from your SolarWinds account. Install the SQL server on the second server. It is important that you during the software installation use a local admin account or a domain admin which has been inserted in the Administrators group on the server. This is true for both the SQL server and the SolarWinds Orion server. Please note the following important points:

1. You may use SQL 2005 or 2008. If you use SQL 2005 make sure it is on SP3 or higher.
2. Install the SQL server with Mixed mode authentication and enable CLR
3. Create an SQL account called SolarWindsSA and a password to your liking. And make sure the account has “Sysadmin” rights (Role).
4. As a thought please be aware that you must – as a minimum - always have the more space free on the SQL server than the max size of your database

5. The SolarWinds database, which is automatically created during installation, will normally grow to approximately 20Gb. If you enable syslogs and SNMP traps the database may grow much larger – i.e. 200Gb.

Install your SolarWinds Orion on the first server. During the install when prompted for the database, please point Orion to your newly created Orion SQL server (Note that if you use the default instance you can just write the server name / IP address. Otherwise you must use the “name\instance” syntax. When prompted for the access to the database use your SolarWindsSA account. During the next phase Orion will create another SQL account called SolarWindsNPM which Orion uses to read/write to the database.

Please note the following about the Orion server:

1. The server must have IIS, SNMP and dotnet 3.5 installed
2. It is easier to install if the Orion server has access to the Internet, but it is not absolutely necessary
3. Naturally both servers should have a fixed IP address.
4. Create a document on the Orion server detailing the setup and accounts used – including your SolarWinds account.
5. Make sure that your servers (Orion and SQL) are fully patched. We introduce software like dotnet which normally requires extra patches

If you have modules you can proceed to install them one at the time. Please note the following:

1. Using the APM module will only work successfully if you ensure that all servers to be monitored are SNMP enabled and that you HAVE AN ADMINISTRATOR ACCOUNT for all servers that you want to monitor.
2. The NetFlow module requires you to open for port 2055
3. The Network Configuration Manager (NCM) “module” has an extra install under Orion Integration that must be installed after the primary NCM install to enable integration with Orion NPM.

### Notes about the Orion installation

During and after the Orion installation, please consider the following:

1. Make sure that you ALWAYS access the Orion server with a local admin account before installation
2. After install the SolarWinds products are locked to the specific server. You may use the license manager from your SolarWinds account to unlock the products or you're welcome to call/e-mail Draware A/S and we will help you to reset your SolarWinds account. However this may take a couple of hours so please be patient.

3. Do not change the name or IP address of the Orion server
4. Always use the SolarWindsSA account to access the database during installation.
5. MAKE SURE that you have a valid backup of the Orion database (NetPerfMon) and if you have the NCM module also the ConfigMgmt databases. Orion keeps all setup, all data, all maps and all statistics in a single database (two if you're running NCM). So if you have a valid DB backup restoring Orion NPM in an event of a crash is easy.
6. Keep an eye on the database size (growth). If you send traps and syslogs to Orion NPM the database might grow uncontrolled leading to a very slow performance and ultimately to crashing/halting NPM operation. We recommend that you only send syslogs of severity warning and higher to Orion and that the retention time for traps and syslogs are kept at no more than 7 days. The nightly Orion maintenance job will summarize data and remove outdated data from the database – i.e. perform database maintenance/grooming.

If you do not use syslogs and traps for anything (i.e. only storage) please consider an alternative eventlog management system - you can see more on [www.draware.dk](http://www.draware.dk) or contact us. SolarWinds Kiwi Syslog server is a very low cost alternative solution in this range.

## First step to Orion implementation

Please proceed as follows to get the best possible Orion NPM installation

1. Add all the Nodes you want to monitor. A node is normally a server, a switch, an access point/WLC, a firewall, a UPS and so forth. A monitored node must have an IP address that you can PING (ICMP) from the Orion server and if you want performance information (i.e. once all nodes are in CPU load, Memory load, interface statistics, errors and discards, custom OIDs) you must SNMP enable the node. Nodes that you only ping will give you availability, latency and packet loss information.
2. If you add ICMP ping nodes you can change the name of your nodes to your liking. In the regard please bear in mind that Orion has 3 different node names:
  - a. "Caption" is the internal name for a node in Orion
  - b. "System Name" is the name of the node returned by a SNMP lookup
  - c. "DNS name" is the name returned by a reverse IP address lookup
3. Once all nodes are in your system think about how long you want to retain the statistics data gathered by Orion. They can be specified under Admin/Polling settings. We recommend that you set these to 90(detailed)/90(hourly)/400(daily)/90(events). For very large installations you may consider lowering these numbers as the database will be impacted (grow) proportionally with the increase from standard of these settings.

4. Meticulously go through each node and add all infrastructure interfaces that you wish to monitor. Be particularly aware of user access switches. You do normally monitor the ports on which the desktops/laptops of your users are connected – only the uplinks from these switches. On servers remember to add all hard drives but avoid floppy disks and CD-ROM drives. Please note the following:
  - a. For each interface/node/volume you add, you will use an Orion NPM license
  - b. Adding interfaces linked to desktops will result in errors every time the user turns off their PC. You can circumvent this by setting this interface (if you still want to monitor it) as “Display interface as unplugged rather than down” under “Edit Interface”.
  - c. When you add an interface with no description present in the switch it will return a number or the default description. Consider changing the name of the interface to reflect its function. This will greatly enhance future reports and web displays as you will immediately see the function of the interface as opposed to “FastEthernet0/1 – Fa0/1” has X% utilization.
5. Consider what kind of GROUPING and LIMITATION you would like to impose on your nodes (and if you need too also on interfaces and volumes). We recommend that you start adding the following groups in the custom property editor:
  - a. DeviceType – i.e. switch, server, firewall, AP and so on
  - b. DeviceLocation – i.e. Physical location in a rack, city or organizational unit
  - c. DeviceGroup – i.e. top location such as country or company
  - d. DeviceSeverity – i.e. how important is this device for your network on a scale from 1-3
6. Fill in the information for all nodes and check that the grouping under All nodes is suitable for your organization. Then make sure that the new device properties are added to the limitation table so you can impose a limitation for a specific account or a specific view in Orion.
  - a. Note: You can often cause a reply on these information as they are read from the SNMP defined values in each device, but if you are adding Ping nodes this information cannot be read and it is also much easier to maintain and control custom properties in Orion as opposed to changing hardware values
7. Consider what accounts you would like to use with Orion. User accounts are used at the initial Orion NPM login screen and they determine WHAT A USER CAN DO AND SEE. Accounts are normally created as either PERSONAL accounts (i.e. John Patrick – Network administrator) or ROLES accounts (i.e. helpdesk or technician). You then proceed to create menu bars for each account followed by views for each account. Please note the following:
  - a. The normal sequences by which you create the above functions are: 1) Login as admin and create a new account with admin rights and the admin menu bar. 2) Logout and login with the new account (you can see the account name in the top right hand corner of the screen. 3) Make all the necessary changes to the account which you will see immediately as you are logged on with that account. 4) Logout and login with the admin account and remove the rights that you do not want (i.e. such as “Administrator Rights”) on the account you

have just created.

8. When you create new views (and please do not alter the existing views – always make a new view or make a copy of an existing view) please bear in mind that the views must communicate what the specific account needs to see. Too much information will simply cloud “the message”. You can tailor each view using the following:
  - a. Resources – They determine the individual items shown in a view and ultimately what the user will see in each view. There are hundreds of resources available from the add resource button in each view definition
  - b. Filters –On each resource you can add a filter that will define the resource to display more specific information. The filters are based on normal SQL queries with the following syntax: “table.heading contains constant” (i.e. Nodes.Caption contains ‘DK’).
  - c. Limitations –They determine what is show in a view (not defined per resource but rather by view). Typical examples as DeviceTypes, DeviceGroups, IP-addresses, Vendor, MachineType and son on.

## Setting up alerts in Orion

Note 1: Only setup alerts that you really want to see. Too many alerts will enviably lead to the result that you delete them all – including the one that is important!

Note 2: When you see something in red or flashing on the Orion screen it is NOT an alert – just a graphical display of a possible error situation. Alerts are defined in System Manager on the Orion server and when triggered you may see them in the Alert resource on the web interface if you have added this resource to you current view.

Note 3: If possible, avoid using the Basic Alerts function. Use the Advanced Alerts whenever possible.

To define and handle alerts we suggest you follow these steps:

1. Start by planning on which alerts you want to see, the people to receive the alerts and the way you want to deliver these alerts:
  - a. In general there are two types of alerts – availability and performance. You can start by defining the availability alerts such as node down and interface down, since these alerts are rather simple. We suggest that you refer to groups of nodes and interfaces as this will make alerting on future nodes and interfaces simpler to handle.
  - b. Define the people to whom the alerts must be sent. This can be i.e. the helpdesk, technicians or external consultants.
  - c. Then define the vehicle by which you want to deliver the alert. The methods most commonly used are e-mail, SMS, NET message and writing to a text file. If you send out e-mails it is normally a good idea to define a group in your e-mail system and send the alerts to that group. If you want to included SMS messages, we recommend our SMSgateway from SYSman (please see [www.draware.com](http://www.draware.com)). Do not use an e-mail to SMS converter at this system is very vulnerable if your e-mail system does not work properly for some reason. We also recommend integration to you helpdesk system where you send your alert to the helpdesk via e-mail. This will ensure that all your alerts are tracked and can easily be

reported on. If you need a nice helpdesk solution we recommend ServiceDesk Plus from ManageEngine. Please see more on [www.draware.com](http://www.draware.com).

2. Test you alerts when you have created them and make sure that they trigger on the right conditions. If you are creating performance alerts (i.e. CPU load > 80% over 20 minutes for all DC servers) please make sure that Orion has been running for 14 days or more. That way you will have an established a baseline for performance (see the 95% graph lines) and know what to set as the trigger value.
3. Document your alerts. Please make sure to fill in the description field of each alerts in a easy to read text so your colleagues can easily understand why the alert is being sent.
4. Consider including a text or a link with every alert specifying:
  - a. Who sent the alert
  - b. How to remediate the alert
  - c. Who to call in case of questions
5. Orion NPM Alert manager has an option to suppress any alerts actions for both Basic and Advanced alerts. Make sure this is only turned on during test and if necessary to stop an unwanted flow of alerts. Otherwise you will never see the alert actions in real life.
6. Examples of common alerts are:
  - a. Alert me when a node goes down
  - b. Alert me when an interface goes down
  - c. Alert me when the CPU load is > 80% over 20 minutes
  - d. Alert me when the CPU load is > 90% over 20 minutes
  - e. Alert me when the interface utilization is > 60% over 20 minutes
  - f. Alert me when Interface Errors and discard rises over 1.000 over 1 hour
  - g. Alert me when there is < 1Gb free space on the C: drive

## Setting up reports in Orion

Orion NPM comes with an extensive set of predefined reports. They can be altered to your specifications and you can create new ones as you please. You can see the report section on the Orion web page or you can include a report as a web resource in a view. You may chose to make reports show up in the web interface (or be hidden) and you can schedule reports. You can export a report to another format such as XLS or PDF but you cannot schedule this export – only as HTML. Also you cannot create reports with graphics (i.e. a pie or bar chart). For this functionality we recommend the tool Report Services included with the Microsoft SQL server.

Reports are defined using the report write tool on the Orion server. You simply follow the tabs listed and make the necessary changes and save the report. Most customers want to see a SLA report over availability of nodes and traffic reports or change management reports from NCM.

## Support and maintenance on SolarWinds products

As long as your SolarWinds product is under active maintenance you have access to the following services:

1. All product upgrades and updates (SP) from your SolarWinds customer portal. As a word of caution you do not necessarily have to install the newest release and we encourage you to wait until the release is accompanied by the first SP.
2. Free technical support from Draware (GMT01 8:30 – 16:30) and the Vendor (24/7). We offer support via phone, e-mail and WebEx (on-line). You may write us at [support@draware.com](mailto:support@draware.com)
3. Access to the “Additional components” section on your customer portal
4. Access to training videos on your customer portal
5. Right to reset you SolarWinds account so you can move your SolarWinds products to a new server. This can be accomplished using the License Manager from you customer portal or by contacting Draware™ A/S directly.

## Contacting Draware A/S

Draware A/S  
Teglgården 46  
DK-3460 Birkerød  
Denmark

Tel: (+45) 45 76 20 21  
Fax: (+45) 45 76 41 21

Web: [www.draware.dk](http://www.draware.dk)  
Support portal: <http://112.draware.dk>  
[info@draware.dk](mailto:info@draware.dk) / [support@draware.dk](mailto:support@draware.dk)

We offer support in Danish, Swedish, Norwegian and English

## Contacting SolarWinds support

Please call (+353) 21 500 2900 and press 3 and 1 (in Denmark you may call 80 60 00 53 for a toll free line). Have your SW number handy. You can also create a support ticket directly from [www.solarwinds.com](http://www.solarwinds.com) . SolarWinds support is only in English.

When you submit a support request you should also create a diagnostics file (from the Orion server using the Diagnostics menu) and either send the file as a response to e-mail or upload the file via <http://solarwinds.leapfile.com> . When asked for an e-mail address use [support@solarwinds.net](mailto:support@solarwinds.net).