

PREDATAR

Getting Started Guide

For Customer – version 2.2

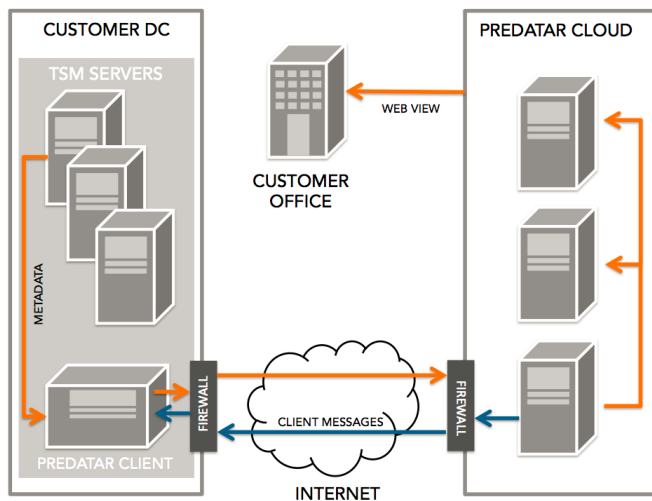


Overview

This guide will assist PredPartner through the process of installing and running Predatar software on Customer's environment in order to integrate with one or more of their Spectrum Protect servers. A technical customer user can independently undertake the installation but the assistance of a Predatar Partner consultant is recommended.

One installation of Predatar client can collect metadata from about 10 Spectrum Protect servers and send it to the PredPartner cloud over the Internet.

The Predatar Client software initiates a connection to the Predatar cloud to transfer the encrypted metadata collected from the SP servers to the Predatar cloud over secure HTTPS connection which uses 2048 bit RSA encryption.



The only component that needs to be hosted in the customer environment is the Predatar Client. It collects metadata via 2 methods from the Spectrum Protect servers:

- Real time collection of the Spectrum Protect server activity log, namely ANR (server) and ANE (client) messages. A typical Spectrum Protect server can easily produce a million lines of Spectrum Protect activity log information in a month. Only Error and Warning messages are trapped and sent to the

Predatar cloud. All informational messages are disregarded. In addition, the Predatar client can also detect “message storms” and suspend the sending of particular ANRs to the Predatar server for a period of time.

- Scheduled collection of Spectrum Protect information from Spectrum Protect server database tables. The frequency of metadata collection is controlled from the Predatar portal.

There are four main steps in order to get the Predatar client software running, which are listed below:

1. Meet hardware and software prerequisites
2. Register Customer and Predatar agent(s) on the Predatar portal
3. Download and install Predatar client software
4. Run Predatar client software

All these steps are explained in the subsequent sections.

Meet hardware and software prerequisites

In order to install and run the Predatar client software on Customer's environment, certain hardware and software requirements have to be met. The following sections explain those prerequisites.

Host server requirement

At least one server will be required upon which the Predatar client software will be installed. The Predatar client software installed on the host server will monitor one or more Spectrum Protect servers that exist in the Customer's environment.

Please use the following checklist to ensure that the host server meets all the necessary hardware requirements :

1GHz or higher CPU	<input type="checkbox"/>
200MB of space in RAM and 50MB required for each Spectrum Protect server to be monitored (This includes Predatar Client memory usage only, excluding operating system requirements and SP BA Client Software requirements)	<input type="checkbox"/>
Approx. 1GB of free space on the disk required for each Spectrum Protect server to be monitored	<input type="checkbox"/>

Please use the following checklist to ensure that the host server meets all the necessary software requirements:

Host Operating System is Windows server 2008 or above (can be 64 bit only) current at Sep 19	<input type="checkbox"/>
Spectrum Protect Backup-Archive client installed and the version is 6.2.2.0 or higher. Note: TSM Server 6.1 is NOT supported by Predatar	<input type="checkbox"/>
Spectrum Protect Backup-Archive client installed with Administrative command line	<input type="checkbox"/>
Network access to all the Spectrum Protect servers on their respective TCP/ IP ports.	<input type="checkbox"/>
Access to your partner's Predatar Cloud host over HTTPS. For the UK cloud, the Predatar Cloud host URLs are: https://serveruk.predatar.com <input type="checkbox"/> https://serveruk.predatar.com:1753 <input type="checkbox"/>	<input type="checkbox"/>

http://serveruk.predatar.com <input type="checkbox"/> (not recommended)	
For the US cloud, the Predatar Cloud host URL is: https://serverus.predatar.com <input type="checkbox"/> https://serverus.predatar.com:1753 <input type="checkbox"/>	
http://serverus.predatar.com <input type="checkbox"/> (not recommended)	
For the German cloud, the Predatar Cloud host URL is: https://server.predatar.de <input type="checkbox"/> https://server.predatar.de:1753 <input type="checkbox"/>	
http://server.predatar.de <input type="checkbox"/> (not recommended)	
(Please ensure the PredPartner host URL is accessible).	
The access to the Predatar server can be verified by browsing to the URL. However, if access to the Internet is only allowed through the proxy then please consult the network administrator to verify the access.	

Please note that the host server can be the same server upon which the Spectrum Protect server is installed, however, it is recommended that the Predatar client software is installed on a separate server to ensure uninterrupted monitoring.

Spectrum Protect server requirement

All the Spectrum Protect servers to be monitored by the Predatar client software need to meet certain requirements. Use the following checklist to ensure all the requirements are met.

An admin account exists on the Spectrum Protect and its password is set to never expire. It will need the necessary permissions to run DedupeStats and automated client restarts. Run the following command to create the admin account and grant necessary access: REG ADMIN PREDATAR SECUREPASSWORD CONTACT="PREDATAR ACCOUNT FOR RUNNING QUERIES" PASSEXP=0 GRANT AUTH PREDATAR CL=SYSTEM	<input type="checkbox"/>
--	--------------------------

<p>All the client messages except informational messages are disabled on the Spectrum Protect server console.</p> <p>Run the following commands to do so:</p> <pre>ENABLE EVENTS CONSOLE ALL NODENAMES=* DISABLE EVENTS CONSOLE INFO NODENAMES=*</pre>	<input type="checkbox"/>
<p>All the server messages except informational messages are disabled on the Spectrum Protect server console to limit processing overhead.</p> <p>Run the following commands to do so:</p> <pre>ENABLE EVENTS CONSOLE ALL DISABLE EVENTS CONSOLE INFO</pre>	<input type="checkbox"/>

Server name: Server IP/ Hostname: Version: Admin login Admin password	Known <input type="checkbox"/>
Server name: Server IP/ Hostname: Version: Admin login Admin password	Known <input type="checkbox"/>
Server name: Server IP/ Hostname: Version: Admin login Admin password	Known <input type="checkbox"/>

It may help to fill in the following table with the details of the Spectrum Protect servers that will be monitored:

Server name: Server IP/ Hostname: Version: Admin login Admin password	SPSRV01 10.0.0.4 8.1.0.0 admin password
Server name: Server IP/ Hostname: Version: Admin login Admin password	Known <input type="checkbox"/>
Server name: Server IP/ Hostname: Version: Admin login Admin password	Known <input type="checkbox"/>
Server name: Server IP/ Hostname: Version: Admin login Admin password	Known <input type="checkbox"/>
Server name: Server IP/ Hostname: Version: Admin login Admin password	Known <input type="checkbox"/>
Server name: Server IP/ Hostname: Version: Admin login Admin password	Known <input type="checkbox"/>
Server name: Server IP/ Hostname: Version: Admin login Admin password	Known <input type="checkbox"/>

Register Customer and Predatar Agents on Predatar portal

Before the Predatar client can be downloaded and installed, Customer needs to be registered by PredPartner as an organisation on the Predatar portal together with all the Spectrum Protect servers that are to be monitored.

Once Customer has been registered on the Predatar portal, an email will be received from PredPartner or from the Predatar portal, which will contain the link to download the installer of the Predatar client software and the link to the download the license file required to install the Predatar client software.

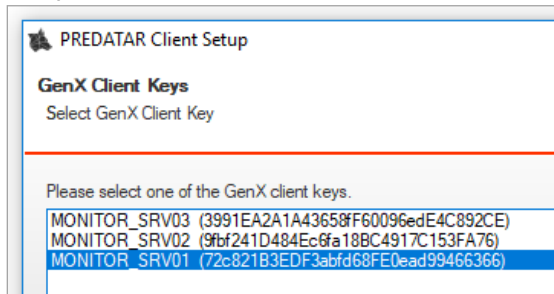
The Customer end user may need to check their Junk or Spam folders for an email from Predatar Outbound if they have not received the details in their inbox.

Download and install Predatar client software

Once the Predatar client software and the license file have been downloaded using the links received in the email, copy both the client installer (exe or zip) and license key file s to the host server(s) on the Customer's network on which the Predatar client software will be installed.

The Predatar client software can then be installed by following the steps listed below:

- i. Right click on the executable file and select 'Run as administrator' from the pop up menu.
- ii. The setup welcome screen will be shown.
- iii. Click 'Next' button .
- iv. Click 'I agree to the terms of this license agreement' and click 'Next' button.
- v. The installer will look for the license key file with the name 'license.lic' in the same location where Predatar client installer was run from. If the installer does not find the license file, then a notification will appear asking you to locate the license file. Press 'OK' button and locate the license file.
- vi. Select the Predatar client key for which you wish to install the Predatar client on this server and press 'Next' button.



- vii. Select the path where you want to install the Predatar clients and then press 'Next' button .
- viii. Optionally, the Predatar Client software can be configured to communicate with the Predatar Cloud via an internal Proxy Server. This configuration step is optional. Click on 'Next' to continue with the installation.
- ix. Specify proxy address, proxy port, proxy user name and proxy password , and click 'Next' button .
- x. Review the settings and click 'Next'.
- xi. The installer will install Predatar client software instance on the server .

- xii. Success message will be shown once the installation has completed. Click 'Finish' to close the setup.

Note: The installer also installs .NET Framework v4.6.2, and might ask for a server reboot after the installation has completed.

Run the Predatar Client

Once the Predatar client installer has finished successfully, a windows service named 'Predatar Client Service' is created on the server.

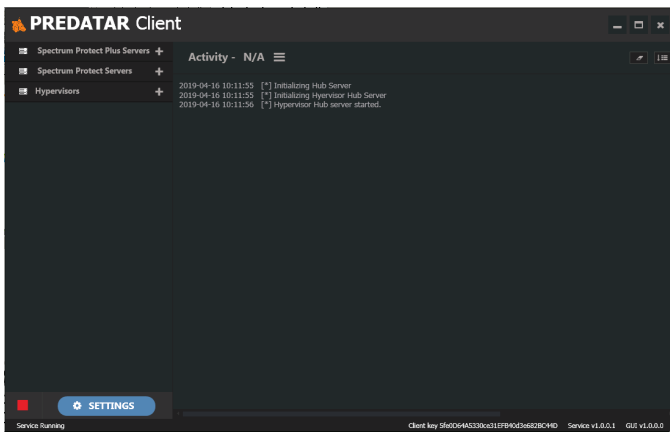
Predatar client windows service is a core component and it collects data from the SP server s.

Run Predatar Monitor

Predatar Client software also includes Predatar GUI component , which allows managing and controlling SP servers being monitored by the Predatar client instance from that server.

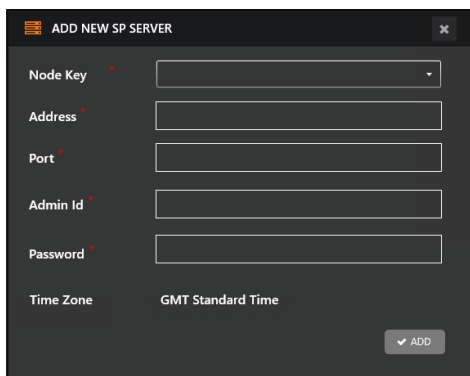
Predatar GUI can be opened by double clicking the 'PREDATARClient' icon on the desktop. It can also be opened from the Start menu and is located at the following path:

Programs → Predatar Ltd → PREDATAR Client → PREDATAR Client.



Adding SP servers for monitoring

On Predatar GUI, click on plus (+) icon next to “Spectrum Protect Servers” menu item.

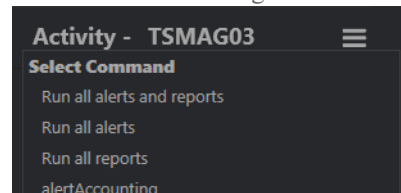


In the pop-up window select node key (SP server name) from the drop down list box, specify SP server host address, port, administrator id and password; and then click “Add”.

Run Data Collection from Predatar Monitor

The steps to run manual data collection using Predatar Monitor are listed below:

1. Open Predatar GUI.
2. Click on the hamburger icon



3. Select 'Run all alerts and reports'.
This will run data collection for all alerts and reports.

After a few minutes, data will start appearing on the portal under Analytics and Events.

Monitoring Predatar Client status

PredPartner can then monitor and confirm connectivity status of each Predatar client on the Predatar portal.

Successful monitoring may take 30 minutes or so to be apparent in the Partner Portal.

Troubleshooting

Symptom	Reason and Action
Email that contains the links to download the Predatar client installer and license file is not received.	It could be that the email has ended up in the spam/junk email folder. If there is no email in the spam/junk email folder either, please contact PredPartner .
Predatar GUIs showing orange error messages saying "Hub server was unable to start"	<p>This indicates that Predatar Client is unable to communicate with the Predatar cloud. Check if the URL to the Predatar cloud is not blocked by the firewall. Also, check if Internet connectivity is available .</p> <p>If local proxy is being used to connect to the Predatar cloud, make sure that proxy allows connection from that server to the cloud and the proxy user name and passwords are correct.</p>
<p>Predatar GUI is showing orange error messages that says one or more of the following:</p> <ul style="list-style-type: none"> • Error running console thread. • The system cannot find the file specified • Error running query thread 	<p>This could be because of the following reasons:</p> <ul style="list-style-type: none"> • The BA client is not installed on the host server. • The BA client is not installed with the Administrative Command Line. <p>Try to connect to any failing SP Servers directly from the dsmadmcmd command line on the Predatar Client host to prove independent connectivity.</p>
<p>Predatar GUI is showing red error messages that says one or more of the following:</p> <ul style="list-style-type: none"> • Session rejected: TCP/ IP connection failure. • Unable to establish session with server 	<p>This could be because the Predatar client is unable to connect to the SP server. There could be several possible reasons for that, some of which are listed below:</p> <ul style="list-style-type: none"> • The host address or the port specified to connect to the SP sever is incorrect. • The host server is unable to connect to the SP server due to a network problem or the connection to the SP server is blocked on the firewall. • There is some compatibility issue between the version of the BA client installed and the version of the SP server. <p>Try to connect to any failing SP Servers directly from the dsmadmcmd command line on the Predatar Client host to prove independent connectivity.</p>
Predatar client windows service is stopping every now and then.	It could be that the anti-virus software is preventing normal operation of the Predatar client software. It is recommended that the Predatar client installation folder should be added to the exclusion list of the anti-virus software.
Predatar client software is using a lot of CPU.	<p>Some of the possible reasons due to which it could happen are listed below:</p> <ol style="list-style-type: none"> 1. Administrative command line is not installed with the Spectrum Protect Backup-Archive client software. 2. The Spectrum Protect server is very busy and info messages are not disabled on the Spectrum Protect console. In this case make sure that the following commands have been run on the Spectrum Protect server:

- DISABLE EVENTS CONSOLE INFO NODENAMES=*
- DISABLE EVENTS CONSOLE INFO

Some reports under Analytics on the Predatar portal are not being populated with any data even though the connection between the Predatar client and Predatar cloud is ok.

This could be due to the following reasons:

- There does not exist any data in the Spectrum Protect server for that report
- The data collection for that report is disabled from the Predatar portal.
- If this is a recent installation the data may not have been populated yet, wait a while and look again

Security FAQs

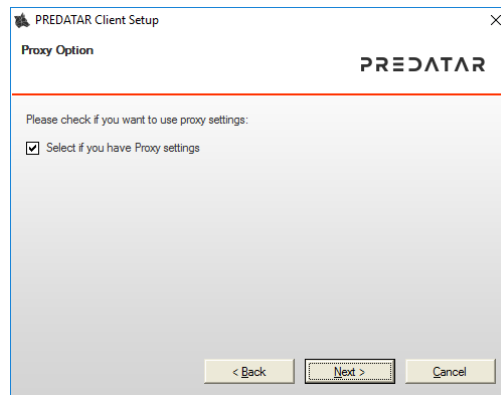
Some frequently asked security questions are discussed in this section.

On which port does the Predatar Client communicate to the Predatar cloud?

The Predatar client can connect to the Predatar cloud using HTTPS (default port 443), HTTPS (port 1753) or HTTP (port 80). However, it is not recommended to use unsecure HTTP channel for communication. Predatar Client machine must be able to access the Predatar cloud through the customer firewall. A single firewall rule may need to be setup to allow outbound connection to the Predatar cloud host address.

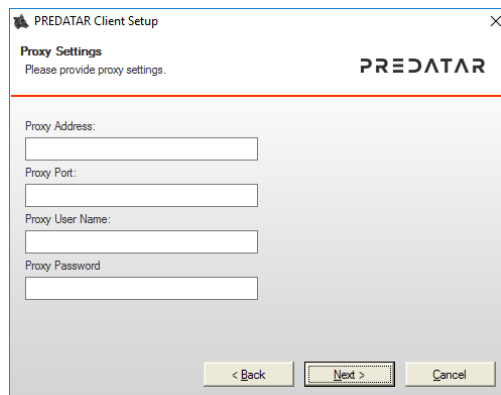
The customer does not want to open up ports on their firewall. How else can the Predatar client access the Predatar cloud?

When you install the Predatar client you have the option to authenticate with a local proxy server.



The screenshot shows the 'PREDATAR Client Setup' window with the 'Proxy Option' screen. The window title is 'PREDATAR Client Setup' and the logo 'PREDATAR' is in the top right. The text reads: 'Please check if you want to use proxy settings:'. There is a checked checkbox labeled 'Select if you have Proxy settings'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

You can enter the following parameters:



The screenshot shows the 'PREDATAR Client Setup' window with the 'Proxy Settings' screen. The window title is 'PREDATAR Client Setup' and the logo 'PREDATAR' is in the top right. The text reads: 'Please provide proxy settings.'. There are four input fields: 'Proxy Address:', 'Proxy Port:', 'Proxy User Name:', and 'Proxy Password'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Is there any communication from the Predatar cloud to the customer's Predatar client?

No. The customer's Predatar client initiates an outbound connection to the Predatar cloud in order to send data. It also periodically initiates an outbound connection to the Predatar cloud over HTTPS in order to receive message data.

For example, suppose a user of the Predatar portal modified a schedule for a Predatar alert or Predatar report then this places a message on the Predatar cloud outbound queue. When the customer's Predatar client connects to the Predatar cloud it pulls down this message and actions the information within it. At no point does the Predatar cloud push this information to the customer's Predatar client.

What data is collected from my Spectrum Protect server and sent to Predatar?

The Predatar client has two main threads connected to each Spectrum Protect server via dsmadm. The first thread uses the specified Spectrum Protect administrator account to periodically query a variety of Spectrum Protect database tables to gather client schedule, capacity and process type information. The second thread uses the same Spectrum Protect administrator account to collect activity log information in real-time. It does not collect “Informational” messages. It collects ANRxxxxE/ W/ D and ANExxxxW/ E messages.

Is this data encrypted before it is sent from the Predatar client to the Predatar cloud?

Yes. The Predatar client collects information from the Spectrum Protect servers. It stores this information in unencrypted format in a queue folder on the Predatar client. Another thread in the Predatar client is used to transfer data to the Predatar cloud. It does this by reading the data out of the queue folder and then transferring the data to the Predatar cloud over secure HTTPS channel which uses 2048 bit RSA encryption. The data is then stored in the Predatar database.

Whilst browsing the Predatar portal does it use HTTP or HTTPS?

Both HTTP (which uses port 80 by default) and HTTPS (which uses port 443 by default) can be used, however, port 80 is not recommended as it not secure.

Predatar also supports an additional port 1753 over HTTPS.

Contact us

Please contact support@predatar.com for any queries.