FortiNAC

Access Data For Custom Reports

Version 8.x

Date:

03/18/2019

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET KNOWLEDGE BASE
http://kb.fortinet.com

FORTINET BLOG
http://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
http://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTINET COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING AND CERTIFICATION PROGRAM
http://www.fortinet.com/support-and-trainingt/training.html

NSE INSTITUTE
http://training.fortinet.com

FORTIGUARD CENTER
http://fortiguard.com

FORTICAST
http://forticast.fortinet.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET

Monday March 18, 2019

Contents

Database Access

Note: REST API is the recommended method for accessing data outside of the Administration UI. For details, see topic FortiNAC REST API in Online Help or Administration and Operation document in the Fortinet Document Library.

You can run MySQL queries against the FortiNAC database to create custom reports. First, you must set up remote access to the database. Then, you will need to connect to the database and extract the appropriate data.

This document describes the scripts used to set up database access, and the database schema for submitting MySQL queries and some examples for setting up an SSH tunnel to the FortiNAC appliance. This document does not describe how to submit queries to the database and generate reports. It is assumed that you know how to create SQL queries and use the extracted data in a report.

Note: You may find DataVision a useful tool. It is an Open Source (free download) reporting tool similar to Crystal Reports that is compatible with MySQL.

Visit http://datavision.sourceforge.net/.

Database Access Requirements

To access the database you must meet the following requirements:

- Access to the FortiNAC appliance CLI
- MySQL
- Database Access scripts shown below must be installed in the /bsc/campusMgr/bin directory
  - CreateDBAccount - adds a remote database user
  - DeleteDBAccount - deletes a remote database user
- An SSH Tunnel must be established between your machine and the FortiNAC appliance.

Setup Database Access

1. Navigate to the command line on your FortiNAC Server or Control Server.
2. Log in as an Administrative user.
3. Navigate to the /bsc/campusMgr/bin directory.
4. This directory contains the CreateDBAccount script.
5. Edit the CreateDBAccount script and set the appropriate privileges for the account being created. Save any changes made to the script. A list of available privileges is contained within the script. By default the privileges are set to SELECT which provides Read-Only access.
6. Run the edited CreateDBAccount script and supply the required parameters. To run the script type the following:

   ```
   CreateDBAccount <username> <password> <serverip or %>
   ```

   Where:

   username is the username for the remote account

   password is the password for the remote account

   serverip is the IP address of the machine used to connect to the database. Using this parameter ensures that the user can connect with this username and password only from that machine. If you wish to allow the user to connect from any machine use % instead of the IP address.

   % is a wild card for the IP address of the machine used to connect to the database. This allows the user to connect with the created username and password from any machine.

   Example:

   CreateDBAccount reports abc123 %
7. The new database user name and password are now available for reports.

Configure SSH Tunnel

FortiNAC's MySQL database does not accept outside connections. To leverage the data in the database you must establish an SSH Tunnel, such that it appears that queries are coming from the FortiNAC appliance itself, and direct database queries to that tunnel. There are several methods for establishing an SSH Tunnel.
This section of the document provides two examples, however you may choose to use another method.

SSH Tunnel From A Linux Machine To FortiNAC

To connect to FortiNAC from a Linux machine in which the Linux machine is communicating via port 13306 and the FortiNAC appliance is listening on port 3306, you could do the following:

1. Navigate to the command line on the Linux machine.
2. At the command prompt type the following:

```
ssh -f -N -L 127.0.0.1:13306:127.0.0.1:3306
admin@<machinename or IP Address>
```

Where:

- 127.0.0.1 indicates to FortiNAC that the connection is internal
- 13306 is the port on the Linux machine
- 3306 is the port on the FortiNAC appliance
- admin is the CLI administrator account for the FortiNAC appliance
- <machinename or IP Address> enter the name of the FortiNAC appliance or its IP Address

Note: Using the command shown above, the SSH tunnel remains in place only until one of the machines is restarted. If either machine is restarted, you must set up the tunnel again.

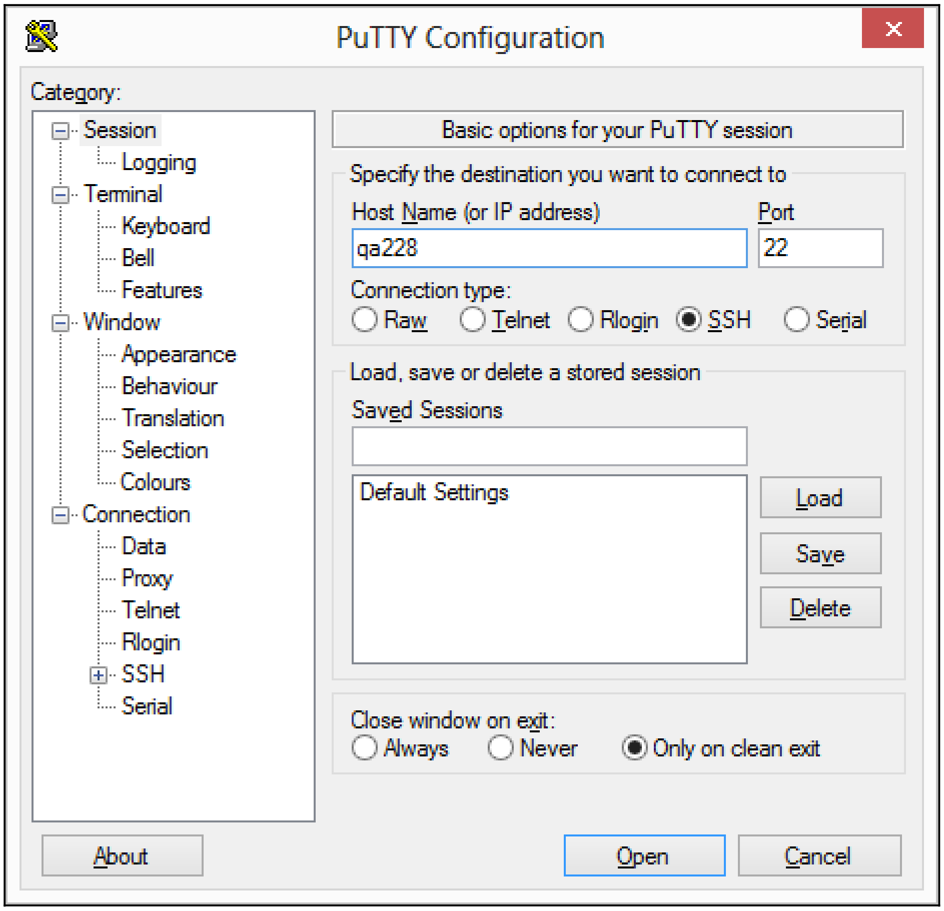
To verify that the tunnel is working,navigate to the command line on the Linux machine and type the following command:

```
mysql -u admin -h localhost --port 13306 -p  --protocol=tcp
```

SSH Tunnel From A Windows Machine To FortiNAC

To connect to FortiNAC from a Windows machine a separate tool is required. In this example, PuTTY is used. The Windows machine is communicating via port 13306 and the FortiNAC appliance is listening on port 3306.

1. Start the PuTTY application.
2. On the **Session** screen, enter the Host Name or IP Address of the FortiNAC Server or Control Server. In the example below, we are establishing a connection to qa228.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): qa228

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

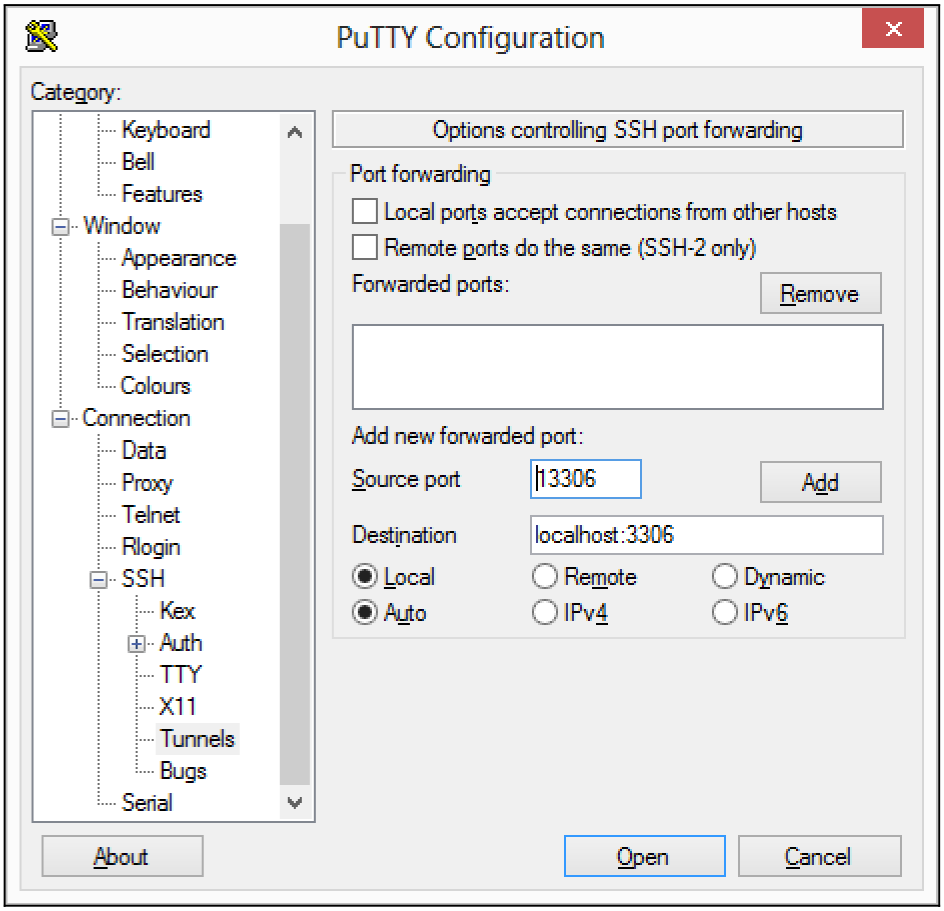
Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 1: PuTTY-Session

3. On the menu tree navigate to **Connection > SSH > Tunnels**.
4. In the **Add new forwarded ports** section, click in the **Source port** field and type 13306.
5. In the **Destination** field enter localhost:3306.
6. Click **Add** to display the information in the **Forwarded ports:** field.



Port forwarding

□ Local ports accept connections from other hosts

□ Remote ports do the same (SSH-2 only)

Forwarded ports:

Add new forwarded port:

Source port: 13306

Destination: localhost:3306

● Local ○ Remote ○ Dynamic

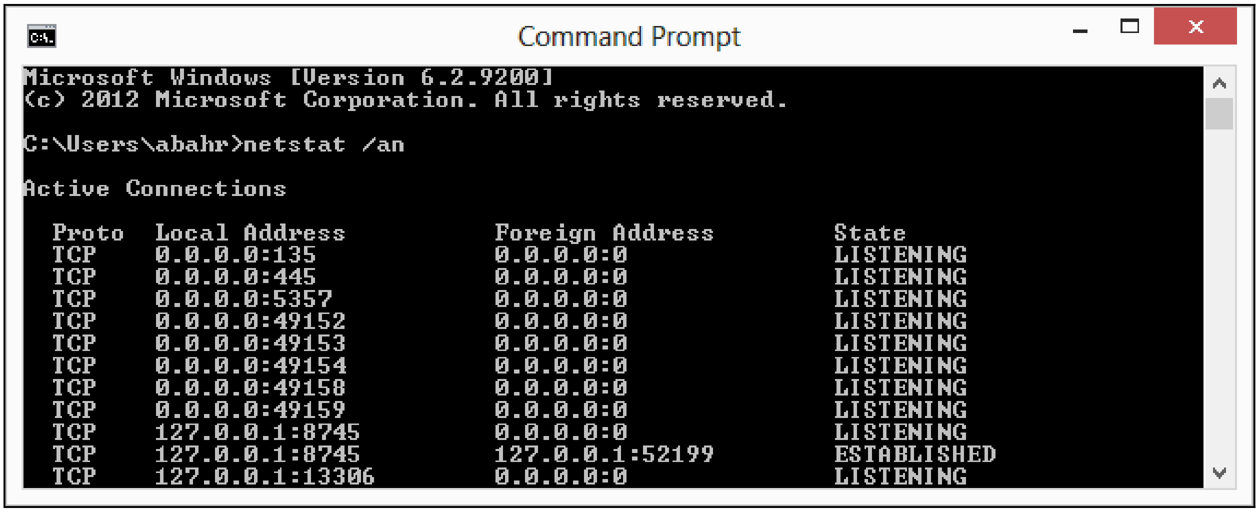
● Auto ○ IPv4 ○ IPv6

Figure 2: PuTTY-Tunnel

7. Click **Open** to establish the tunnel.
8. At the login prompt enter your FortiNAC admin credentials.
9. To verify that the tunnel is established navigate to a command prompt on your Windows machine. At the prompt type the following:

   ```
   netstat /an
   ```

   In the list that is returned, search for the line 127.0.0.1:13306. This indicates that PuTTY is forwarding port 13306 to the remote FortiNAC appliance.



```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\abahr>netstat /an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49158          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49159          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:8745         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:8745         127.0.0.1:52199        ESTABLISHED
  TCP    127.0.0.1:13306        0.0.0.0:0              LISTENING
```

Figure 3: Verify Tunnel

Note: The tunnel established by PuTTY remains in place only as long as both PuTTY and FortiNAC are running. Do not close PuTTY until you are done querying the database.

Database Schema

This section lists the database schema (i.e., tables) that could be relevant to the custom reports. Not every table in the database is included in this document. Database tables that are defined include:

Database Tables List

- AGENTMAC
- AGENTTEST
- AGENTTESTRESULT
- AGENTUPDATE
- ALARMS
- CONNECTIONLOG
- DYNAMIC
- EVENTS
- GUESTREPORT
- HOST RECORD
- POLICY
- POLICYTEST
- PORT
- PORTATTRS
- PORTCHANGES
- REGISTRATIONFAILURES
- REGISTRATIONS
- SCANNINGRESULTS
- SCANTEST
- SELFREGREQUEST
- USERRECORD

AGENTMAC Table

This table contains records for adapters on hosts that have the Persistent Agent installed.

Field	Type	Null	Key	Default	Description
id	int(11)	Unique ID	KEY	NULL	Unique ID for this adapter record.
landscape	double(20,0)			NULL	Unique identifier for records from this database. Used when aggregating records at the FortiNAC Control Manager level.
mac	varchar(255)		KEY	NULL	Physical address of the adapter on the host that has the Persistent Agent installed, such as, 00:1D:09:D6:00:10.
description	varchar(255)			NULL	Manufacturer's description of the adapter, such as, Intel(R) 82566DM Gigabit Network Connection.
version	double(20,0)			NULL	
ip	varchar(255)			NULL	IP address of the adapter as of its last connection to the network.

AGENTTEST Table

This table contains data pertaining to security scans done on hosts for Anti-Virus, Anti-Spywere, and Operating System requirements.

Field	Type	Null	Key	Default	Description
id	int(11)	Unique ID	KEY	NULL	ID associated with the scan performed. The same scan may appear multiple times in the table depending on how many times it has been run.
landscape	double(20,0)			NULL	Unique identifier for records from this database. Used when aggregating records at the FortiNAC Control Manager level.
status	int(11)		KEY	NULL	
category	varchar(255)			NULL	Category of scan done, such as: System Scan, Anti-Spyware, Anti-Virus or Operating System.
test	varchar(255)		KEY	NULL	Item for which the host was scanned, such as AVG 2011.
type	int(11)			NULL	
version	double(20,0)		KEY	NULL	

AGENTTESTRESULT Table

This table contains data pertaining to security scans done on hosts.

Field	Type	Null	Key	Default	Description
id	int(11)	NO	PRI		Unique ID for this record.
landscape	double(20,0)			NULL	Unique identifier for records from this database. Used when aggregating records at the FortiNAC Control Manager level.
status	int(11)			NULL	
userID	varchar(255)			NULL	Unique ID for the user associated with the specified host.
hostName	varchar(255)			NULL	Machine name of the host.
os	varchar(255)			NULL	Host operating system.
policy	varchar(255)			NULL	Policy used to scan the host.
time	double(20,0)			NULL	Time that the scan was run. Time is stored in UTC time (corresponds to Greenwich Mean Time), but the raw data is stored using a Unix convention. Date and time are represented as a Unix timestamp: the number of seconds elapsed since 1 January 1970 00:00:00 Greenwich Mean Time.
type	int(11)			NULL	
version	double(20,0)			NULL	
location	varchar(255)			NULL	Switch and port where the host or device was connected.

AGENTUPDATE Table

If you have enabled global agent updates for the Persistent Agent, this table keeps track of each host , the last known installed version of the Persistent Agent and the number of attempts that have been made to update that host. Based on the data in this table, FortiNAC determines whether or not to update a host's Persistent Agent version when the host connects to the network.

Field	Type	Null	Key	Default	Description
hostId	int(11)	NO	PRI		Unique ID for the host.
attempts	int(11)	NO			Number of attempts that have been made to update this host to the selected version of the Persistent Agent.
lastKnownVersion	varchar(255)			NULL	The last known version of the Persistent Agent installed on the host.

ALARMS Table

This table contains data for alarms triggered by events generated by FortiNAC. Only events that are enabled and have corresponding alarms mapped, will generate data for this table. Alarms and events are archived and purged from the database periodically.

Field	Type	Null	Key	Default	Description
id	int(11)	NO	PRI	NULL	Unique ID for this occurrence of this alarm.
name	varchar(255)	YES		NULL	Name of the alarm that was generated.
elementType	int(11)	YES		NULL	Number associated with the type of element that was identified within the record. See Managed Element Types on page 40 for a complete list of elements and corresponding numerical values.
elementID	int(11)	YES		NULL	Unique ID for the element described in the elementType field. For example, if the elementType is 13 or HelpDesk, this field would contain the user ID of the Help Desk user that triggered this alarm.
severity	int(11)	YES		NULL	Number representing the severity of the alarm. Levels of severity include: • CRITICAL = 1 • MINOR = 2 • WARNING = 3 • INFORMATIONAL=
time	double(20,0)	YES		NULL	Time the alarm occurred. Time is stored in UTC time (corresponds to Greenwich Mean Time), but the raw data is stored using a Unix convention. Date and time are represented as a Unix timestamp: the number of seconds elapsed since 1 January 1970 00:00:00 Greenwich Mean Time.

Field	Type	Null	Key	Default	Description
acknowledge	int(11)	YES		NULL	Indicates whether or not the alarm has been acknowledged by an administrator.
alarmObj	longblob	YES		NULL	
landscape	double(20,0)	YES		NULL	Unique identifier for records from this database. Used when aggregating records at the FortiNAC Control Manager level.
elementName	varchar (255)	YES		NULL	User specified name of the device, such as Lab Controller or Accounting Printer.

CONNECTIONLOG Table

Contains connection history for host connections to the network.

Field	Type	Null	Key	Default	Description
connectionTime	timestamp	NO	MUL	CURRENT_ TIMESTAMP	Time that the host connected to the network.
disconnectTime	timestamp	NO		0000-00-00 00:00:0	Time that the host disconnected from the network.
userID	varchar(255)	NO	MUL		Unique ID of the user associated with the host that connected to the network.
ip	varchar(24)	YES	MUL	NULL	IP address of the host for this connection.
mac	char(17)	YES		NULL	Physical address of the host.
location	varchar(254)	YES	MUL	NULL	Switch and port where the host connected.
bytesIn	int(10) unsigned	NO		NULL	Total number of bytes in for the connection.
bytesOut	int(10) unsigned	NO		NULL	Total number of bytes out for the connection.
loadIn	float	NO		NULL	Average load in for the connection.
loadOut	float	NO		NULL	Average load out for the connection.
peakLoadIn	float	NO		NULL	Average peak load in for the connection.
peakLoadOut	float	NO		NULL	Average peak load out for the connection.

DYNAMIC Table

This table contains data for hosts and devices that display in the Host View.

Field	Type	Null	Key	Default	Description
id	int(11)	Unique ID	PRI		Unique ID for this host record.
type	int(11)			NULL	Number associated with the type of device that was identified within the record. SeeDevice Types on page 1 for a complete list of devices and corresponding numerical values.
ident	varchar(255)		KEY	NULL	User name of the user associated with this host or device.
pcType	varchar(255)			NULL	Contains information about the manufacturer of the adapter, such as, Intel(R) 82566DM Gigabit Network Connection. May also contain user specified information.
mediumType	varchar(255)			NULL	Indicates whether the adapter is wireless or wired for this host.
parent	varchar(255)			NULL	
ip	varchar(255)		KEY	NULL	IP address of the adapter as of its last connection to the network.
physAddr	varchar(255)		KEY	NULL	Physical address of the adapter on the host.
location	varchar(255)			NULL	
status	int(11)			NULL	Indicates whether the adapter is enabled or disabled. • N/A=0 • Online Enabled=1 • Offline Disabled=2 • Online Disabled=3
client	longblob				

Field	Type	Null	Key	Default	Description
creationTime	double(20,0)			NULL	Time that this record was created. Time is stored in UTC time (corresponds to Greenwich Mean Time), but the raw data is stored using a Unix convention. Date and time are represented as a Unix timestamp: the number of seconds elapsed since 1 January 1970 00:00:00 Greenwich Mean Time.
validForTime	double(20,0)			NULL	Amount of time that this record will remain in the database from the date of creation.
offlineTime	double(20,0)			NULL	If the host is offline for this amount of time, this record is deleted from the database.
landscape	double(20,0)			NULL	Unique identifier for records from this database. Used when aggregating records at the FortiNAC Control Manager level.
lastSuccessfulPoll	double(20,0)			NULL	Date and time of the last communication with the Host.
hostID	int(11)		KEY	NULL	Unique ID for this host.
accessValue	varchar(255)			NULL	Security and Access Value — Value that typically comes from a field in the directory, but can be added manually. This value groups users and can be used to determine which role to apply to a user or which policy to use when scanning a user's computer. The data in this field could be a department name, a type of user, a graduation class, a location or anything that distinguishes a group of users. The access value is inherited from the user associated with this host.

EVENTS Table

This table contains a list of events that have been generated and have not yet been archived and purged from the database.

Field	Type	Null	Key	Default	Description
id	int(11)	NO	PRI	NULL	Unique ID for this occurrence of this event.
name	varchar(255)	YES		NULL	Name of the event that was generated.
elementType	int(11)	YES		NULL	Number associated with the type of element that was identified within the record. See Managed Element Types on page 40 for a complete list of elements and corresponding numerical values.
elementID	int(11)	YES		NULL	Unique ID for the element described in the elementType field. For example, if the elementType is 13 or HelpDesk, this field would contain the user ID of the Help Desk user that triggered this alarm.
time	double(20,0)	YES	MUL	NULL	Time the event occurred. Time is stored in UTC time (corresponds to Greenwich Mean Time), but the raw data is stored using a Unix convention. Date and time are represented as a Unix timestamp: the number of seconds elapsed since 1 January 1970 00:00:00 Greenwich Mean Time.
event	longblob	YES		NULL	
landscape	double(20,0)	YES		NULL	Unique identifier for records from this database. Used when aggregating records at the FortiNAC Control Manager level.
elementName	varchar(255)	YES		NULL	User specified name of the device, such as Lab Controller or Accounting Printer.

GUESTREPORT Table

This table contains data associated with guest creation and registration.

Field	Type	Null	Key	Default	Description
guestID	int(11)	NO	PRI	NULL	Unique ID for this guest.
startTime	timestamp	NO	MUL	CURRENT_ TIMESTAMP	Date and time that this guest account was created.
endTime	timestamp	NO	MUL	0000-00-00 00:00:00	Date and time that this guest account will be removed from the database.
userID	varchar(32)	NO	MUL		Guest's user name.
sponsor	varchar(32)	YES		NULL	Admin user that created this guest record.
role	varchar(32)	YES		NULL	Guest's role. Used for role/location based access.
policy	varchar(32)	YES		NULL	Security policy used to scan this guest's computer.
regType	int(11)	YES		NULL	Type of authentication used to authenticate this guest when he logs onto the network. • Local=0 • LDAP=1 • RADIUS=2
startTimeOfDay	int(11)	YES		NULL	If this guest is not permitted to access the networks at all times, this field contains the number of minutes from midnight to the access start time. For example, if this fields contains 480, this indicates that the guest cannot access the network until 480 minutes or 8 hours after midnight.
endTimeOfDay	int(11)	YES		NULL	If this guest is not permitted to access the networks at all times, this field contains the number of minutes from midnight to the access end time. For example, if this fields contains 1439, this indicates that network access will end when 1439 minutes have elapsed since midnight, regardless of when the start time permitted access.

Field	Type	Null	Key	Default	Description
daysOfWeek	int(11)	YES		NULL	If this guest is not permitted to access the networks at all times, this field contains the days of the week during which the guest can access the network.
registrationCount	int(11)	YES		NULL	Number of hosts that can be registered to this guest. The default is 1.

HOSTRECORD Table

This database table contains a list of all hosts or devices that are registered in the Host View that have not aged out of the database.

Field	Type	Null	Key	Default	Description
id	int(11)	Unique ID	PRI		Unique ID for this host.
landscape	double(20,0)			NULL	Unique identifier for records from this database. Used when aggregating records at the FortiNAC Control Manager level.
hostName	varchar(255)		KEY	NULL	Name of the host machine.
owner	varchar(255)		KEY	NULL	Last name of the user that registered this host.
os	varchar(255)			NULL	Operating system of the host machine.
policy	varchar(255)			NULL	Security policy used to scan this host.
hardwareType	varchar(255)			NULL	Type of machine such as workstation.
applications	text			NULL	List of applications installed on the device. This information is provided by the agent. Typically includes Anti-spyware, Anti-virus, Hotfixes and operating system. This information is updated with each successful scan.
creationTime	double(20,0)			NULL	Time that this record was created. Time is stored in UTC time (corresponds to Greenwich Mean Time), but the raw data is stored using a Unix convention. Date and time are represented as a Unix timestamp: the number of seconds elapsed since 1 January 1970 00:00:00 Greenwich Mean Time.
validForTime	double(20,0)			NULL	Amount of time that this record will remain in the database from the date of creation.

Field	Type	Null	Key	Default	Description
status	int(11)			NULL	Indicates whether the host is enabled or disabled. ***Numbers seem to vary widely instead of just being a 1 or a 0. For example on a printer I have 1 for enabled and 3 for disabled, but on a registered host I have 513 for enabled and 515 for disabled. Need more info on this field.
host	longblob				
type	int(11)			NULL	Number associated with the type of device that was identified within the record. SeeDevice Typefor a complete list of devices and corresponding numerical values.
directoryPolicyValue	varchar(255)			NULL	If this host was scanned using Passive Agent Registration, this field contains the policy assigned by the Passive Agent Configuration.
patchManagementID	varchar(255)			NULL	ID number of the most recent patch applied by a patch management server such as BigFix or PatchLink.
patchManagementVendor	varchar(255)			NULL	Vendor name of the patch management server.
serialNumber	varchar(255)			NULL	Serial number of the host.
role	varchar(255)			NULL	Role assigned to this host.
agentVersion	varchar(32)			NULL	Version number of the last agent installed on this host.
agentID	varchar(100)			NULL	ID of the agent.
agentPlatform	varchar(255)			NULL	Indicates the type of agent used, such as Windows or Mac Persistent Agent.
offlineTime	double(20,0)			NULL	The amount of time that has elapsed since the hosts last connection to the network. Used in conjunction with the offlineAgeTime field to determine when to age the host out of the database.

Field	Type	Null	Key	Default	Description
notes	text				Admin notes about host. If this is a guest record, notes may contain guest information entered into Admin specified data fields required during guest registration.
lastSuccessfulPoll	double(20,0)			NULL	Date and time of the last communication with the Host.
reValidation	tinyint(1)	NO		0	Indicates whether or not Device Profiler should confirm that this host continues to match the Device Profiler rule used to classify it the next time the host connects to the network. Only applies to hosts or devices processed by Device Profiler.
reValidationInterval	int(11)			NULL	If enabled, Device Profiler confirms at set intervals that this host still matches the rule used to classify it. Interval options include Minutes, Hours, or Days.
lastReValidation	double(20,0)			NULL	Date and time of the last confirmation that this host matches the Device Profiler rule used to classify it. This is used to determine when the confirmation interval elapsed.
reValidationAction	longblob				If enabled, Device Profiler disables previously profiled devices or hosts that no longer match their associated rule.
imageType	varchar(255)			NULL	Controls the icon displayed for this host record. For example, this field might contain the word Mobile or Printer.
loggedOnUserId	varchar(255)			NULL	User ID of the network user logged onto this machine. This may or may not be the same as the owner. In an environment where machines are shared, such as a lab, the owner may be set to the hostname.

Field	Type	Null	Key	Default	Description
domainId	int(11)			NULL	If this is a device that is registered both in the Host View and the Topology View, this field has the ID number of the domain in Topology View that contains this device. Domains are containers in Topology used to group devices.
offlineAgeTime	double(20,0)			NULL	Amount of time that the host must be offline before the host is aged out of the database. For example, if the host does not connect for a month, it should be removed from the database. The user would then have to re-register the host to reconnect to the network. This field is used in conjunction with the offlineTime field, which contains the running count of offline time.
agentSN	varchar(100)			NULL	
agentTag	varchar(100)			NULL	
managedByMDM	tinyint(1)	NO		0	
mdmCompromised	tinyint(1)	NO		0	
mdmCompliance	tinyint(1)	NO		0	
mdmDataProtection	tinyint(1)	NO		0	
mdmPasscodePresent	tinyint(1)	NO		0	

POLICY Table

This table contains scans configured in FortiNAC. Agents scan hosts using scans to determine the requirements for hosts to connect to the network. In Version 5.3 Policies and Scans were separated. Policies map scans to hosts. Scans are the rules by which hosts must abide in order to be allowed on the network. See the ProfileMapping tables for data associated with Policies.

Field	Type	Null	Key	Default	Description
policyID	int(11)	NO	PRI		Unique ID for this scan.
name	varchar(100)	NO	KEY		User specified name for this scan.
createTime	timestamp	NO		CURRENT_ TIMESTAMP	Date and time that this record was created in the database. A date and time of 1980-11-01 00:01:00 indicates that this scan has been deleted. However, it must remain in the database for reporting purposes.
modTime	timestamp	NO		0000-00-00 00:00:00	Date and time that this record was last modified.
dirValue	varchar(100)			NULL	This field is no longer used.
groupName	char(100)			NULL	Group of users to which this scan will be applied. Used only for System Scans. These are groups that are stored in the Groups View.
defaultReg	varchar(5)	NO		false	This field is no longer used.
defaultRem	varchar(5)	NO		false	This field is no longer used.
defaultAgent	varchar(5)	NO		false	This field is no longer used.
globalDefault	varchar(5)	NO		false	This field is no longer used.

POLICYTEST Table

This table contains individual requirements that are part of a security scan for which the agent tests when it scans a host. For example, on a Windows host, a scan might contain tests for Windows Vista, Windows XP and Windows Server - 2008. Each of theses tests is contained within an individual record in this database table along with the ID of the scan that contains the test.

Field	Type	Null	Key	Default	Description
testID	int(11)	NO	PRI		Unique ID for this test.
policyID	int(11)	NO	KEY		ID for the scan that contains this test. Corresponds to the policyID field in the POLICY table.
os	varchar(100)	NO			Operating system of the host that determines which tests can be run on it. For example, if the host is running a Windows operating system, you would not test for MAC-OS X 10.5 Leopard.
productType	varchar(100)	NO			Type of product for which the test is being run, such as, Operating System, Anti-Virus or Anti-Spyware.
productName	varchar(100)	NO			Name of the product for which the test is being run, such as Norton or Spyware Blaster.

PORT Table

The entries in the table represent physical ports read from the the L2 network devices.

Field	Type	Null	Key	Default	Description
ID	bigint(20)	NO	PRI	auto_increment	Unique database ID for the port.
legacyDBID	bigint(20)			NULL	ID of the port entry from the legacy port database table.
name	varchar(255)		KEY	NULL	Name of the port.
portID	varchar(255)			NULL	The port ID.
displayName	varchar(255)			NULL	The name shown in the GUI.
ifOperStatus	bigint(20)			NULL	The operational status of the read from the device.
ifAdminStatus	bigint(20)			NULL	The admin status of the port read from the device.
portType	bigint(20)			NULL	The type of port, uplink, or access. The port type maps to the ifType defined by the Internet Assigned Numbers Authority(IANA) and descriptions can be found in the ianaiftype-mib : https://www.iana.org/assignments/ianaiftype-mib/ianaiftype-mib
deviceName	varchar(255)		KEY	NULL	The name of the device where this port exists.
deviceID	bigint(20)		KEY	NULL	The database ID of the device.
status	bigint(20)			NULL	The status of the port. 0=good online 1=disabled 2=security risk These values are bit values and can be combined (e.g., a status of 3 = disable and security risk).
domainID	bigint(20)		KEY	NULL	The database ID of the container where this port exists.
ip	varchar(255)			NULL	The IP address of the port.
physAddr	varchar(255)			NULL	The MAC address of the port.
label	varchar(255)			NULL	The label for the port.

Field	Type	Null	Key	Default	Description
ifName	varchar(255)			NULL	The ifName read from the device.
ifDescr	varchar(255)			NULL	The ifDescr read from the device.
ifSpeed	varchar(255)			NULL	The ifSpeed read from the device.
ifIndex	varchar(255)			NULL	The ifIndex read from the device.
connectionState	bigint(20)			NULL	The current state of the connection. See connectionState Mappings below
defaultVlan	varchar(255)			NULL	The default VLAN used when no other value is used.
currentVlan	varchar(255)			NULL	The VLAN the port is currently in.
currentCli	varchar(255)			NULL	The CLI command currently applied to the port.
notes	text				User-defined notes.

connectionState Mappings

Connection State	Mapping	Description
0	NO_CONNECTION	Nothing currently connected.
1	REGISTERED	Registered Host connected.
2	ROGUE	Rogue Host Connected.
3	MULTY_CLIENT	Multiple Hosts (rogue or registered) connected.
4	UPLINK	Uplink - Determined automatically because we’ve seen this port connected to a known network device.
5	DISABLED_ REGISTERED	Disabled Registered Host Connected.
6	DISABLED_ROGUE	Disabled Rogue Host connected
7	USER_DEFINED_ UPLINK	User Defined Uplink
8	DEVICE	Registered Device connected
9	DIRECTORY_USER	Directory User Connected
10	DISABLED_ DIRECTORY_USER	Disabled Directory User Connected
11	ROGUE_SECURITY_ RISK	At Risk Rogue Host Connected
12	REG_SECURITY_RISK	At Risk Registed Host Connected

Connection State	Mapping	Description
13	IP_PHONE	IP Phone Connected
14	DISABLED_IP_PHONE	Disabled IP Phone Connected
15	ROGUE_NOT_ AUTHENTICATED	Unauthenticated Rogue Host Connected
16	REG_NOT_ AUTHENTICATED	Unauthenticated Registered Host connected.
17	THRESHOLD_UPLINK	Uplink state automatically triggered by passing a threshold of hosts connected to a port.
18	PORT_AGGREGATE_ ULINK	Uplink set when an aggregate port is detected.
19	LWAP_UPLINK	Uplink set when a Wireless Access point is detected connect to a port.

PORTATTRS Table

The PortAttrs contains additional port data.

Field	Type	Null	Key	Default	Description
id	bigint(20	NO	PRI		The database ID of the port
name	varchar(255)	NO	PRI		The name of the attribute.
value	varchar(255)	NO			The string value of the attribute.

PORTCHANGES Table

This table contains historical records of port changes such as VLAN changes or changes triggered by a CLI Configuration. This data is displayed in the UI on the Port Changes View.

Field	Type	Null	Key	Default	Description
id	int(11)	NO	PRI		Unique ID for this port change.
time	timestamp	NO		CURRENT_TIMESTAMP	Date and time that the port change occurred. Time is displayed in military time.
portID	int(11)		KEY	NULL	ID of the port experiencing the change.
status	int(11)			NULL	Indicates whether the port was enabled or disabled.
vlan	varchar(32)			NULL	VLAN where the port was placed.
cli	text				Text of the CLI configuration applied to this port.
cliName	varchar(254)			NULL	Name of the CLI configuration applied to this port
role	varchar(255)			NULL	Role the port was in when this change took place.

REGISTRATIONFAILURES Table

This table contains data detailing failed host or device registrations.

Field	Type	Null	Key	Default	Description
time	timestamp	NO	MUL	CURRENT_ TIMESTAMP	Date and time of registration attempt.
userID	varchar(255)	NO	MUL		Users's unique ID.
ip	varchar(24)	YES		NULL	IP address of the host or device for this connection.
mac	char(17)	YES		NULL	Physical address of the host or device, such as 00:19:D1:94:5C:06.
os	varchar(100)	YES	MUL	NULL	Operating system of the host machine.
failureCode	smalint(5) unsigned	NO	MUL	NULL	Reason for the failure.
description	varchar(254)	NO			Description of the failure, such as, Authentication Failure or Physical Address Already Registered.

REGISTRATIONS Table

This table contains data associated with host registrations.

Field	Type	Null	Key	Default	Description
time	timestamp	NO	MUL	CURRENT_ TIMESTAMP	Time of registration.
firstName	varchar(255)	YES		NULL	First name of the user that registered this host.
lastName	varchar(255)	YES		NULL	Last name of the user that registered this host.
userID	varchar(255)	NO	MUL		Users's unique ID.
title	varchar(32)	YES		NULL	User's title (freshmen, faculty, staff).
email	varchar(254)	YES		NULL	User's email address.
phone	varchar(32)	YES		NULL	User's phone number.
address	varchar(254)	YES		NULL	User's street address.
city	varchar(100)	YES		NULL	City name.
state	varchar(2)	YES		NULL	State abbreviation.
zip	varchar(10)	YES		NULL	Zip or postal code.
location	varchar(254)	YES	MUL	NULL	Port and switch to which the host connected.
ip	varchar(24)	YES		NULL	IP address of the host for this connection.
mac	char(17)	YES		NULL	Physical address of the host, such as 00:19:D1:94:5C:06.
hostName	varchar(32)	YES		NULL	Name of the host machine.
hostType	varchar(128)	YES		NULL	Type of host machine.
os	varchar(100)	YES	MUL	NULL	Operating system of the host machine.
sponsor	varchar(32)	YES		NULL	Sponsor account.
guestID	int(11)	NO	MUL	NULL	Guest ID
notes	varchar(255)	YES		NULL	Admin notes about host. If this is a guest record, notes may contain guest information entered into Admin specified data fields required during guest registration.

SCANNINGRESULTS Table

This table contains a detailed list of scans that have been performed on specific hosts and indicates the status of the scan.

Field	Type	Null	Key	Default	Description
scanID	int(11)	NO	PRI	NULL	Unique ID for this scan occurrence.
type	smallint(6)	NO	MUL	NULL	Indicates the type of scan performed, such as, Agent Scan or Admin Scan.
time	timestamp	NO		CURRENT_ TIMESTAMP	Date and time the host was scanned.
policyName	varchar(100)	NO			Name of the security scan used to scan the host.
policyID	int(11)	NO	MUL		ID of the security scan used to scan the host. Corrresponds to the policyID field in the POLICY table.
status	smallint(6)	NO	MUL		Scan status includes • Success=1 • Failure=2 • Not Scanned=3
userID	varchar(32)	NO	MUL		ID of the user associated with this host.
ip	varchar(24)	YES		NULL	IP address of the scanned host.
mac	char(17)	YES		NULL	MAC address of the scanned host.
os	varchar(100)	YES		NULL	Operating System of the scanned host.
location	varchar(254)	YES		NULL	Switch and port to which the host connected.
hostName	varchar(100)	YES		NULL	Machine name of the host.

SCANTEST Table

This table contains a list of tests that were run within scans in the SCANRESULTS table.

Field	Type	Null	Key	Default	Description
scanID	int(11)	NO	MUL	NULL	Unique ID for this scan occurrence.
productType	varchar(100)	NO			Type of product for which the test is being run, such as, Operating System, Anti-Virus or Anti-Spyware.
productName	varchar(100)	NO			Name of the product for which the test is being run, such as Norton or Spyware Blaster.
status	smallint(6)	NO		NULL	The status code: Passed=1 Failed=2 Script Failure=3

SelfRegRequest Table

This table contains guest self-registration requests.

Field	Type	Null	Key	Default	Description
ID	bigint(20)	NO	PRI	auto_ increment	Unique ID for this request record.
createDate	timestamp	NO		CURRENT_ TIMESTAMP	Date and time this record was created.
expireDate	timestamp NULL			NULL	Date and time this request expires.
responseDate	timestamp NULL			NULL	Date and time the sponsor responded to the request.
sponsor	varchar(255)			NULL	Sponsor to whom the self-registration request was sent.
ip	varchar(20)			NULL	IP address of the host requesting guest access.
location	varchar(255)			NULL	Connection location of the host requesting guest access, such as switch and port information.
state	varchar(255)	NO			State of the request, options include: **Expired**—The request has expired because there has been no response to the request for 20 minutes. **Accepted**—The request has been accepted by a sponsor, a guest account has been created and network access has been granted. **Denied**—The request has been denied by a sponsor and the guest does not have network access.
message	varchar(255)			NULL	Message sent by the sponsor to the guest requesting guest access.
UserID	varchar(255)			NULL	Email address entered by the guest when requesting guest access.
guestDBID	bigint(20)			NULL	Email address entered by the guest when requesting guest access.

Field	Type	Null	Key	Default	Description
requestKey	varchar(25)			NULL	Email address entered by the guest when requesting guest access.
guestdata	text	NO			Data requested from the guest when they submit a self registration record.
portalName	varchar(255)			NULL	

USERRECORD Table

This table contains user data for network users, guest users and admin users.

Field	Type	Null	Key	Default	Description
id	int(11)	NO	PRI		Unique ID for this user.
landscape	double(20,0)			NULL	Unique identifier for records from this database. Used when aggregating records at the FortiNAC Control Manager level.
firstName	varchar(255)			NULL	User's first name.
lastName	varchar(255)			NULL	User's last name.
userID	varchar(255)		KEY	NULL	User's unique user name.
dn	varchar(512)			NULL	If the user authenticates through a directory, this field contains directory attributes. If the user authenticates locally this field contains the User Name.
position	varchar(255)			NULL	The position of the user; for example, Professor, or Administration. Or, the grade of the student; for example, year of graduation.
email	varchar(255)			NULL	User's email address.
address	varchar(255)			NULL	User's street address.
city	varchar(255)			NULL	City name.
mailState	varchar(255)			NULL	State abbreviation.
zipCode	varchar(255)			NULL	Zip or postal code.
phone	varchar(255)			NULL	User's phone number.
role	varchar(255)			NULL	User's role. Used for role/location based access.

Field	Type	Null	Key	Default	Description
creationTime	double(20,0)			NULL	Date and time this record was created. Time is stored in UTC time (corresponds to Greenwich Mean Time), but the raw data is stored using a Unix convention. Date and time are represented as a Unix timestamp: the number of seconds elapsed since 1 January 1970 00:00:00 Greenwich Mean Time.
validForTime	double(20,0)			NULL	Date and time this record will be removed from the database.
status	int(11)			NULL	
user	longblob				
password	varchar(100)			NULL	User's password. This field is encrypted.
language	varchar(32)			NULL	Language setting for the user. Defaut=en
country	varchar(32)			NULL	User's country. Field is not available through the UI. Default = US.
notes	text			NULL	Notes pertaining to this user's record.
directoryPolicyValue	varchar(255)			NULL	Security policy used to scan this user's computer.
type	int(11)			NULL	Number associated with the type of user that was identified within the record. See Managed Element Types on page 40 for a complete list of elements and corresponding numerical values.
adminProfileID	int(11)			NULL	ID of the User Profile associated with an administrative user. Profile controls permissions for Guest Manager and Device Profiler.
guestId	int(11)			0	If this user is a guest, this is the guest's unique ID number in the id field in the GUEST table.

Field	Type	Null	Key	Default	Description
mobileNumber	varchar(255)			NULL	Mobile Phone number used for sending SMS messages to guests and administrators.
mobileProvider	varchar(255)			NULL	Mobile provider for the mobile phone number entered in the previous field. Used to send SMS messages to guests and administrators. This field also displays the format of the SMS address that will be used to send the message. For example, if the provider is US Cellular, the format is xxxxxxxxxx@email.uscc.net, where the x's represent the user's mobile phone number. The number is followed by the email domain of the provider's message server.
ncmPropagateHosts	tinyint(4)			NULL	Indicates that the records for hosts owned by this user should be copied to all managed FortiNAC appliances. This field is only used if the FortiNAC server is managed by a FortiNAC Control Manager.
inactivityTime	double(20,0)			NULL	
inactivityAgeTime	double(20,0)			NULL	
lastActivityTime	double(20,0)			NULL	

Managed Element Types

Number associated with the type of element that was identified within the database record. Possible elements and corresponding numbers include:

- CONTAINER = 0
- DEVICE = 1
- PORT = 2
- SUB_COMPONENT = 3
- DOMAIN = 4
- PRINCIPAL_CONTROLLER = 5
- LOADER = 6
- FortiNAC SERVER= 7
- DYNAMIC_MANAGED_CLIENT = 8
- ROGUE_DYNAMIC_MANAGED_CLIENT = 9
- ADMINISTRATOR = 10
- MANAGED GROUP = 11
- CUSTOMER_DOMAIN = 12
- HELPDESK = 13
- OPERATOR = 14
- DIRECTORY = 15
- PLUGINS = 16
- PROCESSES = 17
- CONfIGMGNT = 18
- PACKETSHAPER = 19
- DHCP = 20
- BANDWIDTH = 21
- ROGUEDEVICE = 22
- AUTHENTICATION = 23
- DYNAMIC_MANAGED_USER = 24
- SECURITY = 25
- REMEDIATION = 26
- REGISTRATION = 27
- IP_PHONE = 28
- NON_REG_DYNAMIC_MANAGED_CLIENT = 29
- SCAN_ENGINES = 30
- BSI_SCAN_ENGINE = 31
- NESSUS_SCAN_ENGINE = 32
- HUB_NET_REG = 33
- SECURITY_AGENT_APPLICATION = 34
- NETWORK_CONTROL_MANAGER = 35
- NETWORK_CONTROL_SERVER = 36
- ETHER_CONTAINER = 37
- ETHER_CARD = 38
- DIRECTORY_CONTAINER = 39
- VPN_USER = 40
- SECONDARY_NETWORK_CONTROL_SERVER = 41
- VIRTUAL_COMPONENT = 42
- PATCH_MANAGEMENT_CONTAINER = 43
- BIGFIX = 44
- PATCHLINK = 45
- ADMINISTRATIVE = 46
- DEVICE_PROFILING = 47
- GUEST = 48
- PORTAL = 49
- TOPO_CLIENT = 50
- USER_RECORD = 51
- HOST_RECORD = 52

Sample Third Party Report Integration

Running Reports with DataVision.

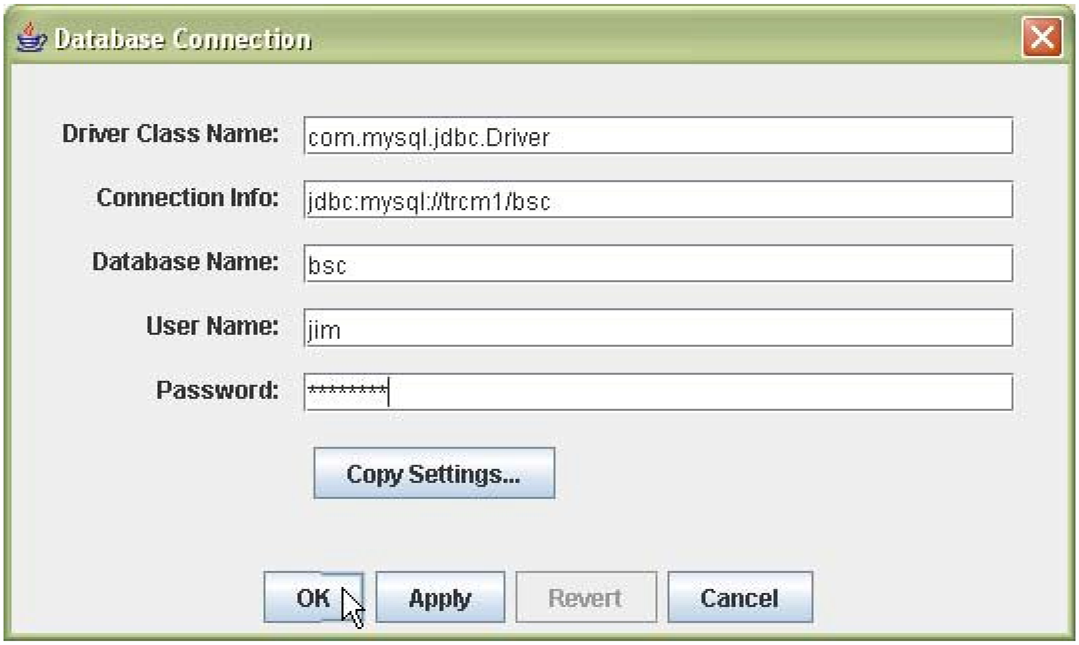
1. Using this document, create a mysql user account.
2. Download the jdbc driver from the FortiNAC appliance (/bsc/buildtools/java/mm.mysql-2.0.8), or find it on the web.
3. Download and untar DataVision from http://datavision.sourceforge.net/ (the download link is listed on the left-hand side of the home page).
4. Edit the datavision.bat file (for windows), or datavision.sh file (Linux) and include your jdbc driver path in the CLASSPATH, and then save the file. In the following example, both the current jdbc driver (bolded) and an older one (mm.mysql-2.0.8-bin) has been added to the CLASSPATH. Each of these drivers were placed in the DataVision directory for simplicity in the path statement.

   ```
   set

   CLASSPATH=%CLASSPATH%;lib\DataVision.jar;lib\jcalendar.jar;l
   ib
   \jruby.jar;lib\iText.jar;lib\bsf.jar;mm.mysql-
   2.0.8\mm.mysql-2.0.8-bin.jar;
   mysql-connector-java-3.1.14\mysql-connector-java-3.1.14-
   bin.jar

   java -classpath %CLASSPATH% jimm.datavision.DataVision %1  %2
   %3 %4 %5 %6 %7 %8 %9
   ```

5. Run the .bat (Windows), or .sh (Linux) file.
6. Select Start a New Report from the DataVision welcome screen.
7. Enter the Database Connection information. (The Driver Class Name and Connection info formats can be found in the jdbc driver's ReadMe file.)



Driver Class Name: com.mysql.jdbc.Driver

Connection Info: jdbc:mysql://trcm1/bsc

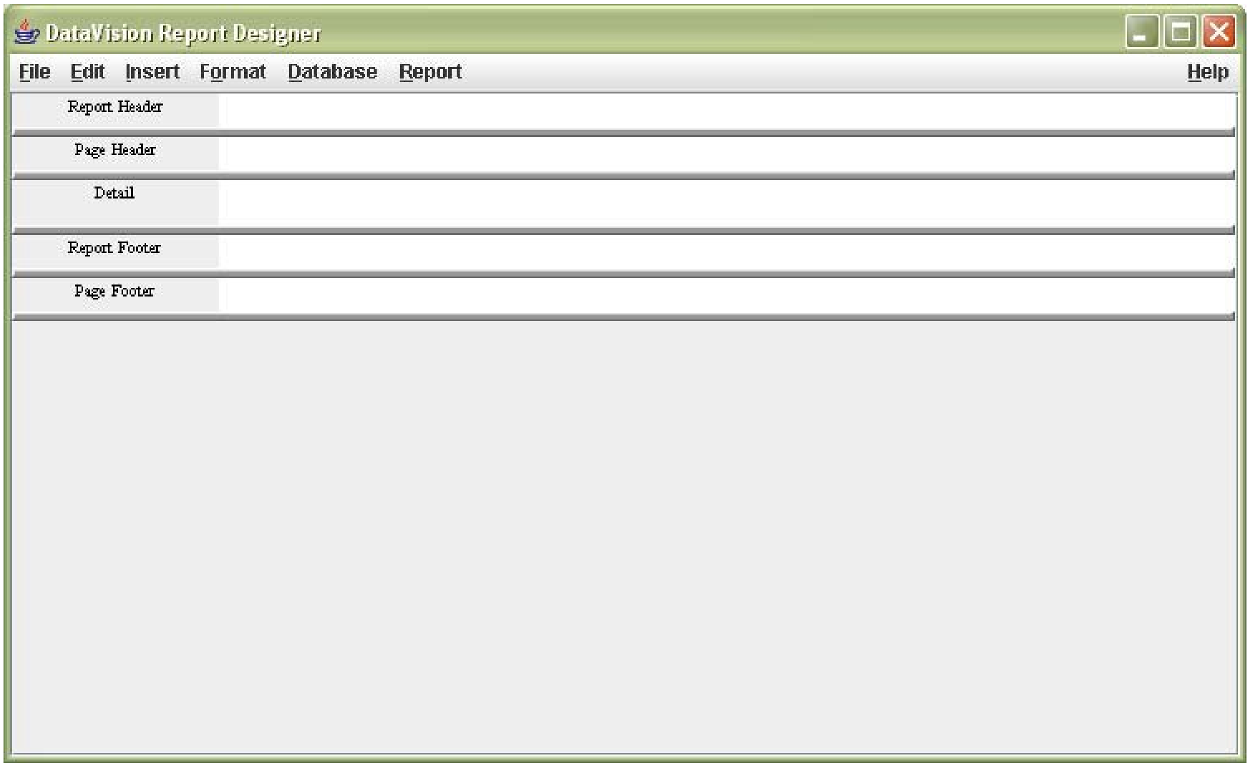
Database Name: bsc

User Name: jim

Password: ********

Figure 4: Database Connection Screen

8. Click Ok to display the DataVision Report Designer window.



9. From the Insert menu, select Database Field to display the Fields window.

10. From within the Fields window, open the All Database Fields folder to display all the available database tables. From here you can begin dragging and dropping fields from within these table folders into the Report Designer. (By adding the fields to the Detail portion of the designer, a title is added dynamically.) The DataVision reports are created in XML, so they can actually be done without the designer.