InformixDB Authentication (PC, SCA)

Thank you for your interest in authenticated scanning! When you configure and use authentication, you get a more in-depth assessment of your hosts, the most accurate results and fewer false positives. This document provides tips and best practices for setting up InformixDB authentication for compliance scans.

A few things to consider

Which technologies are supported?

For the most current list of supported authentication technologies and the versions that have been certified for VM and PC by record type, please refer to the following article:

Authentication Technologies Matrix

Which connections are supported?

DRDA connections including "DRDA over TCP" and "DRDA over SSL/TLS" are supported. The connection strings are "drsoctcp", "drtlitcp", "drsocssl", and "drtlissl". Connection strings starting with "on" are not supported.

What database information is required?

The database name to authenticate to, the unique name of the database server and the port used for DRDA communication where the database is running. We provide default settings which is customizable.

Why should I use authentication?

With authentication we can remotely log in to each target system with credentials that you provide, and because we're logged in we can do more thorough testing. This will give you better visibility into each system's security posture. Is it required? Yes, required for compliance scans and recommended for vulnerability scans..

Are my credentials safe?

Yes, credentials are exclusively used for READ ACCESS ONLY to your system. The service does not modify or write anything on the device in any way. Credentials are securely handled by the service and are only used for the duration of the scan.

What are the steps?

First, set up an IBM Informix user account and privileges (on target hosts) for authenticated scanning. Then, using Qualys Policy Compliance, complete these steps: 1) Add an Informix authentication record to associate credentials with hosts (IPs), 2) Launch a compliance scan, and 3) Run the Authentication Report to view the authentication status (Passed or Failed) for each scanned host.

InformixDB Credentials

We've provided a set of scripts below to help you set up an account and privileges which must exist prior to running scans. Note - These scripts require a super-user account which has privilege to createUser and grantRole. For example, accounts with qualys_scan or dbOwner role.

Please run the scripts provided, in the order shown. The role and scan account needs to be created in the admin database to run successfully.

1) Create a User Account

Prior to IDS version 11.70 -- Informix uses local user accounts that are inherent to the OS, we recommend creating a user account named QUALYSSC for the purpose of scanning the data environment. Note – An administrator will need to add these permissions.

```
database [name of database];
grant connect to qualyssc;
```

IDS version 11.70 and above -- either an OS local user account or a mapped user can connect to a database after providing a password that is validated in an authentication layer outside the database server. You can follow the steps indicated here in IBM documents:
CREATE USER statement | How to set up User Mapping for Non-OS Users

Here are the simplified steps, assuming a local user "dbuser" has been created at the OS level:

```
database [name of database];
CREATE DEFAULT USER WITH PROPERTIES USER "dbuser";
CREATE USER qualys_scan WITH PASSWORD "[password]";
grant connect to qualys_scan;
```

Also ensure the file allow.surrogates in /etc/informix has been updated accordingly with the local user information.

2) Verify Privileges on the Scan Account

Verify that the qualys_scan account has all the privileges in the database to run a successful compliance scan. These privileges are by default granted to the public account, so the script is to verify that the scan account has the necessary privileges to access these tables. Log into the instance using the "qualys_scan" account, then run the script to see if access is available to the account. We provide a script in the zip archive to help you identify missing privileges from the user account to be used for scanning. These scripts are in the files QG_InformixDB_Auth_verx.x.txt. A super user should execute the script by connecting to a database to determine if all the appropriate privileges have been set up correctly. The script will generate an output listing the status of all the prerequisites.

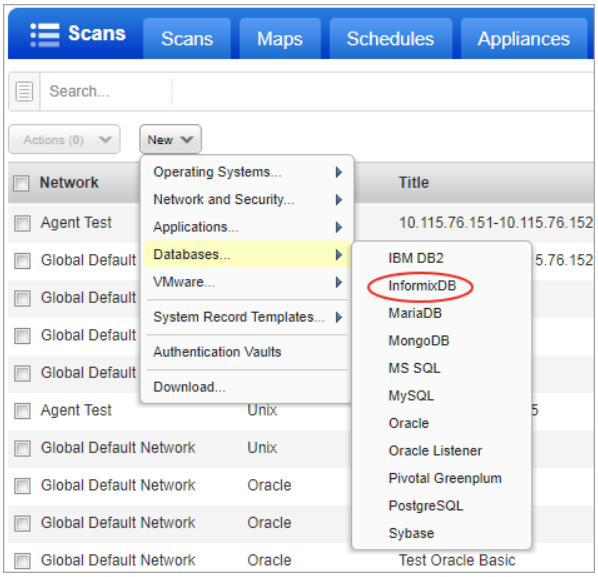
Sample Expected Output:

Prerequisites	Status
CURRENT USER	qualys_scan
SYSROLEAUTH	PASSED - SELECT privilege exists
SYSTABAUTH	PASSED - SELECT privilege exists
SYSTABLES	PASSED - SELECT privilege exists
SYSUSERS	PASSED - SELECT privilege exists
VERSION	IBM Informix Dynamic Server Version 11.70.FC8DE

Did you get different results? Contact your InformixDB DBA to ensure that privileges are set up correctly.

InformixDB Authentication Records

You'll need to create a separate authentication record for each InformixDB instance to be scanned. During scanning we'll authenticate to one or more InformixDB instances on a host using all the InformixDB authentication records in your account. Note - Unix authentication is also required so you'll also need a Unix record for the host running the database.

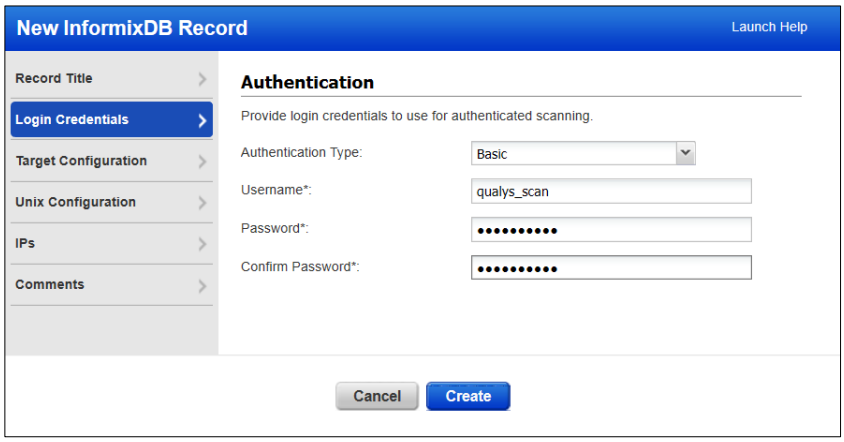


Where do I create records?

Go to Scans > Authentication > New > Databases > InformixDB Record.

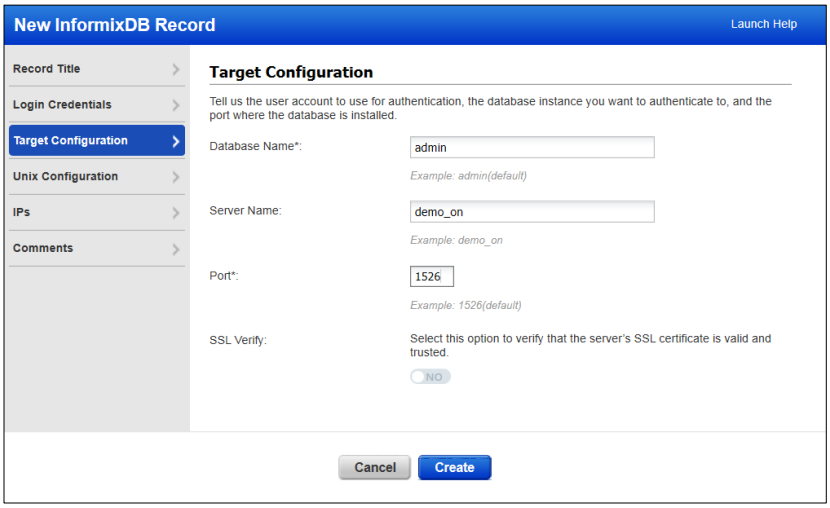
Your login credentials

Enter the credentials (user name, password) for authenticating to the InformixDB server.



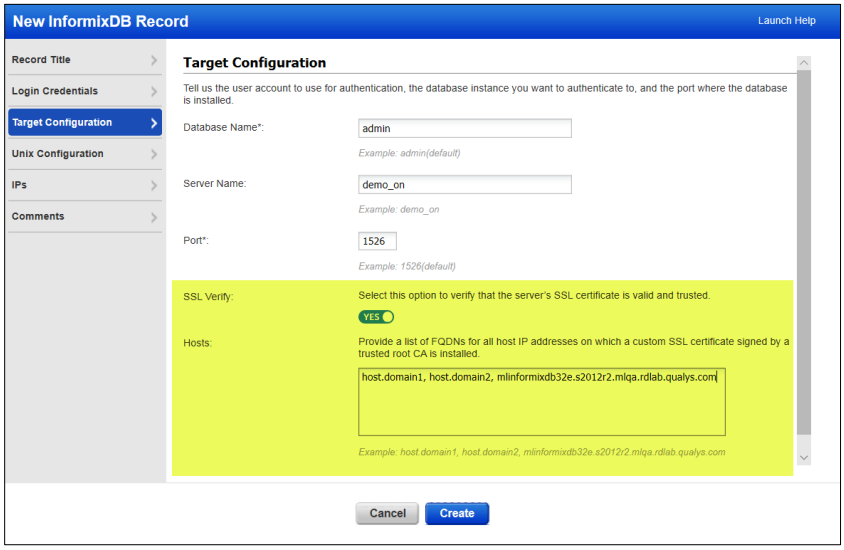
What database information is required?

Tell us the database name to authenticate to, the server name and the port the database is running on (or use the default database name and port).



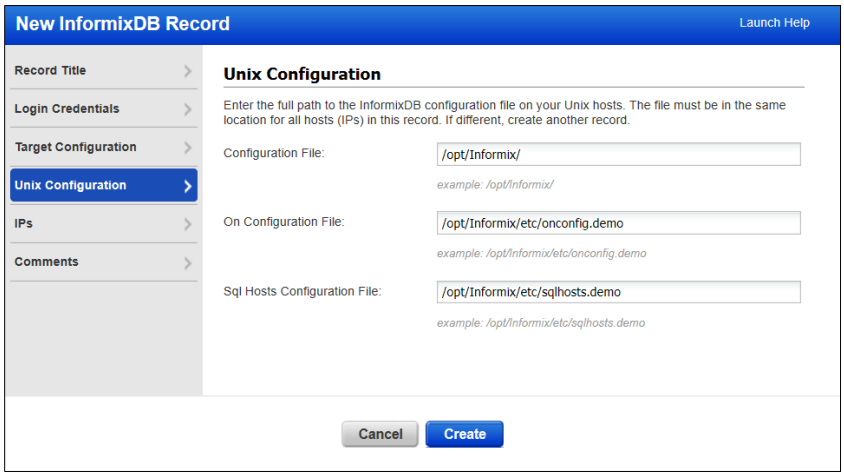
Should I use SSL?

Using SSL provides a secure connection to your database. By selecting "SSL Verify", and if your database server supports SSL, you will be requesting a SSL secured link. The server SSL certificate verification is also enforced. By default, this option is set to NO.



Your InformixDB configuration file

It is essential, though not required, that you provide the location of the InformixDB configuration file, On Configuration File and Sql Hosts Configuration File within the authentication record.



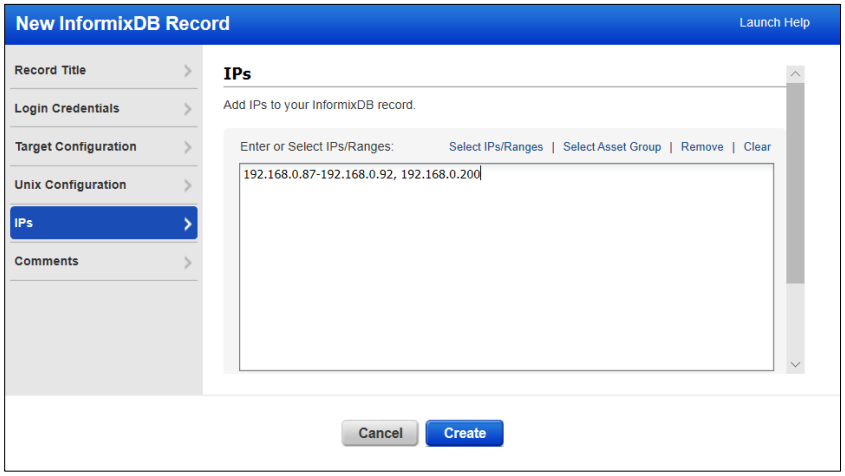
Configuration File - This file is required for certain checks. For Unix, this file helps us gather the information needed to provide the information you are looking for.

On Configuration File - This file contains default configuration parameter values. You can modify the parameter values to improve performance and other characteristics of the instance or database.

Sql Hosts Configuration File - Fields in the sqlhosts file or SQLHOSTS registry key describe connectivity information.

Add IPs to the record

Provide the IP addresses for the InformixDB databases that the scanning engine should log into using the provided credentials.
You can also select IPs/Ranges with the help of Select IPs/Ranges link or Select Asset Group link.



Last updated: May 27, 2022