CYGNA LABS

Cygna Auditing & Security Suite

Installation Guide

Cygna Auditing & Security Suite

For the latest information, visit online documentation at docs.cygnalabs.com

Published 1/11/2022

Version 5.9

Table of Contents

Introduction to Cygna Auditing & Security Suite

Note for BeyondTrust Customers

Cygna Labs assures BeyondTrust's Auditor Suite customers continuity with on going product development, maintenance and support. Please find the information below on respective name changes.

Former name	Current name
PowerBroker Auditor for Active Directory BeyondTrust Auditor for Active Directory	Cygna Auditor for Active Directory
PowerBroker Auditor for Exchange BeyondTrust Auditor for Exchange	Cygna Auditor for Exchange
PowerBroker Auditor for File System BeyondTrust Auditor for File System	Cygna Auditor for File System
BeyondTrust Event Vault for Windows	Cygna Event Vault for Windows
PowerBroker Auditor for SQL Server BeyondTrust Auditor for SQL Server	Cygna Auditor for SQL Server
Change Manager for Active Directory	Cygna Change Manager for Active Directory
Privilege Explorer for Active Directory	Cygna Privilege Explorer for Active Directory
Privilege Explorer for File System BeyondTrust Privilege Explorer for File System	Cygna Privilege Explorer for File System
Protector for Active Directory BeyondTrust Protector for Active Directory	Cygna Protector for Active Directory
Recovery for Active Directory	Cygna Recovery for Active Directory

Overview of the Suite

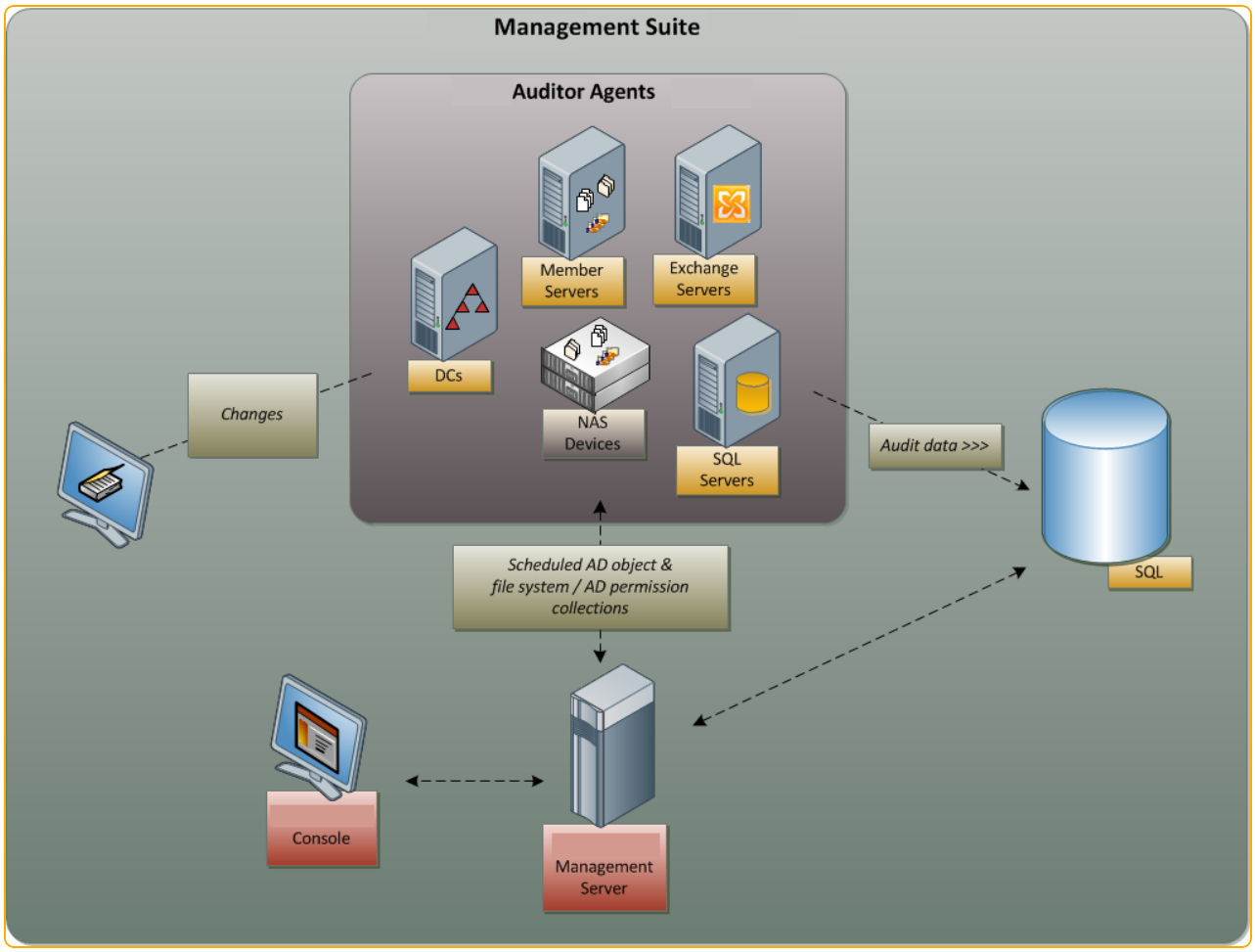
Using Cygna Auditing & Security Suite, you can:

- Deploy agents to selected Domain Controllers (Cygna Auditor for Active Directory)
- Create real-time policies for Active Directory (Cygna Auditor for Active Directory, Cygna Protector for Active Directory)
- Create pre-defined schedules that can be selected when you are creating collectors (Core feature for packages in Auditing & Security Suite)
- Recover deleted objects (Cygna Recovery for Active Directory)
- Rollback objects to a previously saved state (Cygna Recovery for Active Directory)
- Create audit views that can be opened to examine and analyze activity and audit trails for Active Directory, SQL server, Windows file system, Exchange server (Cygna Auditor)
- Create Privilege Explorer views to analyze file, folder, and share permissions on Windows and Active Directory (Cygna Privilege Explorer)
- Gather events from native Microsoft event logs to view and report on (Cygna Event Vault for Windows)

Architecture

This section provides a description of the Cygna Auditing & Security Suite components.

The following figure represents the Auditor components and shows the interactions with Domain Controllers and the SQL Server database.



Server

The server handles the management layers and task engine for the suite.

Agents

Several of the Auditor modules require agents to be deployed to gather real-time information

- Cygna Auditor for Active Directory
- Cygna Auditor for Exchange
- Cygna Auditor for File System
- Cygna Event Vault for Windows

SQL Server

The database stores configuration information and collected data.

Console

The console is used to configure the Auditor settings, set up schedules, and view collected audit and security data.

RSAT Extensions

RSAT extensions are an add-on for Active Directory Users and Computers and other associated native Active Directory management tools. They provide extra actions and information for viewing integrated object activity and audit trail, and performing object rollback and restore.

Requirements

Ensure the following software and hardware requirements are in place before installing the Cygna Auditing & Security Suite. Auditor can be deployed to 32-bit or 64-bit platforms.

Current Version	5.9
Products	Cygna Auditor for Active Directory Cygna Auditor for File System Cygna Auditor for Exchange Cygna Auditor for SQL Server Cygna Protector for Active Directory Cygna Recovery for Active Directory Cygna Privilege Explorer for Active Directory Cygna Privilege Explorer for File System Cygna Change Manager for Active Directory Cygna Event Vault for Windows

Console Software Requirements

Client Operating Systems	Windows 10 Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 Windows Server 2008 (32-bit and 64-bit) Windows 8 (32-bit and 64-bit) Windows 7 (32-bit and 64-bit) Windows Vista SP1 (32-bit and 64-bit)
Additional Software	.Net 4.5 or later for audit views on all clients, Group Policy Management Console (GPMC) for GPO backups Visual C++ Runtime 2013

Console Hardware Requirements

Processor Memory	Pentium 1GHz minimum, 2+ recommended 2 GB RAM minimum, 2+ recommended

Database Software Requirements

Supported Databases	Microsoft SQL Server 2017 Microsoft SQL Server 2016 or SP1 Microsoft SQL Server 2014 SP1 or later Microsoft SQL Server 2012 SP2 or later Microsoft SQL Server 2008 R2 SP2 or later Microsoft SQL Standard or Enterprise Editions in Production. SQL Express has builtin CPU and RAM limitations and is unsuitable for production installs. Microsoft SQL Server Express 2008 R2 SP2 or SP3 for lab evaluations Note: SQL TCP/IP protocol must be enabled. Also it is limited to lesser of 1 Socket or 4 cores and 1GB RAM - https://msdn.microsoft.com/library/cc645993.aspx#CrossBoxScale Microsoft SQL Server Reporting Services SQL Server 2008 R2 or higher Visual C++ Runtime 2013

Database Hardware Requirements

Processor Memory	Pentium 1GHz minimum, 2+ GHz recommended with 2 or more cores 4 GB RAM minimum, 4+ recommended

Server Software Requirements

Server Operating Systems	Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 Windows Server 2008 (32-bit and 64-bit) Visual C++ Runtime 2013
Additional Software	.Net 4.5 or later for audit views on all clients, Group Policy Management Console (GPMC) for GPO backups

Server Hardware Requirements

Processor Memory	Pentium 1GHz minimum, 2+ GHz recommended 2 GB RAM minimum, 2+ recommended

Port Requirements

1433 (and 1434)	By default, SQL Server uses port 1433 and the SQL Browser service uses 1434 (required when using named instances, e.g. SQLEXPRESS uses them by default). Access is required to the correct ports to enable remote connections to SQL Server from both the Cygna Auditing & Security Suite server and any systems running agents.
35000	The Management server service listens on port 35000 by default so you need to open it (or the port you specify during install) on the Cygna Auditing & Security Suite server. If the port isn't open, you cannot remotely connect to it from another machine.
135-139, 445 (UDP/TCP):	Domain Controllers and Server agents don't communicate with the Management server service directly (only the SQL server). You should be able to deploy agents (e.g. Auditor for AD datahandler, Auditor for FS monitors, etc) without opening any non-standard ports. If you turned off some of the default firewall exceptions there may be issues (e.g. File and Printer Sharing) in which case UDP and TCP ports 135-139,445 will need to be opened.
IIS Port 80	By default the web console uses IIS port 80; however, Setup checks to confirm that no other IIS site is already using that port. If so, a warning will be displayed and the user has the opportunity to change the install port to something else.

Note: The Auditor for AD cannot be installed on the same Domain Controller as Change Auditor for AD.

Auditor for AD Bridge and PowerBroker for Windows

If you are using a license of Auditor for AD Bridge and PowerBroker for Windows, we provide a limited set of audited activities with this license. Contact Cygna customer care specialist for more details.

PowerBroker Windows

- All Policy Changes for PowerBroker Windows policy settings
- When a GPO is linked or unlinked to a Domain, Site, or Organizational Unit
- When a Policy link is enabled or disabled
- Policy enforcement or order

AD Bridge

- All Policy Changes for AD Bridge policy settings
- When a GPO is linked or unlinked to a Domain, Site, or Organizational Unit
- When a Policy link is enabled or disabled
- Policy enforcement or order
- All changes on any user, group, or computer object that is Unix enabled by AD Bridge

Prepare for Installation

In preparation for installation, ensure the following permissions and policy settings are in place before installing the suites.

Auditing & Security Suite Permissions

There are four security roles used by Auditor:

- Install User Account: Used to install Auditor.
- Auditor Server Service Account: Used to run the Auditor Management Server service.
- Auditor Agents Service Account: Used to run the agents for several Auditor applications.
- The Management Console or RSAT Extensions User: Used to run Auditor applications and add-ons.

The following sections outline the required permissions for each of these roles.

Install User Account

Local Permissions

- The user must be a member of the Local Administrators group (either directly or through nesting) on the local machine. The user must also be a member of, and have the appropriate rights for, the domain.
- If the Auditor Suite is being installed on a Domain Controller, the user must be a Domain Admin or Enterprise Admin.

SQL Server Permissions

- The user must have a log-in for the target SQL Server.
- The user must have a db_creator Server Role unless the database is being created manually from a .sql file.

Active Directory Permissions

- The user needs general read permissions granted by default to Authenticated Users.

When running the Configuration wizard:

- Create child objects in the Computer object where the Management Server software will be installed.

- Write all properties for Service Connection Point objects inside the Computer object where the Management Server software will be installed.
- If upgrading from a previous version, the user needs read permissions on the CN=Services container in the Configuration Name Context.

Auditor Server Service Account

By default the Auditor Management Server service will run as Local System. It is recommended that this not be changed; however, if you want to change it, the following permissions are required.

Local Permissions

- The user must be a member of the Local Administrators group (either directly or through nesting) on the local machine.
- For versions prior to 5.8 or upgrades to 5.8 or later, the user needs full access to the Program Files\Beyondtrust\PowerBroker Management Suite\Server folder
- For a new installation, the user needs full access to the installation folder
- For Recovery for AD, the user requires full access to the GPO backup share.

SQL Server Permissions

- The user must have a login for the target SQL Server.
- The user must have a db_owner database role or db_datawriter and db_datareader database roles on the database.
- The user must be able to grant execute permission on all stored procedures. There is no built-in role for this.

Active Directory Permissions

- The user requires Read/Write permissions in the child object under the Computer object.
- The user needs to be a member of the Group Policy Creator Owners group or equivalent. This allows backup and restore of GPOs.

For Deploying Agents:

You can use the current logged on user credentials or select an alternate user name and password to use for the deployment. The user account requires the following:

- Must be an Enterprise Admin or Domain Admin. This is because there is no local administrators group for a Domain Controller.
- Read rights to the registry on the remote DC.

- Can create a share on the remote DC and copy files to it.
- Can remotely create a service, edit it, and start it.

Auditor Agents Service Account

By default, the Agent service will run as Local System. It is recommended that this not be changed however, if you want to change it then the following permissions are required.

Local Permissions

- The user must belong to the Domain Admin group for interacting with the operating system and Active Directory.
- The user must have “Log on as a service” permissions.

SQL Server Permissions

- The user must have a db_owner database role or db_datawriter and db_datareader database roles on the database.
- The user must be able to grant execute permission on all stored procedures. There is no built-in role for this.

Console or RSAT Extensions User

Active Directory Permissions

- The user must have appropriate Active Directory rights to perform the desired task. For example, rollbacks occur on the client side as the logged-on user
- By default, the Permissions assigned to nodes in the Console is: Domain Admins - Full Control and Enterprise Admins - Full Control. Permissions can be changed on applicable nodes by right-clicking the node and selecting Permissions.

Audit Policy Settings

Auditor for AD can attempt to determine whether a password change is one of the following:

- Password Change: the user has changed their own password
- Password Reset: the account password has been reset by an Administrator

For this to work properly, an additional Audit Policy must be set in the Default Domain Controllers GPO (or a similar GPO that is applied to all DCs). You must enable auditing of Successful Account Management events (Policies \ Windows Settings \ Security Settings \ Local Policies \ Audit Policy).

The following 3 policy settings should be enabled:

POLICY	SETTING
Audit account logon events	Success
Audit account management	Success
Audit logon events	Success

If you do not have the above audit policies enabled on the DC, the password change/password reset event is audited as a 'change to password last set' and due to how AD processes password changes, the Auditor for AD agent only sees it as being performed by the ANONYMOUS LOGON or SYSTEM event.

With the above audit policies set, more accurate event summary text is captured, and also the 'WHO' from ANONYMOUS/SYSTEM will be changed to the actual user making the change.

Install Cygna Auditing & Security Suite

The install of Cygna Auditing & Security Suite includes the following key steps:

- Running the Setup.exe file.
- Installing the suite using the install wizard.
- Using the Configuration Tool to configure the server, database, management console, and web console.

Note: Multiple Auditor Management Server installations can be installed in a single forest. However, it should only be done with the assistance of a Cygna Labs Technical Support representative. Contact Cygna Labs Support for additional details.

The Server, Console, Packages and Web Console are all installed using the installation wizard.

1. Double-click the Setup.exe.
2. On the User License Agreement page, click the terms and conditions check box to agree and then click Next.
3. On the Install Options page, click each button for the options you want to install and then click Next.
4. Upload your license file. Click in the license box to browse to the location.
5. There is an option to start a 30 Day Trial by selecting the green button. This will provide a time-limited fully functional 30 day expiring license for the Suite and includes the following packages.
   - Cygna Auditor for Active Directory
   - Cygna Auditor for File System
   - Cygna Auditor for Exchange
   - Cygna Auditor for SQL Server
   - Cygna Recovery for Active Directory

   The license will display all of the Auditor modules included in the license.
6. Select the modules you want to install, and then click Next.
7. Select the installation path or use the default path provided, and then click Next.
8. Click Install.

   The wizard will display each component of the Suite and a green check mark will appear with successful completion of each component.

9. Click Run Automatic Configuration for the Web console configuration. The Automatic Configuration installs the following roles:
10. Provide credentials with access to the database and then click SUBMIT.
    - Default Document
    - Directory Browsing
    - HTTP Errors
    - Static Content
    - HTTP Redirect
    - HTTP Logging
    - Static Content Compression
    - Dynamic Content Compression
    - Basic Filtering
    - Basic Authentication
    - .Net 3.5 Extensibility
    - .Net 4.5 Extensibility
    - ASP.NET 3.5
    - ASP.NET 4.5
    - ISAPI Extensions
    - ISAPI Filters
    - IIS 6 Metabase Compatibility
11. Select the Install Updater check box to install the Cygna Updater tool. The Updater is a service that will automatically update Cygna Auditor Suite when new versions are available.
12. Select the Enable automatic updates check box and enter the number of days you want Updater to look for updates. To disable this feature, clear the Enable automatic updates check box.

Note: Once the server is installed the configuration tool will open. Additionally, when opening the Web Console for the first time or exiting the wizard, the Configuration Tool will open.

Configure the Management Server

To configure the Management Server:

1. The final page of the wizard contains two links. Select OPEN DESKTOP CONSOLE. Before the console opens the Configuration wizard will appear.
2. On the Welcome page, the Auditor components are listed with indicators showing if they are successfully configured. Note that this page is different based on whether the Auditor Management Server has been previously configured. Click Next.
3. On the Service Configuration page, select the check box to change the default service account. This account is used by the Management Server service.

   Optionally, you can choose to run as Local System Account.

For more information, please see Auditor Server Service Account for detailed permission requirements.

4. Enter the account name and password.
5. Click Next.
6. On the Port Configuration page, enter a port.
   - This port is used by the Management Server when gathering data.
   - The default value is 35000. If this value is used by another application, provide a port number that is not in use.
7. Click Next to continue.
8. On the Windows Firewall Status page, review the Windows Firewall settings. Change settings as necessary by clicking the Enable button for each category. Click Next when all connections are configured.

Ensure the port number provided earlier can accept incoming connections. Otherwise, connection issues to the Management Server can occur.

9. On the Database Configuration page, review the information about SQL Server. After you review the information, click Next.

If you are evaluating Auditor, you can click the link to download SQL Server Express.

10. Configure the BeyondTrust database settings.
    - Server Name: Select the database server from the drop-down list.

    If the SQL Server Browser service is running, a list of servers and instances will be displayed. If the SQL Server Browser service is not running, servers and instances may not be displayed.

If you do not want to start the browser, enter the database information in the format: server name, port number

- Database: Select an existing database from the list, or click New Database to create a database.
- Authentication: Select a mode of authentication from the list: Windows Authentication or SQL Server.

11. Click Next.
12. On the Active Directory Extension page, click the Enable button to allow specialized Auditor functionality in Active Directory, referred to as RSAT extensions. Click Next.
13. The Configuration Complete page indicates if components are successfully set up. Click Finish.
14. When the setup wizard is complete, click Finish.

Find the SQL Server Port Number

To find the port number:

1. Start SQL Server Configuration Manager.
2. Expand the SQL Server Network Configuration node.
3. Select Protocols for MSSQLSERVER.
4. Double-click TCP/IP to open the Properties dialog box.
5. Review TCP port information.

Configure Web Console

The Web Console is installed during the installation. The installation of the Web Console will do the following:

- Deploy all files to the specified directory
- Create an IIS website
- Create an application pool
- Attempt to run a SQL script to create tables in the database

The first time the Web Console is launched, the Web Configuration Tool will appear. The Web Configuration Tool has two easy steps which are required in order to utilize the Web Console.

Step One

The Web Console requires access to the database. If you did not select SQL Authentication during the database configuration, you can select one of the below options; otherwise SQL Authentication is entered by default.

The options are :

- The identity of the application pool to a domain user that already has access to the database.
- A service account to grant database reader and writer rights to.

Step Two

The Web Console requires default administrators be chosen. You can choose multiple users and groups. This feature is helpful in the event that you want to assign specific users to audit data for specific modules only.

To delete users or groups select the trash can icon next to their title. After you make your selections, click Complete.

Use TLS 1.2 Security Protocol

SQL Server supports the TLS 1.2 security protocol.

For more information about the implementation, please see the following web site:

TLS 1.2 support for Microsoft SQL Server

You must install an updated SQL Server Native Client driver to ensure successful connections between Cygna Auditor and SQL Server. The driver is automatically installed and available for all remote agents. For manual deployments, there are two ways to get the driver:

- The driver is installed when you install Auditor and is available here:

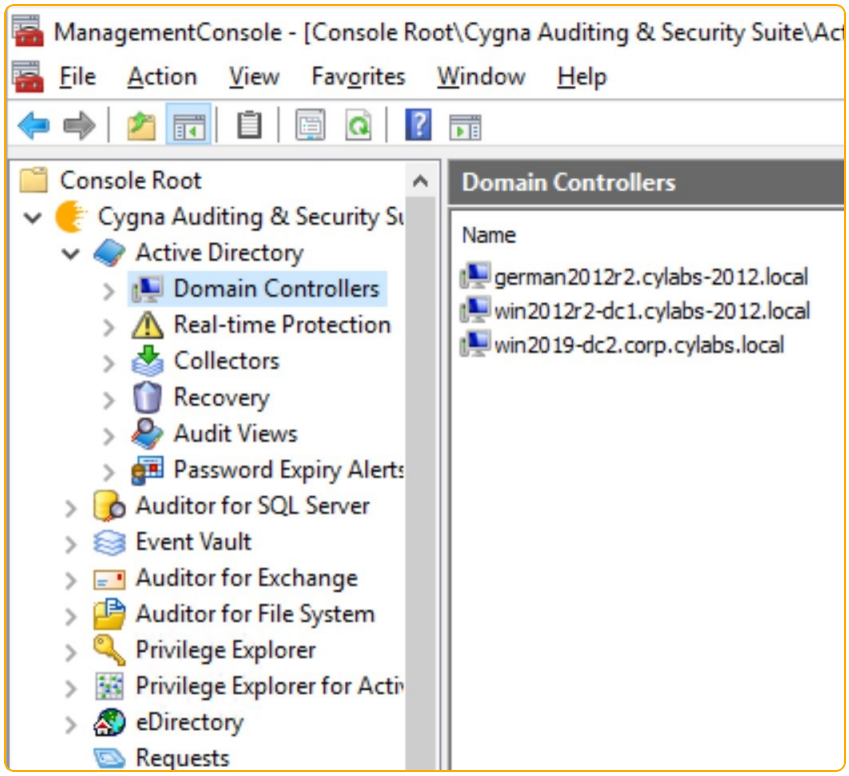
  <*InstallDir*>\Server\SQL driver

- You can download the driver from Microsoft

  Installing SQL Server Native Client

Verify SQL Native Client is Updated on the Domain Controller

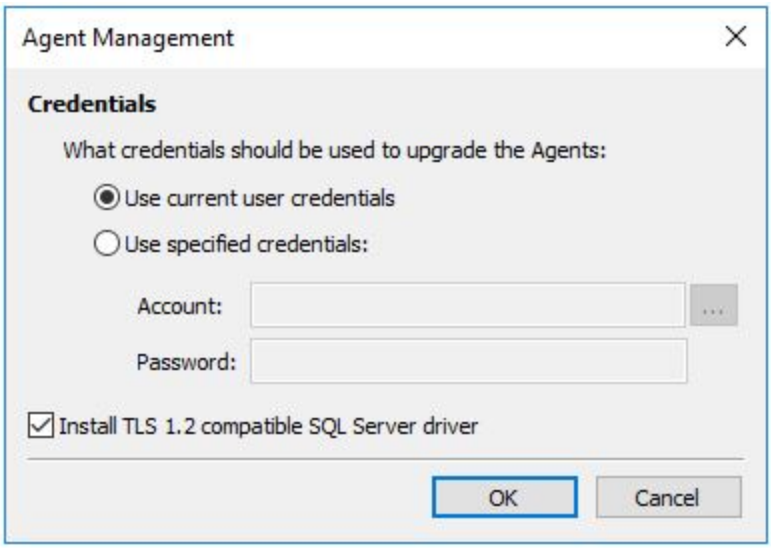
1. Go to the Domain Controller node.



2. On the information page for the domain controller the TLS 1.2 Ready column indicates if the agent was updated with the latest driver for SQL Native Client.

Upgrade SQL Native Client on Remote Agents

1. Go to the Properties page for the agent.
2. Click the Upgrade Now button.



3. Select the Install TLS 1.2 compatible SQL Server driver check box.
4. Click OK.

The driver is ready after the agent is restarted.

Upgrade

Auditor 4.1 (and earlier) events are dynamically converted to the v5.x format on-the-fly when a report is run on the data. However, you can migrate the events if you want to view extended information (for example, canonical name).

You can migrate the events using the MigrateData5.exe tool located in the install directory:

\Program Files\Blackbird\Server

Review the following recommendations before proceeding:

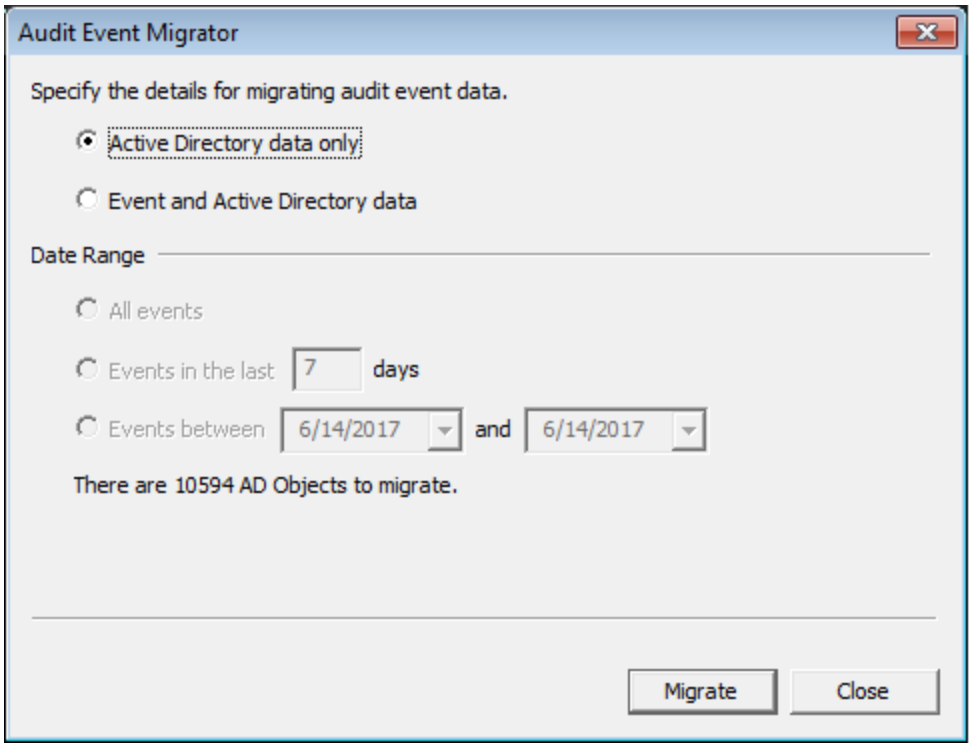
- Back up your existing Auditing & Security Suite database before proceeding with the migration.
- Run the migration overnight to run during the typical low utilization period.
- Performance varies based on the amount of data being migrated and the available resources on the database. Therefore, we recommend you select a short range of events, take note of the number of events (listed on the bottom line of the window), note the time taken to migrate the events, and extrapolate this to calculate the throughput of the remaining events.

The user running the migration requires at least db_datawriter permissions for the Cygna Auditing & Security Suite database.

Note: You must upgrade at least one deployed Domain Controller agent to 5.0 before you can migrate events.

To migrate your events:

1. Run MigrateData5.exe.



2. Select the event to migrate:
    - Active Directory data only: Migrates the Active Directory object information. Note that in v5.x, additional object name-type data is stored so events are more descriptive.
    - Event and Active Directory data: Migrates v4.x events to v5.x and gathers the extra Active Directory object information.
3. Select a range of events to migrate:
    - All events
    - Events in the last x days
    - Events between the selected time range
4. Click Migrate.

The Auditor for Active Directory data will now be migrated. You can monitor the status on the progress bar displayed during the migration.