



Goverlan Reach Quick Start Implementation Guide

Introduction

This quick start guide will assist you with installing and configuring Goverlan Reach. It is designed to progress from the simple configuration options of Goverlan Reach to the more complex installations.

Step 1 – Console and Agent Installation – Complete these steps to begin to manage your internal systems and Active Directory quickly with Goverlan Reach.

Step 2 – Console Database Configuration – Move on to these steps for teams of Goverlan Reach Users who wish to use Team Collaboration features.

Step 3 – Goverlan Policy Distribution – Move on to these steps for configuring Goverlan Reach Policy distribution and added features such as centralized auditing and external device management.

This guide is not a replacement for the full Goverlan Reach User Guide. The full guide can be found at <https://www.goverlan.com/support>

Step 1 – Console and Agent Installation

The Goverlan Reach Console does not require a centralized database or server for most of its functions. If you do not intend to use the Reach Server or a centralized database, simply follow these steps.

Pre-Requisites

The following prerequisites should be considered before deployment.

System Requirements for Reach Console

Number of endpoints	200 Max
Number of operators	1 Max
CPU	Dual Core – 2.2Ghz or greater
Memory	4GB installed RAM
Network	1Gbps NIC speed
Disk (Application + Built-In DB)	1GB Free Disk Space

Network Ports

The Reach Agents listen on Port 22000 by default. This port may be blocked. Please allow a Windows Firewall rule to allow the Agents to be available on this port. Please see the Appendix A of the following security documentation for all network requirements.

https://www.goverlan.com/pdf/Goverlan_Reach_Security_Whitepaper.pdf

Endpoint Security Exclusions

Goverlan Reach Agents operate as a Window Service. Several Endpoint Security applications may interfere with the agent's functionality.

Please whitelist the following directory using your endpoint security system.

C:\Program Files\Goverlan Inc.

fastConnect (Logged-in Workstation Detection)

fastConnect is the ability to detect where a user is logged-in, in real-time. In order for this feature to work “out of the box” the following pre-requisites must be present.

- All users must be configured with a roaming or terminal services profile
- All Goverlan operators must have Read Permissions to the user profile.

If these pre-requisites cannot be met, a Goverlan Reach Server is required. The server will handle all request for fastConnect. Proceed to Step 3 – Goverlan Policy Distribution for more information.

Goverlan Reach Console Installation

The Goverlan Reach console is very easy to install.

1. Log in to the <https://my.goverlan.com> and select the Console Tab.
2. Click Downloads for this Product.
3. Download the latest Goverlan Reach Console.
4. You may run the EXE directly from the desktop.
5. Sign in using your my.Goverlan.com account ID.

Note: There are silent install switches that can be used.

<https://www.goverlan.com/knowledge/article/goverlan-agent-product-switches/>

Goverlan Reach Agent Installation

The Goverlan Reach Agent can be installed using several methods:

- Push installation from the Reach Console
 - Right click any system and select Agent Install.
or
 - Run a Process Automation – for more information, see [Process Automation](#).
or
 - Using the Goverlan Agent Manager
 1. Open the Goverlan Reach Console
 2. Go to Application → Goverlan Agent Manager
 3. Add systems to the list by clicking the + sign.
 4. Once the systems have been added to the list, right click and select “Install Goverlan Agent”

Note: There are pre-requisites for a push or ad-hoc installation of the agents. Please see [Automatic Installation and Maintenance](#) for more information.

- Generating an agent installer EXE or MSI.
 1. Open the Goverlan Reach Console
 2. Go to Application → Goverlan Agent Manager
 3. Use the “Generate Agent Installer” drop down
 4. Select “Customize Agent before Installation” to distribute settings with your agent. For more information, see **Configuring Policies**.
 5. Select Generate Agent Installer → As a Service or On-Demand Session → MSI or EXE package
 6. You will be asked where to save the MSI or EXE file.

You may use the EXE or MSI file with your choice if software deployment platform. Installation parameters can be found at

<https://www.goverlan.com/knowledge/article/goverlan-agent-product-switches/>

Step 2 – Console Database Configuration

The Goverlan Reach Console uses a database to store offline cached content and console configurations. By default, the Goverlan Reach Console uses a file-based database.

However, when multiple consoles connect to a centralized standalone database, they may utilize team collaboration capabilities.

Note: This step is OPTIONAL. It is not required to move on to Step 3.

Pre-Requisites

The following prerequisites should be considered before deployment.

System Requirements for the Reach Console standalone database

Console Standalone DBs must run on SQL Server or SQL Server Express

Number of endpoints	200 or more
Number of operators	2 or more
SQL Server Version	SQL Express or SQL Server 2008 R2 and above
Database disk space	5GB Free Disk Space for MDF & LDF files

For full SQL or SQL Express configuration tips, please see this article:

<https://www.goverlan.com/knowledge/article/goverlan-sql-server-configuration/>.

Creating the Reach Console Database

Once the SQL Server is configured, use these steps to create to configure your console to use it.

Configuring the Console Database

The database configuration must first be applied to a console for the DB creation to happen.

This can be done with the following methods:

Note: Do not pre-create the database. The Reach Console must create the database.

Direct configuration in the Reach Console

1. Open the Goverlan Reach Server Console
2. Go to Application → General Settings → Database Settings

- a. Select Microsoft SQL Server from the drop-down list
- b. Database Name = (Leave the Default Value of GoverlanV9_DB)
- c. Database Server = SERVER\SQLINSTANCE

Note: if your SQL Server is not using the SQL Browser service, you will need to enter the SQL port number here. SERVER\SQLINSTANCE,1433

- d. Leave User ID and Password blank unless you plan to use SQL Authentication.
- e. Click OK and relaunch the Reach Console.

Note: When relaunching the console, it is best to Right Click -> RUN AS DIFFERENT USER and run it as an account that has DB creator rights for SQL Server. The DB must be created by the application.

3. Once the DB is created, give all Goverlan Reach users “db_datareader” and “db_datawriter” permissions on the newly created GoverlanV9_DB database.

Once the database is configured, manually enter the DB configuration for any other Reach Console users. Alternatively, proceed to Step 3 – Goverlan Policy Distribution to automatically publish the database settings and other Goverlan related configurations for your organization.

Step 3 – Goverlan Policy Distribution

Goverlan Reach settings may be distributed to your consoles and agents.

There are several methods for distributing Goverlan Reach Settings:

	Console Settings	Agent Settings	Centralized Auditing	External Device Management
The Goverlan Reach Server	✓	✓	✓	✓
Goverlan Admin GPO	✓	✓		
Direct Registry Modification	✓	✓		
Process Automation		✓ ¹		
Goverlan Agent Manager		✓ ²		

¹ This method requires a Goverlan Reach Enterprise license.

² The settings available using the Agent manager are limited.

Option 1 – Goverlan Reach Server

Pre-Requisites

System Requirements for the Reach Server

The Goverlan Reach Server can have several hardware requirements depending on its specific configuration. Please see [Goverlan Reach Server Hardware Requirements](#).

Firewall Ports

Goverlan Reach Server Service and Communication

The Reach Server Service listens on Port 22100 by default. This port is used for policy distribution.

Optional Reach Gateway Service

The optional Reach Gateway Service listens on port 15155 by default. This port is used for external device management. This service requires an external firewall rule to allow connections from the internet to the server. For more information, see [Reach Server Implementation](#).

These ports may be blocked. Please allow a Windows Firewall rules to allow the server to be available. These ports are user configurable via the Server Console.

Please see the Appendix A of the following security documentation for all network requirements.

https://www.goverlan.com/pdf/Goverlan_Reach_Security_Whitepaper.pdf

Endpoint Security Exclusions

Several Endpoint Security applications may keep our services from operating properly. Please whitelist the following directory.

C:\Program Files\Goverlan Reach Server v3.

Database Considerations

The server has the option to use a built-in file-based database or a full SQL or SQL Express database.

See this article for new SQL Express or SQL Server database configurations. Please consult your database administrator for existing SQL Server implementations.

<https://www.goverlan.com/knowledge/article/goverlan-sql-server-configuration/>

Advertising the Server

The server must be advertised to the agents and consoles. See this article for different ways to accomplish this.

<https://www.goverlan.com/knowledge/article/advertising-goverlan-reach-server/>

The most secure method for advertising the server is a DNS SRV record.

Installing the Goverlan Reach Server

The Goverlan Reach Server can be downloaded from <https://my.goverlan.com>

1. Log in to the <https://my.goverlan.com> and select the Server Tab.
2. Click Downloads for this Product.
3. Download the latest Goverlan Reach Server installer.
4. You may run the EXE directly from the desktop.
5. Sign in using your my.Goverlan.com account ID.

Configuring the server for operation

1. Configure the DNS SRV Record (or other method of advertising the server)
2. Create a Service Account for the server to run as.
3. The service account must
 - a. be a local admin of the server machine
 - b. have the Logon as a Service right
 - c. (Optional) Must have the DBCreator SQL role for the SQL Server option.
4. Database Settings → Choose File Based or SQL Server based.
 - a. For SQL Server based installs:
 - i. Select Microsoft SQL Server from the drop-down list
 - ii. Database Name = (Leave the Default Value of GoverlanGCS)
 - iii. Database Server = SERVER\SQLINSTANCE
Note: if your SQL Server is not using the SQL Browser service, you will need to enter the SQL port number here. SERVER\SQLINSTANCE,1433
 - iv. Leave the User ID and Password blank unless you plan to use SQL Authentication.
 - v. Click OK and start the Reach Server Service.
5. After the service is started, you may remove the DBCreator right from the service account.

Option 2 – GPO Admin Template

Goverlan Reach comes with GPO templates that contain a full set of Goverlan Reach related policies.

The GPO Templates are in the Reach Console installer directory:

C:\Program Files\Goverlan Reach Console v9\GPO Templates

Import the template to your domain controller and create GPOs to assign to your AD OUs.

The policies are in:

Computer Configuration \ Policies \ Administrative Templates \ Goverlan Global Policies.

Option 3 – Direct Registry Modification

All policies can be directly applied to Reach Agents and Consoles via the registry. Contact support for a complete list of registry values.

Option 4 – Process Automation

Goverlan Reach Enterprise Edition consoles come with a set of policies that can be configured using a Process Automation.

Note: This method can push Reach Agent settings only (not Console settings).

The policies are in the Action Module Screen of Process Automation in the following location:

Add \ Remove → Execute → Goverlan Agent

For more information on Goverlan Reach Process Automations see [Goverlan Reach Process Automation](#)

Option 5 – Goverlan Agent Manager

The Goverlan Agent Manager can push a limited set of policies to the Goverlan Reach Agents. The Agent Manager may also generate EXE's or MSI's with pre-configured settings built in.

Note: This method can push Reach Agent settings only (Not Console settings).

Pushing Policies with the Agent Manager

1. In the Goverlan Reach Console, navigate to Application → Goverlan Agent Manager
2. Use the + sign to add a series of machines to the view.
3. Once the machines are added, right click them and select “Push Client Configuration”

Pre-Configured EXE or MSI

See “[Reach Agent Installation](#)” for more information.

Policy Examples

Various policies may be applied to your consoles. Here are two examples that will show the basics of how all policies are configured. You may use these steps as a guide to apply any Goverlan Reach policies.

Example 1 - Configuring the Console DB policy for Reach Consoles

Reach Server Method

1. Open the Reach Server Global Policy Tab.
2. Drag "Database Configuration" to the All Users and Devices node.
3. Enter the following settings:
 - a. Database Type = 2
 - b. Database Name = (Leave the Default Value of GoverlanV9_DB)
 - c. Database Server = SERVER\SQLINSTANCE
 - d. Leave User ID and Password blank unless you plan to use SQL Authentication.
4. Leave all remaining values default.
5. Click the "Publish Changes" Button to make the settings live.

GPO Template Method

1. The GPO Template is in the Console installer directory. C:\Program Files\Goverlan Reach Console v9\GPO Templates
2. Import the template to your domain controller and configure the following GPO Setting
 - a. Computer Configuration \ Policies \ Administrative Templates \ Goverlan Global Policies \ Goverlan Common Settings \ Database Configuration and Features
 - i. Database Type = Microsoft SQL Server
 - ii. Database Name = (Leave the Default Value of GoverlanV9_DB)
 - iii. Database Server = SERVER\SQLINSTANCE
 - iv. Leave User ID and Password blank unless you plan to use SQL Authentication.

Example 2 – Requiring a User Acceptance Prompt for Remote Control

Reach Server Method

1. Open the Reach Server Global Policy Tab.
2. Drag “Remote Control Client Side Configuration” to the All Users and Devices node.
Note: Create additional filters under the “All Users and Devices” node to apply policies at different levels. See <https://www.goverlan.com/knowledge/article/understanding-policy-scopes/>
3. Enter the following settings:
 - a. Pre-Session Action = 2
4. Leave all remaining values default.
5. Click the “Publish Changes” Button to make the settings live.

GPO Template Method

1. Create a new GPO and target systems where the Reach Agent is installed.
2. Locate the following GPO Item:
 - a. Computer Configuration \ Policies \ Administrative Templates \ Goverlan Global Policies \ Remote Control Client Settings
 - b. Open the Pre-Session Action setting
 - c. Enable the policy and set it to **Prompt the Local User for Approval**
3. Save the policy and wait for the GP Update cycle to complete on your systems.

Direct Registry Modification Method

The following registry key can be set on your agent systems that will force the User Acceptance Prompt policy.

HKLM\Software\Policies\Goverlan Inc\Global Policies\GRMS

DWORD PreSessionAction = 1

Process Automation Method

This method requires Goverlan Reach Enterprise Edition. See

<https://www.goverlan.com/knowledge/article/overview/> for more information on creating

Process Automations:

1. Create a new Process Automation

2. Create the following Action Module
 - a. Add \ Remove → Execute → Goverlan Agent
 - b. Set RMC Client Settings
 - c. Pre Action = 1
3. Run the automation on the systems where the Goverlan Agent is installed.

Goverlan Agent Manager Method

This method assumes the agent is already installed on your systems. If you need to install the agent, please go to Step 1 – Console and Agent Installation.

1. Open the Goverlan Reach Console
2. Go to Application → Goverlan Agent Manager
3. Add systems to the list by clicking the + sign.
4. Once the systems are added to the list, Right Click and select “Push Client Configuration”
5. Under Remote Control Behavior → When a session starts → Pre-Session Action, select “Prompt Local User for Approval”
6. Click Push Settings.

Goverlan Reach Server Hardware Requirements

Basic Configuration (Global Policy and Auditing Role)

CPU	Quad Core – 2.2Ghz or greater
Memory	8GB installed RAM
Network	1Gbps NIC speed
Disk (Application + Database)	5GB Free Disk Space
SQL Server Version	SQL Express or SQL Server - 2008 R2 and above

Basic Configuration + Gateway Services Configuration

Number of simultaneous external connections ¹	< 6	6-12	13-24	25-48	48 and greater
CPU Cores All 2.2Ghz or greater	4	6	12	16	16
Memory	8 GB	8 GB	12 GB	12 GB	16 GB
Network	1 Gbps	1 Gbps	3 Gbps	5 Gbps	6.5 Gbps
Disk (Application + Database)	5GB	10 GB	20 GB	40 GB	80 GB
Minimum Windows OS Version	Server 2008 R2	Server 2008 R2	Server 2012	Server 2012	Server 2012
Minimum SQL Server Version	Express 2008 R2 Server 2008 R2	Express 2008 R2 Server 2008 R2	Server 2012	Server 2012	Server 2012

1. Each operator may establish multiple simultaneous connections during a single support session. On average, approximately 3 connections can be made during a support session.