GOVERLAN | REACH

Extend the reach of your IT services with the industry's
most preferred . powerful . secure solution

Security Whitepaper

GOVERLAN.COM

Last updated on: May 10, 2019

Table of Contents

Introduction

Goverlan Reach is a powerful remote administration solution targeted towards enterprise IT and MSPs. This document includes all security concepts used in Goverlan Reach such as encryption, authentication, and authorization mechanisms.

Overview

Goverlan Reach is a combination of desktop software (known as the Reach Console) and an optional server software (known as the Reach Server). The Reach Console is installed on each operator's machine. The optional Reach Server is not required for most of Goverlan Reach's features. However, it's presence enhances the security and auditing offerings of Goverlan Reach. The Goverlan Reach Server can be installed on any server class machine.

Using Goverlan Reach, the operator can perform a comprehensive set of administration tasks on remote machines either inside or outside of the corporate network. It does so by communicating with the Goverlan Reach Service Agent that is installed on each remote machine (this process can be automated by Goverlan Reach). Goverlan Reach also manages Active Directory items such as user computer or group objects.

The Goverlan Reach solution allows an operator to perform the following duties with total security:

- Perform Active Directory account management.
- Perform administrative duties on remote computers silently and without end-user interaction.
- Take over a remote computer's screen, keyboard and mouse.

Stable, Secure & Self-Managed Agent

Goverlan Reach requires an agent on the remote machines to be able to perform remote administration tasks.

Any new installation of software on a computer is always of great concern to IT administrators as:

- It introduces a new unknown that may affect system stability.
- A service agent can be corrupted or made unavailable by the end users, rendering remote administration unavailable.
- It introduces a new entry point on each remote machine which can be used to compromise a system.

These concerns have been design priorities since the inception and ongoing development of Goverlan Reach Agents.

Since the production release in 1999, the Goverlan Reach Agents have been installed on computers and business critical servers within large infrastructures with no report of system degradation or any other issues. We realize that we offer a solution to ease IT management tasks and not to burden them by introducing instabilities or security breaches.

Stable

The Goverlan Reach agents are less than 20MB in size with no external dependencies (for instance the .Net framework). The Goverlan Reach Agent is compatible with Windows XP to the latest Microsoft operating systems and is available in 32 & 64 bit architectures.

The Goverlan Reach Service spends 99% of its time in an idle state waiting for requests from a Goverlan Reach operator. Every 30 seconds, it performs a self-cleaning to release unused memory to maintain a very low footprint.

Encrypted & Secure

All communications between the Reach Console and the Goverlan Reach agents or the Reach Agents and the Reach Server take place via 3 TCP ports. All ports are configurable.

- Reach Agents Listen on 22000 by default.
- Reach Servers Listen on 22100 and 15155 by default.

To ensure a secure connection and protect against malicious hacking, our communication protocol encrypts all data transmitted between the Reach Console, agents and server at the lowest level. Goverlan Reach uses AES 256-bit encryption. Goverlan Reach can also be configured to use FIPS 140-2 compliant cryptographic libraries only.

Once the data frame is decrypted on the client side, the frame is then securely authenticated using Microsoft SSPI (Security Service Provider Interface). Microsoft's SSPI technology allows clients and servers to establish and maintain a secure channel, provide confidentiality, integrity, and authentication. Using SSPI, Goverlan Reach guarantees the identification of the administrator to the client and impersonates the administrator's credentials locally to authorize the request.

Self-Managed

The Goverlan Reach Agents are self-managed. There is no need to manually pre-install them on your machines to use Goverlan Reach. Installation, maintenance, and removal of agents are automatically performed by the Goverlan Reach Console remotely*.

In the event that an end-user tampers with the agents (service stopped or disabled, files deleted), the Goverlan Reach Console automatically re-installs and initializes the agents, and the administrator can continue with their work.

How Goverlan Reach authorizes a transaction

An important aspect of the Goverlan Reach security model is that it uses native Windows Local Account or Active Directory authentication and privileges. No proprietary authentication takes place while executing a task in Active Directory or on a remote machine.

Every transaction is performed under the credentials of the Goverlan Reach operator (or specified alternate credentials) and is approved/rejected and audited by the native Windows security layer. If a user does not hold the necessary privileges to perform an action, Goverlan Reach simply returns an Access Is Denied message. Essentially, Goverlan Reach does not provide its user with any more privileges than the ones allocated to them in Active Directory.

- The installation, update, or removal of the Goverlan agents always requires local administrative privileges on a client machine.
- Initiating a remote control session requires local administrative privileges on the remote machine by default (this can be configured).†
- Active Directory actions are authenticated and approved using the Goverlan operator's native account privileges.
- Performing management tasks on a remote machine requires local administrative privileges.

* Remote installation and maintenance of the agents require local administrative privileges and access to administrative shares.
† Goverlan's authentication and encryption methods apply to communication via the Goverlan protocol only. Goverlan RC supports using alternative connection methods such as Intel vPRO, MSRDP, VNC, and Telnet/SSH. Authentication and encryption of these protocols fall outside the scope of the Goverlan security model.

Alternate Credentials

In the event a Goverlan Reach operator does not hold the required privileges to perform an action, alternate credentials can be used. Goverlan Reach can save the provided credentials in an encrypted local database.

Alternate credentials can be configured for individual machines, IP ranges, AD domains or External Sites. Credentials can also be stored for any remote control protocol that Goverlan supports, such as Intel vPRO, Telnet/SSH, VNC, and RDP.

Support for Microsoft LAPS

As of Goverlan v9.01.20, Microsoft Local Administrator Password Solution (LAPS) is supported. Using Goverlan Reach, helpdesk engineers and system administrators can enjoy the convenience of a IT remote support solution while security compliance stays tight with MS-LAPS.

Securing Remote Control Access

Once the Goverlan Reach Agents are installed on your machines, Goverlan Reach operators will be able to initiate remote control sessions. By default, an operator must hold local administrative privileges on a machine to remote control it except in the case of “On-Demand” sessions with external machines. On-demand sessions require the exchange of an OTP (“One Time Password”) that is generated by the Goverlan Reach Server and displayed to the end user.

The behavior of Goverlan Reach on the client machine (remote control operating modes) can be configured as follows:

- The remote control session is automatically approved, and a visual notification banner is displayed on the client machine. This notification banner provides information about the administrator and allows the end-user to terminate the session or to send a message to the operator. This is the default behavior.
- The end user is prompted to approve the remote control session before it is started.
- The remote machine is set into a locked state prior to the start of the remote control session.
- Remote control services are disabled on the local machine.
- No visual notification is displayed on the end-users’ machine (Stealth mode).

Additional behaviors can be defined after a remote control session is terminated:

- Set the machine in a locked state.
- Log off the user.
- Display a notification message to the end user indicating that the machine was remote controlled.
- Send a notification email to someone.

Auditing Activities

Accountability and traceability are essential to a remote administration solution. Goverlan Reach registers an audit trace for every action executed by the operator.

Goverlan Reach auditing provides the following information:

- The identity of the administrator who initiated the action (login ID)
- The name and IP address of the machine from which the action originated.
- The identity of the user logged-in to the machine if any.
- The start date & time stamp of the action.
- The end date & time stamp of the action.
- The action that was performed by the operator.

Default Auditing

By default, Goverlan Reach audit traces are registered locally on the remote machine in the application event log.

Centralized and secured auditing can be configured using the Goverlan Reach Server (See: Centralized & Secured Settings Distribution and Auditing)

Centralized & Secured Settings Distribution & Auditing

Goverlan Reach security and auditing settings are centrally configurable and manageable via the Goverlan Reach Server or the Goverlan Reach Group Policy Admin Template.

Global configurations are available such as communication ports, remote control session approval modes and notifications, auditing and many other aspects of control.

Goverlan Reach Gateway Service

The Goverlan Reach Gateway Service is a component of the Goverlan Reach Server. The Gateway Service allows Goverlan Reach Console operators to support systems that are outside of the corporate network. These external endpoints may be equipped with the Goverlan Reach agent and are available for management regardless of their location.

Reach Gateway Security

The Goverlan Reach Gateway Service will require an inbound “Port Address Translation” (Port Forwarding) rule from the internet to the network where the Goverlan Reach Gateway Service is located. This may be a DMZ or other network location.

Since the Reach Gateway Service is required to be exposed to the internet, there are several layers of security that the Goverlan Reach Gateway service employs.

- TLS 1.2 and AES 256 Bit end to end encryption
- Unique Goverlan Account ID verification on both the External Agents and the Reach Gateway Service

External Reach Agent Security

Once the Goverlan Reach Agent has established a connection with your Reach Gateway Service using the above security features, it will also require one of the following:

- A local Windows admin account
- A OTP (One Time Password) that is generated by the Goverlan Reach Server.

On-Demand Sessions

OTPs are generated by the end user and given to the Reach Operator. The Reach Operator then enters the OTP into the Reach Console and is allowed access to the remote system.

The end user also can elevate the session and allow the Reach Operator to access UAC protected areas.

Upon ending the remote assistance session, the end user will be able to review all management tasks that were performed on the local machine during the session.

Conclusion

Goverlan Reach has been designed to fulfill the remote administration needs of many diverse business models while preserving security and integrity. This is done by integrating with the existing security infrastructure instead of adding a proprietary layer of authentication and hosted credential stores.

All communication is encrypted and then authenticated before being processed. All remote executions are audited and can be traced.

Finally, the security settings controlling the behavior of Goverlan Reach can be securely distributed and controlled centrally.

We believe that the level of security provided with the implementation of Goverlan Reach will answer all security requirements. If some security concerns have not been addressed by this document, please ask our support department at www.goverlan.com/support.

Appendix: Technological Summary

Network Ports

Network ports used by Goverlan Reach

22000	Goverlan Reach Agent	Used by the majority of the agent actions.
22100	Goverlan Reach Server (Global Policies & Auditing)	Used by the Reach Console and internal agents for auditing and policy distribution.
15155	Goverlan Reach Server (Gateway Service)	Used by the Reach Gateway Service to bridge connections between Reach Consoles and External Reach Agents.
8081	Goverlan License Server	Used by the Goverlan Reach Server with License Server enabled.
389	LDAP	Used by Goverlan Reach consoles for Active Directory integration.
135	RPC	Used by the Goverlan Reach Consoles for specific remote management tasks.
445	SMB	Used by the Goverlan Reach Consoles to push and manage agent files on endpoints.
53 (TCP or UDP)	DNS	Used by the Goverlan Reach Consoles and agents.
1434,1433	Microsoft SQL Server	Optionally used by Goverlan Reach Consoles and Servers to store data.

Database Technologies

Data Storage

SQLITE	Goverlan Reach Console	Default DB used to store operator data and offline machine data.
LocalDB	Goverlan Reach Server	Default DB used to store Reach Server configuration and audit data.
Microsoft SQL Server	Goverlan Reach Server and Consoles	Alternate DB technology used to store operator, auditing and server configuration data.

Encryption and Verification

- AES 256 Bit Encryption used on all endpoints.
- TLS 1.2 used with all external Reach Agents and Servers via the Goverlan Reach Gateway Service.
- Optional FIPS 140-2 configuration using only FIPS 140-2 approved cryptographic libraries.

Authentication

- Windows SSPI authentication (Kerberos or NTLM supported)
- One-Time-Password exchange (for On-Demand Sessions)