GOVERLAN®
manage complexity simply

Security White Paper

The Goverlan Solution

Goverlan Remote Administration Suite and Goverlan Remote Control software are a part of the Goverlan solution and are powerful remote machine administration and management solutions. The Goverlan solution as a whole is designed to answer the highest security requirements of a corporate network.

The security aspect of the Goverlan solution is addressed in this paper presenting an overview of the security model and architecture implemented in Goverlan, along with its encryption, authentication and authorization mechanisms.

GOVERLAN®
manage complexity simply

Contents

Overview of Goverlan

Stable, Secure & Self-Managed Agent

- Stable
- Secure & Encrypted
- Self-Managed

Understanding how Goverlan authorizes a transaction

- Alternate Credentials
- PKI Compliance - Using Smart Card Logon

Securing Remote Control Access

- Auditing Remote Control Activities

Centralized & Secured Settings Distribution and Auditing

- Ad-hoc security behavior
- Centrally Manage Behavior using a GPO
- Centrally & Securely Manage Behavior and Auditing using the Goverlan Central Server

Conclusion

Overview of Goverlan

The Goverlan solution is a desktop software installed on each operator's machine. Using Goverlan, the operator can perform a comprehensive set of administration tasks on remote machines as well as in Active directory. It does so by communicating with the Goverlan Service Agent which is installed on each remote machine (this process can be automated by Goverlan).

The Goverlan 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 via a remote control session.

Stable, Secure & Self-Managed Agent

The Goverlan solution requires an agent on the remote machines in order to be able to perform remote administration tasks on these machines.

Any new installation on computers is always a great concern for IT as:

- It introduces a new unknown which 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 hack into a system.

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

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

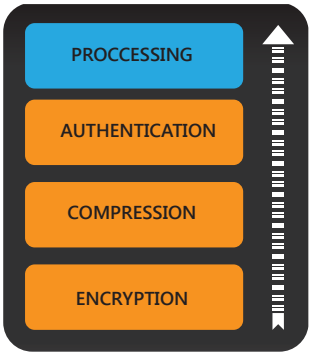
Stable

The Goverlan agents are less than 5MB in size with no external dependencies (for instance the .Net framework). The same agent supports all OS(s) from Windows 2000 to the latest Microsoft operating system (32 & 64 bit architectures).

The Goverlan Service (GovSRV) spends 99% of its time in idle state waiting

for requests from a Goverlan operator. Every 30 seconds, it performs a self-cleaning to release unused memory in order to keep a very low foot print.

Encrypted & Secure



All communications between the Goverlan management console and the Goverlan agents take place via a single TCP port (by default, port 21159) allowing for easy firewall configuration. There is no middle web-service tier involved between the administrator and the client.

To ensure a secure connection and protection against malicious hacking, our communication protocol encrypts all data transmitted between the client and the administrator at the lowest level. Goverlan uses the 128-bit RC4 stream cipher* from RSA Security.

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

Self-Managed

The Goverlan Agents are self managed. You do not need to manually pre-install them on your machines in order to use Goverlan. The installation, maintenance and removal of the agents is automatically performed by Goverlan remotely†.

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

Understanding how Goverlan authorizes a transaction

An important aspect of the Goverlan security model is that it uses the native Windows / 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 user (or specified alternate credentials) and is approved/rejected and audited

* In cryptography, RC4 (also known as ARC4 or ARCFOUR meaning Alleged RC4 is the most widely-used software stream cipher and is used for file encryption in products. It is also used for secure communications, as in the encryption of traffic to and from secure web sites using the popular protocols such as Secure Sockets Layer (SSL) (to protect Internet traffic).

† Remote installation and maintenance of the agents require local administrative privileges and access to administrative shares.

by the native Windows security layer. If a user does not hold the necessary privileges to perform an action, Goverlan simply returns an *Access Is Denied* message. Essentially, Goverlan 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 an 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 a management tasks on a remote machine requires local administrative privileges.

Alternate Credentials

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

Alternate credentials can be configured for individual machines, entire IP ranges, or AD domains.

PKI Compliance - Using Smart Card Logon

Some of our clients, in particular, financial institutions and the U.S. military, have a highly secure infrastructure that uses Public Key Infrastructure (PKI). Smart Card Logon is used exclusively for authentication.

Goverlan fully supports Smart Cards. With Goverlan, you can authenticate and authorize a task using a smart card logon certificate. The Goverlan Remote Control product supports Smart Card Logon Redirection, a process by which the administrator can use his/her local smart card reader to execute an interactive logon on a remote machine via a remote control session.

Securing Remote Control Access

Once the Goverlan Agents are installed on your machines, Goverlan operators will be able to initiate remote control sessions. By default, an operator must hold local administrative privileges on a remote machine in order to remote control it.

The behavior of Goverlan 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

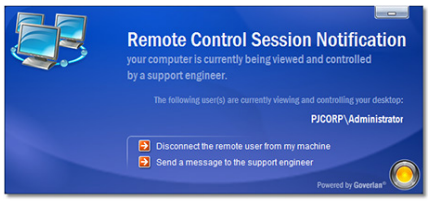


figure 1

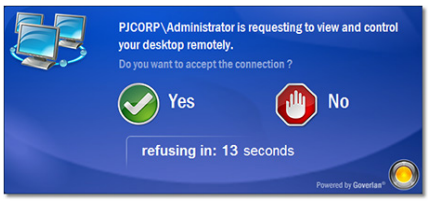


figure 2

notification banner provides information about the administrator and allows the end user to terminate the session, or to send a text message to the operator (figure 1). This is the default behavior.

- The end user is prompted to approve the remote control session before it is started (figure 2).
- 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.
- Logoff the user.
- Display a notification message to the end user indicating that the machine was remote controlled.
- Send a notification email to someone.

Auditing Remote Control Activities

Accountability and traceability are essential to a remote administration solution. Goverlan registers an audit trace for every remote control session executed.

Goverlan Remote Control audits provide the following information:

- The identity of the administrator who initiated the remote control session (login ID)
- The name and IP address of the machine from which the remote control session originated.
- The identity of the user logged-in to the machine if any.
- The start date & time stamp of the remote control session.
- The end date & time stamp of the remote control session.
- Whether or not the remote control session was in stealth mode.

Default Auditing

By default, Goverlan audit traces are registered locally on the remote machine in two locations:

- In the application event log.
- As proprietary information in the registry (which can be queried remotely via the Goverlan Remote Control and Goverlan Management Console products).

Advanced Auditing

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

Centralized & Secured Settings Distribution and Auditing

The behavior to be adopted by the Goverlan solution on the operator and client side is configurable and manageable centrally.

Behaviors dictate global configurations such as communication port, remote control session approval modes and notifications, auditing and many other aspects of controls.

Ad-hoc security behavior

The ad-hoc behavior of Goverlan resulting from a default implementation of this solution is neither loose nor overwhelmingly secure. It is configured to answer the security requirements of most environments:

- Local administrative privileges are required to install/update the Goverlan agents.
- The right to perform Active Directory tasks and remote machine management tasks is granted based upon the Windows account's privileges.
- Local administrative privileges are required to initiate a remote control session. Once authorized, remote control sessions are automatically approved and a visual notification banner is display on the end-user's screen.
- Remote control sessions audits are registered locally on the machines being remote controlled.

Centrally Manage Behavior using a GPO

To centrally configure and manage the behavior of the Goverlan solution across your infrastructure, you can optionally use the provided Group Policy Administrative Template.

The Goverlan GPO allows you to centrally configure every behavioral

aspect of Goverlan on the operator and client side.

You can additionally use the Goverlan GPO to customize most text displayed on the client machines, enabling you to personalize the user interface to include company or department information.

Centrally & Securely Manage Behavior and Auditing using the Goverlan Central Server

If the configuration of global settings via a Group Policy Object does not answer your compliance and security requirements, you can implement the Goverlan Central Server.

The Goverlan Central Server (GCS) allows you to centrally and securely manage behaviors and auditing.

Using the GCS, settings distribution and audit registrations are performed directly from every Goverlan end-point to the Goverlan server using an encrypted channel, bypassing locally configured settings or registry values. These settings and audit traces cannot be tampered with, even by local or domain administrators.

Conclusion

The Goverlan solution has been designed to fulfill the IT needs of many diverse business cultures 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.

Every piece of communication is encrypted and then authenticated before being processed. Every remote control session is audited and can be traced.

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

We believe that the level of security provided with the implementation of Goverlan will answer all security requirements. If some security concerns have not be addressed within this document, please inquire our support department at support@goverlan.com.

Published by

PJ Technologies, Inc.
2655 S LeJeune Road S1001
Miami, FL 33134

www.goverlan.com