Goverlan Reach RC v9

User Guide

What is Goverlan Reach RC

Goverlan Reach RC provides IT Admins with secured Keyboard, Mouse and Video(KVM) control over any remote machine that needs to be managed. The Reach RC module includes multiple connection protocols like RDP. VNC, SSH and Telnet to give admins versatility for the device types they manage in one centralized console.

Getting Started

The Goverlan Client

- Goverlan supports multiple connection protocols, each with its own requirements. The default Goverlan Protocol requires that the Goverlan Client be installed on the remote machine.

  You do not need to pre-install the Goverlan Client, Goverlan can automatically install and maintain the Client on-demand. (See Understanding the Goverlan Client). This is executed via Windows Print & File Sharing on your client machines (C$/ADMIN$ & Port 445). A standalone setup package is available in the installation directory of Goverlan for manual installation (See Installing the Goverlan Client & Goverlan Agent Installer Resource Kit).

- By default, Goverlan uses Port 22100 to communicate directly with the Goverlan Client after installation. If a firewall exists between your machine and the remote machine, the firewall must be configured to allow the Goverlan Client port communication. This default port is also configurable if you prefer a different port. (See Configuring Windows Firewall & Changing the Default Goverlan Client Port.)

- Goverlan Reach functionality is built into the Goverlan Client, as long as the Goverlan Reach infrastructure is configured. For more information refer to the Goverlan Reach section.

Authorization & Authentication

- By default, only users holding local administrative privileges on a remote machine are authorized to initiate a remote control session (to grant access to non-local admins, see Configuring Authorization).

- Goverlan automatically uses your credentials when authenticating to the remote machine. If you are executing a task that requires privileges higher than those you hold, Goverlan will automatically prompt you for alternate credentials Goverlan Credential Manager.

Detecting your user's logged-in workstations with fastConnect

Instantly access user machines via username without the need of knowing their machine name. The following prerequisites are needed for this feature to function properly:

© Copyrights Goverlan Inc. – All Rights Reserved

- Your Active Directory User accounts must be configured with a roaming profile (accessible by the Goverlan operators). If no roaming profile is configured, then you need to create a Goverlan Central Data Repository.
- The Goverlan Client must be installed on your client machines. The Client monitor login/logout events and register the historic information used for the detection.

Branding and Configuring Goverlan Client Behavior

- Client Side behaviors are fully configurable. By default, an authenticated remote control request is automatically authorized and a visual notification banner is displayed. You can configure other behaviors to meet company guidelines and requirements. (See Customizing Goverlan Client Behavior)
- Most Goverlan user interface elements displayed on your client machines can be branded with your own text and images. (See Branding Reach RC)

Making your first connection

There are multiple ways to initiate a remote control session:

- By Computer name (Short, FQDN) or IP Address. (See Making your first Goverlan Reach RC Connection)
- By Username via our fastConnect feature, which takes out the need to ask your user for machine information. (See Using fastConnect for User Workstation Detection)
- By Reach node/site name (See Accessing Reach nodes)

Smart Card Redirection and FIPS 201 compliance

Goverlan Reach RC will allow users to supply smart card credentials to a remote system that is FIPS 201 compliant. Goverlan supports both T0 and T1 (PIV, Common Access Card, etc…) protocols and will work with any PKI compliant infrastructure using smart cards.

Goverlan Reach RC accomplishes this by using the Goverlan Smart Card Reader Driver on the remote machine. This driver and the Goverlan Client must be installed on the remote system before any smart card authentication can be used.

- Installing the Goverlan Smart Card Redirection Driver on a remote system
- Working with Smart Card Redirection

Supported Goverlan Connection Protocols

Goverlan Reach RC supports multiple protocols that connect to a wide array of devices. Here is a list of all supported protocols:

- Goverlan Proprietary Protocol (GPP)
- Intel® vPRO™

© Copyrights Goverlan Inc. – All Rights Reserved

- Microsoft RDP
- VNC
- Telnet/SSH
- Windows Remote Command Line

Helping users outside of your organization with Goverlan Reach

With Goverlan Reach, you will be able to remote control any machine that is not on your internal LAN and connected to the internet. (See Goverlan Reach)

Starting a Remote Control Connection

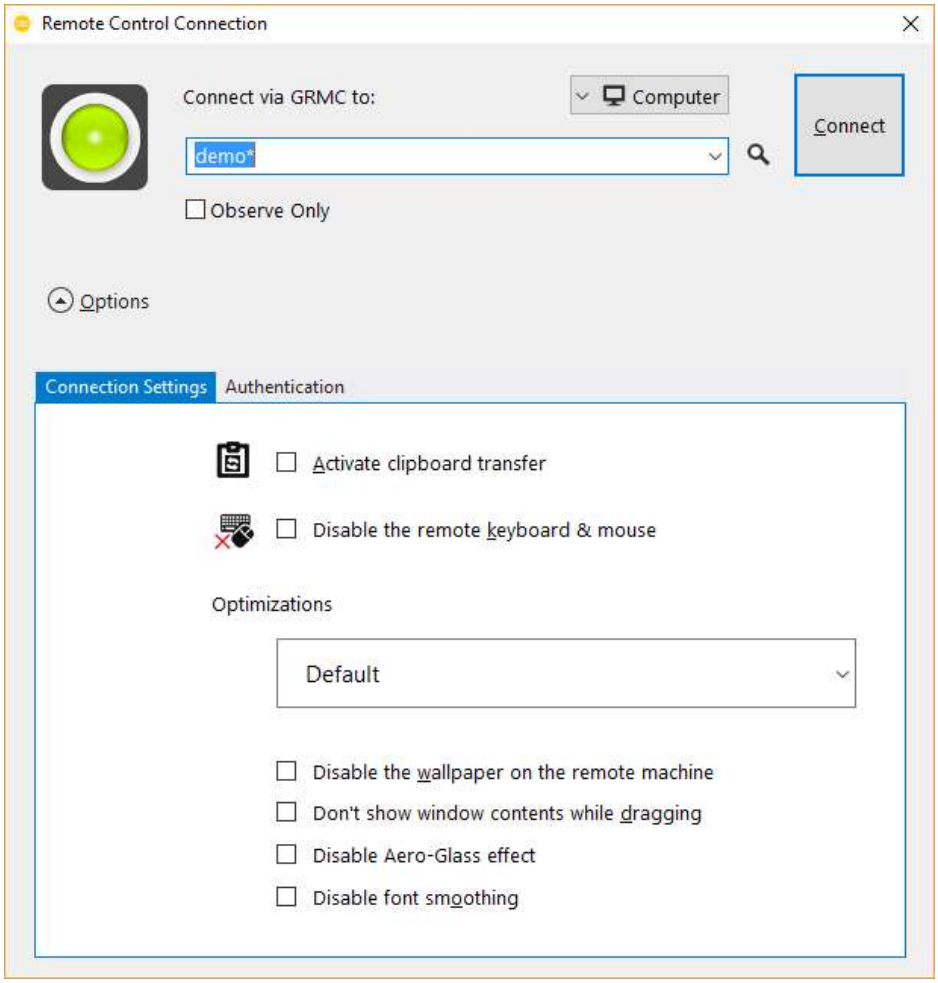
Goverlan Reach RC makes it easy to start helping users. To make a Goverlan Reach RC connection with the Goverlan Proprietary Protocol (GPP), the remote Windows computer must have the Goverlan Client installed. For more information, see Installing the Goverlan Client.

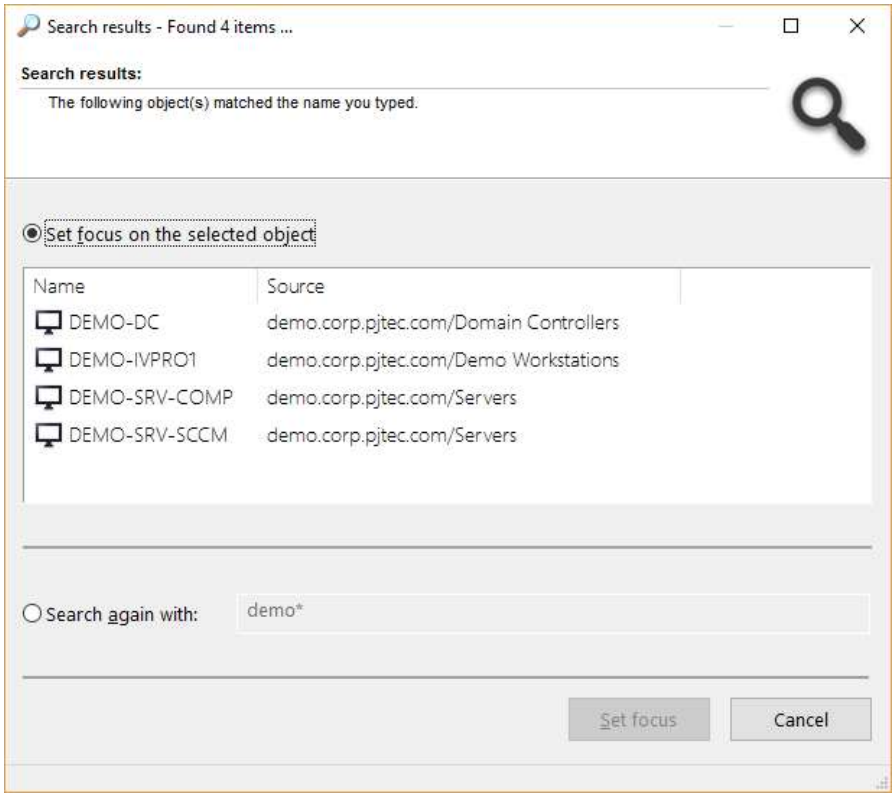
Connecting to a remote computer by computer name or IP address

Locate and click the Connect button in the center of the screen.

Enter the name of the computer or its IP address.

© Copyrights Goverlan Inc. – All Rights Reserved



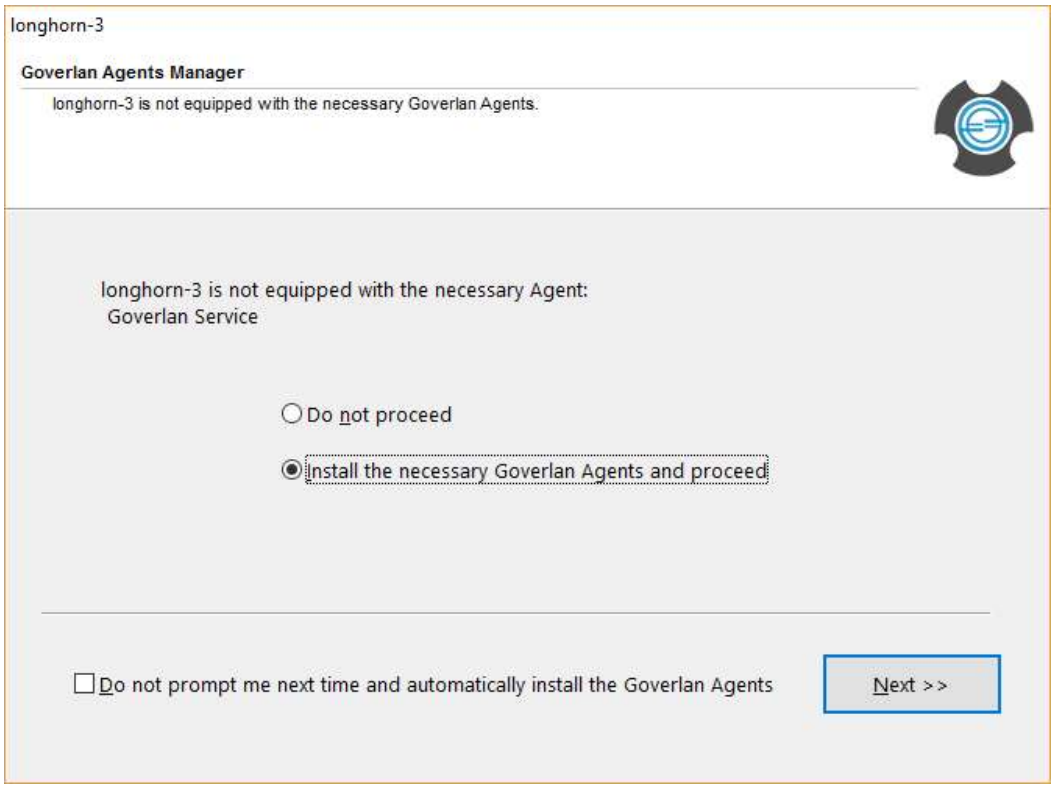


NOTE: The "Connect via" box supports wildcard searches. Enter the partial name of a target computer Active Directory (AD) account name and Goverlan will find it in the directory.

© Copyrights Goverlan Inc. – All Rights Reserved

Once you have found the computer you wish to connect to, choose any of the optimization settings you require and click Connect.

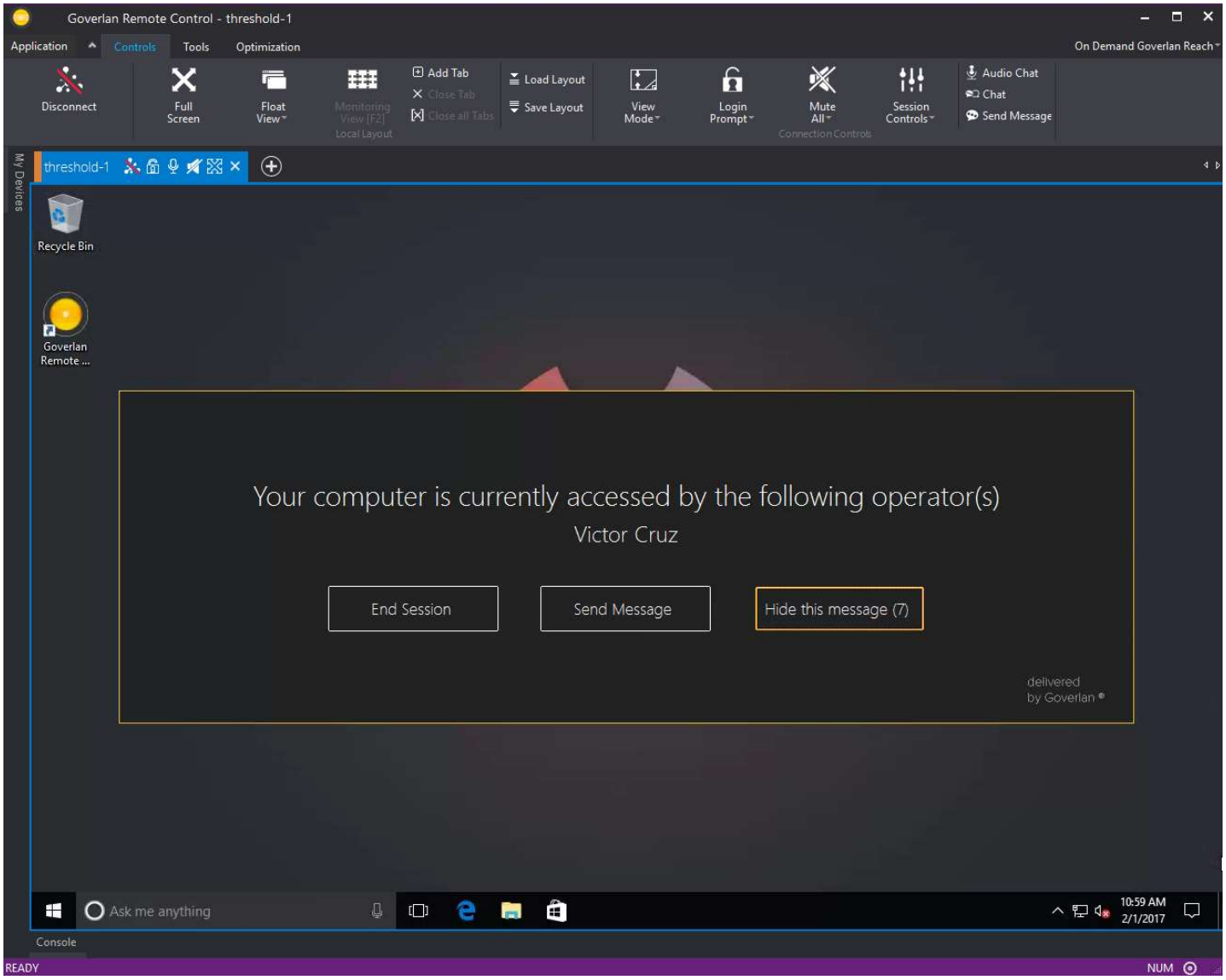
If the Client is not installed, Goverlan will ask to install it.



Click Next to proceed.

The Goverlan Client is now installed and your remote control session will start.

© Copyrights Goverlan Inc. – All Rights Reserved



Notification Banner

Once connected to a target for the first time, the user will see a notification banner. The image and text on this banner can be customized. For more information, see Branding Goverlan Reach RC.

User Notification Options

Goverlan Reach RC supports several Pre and Post Session Actions including User Acceptance, Email Notifications and more. For more information, see, Controlling Client Behavior.

REFERENCES

- Installing The Goverlan Client
- Configuring the Central Data Repository
- Branding Goverlan Reach RC
- RDP and Citrix Shadowing

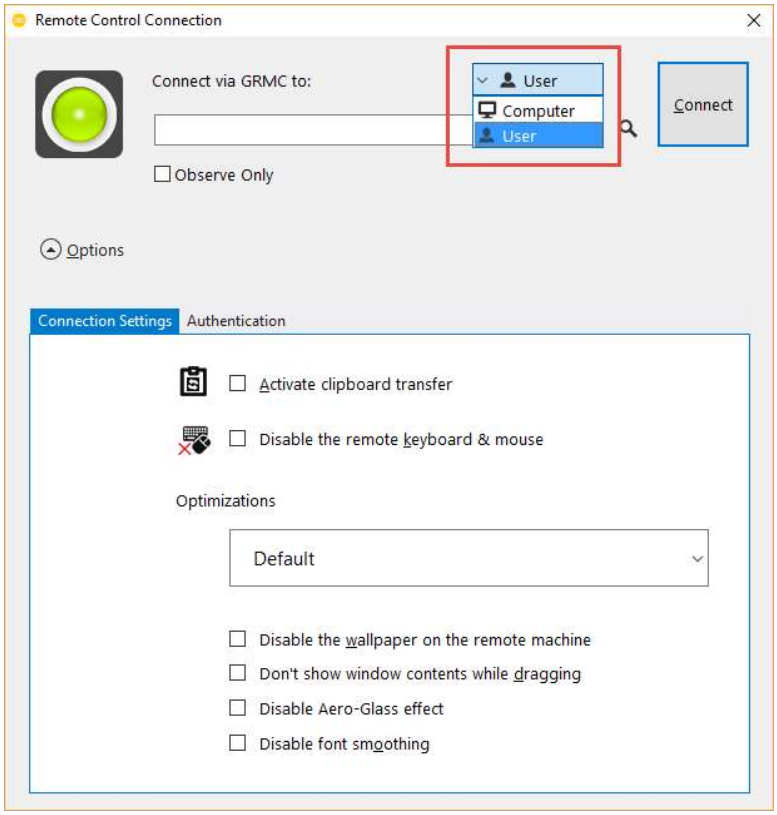
© Copyrights Goverlan Inc. – All Rights Reserved

Starting a Remote Control Connection using *fast*connect

Goverlan fastConnect allows you to discover all the login sessions of any user with an Active Directory account and select the one you wish to control. To configure fastConnect, see Configuring the Central Data Repository.

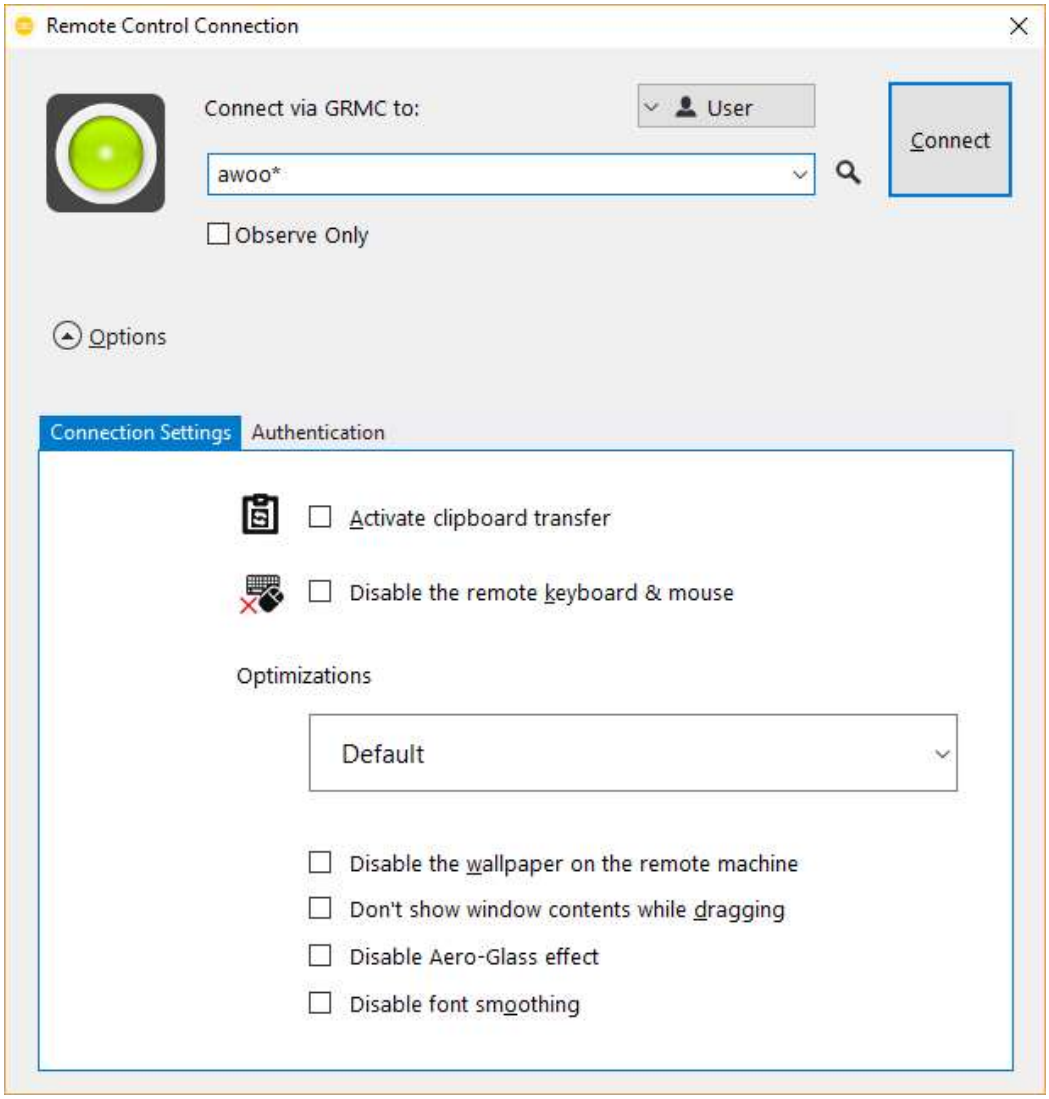
- Locate and click the Connect button in the center of the screen.

- Select "User" from the drop down.



- Enter the name of the user you wish to help.

© Copyrights Goverlan Inc. – All Rights Reserved

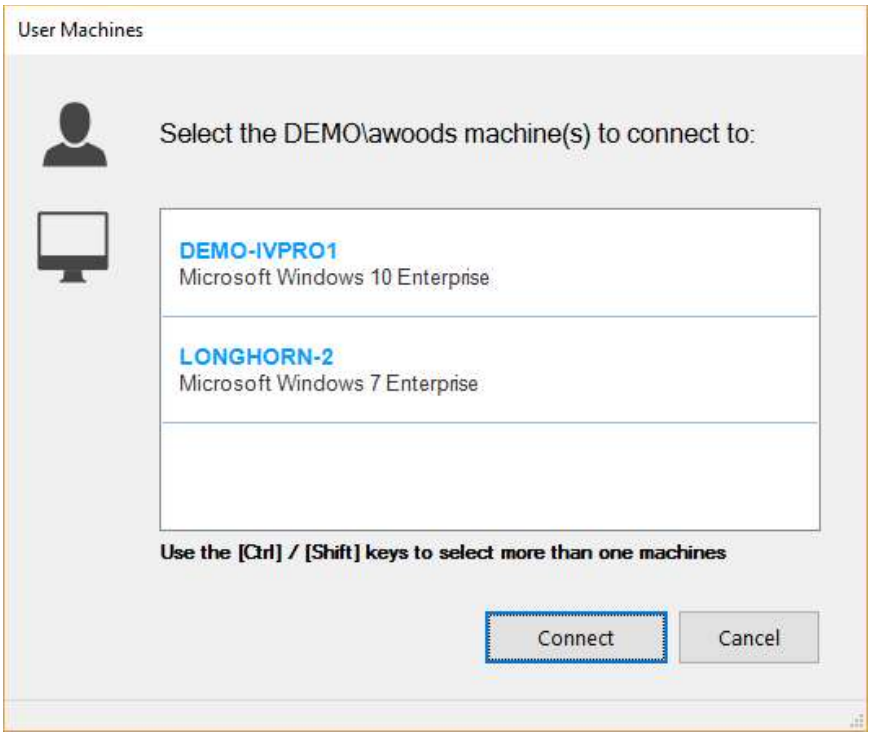


NOTE: The "Connect via" box supports wildcard searches. Enter the partial name of a user AD account and Goverlan will find the account in the directory.

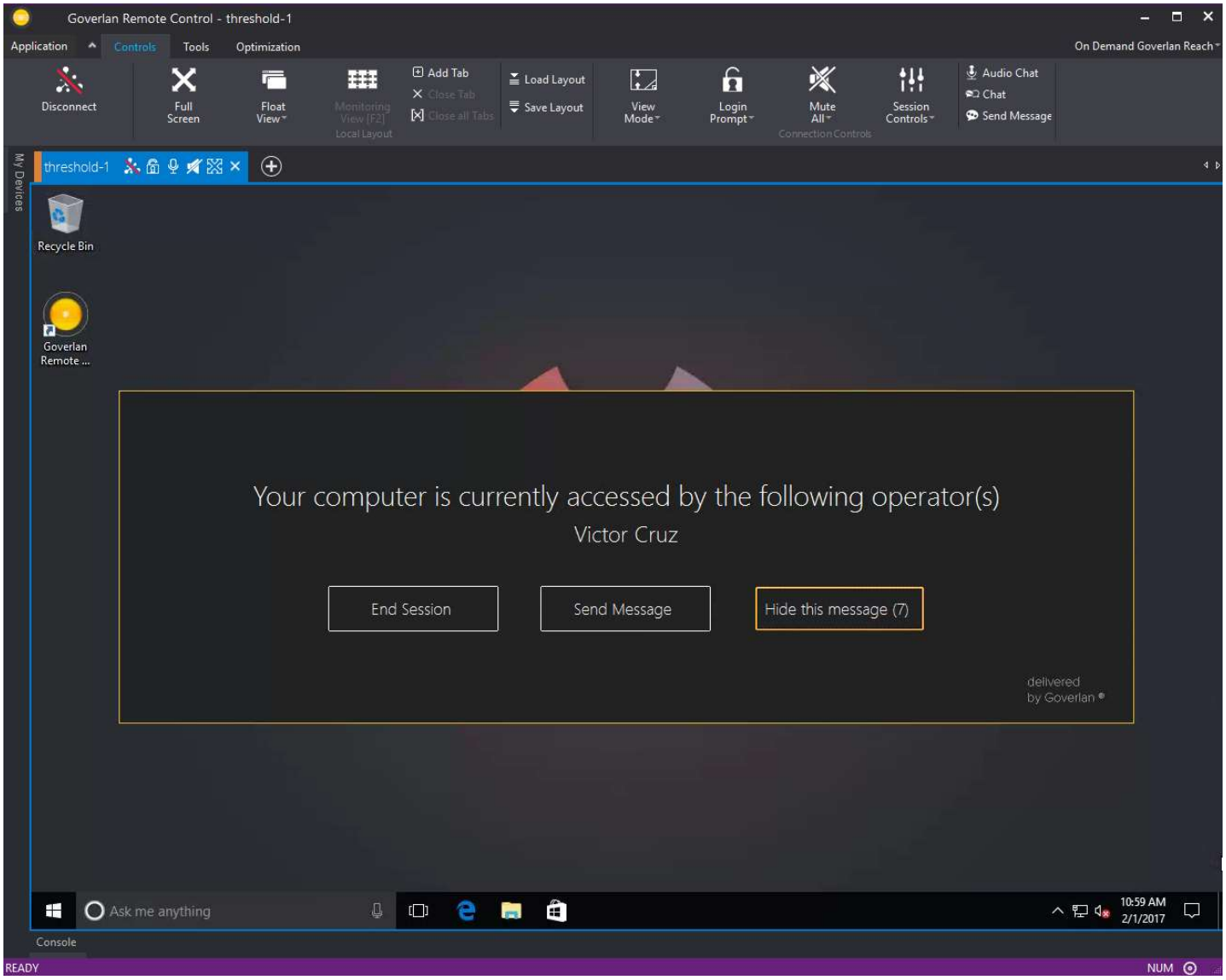
- Goverlan will display a list of log on sessions for that user. These can be any physical session or RDP/Citrix session. For more information about shadowing user sessions see, RDP and Citrix Shadowing.

© Copyrights Goverlan Inc. – All Rights Reserved

- Select the session you wish to control and click Connect.



© Copyrights Goverlan Inc. – All Rights Reserved



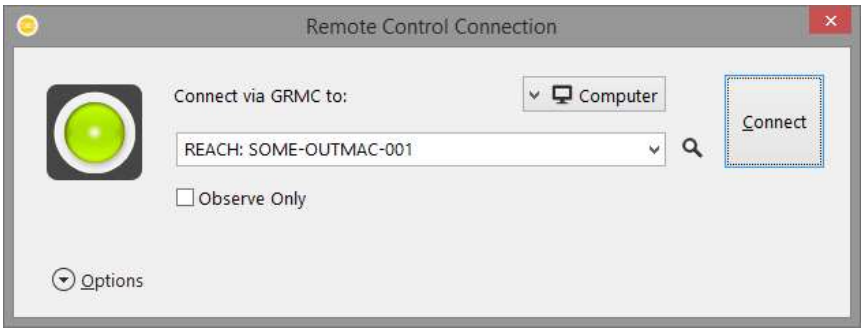
Starting a Remote Control Connection using Goverlan Reach

Goverlan Reach allows you to access nodes that are outside of your internal LAN through the internet. For more in-depth information on Reach refer to the Goverlan Reach section in this guide.

- Locate and click the Connect button in the center of the screen.

© Copyrights Goverlan Inc. – All Rights Reserved

- Enter the prefix REACH: followed by the node name or search string. For instance, to open a remote control session to an external Goverlan Reach machine named: **SOME-OUTMAC-001**, enter:



The connection string above assumes that **SOME-OUTMAC-001** is registered to the root of the Goverlan Reach Repository. However, most Goverlan Reach nodes will use an organization name or their local Active Directory Domain information to register themselves.

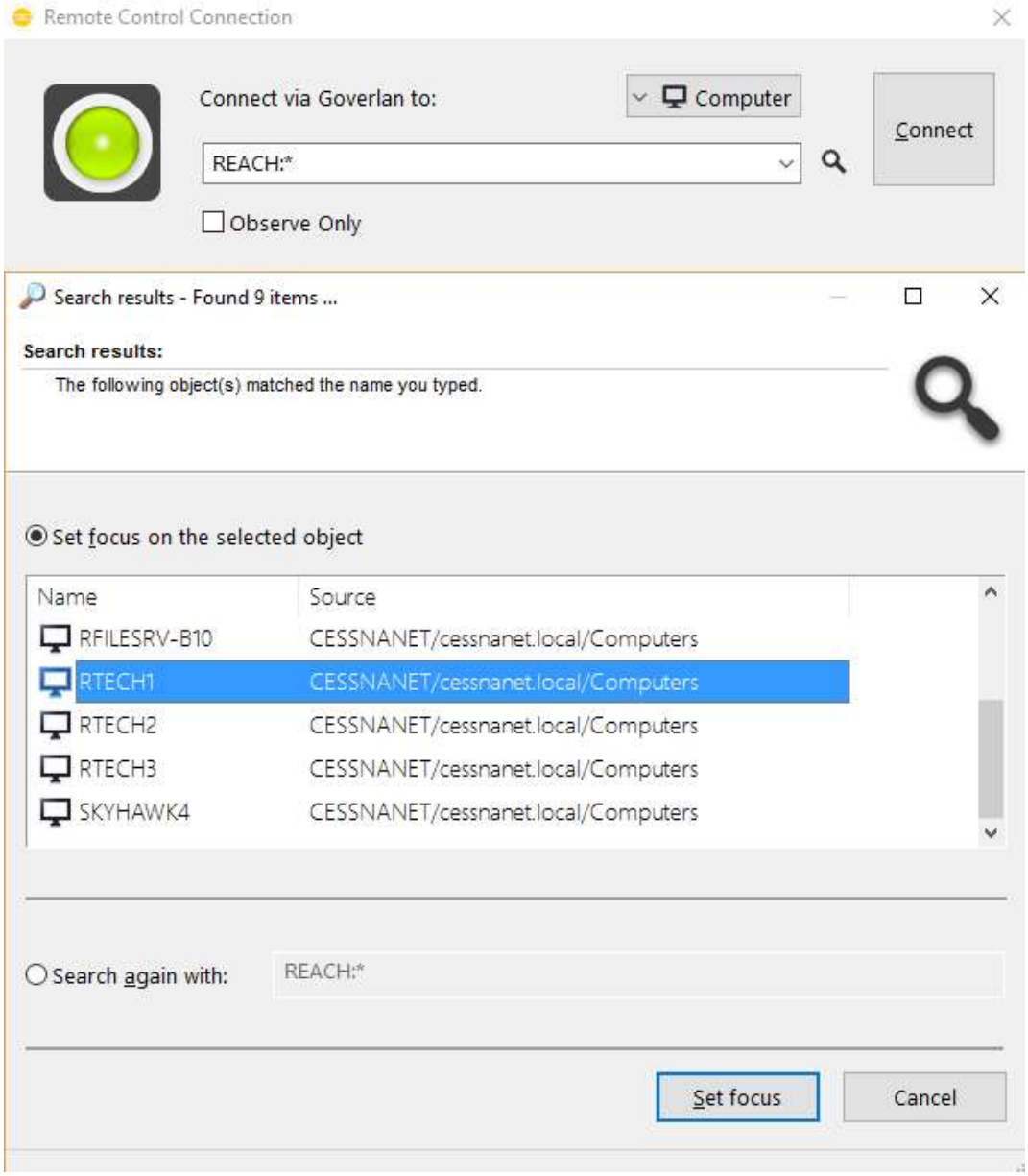
If the exact path of a Goverlan Reach node is not known, the node can be searched for using the ***** wild card character in the connect string. For instance, enter **REACH: SOME-OUTMAC-001*** and a search for SOME-OUTMAC-001 will be initiated, irrespective of its location within the Goverlan Reach Repository.

Other search examples:

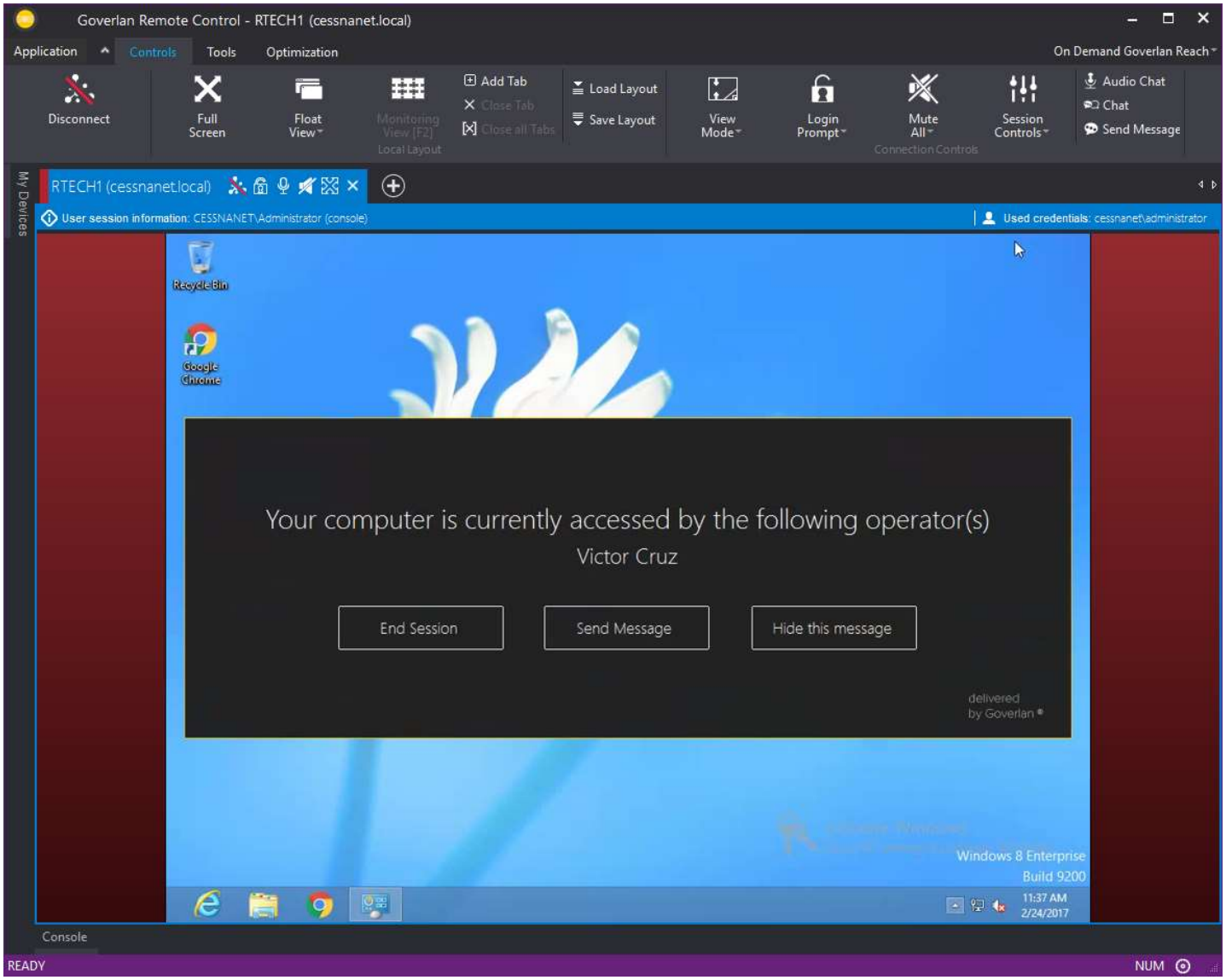
REACH:*	Returns the entire repository
REACH:CLIENT-ORG/*	Returns all machines registered in the *CLIENT-ORG* container
REACH: Domain Controllers*	Returns all machines registered in any Active Directory container titled *Domain Controllers* across all client sites.

© Copyrights Goverlan Inc. – All Rights Reserved

- Double-click the Reach node to initiate the connection



© Copyrights Goverlan Inc. – All Rights Reserved



RDP and Citrix Shadowing

Use Goverlan Reach RC to connect to any terminal server based connection. This includes RDP, RDS or Citrix XenApp session. Shadowing allows you to share the same session as the user, see what the user sees, and assist with applications or session specific issues such as drive or printer mappings.

Pre-requisites for Session Shadowing

To shadow sessions with Goverlan, the Goverlan Client must be installed on any server that hosts logon session. For RDS environments, this will be the Remote Desktop Session Host (RDSH) servers. In XenApp

© Copyrights Goverlan Inc. – All Rights Reserved

environments, this will be the Presentation servers. For more information about The Goverlan Client, see Installing The Goverlan Client.

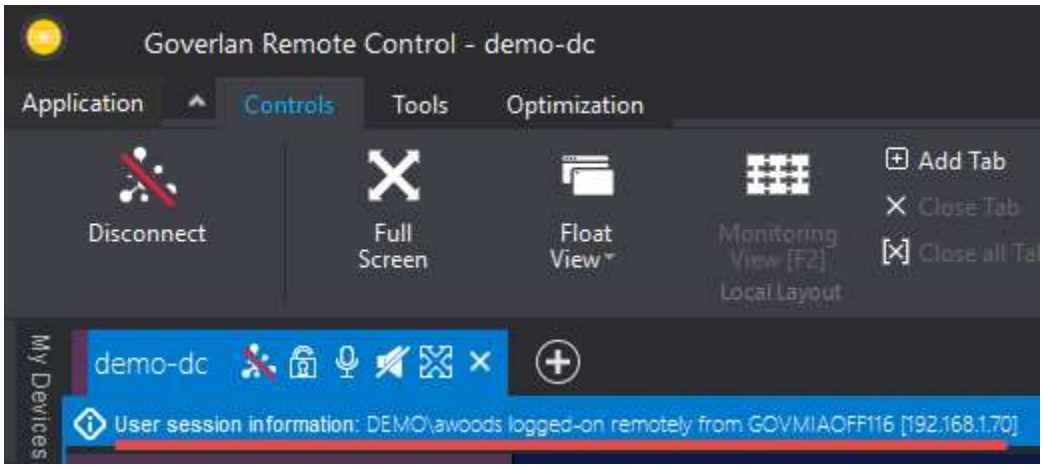
Use fastConnect to find logon sessions

fastConnect can tell you where any user is logged in. This will include any RDSH server or Presentation server that has the Goverlan Client installed. For more information about fastConnect, see Getting Started with Goverlan Reach RC.

You will be placed into the session once a server from the fastConnect list has been selected. You will be able to share mouse and keyboard control and see what the user sees. The Goverlan operator will also be able to see the entire desktop of users who are in seamless mode during RDP or Xen sessions. This will allow the operator to see hidden error messages, adjust mapped drives, see mapped printers or manage any profile specific settings.

Session Status

View session details in the **User session information** section.



Session Select Screen

Click the **User session information** link. This will show the session select screen. The session select screen will display a list of all logon sessions on that server. Click on any logon session to control it as well as the physical console.

REFERENCES

- Installing the Goverlan Client
- Getting Started with Goverlan Reach RC

Performance Monitoring

© Copyrights Goverlan Inc. – All Rights Reserved

Goverlan Reach RC will allow you monitor several Windows computers with an "At-A-Glance" view of all your concurrent remote control session. For more in-depth monitoring on a per machine basis, refer to the Goverlan Task Manager.

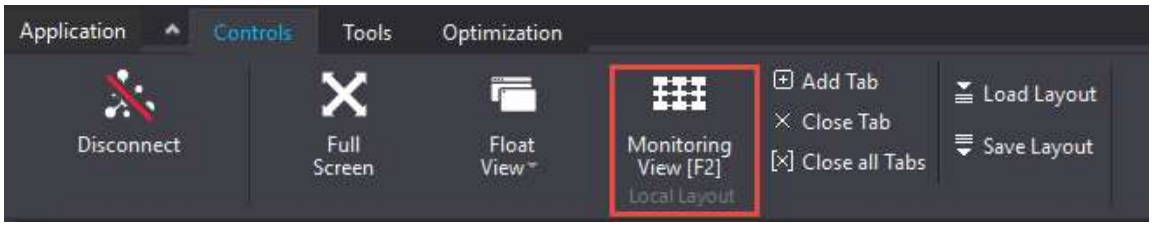
Setting up Monitoring View

Monitoring view is a powerful "Single Pane" monitoring view, which allows you to select several computers, connect to them via a predefined connection protocol and see them in one easy to use workspace.

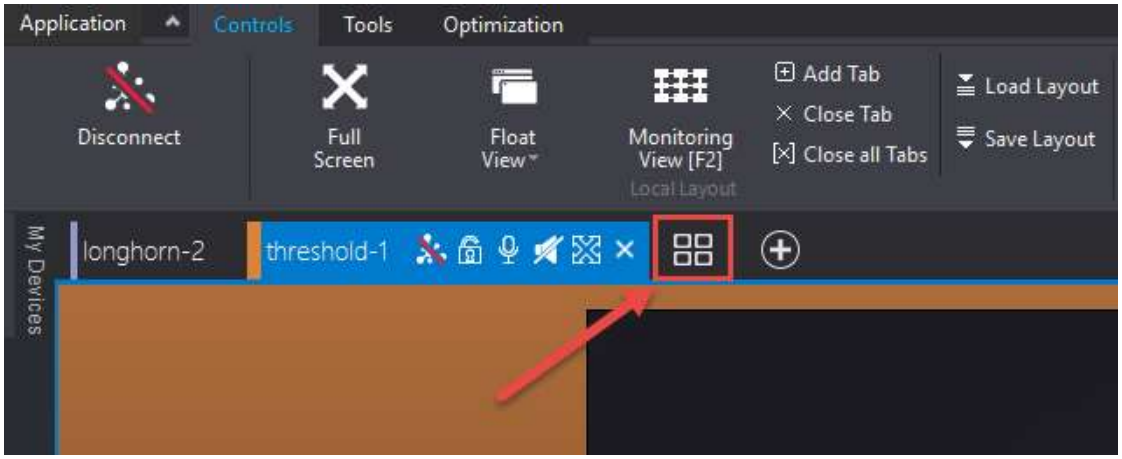
Creating a Monitoring View from a few open connections

Using the Connect button or the Favorites view, open as many connections as you like in Goverlan Reach RC. For more information, see Basic Controls.

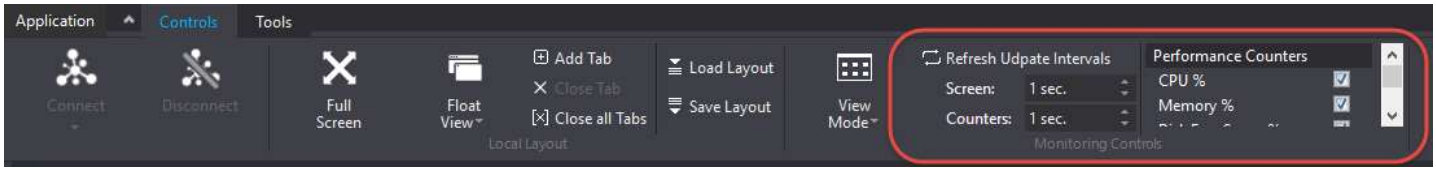
Once you have more than one connection in Goverlan Reach RC, the Monitor View option becomes available in the Main Tab of the Command Bar.



Note: You can also start Monitoring View with a special tab.



When Goverlan Reach RC is in Monitoring View, the Command Bar shows the Monitoring View Controls. Use these controls to add or remove performance counters or control the update speed of the live thumbnails and performance counters.

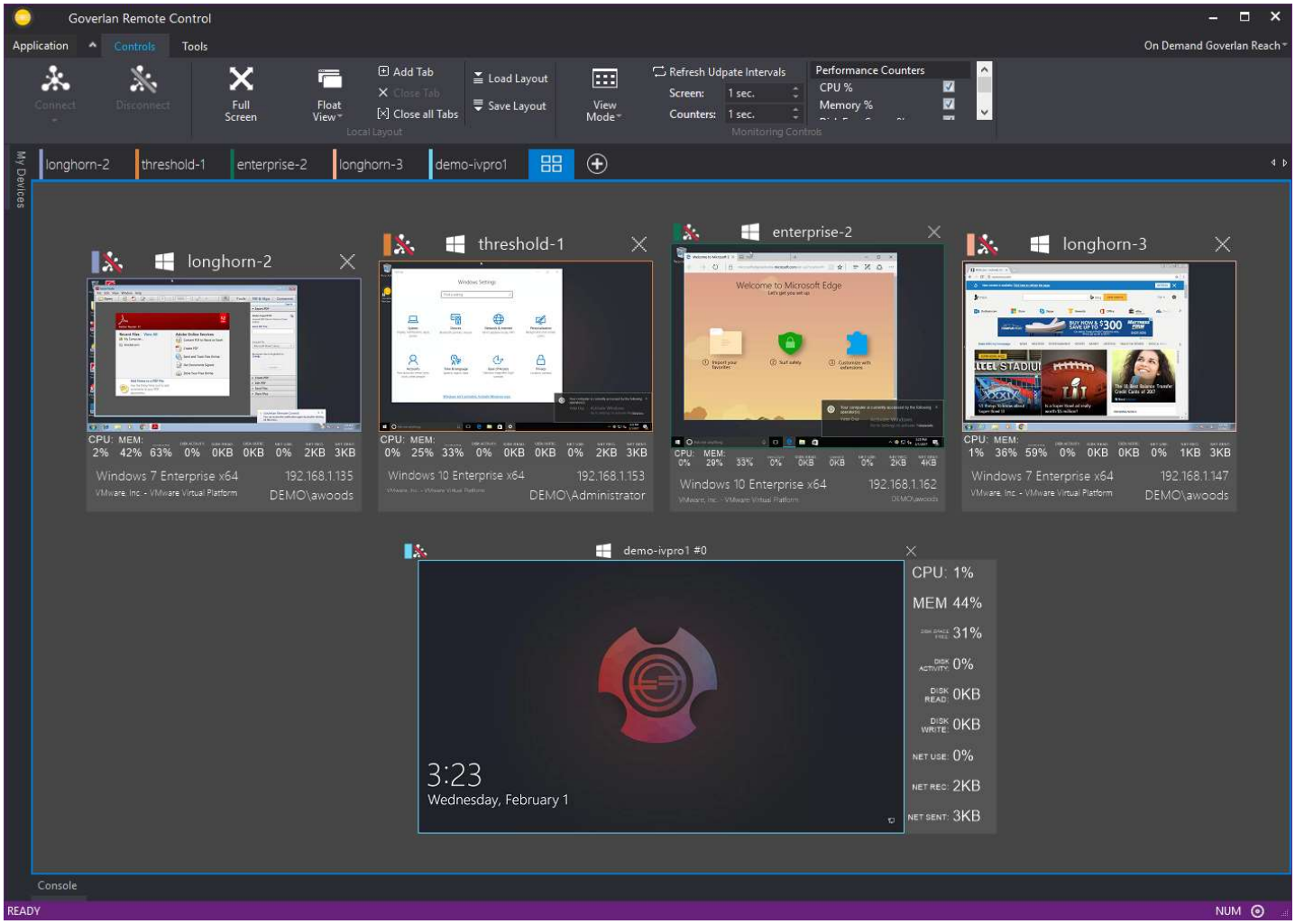


See Managing your Workspace for instructions on how to save Monitoring View layouts and reloading them.

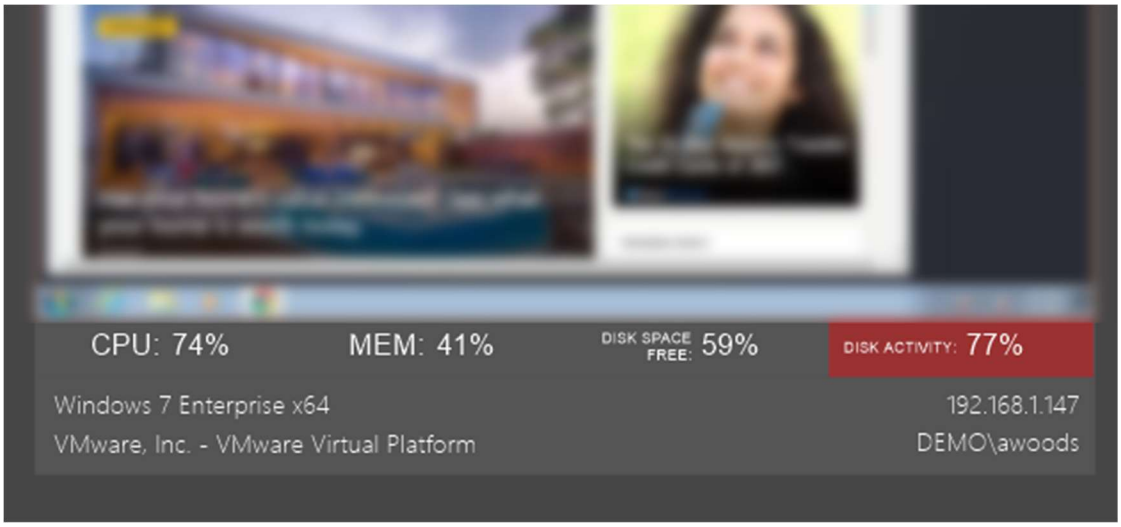
© Copyrights Goverlan Inc. – All Rights Reserved

Observing Monitoring View Counters

Once you have Monitoring View set up you can begin looking at various performance counters displayed below each thumbnail view of any connected system.

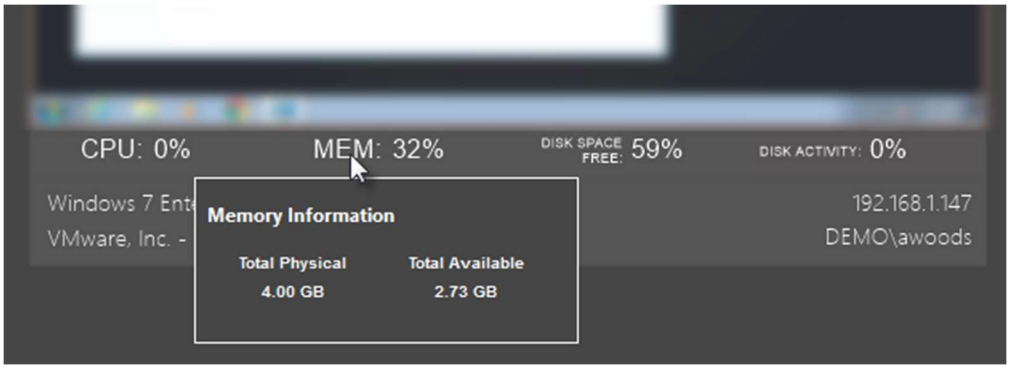


The performance counters are displayed in a heat map format. Resources that are working harder will be displayed in a heavier color so they can be easily identified if there is an issue.



You can mouse over any performance counter for more information about that resource.

© Copyrights Goverlan Inc. – All Rights Reserved



REFERENCES

- Basic Controls
- Managing your Workspace

Auditing Remote Control Events

Goverlan Reach RC sessions are logged for auditing purposes.

What information is logged during a remote control session?

The following information is captured during a remote control session.

Client	Client User	Start Time	End Time	Admin User	Admin Machine	Session ID	Misc

- Client - The target computer that is being controlled
- Client User - The logged-in user. This can be the console user or an RDP/Citrix session
- Start Time - The time the remote control session was started
- End Time - The time the remote control session was ended
- Admin User - The Goverlan operator
- Admin Machine - The computer that the Goverlan operator is logged in to
- Session ID - The logon session of the target user
- Misc - This column represents

Where can Audit information be found?

The Goverlan Client is responsible for logging remote control sessions. Information is recorded in several locations for redundancy and flexibility.

© Copyrights Goverlan Inc. – All Rights Reserved

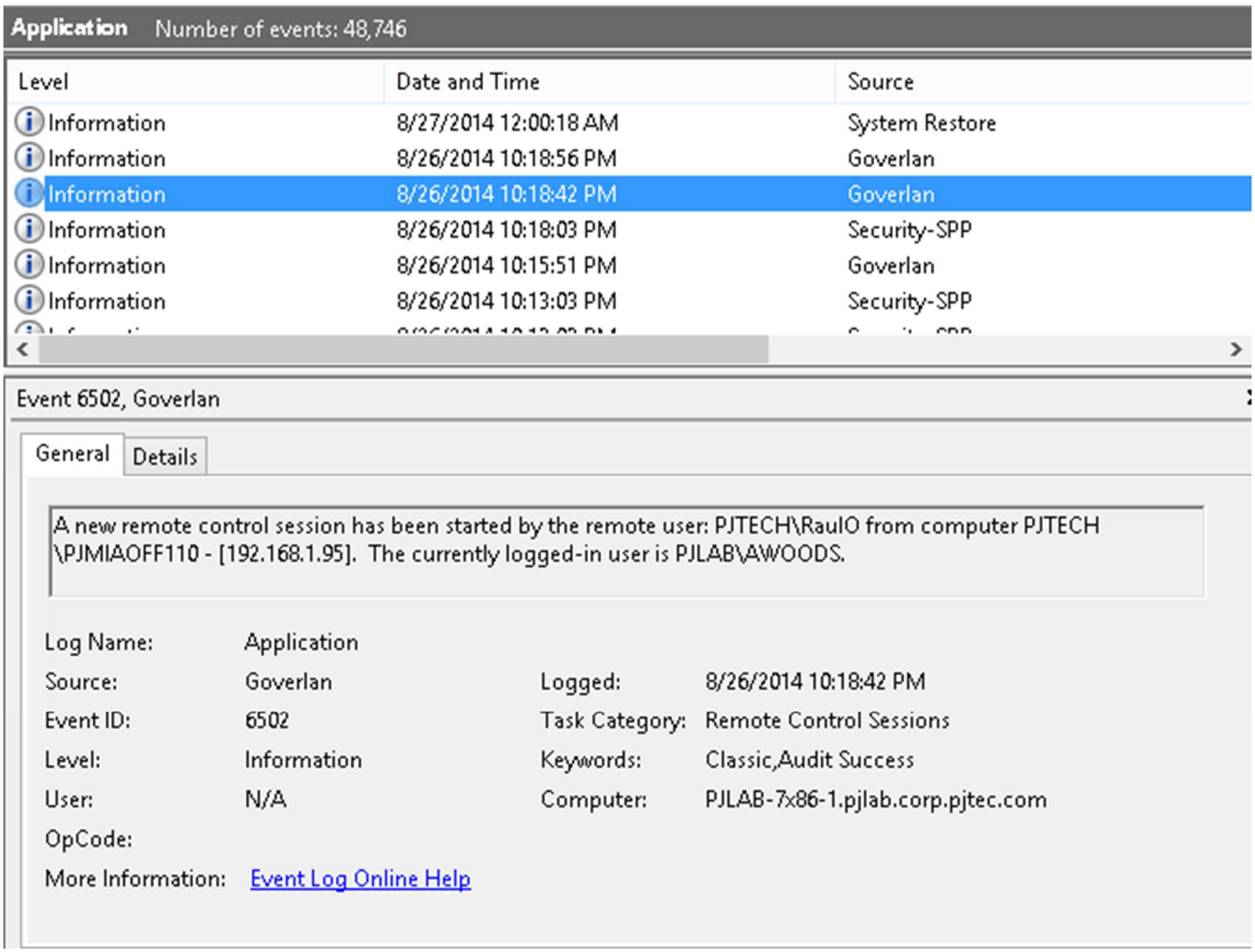
Audit information is stored in the following locations:

- Windows Application Event Log (on the target workstation)
- Goverlan Client proprietary log
- Goverlan Reach Server

Windows Application Event Log

By default, the Goverlan Client logs event 6502 in the Application log.

When the session is ended, the Goverlan Client will log event 6505.

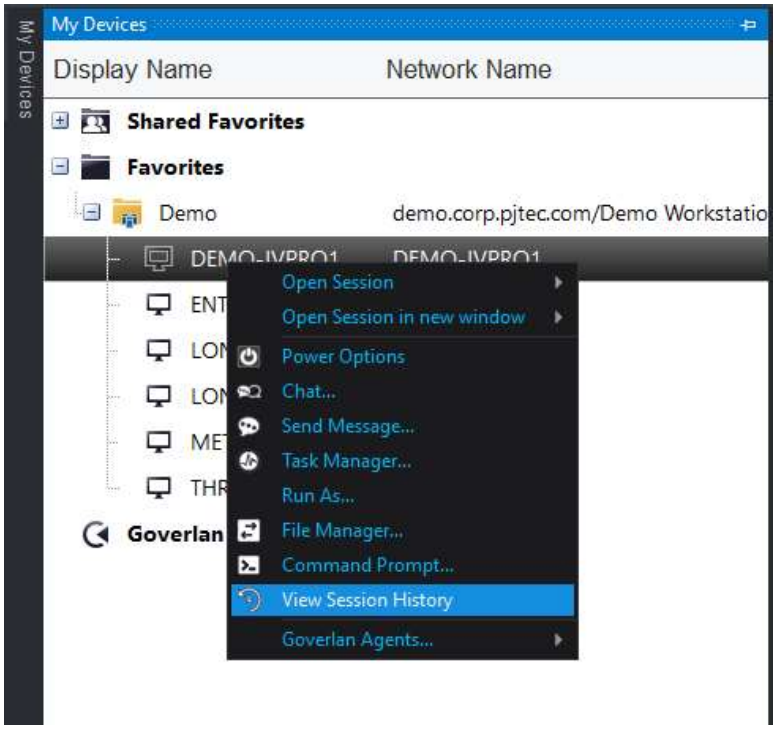


Goverlan Client proprietary log

The proprietary log is maintained by the Goverlan Client and can be accessed from the Goverlan Reach RC UI.

Access the log from the Favorites section. Right click any workstation and select View Session Log.

© Copyrights Goverlan Inc. – All Rights Reserved



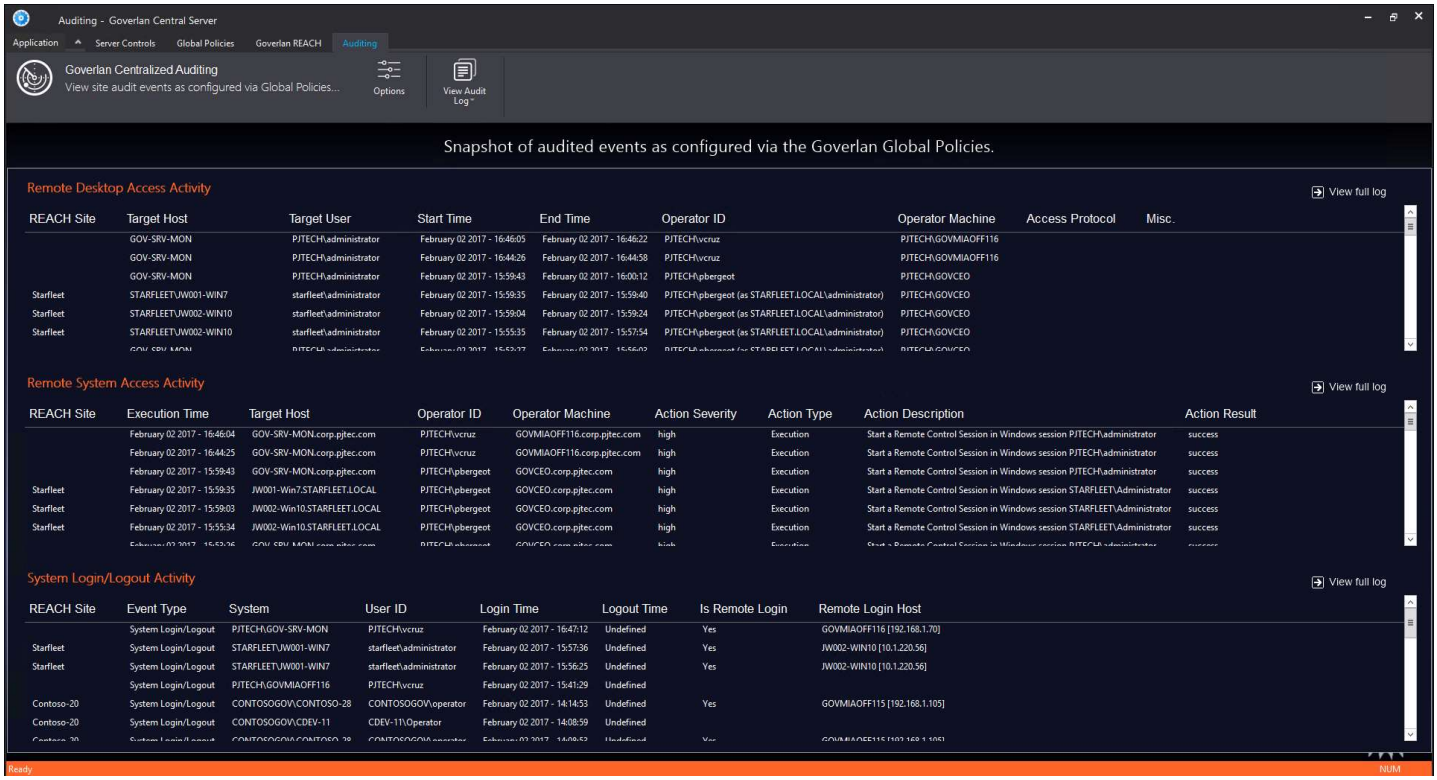
The Goverlan Session History is an audit log of all remote-control events that took place on the target computer.

The Goverlan Reach Server

The Goverlan Reach Server will automatically collect Remote Control logs and centrally store them. For more information about the Goverlan Reach Server, see Introduction to the Goverlan Reach Server.

In the Goverlan Reach Server console, click on the Audit tab on the Command Bar to view the real-time audit log. For more information on this screen see, Utilizing the Centralized Auditing Feature.

© Copyrights Goverlan Inc. – All Rights Reserved



Storing Goverlan Client logs on a custom network share

Goverlan Reach RC logs can be stored on a custom network share. Custom shares can be used to backup or centralize logs when there is no Goverlan Reach Server present.

Configuring a Custom Share for Remote Control logging

Configure a network share on your network where Users have Read and Write access. Goverlan users must have at least read access to the share.

There are three options for configuring the Goverlan Client to use the network share for storing logs.

- Goverlan Administrative GPO
- Goverlan Reach Server Policy
- Goverlan Scope Action

Goverlan Administrative GPO

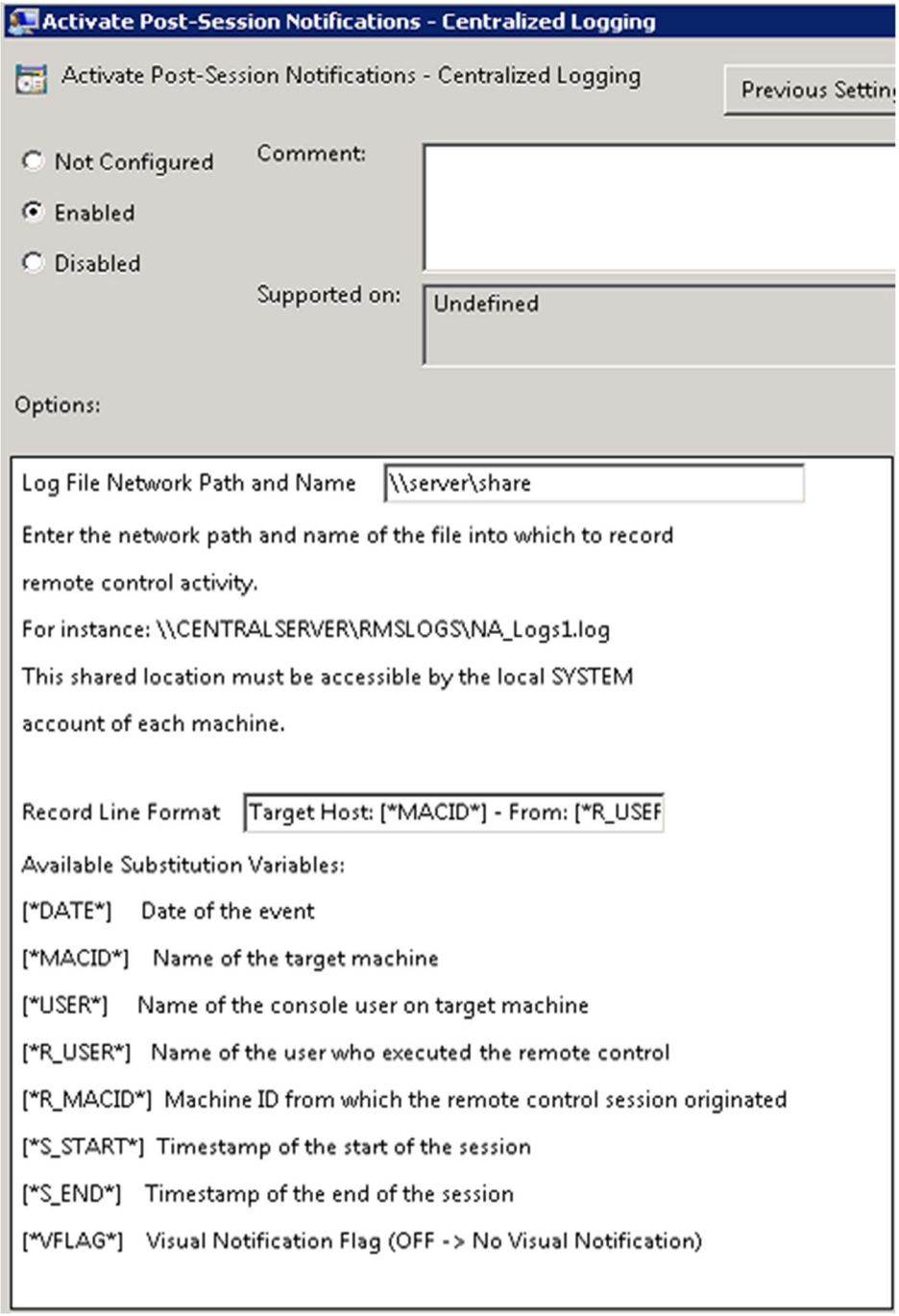
The Goverlan Administrative GPO can be used to push policies and settings to The Goverlan Client. For more information, see the Goverlan Administrative GPO Template.

Locate the following policy in the GPO Policy

Computer Configuration → Policies → Administrative Templates → Goverlan Universal Settings → Remote Control Client Settings

Using the Goverlan Admin GPO allows you to also reconfigure the format of the log.

© Copyrights Goverlan Inc. – All Rights Reserved



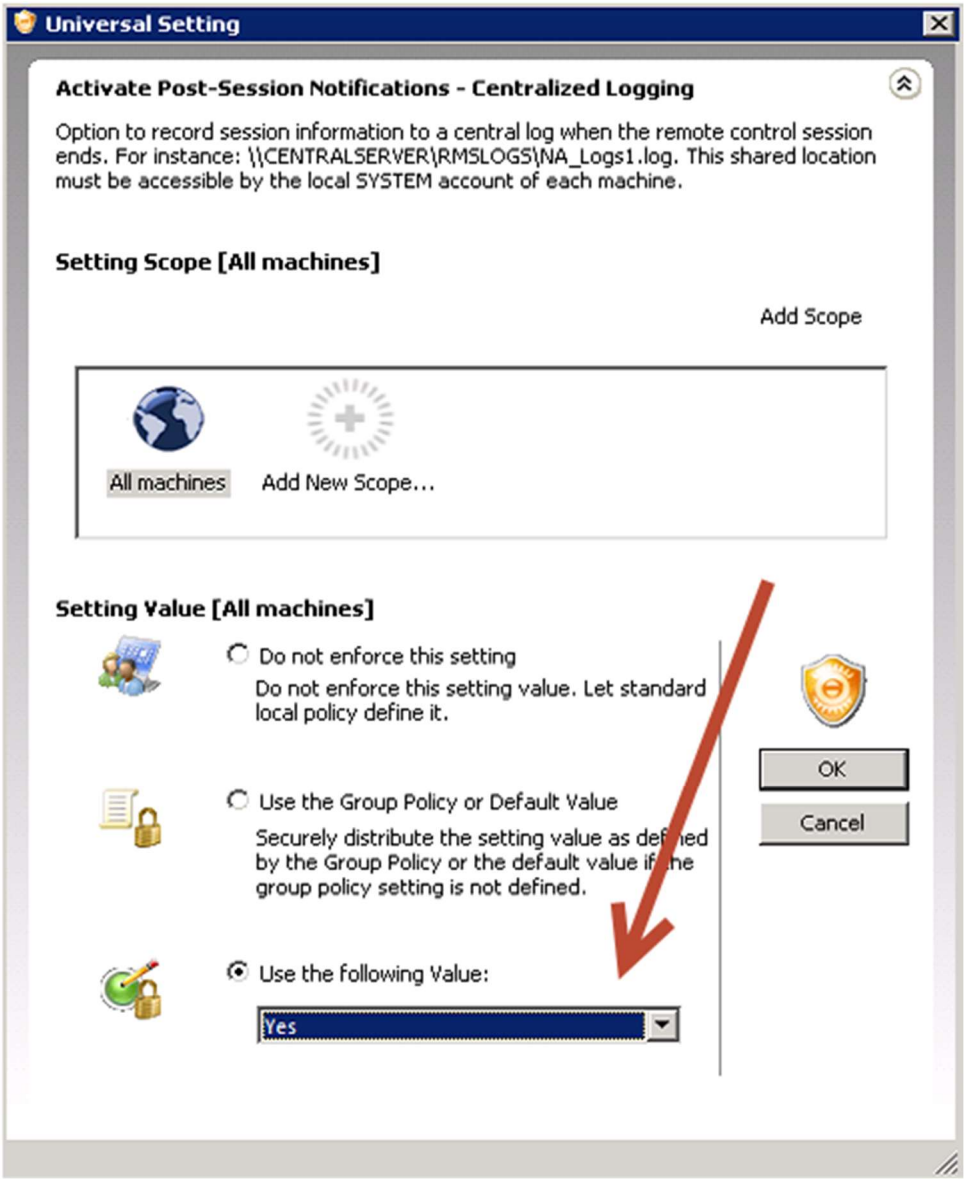
Goverlan Reach Server Policy

Use the GRS to set a policy for the custom location. For more information about Universal Settings Distribution Policies, see Using Universal Settings Distribution.

Configure the following policies

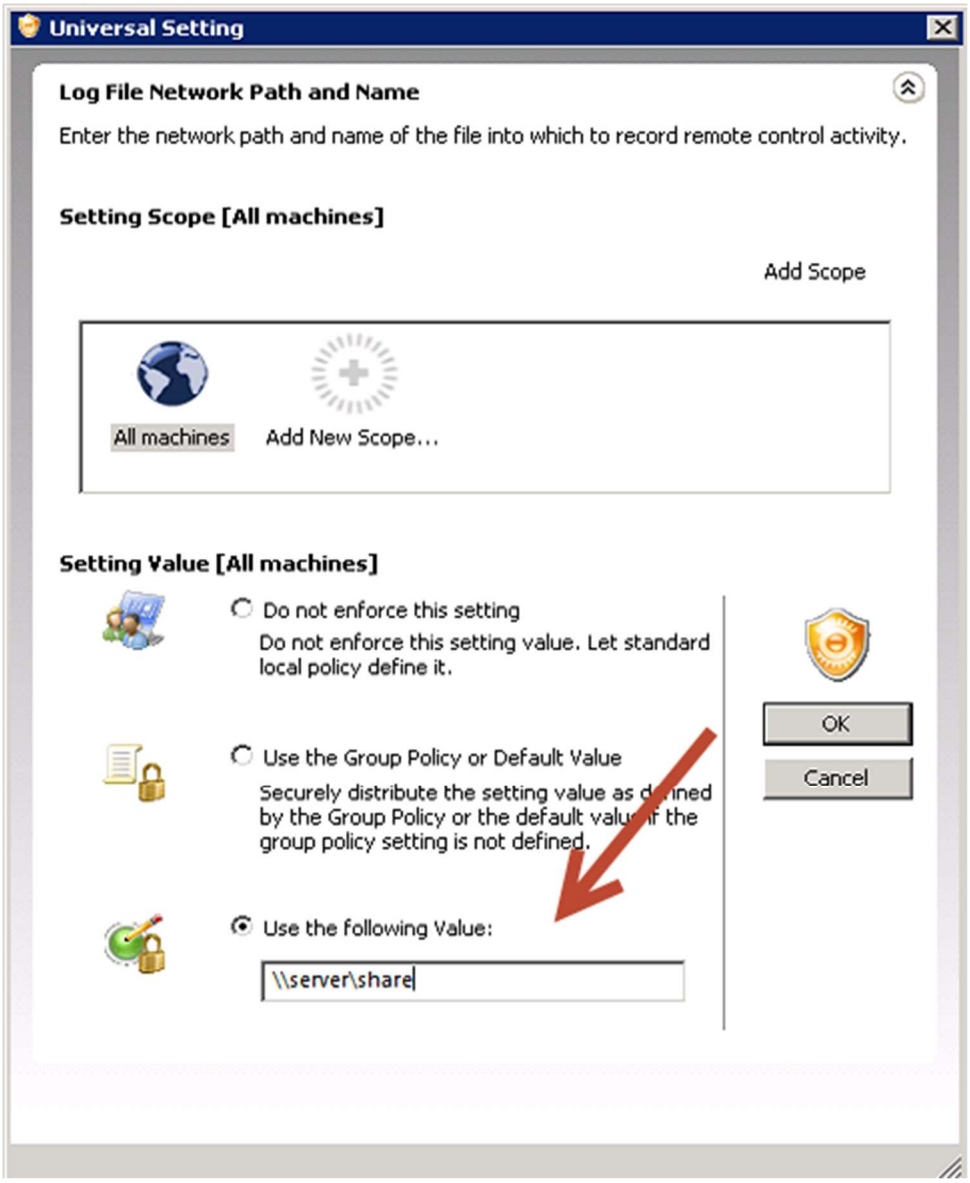
Activate Post Session Notifications - Centralized Logging

© Copyrights Goverlan Inc. – All Rights Reserved



Log File Network Path and Name

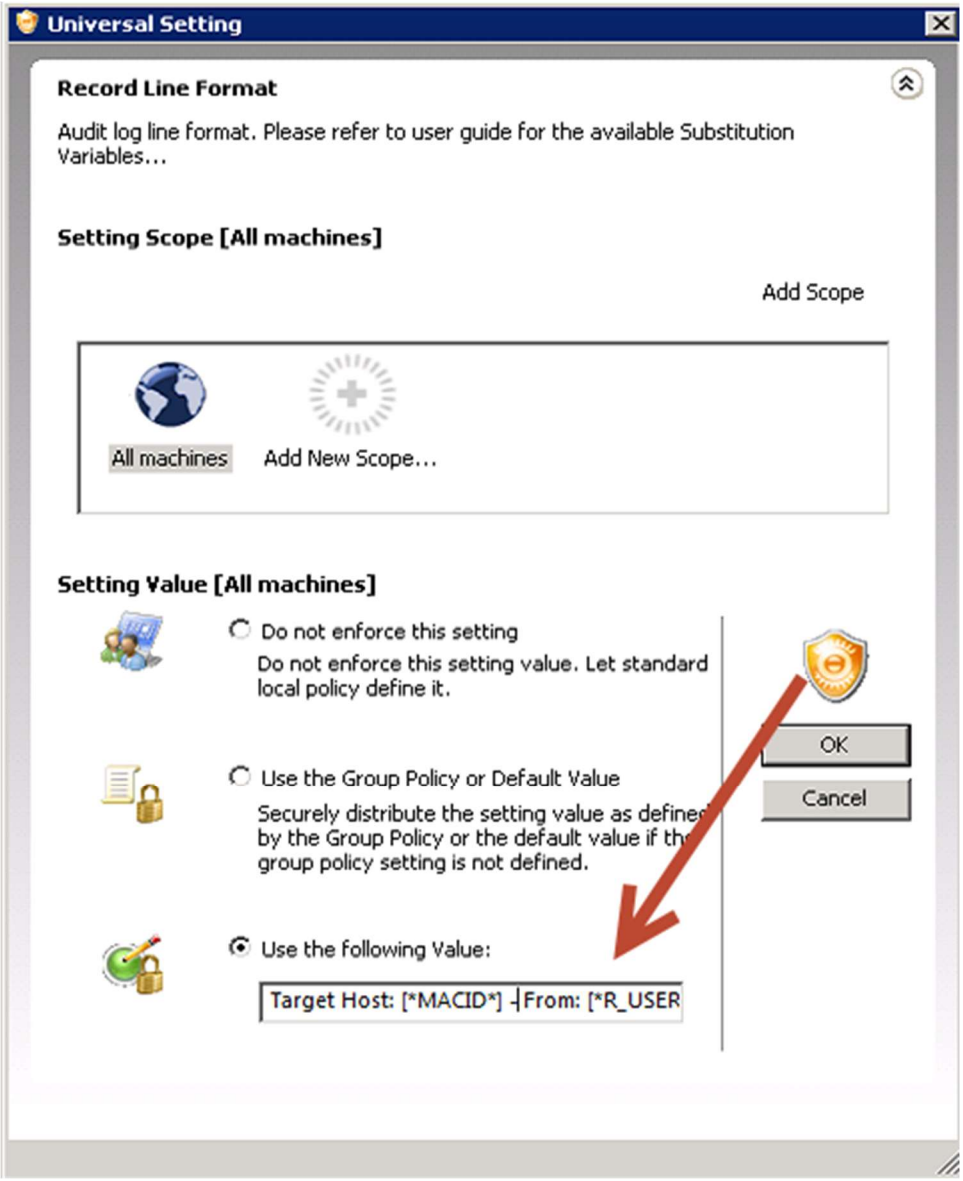
© Copyrights Goverlan Inc. – All Rights Reserved



Record Line Format

Use the same variables as shown in the Goverlan Administrative GPO section above.

© Copyrights Goverlan Inc. – All Rights Reserved



REFERENCES

- Utilizing the Centralized Auditing Feature
- Goverlan Administrative GPO Template
- Using Universal Settings Distribution

Goverlan Reach

Configuring Goverlan Reach

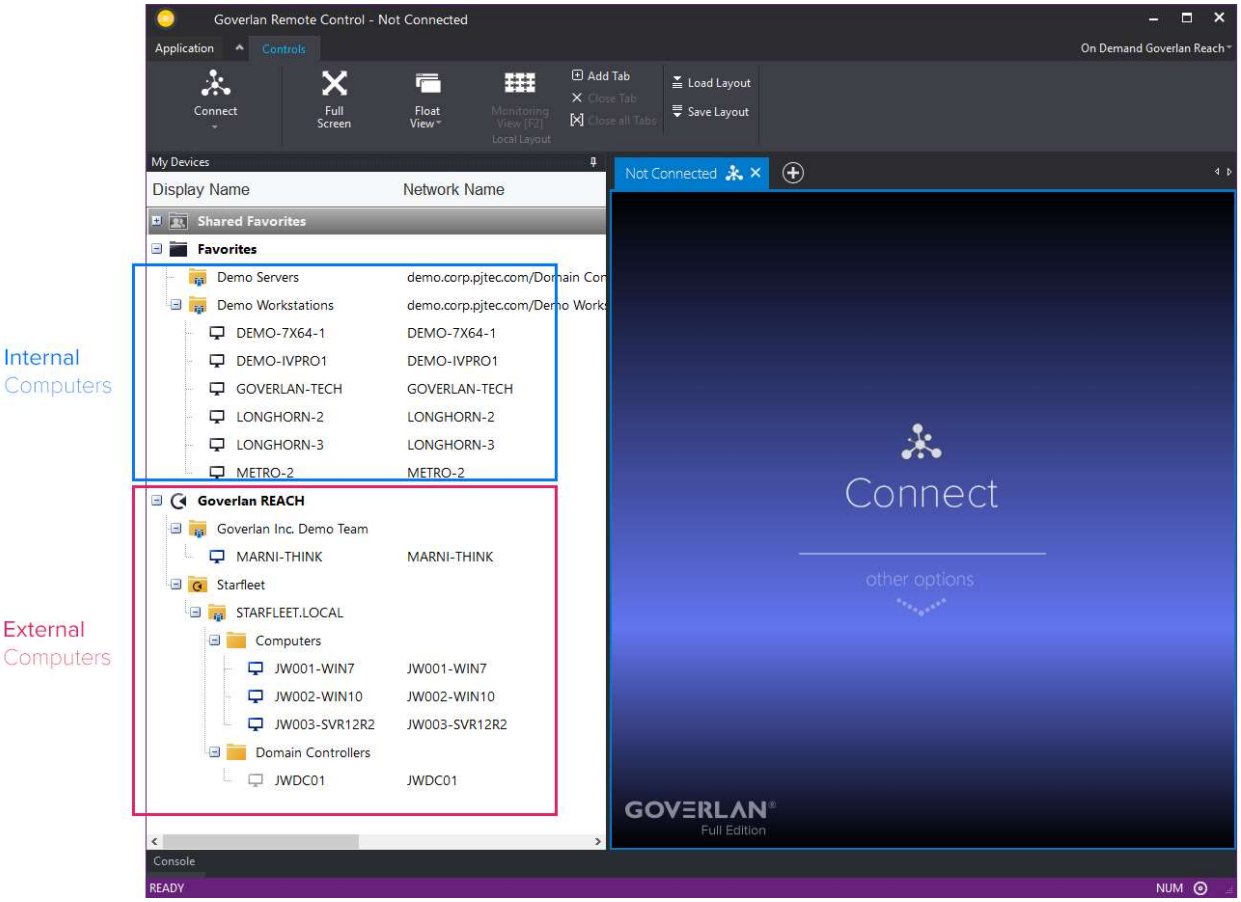
For more information on how to configure Goverlan Reach, please refer to the Goverlan Reach – Implementation Overview User Guide.

© Copyrights Goverlan Inc. – All Rights Reserved

Accessing Reach Nodes

Once the Goverlan Reach infrastructure is implemented, Reach equipped computers start monitoring to determine whether they are inside or outside of the Reach authoritative network.

- If Reach nodes are within the private network, they can be managed using the standard access methods via Active Directory or directly by specifying the system's network address.
- If Reach nodes are outside the private network, they can be managed by browsing through the Goverlan Reach Repository.



Goverlan Reach Repository

The Goverlan Reach Repository holds all registrations of computer nodes that are outside of your private network. Computer nodes are organized by folders defined by Reach Site names as well as by any Active Directory hierarchy of remote client sites. The Reach Repository can be browsed, searched and used to configure the scope credentials for a set of machines.

Browsing the Reach Repository

To browse the Reach Repository, simply double click on any container within the Goverlan Reach folder. This will disclose the child containers for your Reach, starting with Reach Site Names.

Open a Reach Site folder to display its nodes. If a Reach Site is configured with its own Active Directory hierarchy, it will be displayed in the Reach Repository.

© Copyrights Goverlan Inc. – All Rights Reserved

NOTE: Only the Active Directory path of registered computers is displayed within Reach.

The active/offline status of a Reach node is indicated via its computer icon. Offline nodes cannot be managed as they are either Powered OFF, or may be back on the private network (in case of travelling corporate users).

Searching the Reach Repository

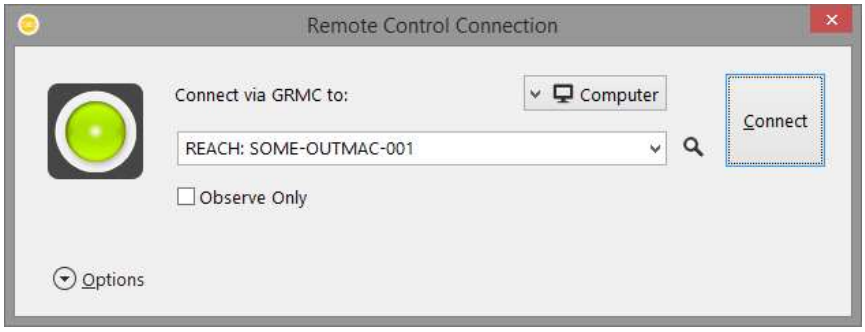
Reach nodes can be found by searching the Reach Repository. The Reach Search features are available while browsing the Reach Repository and every time a computer name is requested within the Goverlan interface.

To search while browsing the Reach Repository, right-click the parent container to search and select the Search feature:

Enter a partial node name including wild card (*) before or after the search string to view all reach nodes matching your search criteria within the selected container.

Connecting to Reach nodes

To connect to Reach Nodes or search for Reach nodes via the connect area, enter the prefix REACH: followed by the node name or search string. For instance, to open a remote control session to an external Goverlan Reach machine named: **SOME-OUTMAC-001**, enter:



The connection string above assumes that **SOME-OUTMAC-001** is registered to the root of the Goverlan Reach Repository. However, most Goverlan Reach nodes will use an organization name or their local Active Directory Domain information to register themselves.

If the exact path of a Goverlan Reach node is not known, the node can be searched for using the ***** wild card character in the connect string. For instance, enter **REACH: SOME-OUTMAC-001*** and a search for SOME-OUTMAC-001 will be initiated, irrespective of its location within the Goverlan Reach Repository.

Other search examples:

© Copyrights Goverlan Inc. – All Rights Reserved

REACH:*	Returns the entire repository
REACH:CLIENT-ORG/*	Returns all machines registered in the *CLIENT-ORG* container
REACH:Domain Controllers*	Returns all machines registered in any Active Directory container titled *Domain Controllers* across all client sites.

Configuring Reach Credentials

Goverlan Services require Windows credentials to perform any action on a remote system. The provided credentials must hold the necessary level of privileges to execute the action requested.

By default, remote control sessions require Local Administrative privileges (this can be configured).

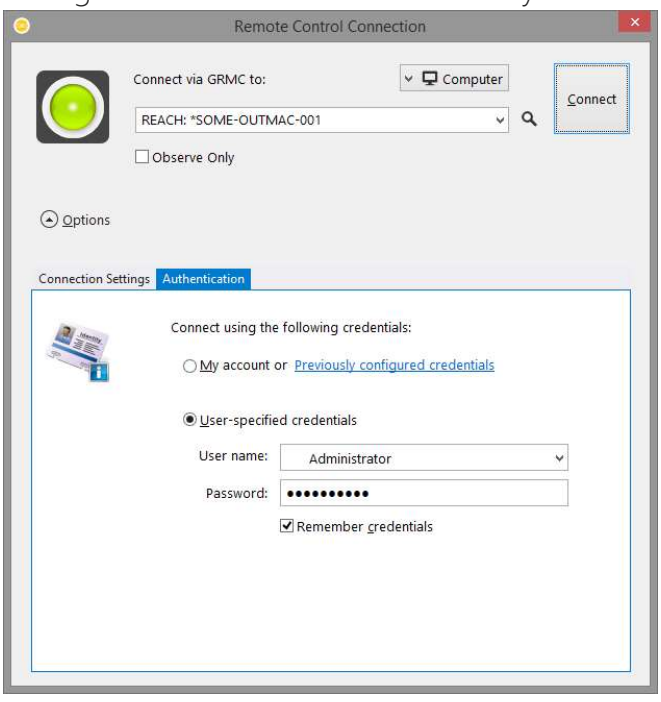
Goverlan automatically prompts for credentials if the action taken has failed due to a lack of privileges. Per-machine credentials, and per-container credentials can be configured as well.

Per-Machine Credentials

If the remote endpoint is located at the root of the Goverlan Reach Repository, or if a unique administrator password is configured for each endpoint, per-machine credentials must be specified.

To configure per-machine credentials you can either:

- Initiate a management action on the remote machine and wait for the Goverlan credentials prompt.
- Configure the credentials the first time you connect to the machine:

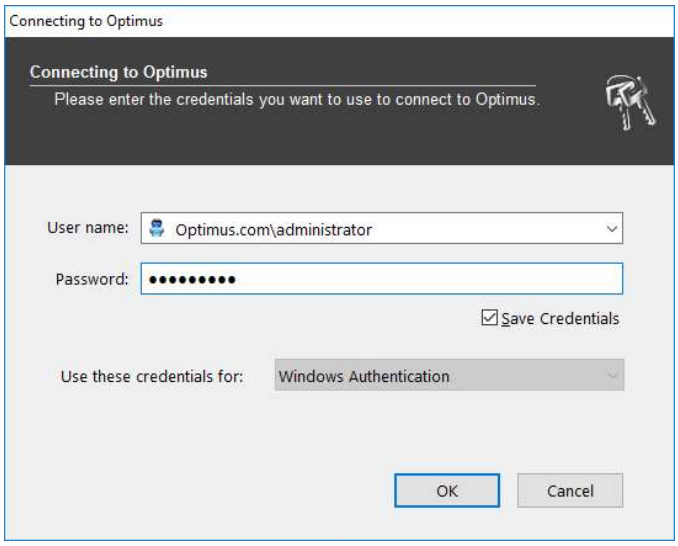


Once the credentials have been configured, they will be reused for subsequent connections to the same machine. These credentials can be modified or removed via the *Credentials Manager*.

Per-Container Credentials

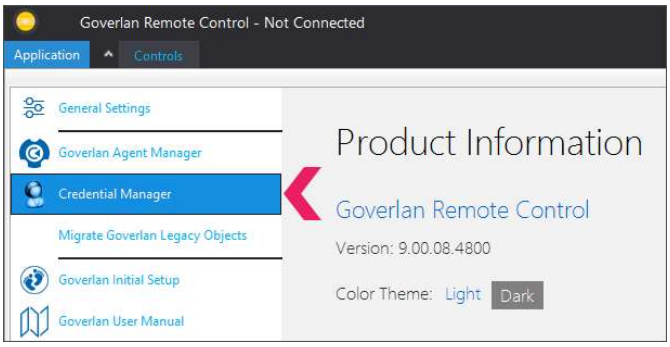
Credentials for a scope of machines can be configured on any of the parent containers. Right click on a Goverlan Reach Repository container and select **Configure Credentials for this Realm:**

Specify the credentials to be used for all the nodes that belong to this realm. Make sure to indicate the proper domain authority in your credentials:



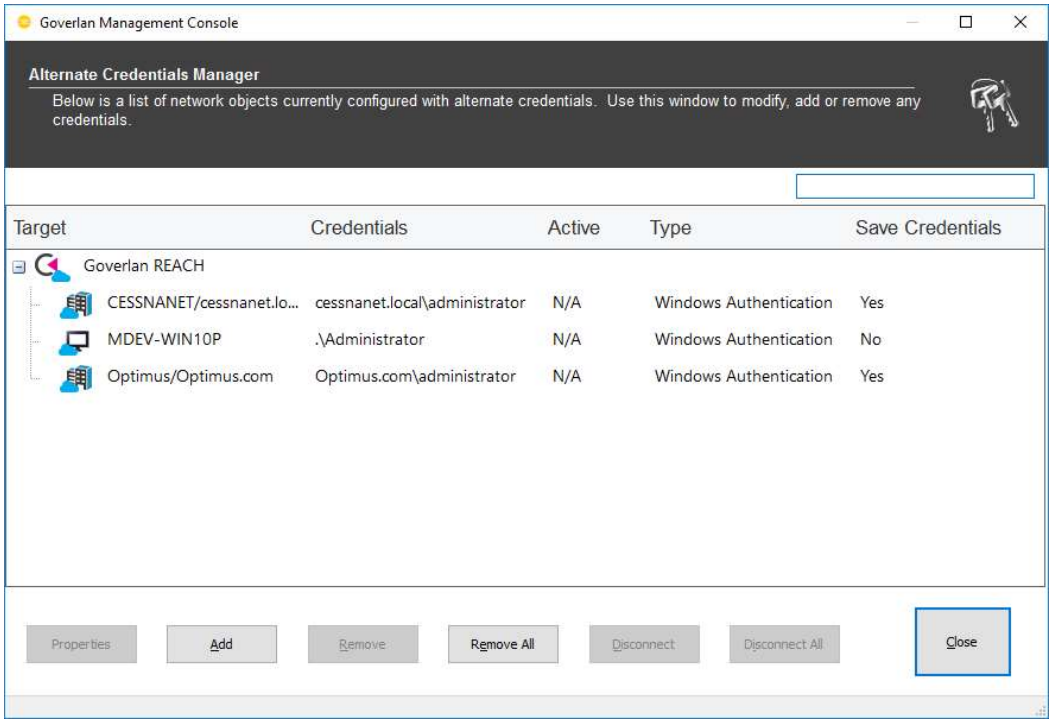
Credential Manager

Once the credentials are configured, they are stored in the Goverlan Credentials database that can be accessed via the Application menu:



The Credential Manager can be used to view and modify configured credentials.

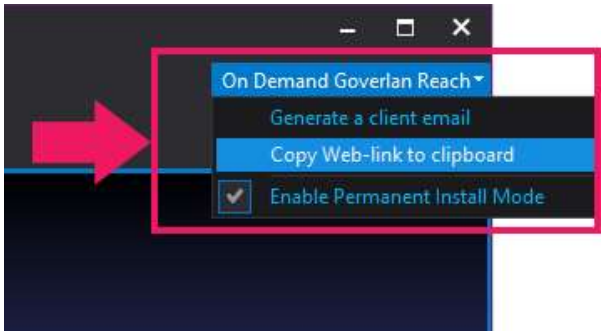
© Copyrights Goverlan Inc. – All Rights Reserved



On-Demand Goverlan Reach

Using Goverlan Reach, you will be able to remotely access any user, anywhere if they are connected to the internet. This is done via On-Demand Reach sessions.

To initiate a Goverlan Reach On-Demand session, Operators click on the **On Demand Goverlan Reach** option in the top right corner of the Goverlan Operator software:

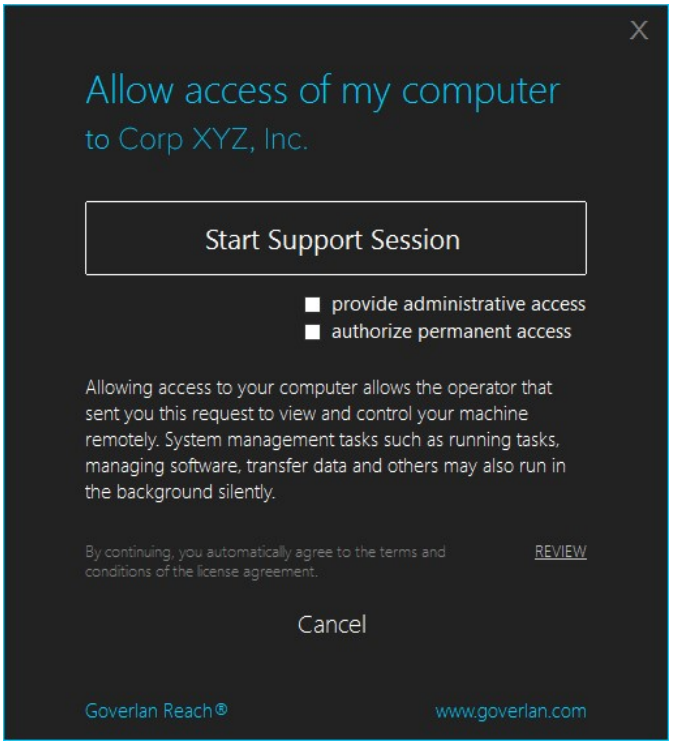


- **Generate a client email** - Automatically launches your default email client with a template that includes the weblink to download the Goverlan Reach client that pertains to your configured Goverlan Reach server.
- **Copy Web-link to clipboard** - The weblink will be available from your clipboard to paste in a live chat session or custom e-mail.
- **Enable Permanent Install Mode**: Enable this option to generate a client support package. The remote user will be presented with an option to permanently install the Goverlan Reach Client on the user's machine as a service. Permanent installations will make the node available for both

© Copyrights Goverlan Inc. – All Rights Reserved

attended and unattended support session. If this setting is turned off, the user can only start on-demand support sessions.

The Goverlan Reach Web-Link redirects the client to our default Client Portal in which the Goverlan Reach Client will be available. Once this is opened, the user will be prompted to start the support session.



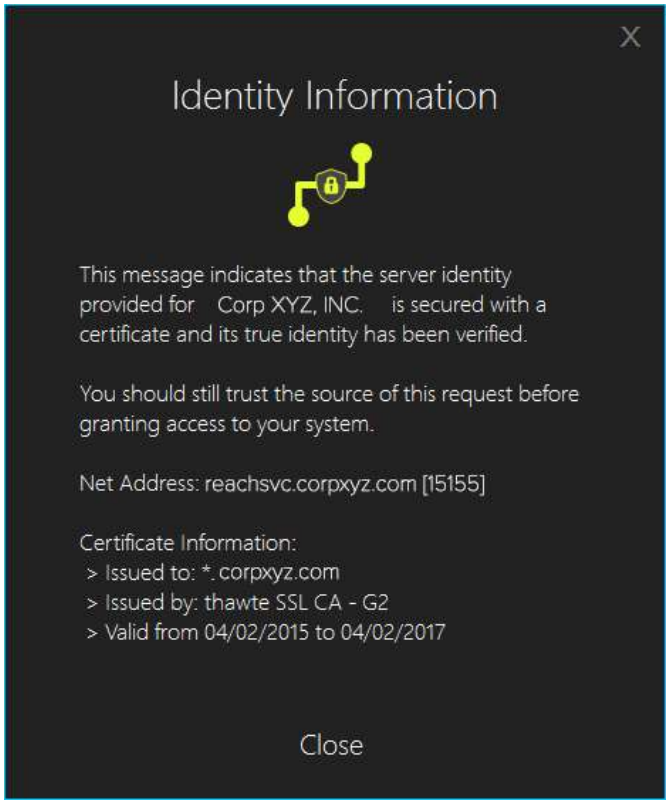
If the Reach Client is started without local administrative privileges, the user is presented with an option to grant such privileges. Ask the user to enable this option if you wish to gain access to UAC prompts.

Once the user starts the support session, they are presented with a Session ID:

Security Note

As best practice, your Goverlan Reach Server public facing address should be configured with a TLS identity certificate. Service identity validation is then confirmed to the end user. The user can click on the "*Server identify verified*" link to display certificate information:

© Copyrights Goverlan Inc. – All Rights Reserved

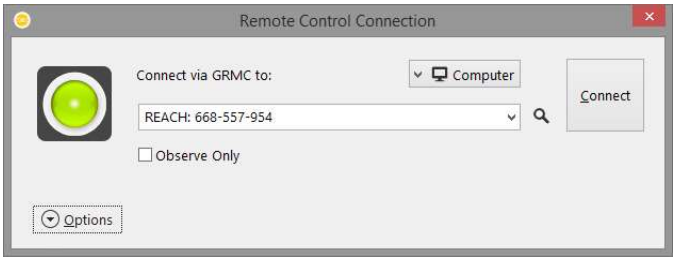


If your Reach Server public facing address is not configured with an identity certificate, the Reach Session ID window will turn red as follows:

Connecting to the Reach Session ID

Once the Session ID is transmitted to the Operator, the Operator can perform any Goverlan management task on the remote system by using REACH:*SESSION-ID* as a computer name.

For instance, to initiate a remote control session to the Session ID *668-557-954*, the connection string would be: REACH:668 557 954

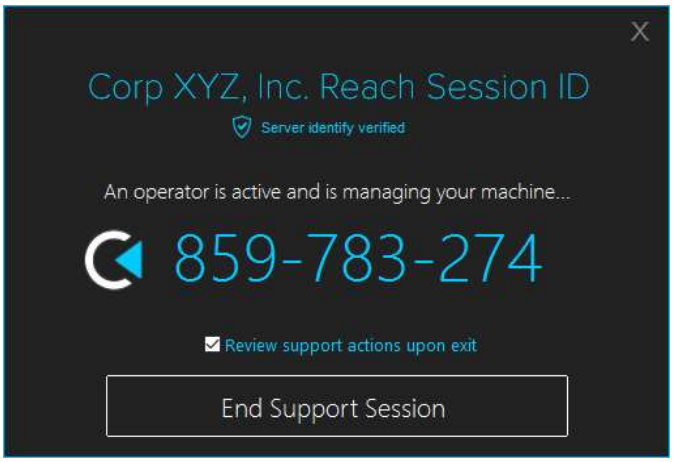


© Copyrights Goverlan Inc. – All Rights Reserved

NOTE: Spaces and dashes can be used to specify a session ID, so REACH: 668557954 or REACH: 668 557 954 or REACH: 668-557-954 are all acceptable entries.

Ending a Support Session

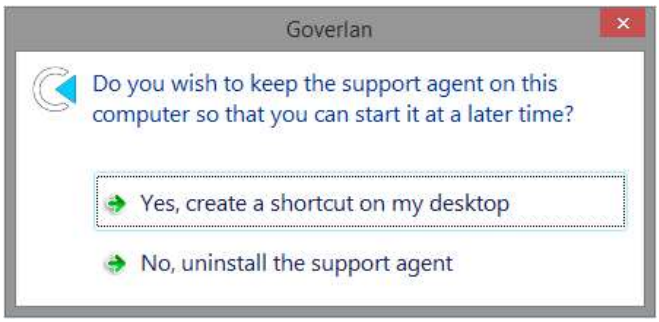
Upon first connection with the remote client, the support session is started and the user sees the following screen:



It is important to understand that On-Demand Reach Support Sessions do not need to start and end with a remote control session. The Reach Session ID can be used and re-used with other Goverlan Services. For instance, you can connect to the remote system directly from other Goverlan Tools such as the Goverlan Task Manager, initiate file transfers, or push power actions even if no remote control session is active.

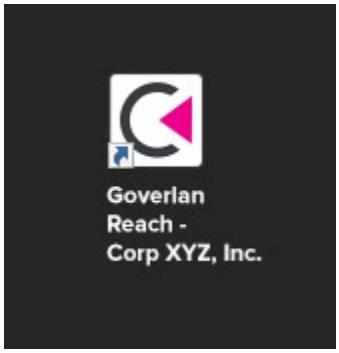
If the remote user doesn't end the session by clicking **End Support Session**, you can use the Goverlan services to manage the remote machine.

Once the user terminates the session, the option to keep or remove the Reach Session Starter is presented:



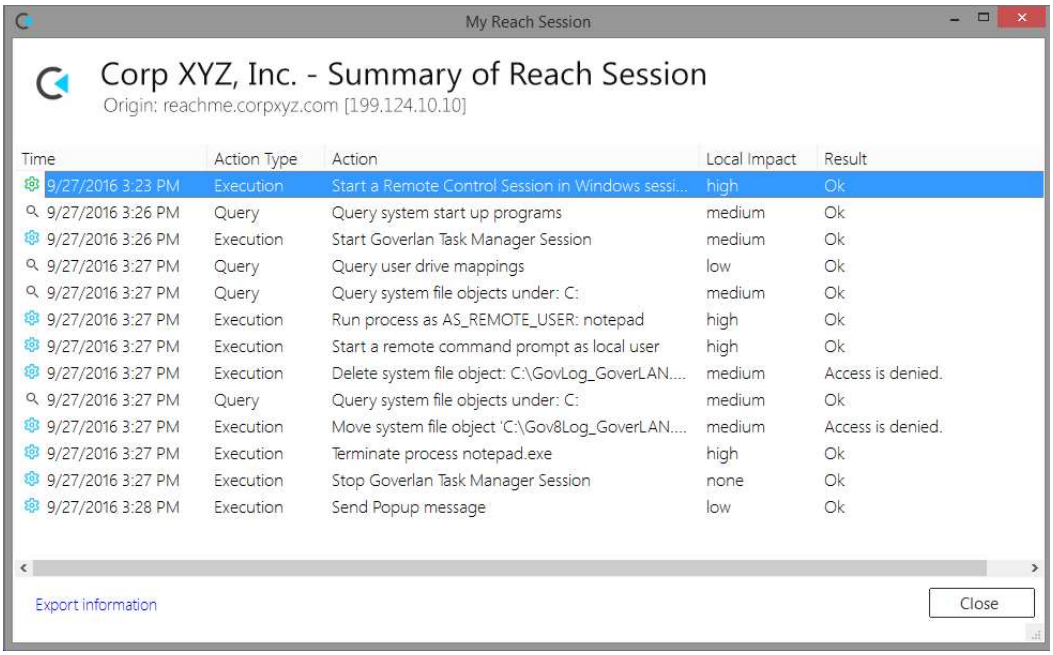
Selecting ***Yes*** generates a shortcut on the user's desktop that can be used at any time to re-open a support session.

© Copyrights Goverlan Inc. – All Rights Reserved



Reviewing Operator Actions

During an On-Demand Reach session, all Operator actions are audited and logged. If the end user selects to review the support action upon exit, the log is displayed once the support session ends.



NOTE: The audit log is also registered in the Application log of the event viewer.

© Copyrights Goverlan Inc. – All Rights Reserved

Navigating Goverlan Reach RC

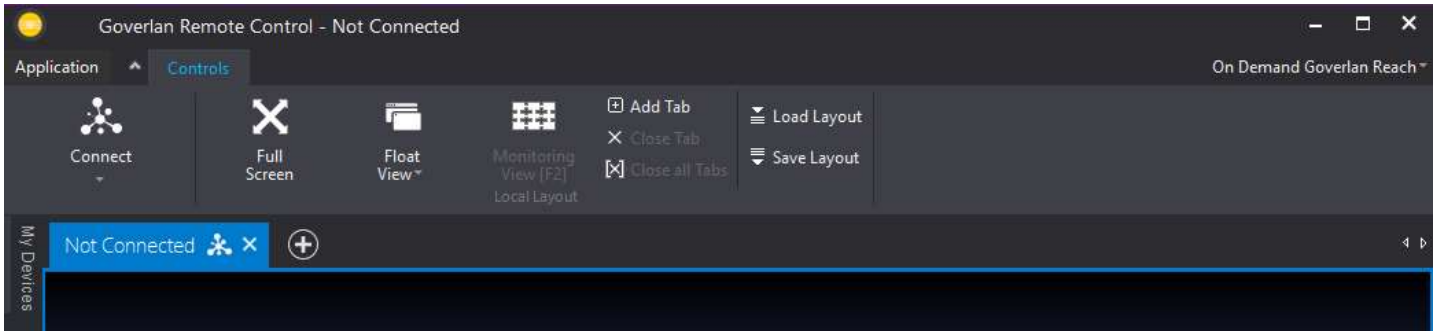
Basic Controls

Goverlan uses a Microsoft Office-style interface to help you get around in a familiar UI. Before the connections is made, Goverlan Reach RC Requires the Goverlan Client. For more information, see Installing The Goverlan Client.

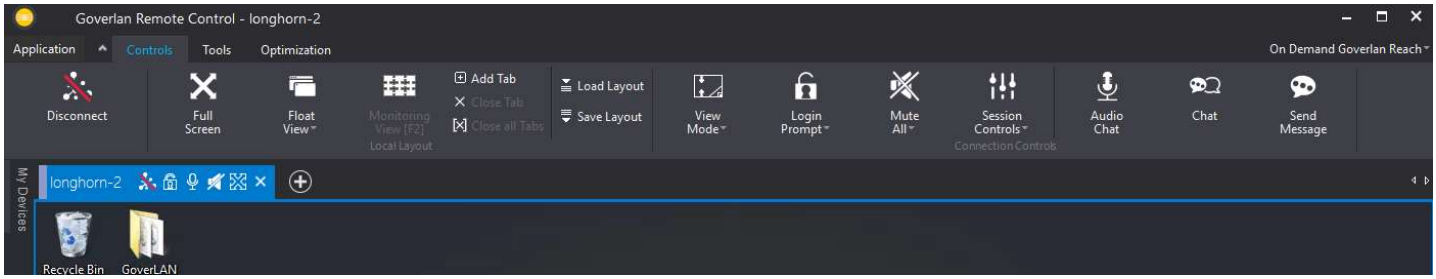
The Command Bar

The Command Bar is located at the very top of Goverlan and has two modes. Not Connected and Connected. Command Bar content will change depending on the state.

Not Connected



Connected



Once connected to a computer with Goverlan Reach RC, the context of the Command Bar will change, giving you access to more features.

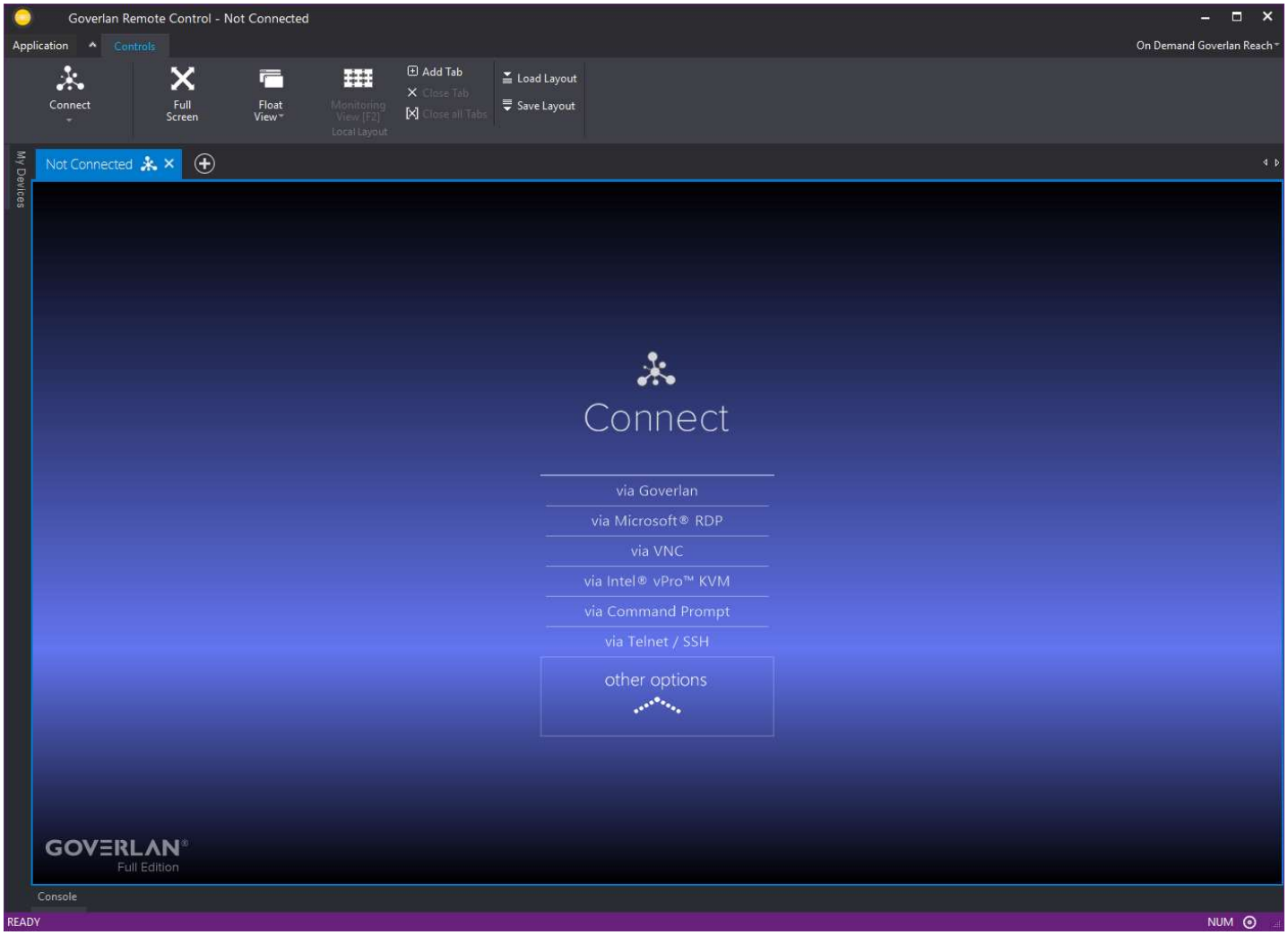
Accessing different Connection Protocols

Goverlan Reach RC supports several different protocols to access a variety of devices on your network.

To access these protocols, use the "More Options" drop down menu under the Connect button in the center of the Goverlan Reach RC interface, or the Connect button in the Command Bar.

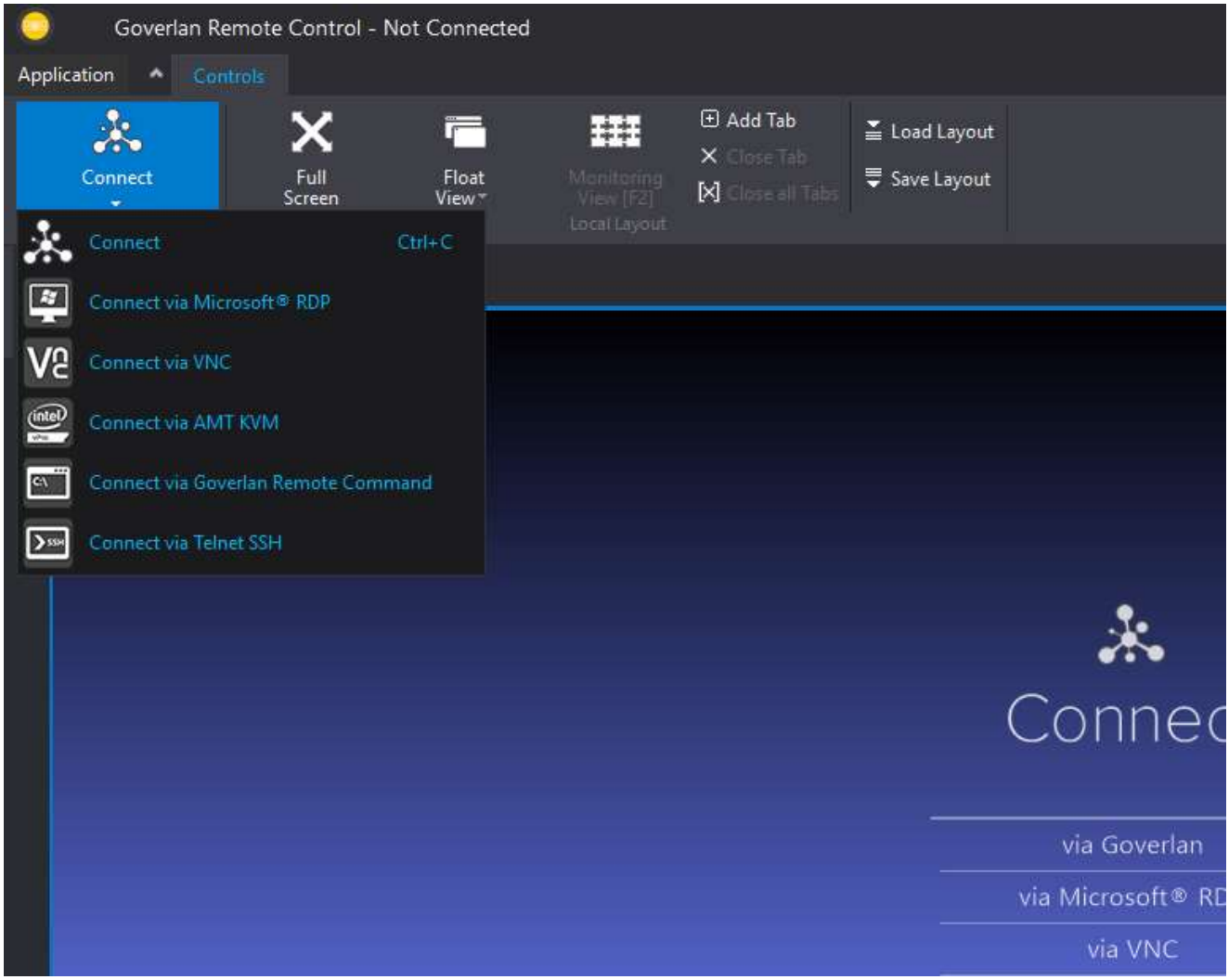
More Options

© Copyrights Goverlan Inc. – All Rights Reserved



Connect Button in the Command Bar

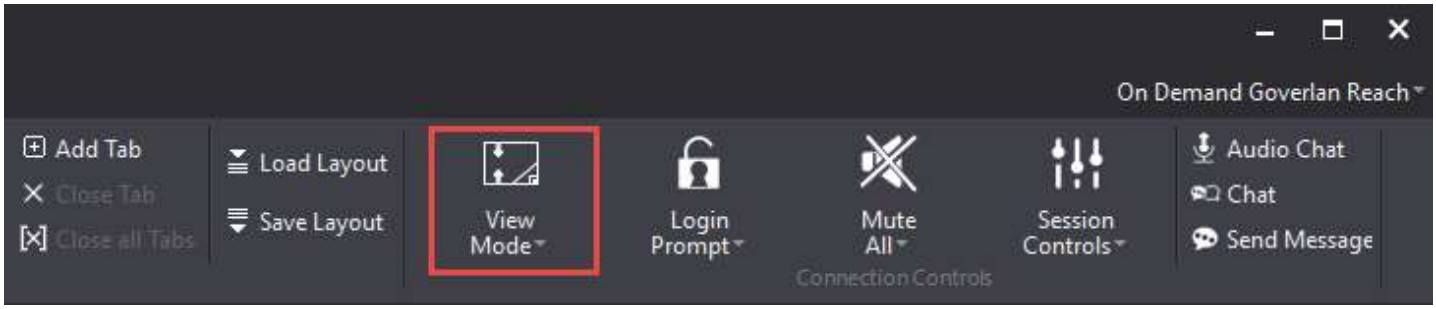
© Copyrights Goverlan Inc. – All Rights Reserved



Changing the View Mode

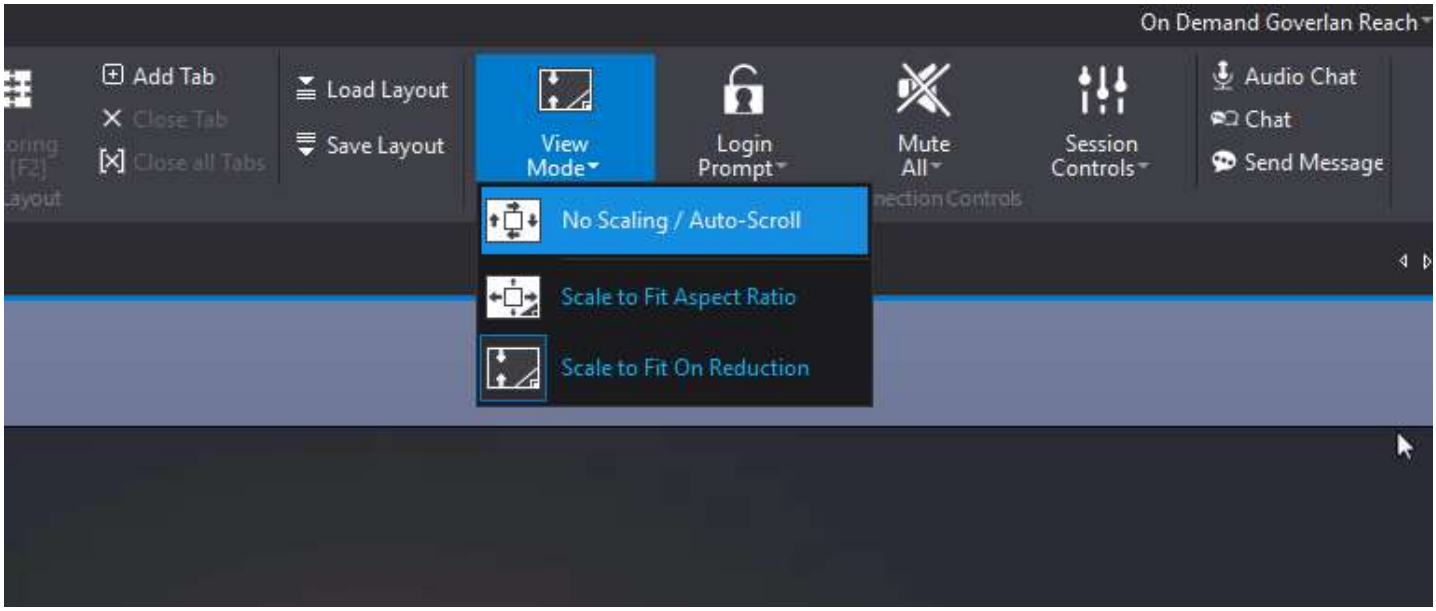
When connected to a computer, Change the View mode or Scaling to best fit your workspace.

While connected to the computer, go to the Command tab and locate the View Mode button.



Click the Drop Down arrow below the button to access the view mode settings

© Copyrights Goverlan Inc. – All Rights Reserved



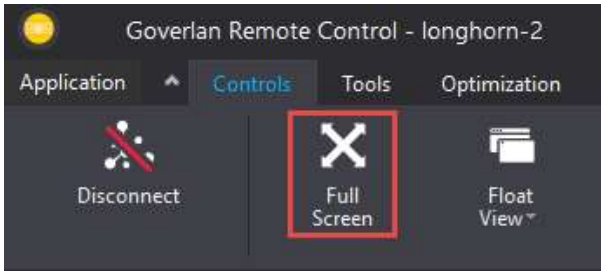
View Mode Settings

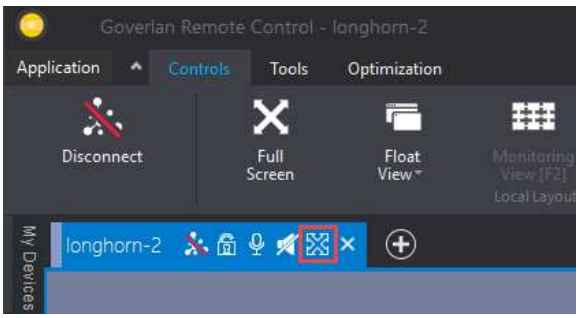
The following options are available for changing the view mode.

- No Scaling - Goverlan will maintain the screen size of the target computers resolutions. If the target is configured with a high resolution, you may need to scroll manually to see everything.
- No Scaling / Auto Scroll - This setting is identical to No Scaling except Goverlan will automatically scroll based upon the where the mouse cursor is.
- Scale to Fit - Scale to Fit will change the aspect ratio to the size of the Goverlan window. When the Goverlan window is resized, the remote control session will resize accordingly.
- Scale to Fit Aspect Ratio - This setting will scale the view to fit the Goverlan window while respecting the aspect ratio of the target screen.
- Scale to Fit On Reduction - This setting is identical to Scale to Fit Aspect Ratio except the screen will only be scaled when the Goverlan window is smaller than the target computers screen.

Full-Screen Mode

Goverlan Reach RC sessions can also be set to full-screen mode. The full-screen button can be located on the Command Bar or on a Connection Tab.





REFERENCES

© Copyrights Goverlan Inc. – All Rights Reserved

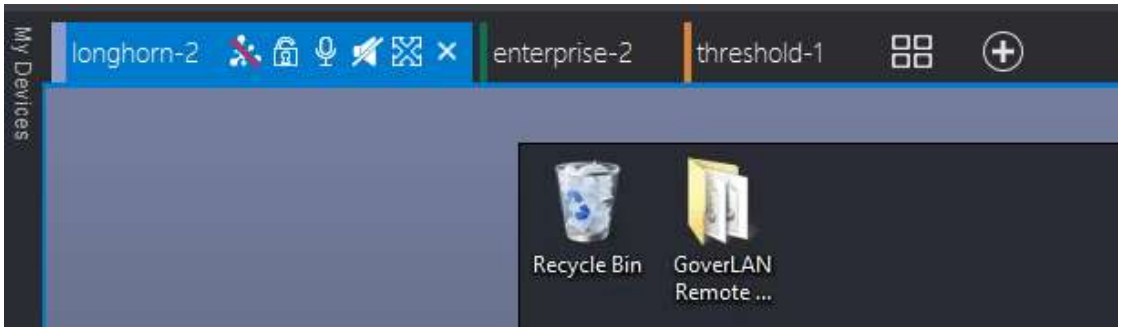
- Installing the Goverlan Client
- Performance Monitoring
- Auditing of Goverlan Reach RC Events

Managing Your Workspace

Goverlan Reach RC provides many flexible options for creating a workspace to view and manage remote connections. Use the Monitoring View or Float View to create a dashboard or remote control connections. Save customized workspaces for easy reconnecting to important resources. For more information, see Performance Monitoring.

Tabbed Goverlan Interface for Remote Control Connections

Goverlan Reach RC's tabbed interface allows control over many computers at once. Open as many tabbed connections as needed and easily switch between them. Mix and match different connection protocols with different tabbed views.



Each tab is equipped with shortcuts for commonly accessed features, including Disconnect, Full Screen, Send Ctrl+Alt+Del and Observe Only mode.

Adding a new tab

Click the Plus Sign tab to add a new tab and start a new connection

Monitoring View Tab

Click the Monitoring View tab to start the Goverlan Monitoring View with all the existing connected tabs. To learn more about Goverlan Monitoring View, See Performance Monitoring.

Float View

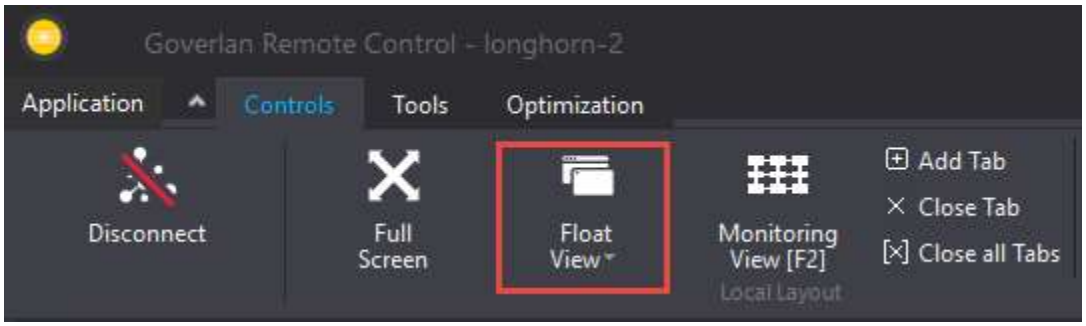
Float Views will allow you to have several child windows that are connected to different nodes over any protocol that Goverlan supports. Before using Float Views, you must first establish a remote control connection. For more information about opening remote control connections, see Basic Controls.

Once connected, create a Float View with one of the following methods:

Using the Command Bar on the Main Tab

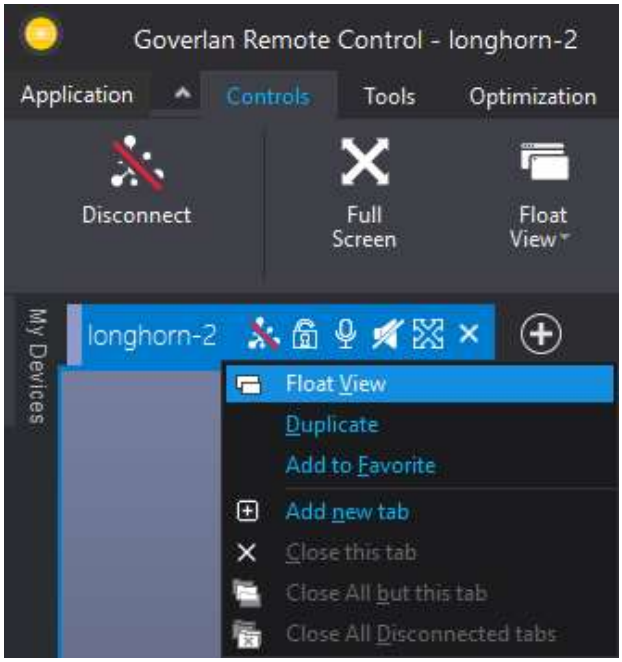
© Copyrights Goverlan Inc. – All Rights Reserved

Clicking the Float View button while you have a connection established will pop the remote control session out into its own window. You can position and resize this view anywhere on your desktop.



Using the Connection Tab

Right click on any connection tab and select Float View



Using Monitoring View Thumbnails

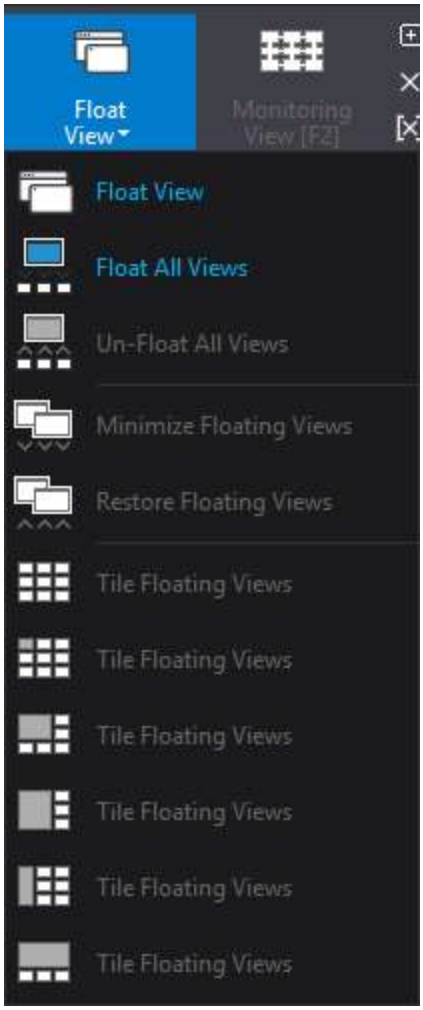
Right click any thumbnail in Monitoring View and select Float View. For more information about Monitoring View, see Performance Monitoring.

© Copyrights Goverlan Inc. – All Rights Reserved

Managing multiple floating Windows

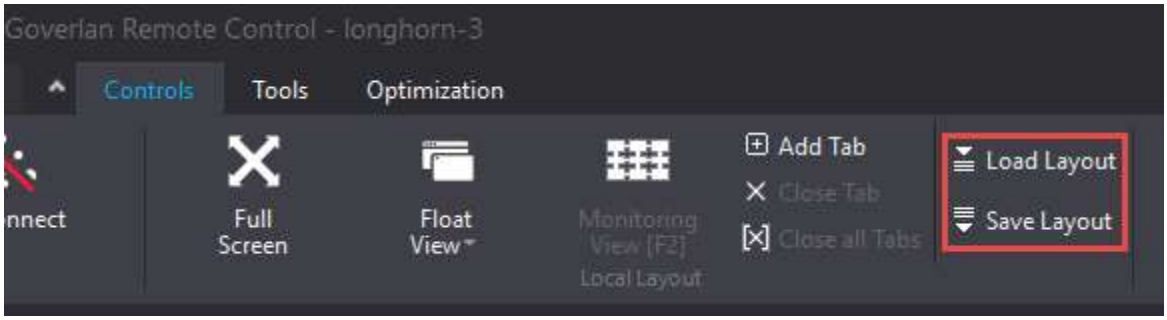
When you have several floating windows, you can automatically arrange them using the Float View drop down options. These options will automatically float or un-float all windows or arrange the currently floating windows in a specific arrangement.

© Copyrights Goverlan Inc. – All Rights Reserved



Remote Control Layouts

Goverlan layout files allow you to save your current connections and window positions when using Monitoring Views or Float Views. Layout controls can be found in the Command Bar on the Main Tab. For more information about Monitoring View, see Performance Monitoring.

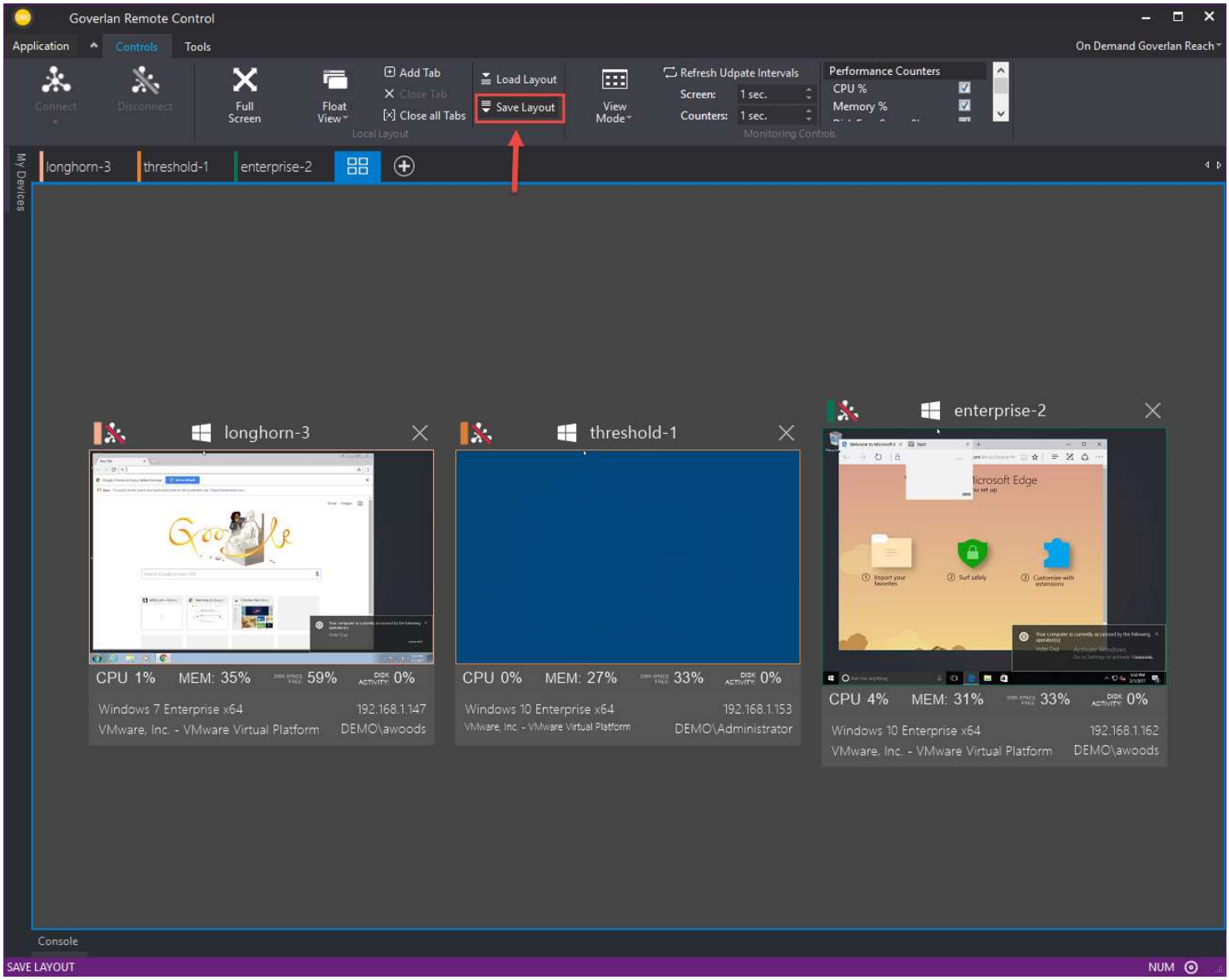


Saving a layout file

Before you can save a layout file you must first establish all your remote control connections. For more information about opening remote control connections, see Basic Controls.

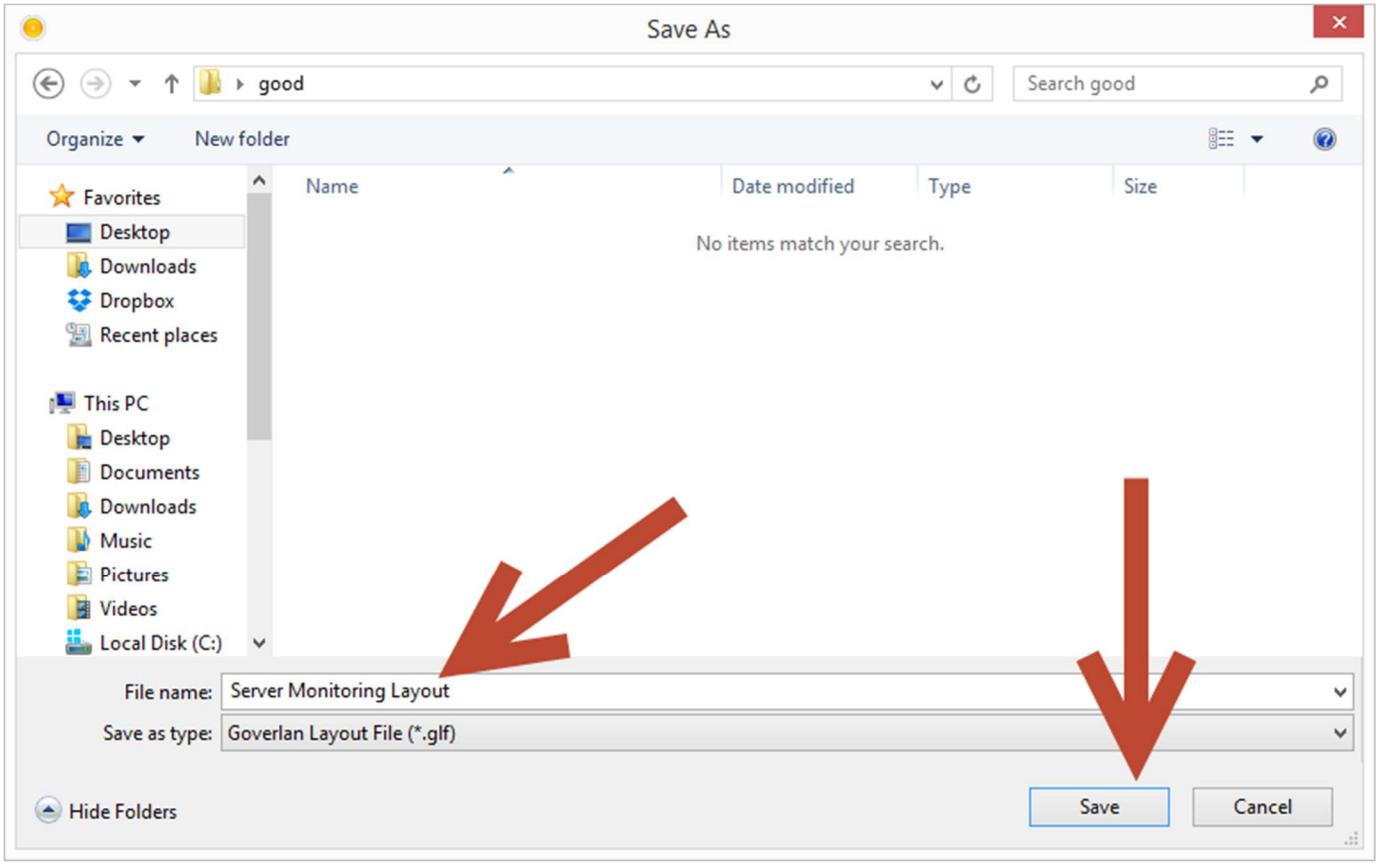
Once you have your workspace in the desired state, click the Save Layout button.

© Copyrights Goverlan Inc. – All Rights Reserved



Name and save the layout file

© Copyrights Goverlan Inc. – All Rights Reserved



Loading layout files

Layout files can be used to quickly restore connections and window positions. Simply double click the layout file or use the Load Layout button.

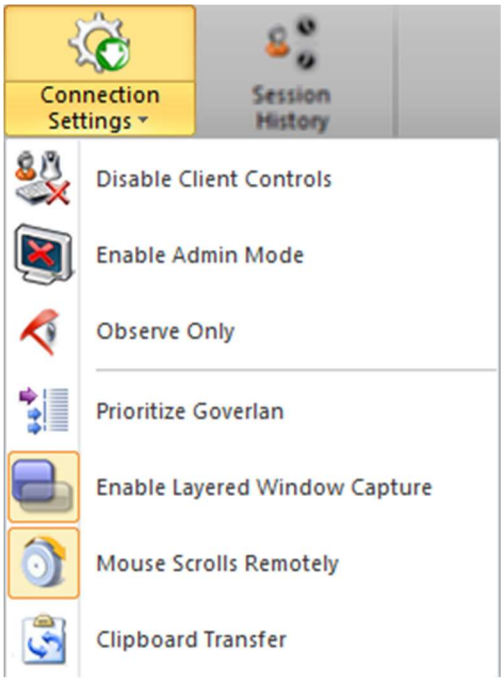
REFERENCES

- Basic Controls
- Performance Monitoring

Connection Settings

Goverlan Reach RC provides several features while you are in an existing remote control session.

© Copyrights Goverlan Inc. – All Rights Reserved



Disable Client Control

Disabling Client Controls will stop the target mouse and keyboard from working.

Observe Only Mode

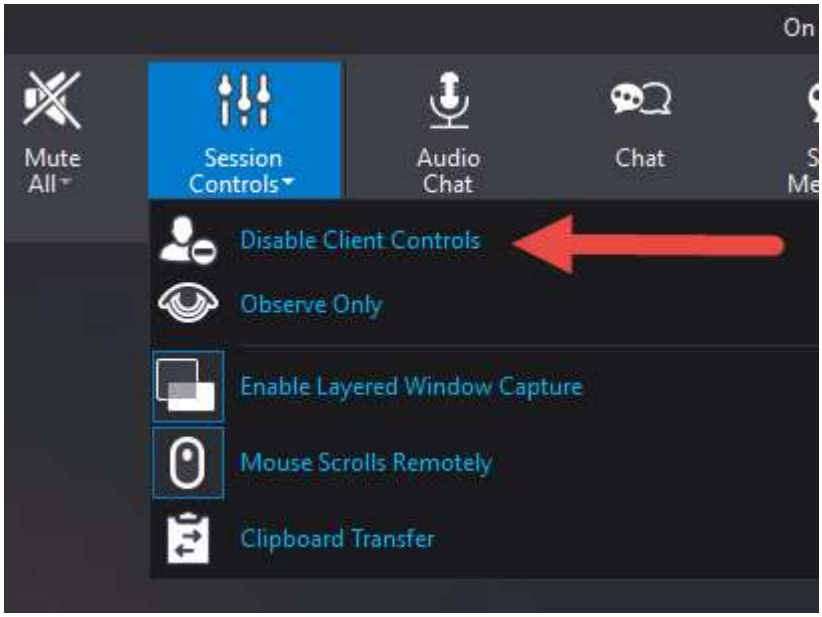
Observe Only mode will allow you to observe the remote control session only. The technicians keyboard and mouse inputs will not be sent over to the target computer.

Observe Only can be enabled in a few different places.

In the Connect To box

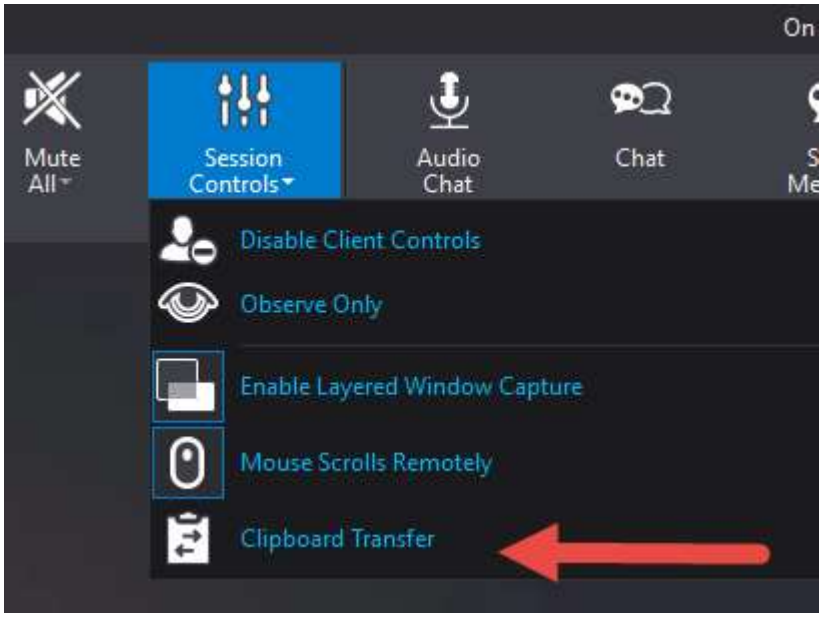
Via the Session Controls button in the ribbon:

© Copyrights Goverlan Inc. – All Rights Reserved



Enabling Clipboard Transfers

Enabling Clipboard Transfers will allow the operator to share the clipboard contents for copy/paste and file transferring.



REFERENCES

- Branding Goverlan Reach RC

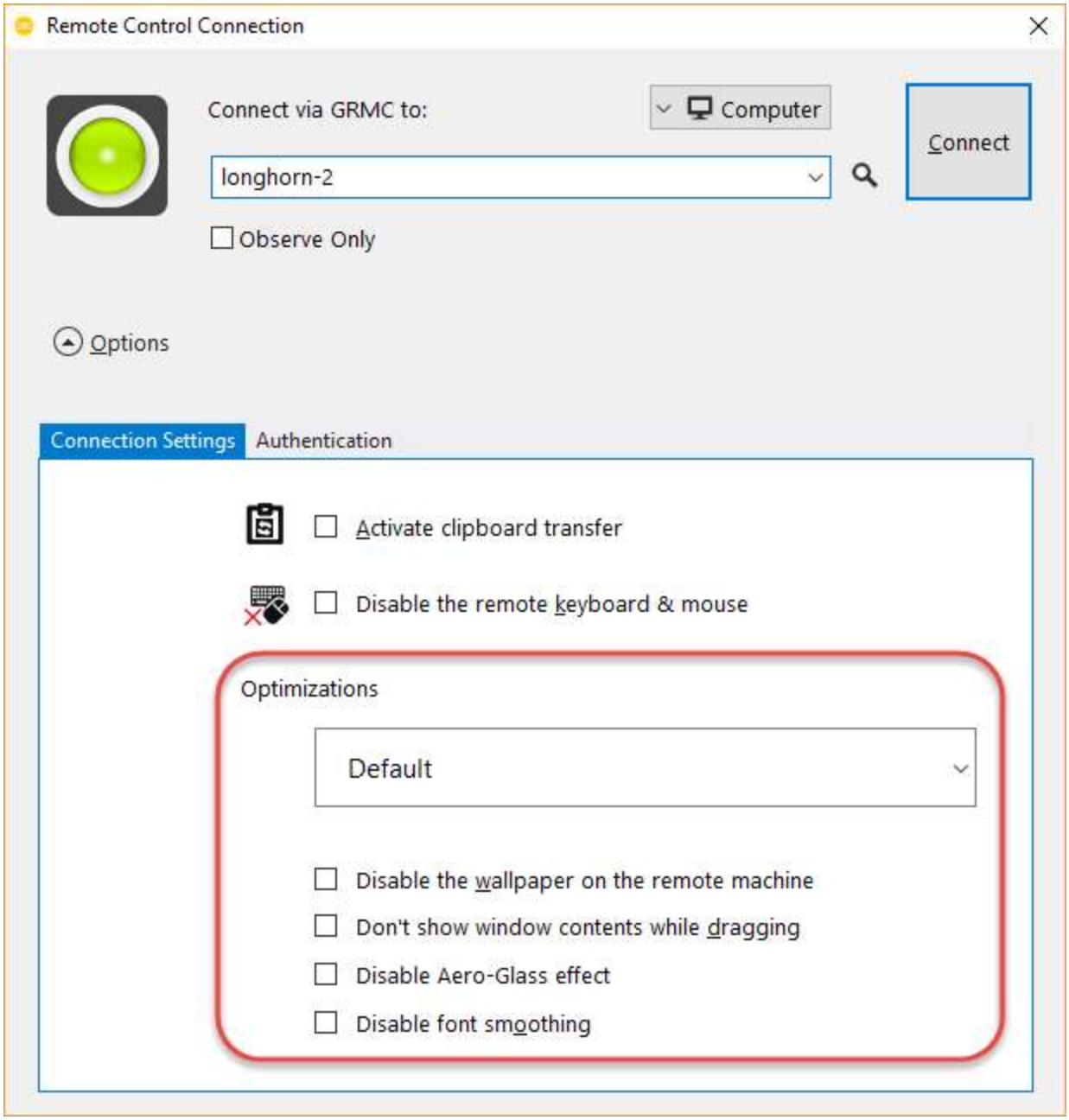
© Copyrights Goverlan Inc. – All Rights Reserved

Optimization Settings

Goverlan Reach RC uses several different methods to provide the best possible experience for the Goverlan operator. Goverlan Reach RC sessions use compression algorithms to ensure proper bandwidth usage.

Optimizing before you connect

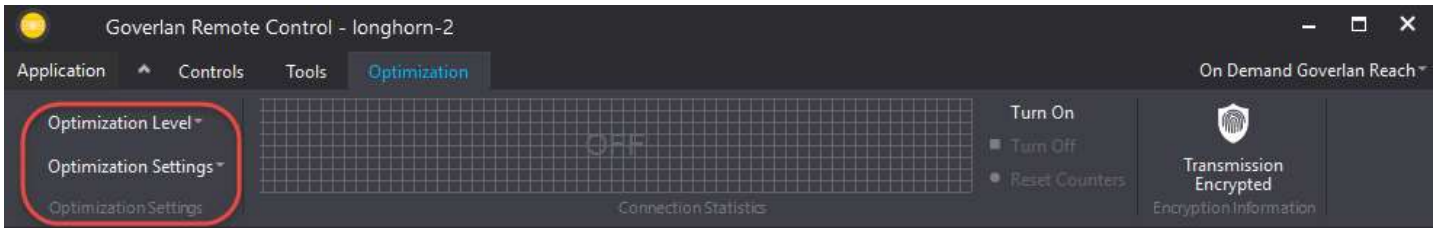
If you would like to change settings that affect performance on slower networks before you begin a remote control connection, use the Connection Settings Tab.



Changing optimization settings during a connection

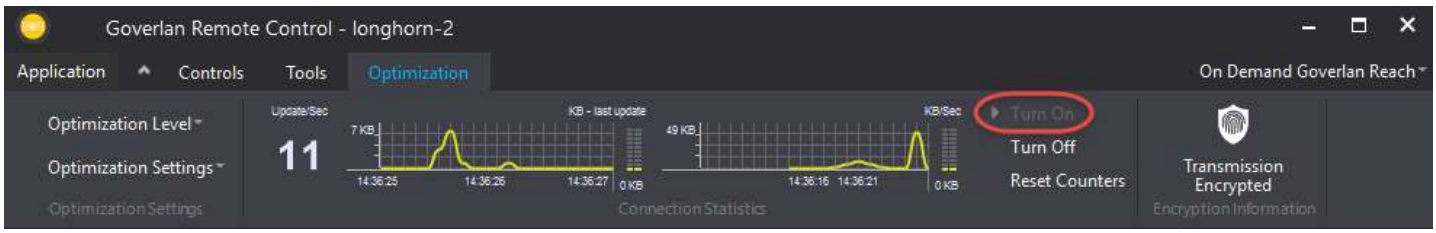
© Copyrights Goverlan Inc. – All Rights Reserved

Once you have established a connection, you can change the optimization settings using the Optimization Tab in the Command Bar.



Monitoring Remote Control performance

In the Optimization tab, click the Turn On button to activate the Connection Monitor.



The Optimization Graph will tell you the frame rate (updates per second), the compression rate and the transfer rate.

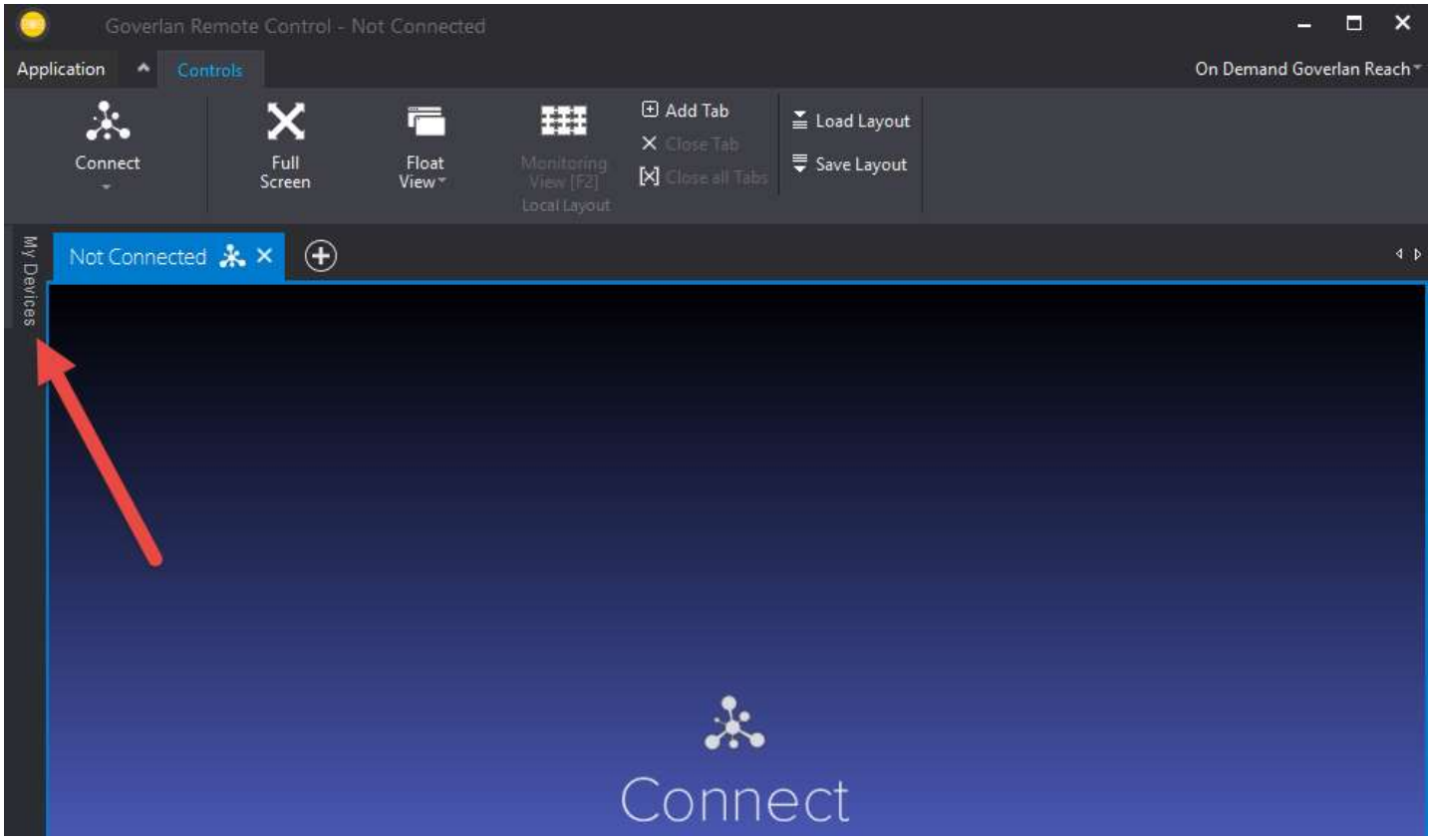
My Devices Panel

The My Devices panel allows you to organize and manage computers and devices on your network. Most functions and tools can be accessed right from the My Devices panel without having to start remote control session.

Opening the My Devices panel

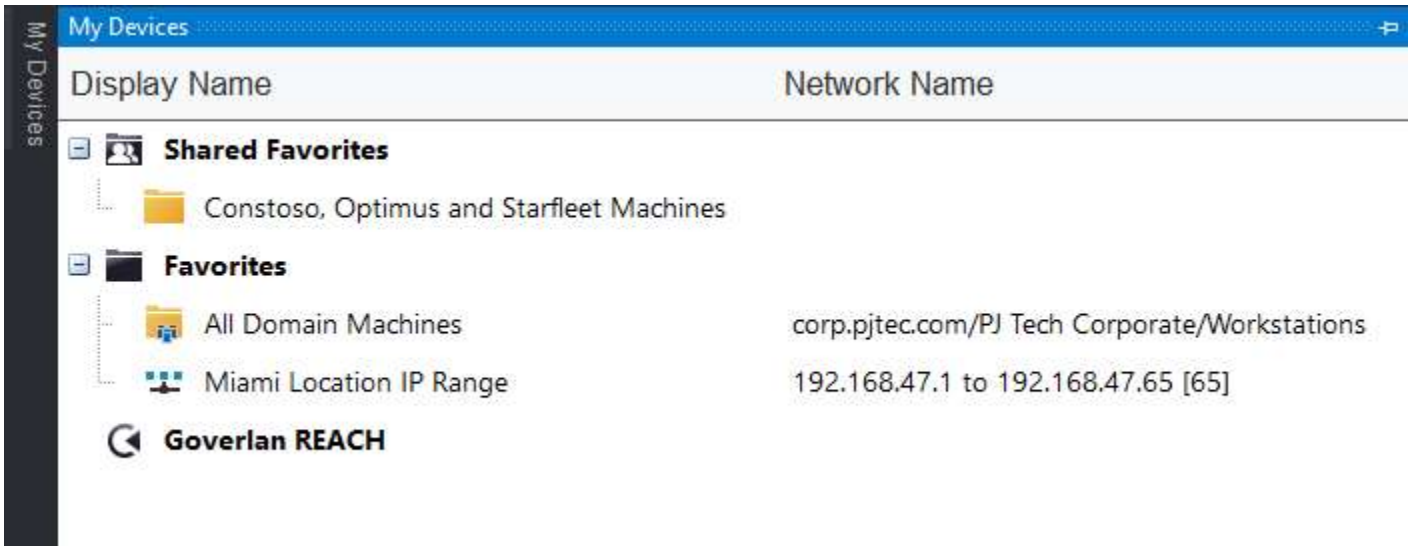
The My Devices panel can be opened from the My Devices tab

© Copyrights Goverlan Inc. – All Rights Reserved



Adding Containers

The My Devices panel contains two root folders. Favorites and Shared Favorites.



Shared Favorites

Shared Favorites are containers and devices that can be can be seen by other Goverlan users. Shared favorites require that the SUREDATA configuration be complete and accessible by all other Goverlan users. For more information about Team Collaboration and sharing, see Configuring Team Collaboration.

Container Types

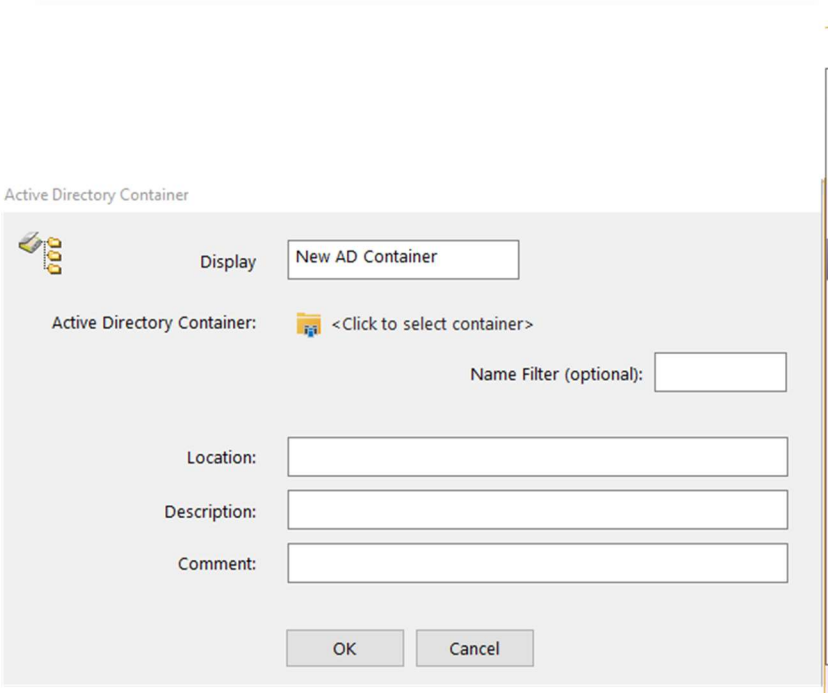
There are three types of containers that can be added to Goverlan.

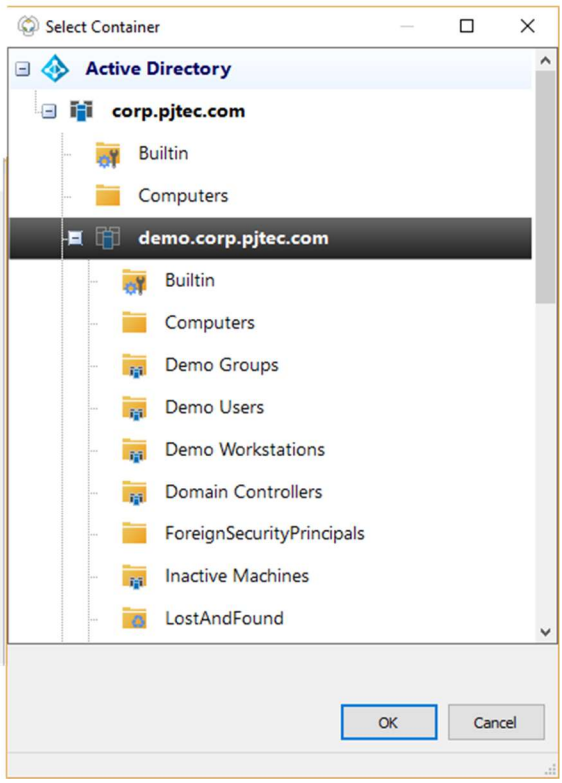
© Copyrights Goverlan Inc. – All Rights Reserved

- Static Containers - These are standard static folders. Other containers, devices, or Goverlan Reach devices can be added to these folders.
    - Static Reach Containers – When adding nodes to a static container, Reach nodes can also be added to any static container via the Advanced menu.
- Active Directory Containers - These are containers based on an OU. These are live containers and will always change as computers are added or removed from the OU.
- IP Range Containers - These containers are based on an IP subnet. These are live containers and will always change as devices are configured with an IP in that subnet. IPv4 and IPv6 ranges are supported

To add your first container, right-click the Favorites folder and select Add Container

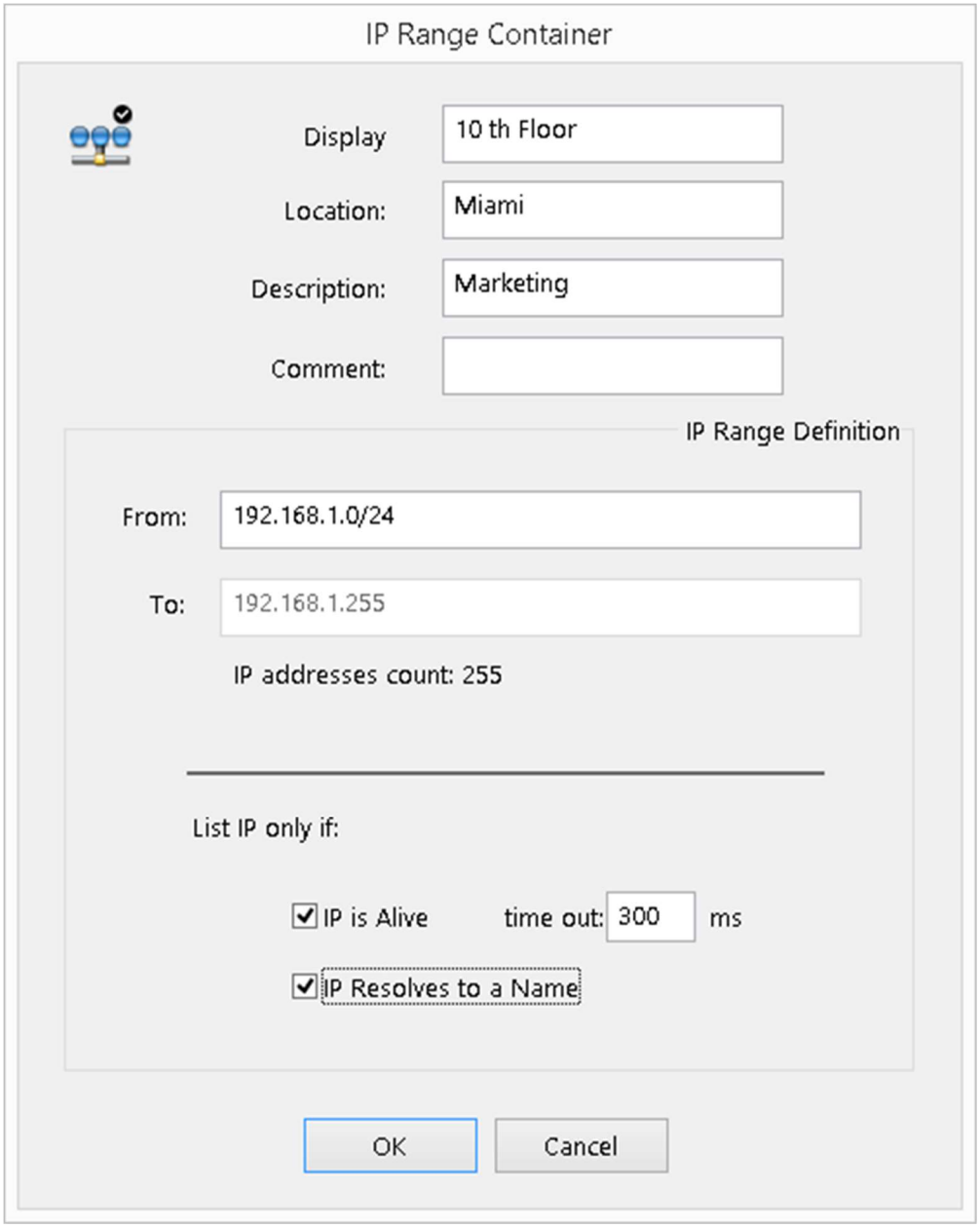
AD Container Configuration





IP Range Container Configuration

© Copyrights Goverlan Inc. – All Rights Reserved



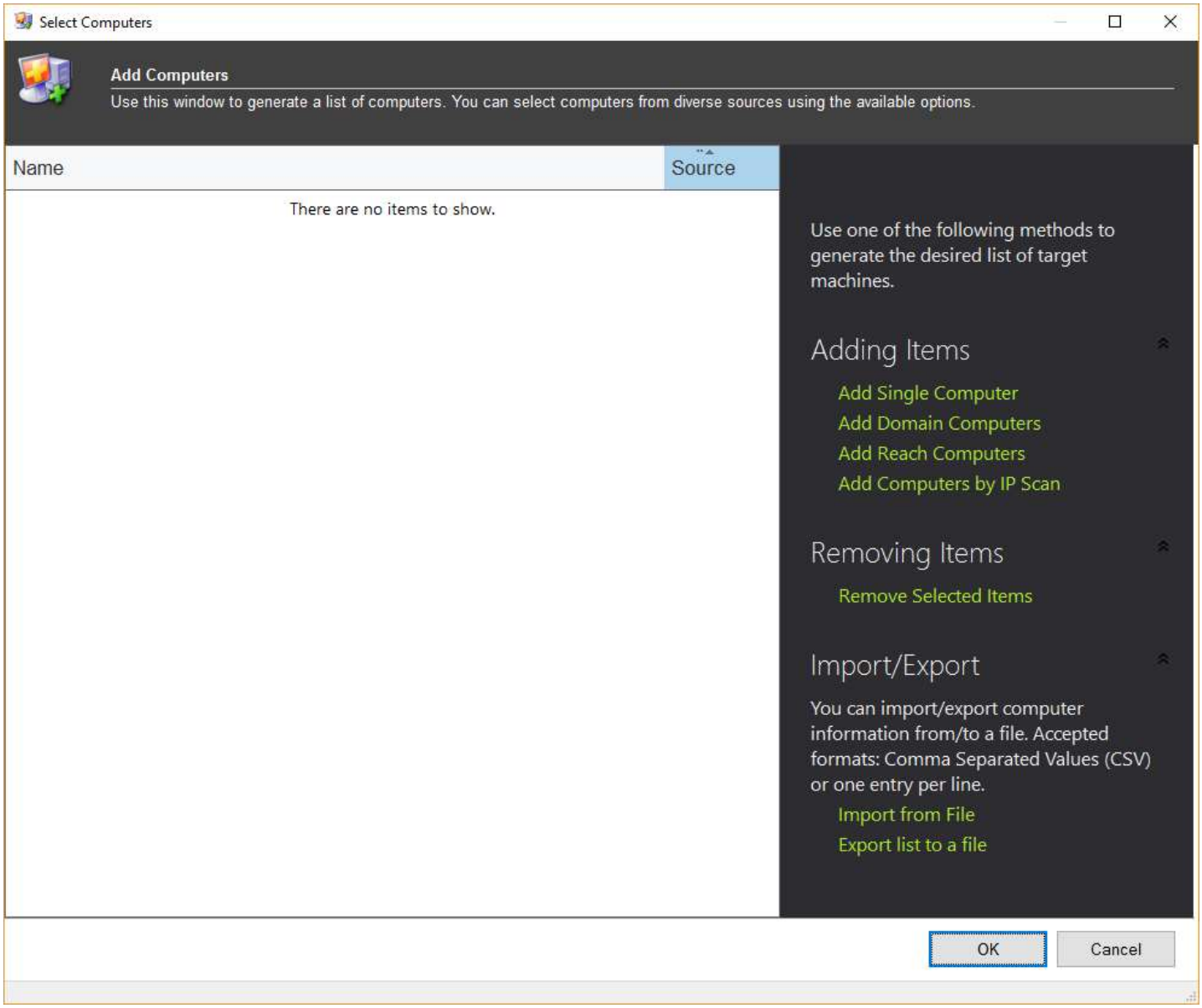
Adding Computers/Devices

Goverlan supports many different protocols, any device that communicates over these protocols can be added in the Favorites section.

Right-click the Favorites folder or any Static Container and select Add Computer.

Use the Advanced button to search for advanced search or importing options

© Copyrights Goverlan Inc. – All Rights Reserved

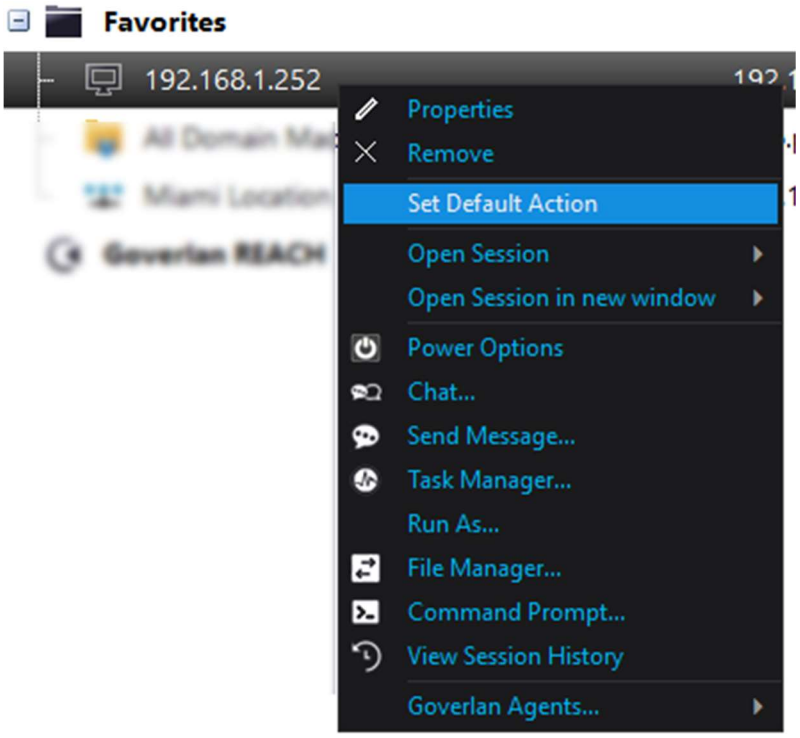


Setting Default Actions

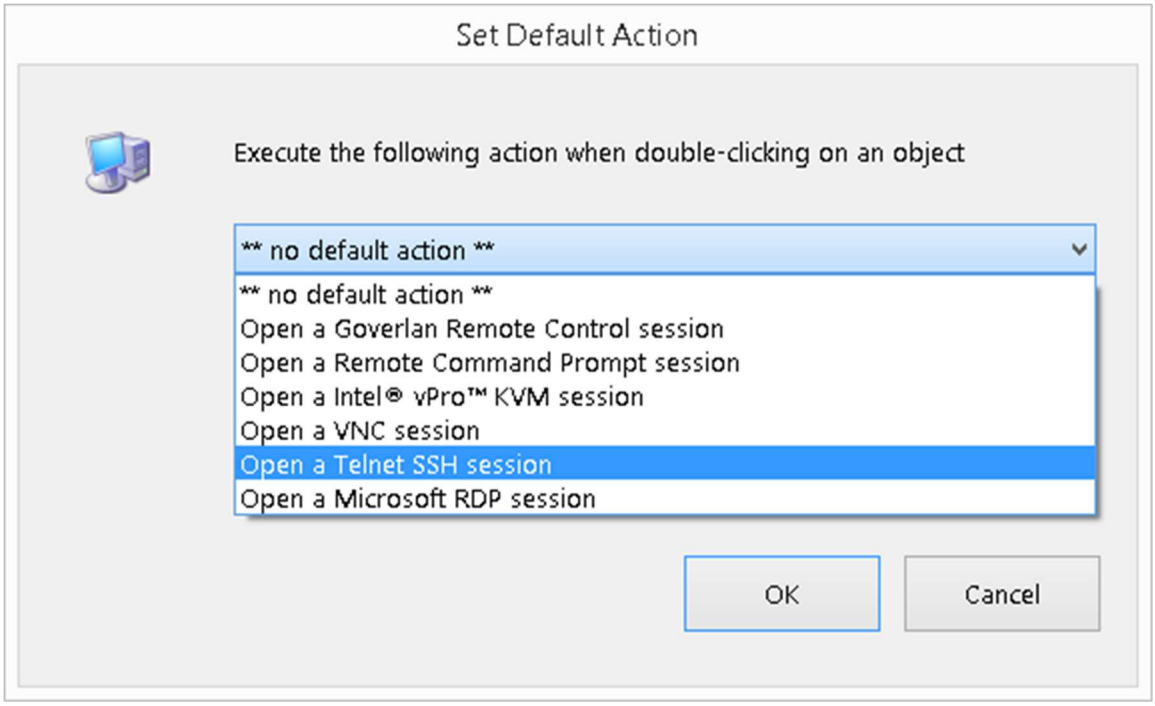
Setting a Default Action will assign a specific protocol to the computer/device or on the container level.

To set the Default Action, right click the computer/device or container and select Set Default Action.

© Copyrights Goverlan Inc. – All Rights Reserved



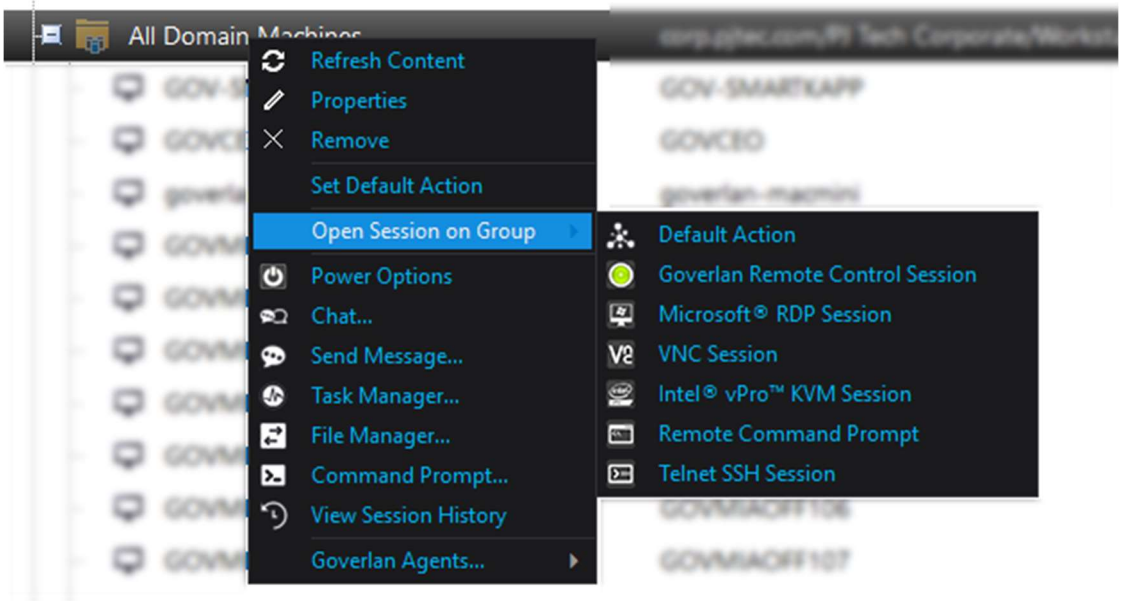
Use the drop-down menu to set the default protocol for that device.



Open session on group

Start the Goverlan Monitoring View by right-clicking any container and selecting Open Session on Group. For more information about Monitoring View, see Managing your Workspace, or Performance Monitoring.

© Copyrights Goverlan Inc. – All Rights Reserved



Right Click Actions

Perform the following actions by right clicking on any device.

- **Properties** - A simple properties window for the device
- **Power Options** - View the status of a Windows based computers and control its power state. This includes Intel vPro options. See Power Options
- **Chat** - Initiate a chat session with the target workstation. See Chat and Push messages
- **Send Message** - Send a push notification to the target workstation. See Chat and Push messages
- **Task Manager** - Start the Goverlan Advanced Task Manager. See Goverlan Task Manager Overview
- **Run As** - Start a command on the remote workstation. See Goverlan Task Manager Overview
- **File Manager** - Start the Goverlan File Manager focused on the target workstation. See Using the File Manager
- **Command Prompt** - Open a remote command prompt focused on the target workstation. See Windows Remote CMD
- **View Session Log** - Open the Goverlan Reach RC Session Log. See Auditing of Goverlan Reach RC Events
- **Goverlan Client** - Install or Remove the Goverlan Client. See Installing the Goverlan Client

REFERENCES

- Configuring Team Collaboration
- Managing your Workspace
- Performance Monitoring
- Power Options

© Copyrights Goverlan Inc. – All Rights Reserved

- Chat and Push messages
- Goverlan Task Manager Overview
- Using the File Manager
- Windows Remote CMD
- Auditing of Goverlan Reach RC Events
- Installing the Goverlan Client

Goverlan Reach RC Client Settings

Customizing Client Behavior

Goverlan allows you to customize many aspects of the Client behavior. This feature allows the Goverlan Client to perform actions before or after a remote control session is initiated.

Goverlan Client behavior is performed via settings distribution by either using a Group Policy Object (for Active Directory environments), or via the Goverlan Reach Server (see: Using Universal Settings Distribution).

Customizing Goverlan Client Behavior via a Group Policy Object

Once you have uploaded the provided Goverlan Group Policy Administrative Templates onto your Active Directory, expand Computer Configuration > Policies > Administrative Templates > Goverlan Universal Settings > Remote Control Client Settings.

Once you have configured the Group Policy settings, you will need to wait for those to be distributed onto your machines before you can see the text modifications. To test your settings on a client machine, open a command prompt on this one and execute a gpupdate.exe command.

Customizing Goverlan Client Behavior via the Goverlan Reach Server

You can also use the Goverlan Reach Server to distribute Goverlan Client Behavior settings onto your machines. Once you have implemented and registered a Goverlan Reach Server, use the Universal Settings Distribution feature to configure the Goverlan Client behavior customizations.

Once your changes have been published, the Goverlan Client behavior modifications are instantaneously reflected on your client machines.

© Copyrights Goverlan Inc. – All Rights Reserved

Pre-Session Actions

Pre-Session options determine how the Goverlan Client will respond to an incoming remote control session. The following options are available for Pre-Session Actions:

- No Action - This setting is the default setting. No action will be performed when a session is established.
- Prompt Local User for Approval - This setting will allow the remote use to accept or deny an incoming session.
- Disable Remote Control - This setting will disable the ability to initiate a Remote Control session with the remote system.
- Lock the Computer - This setting will lock the remote workstation when a new session is attempted.
- Logout the local user - This setting will log off the remote user when a session is attempted.

Post-Session Actions

Post-Session actions determine how the Goverlan Client will respond after the session is completed. The following options are available for Post-Session actions:

- No Action - This is the default setting. No Action will be performed when the session is completed.
- Lock the computer - This setting will lock the screen of the remote system when the session is completed.
- Logout the local user - This setting will log out the remote user after the session is completed.

Post-Session Notification Pop-up

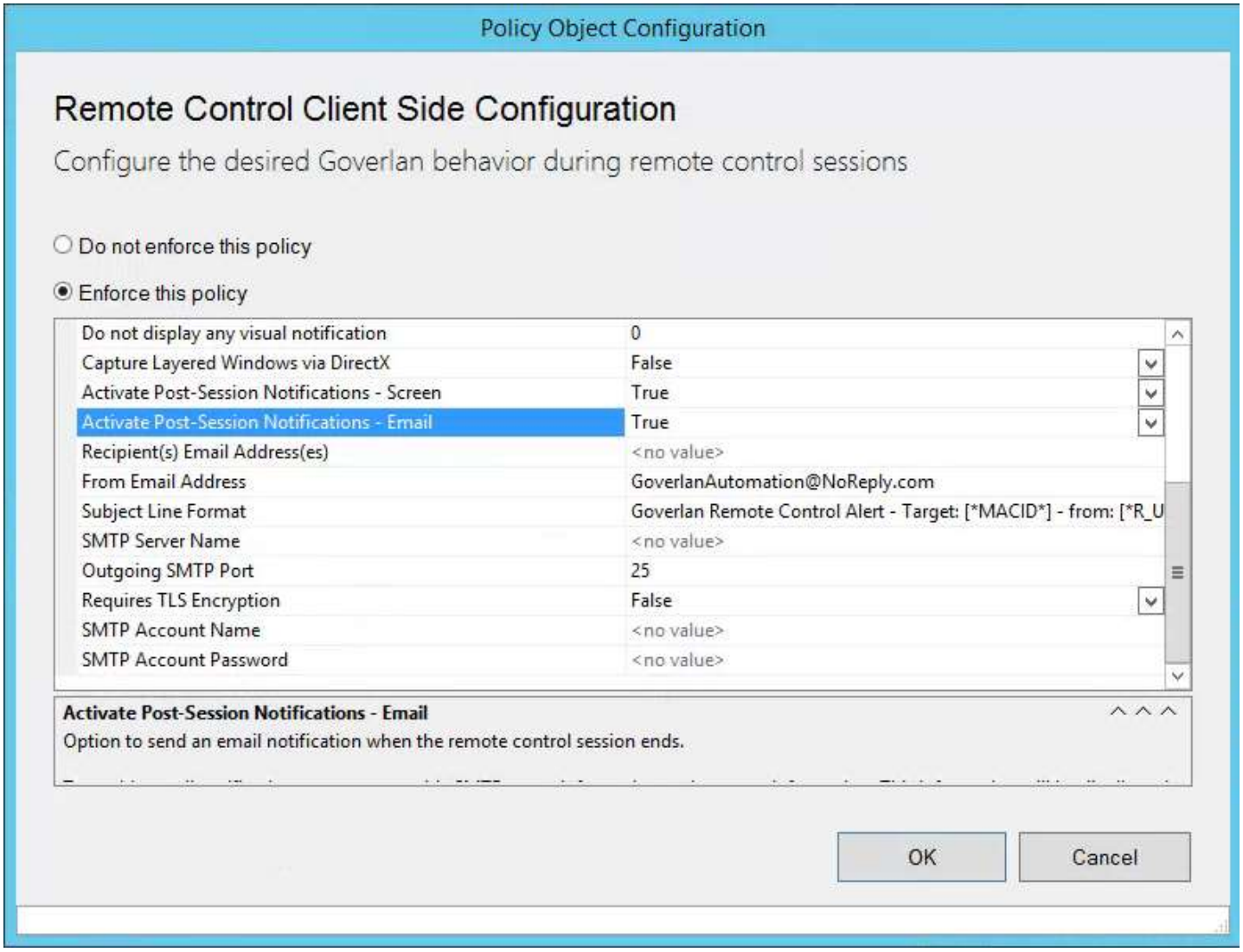
The Post-Session Notification Pop-up can be displayed after a session is complete.

Post-Session Email Notification

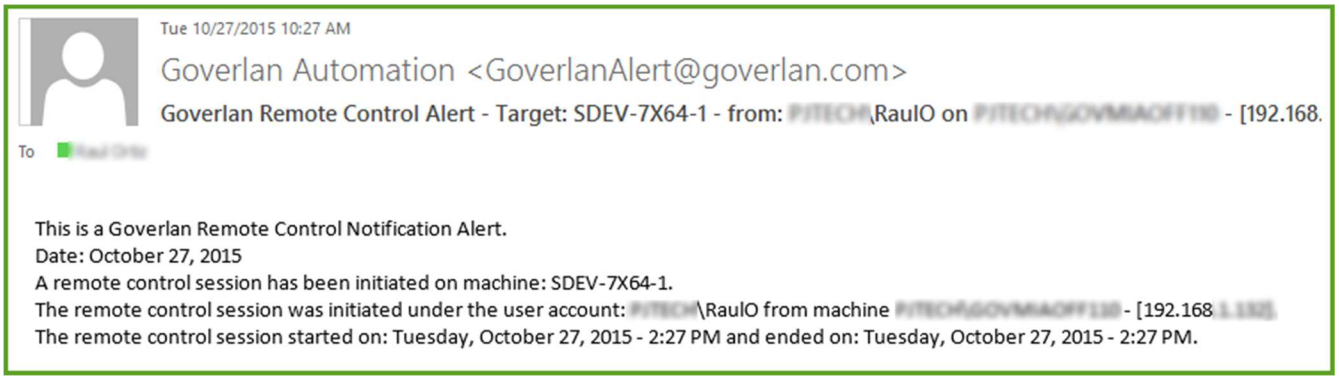
The Email Notification feature will send an email to a specified account after a session completes.

The following settings need to be configured via the GPO Admin Template or the GRS.

© Copyrights Goverlan Inc. – All Rights Reserved



Email Example:



Configuring Authorization

All Goverlan Reach RC sessions need to be properly authorized to successfully open. By default, the person initiating the remote control session must be a Local Administrator of that machine. However, it is possible to configure a machine to accept Goverlan Reach RC sessions from a specified set of user accounts, bypassing this requirement.

© Copyrights Goverlan Inc. – All Rights Reserved

Explicitly authorizing a set of accounts to initiate remote control sessions on a machine doesn't mean that the remote control session will be approved. Remote Control sessions can be attempted. For instance, if a machine is configured to prompt the console user to approve a remote control session, and the console user rejects the session, the session will not continue, even though it was authorized.

Explicitly Authorizing User Accounts with No Local Administrative Privileges

You can configure a machine or a set of machines to accept remote control sessions from accounts which do not belong to the local administrator's group. To do so, create a local group named 'Goverlan Remote Control Admins' and add the authorized accounts to the group. A user account doesn't need to be a direct member of the Goverlan Remote Control Admins local group. It can belong to a domain global group which belongs to Goverlan Remote Control Admins.

Configuring authorization on a single machine

- Create a local group named: **Goverlan Remote Control Admins** in the machine's local account database.
- Insert the domain accounts which are authorized to initiate remote control sessions on that machine.

Configuring authorization for all machines in a domain

- Create a **domain local group** named: **Goverlan Remote Control Admins** in the domain which contains all the machines to configure.
- Insert the domain accounts which are authorized to initiate remote control sessions on that machine.

In the case above, all computers which belong to the domain where the Goverlan Remote Control Admins local group has been created will use the group for authorization of local remote control sessions.

> **Note:** In this configuration, a Goverlan Remote Control Admins local group defined on a machine takes precedence over the Goverlan Remote Control Admins local group defined at the domain level.
>
> **Note:** The name of the group MUST be called **Goverlan Remote Control Admins**.

Custom Branding

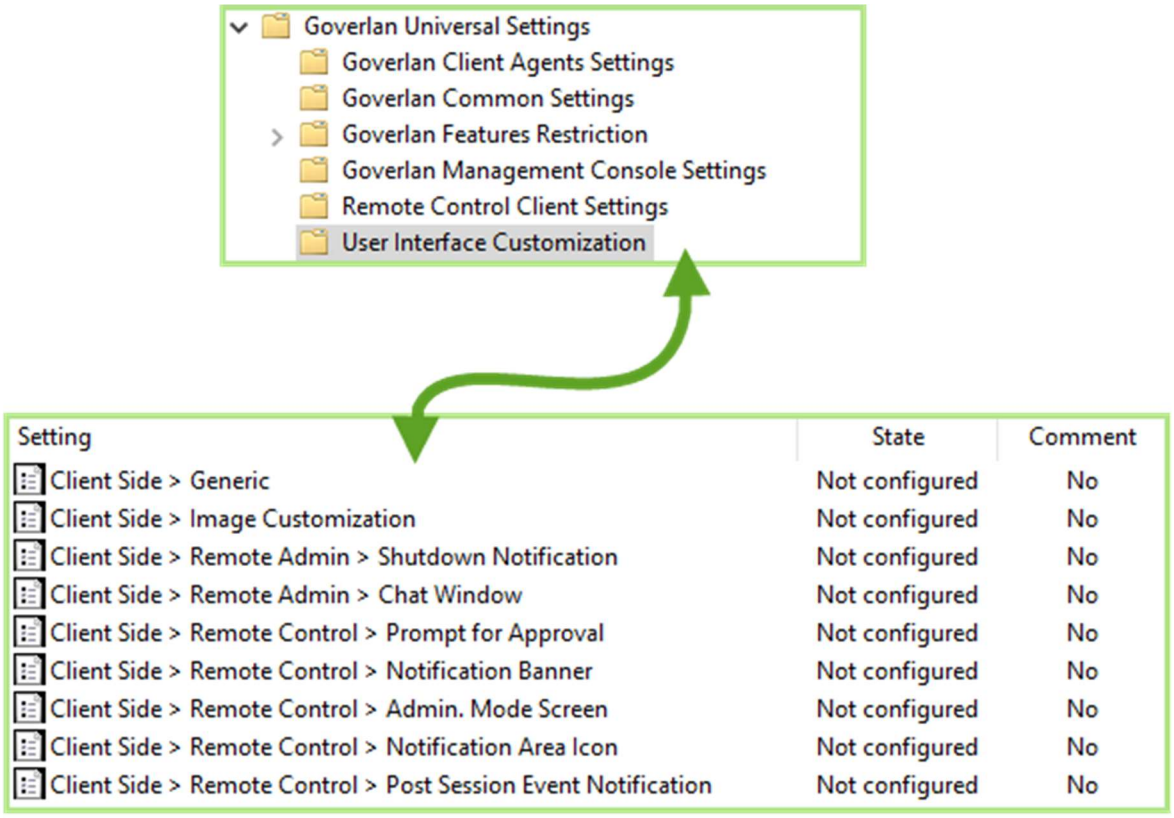
Goverlan allows you to customize most text displayed on the client machine as well as some images. This feature allows you to perform company branding or to localize the client side user interface into another language.

User Interface customizing is performed via settings distribution by either using a Group Policy Object (for Active Directory environments), or via the Goverlan Reach Server (see: Using Universal Settings Distribution).

© Copyrights Goverlan Inc. – All Rights Reserved

Customizing Text via a Group Policy Object

Once you have uploaded the provided Goverlan Group Policy Administrative Templates onto your Active Directory, expand the Goverlan Universal Settings > User Interface Customization category



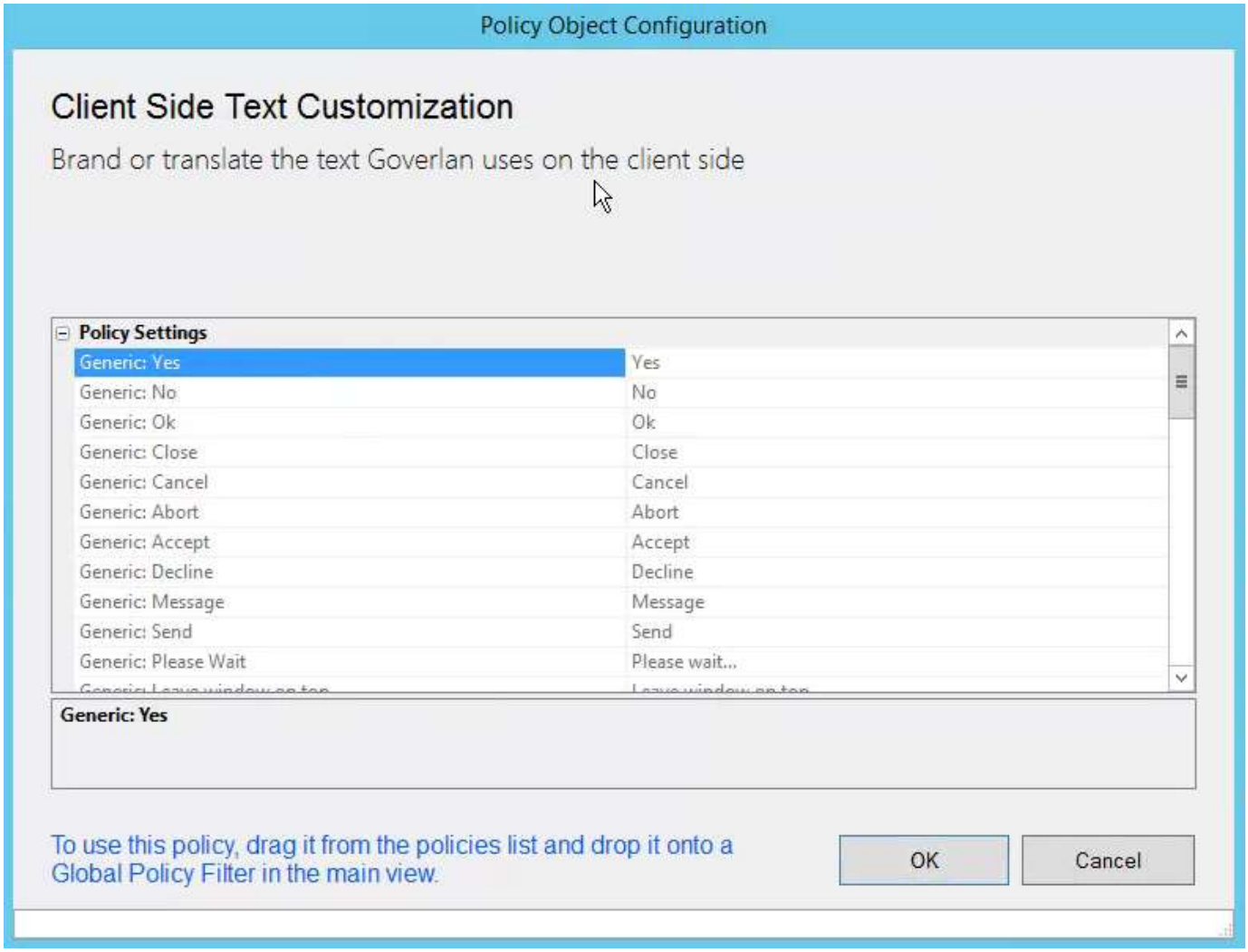
The User Interface Customization folder contains a setting policy for each of the user interface items on the client's side. To modify the text of an item, enable the setting item and change its contents.

Once you have configured the Group Policy settings, you will need to wait for those to be distributed onto your machines before you can see the text modifications. To test your settings on a client machine, open a command prompt on this one and execute a gpupdate.exe command.

Customizing Text via the Goverlan Reach Server

You can also use the Goverlan Reach Server to distribute text customization onto your machines. Once you have implemented and registered a Goverlan Reach Server, use the Universal Settings Distribution feature to configure the text customizations.

© Copyrights Goverlan Inc. – All Rights Reserved



Once your changes have been published, the text modifications are instantaneously reflected on your client machines.

Text Customization Definition

Text customizations are divided by category. Except for the Generic category, each defines a specific user interface window on the client machine. The following defines these categories.

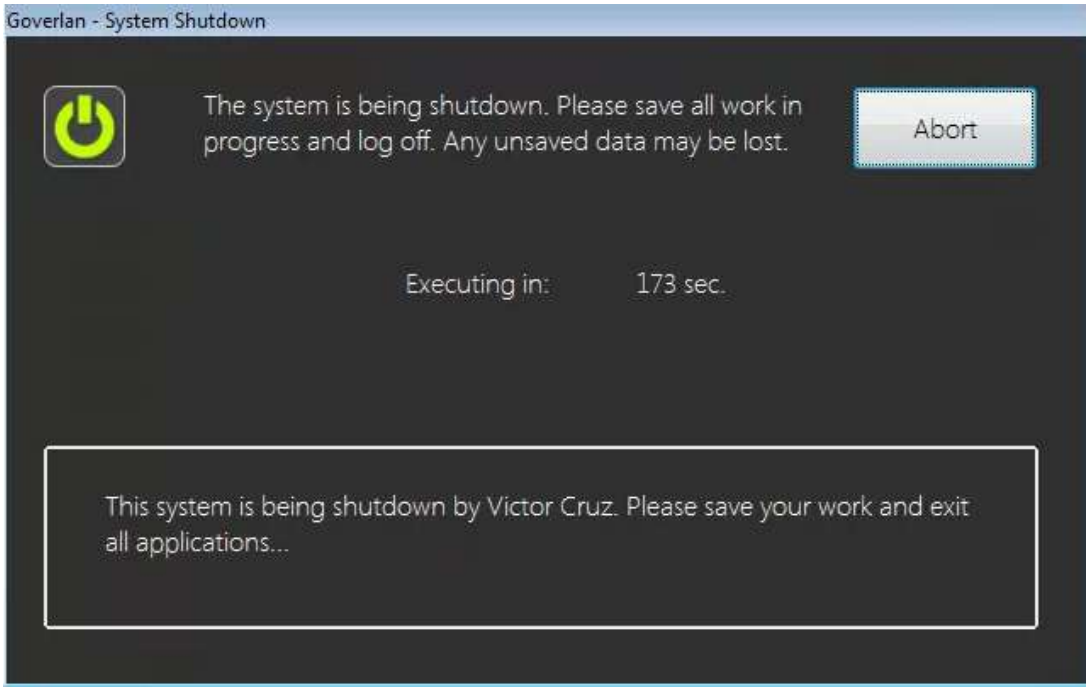
Client Side > Generic

This setting set defines generic strings used on the client side. For instance, the string to be used for "Yes", "No", "Ok", "Close" etc.

Client Side > Remote Admin > Shutdown Notification

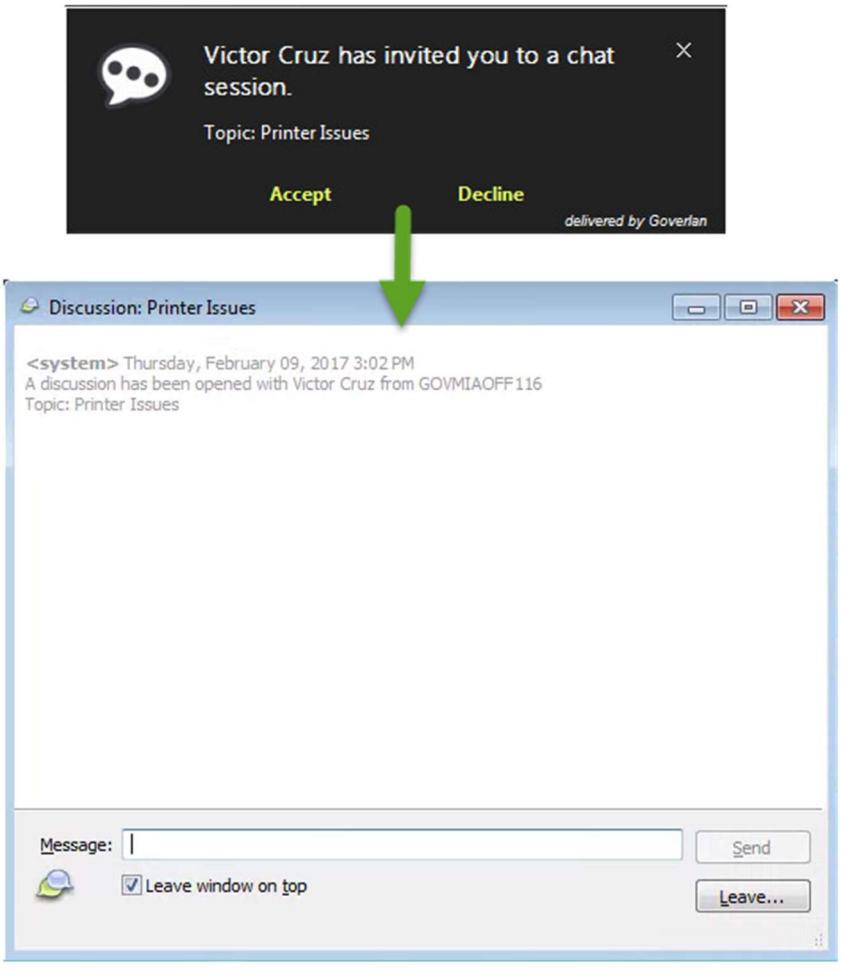
This setting set defines the text used during the notification of a Shutdown, Reboot, or Logoff action:

© Copyrights Goverlan Inc. – All Rights Reserved



Client Side > Remote Admin > Chat Window

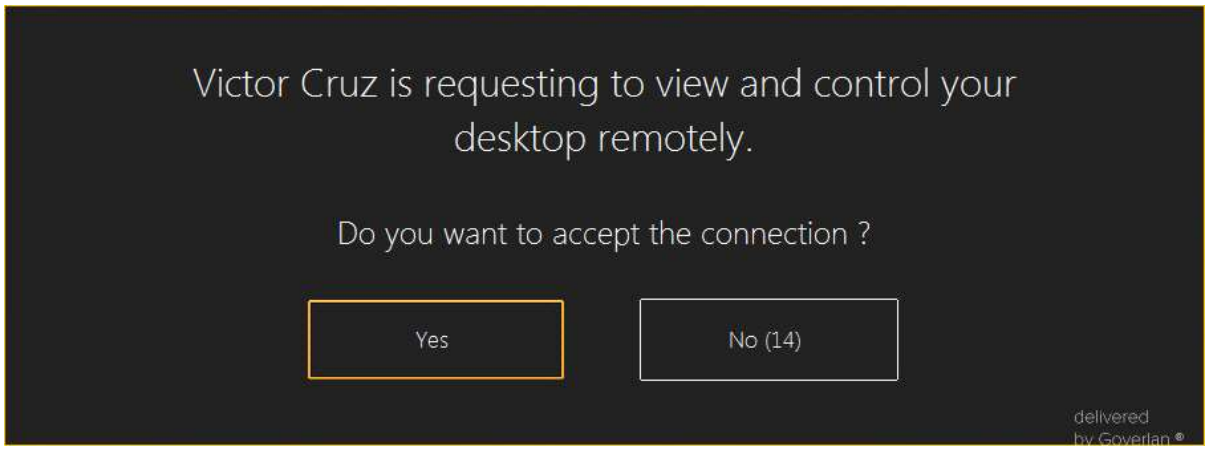
This setting set defines the text used by the Chat client window:



Client Side > Remote Control > Prompt for Approval

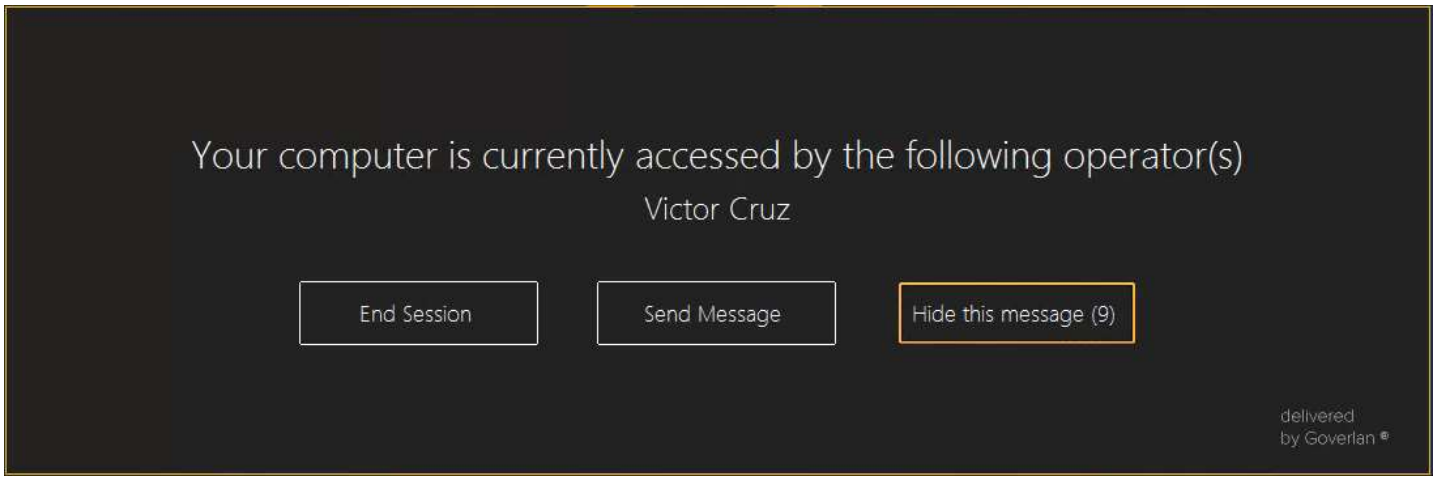
© Copyrights Goverlan Inc. – All Rights Reserved

This setting set defines the text used by the Goverlan Reach RC Prompt for Approval window during a remote control session:



Client Side > Remote Control > Notification Banner

This setting set defines the text used by the Goverlan Remote Control Notification window displayed on the client machine during a remote control session:



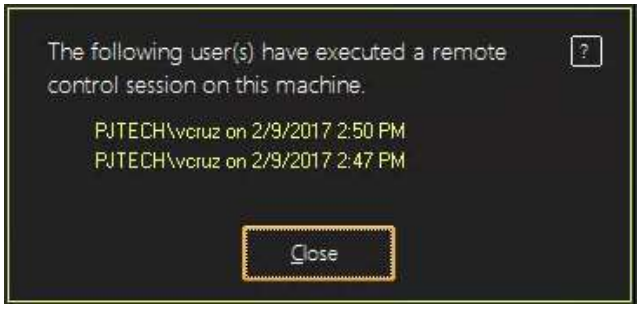
Client Side > Remote Control > Notification Area Icon

This setting set defines the text displayed on the client's machine during a remote control session when the end user places the mouse cursor over the Goverlan Reach RC icon in the Windows notification area:

Client Side > Remote Control > Post Session Event Notification

This setting set defines the text used by the Goverlan Reach RC Notification window displayed on the client machine after a remote control session has terminated:

© Copyrights Goverlan Inc. – All Rights Reserved

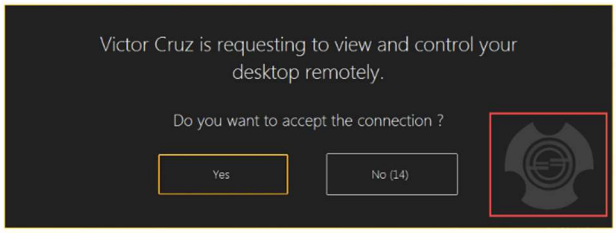


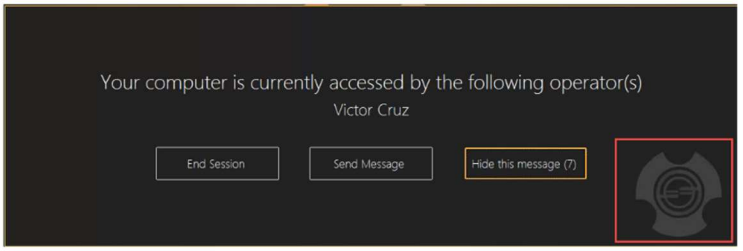
Client Side > Image Customization

These settings define the images to be used by miscellaneous windows on the client side. To change the image of a window, generate a transparent image of the requested size in a transparent PNG 24-bit format. Place the image in a network share and specify its full UNC path including file name in the appropriate policy setting.

Logo Branding - 128x128 - PNG

A 128 by 128-pixel image which is used by the Remote Control > Prompt Local User for Approval as well as Remote Control > Notification Banner windows.





E.G.: \\SOMESERVER\SOMESHARE\Goverlan_ImagesCoLogo_128.png

Supported Connection Protocols

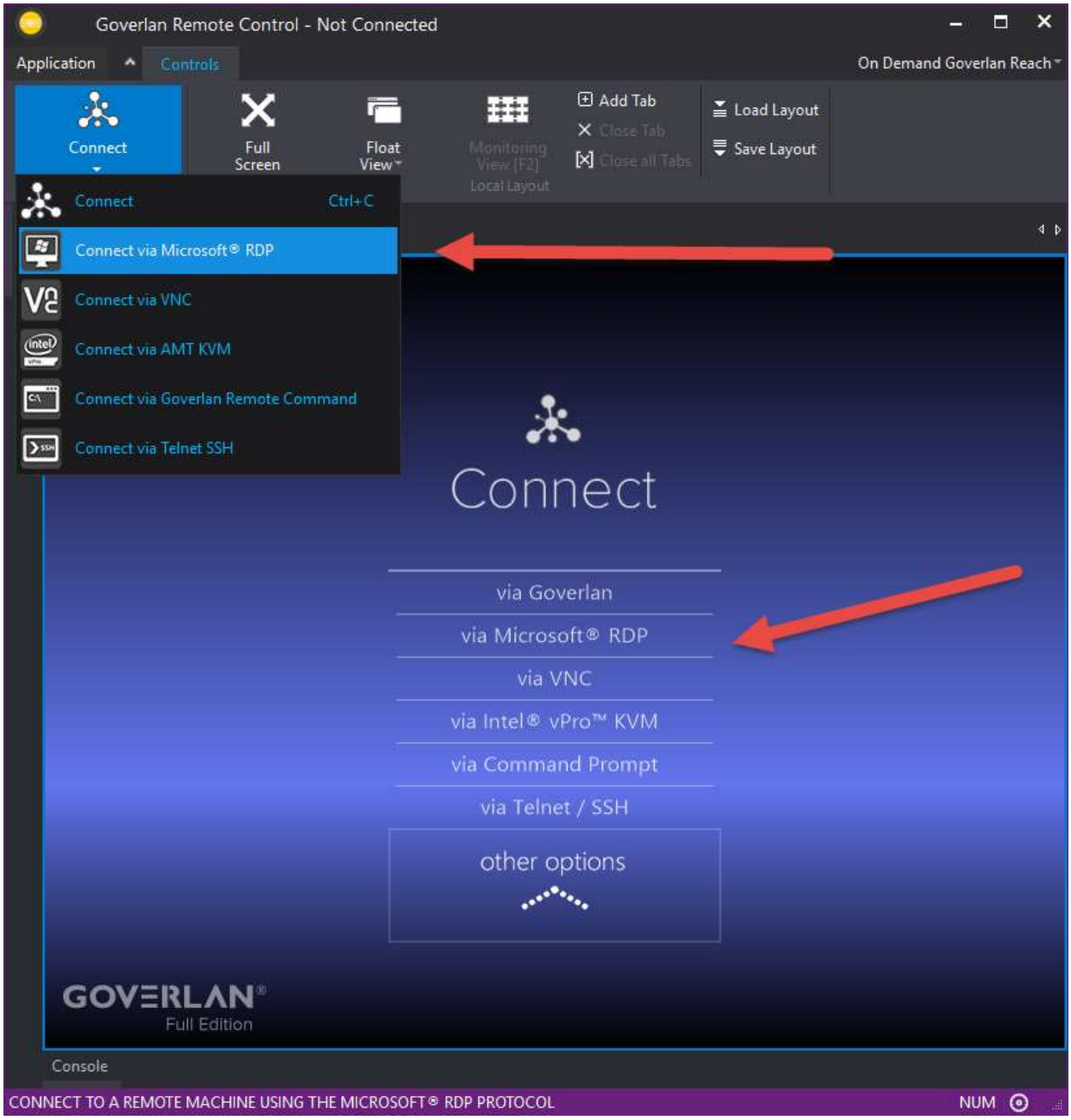
Microsoft RDP Protocol

Goverlan Reach RC can connect via Microsoft RDP.

Establishing an RDP session with Goverlan

Use the Connect button in the Command Bar or in the More Options section.

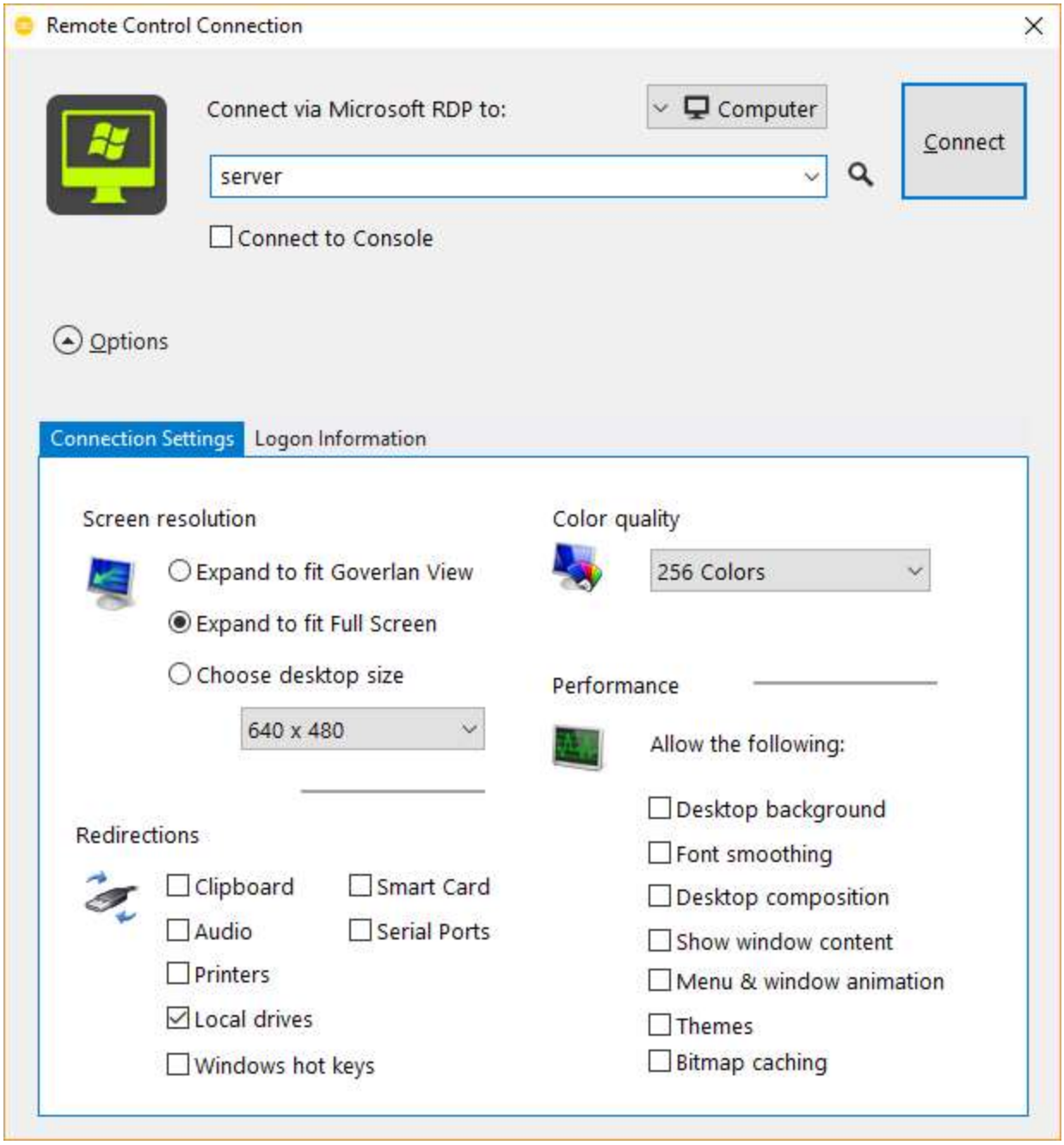
© Copyrights Goverlan Inc. – All Rights Reserved



RDP Connection Settings

Goverlan Reach RC supports many RDP options

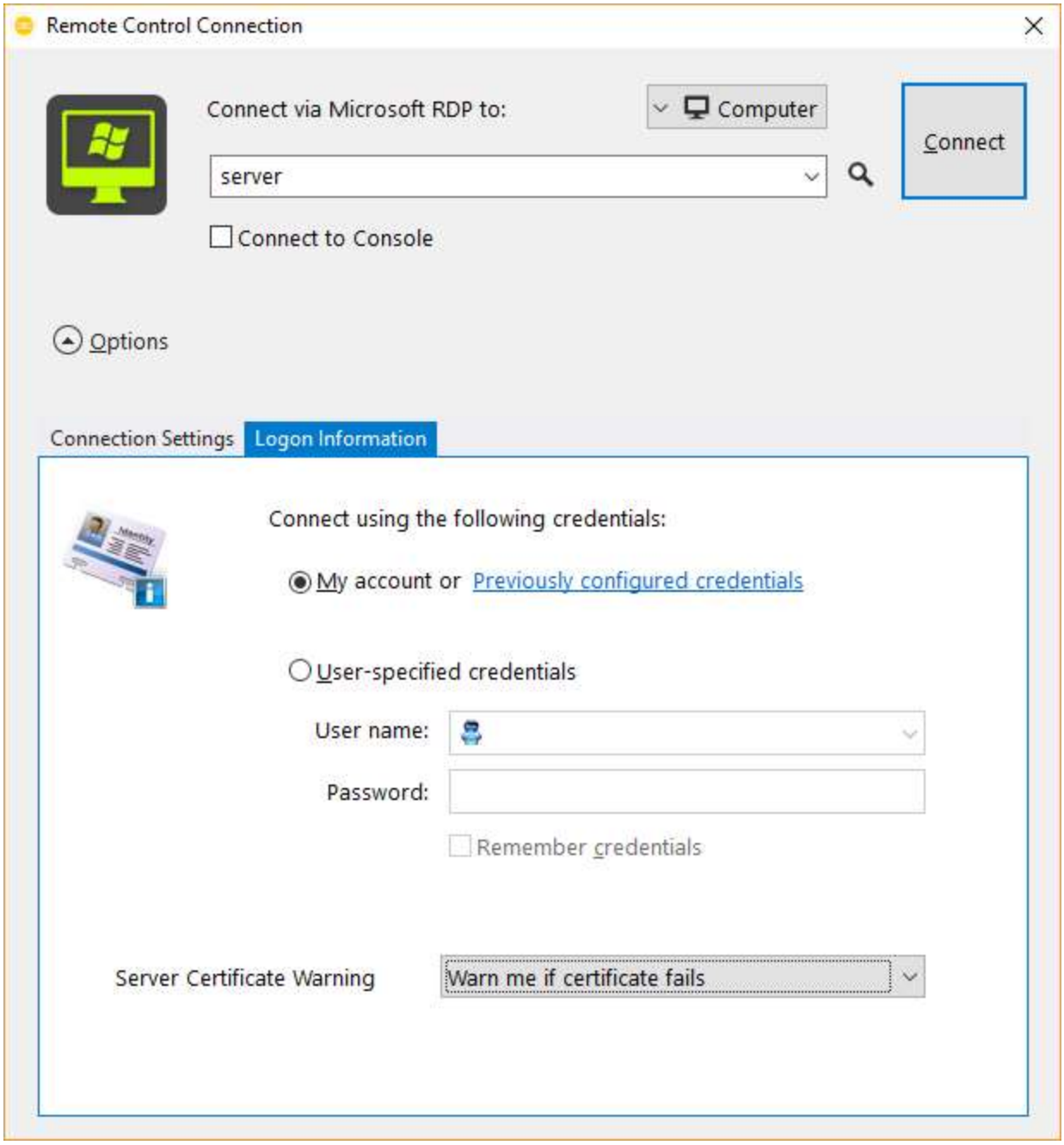
© Copyrights Goverlan Inc. – All Rights Reserved



Saving RDP Credentials in Goverlan Reach RC

Use the Logon Information Tab to save RDP credentials. Credentials will be stored in the Credential Manager. For more information on the Credential Manager, see Goverlan Credential Manager.

© Copyrights Goverlan Inc. – All Rights Reserved



Certificate based RDP Connections

Goverlan supports Certificate RDP connection. Use the Security drop down and select the appropriate connection type.

REFERENCES

- Goverlan Credential Manager

© Copyrights Goverlan Inc. – All Rights Reserved

VNC

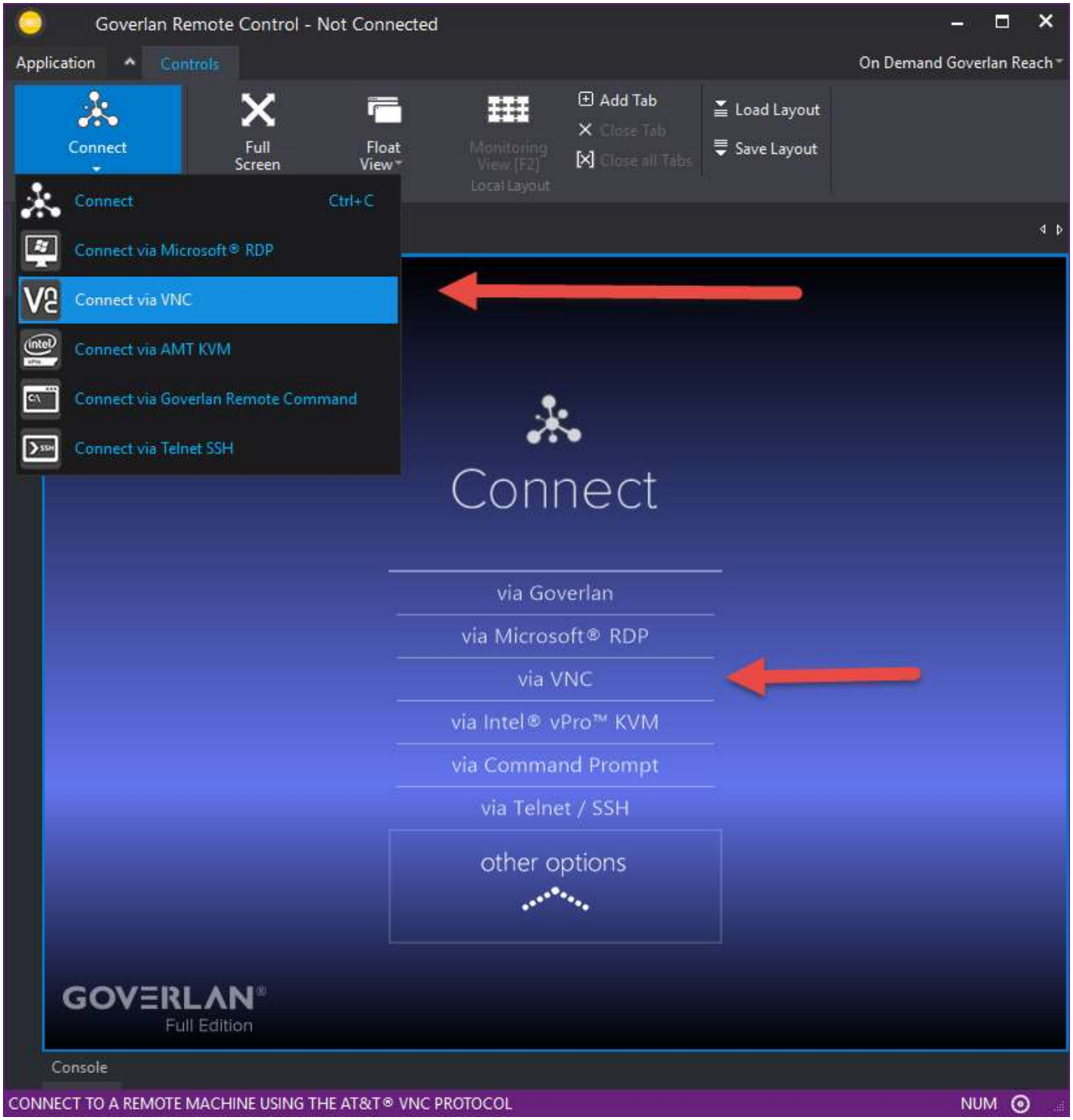
Initiate VNC Connections to Mac, Linux or any other devices running VNC server software.

> NOTE: Mac/Linux Remote Desktop Access must be configured first. Please consult your operating system guides for enabling Remote Desktop Access.

Starting a new VNC connection.

Step 1: Choose VNC from the Connection drop down on the Command Bar or from the Connections Button.

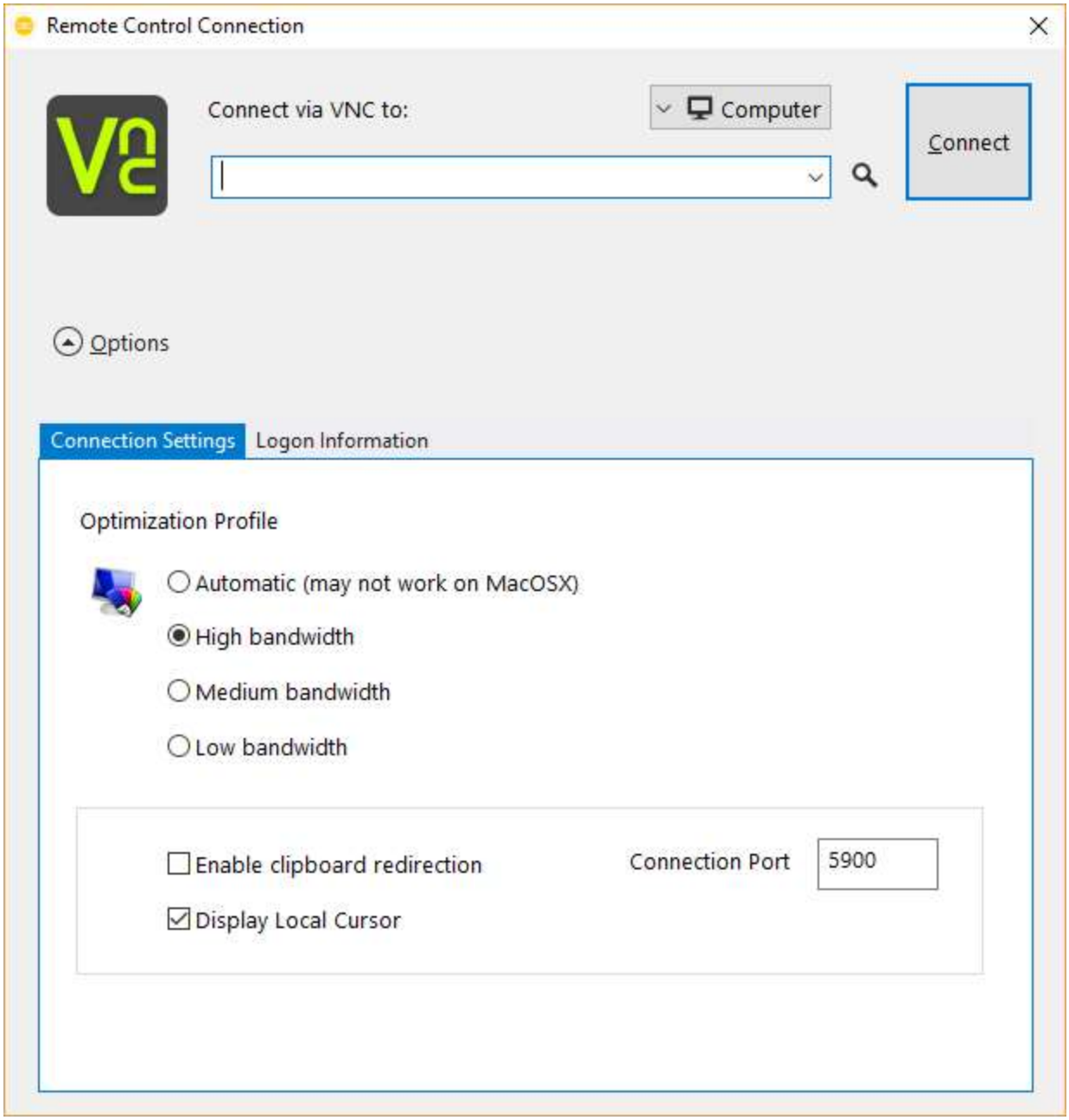
© Copyrights Goverlan Inc. – All Rights Reserved



Step 2: Enter the target system host name or IP address and choose any connection options

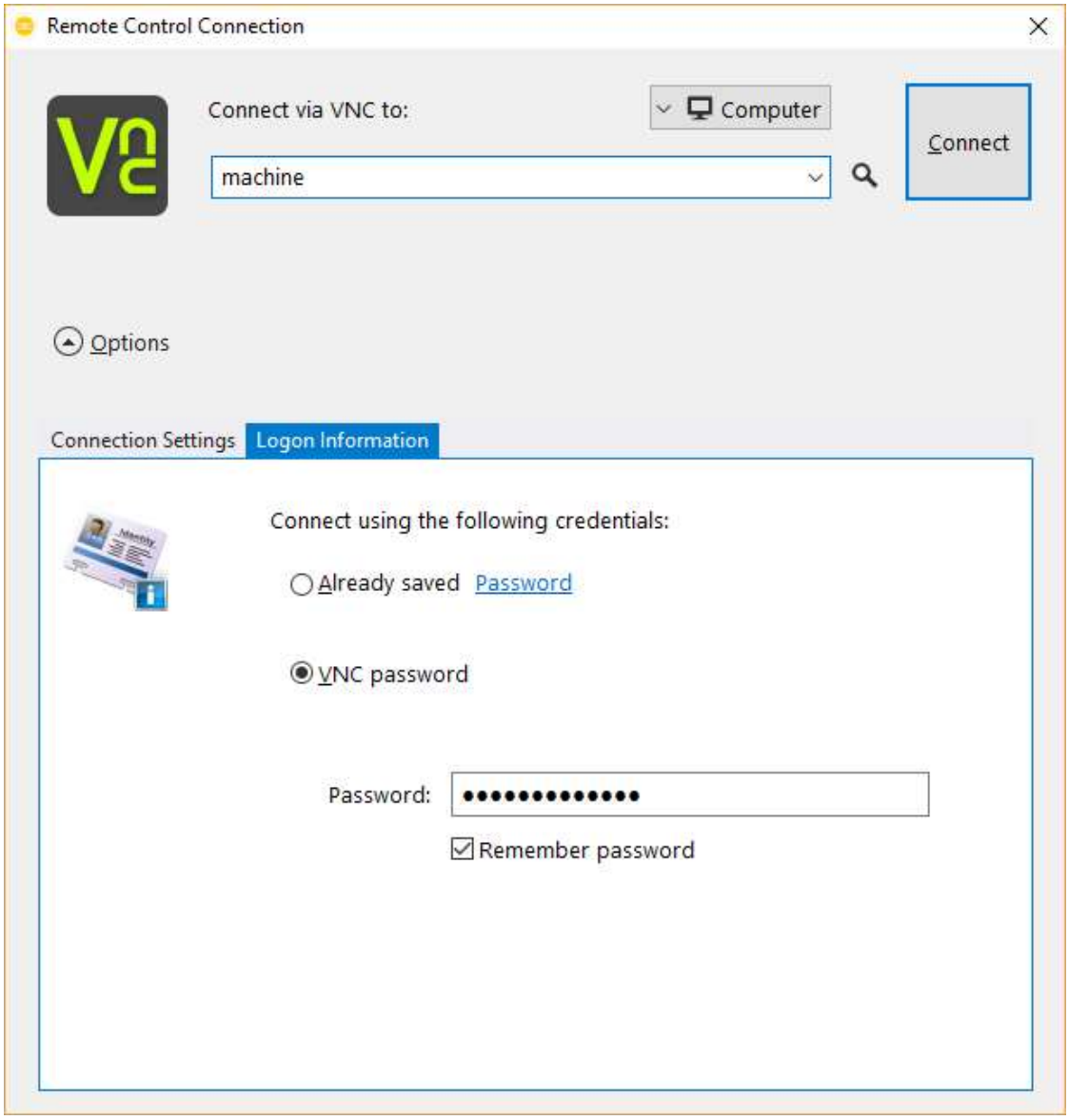
Use the Credential Manager to store VNC credentials for later user. For more information, see Goverlan Credential Manager.

© Copyrights Goverlan Inc. – All Rights Reserved



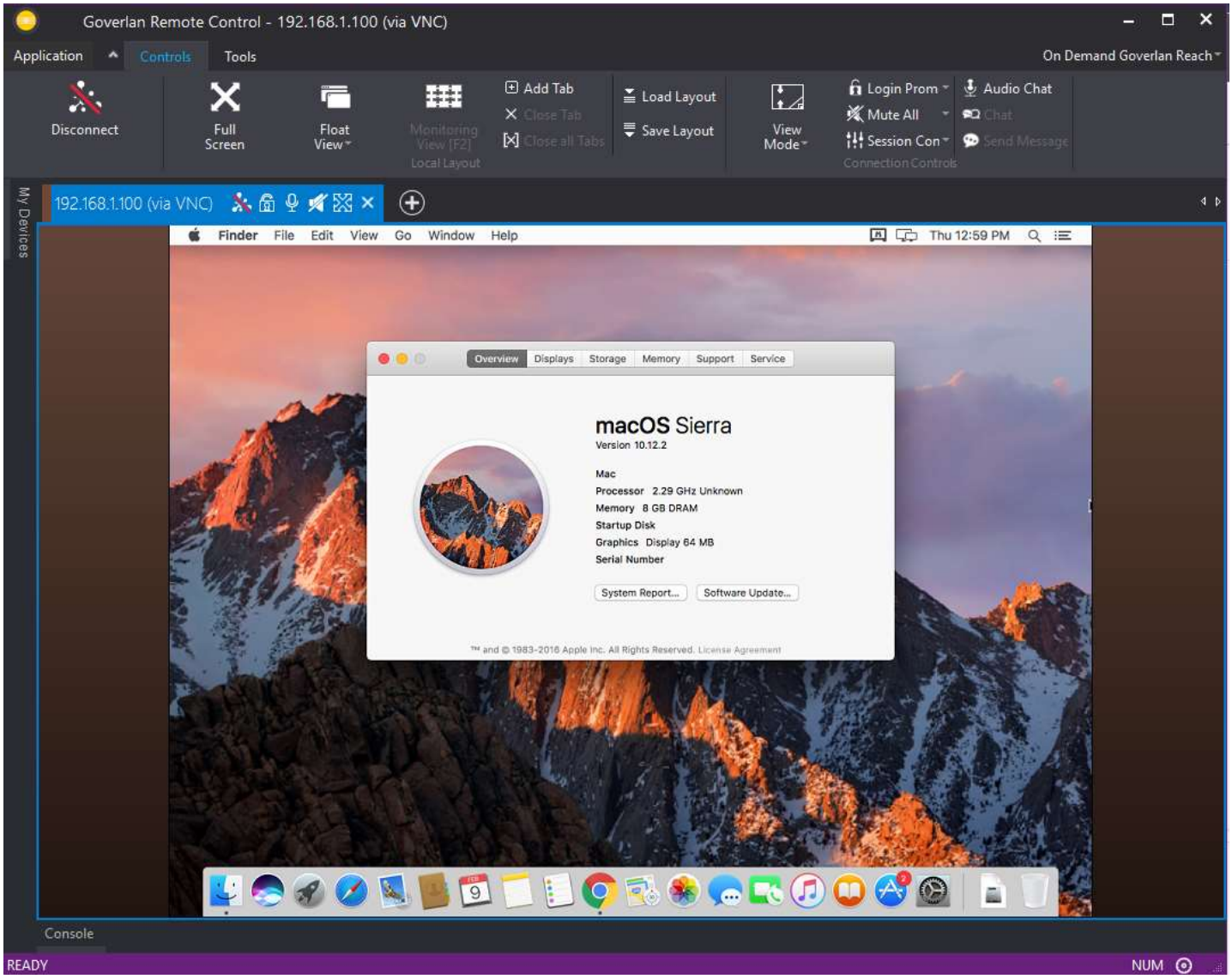
Step 3: Provide VNC Credentials

© Copyrights Goverlan Inc. – All Rights Reserved



Click the Connect button to establish a connection.

© Copyrights Goverlan Inc. – All Rights Reserved



REFERENCES

- Goverlan Credential Manager

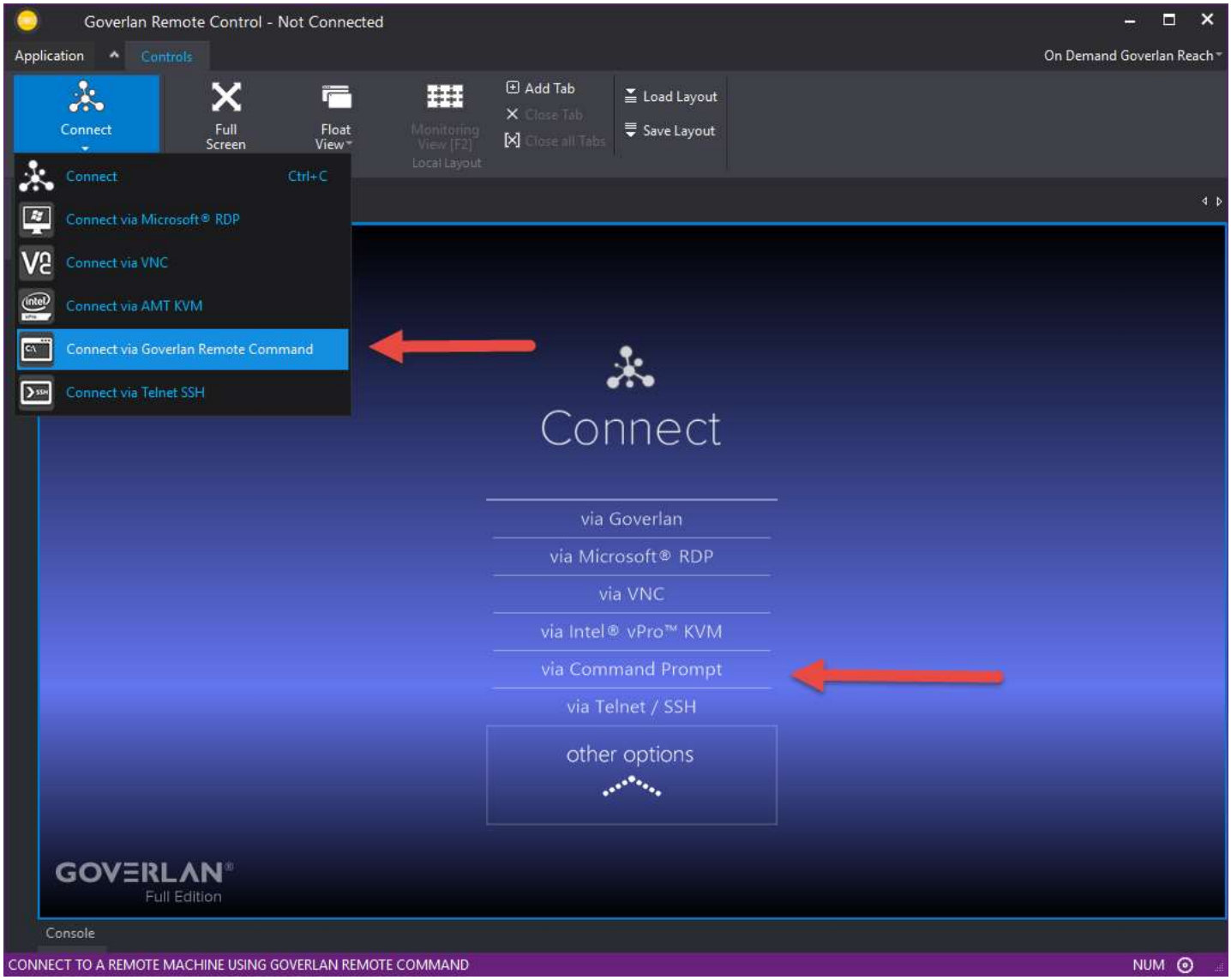
Windows Remote Command Line

Goverlan Reach RC provides easy access to the Command Line or PowerShell Command Line of any Windows system on your network.

Accessing a system by Windows Remote CMD

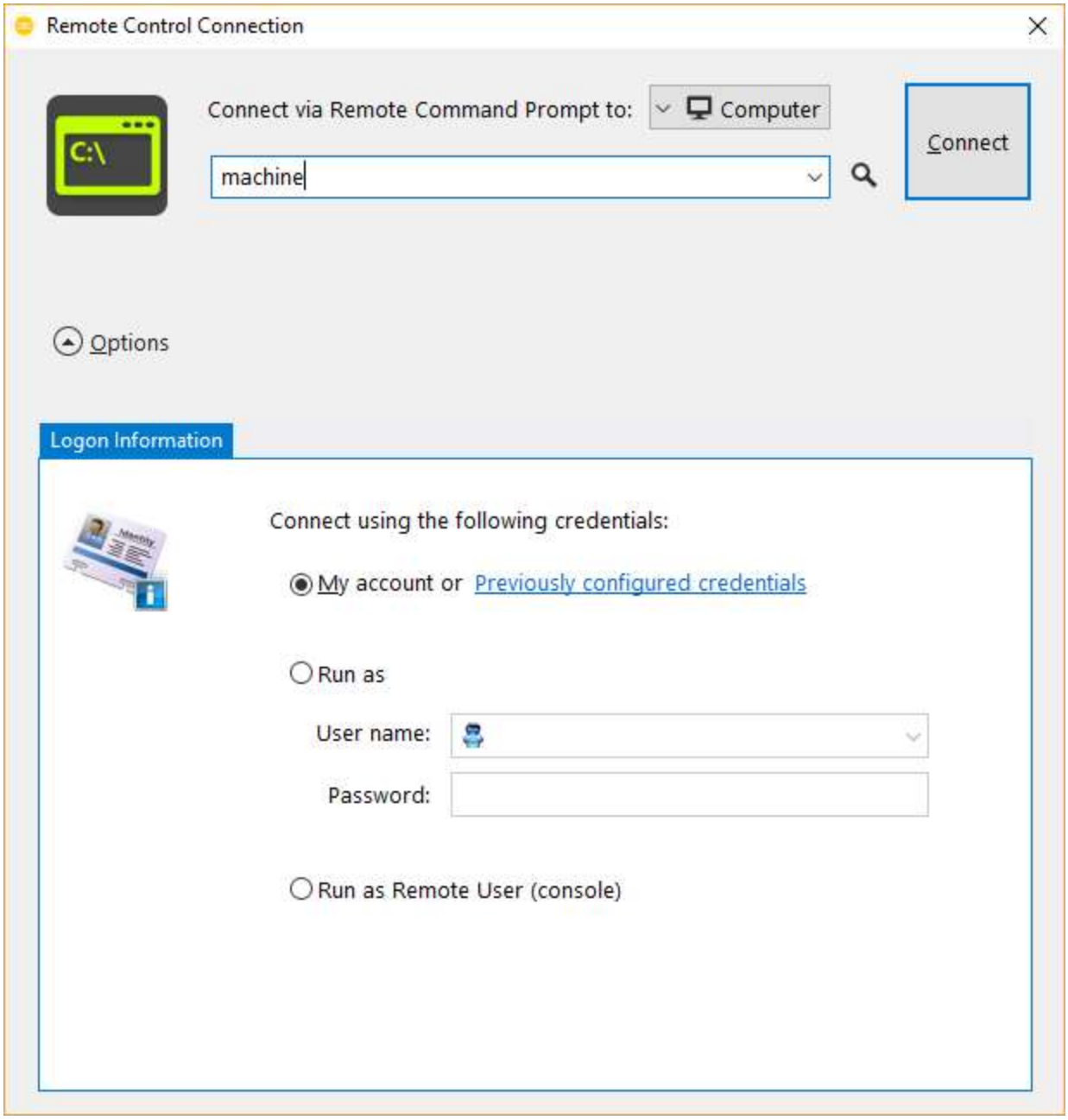
Choose **via Command Prompt** from the More Options drop down or the Connect button drop down in the Command bar.

© Copyrights Goverlan Inc. – All Rights Reserved



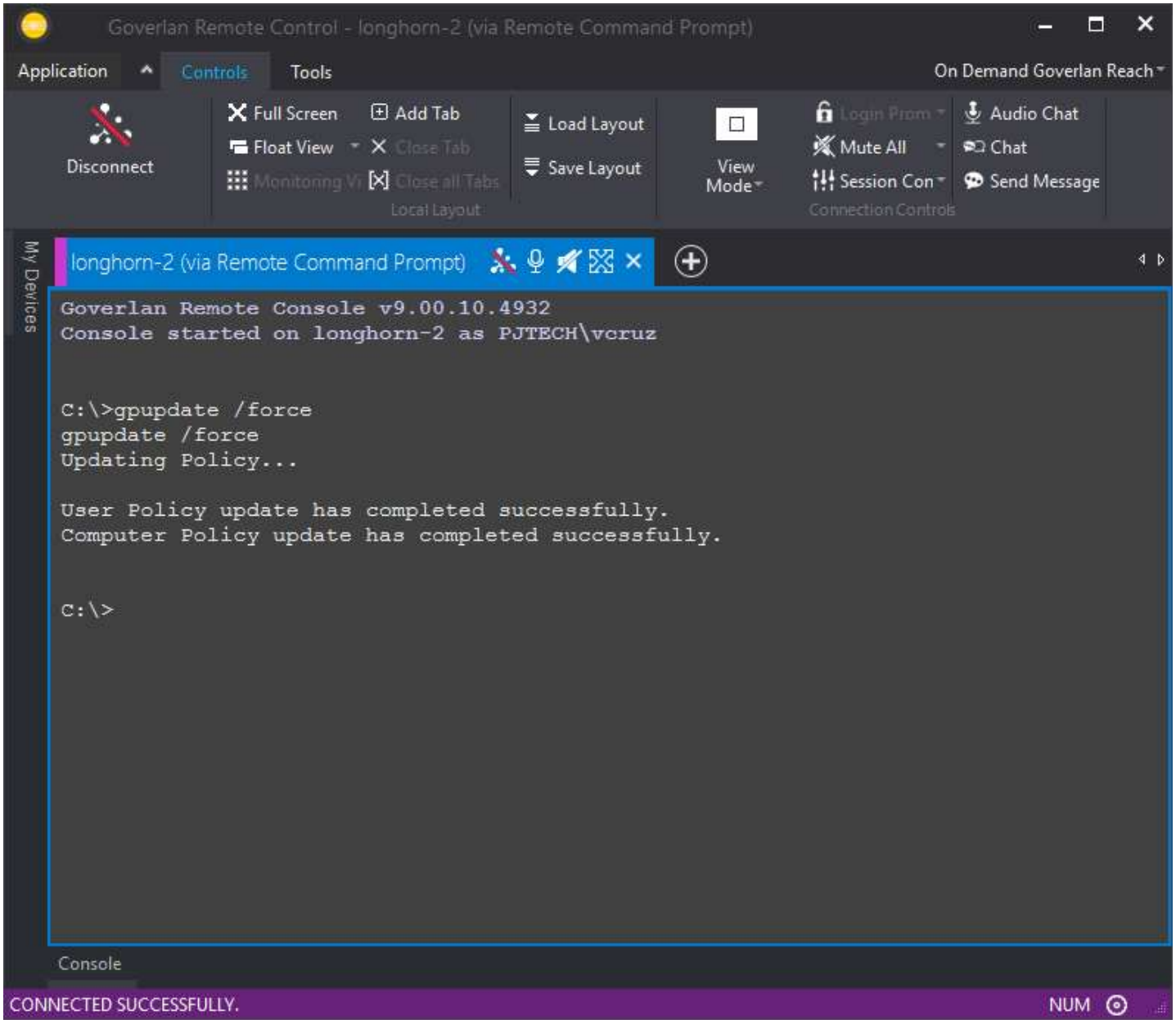
Enter the host name or IP address of the target system and specify the credentials to log in as. Goverlan will use the operator's credentials by default.

© Copyrights Goverlan Inc. – All Rights Reserved



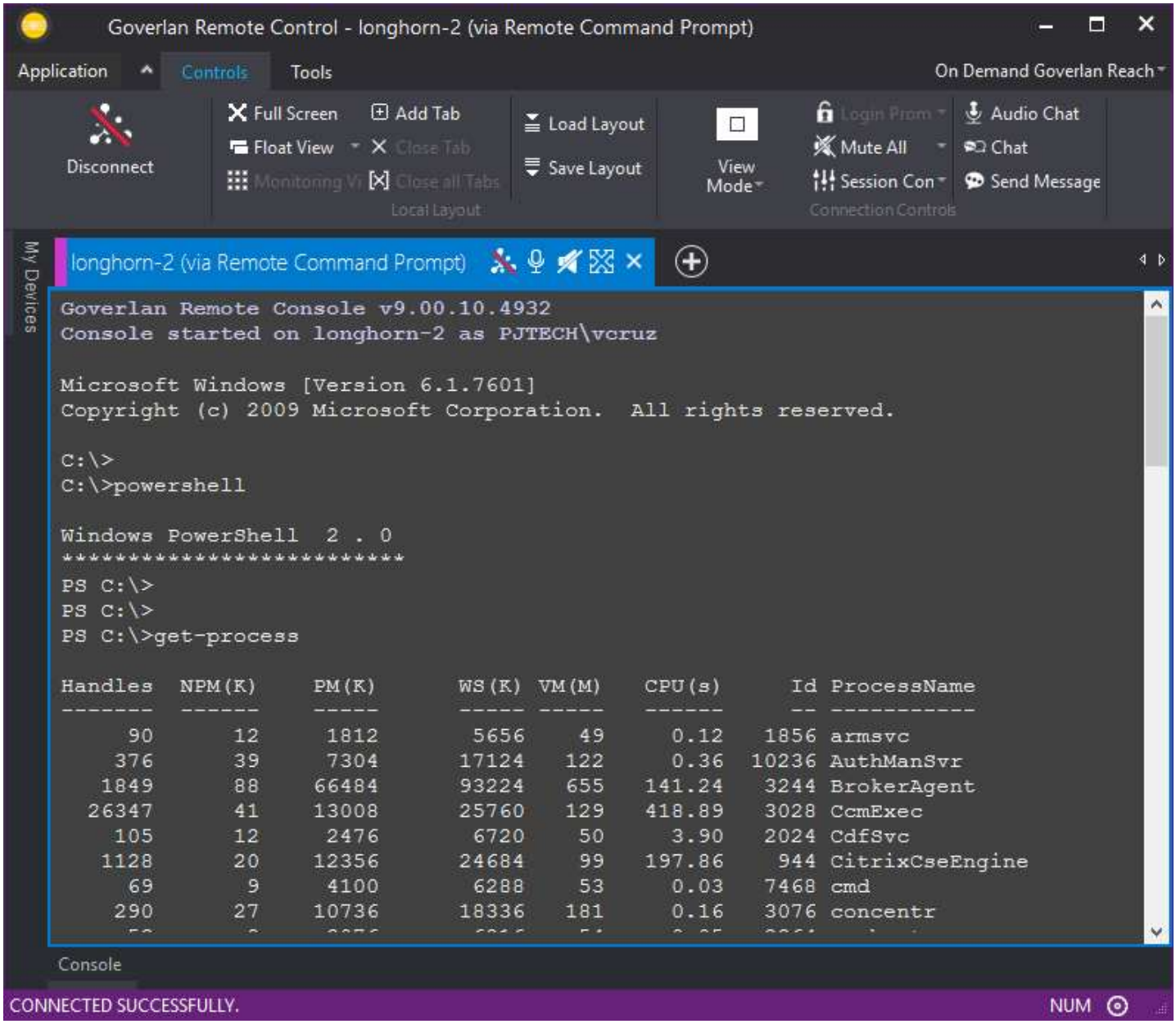
Use the Goverlan Remote Command Prompt connection to run any commands directly on the target system.

© Copyrights Goverlan Inc. – All Rights Reserved



Invoke the PowerShell command prompt by typing the command **PowerShell**.

© Copyrights Goverlan Inc. – All Rights Reserved



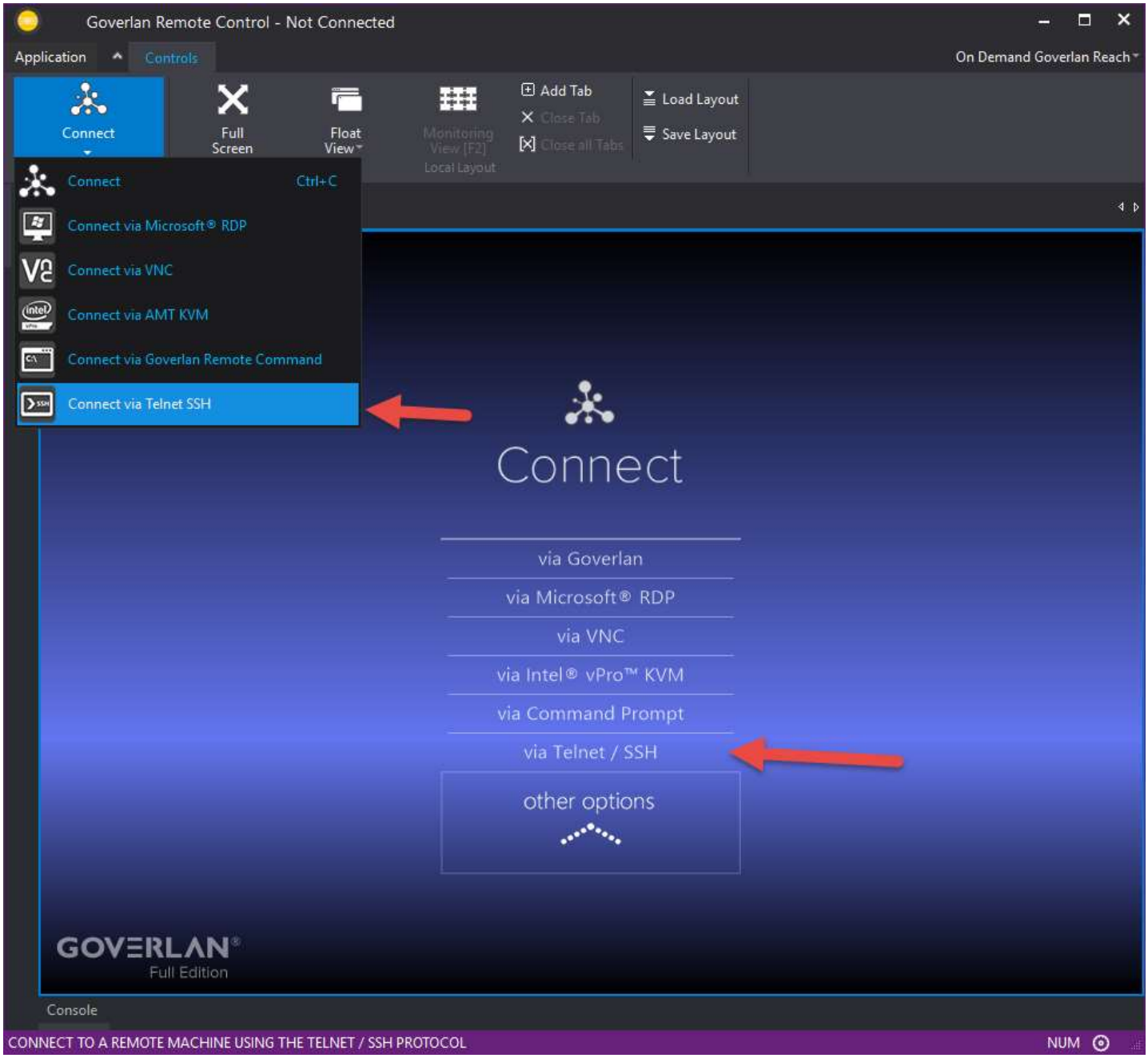
SSH and Telnet

Use Goverlan Reach RC to connect to any Telnet or SSH device such as network devices or printers.

Starting a new Telnet/SSH connection

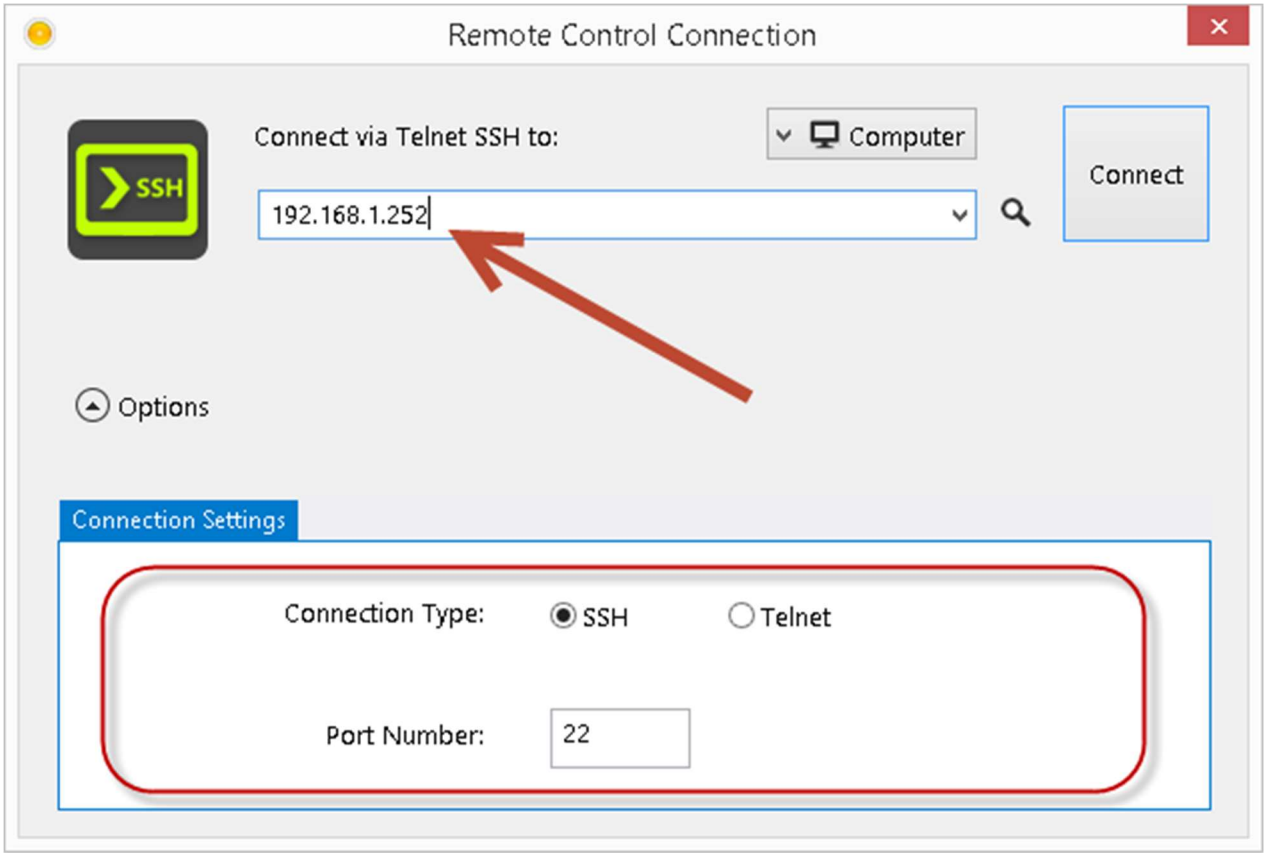
Choose via Telnet SSH from the More Options drop down or the Connect drop down in the Command Bar.

© Copyrights Goverlan Inc. – All Rights Reserved



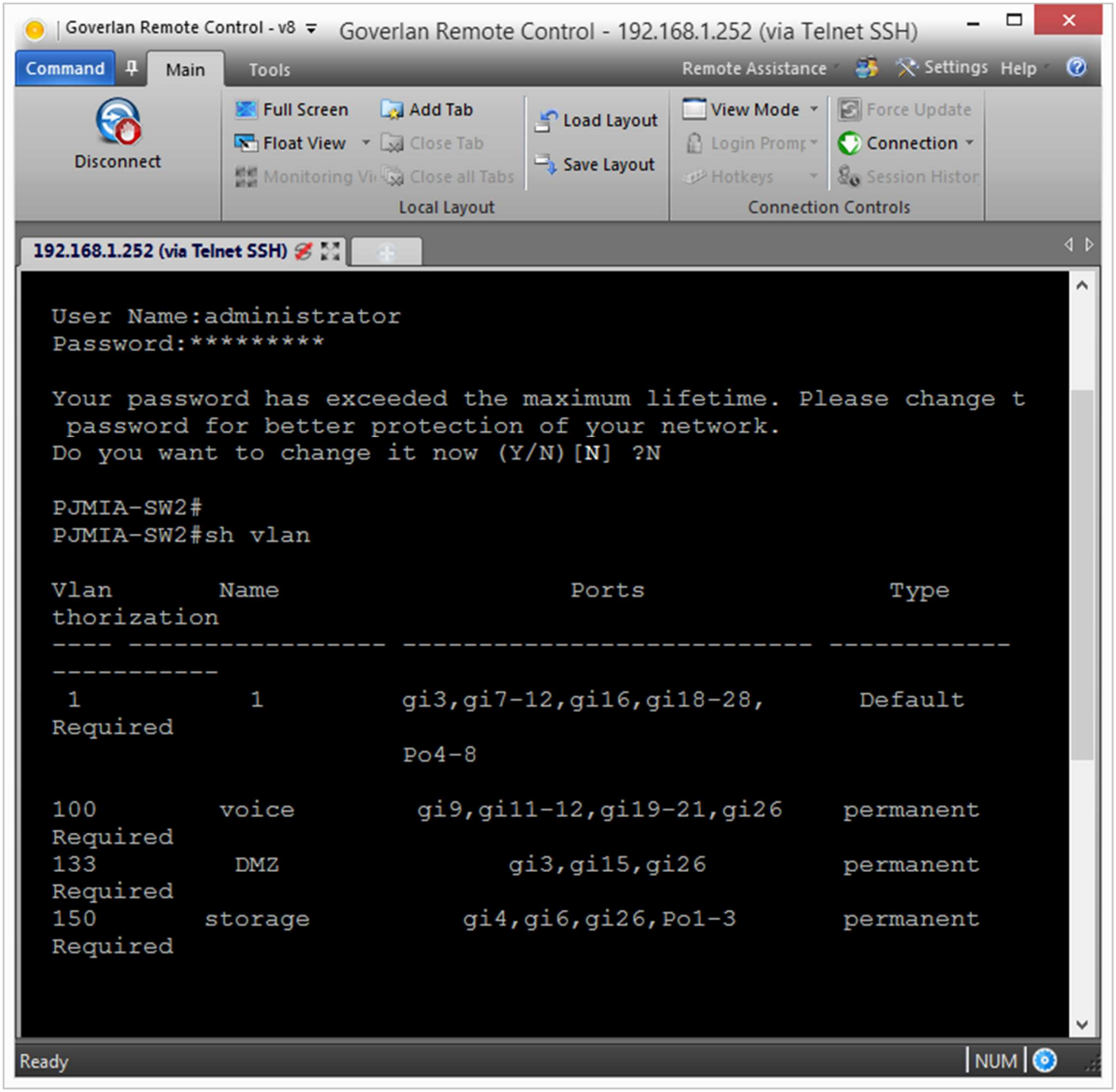
Choose the Connection type and the port number if it is not standard.

© Copyrights Goverlan Inc. – All Rights Reserved



Click the Connect button to establish the connections.

© Copyrights Goverlan Inc. – All Rights Reserved



Intel vPro

Configuring Intel vPro

vPro is Intel's application of Active Management Technology. vPro gives IT administrators the ability to manage their systems via a built-in hardware device. Goverlan gives you access to Intel vPro features in an intuitive and easy to understand format.

NOTE: Your Intel vPro system must be provisioned and configured before you can access the features. Please consult your hardware vendor's technical guides for details.

© Copyrights Goverlan Inc. – All Rights Reserved

Intel vPro provisioning and configuration considerations

Intel vPro has many different configuration options. Goverlan is designed to automatically detect different configurations and apply settings accordingly.

Provisioning Modes

Client Control Mode: Client Control Mode refers to vPro systems that have been configured by the local MEBx software directly. When a system has been provisioned in Client Control Mode, all KVM functionality will require user acceptance.

Admin Control Mode: Admin Control Mode refers to vPro systems that have been configured by an Intel SCS server or third party provisioning server.

Authentication Options

Intel vPro systems require authentication before a feature can be accessed. Use the Goverlan Credential Manager for seamless authentication to the Intel vPro chip. For more information, see Goverlan Credential Manager.

Custom ACLs: Custom Access Control Lists can be configured directly in the MEBx or by a provisioning server. Add your custom user account to the Goverlan Credential Manager for seamless access to Intel vPro features.

Active Directory Integrated: Intel vPro supports Kerberos Authentication for accessing features. Goverlan automatically detects this configuration and will attempt to use the Goverlan operators Active Directory Credentials. Alternate Credentials can be added to the Credential Manager if necessary.

NOTE: To use Active Directory/Kerberos authentication, you must specify the fully qualified domain name of the target system.

TLS Encryption

Intel vPro can be configured to require TLS before allowing any connection. Goverlan will automatically detect if the Intel vPro system is using TLS.

To establish TLS connections with Goverlan Reach RC, you must do/have the following:

- you must specify the fully qualified domain name in the "Connect To" field
- The organizations root certificate must also be in the Windows Certificate store.

Intel vPro Port Redirection

Intel vPro systems use TCP 16994 for KVM connections to a system. Intel vPro can also use the standard VNC port for KVM connections. TLS and Kerberos/Active Directory Authentication are not available with the standard VNC port.

REFERENCES

© Copyrights Goverlan Inc. – All Rights Reserved

- Goverlan Credential Manager

Intel vPRO KVM

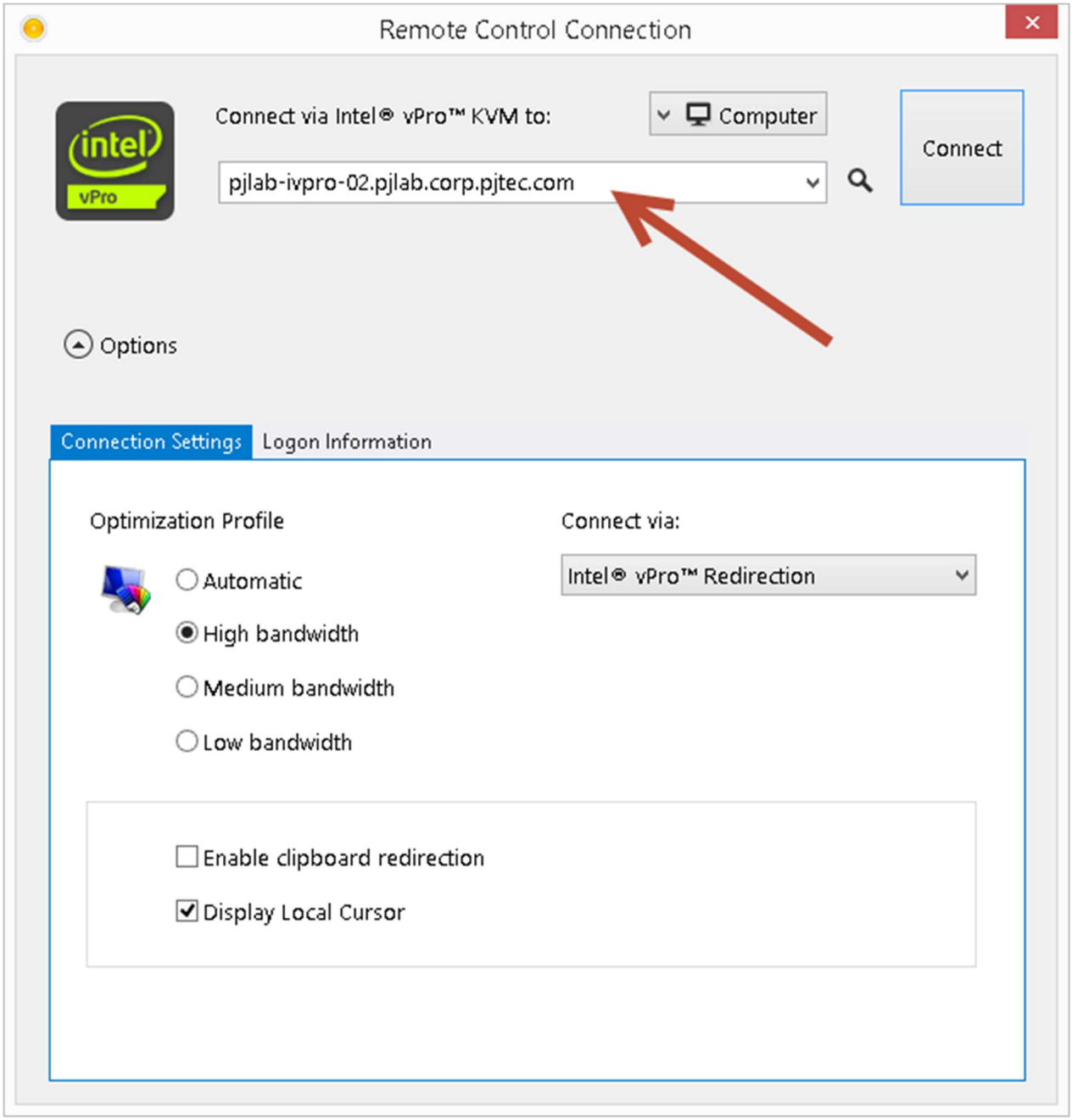
Goverlan Reach RC can now harness to power of the Intel vPro out-of-band KVM. Intel vPro KVM features allows out-of-band KVM access to any Intel vPro enabled workstation. Be sure to read Configuring Goverlan for Intel vPro for all of the Intel vPro considerations.

Establishing an Intel vPro KVM Session

Use the More Options button or the arrow below the Connect button in the Command Bar and select via Intel vPro KVM.

Enter the host name or IP address of the target Intel vPro system

© Copyrights Goverlan Inc. – All Rights Reserved

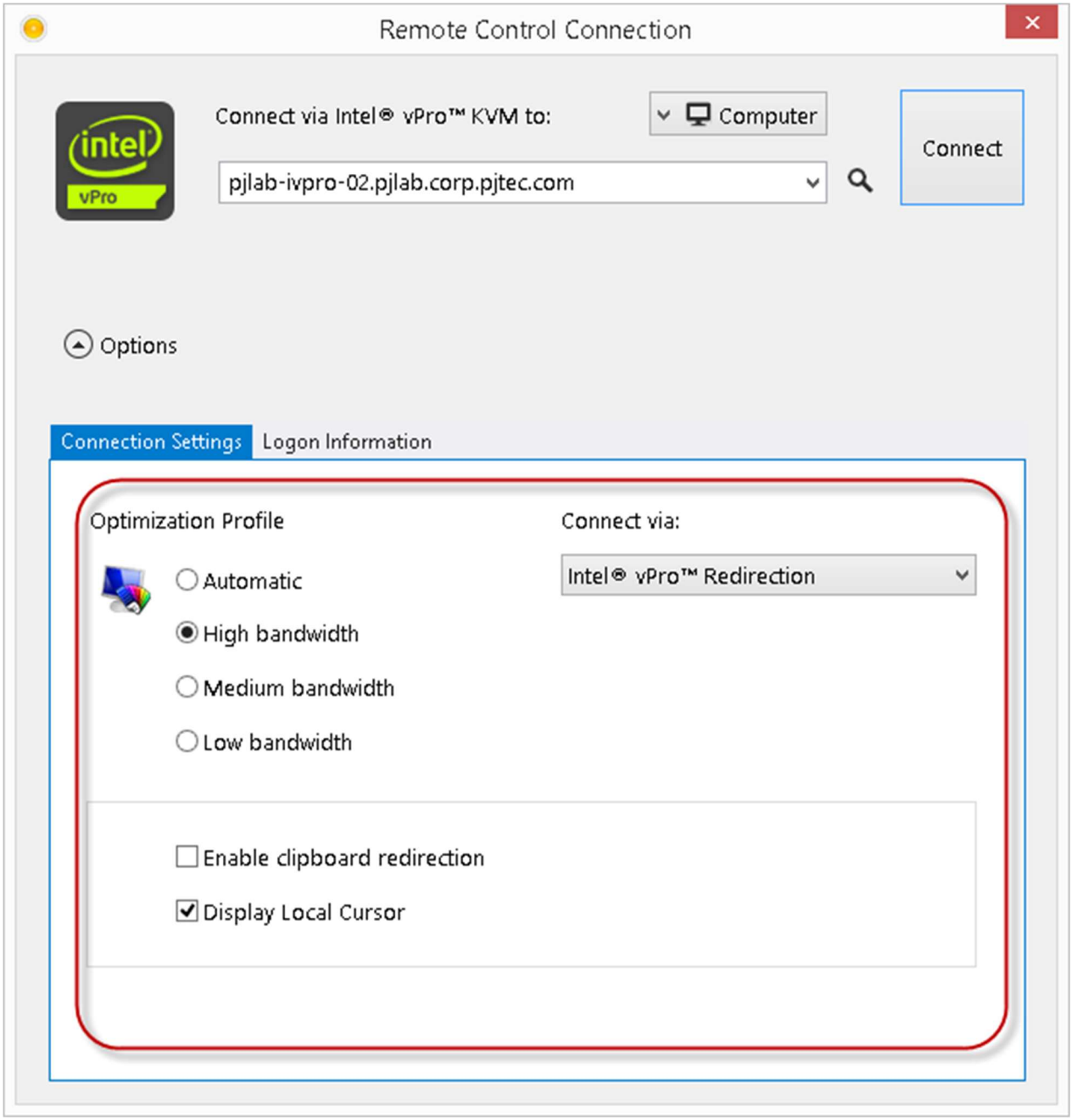


Note: If your Intel vPro systems are configured to use TLS or Kerberos/Active Directory authentication, enter the fully qualified domain name (FQDN). For more information about authentication modes, see Configuring Goverlan for Intel vPro.

Specify your connection options

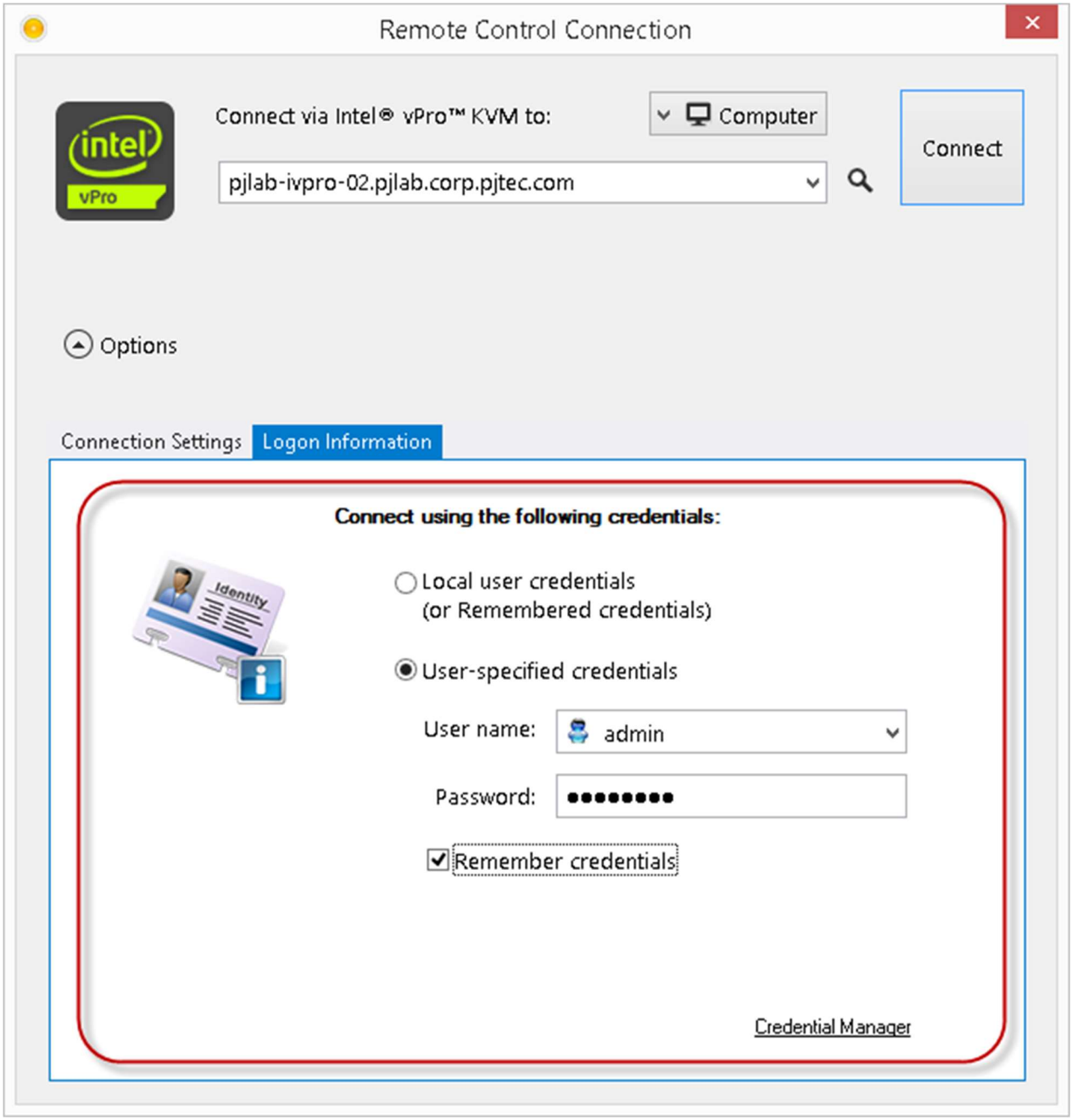
NOTE: Intel vPro can be configured to use the standard VNC port (5900) or the Intel vPro redirected ports. For more information about Intel vPro Redirection, see Configuring Goverlan for Intel vPro.

© Copyrights Goverlan Inc. – All Rights Reserved



Use the Logon Information Tab to specify alternate Active Directory credentials or Intel vPro ACL credentials.

© Copyrights Goverlan Inc. – All Rights Reserved



User Acceptance

User Acceptance is controlled by the Intel vPro chip or from a policy from the provisioning server.

Note: Intel vPro requires user acceptance if the system is configured in Client Control Mode. For more information about provisioning modes, see Configuring Goverlan for Intel vPro.

Goverlan YouTube video demonstration of Intel vPro KVM features.

https://www.youtube.com/watch?v=bocSXqdwttE

© Copyrights Goverlan Inc. – All Rights Reserved

NOTE: Intel vPro is a hardware specification and must be purchased. Please consult your hardware vendor for more information.

REFERENCES

- Configuring Goverlan for Intel vPro

Intel vPRO Power Options

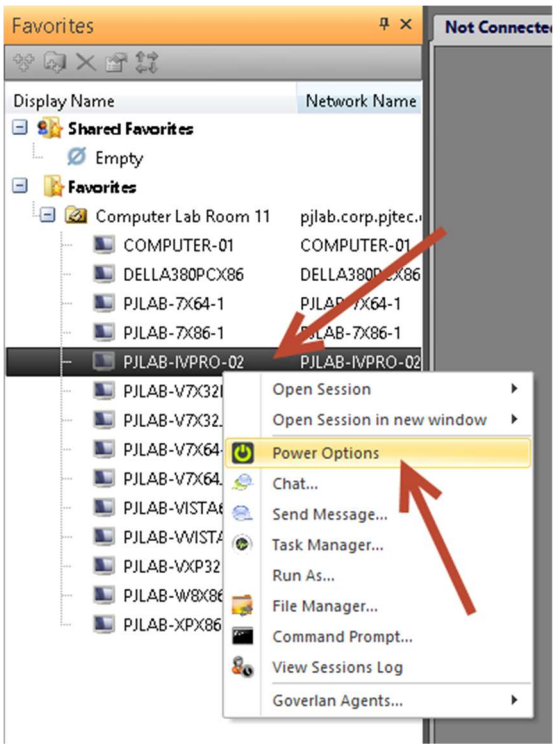
Use Goverlan Reach RC control the out of band power state of any vPro enabled desktop. For more information about Intel vPro and Goverlan, see Configuring Goverlan for Intel vPro. The features shown here are for specific Intel vPro options. For more information about the Power Options Dashboard, see Power Options.

Opening the Power Options Dashboard

You can find the Power Options Dashboard for any workstation in the following locations.

In the My Devices Panel

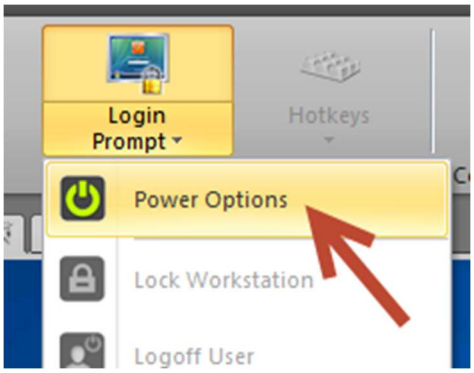
Right click any Windows system in the My Devices Panel and select **Power Options.**



In the Login Prompt Menu

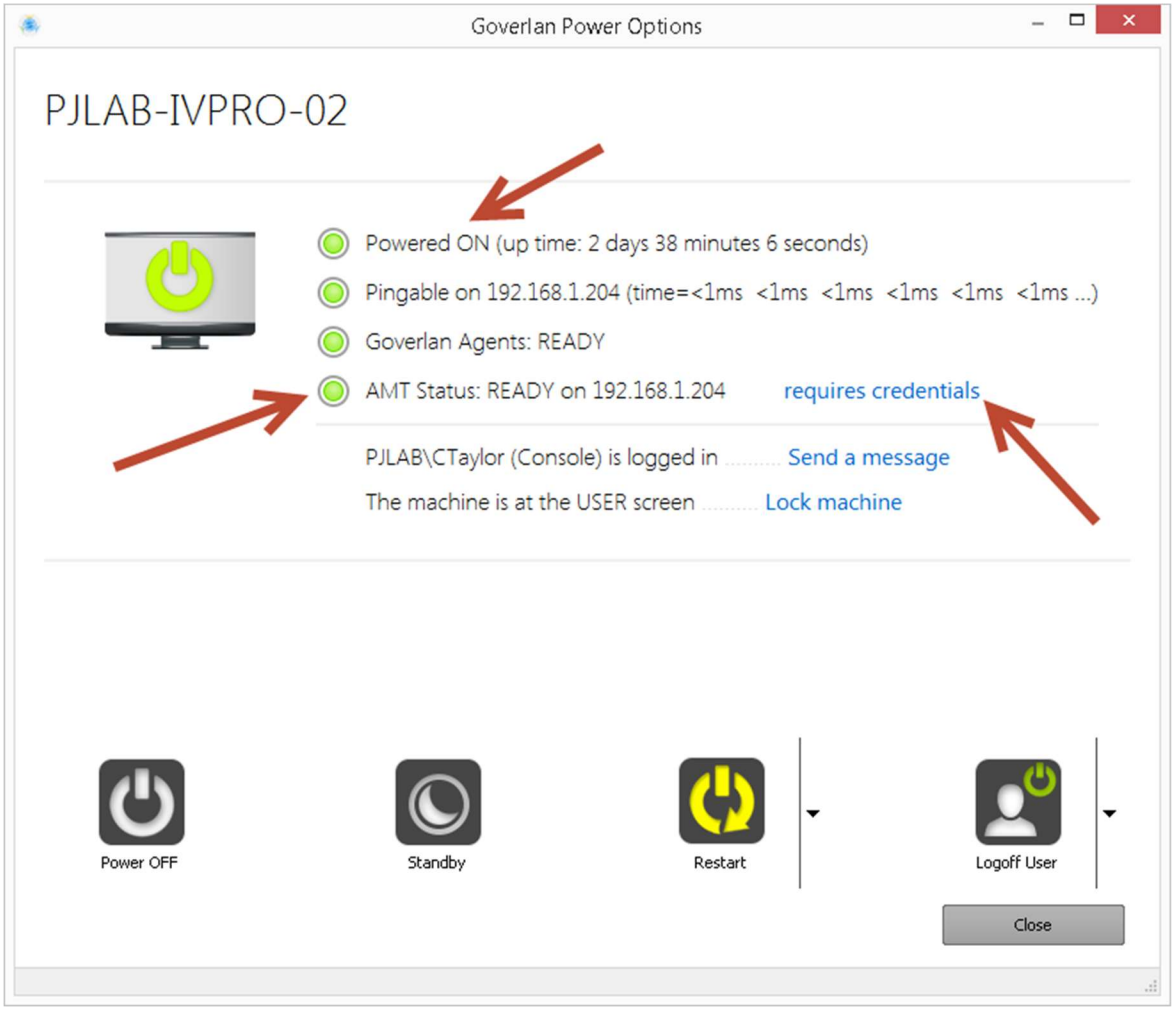
While in a Remote Control session, use the Login Prompt drop down in the Command Bar and select **Power Options**

© Copyrights Goverlan Inc. – All Rights Reserved



Power Options Dashboard Intel vPro features

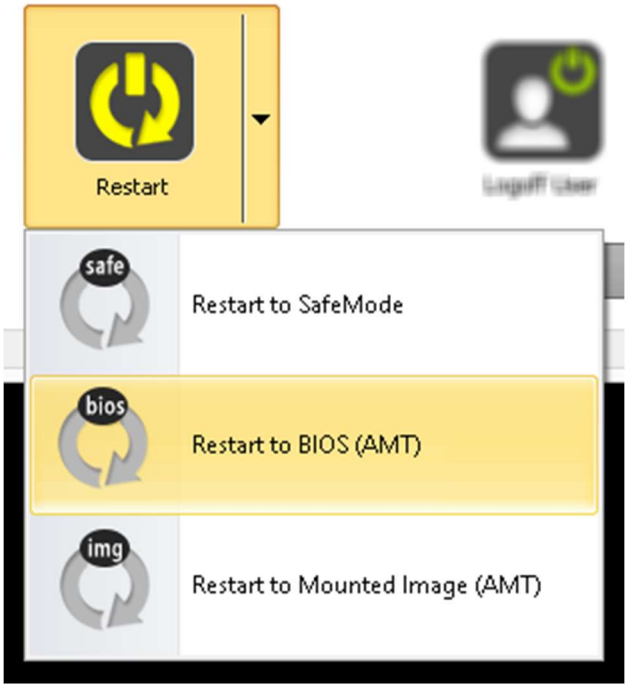
The Power Options Dashboard has many features for Intel vPro enabled systems. The **Powered On** monitor will retrieve the power status directly from the Intel vPro chip. Goverlan will query the status of the AMT chip and inform you if Intel vPro credentials are required.



Rebooting to BIOS

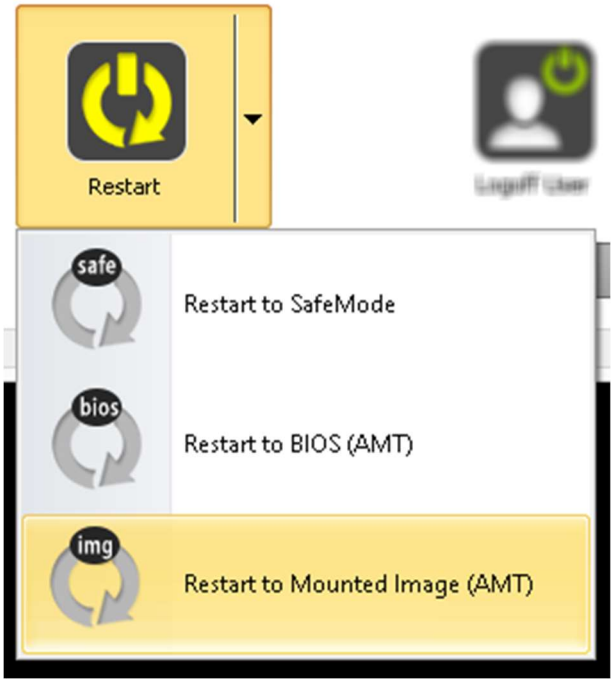
Use the Restart Menu to Restart an Intel vPro enabled system to the BIOS.

© Copyrights Goverlan Inc. – All Rights Reserved



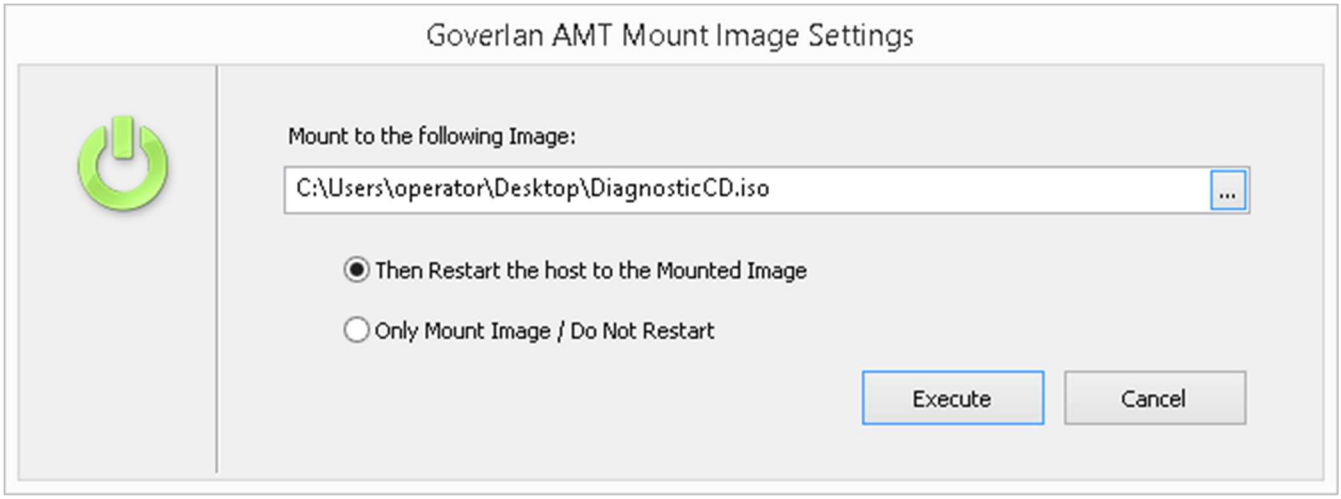
Rebooting to ISO Image

Use the Restart Menu to restart an Intel vPro enabled system to a specified ISO Image.



Choose the ISO image location and select "**Then restart the host to the Mounted Image**" and click Execute.

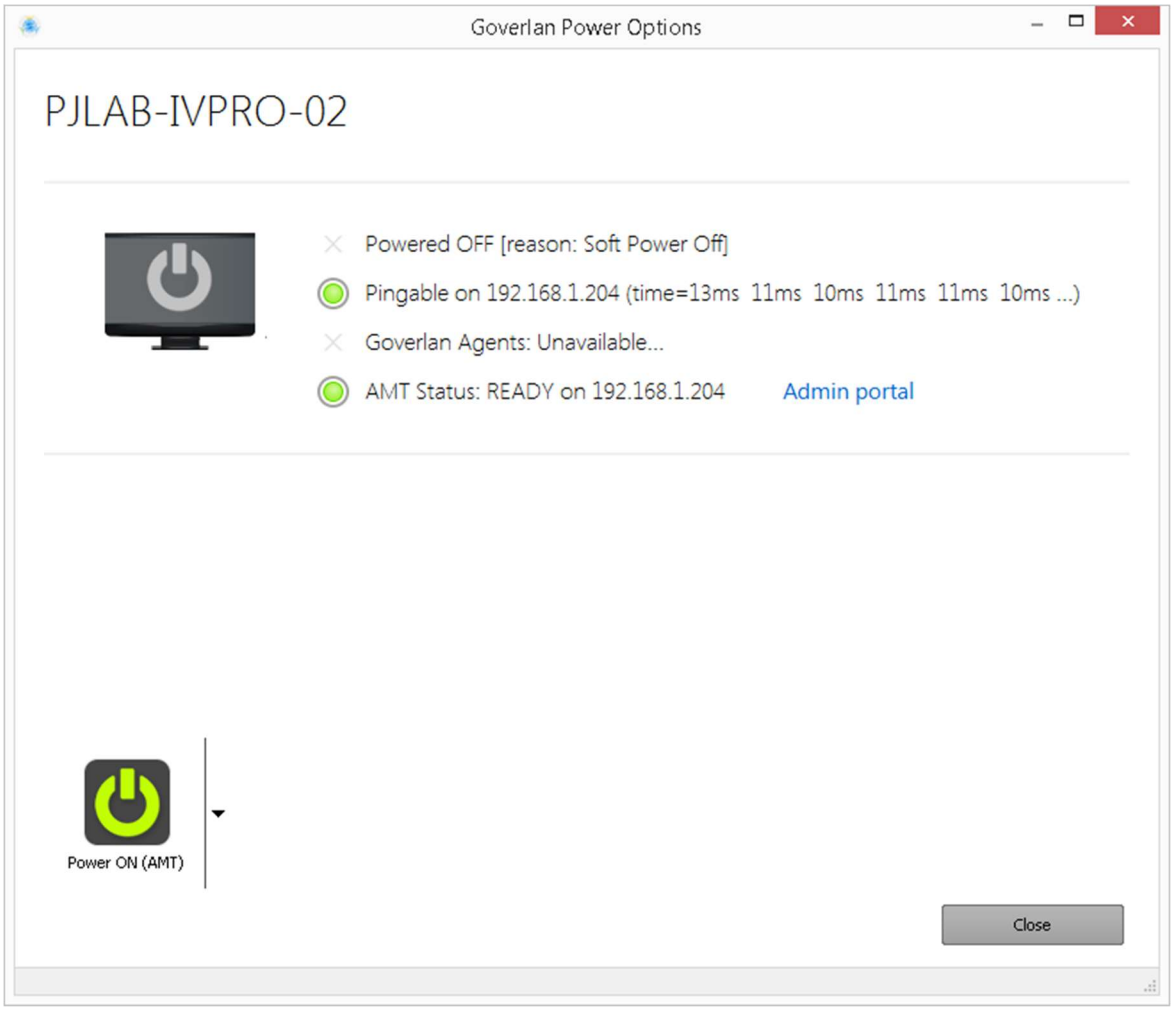
© Copyrights Goverlan Inc. – All Rights Reserved



Powering up a system that is completely powered down

Use the Power Options Dashboard screen to power up an Intel vPro system that is completely off.

If the system is completely powered down but the Intel vPro chip is available, use the Power On (AMT) button to turn this system on. This is not a Wake on Lan operation. For more information on Wake on Lan see, Power Options.



© Copyrights Goverlan Inc. – All Rights Reserved

Goverlan YouTube video demonstration of Intel vPro Power features.

https://youtu.be/r7IT-NdSS4s

NOTE: Intel vPro is a hardware specification and must be purchased. Please consult your hardware vendor.

REFERENCES

- Configuring Goverlan for Intel vPro
- Power Options

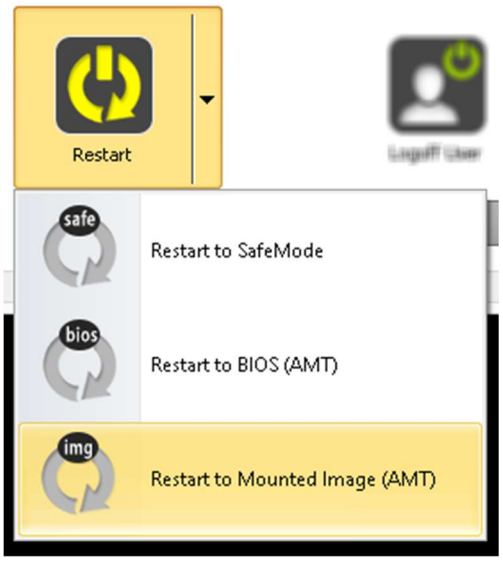
ISO Mounting and IDER

Goverlan Reach RC allows you to reboot any Intel vPro enabled workstation to an ISO image for any management purposes. This is a very powerful feature and has many uses. For more information about Intel vPro and Goverlan, see Configuring Goverlan for Intel vPro.

Rebooting to ISO Image

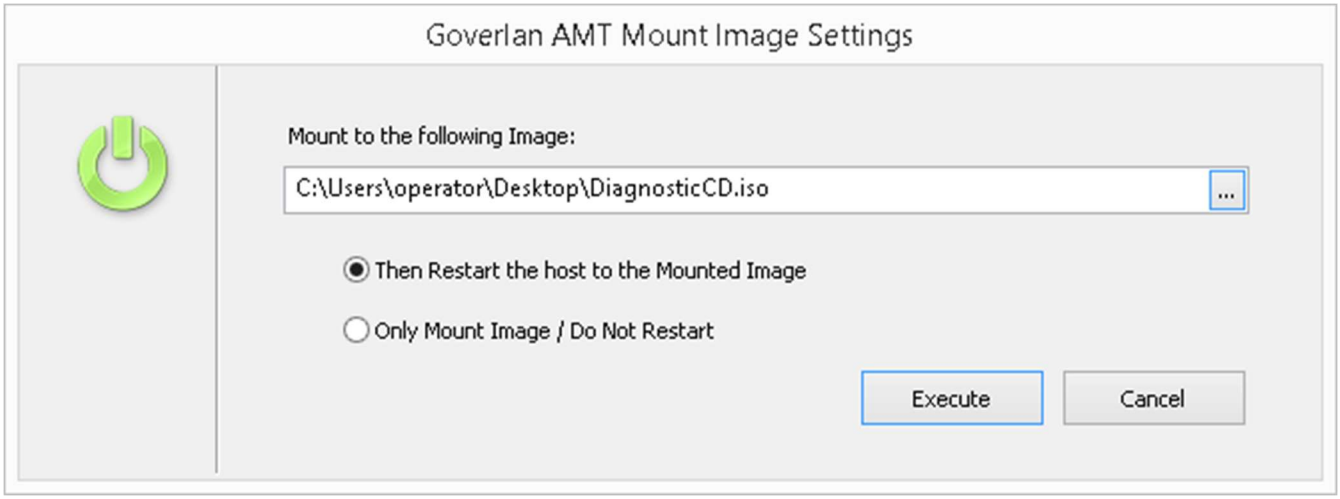
Open the Power Options Dashboard. For more information, see Power Options.

Use the Restart Menu to restart an Intel vPro enabled system to a specified ISO Image.



Choose the ISO image location and select "Then restart the host to the Mounted Image" and click Execute.

© Copyrights Goverlan Inc. – All Rights Reserved



Goverlan YouTube video demonstration of Intel vPro ISO Mounting features.

https://www.youtube.com/watch?v=OsrZm_HT1Ak

NOTE: Intel vPro is a hardware specification and must be purchased. Please consult your hardware vendor.

REFERENCES

- Configuring Goverlan for Intel vPro
- Power Options

Working with Smart Cards

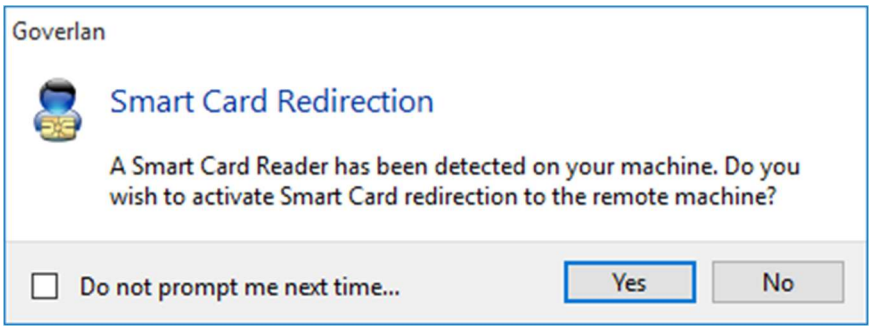
Working with Smart Card Redirection

On FIPS 201 compliant sites, Goverlan Reach RC allows users to supply smart card credentials to authenticate on remote systems. In order to redirect a local smart card to a remote machine, the Goverlan Smart Card Reader Driver must be installed on remote computer.

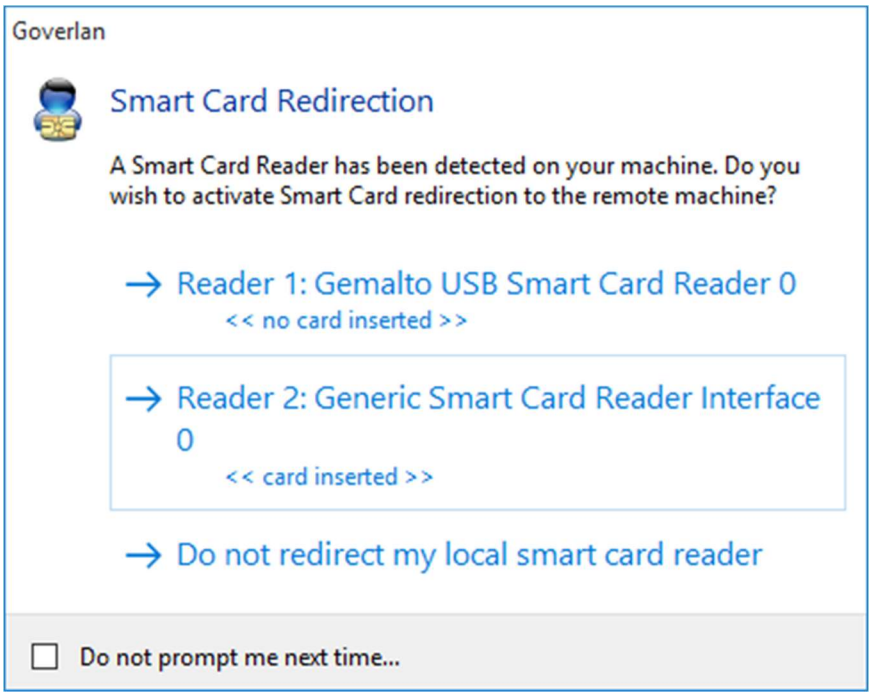
Goverlan Reach RC automatically detects any local smart card readers on the operator's system and automatically prompts you to enable Smart Card redirection. Once this detection is complete Goverlan will ask the operator to select the local smart card reader to redirect.

Once the reader is detected:

© Copyrights Goverlan Inc. – All Rights Reserved



More than one reader is detected:



Redirection Prompt Behavior

Use the Goverlan Settings screen to set one of the following options for Smart Card Redirection prompting.

- Automatically redirect my smart card reader - This setting will automatically redirect the smart card reader with no prompt.
- Prompt me to redirect if a reader is detected - This setting will prompt the Goverlan operator to choose which local reader to redirect.
- Disable Smart Card Redirection - This setting will suppress any Smart Card redirection prompts.

Smart Card Redirection Activity Indicator

The Activity Indicator will be displayed once redirection is active. The activity indicator will flash when smart card data is being transferred between the remote system and Goverlan Reach RC.

With no activity.

© Copyrights Goverlan Inc. – All Rights Reserved

With activity.

Simulate Smart Card Reinsert.

Click the Activity Indicator to reveal the Smart Card Reinsert control. Selecting this will initiate a smart card reinsert command on the remote system.

Installing the Goverlan Smart Card Driver

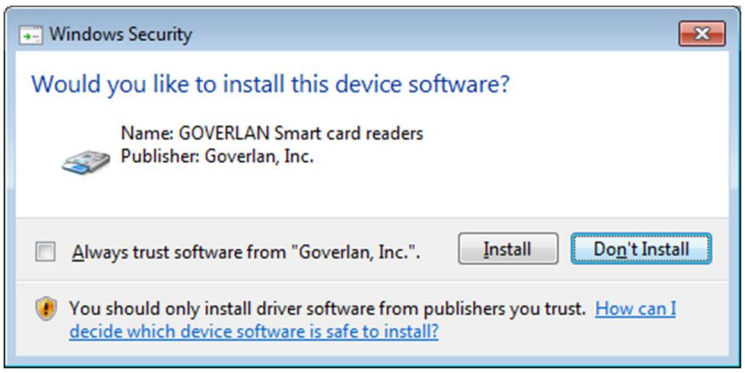
The Goverlan Smart Card Reader Driver is required to be installed on any remote system that supports Smart Card login.

The driver installer is in the Goverlan installation directory.

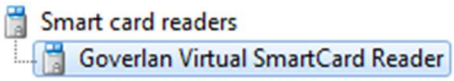
- C:\Program Files (x86)\Goverlan v8\SmartCardDriver\GovSmartCardDriver_v8_Setup.exe
- C:\Program Files (x86)\Goverlan Remote Control v8\SmartCardDriver\GovSmartCardDriver_v8_Setup.exe

Copy GovSmartCardDriver_v8_Setup.exe to a computer on your network and run the installer. This process will need to be completed on each computer that requires a smart card login.

Follow through with the installation wizard and click INSTALL on the following screen.



The Goverlan Smart Card Reader Driver will appear under "Smart Card Readers" in the Windows Device Manager.

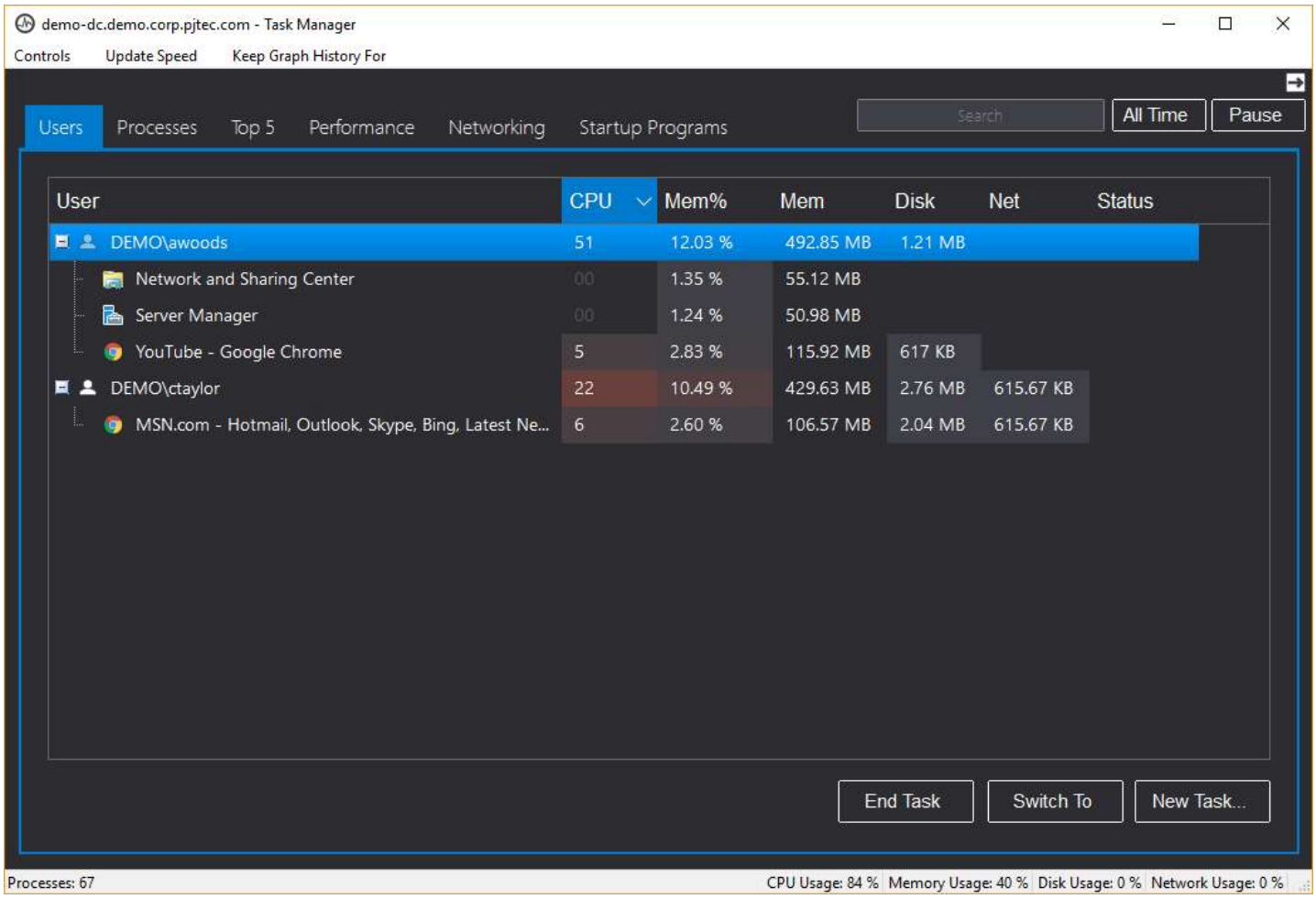


Connection Tools

© Copyrights Goverlan Inc. – All Rights Reserved

Goverlan Task Manager

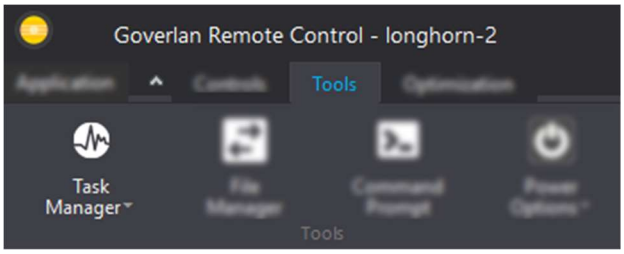
The Goverlan Task Manager has been completely overhauled in Goverlan v9, providing additional functionality not found in the native Windows Task Manager.



Starting the Task Manager

While in a remote control session

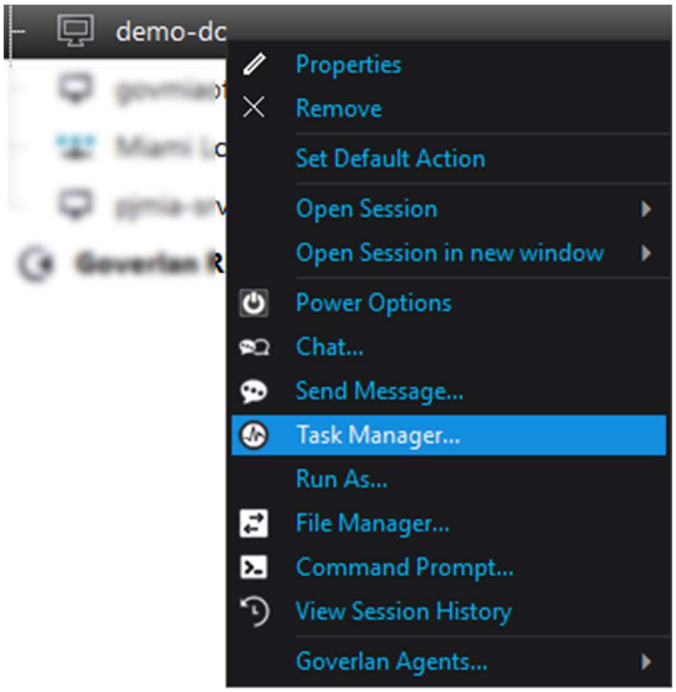
Go to the Tools tab in the Command Bar and click the Task Manager button.



From the favorites menu

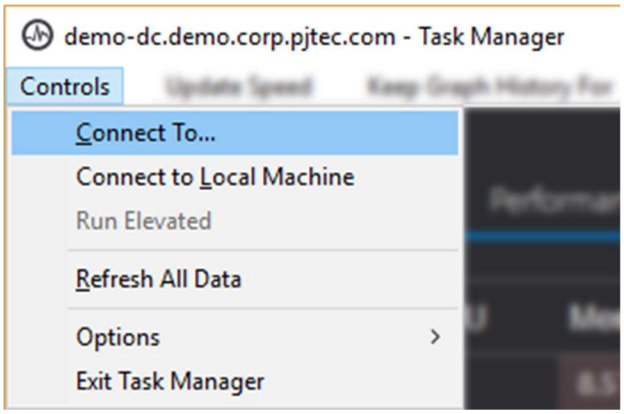
Right click any computer in your Favorites list and select Task Manager.

© Copyrights Goverlan Inc. – All Rights Reserved



Connecting to other machines through the Task Manager

Once the Task Manager is opened, you can set the focus to another machine by selecting Controls > Connect To... or Controls > Connect to Local Machine.



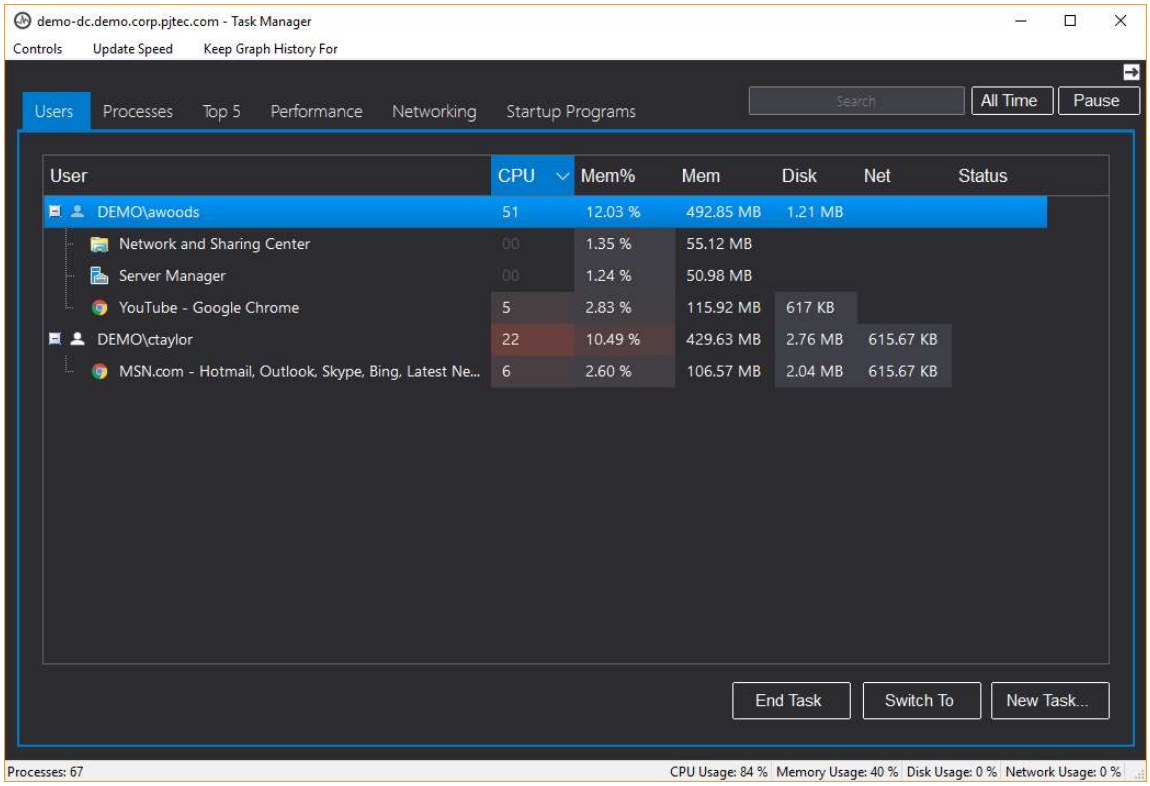
The Goverlan Task Manager is hosted by its own process(GovTools.exe), so closing Goverlan doesn't close any opened Task Manager session.

Task Manager View Modes

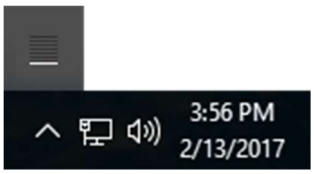
The Task Manager can display its information in 3 view modes:

© Copyrights Goverlan Inc. – All Rights Reserved

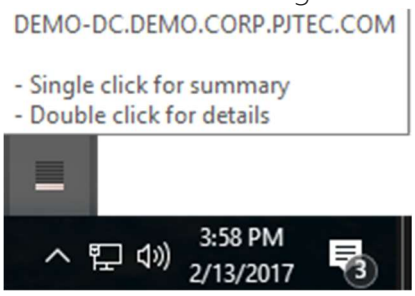
1. Normal View Mode



2. Minimized View Mode

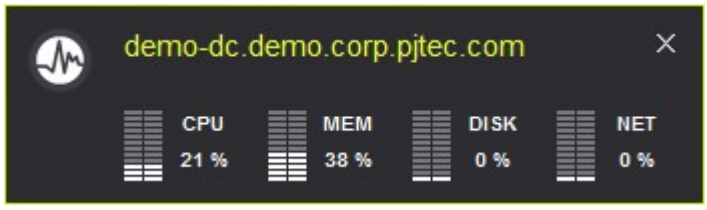


- The Task Manager inserts an icon in the Windows notification area. This icon is always visible
- This icon reflects the current CPU usage of the focused machine. To view more performance counters, place the mouse cursor over it and a tooltip appears which displays the CPU, Memory, Disk and Network usage counters.



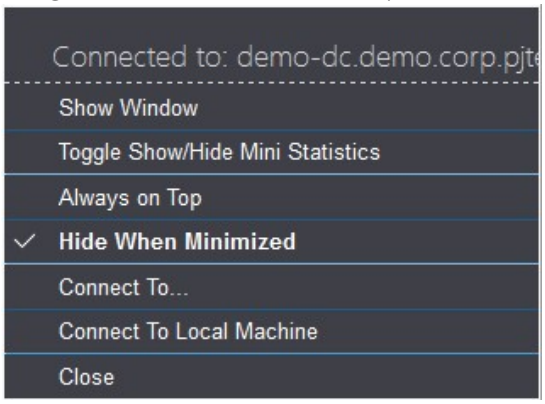
• Single click on this icon to trigger the Summary View Mode (see below)

© Copyrights Goverlan Inc. – All Rights Reserved

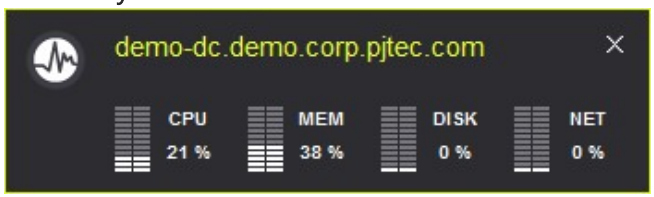


• Double click on this icon to trigger the Normal View Mode (see above)

• Right-click on this icon to open the context sensitive menu.



3. Summary View Mode

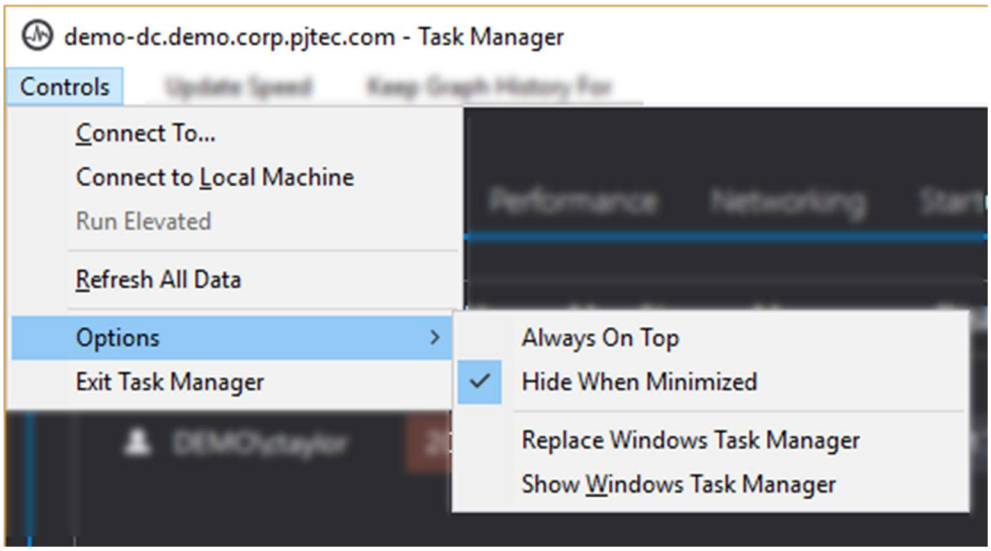


The Summary View Mode only displays the primary performance counters of the focused machine. This view mode is designed for monitoring. To start the Summary View Mode, single click on the Task Manager Icon in the Windows notification area. To close the Summary View Mode, click on the Close button or single click again on the notification area icon.

Task Manager Options

© Copyrights Goverlan Inc. – All Rights Reserved

Use the Controls > Options menu to control the behavior of the Goverlan Task Manager.

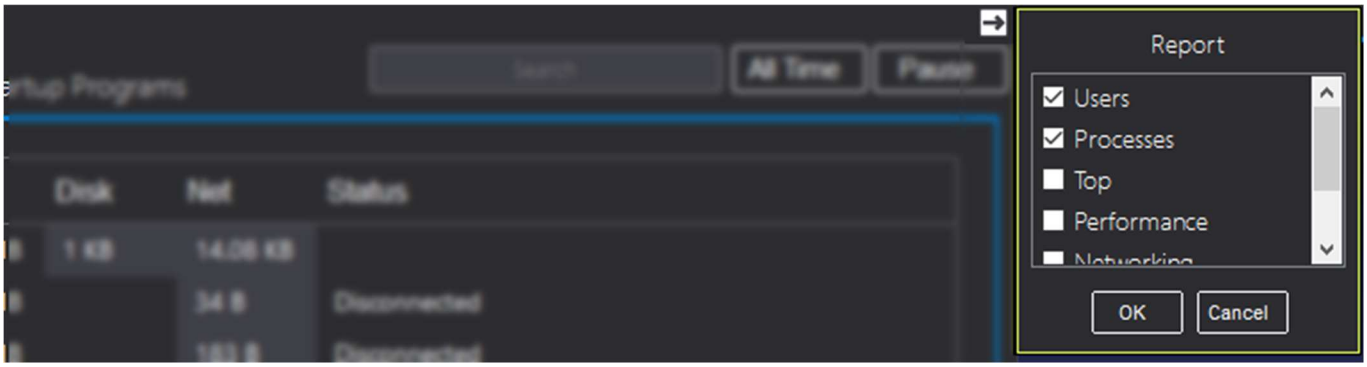


Always On Top	Enable to keep the Task Manager window on top of all other windows.
Hide When Minimized	If enabled, minimizing the Task Manager removes its entry from the Windows Taskbar. Once hidden, you can restore the Task Manager by double-clicking on its icon in the Windows Notification area.
Replace Windows Task Manager	Enable this option if you want the Goverlan Task Manager to be your default task manager. Once enabled, starting the default task manager on your machine will open the Goverlan Task Manager (versus the Windows Task Manager). Note: You can start the standard Windows Task Manager from the Goverlan Task Manager by selecting View > Show Windows Task Manager from the menu.
Show Windows Task Manager	Select this option to display the native Windows Task Manager. This is useful if you have configured the Goverlan Task Manager to be the default task manager on your machine and you wish to use the Windows Task Manager temporarily.
Refresh All Data	Requests the Task Manager to re-query all data from the client machine. Use this option if the information displayed by the task manager seems de-synchronized or if the connection with the client machine is lost.

© Copyrights Goverlan Inc. – All Rights Reserved

Update Speed	Use this menu to configure the update frequency of the Task Manager.

To export the information displayed by the Task Manager to a text file, click on the report button located at the top-right corner of the window.



GoverTmpReport.txt - Notepad

File Edit Format View Help

```
Goverlan Report
---------------------------
Date: 02/23/17 @ 16:03:20
Created by: vcruz


********************************************************************************
             Task Information - demo-dc.demo.corp.pjtec.com
********************************************************************************

************************************
****    Running Applications    ****
************************************

User                  CPU     MEM %      MEM          DISK     NET          STATUS
-------------------------------------------------------------------------------------------------
DEMO\Administrator    2       5.06 %     207.37 MB    1 KB     13.11 KB
DEMO\awoods           0       7.72 %     316.23 MB    0 KB     0 B          Disconnected
DEMO\ctaylor          0       3.63 %     148.82 MB    0 KB     0 B          Disconnected


************************************
*****     Running Processes     *****
************************************
Count:    68
```

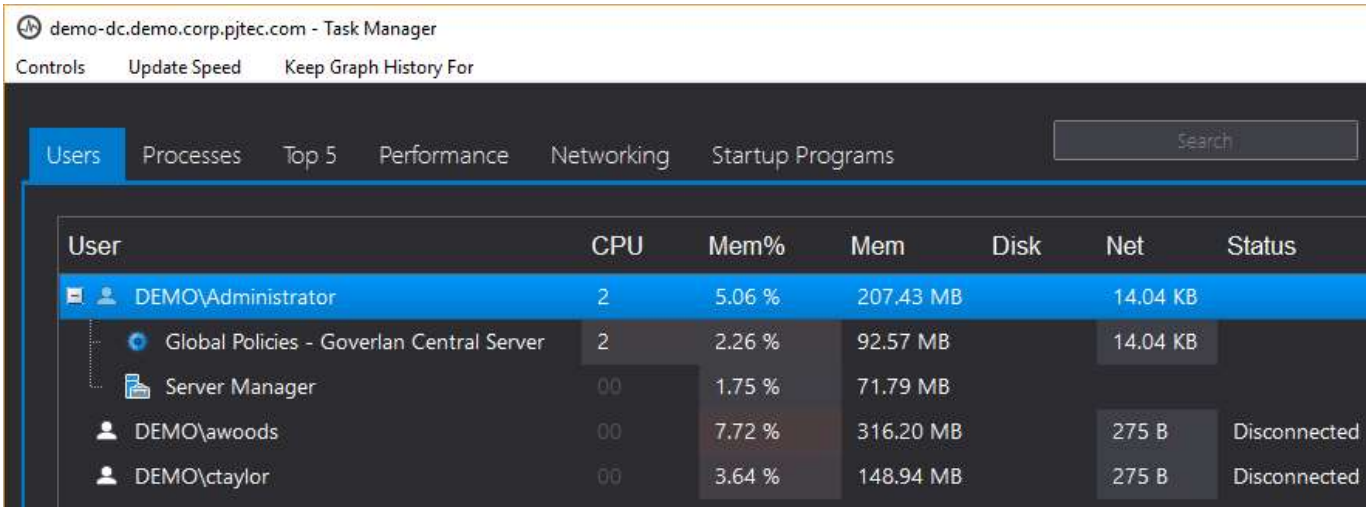
Working with UAC

On Windows Vista or later, the Goverlan Task Manager automatically detects if UAC is active and allows you to restart the process with elevated privileges. In such an environment, the Controls > Run Elevated menu entry is accessible. If you execute an action which requires elevated privileges, Goverlan automatically prompts you to switch to elevated mode.

© Copyrights Goverlan Inc. – All Rights Reserved

This option is disabled if UAC is not detected.

Users Tab



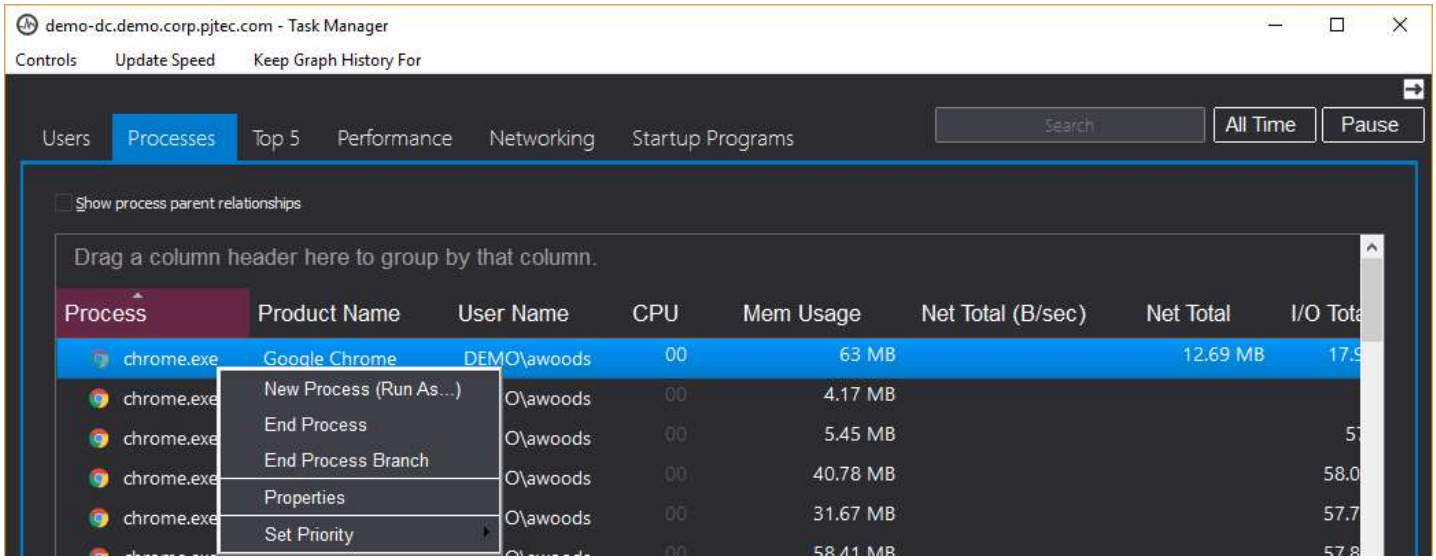
The Users tab displays all apps that are running on the machine that are organized by Username.

- To view detailed information about any application that the user is running, expand the user's processes, right click the application and select Properties. You can also double-click it.
- To terminate an application right click it > End Process. You can also click on the End Task button after highlighting it.
- To modify the priority of the application, right click it, select the Set Priority submenu and click on the desired property.
- To start a new process, click on the New Task... button. The New Task button starts the Run As feature.

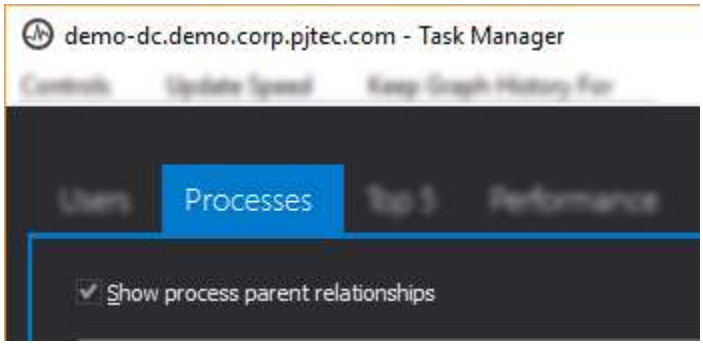
Processes Tab

This tab displays extended information, including performance counters on all running processes on the system and their network usage, per process. Just like the Users tab, all the right click menu options are available per process.

© Copyrights Goverlan Inc. – All Rights Reserved



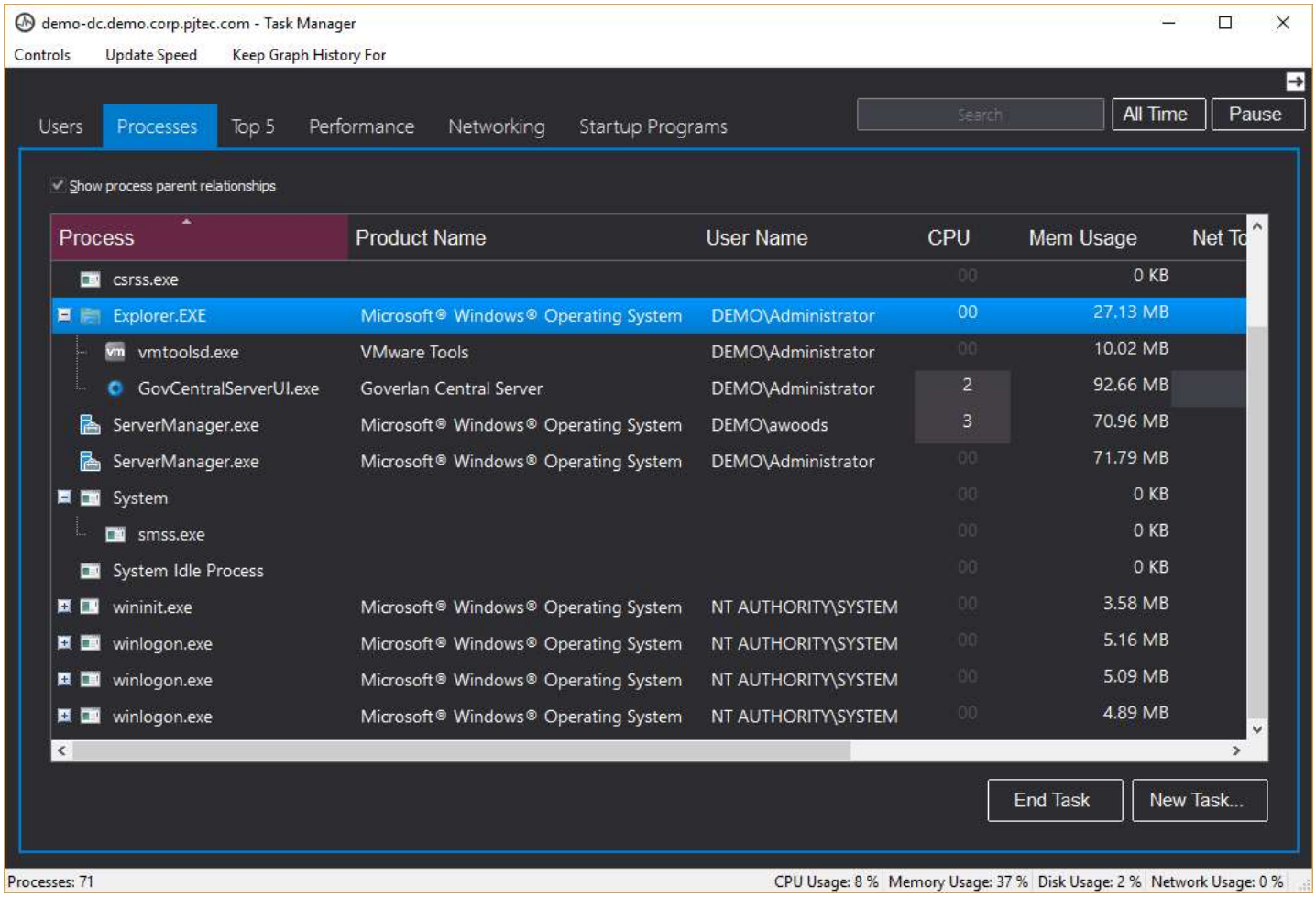
Show process parent relationships



Processes can either be displayed as a flat list or in a parent relationship tree format. You can switch between the two modes by Enabling / Disabling the Show process parent relationships option.

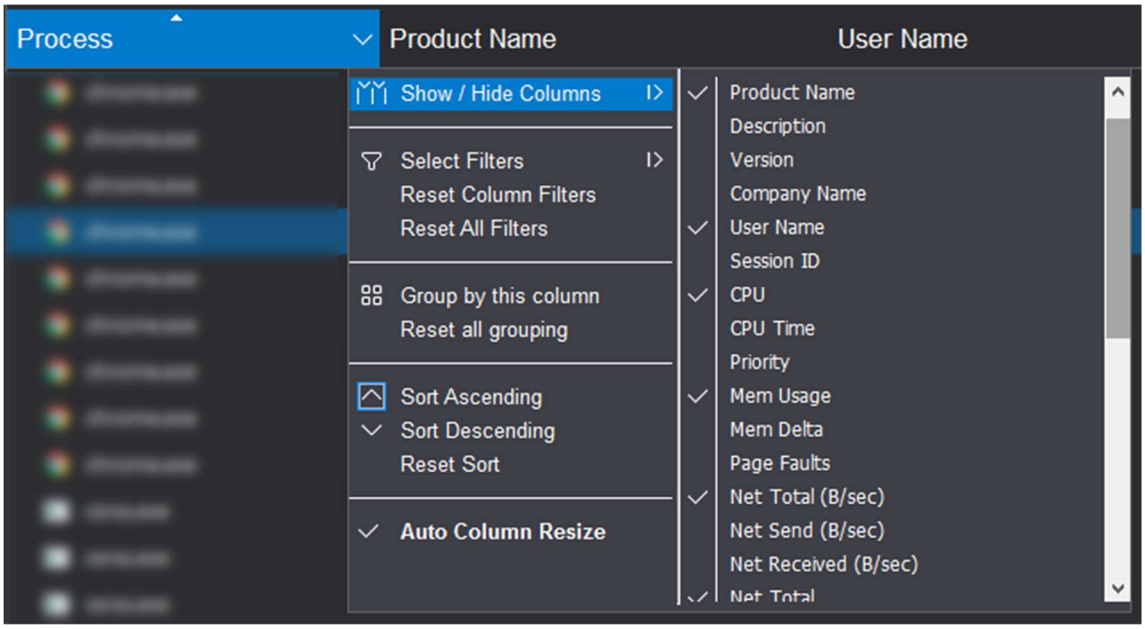
Each process, except for the root processes, have a parent process (the process which spawned them). Each process can also spawn new processes which become their child processes. The parent relationship view mode shows the processes in a parent/child tree format, highlighting how a process was created. For instance, the list of running processes, as displayed above, can also be viewed in the parent to child tree as follows:

© Copyrights Goverlan Inc. – All Rights Reserved



This view format is very useful to recognize processes initiated by the console user (the processes parent is always Explorer.exe) versus processes started by the system such as services. You can also collapse entire branches to emphasize certain processes.

Viewing detailed process information



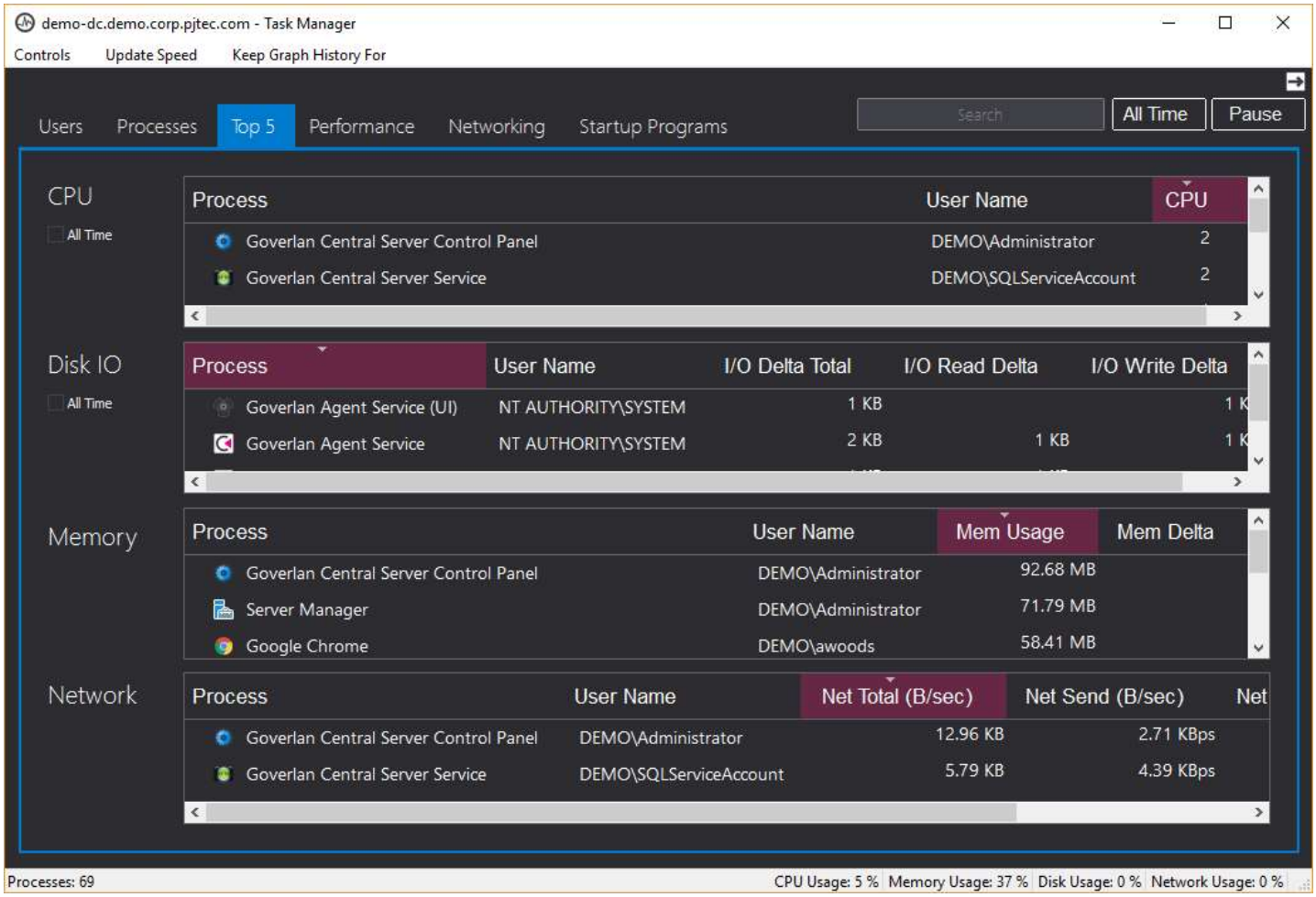
© Copyrights Goverlan Inc. – All Rights Reserved

The Processes tab can display a lot of information about each process. Most information is hidden by default in order to avoid cluttering the interface.

- To display extended information for all processes, right-click on the columns header and Check / Uncheck the columns to be displayed.
- To display extended information for a process, double-click on it to view its properties.

Top 5 Tab

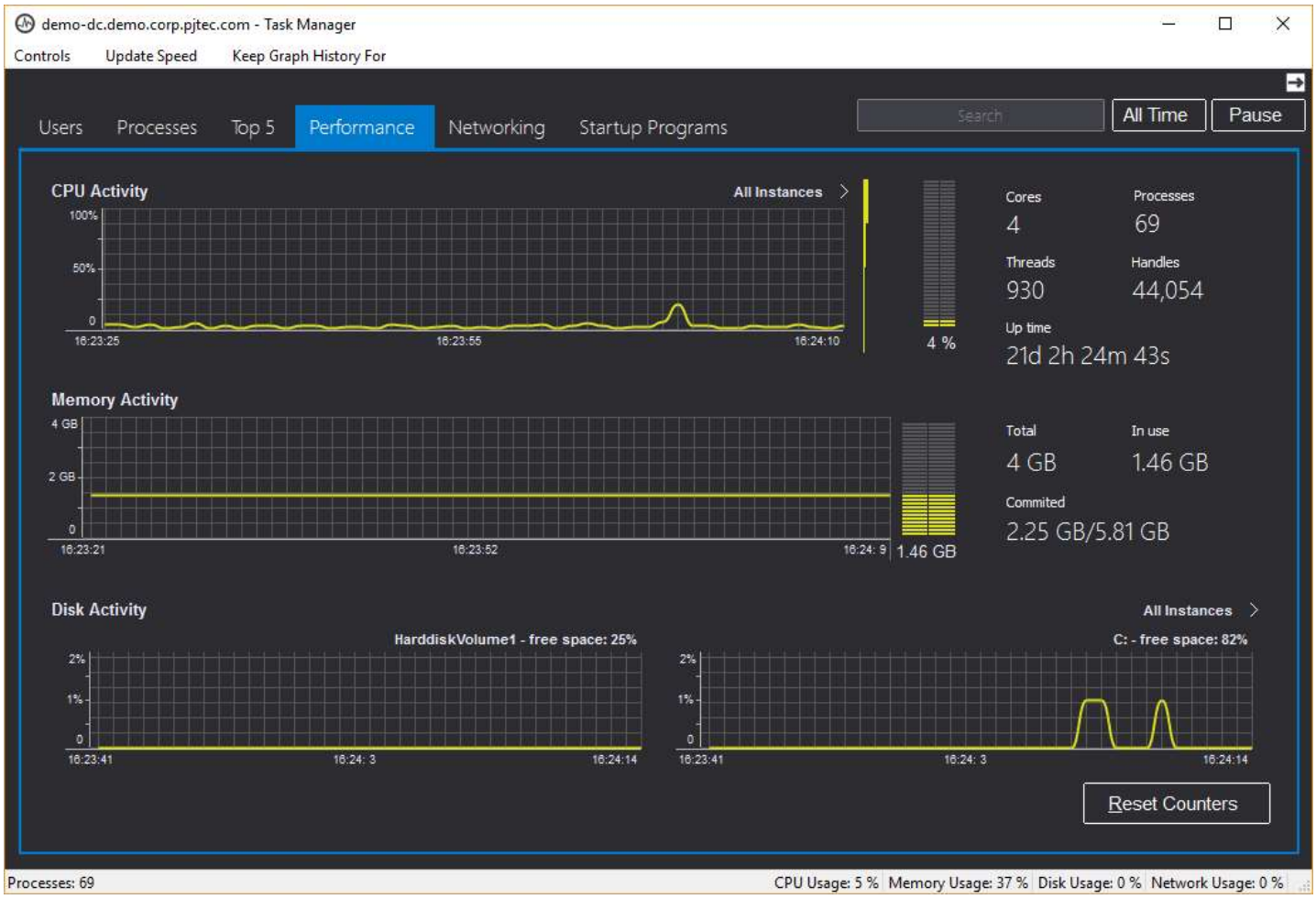
Use this tab to determine the most resource-consuming processes on the target machine. The Top 5 tab displays the five most active processes for CPU usage, Disk IO, Memory usage and Network usage:



The CPU and Disk IO sections can display either instantaneous values (i.e., the processes which are currently consuming the most resources) or the All-Time Values which correspond to the processes which have consumed the most resources since the system started.

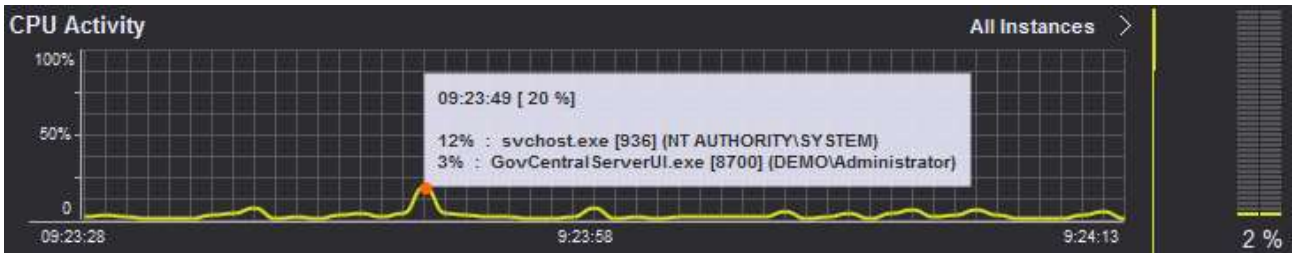
© Copyrights Goverlan Inc. – All Rights Reserved

Performance Tab



The performance tab displays real-time CPU, Memory usage, and Disk Activity information. The refresh update speed can be controlled selecting the Update Speed menu. Performance counter information is also always displayed in the Task Manager bottom status bar.

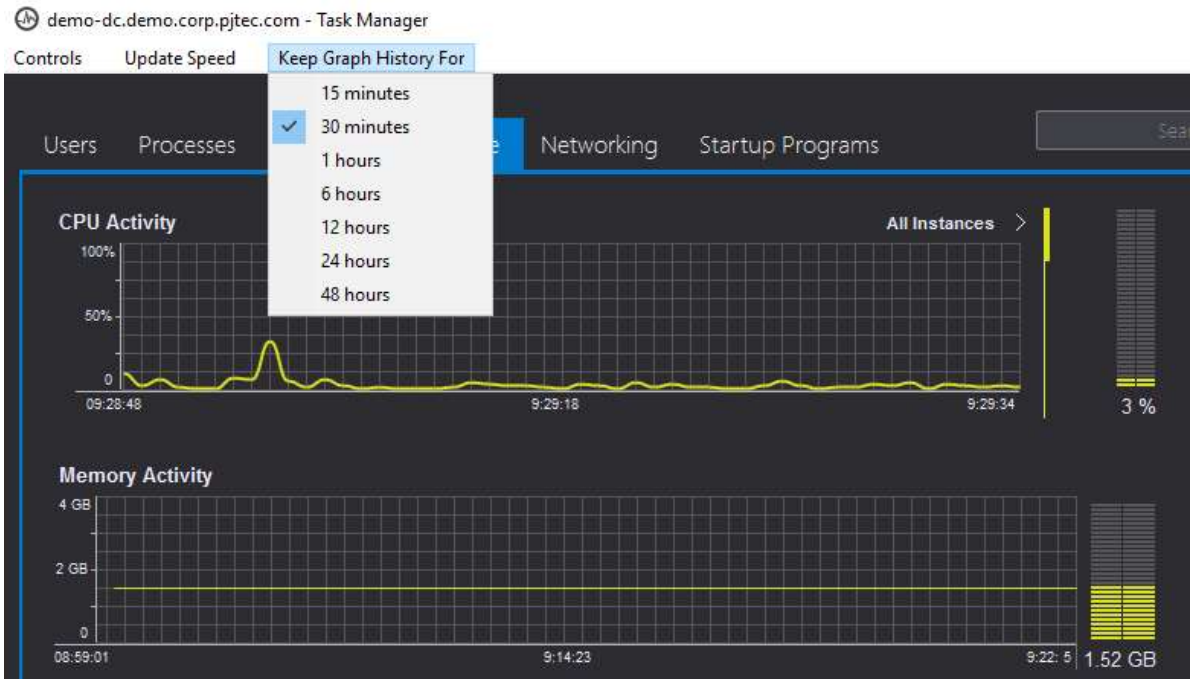
Detailed Process Monitoring



Placing the mouse over any portion the graphs timeline will show which processes were the cause of the spike, the percentage of use, its process ID, the user account that is running the process and the time at which the spike occurred. All graphs in the Performance tab have this ability.

© Copyrights Goverlan Inc. – All Rights Reserved

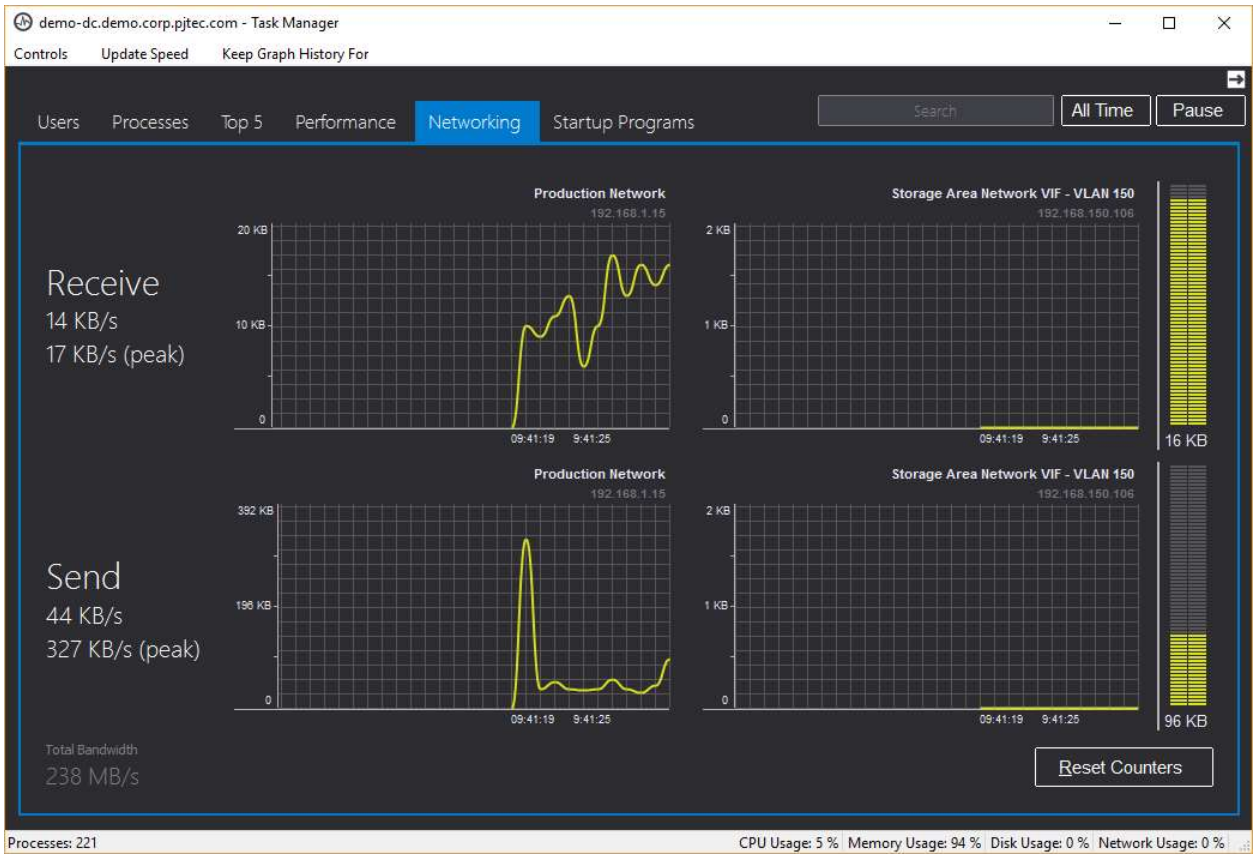
Keep Graph History For



Each graph keeps historical data and the duration at which this data is kept can be set via this menu. This is useful for monitoring a process over time to determine the stability of each process on any given machine. A timeline at the bottom of the graph displays the time frame currently being displayed. You can also right-click within the graph and enable the Scale to Fit option to view the full set of recorded information. To reset the history of the performance counters, click on the Reset Counters button.

© Copyrights Goverlan Inc. – All Rights Reserved

Networking Tab



The Networking tab displays real-time network usage performance information. The information presented in this view represents the statistics for each network interface available on the computer and is divided into the Receive and Send graphs.

Startup Programs

Use this tab to view the currently configured startup program on the computer. A startup program is a process which automatically starts when a user logs in. For instance, Microsoft Messenger is often configured to automatically start upon logging in. However, having too many programs configured to start automatically may result in a lengthy and slow login process.

Understanding Startup Information

The Startup Programs tab lists all currently configured startup programs. The list displays default information for each program such as the process name and description, however, more information is available. To modify the information displayed in the list, right-click on a column header and enable/disable the appropriate categories.

A program can be configured to automatically start in multiple ways. The Type information column displays some generic description of where the configuration has been found. This value can be:

- Registry - [All Users | User Side]
  The startup information was found in the registry under one of the Windows. Run keys.

© Copyrights Goverlan Inc. – All Rights Reserved

- Windows Startup Group [All Users | User Side]
  The startup information was found in the user profile under a Startup folder.

To see the exact location where the startup information was found, enable the Found In column (again, right click within a column header and select the desired column). The Found In column shows the exact registry path or folder path where the configuration settings were found.

Removing Startup Programs

To stop a program from automatically starting, select it from the list and click on the Remove button. Note: This operation cannot be undone and it does not terminate the currently running processes. It only removes the startup configuration settings for the program.

If you wish to terminate the process initiated under the startup configuration, select the item and click on the Go to Process button before removing the startup program item. If the process is still running, the focus is automatically set on it in the Processes tab. You can then terminate the process.

Disabling Startup Programs

Disabling a startup program prevents it from running the next time the user logs in. However, the entry is remembered and can be re-enabled at any time.

- To disable a startup program, select it from the list and click on the Disable button. A disabled startup program is indicated with a red cross.
- To re-enable a startup program, select it from the list and click on the Enable button.

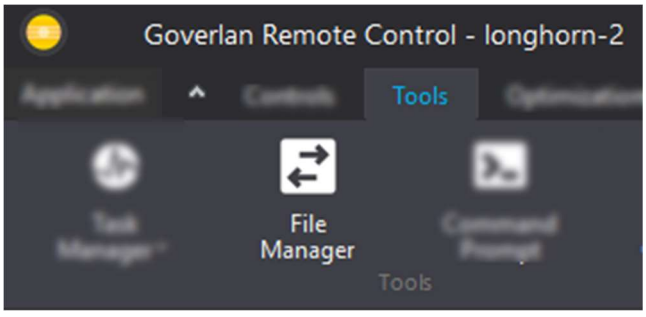
The File Manager

View, send and receive files from the remote file system with the File Manager

Opening the File Manager

While in a remote control session

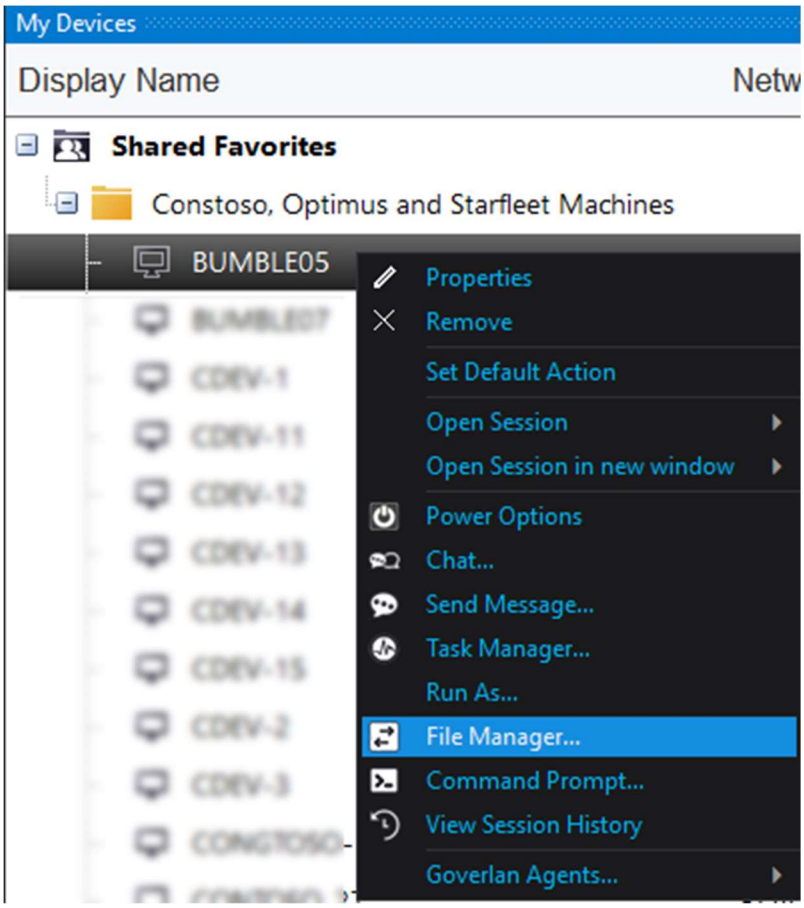
Go to the Tools tab in the Command Bar and click the File Manager button.



From the favorites menu

Right click any computer in your Favorites list and select File Manager.

© Copyrights Goverlan Inc. – All Rights Reserved

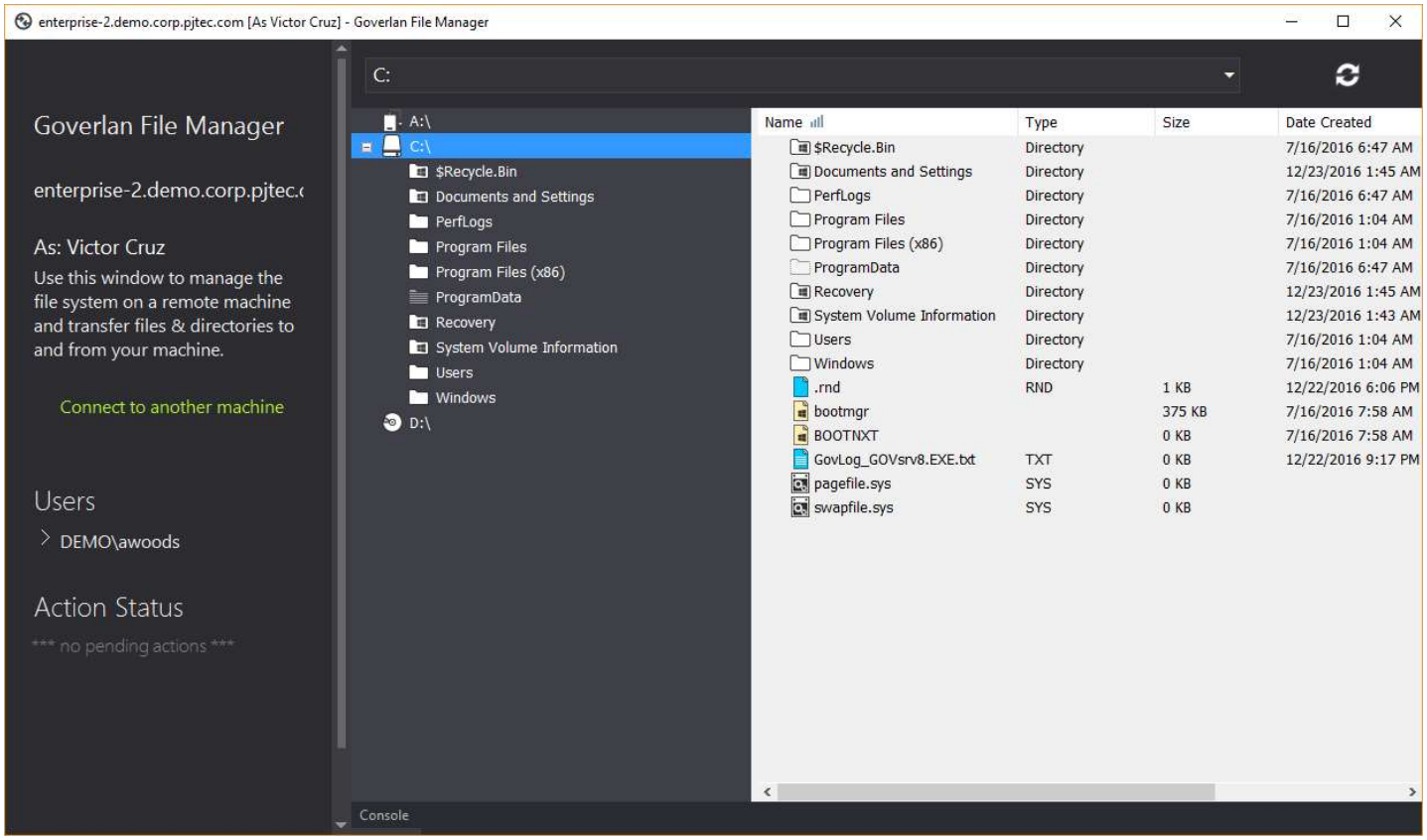


Using the File Manager

Viewing Files

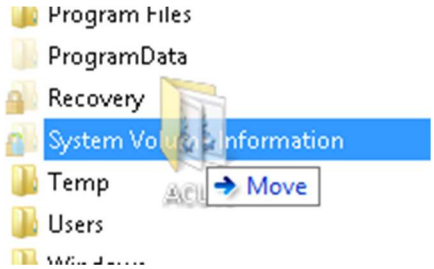
Use the main browser window to view the remote file system. Navigate folders and drives with the tree view or via the navigation bar.

© Copyrights Goverlan Inc. – All Rights Reserved



Sending Files

To send file to the remote file system, simply drag and drop files in to the browser window.



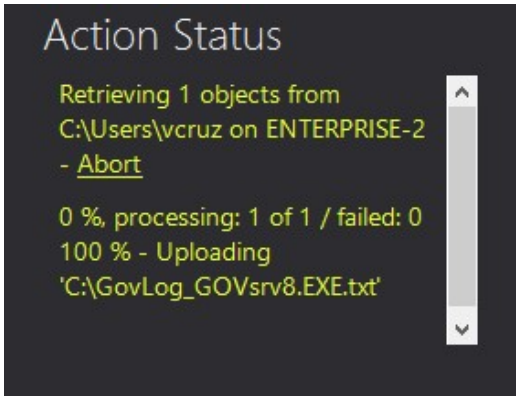
Retrieving Files

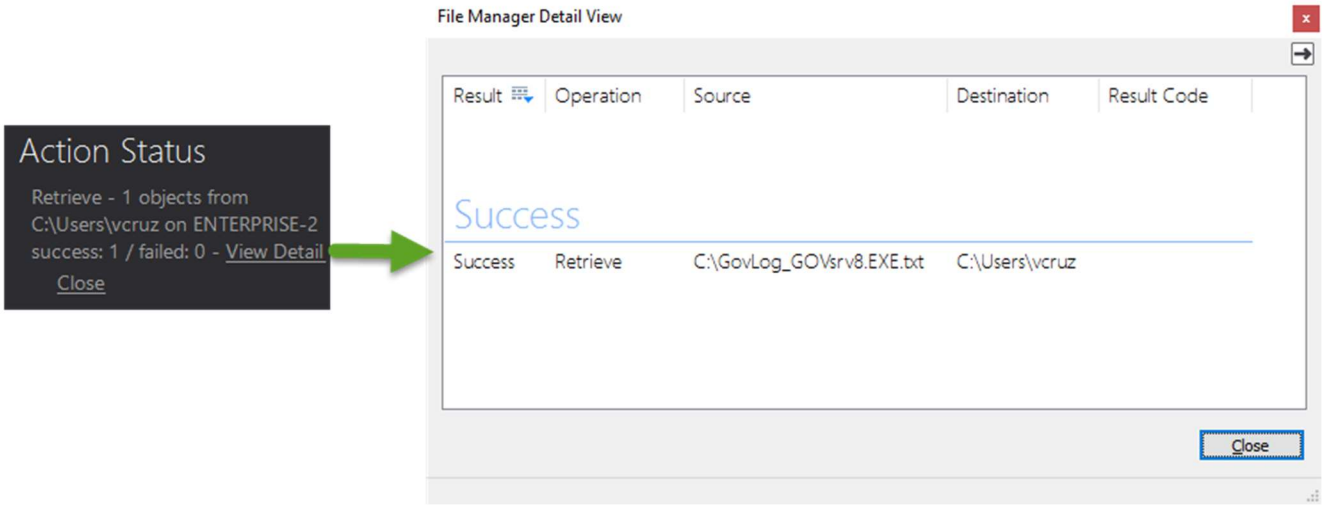
To retrieve files from the remote file system, right click the object and select **Get Files** or click the **Get Files** button

Send/Receive Status

All file transfers will include a status of the operation. A detailed status is available when the transfer is complete.

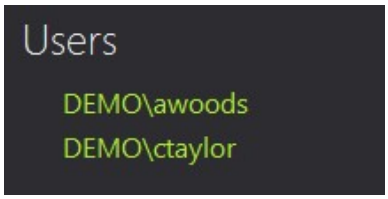
© Copyrights Goverlan Inc. – All Rights Reserved





Multiple Users

The file manager will display each user account that is logged in to the system. Switch to the desired user to see the of their mapped drives.



Chat and Push Messages

Stay connected with your users through Goverlan Chat and Push Notifications.

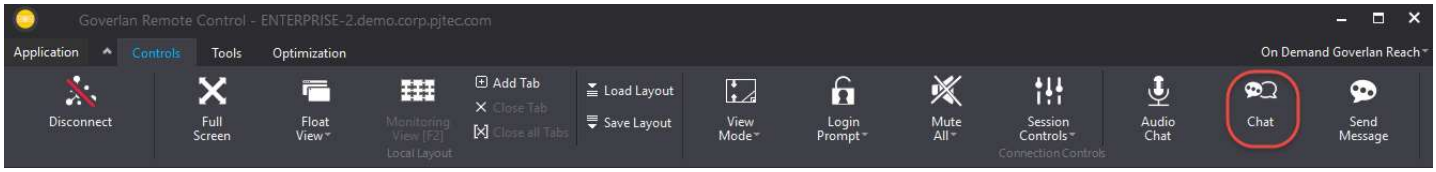
Starting Goverlan Chat Sessions

Initiate Chat sessions while in or out of a remote control session.

Starting chat sessions during a remote control session

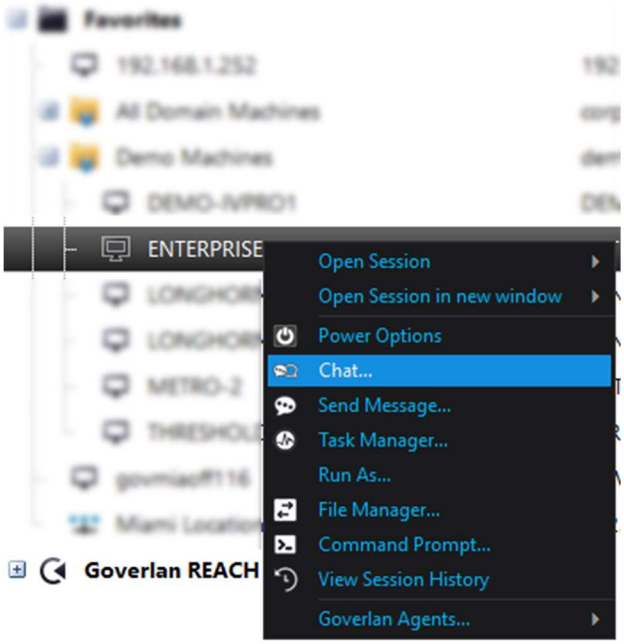
Go to the Controls tab in the Command Bar and click the Chat button.

© Copyrights Goverlan Inc. – All Rights Reserved



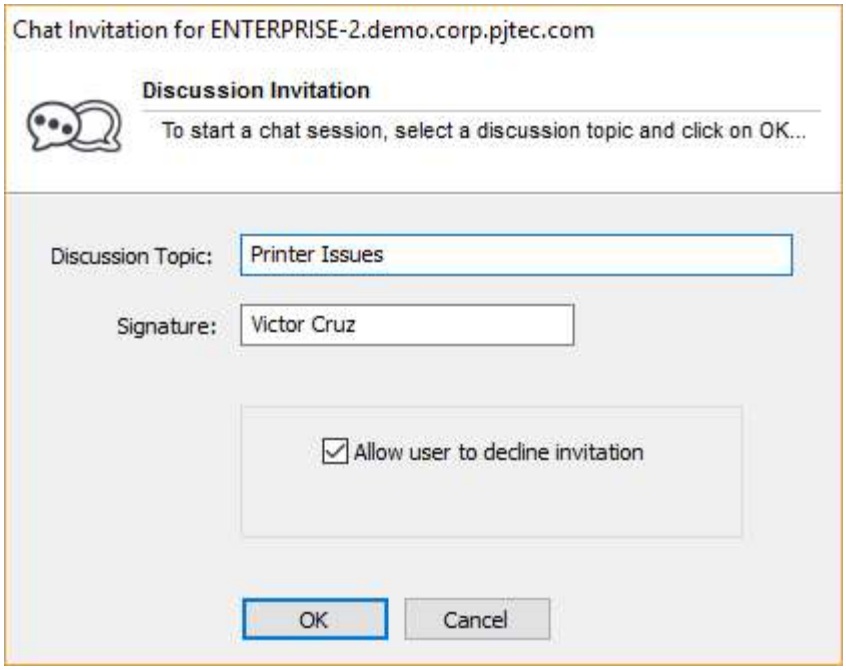
Starting chat sessions from the favorites menu

Right click any computer in your Favorites list and select Chat.



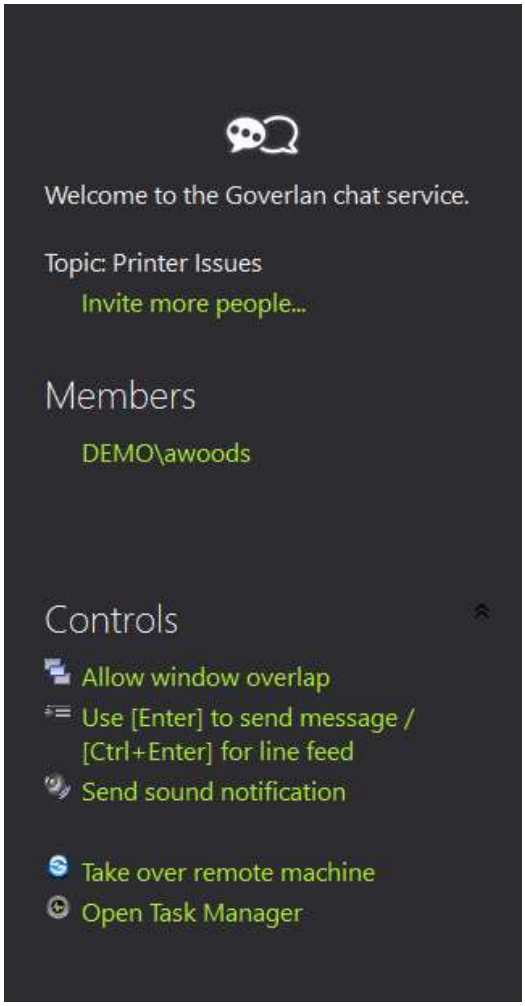
Discussion Invitations

The operator can establish a discussion topic to define the issues that will be discussed. By default, the signature is the operators AD display name.



Chat Controls

© Copyrights Goverlan Inc. – All Rights Reserved



Goverlan Chat has the following controls:

- Invite More People - Use this option to invite other Goverlan Operators or even other users. Initiations are done by computer name.
- Members - Use the members list to remove users from the chat session.
- Use [Enter] to send a message / [Ctrl + Enter] for a line feed - Choose how you wish to send messages.
- Send sound notification - Send a sound notification to alert the chat members.
- Take over the remote machine - Initiate a remote control session to the target users workstation
- Open the Task Manager - Open the Goverlan Advanced Task Manager focused on the target user's workstation.

Message Templates

Create and save message templates for commonly used responses.

Saving message templates

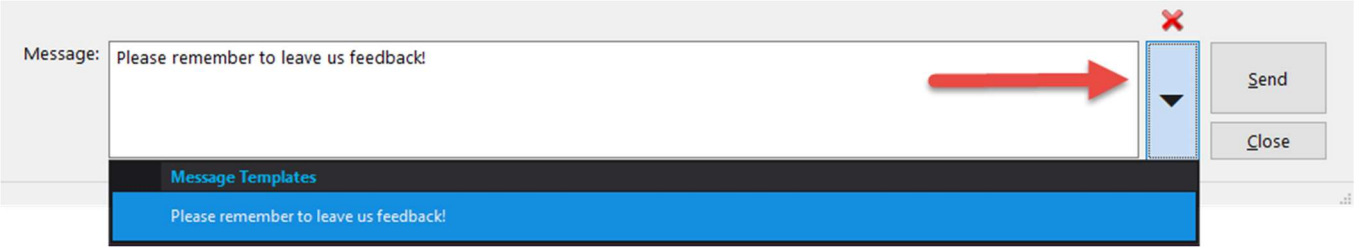
Type your message in the Message box

Click the to add the message as a template

© Copyrights Goverlan Inc. – All Rights Reserved

Retrieving and sending messages templates

Click and select the message you wish to send then click Send

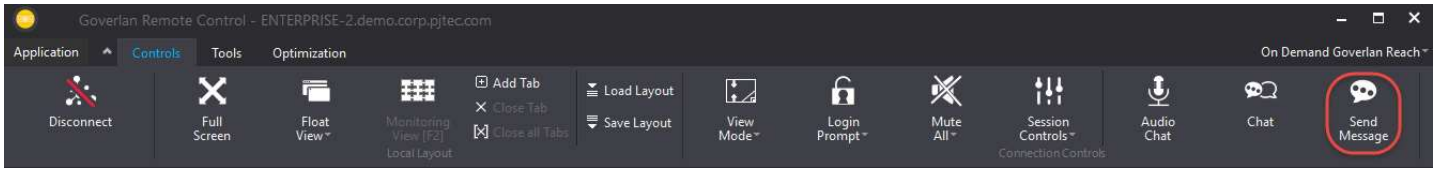


Sending one way push notifications

Use push notifications to send text alerts to your users.

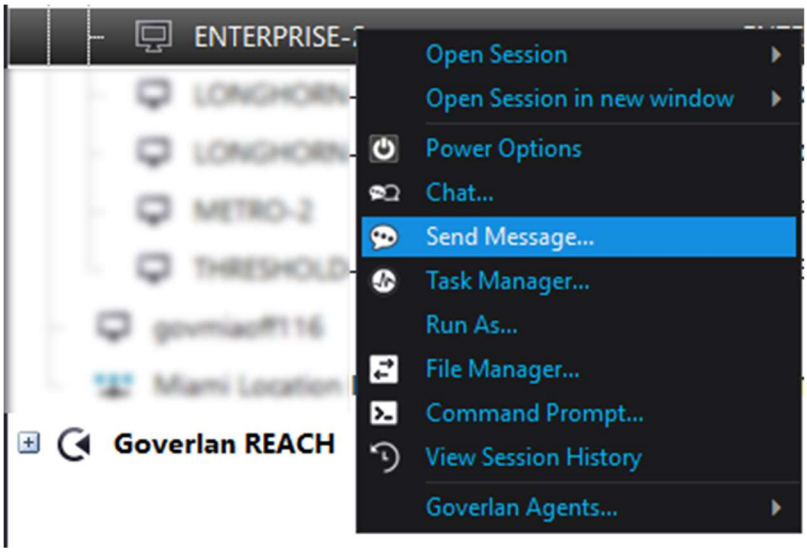
Creating new Push Notifications

Go to the Controls tab in the Command Bar and click the Send Message button.



Sending push notifications from the favorites menu

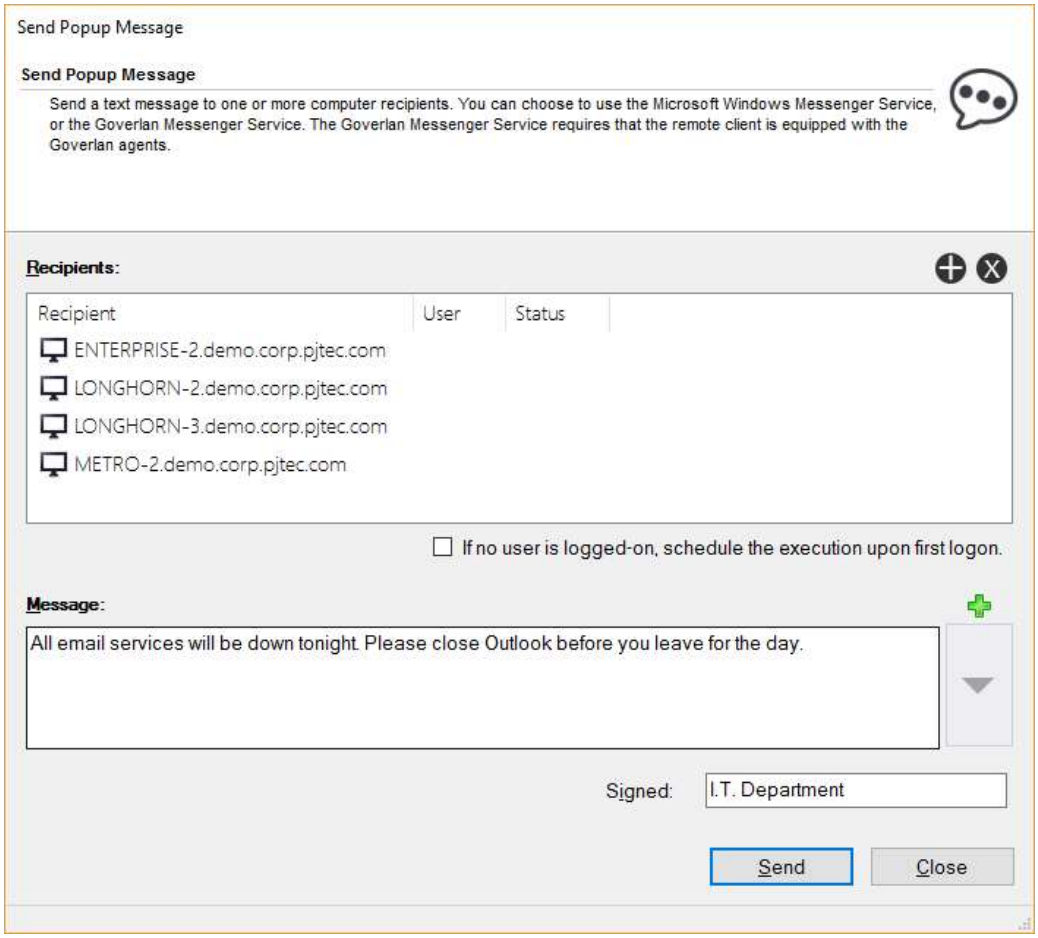
Right click any computer in your Favorites list and select Send Message.



Popup Message Options Window

The Popup Message window will allow you to add or remove recipients of the message.

© Copyrights Goverlan Inc. – All Rights Reserved



Message Templates

Create and save message templates for commonly used messages.

Saving message templates

Type your message in the Message box

Click the to add the message as a template

Retrieving and sending messages templates

Click and select the message you wish to send then click Send

Power Options

Power Options

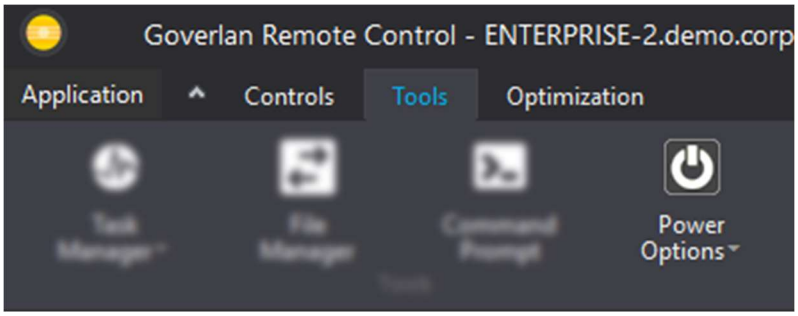
The Power Options Dashboard is an at-a-glance screen that provides a complete status of the workstation

Opening the Power Options Dashboard

Opening the Power Options Dashboard while in a remote control session

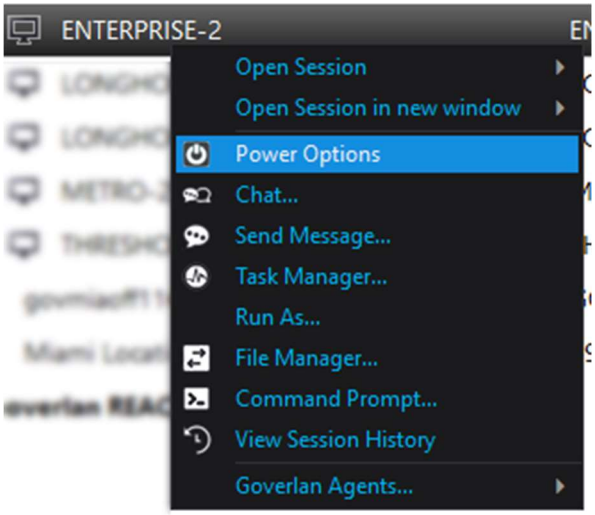
Go to the Tools tab in the Command Bar and click the Power Options drop down button.

© Copyrights Goverlan Inc. – All Rights Reserved



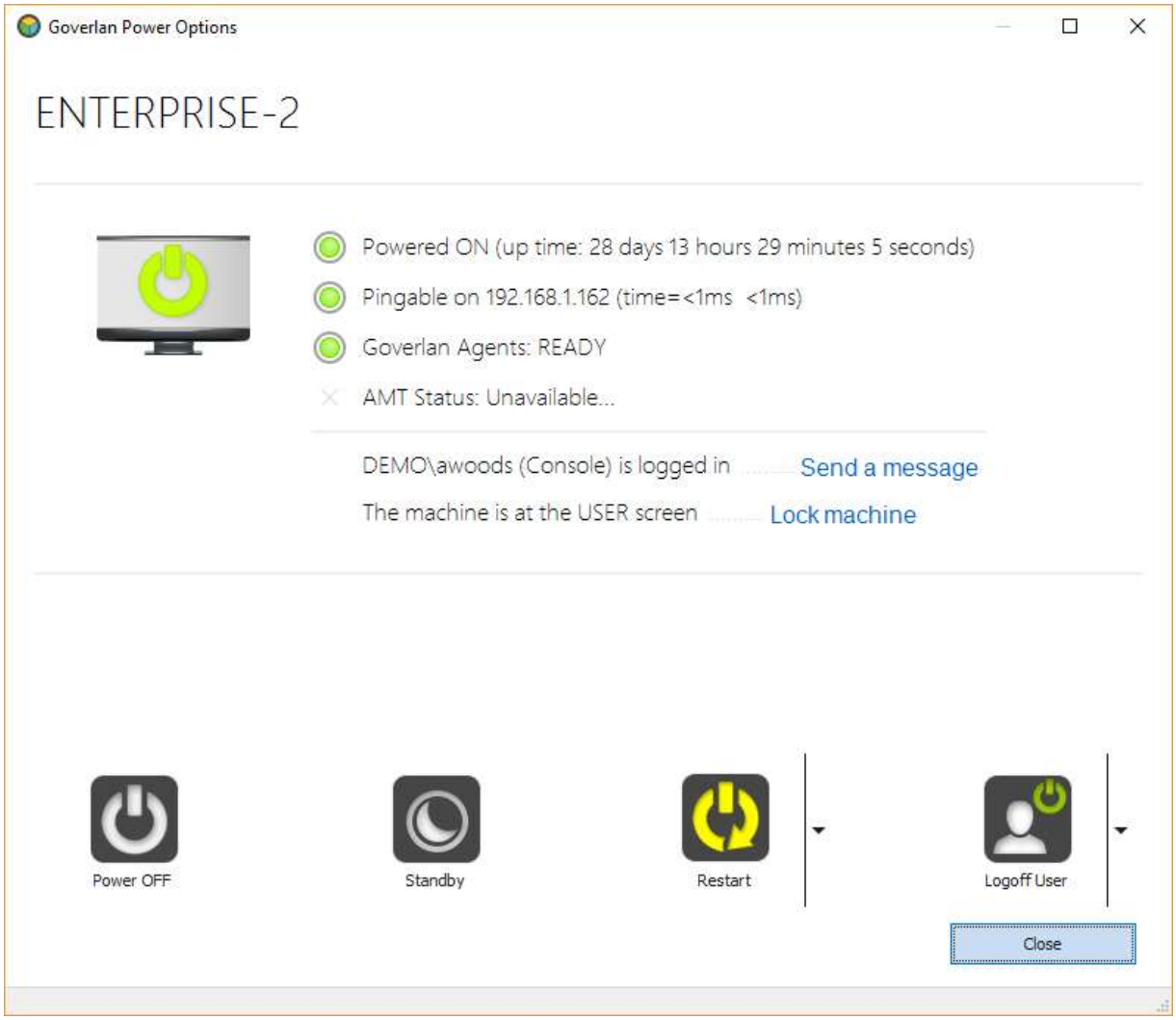
Opening the Power Options Dashboard from the favorites menu

Right click any computer in your Favorites list and select Power Options.



Power Options Dashboard features

© Copyrights Goverlan Inc. – All Rights Reserved



Power Status

Powered ON (up time: 1 day 1 hour 55 minutes 56 seconds)

The power status monitor shows the current power state and uptime of the computer. These states include

- Powered On
- Soft Power Off
- Powered Off
- Standby

Ping Status

Pingable on 192.168.1.204 (time=<1ms 1ms <1ms <1ms <1ms <1ms ...)

The Ping status monitor displays the IP address and the ping return times

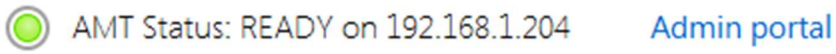
Client Status

Goverlan Agents: READY

© Copyrights Goverlan Inc. – All Rights Reserved

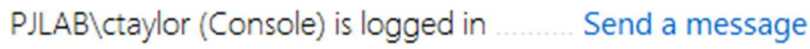
The Client Status monitor shows the current state of the Goverlan Client

Intel vPro AMT Status



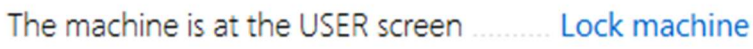
The AMT Status monitor shows the availability of the AMT chip. See Configuring Goverlan for vPro for more information.

Logged In User



The Currently logged in user will displayed here. If multiple users are logged in, the console user will be displayed as well as the number of active logon sessions.

Screen Status

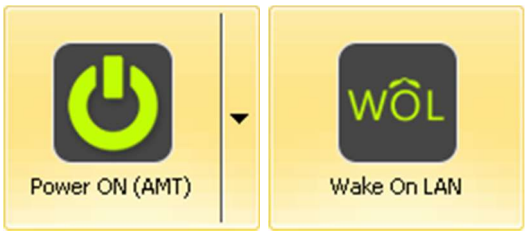


The current status of the console will be displayed such as Lock Screen or User screen.

Power Controls

The Power Control buttons will change depending on the current status of the computer.

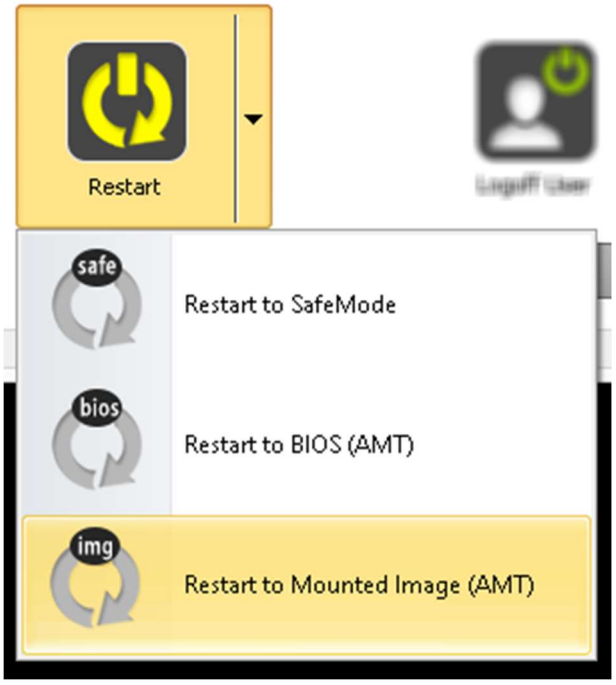
Power Button



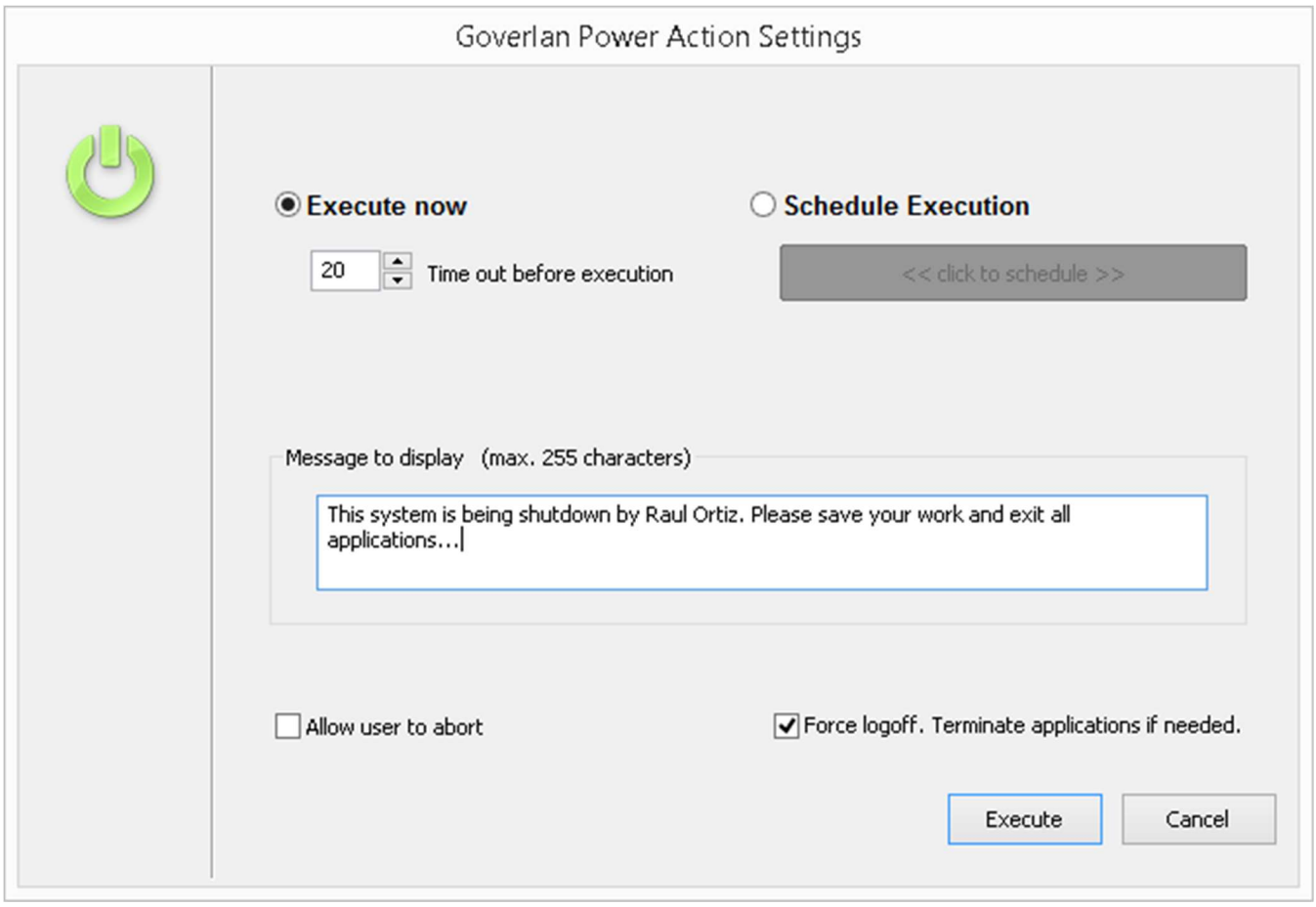
The power button has three states. Power Off, Power On (AMT) or Wake on Lan. For more information about Power On (AMT) see Intel vPro Power Options.

Restart Menu

© Copyrights Goverlan Inc. – All Rights Reserved



The Restart Menu contains several options for restarting a system. The standard Restart button will display options for letting the user abort the restart or scheduling the restart for later. A custom message can also be displayed during the countdown timer.

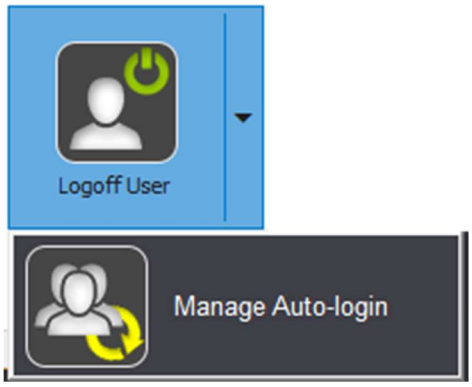


Restart to Safe Mode - Goverlan can restart a system into Safe Mode then re-establish the connection when safe mode is up.

© Copyrights Goverlan Inc. – All Rights Reserved

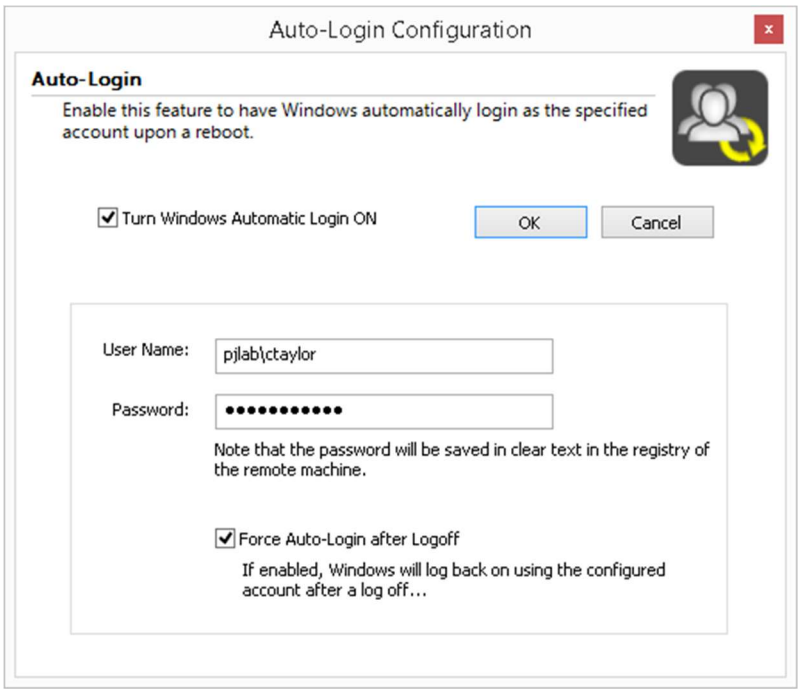
Restart to BIOS (AMT) or Restart to ISO (AMT) - Reboot any Intel vPro enabled workstation to BIOS or ISO Image. See Configuring Goverlan for vPro for more information.

Logoff User Menu



The Logoff User control will allow you to log off any user logged in to the system This includes RDP based sessions and Citrix XenApp Sessions. See Managing Windows Auto Login for more information.

Control Windows Auto Admin Logon setting. Applying this setting will make Windows automatically log in to the specified account.



REFERENCES

- Configuring Goverlan for vPro
- Managing Windows Auto Login

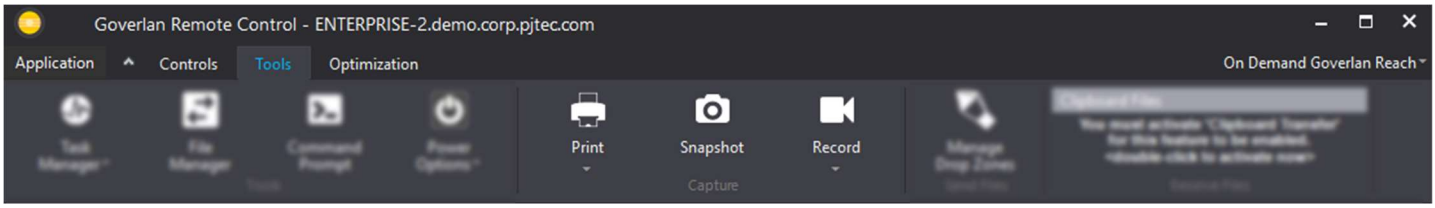
Screen Capture

Use Goverlan Reach RC to record, take a screenshot, or print the screen.

© Copyrights Goverlan Inc. – All Rights Reserved

Screen capturing tools

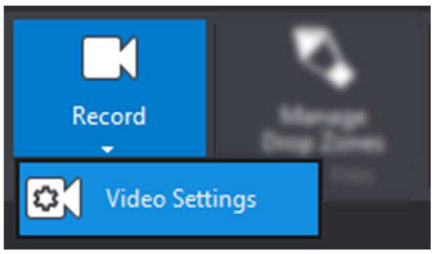
Access the screen capturing tools in the Tools tab of the Command Bar while in a remote control session.



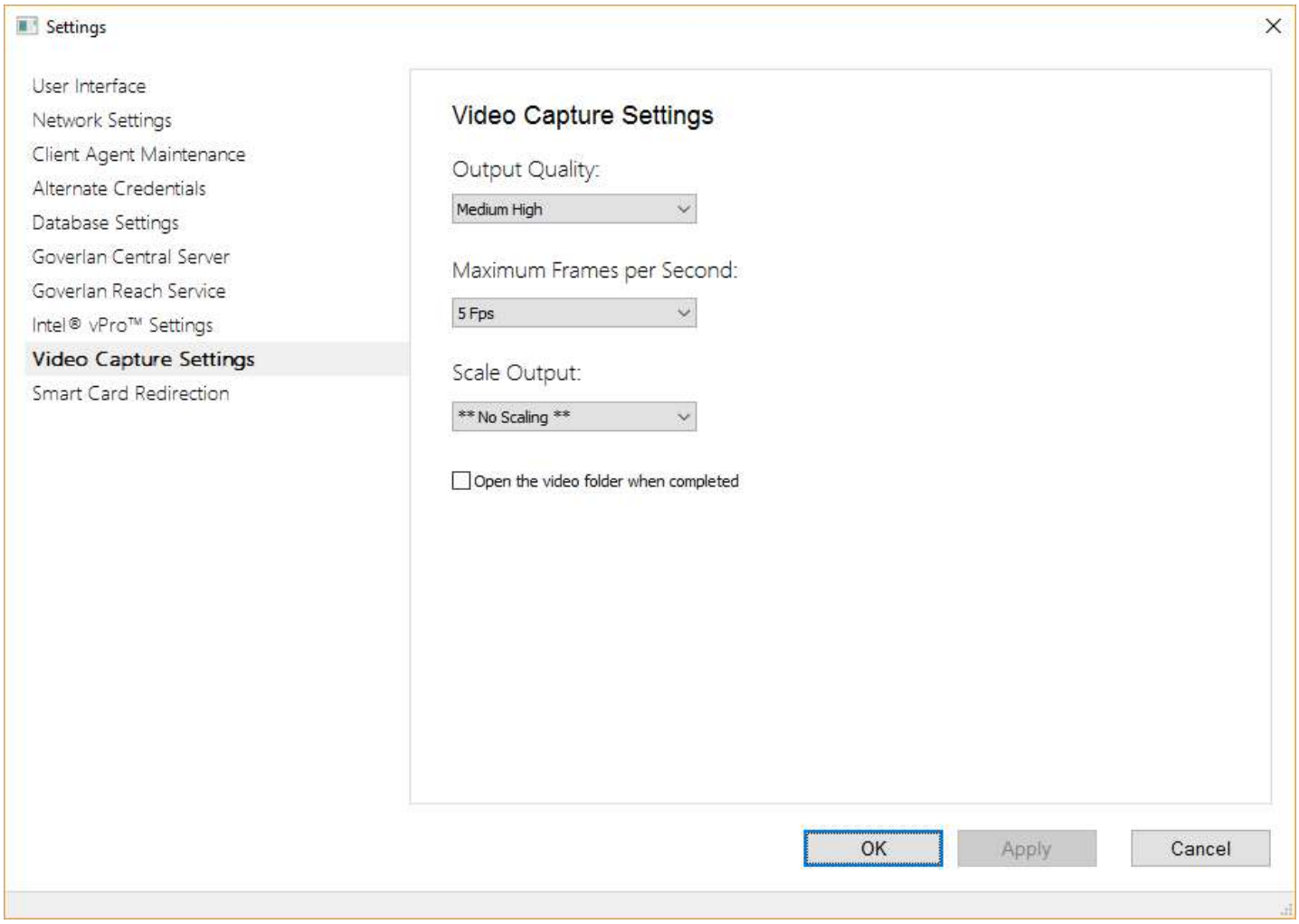
Screen Recording

Goverlan Reach RC can record a remote control session to AVI or MOV format.

Accessing Video Settings

Click the Record drop down button 

or go to Settings --> Video Capture Settings



© Copyrights Goverlan Inc. – All Rights Reserved

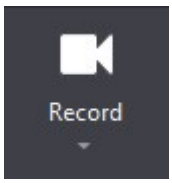
The following settings are available:

- Output Quality - This changes the output resolution of the video
- Maximum frames per second - This will determine how many samples will be taken in one second
- Scale Output - This setting changes the aspect ratio of the video
- Open the video folder when completed - This setting will open the folder where the video is saved when the recording is completed

Starting a recording

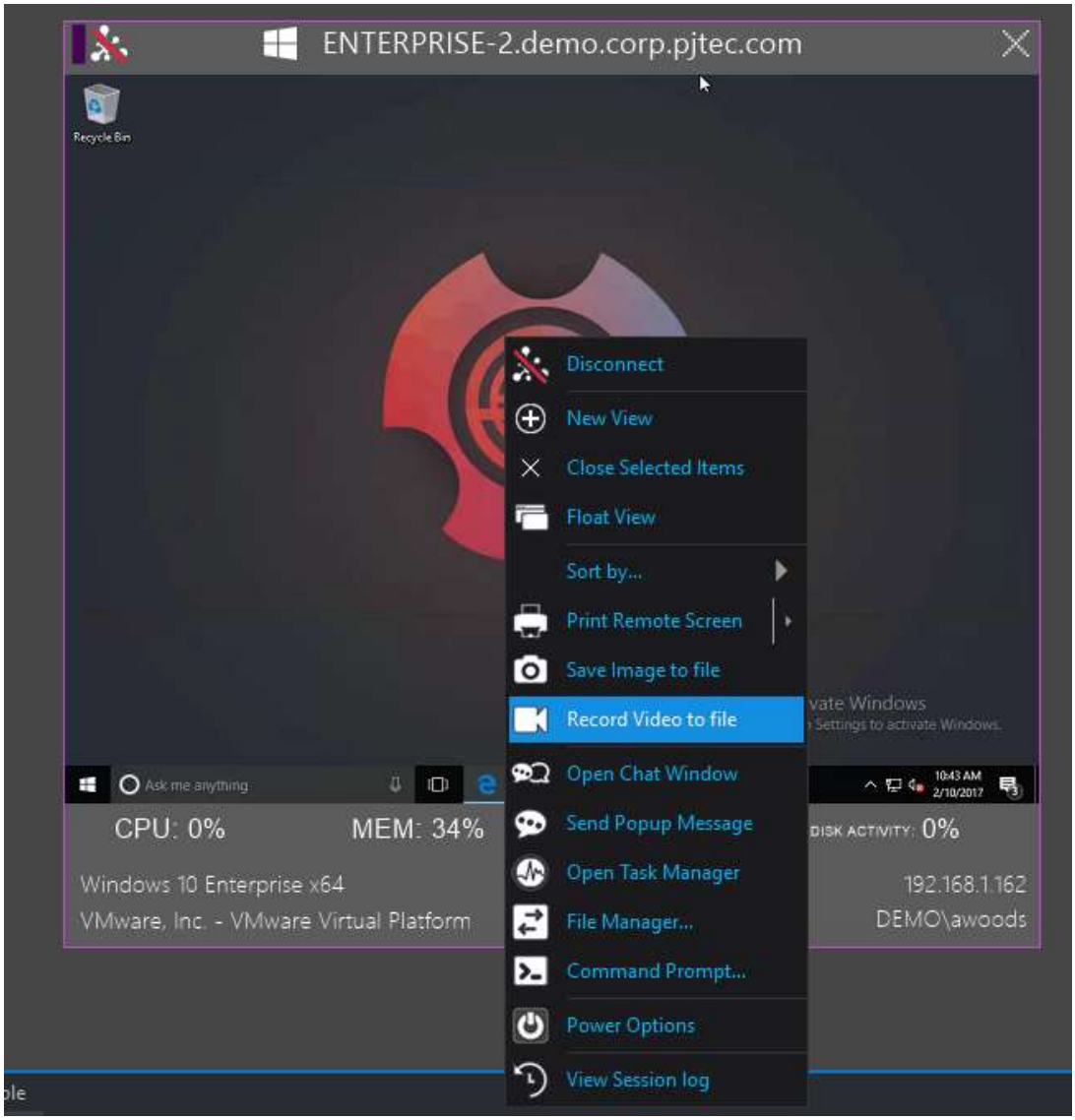
There are three options for starting a recording:

Click Record button in the Tools tab on the Command Bar.



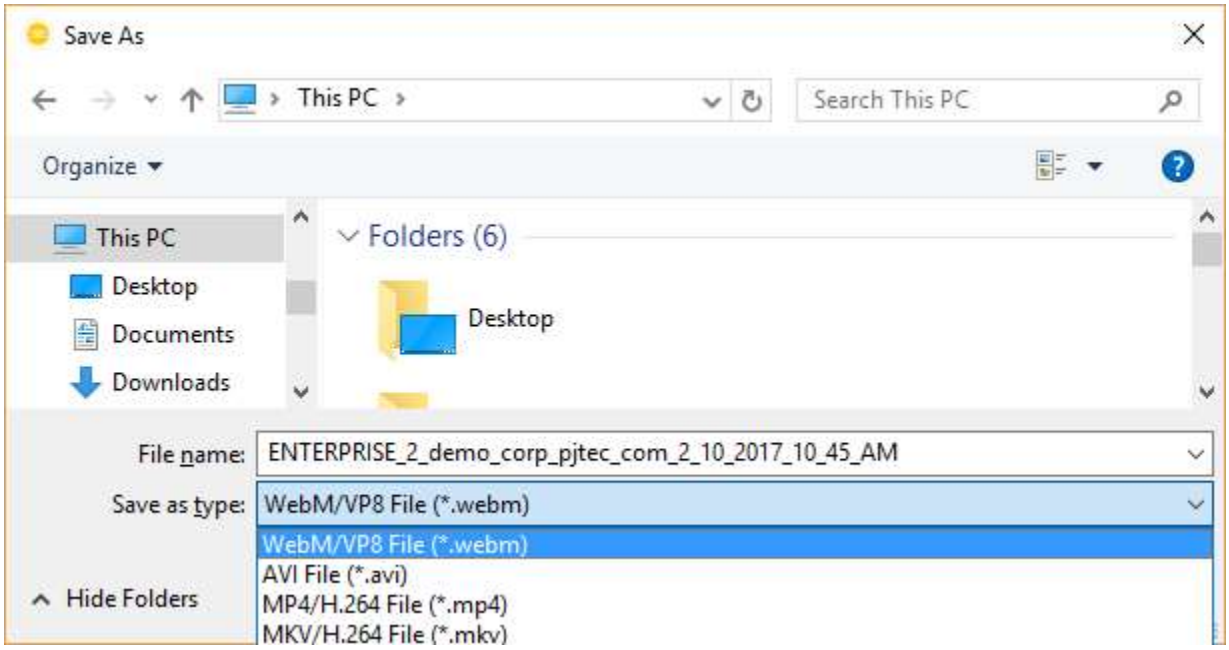
Right click a computer thumbnail in the Monitoring View. For more information about the Monitoring view see Performance Monitoring.

© Copyrights Goverlan Inc. – All Rights Reserved



Saving a Recording

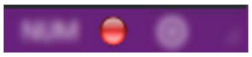
You can save video recordings in WebM/VP8m, AVI, MP4/H.264, MKV/H.264.



© Copyrights Goverlan Inc. – All Rights Reserved

Monitoring and stopping video recording

This icon will appear in the status bar when a recording is in progress

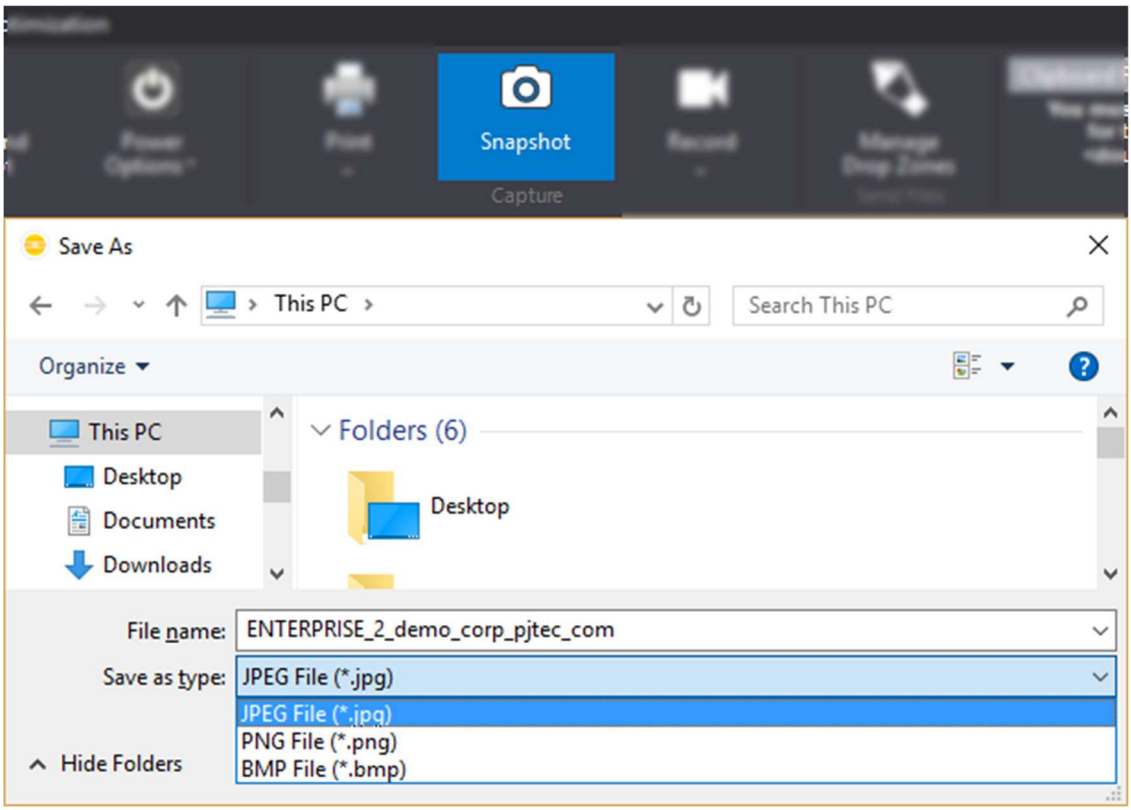


Click the recording button to show a list of in progress recording and click on a recording to stop it

The video will be saved in the location specified.

Screenshots

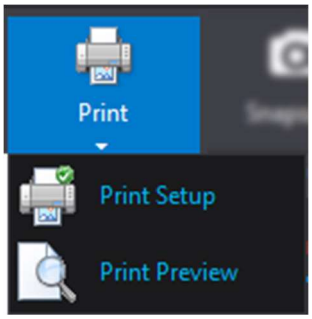
Use the Screenshots button to take a quick picture of the screen and save it to JPEG, PNG or BMP format



Screen Printing

Print a screenshot quickly with Print button

© Copyrights Goverlan Inc. – All Rights Reserved



REFERENCES

- Performance Monitoring

Windows Auto-Login

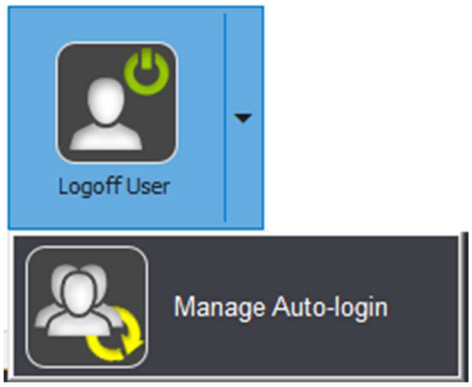
Windows Auto Admin Login is a Windows feature that allows an administrator to specify an account to automatically log in as. This is useful for administrative tasks that require automation, large lab environments or kiosk based workstations. Goverlan Reach RC allows you to access the Auto Admin settings and change them.

Accessing Auto Admin Login settings

Auto Admin Login can be accessed from 2 locations

Power Options Dashboard

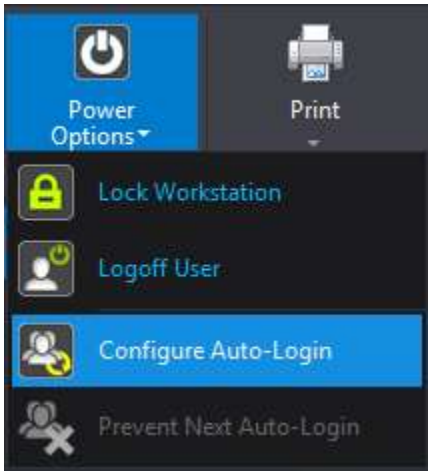
Use the Logoff User drop down click **Manage Auto Login.** For more information about the Power Options Dashboard see Power Options.



Power Options drop down menu

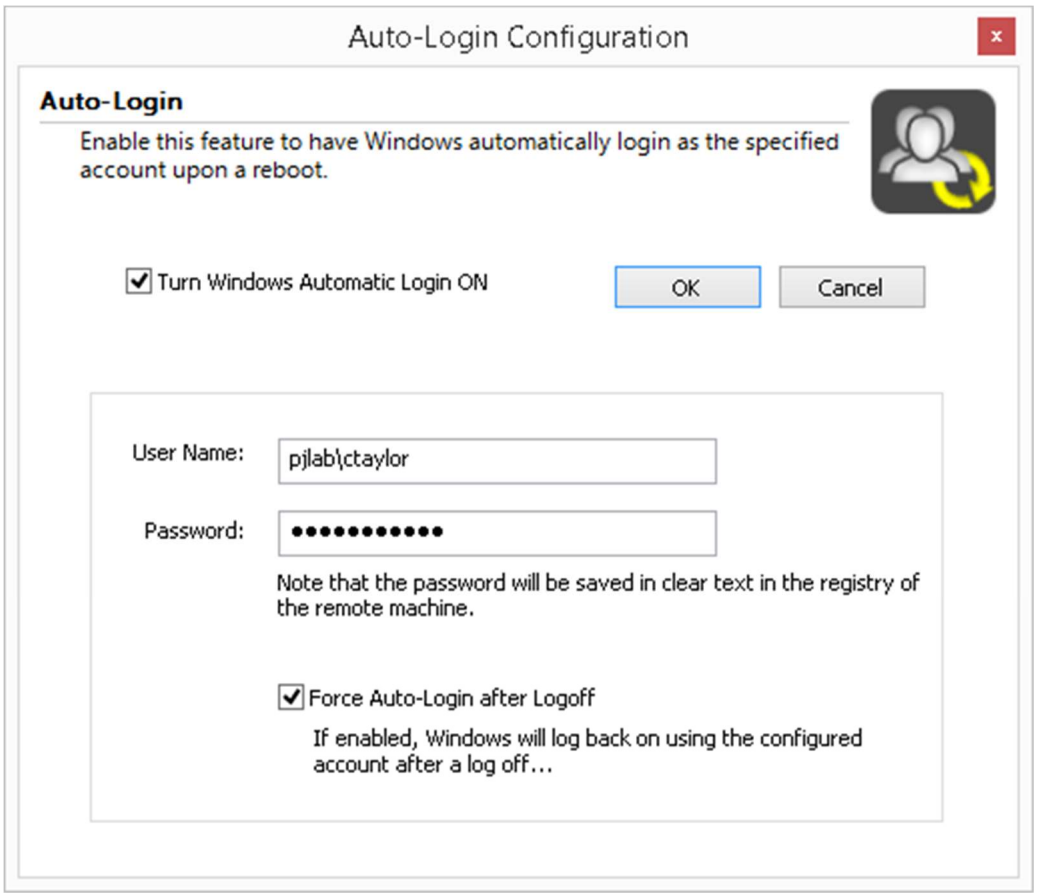
Use the Power Options drop down menu in the Tools tab of the Command Bar and select **Configure Auto Login**

© Copyrights Goverlan Inc. – All Rights Reserved



Auto Login Configuration

Select the Turn Windows Automatic Login ON box to reveal the settings.



The settings include

- User Name - This is the account that the system will use to automatically log in
- Password - This is the password to the account that the system will use to automatically log in
- Force Auto Login after Logoff - If the system is logged off, Windows will automatically log back in

NOTE: Windows Auto Login stores the password in clear text in the registry.

REFERENCES

© Copyrights Goverlan Inc. – All Rights Reserved

- Power Options