LANDesk® Management Gateway

Users Guide to Using the Management Gateway 4.2 and prior versions

LANDesk® | make IT happen
An Avocent® Company

Contents

Introduction

This whitepaper is designed to help users of the Management Gateway to configure remote control both on the client and viewer. This document is also designed to aid with troubleshooting and configuring common communication problems with a LANDesk Management Agent that is connecting through the Management Gateway.

Scope

The scope of this whitepaper is limited to using the Management Gateway although some of this information may be of use to administrators as well. Some of the instructions given in this document may require administrator access on the remote computer or core server which may or may not be available.

Technology Overview

The Management Gateway is an appliance that is designed to bridge incoming connections. Connections can be established from several different sources: LANDesk Core Server, Remote Control Client, Remote Control Viewer, LANDesk Management Agent, etc. When two of these connections are bridged by the Management Gateway an SSL Tunnel is established between the two sources and allows exclusive communication.

Remote Control Viewer

The Remote Control Viewer and Client act similar to a client-server system. The remote control client sits in wait either on the computer itself or posted to the Management Gateway. The viewer then searches out the client and requests a connection. The viewer and client are technically separate from LANDesk in general but security authentication and other features may be involved.

Installation

From the Management Gateway

1- Browse to the main Gateway webpage.
2- Click on Management Gateway Utilities
3- Click on “System Tools” and select “LANDesk remote assistance viewer”

From the Web Console

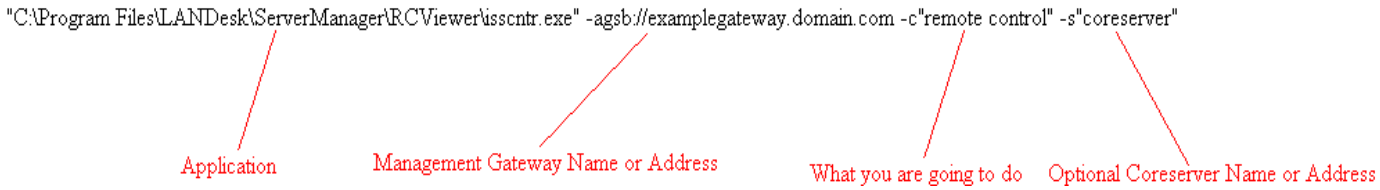
1- The remote control viewer will automatically install itself once you attempt to remote control a device from the web console. If removal or reinstallation is needed see “Removing the Remote Control Viewer” later in this document.

From the LANDesk Core Server

1- C:\inetpub\wwwroot\common\ENURCSetup.exe

Creating Shortcuts and Switches

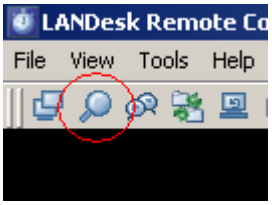
After the Remote Control Viewer is installed you can create a shortcut that will point directly towards the Management Gateway of your choice.



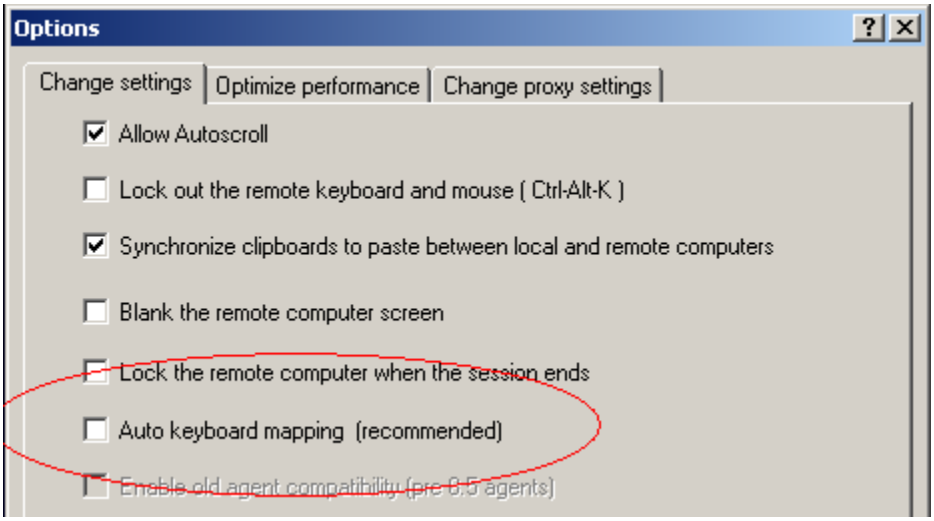
Viewer Options

Most of the options in the Remote Control Viewer are self-explanatory. Simply moving your mouse over the icon on the main screen will display the buttons purpose. However, there are a few options that may be confusing or work in a way that you should know.

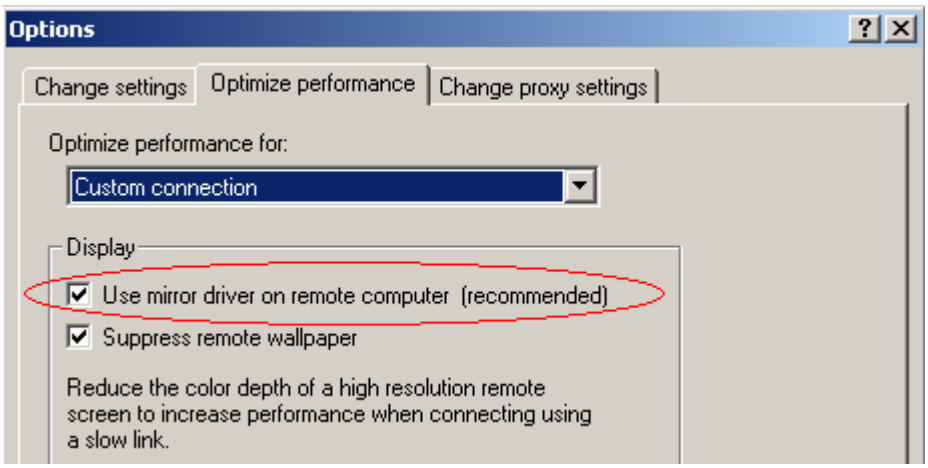
Start/Stop Viewing of the Remote Computer – This button (see below) does exactly what it says. However, the button works if you are actually connected to a computer or not. If you connect to a remote computer and you cannot see the screen then be sure to check if this button is pushed or not.



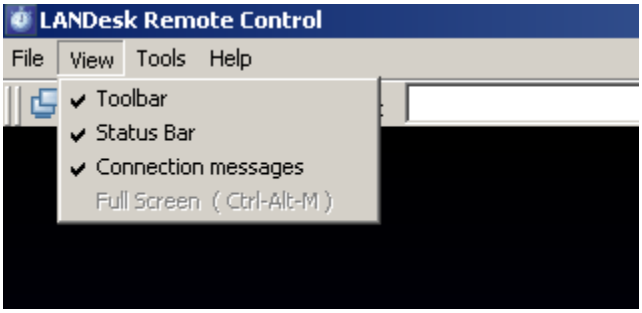
Auto keyboard mapping (recommended) – This option also does what it says however only basic key mapping is supported. Foreign language keyboards may have some difficulty with this setting especially in regards to special characters.



Use mirror driver on remote computer (recommended) – This option (shown below) is a method of increasing performance for remote control. The mirror driver is a component that is typically installed with a LANDesk Management Agent. This driver was designed by Microsoft Standards to basically route video directly to the connection. The driver itself is compatible with most video cards and drivers but there are some combinations that may result in problems. Distorted video and blank screens are just some of the issues seen when the client has a problem with this driver. Using the mirror driver is not required and some of the newer video cards and operating systems may work just fine without it.



Viewing Connection Messages – Underneath the View option on the viewer menu you can turn on/off Connection Messages. I personally like to close the connection messages Window at the bottom of the screen to allow more room to work on the client but this menu is very important when you are having connection issues. The window will display a lot of valuable information including IP address, name, remote control information, and failure messages.



You should become familiar with all the options located under the Tools and Options menu in the Remote Control Viewer. These options can either fix your remote control issues or make the experience much more enjoyable.

Prompting for Credentials

The Management Gateway uses separate user accounts than the domain or the LANDesk Core. Therefore when a remote control session is established through the Management Gateway you will always be prompted for credentials at least once. If you get prompted for credentials a second time then there may be a problem with your permissions or the configuration on the client system. By default the Remote Control Viewer will send the credentials of the person logged into the Operating System instead of the person logged into the console or the Remote Control Viewer.

Removing the Remote Control Viewer

The Remote Control Viewer installs as a standard windows application and therefore can be removed using Add/Remove Programs in Windows.

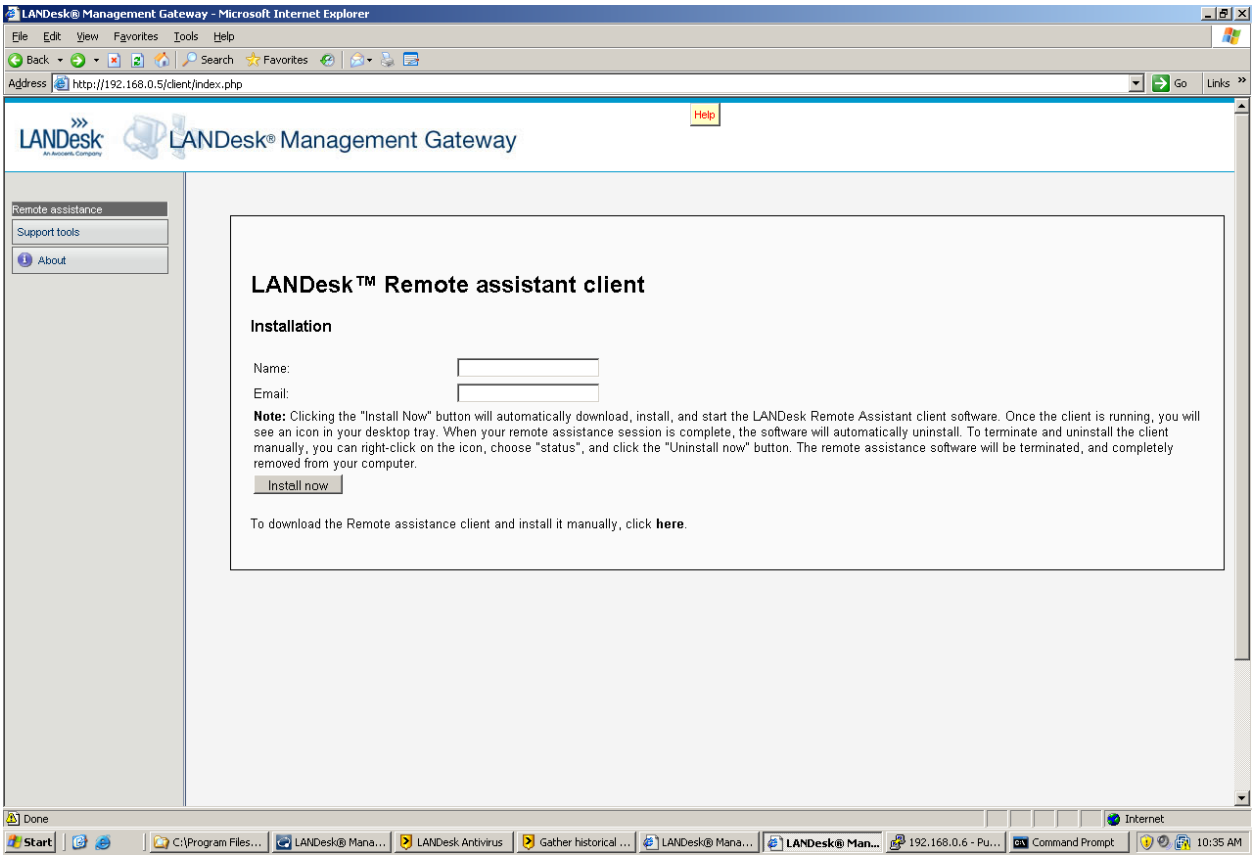
Remote Control Client

The remote control client is the application that needs to be run on a target computer in order for remote control to take place. This application can be executed or used in several forms as listed below.

On-demand Clients from the Gateway

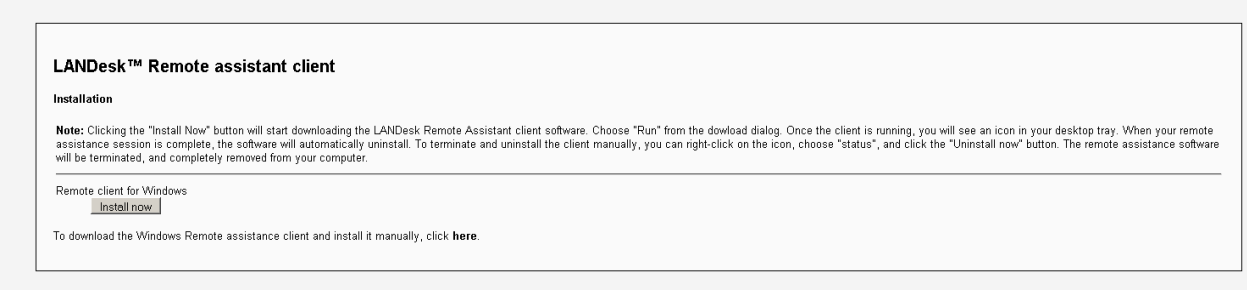
The Management Gateway has a public facing web page. The web page has several options but the primary purpose of the page is to provide access for the Remote Control Client. This page has changed somewhat over the years as different versions of the Management Gateway have been released. The "Client" webpage can be accessed by clicking on the "Management Gateway Utilities" link on the default homepage of the Management Gateway.

ISO release and the first generation Appliance (version 4.0) – These two releases of the Management Gateway utilized an Active X Control on the client webpage. A user would enter their name and email address and click the "Install Now" button as shown in the screen shot below:



As browsers advanced Active X Controls became more and more dangerous to use. As a result most current browsers block Active X Controls which makes it difficult to utilize the Client webpage on the Gateway. A work around is typically to install the On-demand Remote Control Client manually as described later on in this section.

Second Generation Appliance (version 4.2) – This version of the appliance saw a slight upgrade that removed the Active X Controls. There is still an occasional issue with clients that are behind a Proxy or in other locked down networks but most clients work fine by using the "Install Now" button shown below. The previous ID codes that were gathered on the web page were changed to automatically collect the hostname on the client.

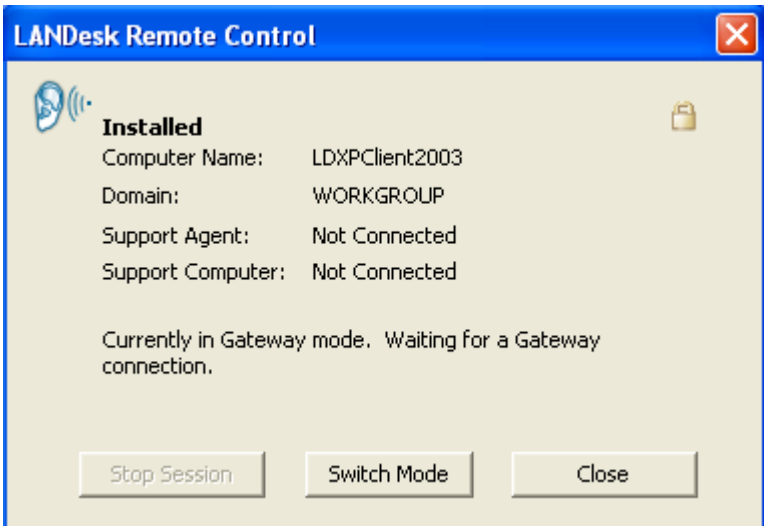


On-demand Clients using a Self-Contained Executable

A self-contained on-demand Remote Control Client executable can be created on the LANDesk Core server. This option is located under Configure – Management Gateway – Certificates Tab. The self-contained executable functions just like the one on the Management Gateway itself with a few other configurable options. The options available are not part of the scope of this document but the executable can be hosted on any website and functions just like the manual method described later.

LANDesk Agents and the Management Gateway

If the target client that you wish to remote control has a LANDesk Management Agent installed then remote control is already present and either needs to be disabled for on-demand remote control or the mode needs to be set to "Gateway Mode". See the screenshot below



The window above appears after you double-click the remote control icon by the clock on the client system. The "Switch Mode" button is available if the client certificate contains Gateway information. If the "Switch Mode" button is grayed out then this client was installed before a Management Gateway was configured on the core server.

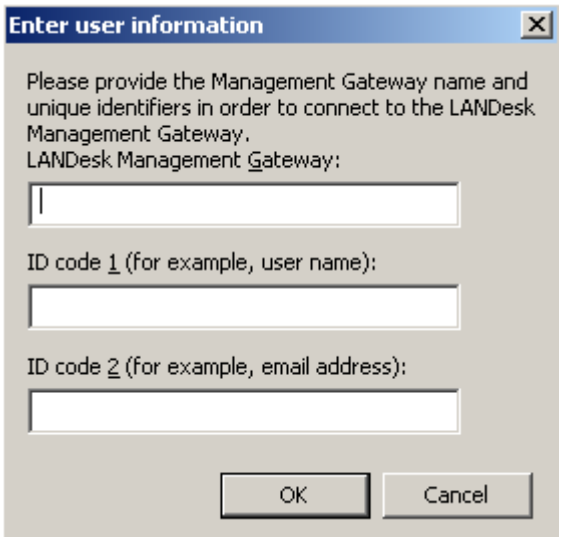
Clicking the "Switch Mode" button will stop the remote control service and restart it in opposite mode. If the client is currently in "Gateway Mode" as shown above then it would restart in "Direct Mode". Direct Mode only functions if the client is on the domain and/or the viewer has direct access to the device.

The important thing to note about LANDesk Agents and on-demand remote control is that on-demand will not work if another remote control service is already running. The running remote control service will need to be stopped using "Services.msc" before executing the on-demand client. In some cases multiple instances of remote control can load into memory and cause more problems. If you are having trouble establishing remote control with an

established LANDesk Agent then you may want to check Task Manager (Control + Alt +Delete) and look for any processes that start with ISS. Issuser.exe is the primary application for remote control clients but other applications (like issproxy.exe) may be running as well and need to be shut down.

Installing the On-demand Client Manually

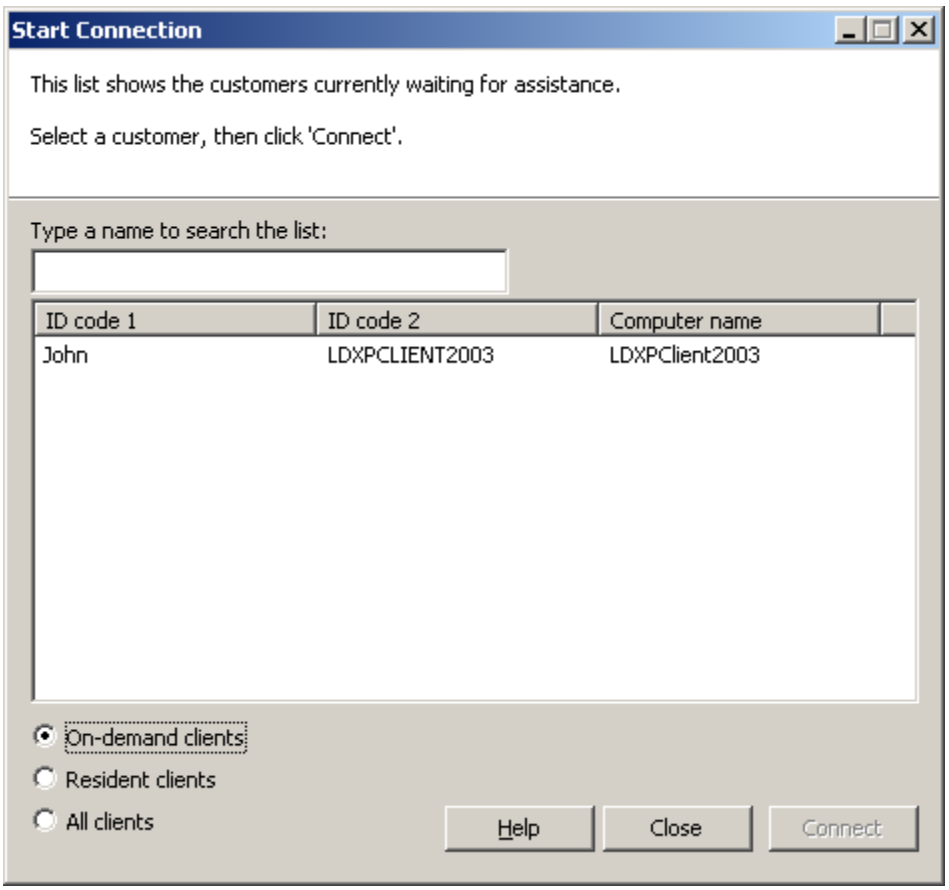
On each version of the Management Gateway the client web page contains a manual link to download the on-demand remote control client. This manual download can not only benefit the Active X version of the client but it can work in other circumstances as well. The manual download of the on-demand client on the 4.2 version of the Gateway looks and works the same as the automatic install but the 4.0 and previous versions will look like this:



ID code 1 and 2 can technically be anything you like but these fields are what will show up on the Management Gateway when the client is available for remote control. The LANDesk Management Gateway field will need to be either the IP address or the domain name of the destination Management Gateway.

Starting Remote Control with the Client

Once a device has installed the Remote Control Client through any of the means mentioned so far it will be posted to the Management Gateway. Once you finish logging into the Remote Control Viewer you can see the list of available clients.



Selecting On-demand or All Clients will show all clients that are available in regards to on-demand. When the On-demand Client installs, depending on the method it will show what was entered in the client fields or it may automatically post the computer information.

Note: Remote Control sessions have a built-in timeout of 10 minutes. If no activity is detected then the connection will be closed. A simple click can reset the timer and keep the session active.

LANDesk Management Agents

Remote Control is not the only thing the Management Gateway is good for. Any LANDesk managed device that has access to the internet has the option of connecting back to its core server and submit Inventory Scans, Security Scans, and other agent tasks. A complete technical discussion on how this works is not part of the scope of this document, however a basic understanding will help in troubleshooting and configuring scheduled tasks correctly.

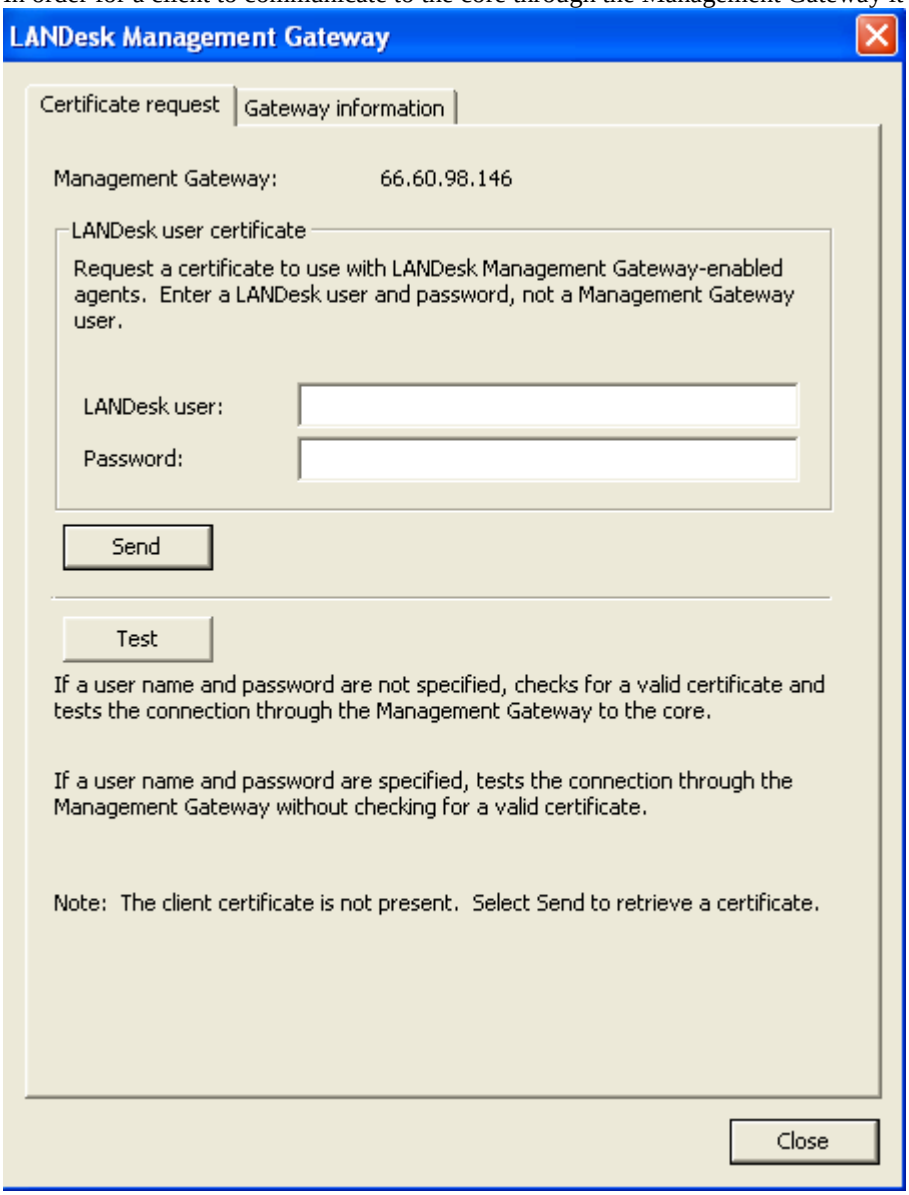
When a managed device (a computer with a LANDesk Agent installed) is outside of the domain it cannot contact the core server directly. In these cases the applications (Inventory, Security, Policies, etc) that run on the client will contact another executable call Proxyhost.exe. A proxy as most people know is something or someone that acts on behalf of another. The same is true in regards to Proxyhost.exe. If the Inventory Scanner on the device needs to send in a scan, request a file, etc. then it will contact Proxyhost.exe who then contacts the Management Gateway on the applications behalf. An SSL Tunnel is established to the Management Gateway which is then bridged with an SSL Tunnel coming from the core server. The client then has direct secure access to the core in which to conduct its business. As far as communication is concerned the SSL Tunnel allows only communication with the core server and nothing else.

Due to the technology described above (and some not mentioned) a few rules regarding usage of the Gateway are required:

- *The coreserver name used on the client should be the hostname of the core server*. In some cases the Fully Qualified Domain Name (FQDN) will work but an IP address will never work. The coreserver name is stored on the client in the following registry key: HKLM\SOFTWARE\Intel\LANDesk\LDWM.
    - *Note*: The inventory scanner shortcut will have core server entries of its own and will need to be changed separate.
- *A software distribution package needs to reside on the core server and it needs to be a web share.* Due to the SSL Tunnel etc the client can only see the core and nothing else. Also, it will only have access to download files from a web share.
- *Any scheduled tasks for clients connecting through the Management Gateway need to have a Policy distribution method*. Despite the SSL Tunnel the core really doesn't know where the connecting client is coming from and can only respond to requests. As a result scheduled tasks cannot be pushed to a client and a policy (or pull method) is required.

Requesting Client Certificates

In order for a client to communicate to the core through the Management Gateway it must request certificates.



The application shown above is called Brokerconfig.exe. This client executable is responsible for communicating with the core server and retrieving certificates. Brokerconfig.exe can request certificates on or off the network. If the client is on the network then credentials are not needed. However, if the client is off the network then credentials of a user account on the LANDesk Core server with the proper rights will need to be used.

The second tab of this application will contain options on how to reach the core server. By default "Dynamically determine connection route" is selected. This option will try to resolve the core first and if that fails it will attempt to communicate with the Management Gateway. If the application can resolve the core name (not necessarily connect to it but just resolve it) it will stop and only attempt direct communication with the core. As a result itls usually a good idea if you're having problems retrieving certificates from the core to change the option to one of the other selections that apply to where the client is located.

Note: If the agent was installed before the Management Gateway was configured on the core server then Gateway information may not automatically show up in this application. If Gateway information is not present then it can be entered manually or a reinstall of the agent can take place.

Software Distribution and Patching

Due to the design of the Management Gateway the Core Server doesn't have the ability to contact any clients connecting through the Gateway. The core more or less responds to requests via the connecting client SSL Tunnel. This design limits how you can distribute software packages and patches through the Gateway and results in a few requirements in order to make the process work. The following is a list of guidelines to follow for all scheduled tasks for a Management Gateway Client:

1- All tasks are required to have a distribution type of policy so a push will not work. If anything is needed from the client it must take the form of a policy so the client will check-in with the core and receive the request. For example: If an inventory scan (outside of the regular scan) is needed then it needs to be scripted in a custom script.
2- All software distribution packages and patches must reside on the core server. The Management Gateway bridges an SSL Tunnel between the client and core server. This tunnel enables the client to communicate with the core but ONLY the core.
3- All software distribution packages and patches need to be shared via a Web Share. Also due to design a client will not be able to download files from the core on anything other than a Web Share.
4- Broker Certificates on the client are required. See previous section.
5- The core server entry in the registry on the client needs to be either the hostname or FQDN of the core. General rule of thumb for the Management Gateway: "A hostname will work most of the time, the FQDN will work some of the time, but an IP address will never work". The core server entry is located in the registry under: HKLM\Software\Intel\LANDesk\LDWM\Coreserver

Note: The inventory scanner on a client system uses references in the shortcut to contact the core server and not the previously mentioned registry key. If you are experiencing problems with Inventory and not a Security Scan for example then make sure you are checking the correct location.

Advanced Troubleshooting and Errors

Listed below are some issues, errors, and other items to be aware of.

Issue: Trouble connecting with the remote control viewer
Possible Symptoms: The viewer appears to hang when connecting. The viewer takes a long time to connect. (Note this can be normal on some operating systems) You don't see any clients when attempting to remote control through the Management Gateway.
Resolution: Close all processes that start with "iss" and restart the viewer. The application issproxy.exe appears to be the main cause of this random issue but other remote control applications could be running as well.

Common Errors and Resolutions

The errors listed below are what can appear in the Remote Control Viewer when attempting to connect to a client system.

"Unable to contact the server on." – This message is related to Integrated Security for Remote Control. The viewer needs to send a signed rights document to the core server and request permission. The error message is saying that the viewer doesn't know what coreserver it should send the information to. The typical resolution to this message is to add the optional –S switch to the shortcut as noted previously.

"Unable to contact the server on <server name>" – This message is similar to the above message but the difference is that the Remote Control Viewer knows what core to connect to it just cannot connect to that core. In technical details the viewer is trying to reach the following on the core server:

https://CoreNameOrIP/landesk/managementsuite/core/ssl/remotecontrol/RemoteControlService.asmx

The normal resolution to this is to investigate what ports are open between the remote control viewer machine and the core server. Port 443 needs to be open to the core server in order to POST to IIS.

"Unable to establish a secure session with the remote computer (-5)" – This message is also related to Integrated Security for remote control. In this case the credentials of the operating system that the remote control viewer is on were passed to the core server and for some reason the core server couldn't grant access. There are several possible resolutions for this issue but most of them involve the core server itself. As noted in community.landesk.com the COM+ objects are the most common cause but it can also be because of simple permissions in LANDesk.

Conclusion

With the proper utilization the Management Gateway can be a very powerful tool in managing and remote controlling clients outside of the network.

About LANDesk Software

The foundation for LANDesk's leading IT management solutions was laid more than 20 years ago. And LANDesk has been growing and innovating the systems, security, service and process management spaces ever since. Our singular focus and our commitment to understanding customers' real business needs—and to delivering easy-to-use solutions for those needs—are just a few of the reasons we continue to grow and expand.

LANDesk pioneered the desktop management category back in 1993. That same year, IDC named LANDesk the category leader. And LANDesk has continued to lead the systems configuration space: pioneering virtual IT technology in 1999, revolutionizing large-packet distribution with LANDesk® Targeted Multicast™ technology and LANDesk® Peer Download™ technology in 2001, and delivering secure systems management over the Internet and hardware-independent network access control capabilities with LANDesk® Management Gateway and LANDesk® Trusted Access™ Technology in 2005.

In 2006, LANDesk added process management technologies to its product line and began integrating the systems, security and process management markets. LANDesk also extended into the consolidated service desk market with LANDesk® Service Desk, and was acquired by Avocent to operate as an independent division.

Today, LANDesk continues to lead the convergence of the systems, security, process and service management markets. And our executives, engineers and other professionals work tirelessly to deliver leading solutions to markets around the globe.