



10ZiG Manager Cloud Setup Guide

Welcome to the 10ZiG Manager Cloud Setup guide. This guide will help you install all of the components within the 10ZiG Management suite. Please take note of the following system requirements and software prerequisites for proper installation and functionality.

About:

The 10ZiG Manager Cloud Setup provides an easy and effective way to install all the tools for managing and controlling all of your 10ZiG Thin Client devices. The components include the 10ZiG Manager Server, 10ZiG Manager Console, 10ZiG Cloud Connector and the 10ZiG Web Console. The installation software is designed to be as minimal as possible but will require some user input to correctly configure these tools.

System Requirements

Below is a table of the minimum and recommended system requirements. When the Manager Server and the Web Console are used on the same machine, the CPU, system memory and drive space should be increased to prevent errors from occurring.

Note: Do Not Install the 10ZiG Manager or any of its components on an Active Directory (AD) Domain Controller.

10ZiG Manager Server		
	Minimum	Recommended
Operating System	Windows 8.1 64 Bit	Windows 8.1 64 bit or higher
CPU	Dual Core 1.5Ghz	Quad Core 2.5Ghz
System Memory	2GB	4GB
Drive Space	2GB	8GB
10ZiG Manager Console		
	Minimum	Recommended
Operating System	Windows 8.1 64 Bit	Windows 8.1 64 bit or higher
CPU	Dual Core 1.5Ghz	Quad Core 2.5Ghz
System Memory	2GB	4GB
Drive Space	2GB	8GB
10ZiG Cloud Connector		
	Minimum	Recommended
Operating System	Windows 8.1 64 Bit	Windows 8.1 64 bit or higher
CPU	Dual Core 1.5Ghz	Quad Core 2.5Ghz
System Memory	2GB	4GB
Drive Space	2GB	8GB
10ZiG Web Console		
	Minimum	Recommended
Operating System	Windows 8.1 64 Bit	Windows 8.1 64 bit or higher
IIS Server	IIS 7	IIS 8
Web Browser	Chrome 21, Firefox 28, IE10	Chrome 53, Firefox 49, IE11
CPU	Dual Core 1.5Ghz	Quad Core 2.5Ghz
System Memory	2GB	4GB
Drive Space	2GB	8GB

IIS Required Features

The Web Console installer will automatically enable the necessary Windows features. You will need to manually enable these features should the installer fail to do so. To manually enable these features you will need to navigate to the System Control Panel, Programs and Features and then click on “Turn Windows Features on or off”. Below is a list of all the required features for each IIS type.

IIS 7 Required Windows Features

- Internet Information Services
 - Web Management Tools
 - IIS Management Console
 - World Wide Web Services
 - Application Development Features
 - .NET Extensibility
 - ASP
 - ASP.NET
 - ISAPI Extensions
 - ISAPI Filters
 - Common HTTP Features
 - Default Document
 - Static Content
 - Security
 - Basic Authentication
 - Request Filtering

IIS 8 Required Windows Features

- .NET Framework 3.5 (includes .NET 2.0 and 3.0)
- .NET Framework 4.5 Advanced Services
 - ASP .NET 4.5
 - WCF Services
 - TCP Port Sharing
- Internet Information Services
 - Web Management Tools
 - IIS Management Console
 - World Wide Web Services
 - Application Development Features
 - .NET Extensibility 4.5
 - ASP.NET 4.5
 - ISAPI Extensions
 - ISAPI Filters
 - WebSocket Protocol
 - Common HTTP Features
 - Default Document
 - Static Content
 - Security
 - Basic Authentication
 - Request Filtering

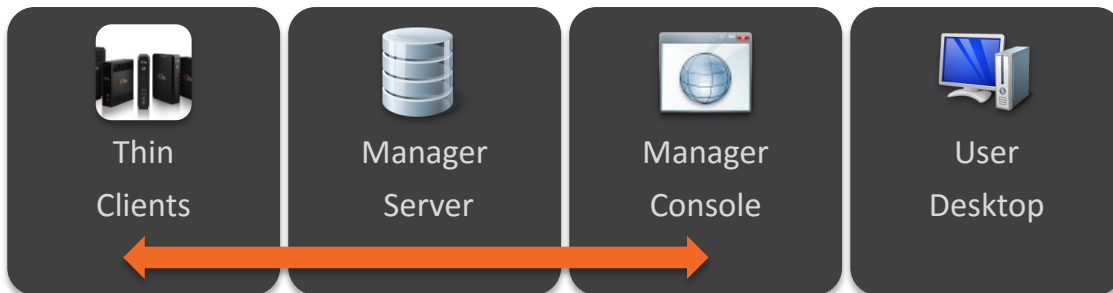
Contents

10ZiG Manager Cloud Setup Guide.....	1
About:	1
System Requirements	2
IIS Required Features	3
Contents	5
How it works:	6
Manager Server.....	6
Manager Console	6
Cloud Connector	6
Web Console	7
Web Console with the Cloud Connector.....	7
Installation	8
Component Selection.....	8
Manager Server.....	10
Cloud Connector	14
Web Console	18
Installation Complete.....	21
Appendix	22
Port Usage.....	22
Drive Space Consideration	22
System Memory Consideration:	22
DNS Service Location Record (SRV)	23

How it works:

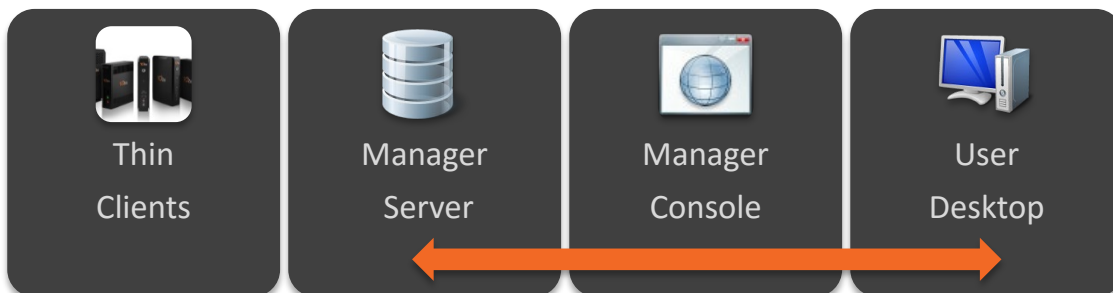
Manager Server

The 10ZiG Manager Server is the core component for managing your thin client devices. It is responsible for discovering, monitoring and communicating with the thin clients. The Manager Server stores vital information to provide client maintenance and configuration functionality.



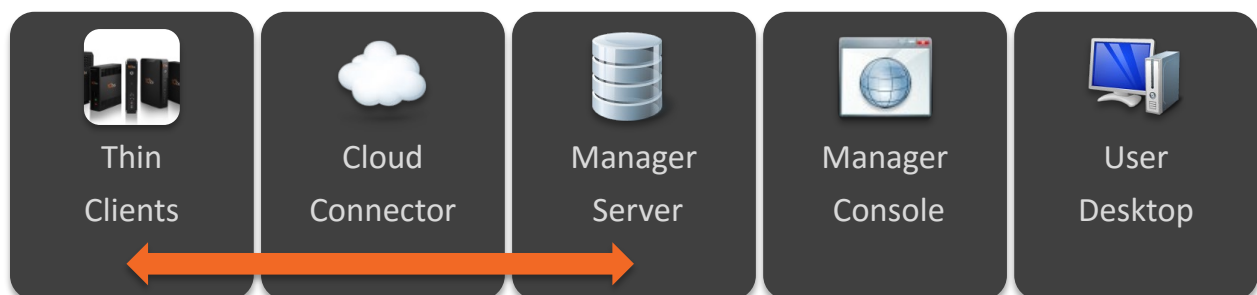
Manager Console

The 10ZiG Manager Console provides a user interface for the Manager Server allowing administrators to monitor thin client status and perform the various management, configuration and recovery tasks.



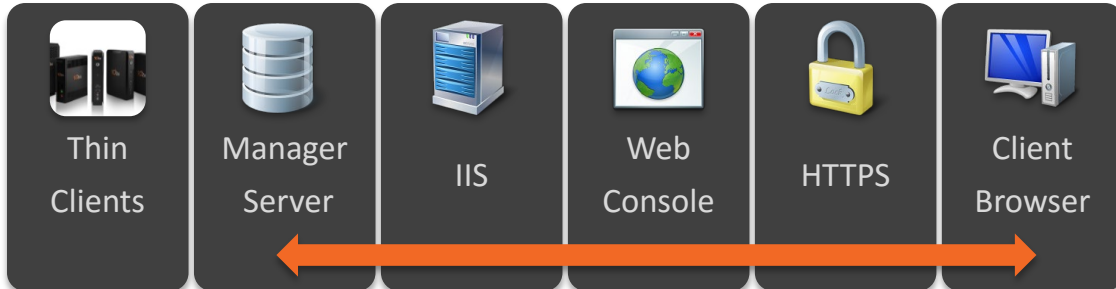
Cloud Connector

The 10ZiG Cloud Connector is a communications relay service which provides secure connectivity between thin clients and the manager server across the internet. It also is used as a proxy between the client browser and the Web Console.



Web Console

The 10ZiG Web Console provides an internet-based user interface to the Manager Server. Utilizing Microsoft Internet Information Services (IIS) on your server, our web application communicates directly to any specified 10ZiG Manager Server within your network.



Web Console with the Cloud Connector

In addition to handling cloud based thin clients, the Cloud Connector also routes Web Console and VNC network traffic to the users' browser. The user connects directly to the Cloud Connector when used in conjunction with the Web Console. The example below shows the Cloud Connector relationship with the Web Console.



Installation

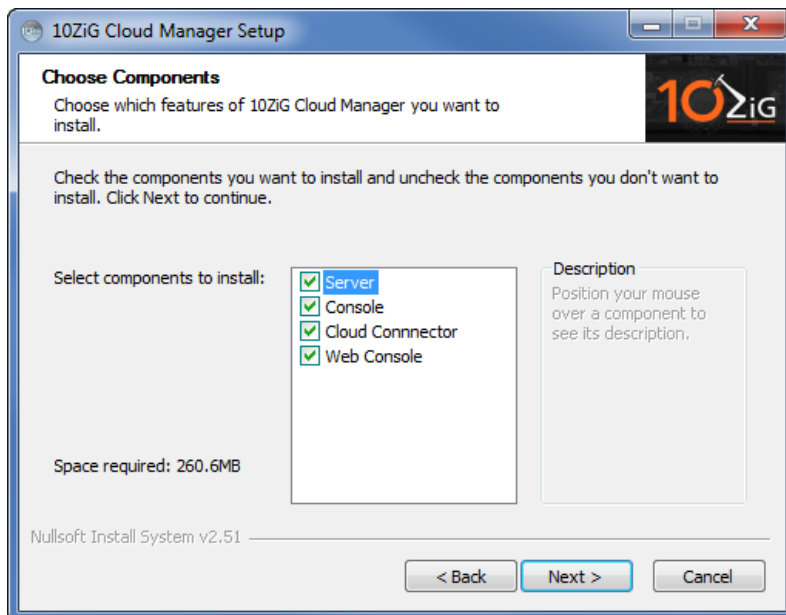
The 10ZiG Cloud Manager setup is a simple process. The installer allows you to choose all or individual components to install. For this guide, we will be installing all the components and walking you step by step through each process.

To start the Manager Cloud Setup, simply run the executable file MgrCloudSetup_v3.0.2.xx.exe.

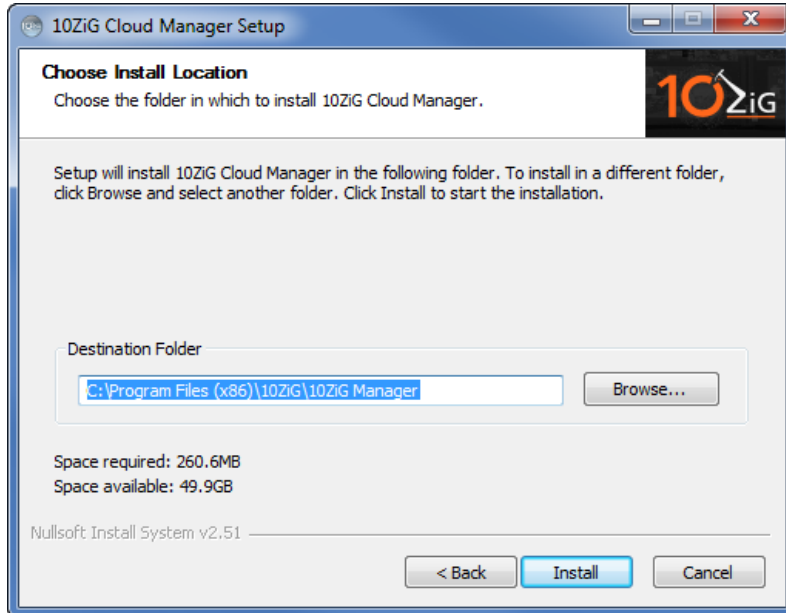


Component Selection

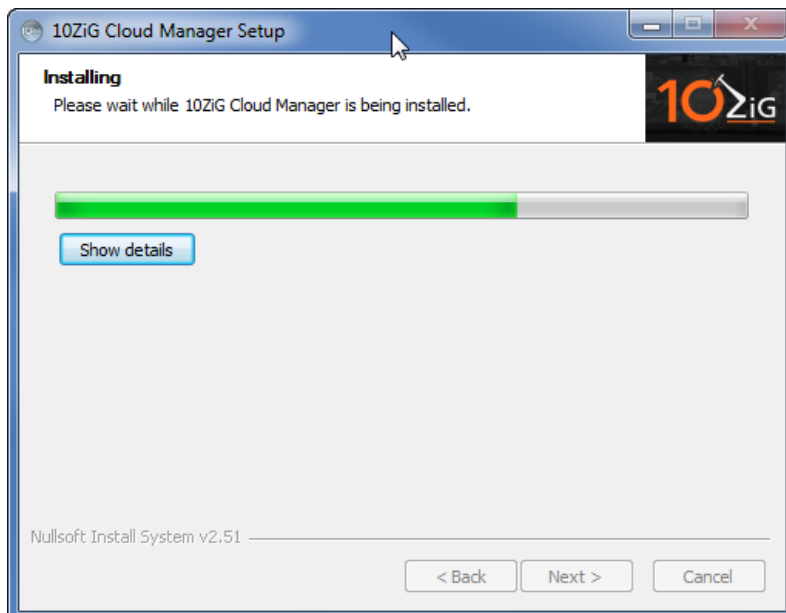
Clicking the next button will take you to the component selection screen. Here you can choose to install all or just the individual components you need.



The next screen will allow you to specify the installation path, but it is recommended to accept the default path.



You will see a progress bar indicating the selected components are being installed.



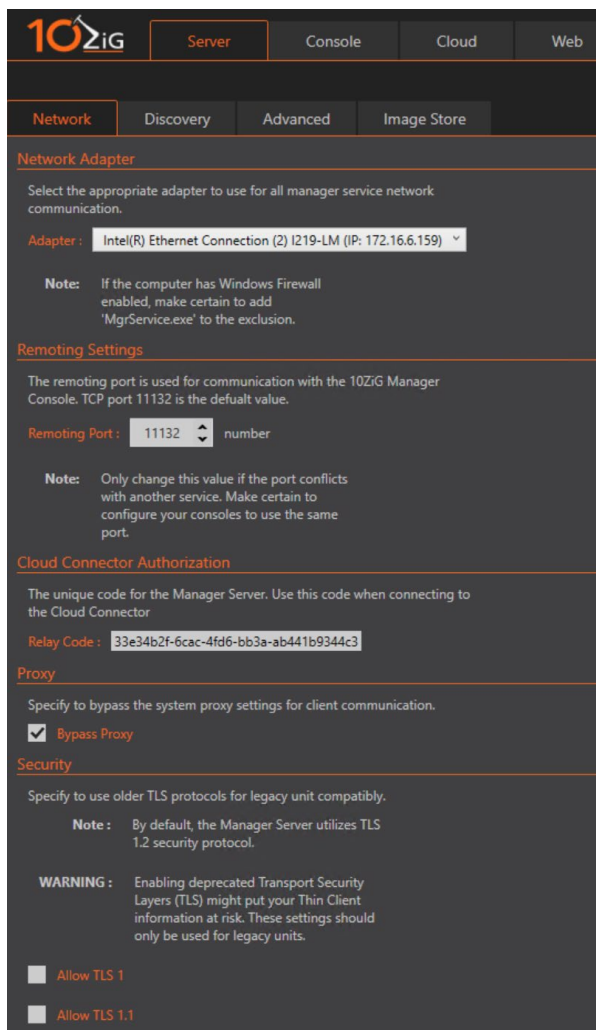
Manager Server

If the Manager Server was selected, you will be prompted to configure it. There are three tabs Network, Discovery and Advanced, and each tab has various settings. You can hover the mouse cursor over the setting to view the description.

Important: To prevent any installation errors, uninstall any previous versions of the Manager Server prior to installing the latest version.

Network

If the server has more than one network adapter, select the primary adapter to be used for manager communications. Change the remoting port only if necessary.



The screenshot displays the configuration interface for the 10ZiG Manager Server. The interface is dark-themed with orange accents. At the top, there are navigation tabs: 'Server' (selected), 'Console', 'Cloud', and 'Web'. Below these, there are sub-tabs: 'Network' (selected), 'Discovery', 'Advanced', and 'Image Store'. The main content area is divided into several sections:

- Network Adapter:** A section with the instruction "Select the appropriate adapter to use for all manager service network communication." Below this is a dropdown menu for "Adapter" showing "Intel(R) Ethernet Connection (2) I219-LM (IP: 172.16.6.159)". A note below states: "Note: If the computer has Windows Firewall enabled, make certain to add 'MgrService.exe' to the exclusion."
- Remoting Settings:** A section with the instruction "The remoting port is used for communication with the 10ZiG Manager Console. TCP port 11132 is the default value." Below this is a "Remoting Port" field with a spinner set to "11132" and the label "number". A note below states: "Note: Only change this value if the port conflicts with another service. Make certain to configure your consoles to use the same port."
- Cloud Connector Authorization:** A section with the instruction "The unique code for the Manager Server. Use this code when connecting to the Cloud Connector." Below this is a "Relay Code" field containing the value "33e34b2f-6cac-4fd6-bb3a-ab441b9344c3".
- Proxy:** A section with the instruction "Specify to bypass the system proxy settings for client communication." Below this is a checkbox labeled "Bypass Proxy" which is checked.
- Security:** A section with the instruction "Specify to use older TLS protocols for legacy unit compatibly." Below this is a note: "Note: By default, the Manager Server utilizes TLS 1.2 security protocol." A warning follows: "WARNING: Enabling deprecated Transport Security Layers (TLS) might put your Thin Client information at risk. These settings should only be used for legacy units." At the bottom of this section are two checkboxes: "Allow TLS 1" (unchecked) and "Allow TLS 1.1" (unchecked).

Discovery

This tab allows you adjust how the Manager Server polls and discovers new thin clients.

The screenshot shows the configuration interface for the Discovery tab. It is divided into several sections:

- Discovery Options:** Includes a "Discovery Timeout" spinner set to 30 seconds and a checked checkbox for "Use Broadcast Discovery".
- Multicast:** Includes a disabled checkbox for "Use Ping Discovery" and a "Ping Timeout" spinner set to 500 milliseconds. A note explains that enabling ping discovery optimizes thin client discovery times.
- Automatic Discovery:** Includes a checked checkbox for "Enable automatic discovery" and a "Discovery Interval" spinner set to 250 seconds.

Other visible options include "Use TCP Discovery (Linux and WinCE only)" which is checked, and "Use Broadcast Discovery" which is checked. The interface also shows navigation tabs for "Server", "Console", "Cloud", and "Web", and sub-tabs for "Network", "Discovery", "Advanced", and "Image Store".

The Manager Server can consume a higher amount of resources when automatically discovering a large number of thin clients or connecting via minimal bandwidth. To reduce this, the “Discovery Interval” can be increased to 300 seconds (5 minutes) or greater. Additionally, a DNS Service Location (SRV) record can be created within your DNS system that will direct thin clients to the Manager server so they can “check-in” when they come online and announce when they are going offline. If the account you are using to install the 10ZiG Manager has DNS administrator privileges within a Microsoft DNS infrastructure, the “Server Settings” dialog will ask if you wish to automatically create this record when you click “OK”. If you are not a DNS administrator or need to manually create the record, please see the [appendix section](#) detailing the procedure.

Advanced

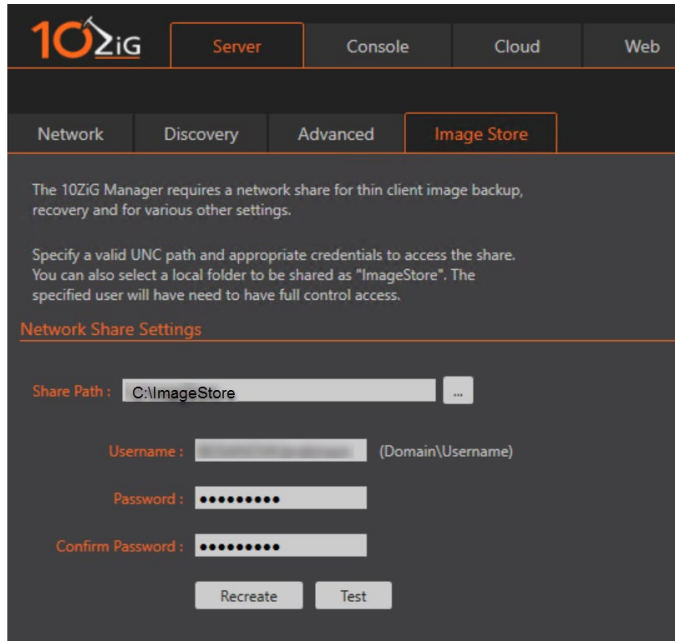
This tab allows you to configure the advanced settings for the Manager Server. These settings should be left as default unless there is a specific need or directed otherwise by technical support.

The screenshot shows the 'Advanced' settings page for the 10ZiG Manager Server. The page is divided into several sections:

- Group Options:** A checkbox for 'Hide Grouped Clients' is currently unchecked.
- Discovery Options:** A 'Discovery Timeout' of 60 seconds is set.
- Wake-On-LAN:** A 'Port' of 9 is set.
- Boot Server:**
 - 'Enable Boot Server' is checked.
 - 'TFTP Host' is set to 'localhost'.
 - 'Enable TFTP Server' is checked.
 - 'Root Path' is set to 'C:\Program Files (x86)\10ZiG\10ZiG Manager\1'.
 - 'Timeout' is set to 5 seconds.
 - 'MTU' is set to 0.
 - A warning message states: 'WARNING : Setting this value higher than the effective path MTU will cause problems with PXE booting. Leave this field blank to indicate the TFTP server should use the system default.'
 - 'Allow file upload' is unchecked.
 - 'Allow overwriting existing files' is unchecked.
- Logging:** 'Logging Level' is set to 'Debug'.
- Firmware Timeout:** This section is partially visible at the bottom.

Manager Network Share

You will be prompted to choose a network share path for the Manager Server. Enter in the desired share or UNC path and user credentials.



The screenshot shows the 10ZiG Manager interface with the 'Server' tab selected. Under the 'Image Store' sub-tab, there is a section titled 'Network Share Settings'. The interface includes the following fields and buttons:

- Share Path:** A text input field containing 'C:\ImageStore' and a browse button (three dots).
- Username:** A text input field with a placeholder '(Domain\Username)' to its right.
- Password:** A password input field with masked characters (dots).
- Confirm Password:** A second password input field with masked characters (dots).
- Buttons:** 'Recreate' and 'Test' buttons located at the bottom of the settings section.

Cloud Connector

If the Cloud Connector component has been selected, you will be prompted to configure additional settings on how it will communicate.

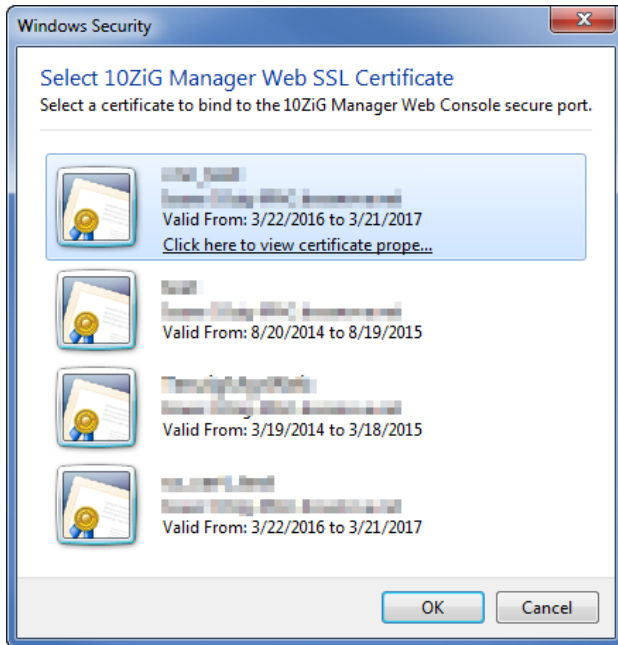
Note: It is recommended to use the default SSL\TLS port of 443 if available.

Select a port number and a SSL certificate for the connector. You can have the installer generate a Self-Signed Certificate, import or select a previously installed certificate.

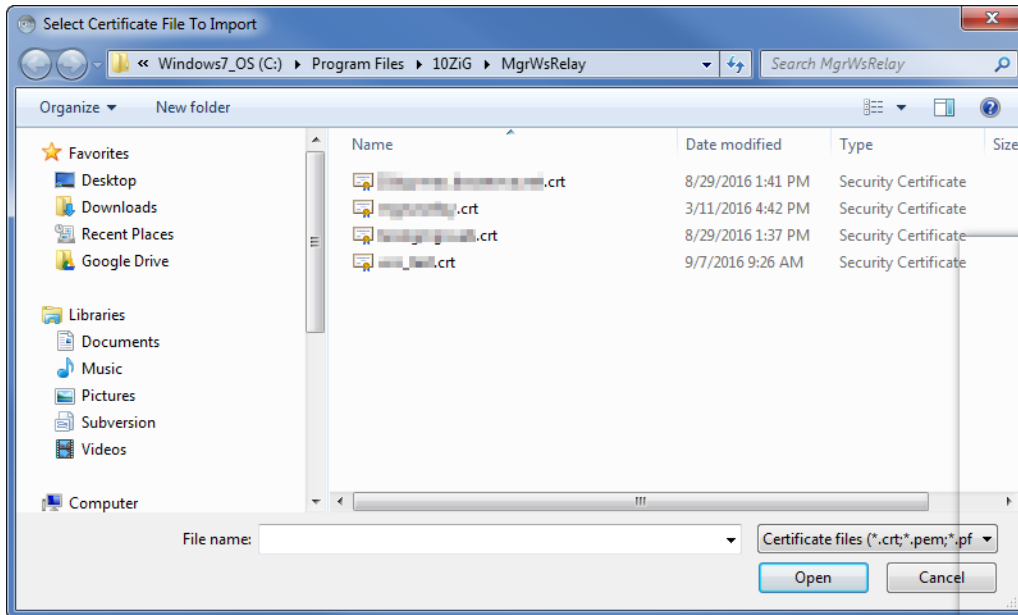


Important: When hosting the Web Console on the same computer, ensure the Web Console port is different from the one configured here.

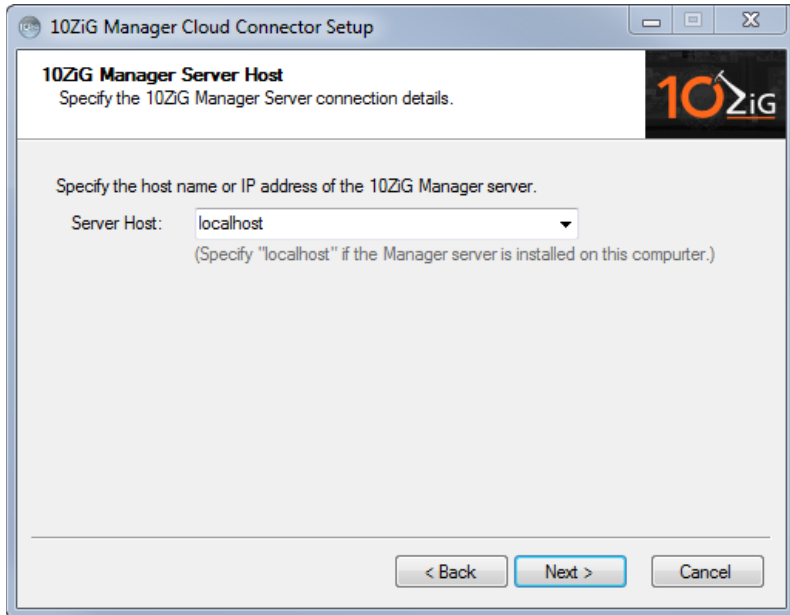
Selecting an installed certificate



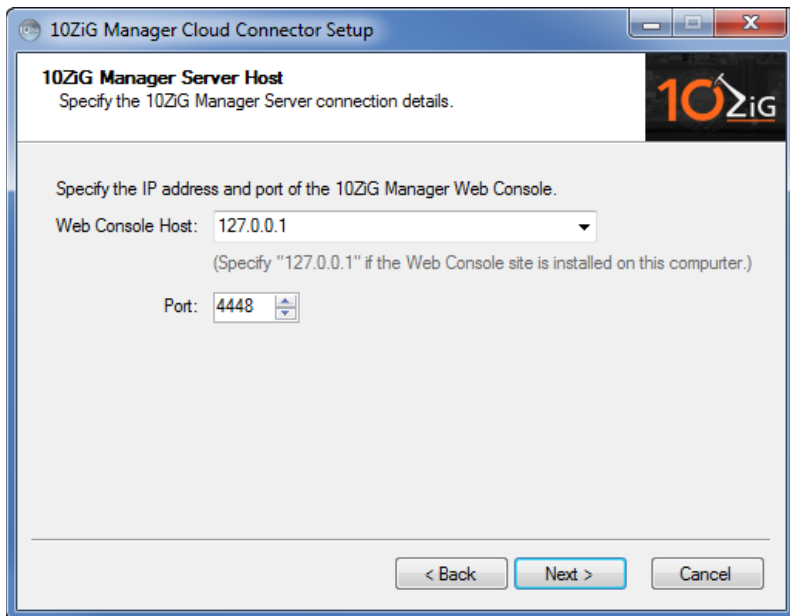
Importing a SSL Certificate



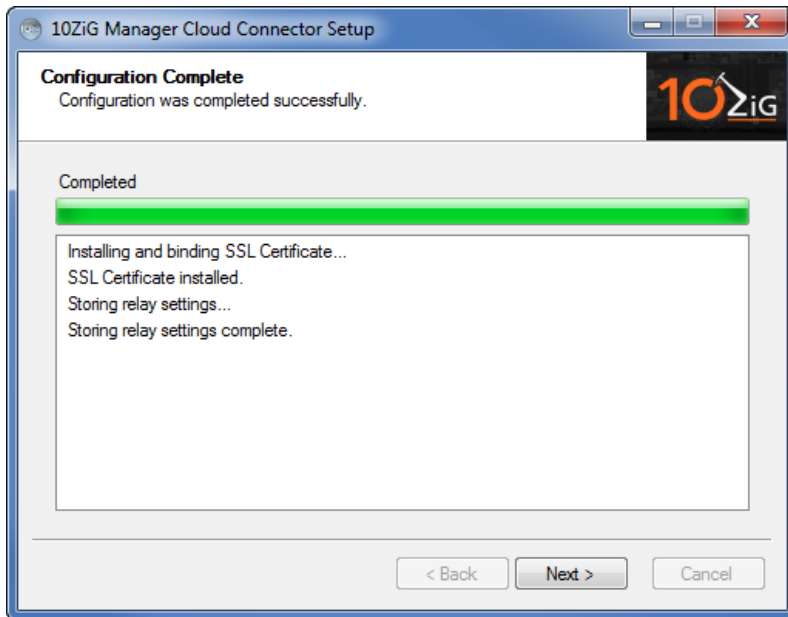
Enter in the address of the Manager Server (Standalone Installer Only)



Enter in the address of the Web Console and the port (Standalone Installer Only)



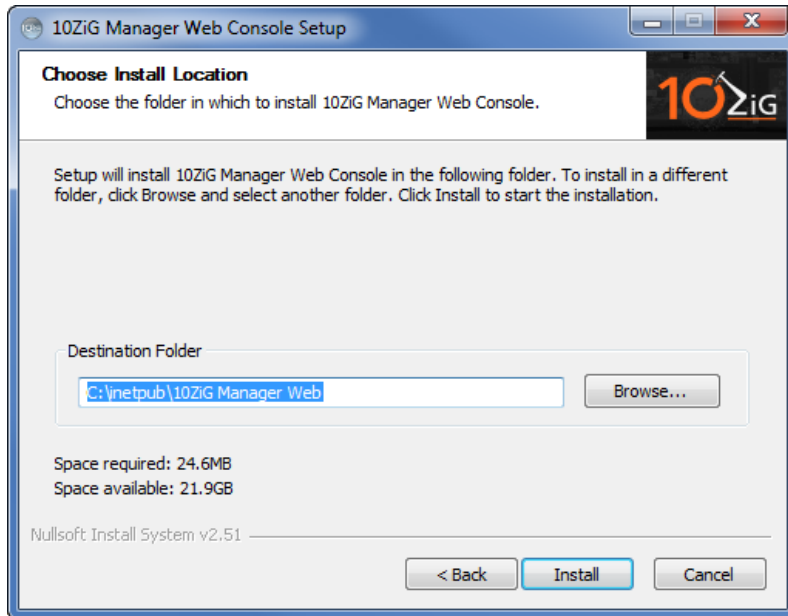
When the setup for the Cloud Connector has completed, the dialog will appear as follows.



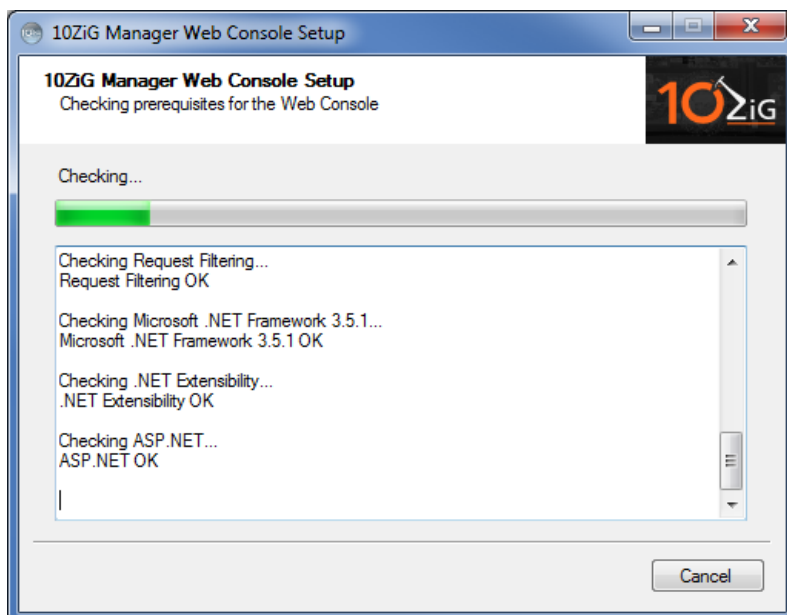
Web Console

If the Web Console component was selected, you will be prompted to select the installation path, port number and SSL certificate. If you are installing the Web Console on the same computer as the Cloud Connector, you must choose a different port number than the Cloud Connector.

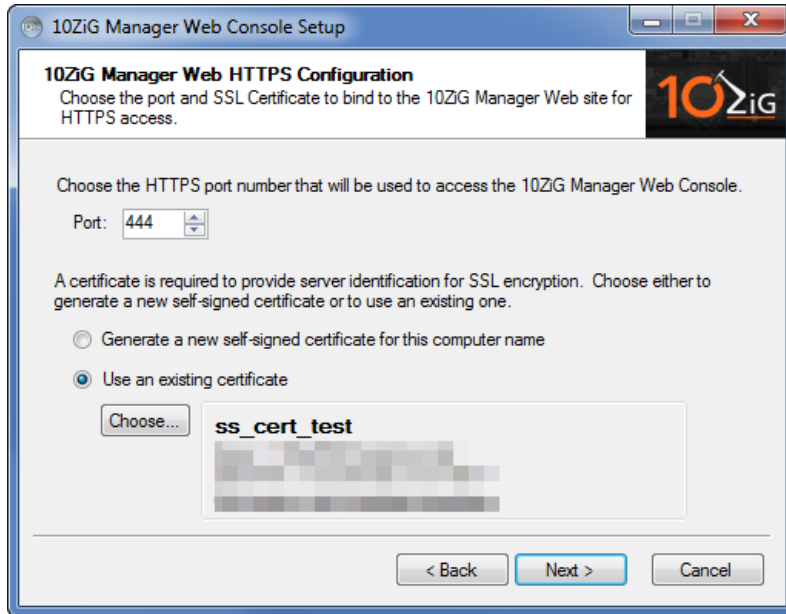
Specify the installation path, but it is recommended that you accept the default path.



After all of the files have been extracted, the installer will check if the necessary Windows features are present. If there are missing features you will be prompted with a dialog window to automatically install them. Once all the required features are installed, the installation will continue.



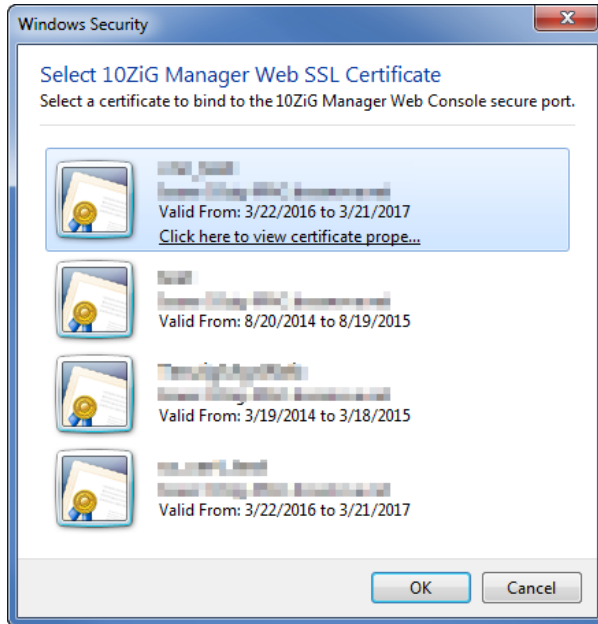
The installer will try to use the port 443 and detect if it is use. If it is in use, the installer will select the next available port number. (Standalone Installer Only)



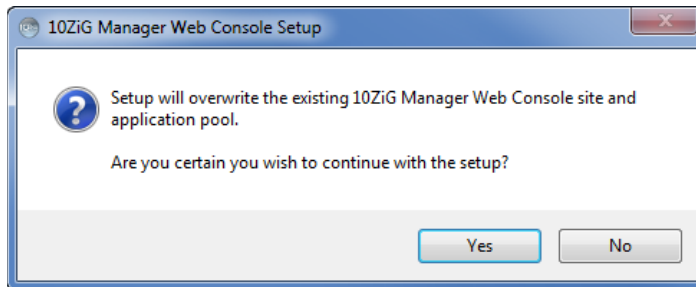
Note: Certain programs like Skype and other messaging programs will hold on to port number 443 by default. Due to the nature of these programs, the installer may not be able to determine if the port is in use! Either set the conflicting program's port to another value or select a different port value within the installer.

Important: When hosting the Cloud Connector on the same computer, ensure the Web Console port is different from the one configured here.

Select your SSL certificate by clicking on the 'choose' button or have the installer generate a Self-Signed Certificate which is stored in the trusted root of the operating system. (Standalone Installer Only)

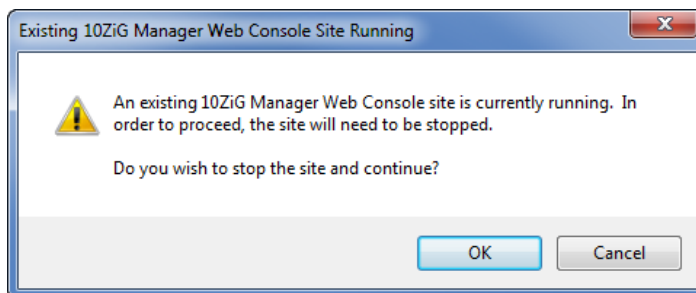


If you are upgrading or there is already an existing Web Console on the host machine you will be prompted to override the existing settings.



If there is an existing Web Console site on the machine and it is currently running, you will be asked to stop it to continue. This is important as it will need to change the settings and restart it.

Note: This will logoff any currently connected users



Installation Complete

All done! Click finish to close the installer. If any of the newly enabled features requires a reboot, you will be prompted to do so.

Note: It is important to complete the installation process and reboot (if required)



Appendix

When using the 10ZiG Manager Server, 10ZiG Cloud Connector and the 10ZiG Web Console on the same machine, there are several things you will need to be aware of before you start using them.

Port Usage

- When specifying the port numbers during the setup, ensure that Cloud Connector and the Web Console are using different port numbers. Example: Cloud Connector on port 443 and Web Console on port 444.
- The Web Console port can be changed through the Web Console Settings tool that is installed with the Web Console. It is recommended to utilize this settings tool as it will also set the necessary values for the Cloud Connector.

Drive Space Consideration

- The Manager Server stores all installed firmware update packages in the network share that was entered in during the installation. This can cause the folder to become very large so it is recommended to remove obsolete firmware version when possible. It is recommended in end user environment that a couple of firmware version are kept on hand.
- When the Manager Server discovers thin clients for the first time, their configuration is retrieved and stored. This means that the size of the configuration repository folder within the network share will grow based upon the amount of thin clients that is found.

System Memory Consideration:

- The Manager Server and Web Console utilizes multithreading tasks and operations. There should be sufficient system memory allocated to the operating system when using these managing programs. See the system requirements table below for more information about this requirement.

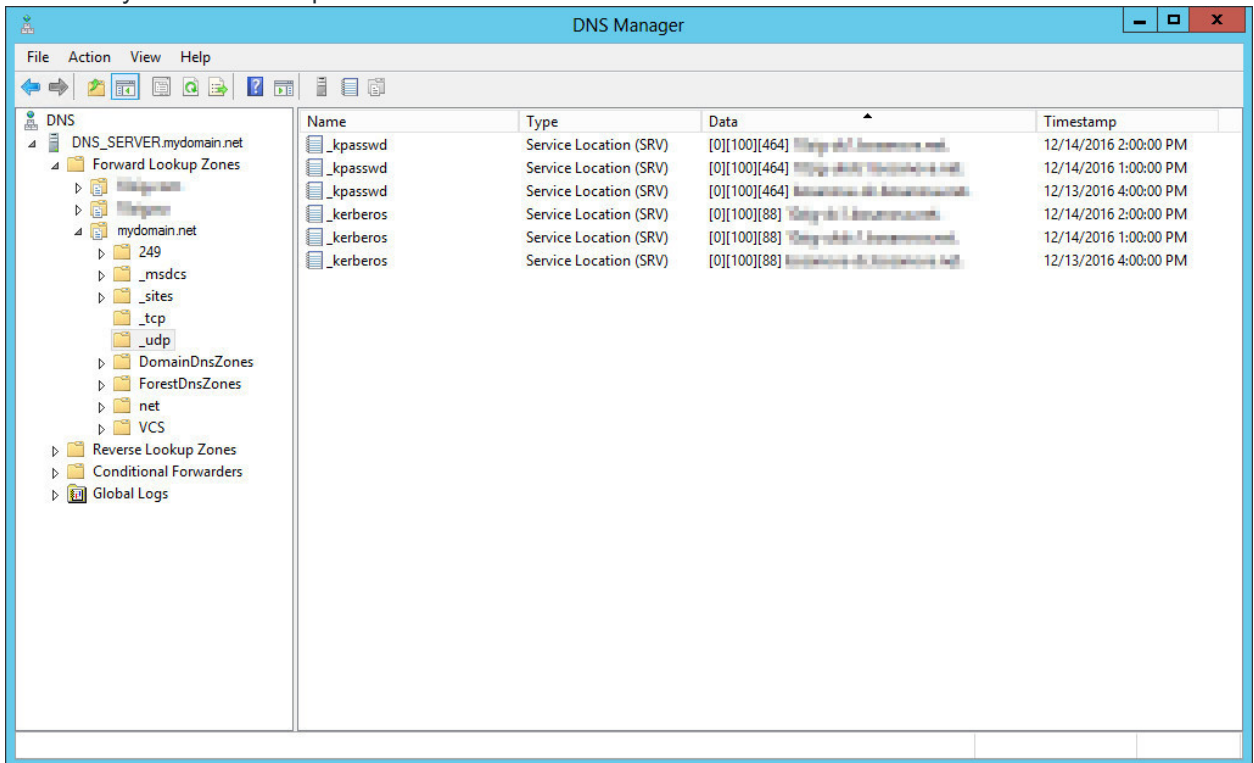
DNS Service Location Record (SRV)

A DNS Service Location record can be created to provide the host name of the computer and port on which the 10ZiG Manager server is located allowing thin clients to “check-in” when they come online or notify when they go offline. This mitigates the need for the Manager server to poll IP addresses to discover new clients or refresh the status of existing clients. The following instructions detail how to manually create an SRV record on a Microsoft DNS server.

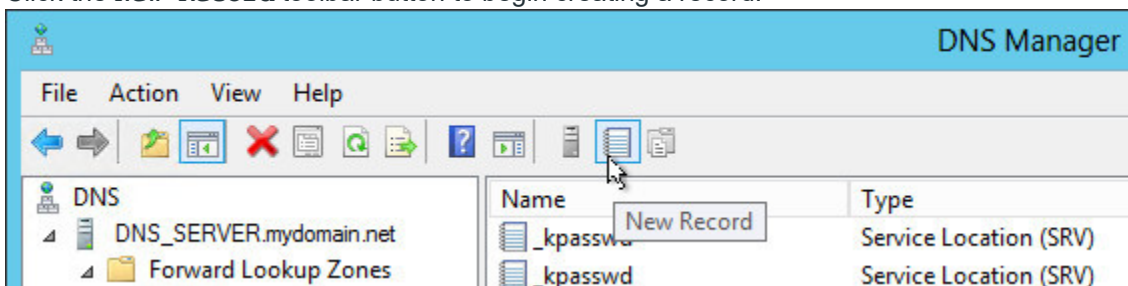
UDP SRV Record

The UDP record is used by thin clients not connected via the Cloud Connector, usually on the same local network. The following steps detail how to create this record type.

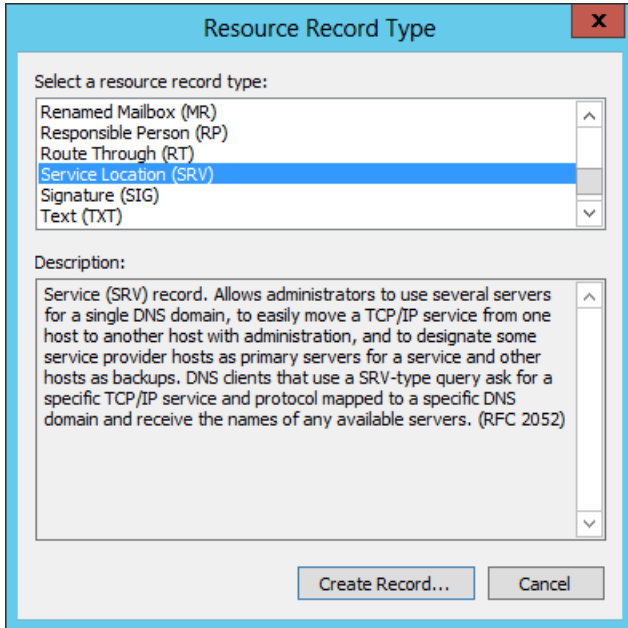
1. Launch the Microsoft DNS Manager on your DNS server from the **Administrative Tools** Start menu folder or from the **Server Manager** console.
2. Expand the DNS domain tree to navigate to the `_udp` subdomain in the **Forward Lookup Zones** of your domain as pictured below.



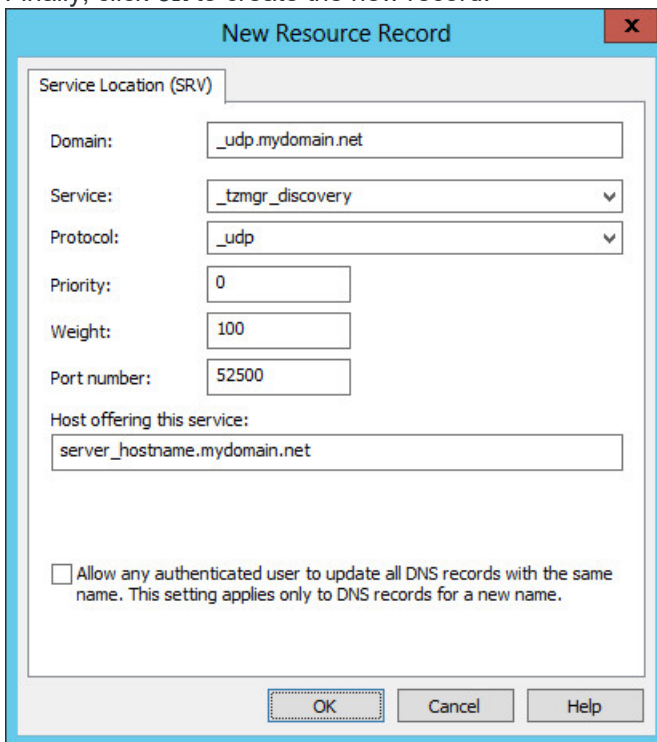
3. Click the **New Record** toolbar button to begin creating a record.



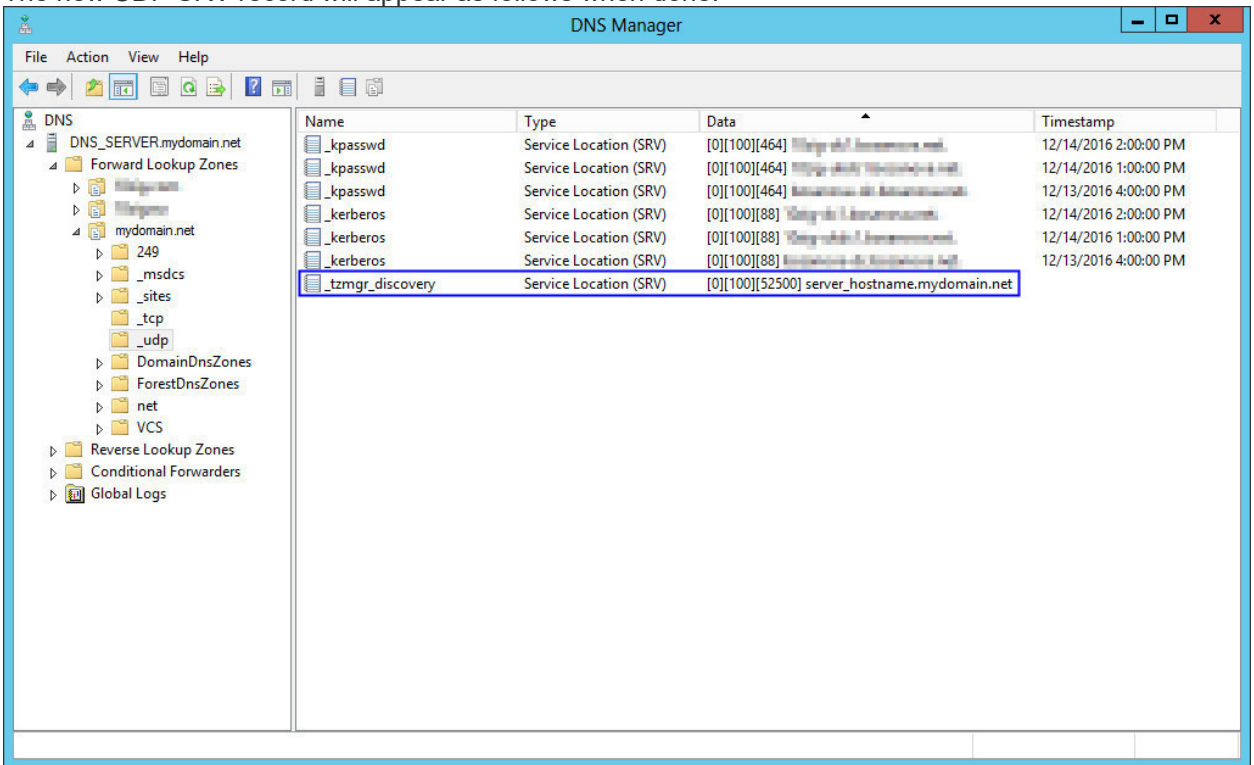
- The **Resource Record Type** dialog window will appear. Scroll down list to find and select **Service Location (SRV)**, then click the **Create Record...** button.



- Specify the record details as pictured below.
 Service: **_tzmgr_discovery**
 Protocol: **_udp**
 Port number: **52500**
 Host offering this service: Enter the host name of the 10ZiG Manager computer.
 Finally, click **OK** to create the new record.



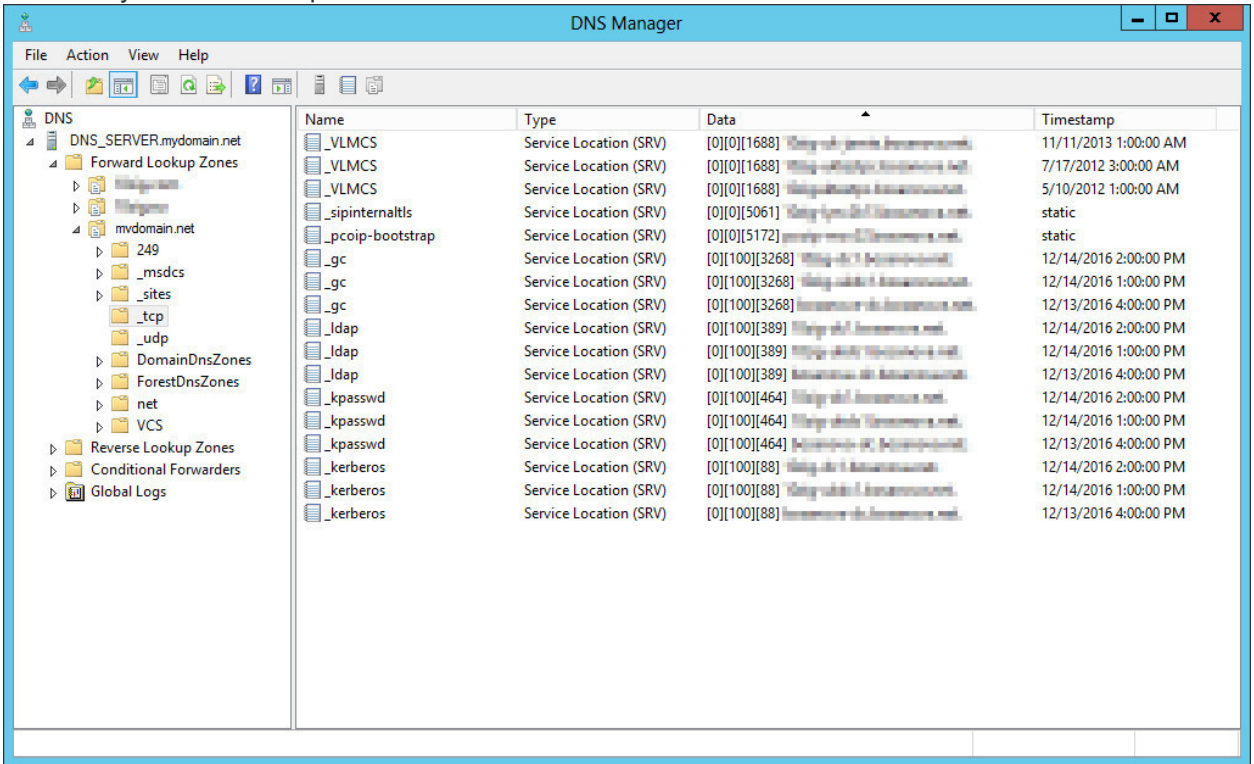
6. The new UDP SRV record will appear as follows when done.



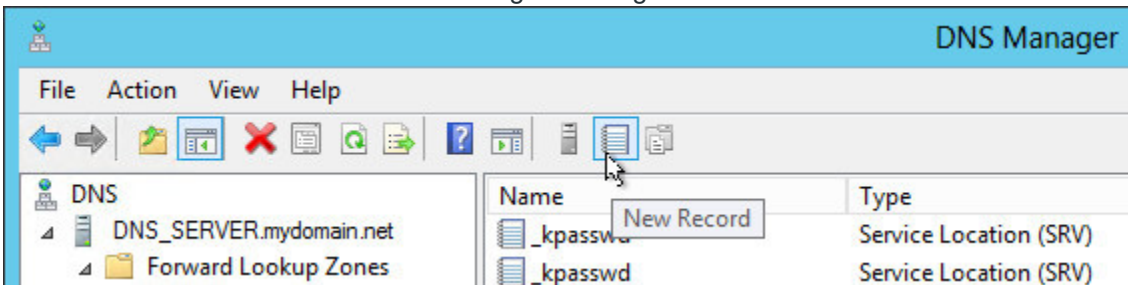
TCP SRV Record

A TCP SRV record can also be created in your DNS infrastructure to provide Cloud-Agent-enabled thin clients location information of the Manager server. The process is similar to creating the UDP record except for a couple of key differences. The procedure is detailed as follows.

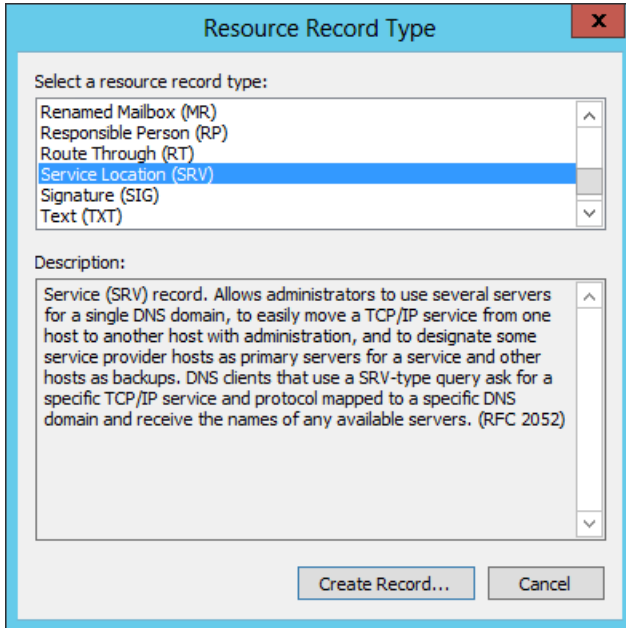
1. Launch the Microsoft DNS Manager on your DNS server from the **Administrative Tools** Start menu folder or from the **Server Manager** console.
2. Expand the DNS domain tree to navigate to the **_tcp** subdomain in the **Forward Lookup Zones** of your domain as pictured below.



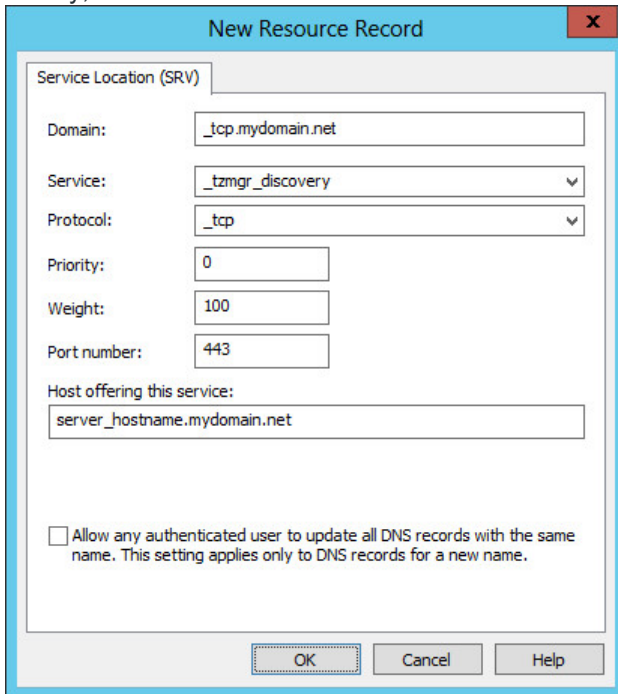
3. Click the **New Record** toolbar button to begin creating a record.



- The **Resource Record Type** dialog window will appear. Scroll down list to find and select **Service Location (SRV)**, then click the **Create Record...** button.



- Specify the record details as pictured below.
 Service: **_tzmgr_discovery**
 Protocol: **_tcp**
 Port number: Specify the port of the Cloud Connector.
 Host offering this service: Enter the host name of the computer where the Cloud Connector has been installed.
 Finally, click **OK** to create the new record.



6. The new TCP SRV record will appear as follows when done.

