10ZiG MANAGER SECURE CONNECTOR

INSTALLATION GUIDE FOR REMOTE CLIENTS

Version: 1.0

Document Reference: TZMCC0001

Date: September 2020

Great care has been taken to ensure that the information contained in this document is accurate and complete. Should any errors or omissions be discovered, or should any user wish to suggest improving this document, they are invited to send the relevant details to:

10ZiG Technology

North America (Rest of the world): info@10zig.com

EMEA: info@10zig.eu

DISCLAIMER

10ZiG Technology reserves the right to revise or make changes or improvements to the products described in this document or to the document itself at any time without obligation to notify any person of such revision or improvements.

DOCUMENT VERSION CONTROL AND REVIEW HISTORY

Document Version Control

Version	Created by	Date	Authorised & Checked
1.0	S.Hayles	18/09/2020	K.Greenway

REVIEW HISTORY

September 2020

Creation of this document

CONTENTS

LIST OF FIGURES

OVERVIEW

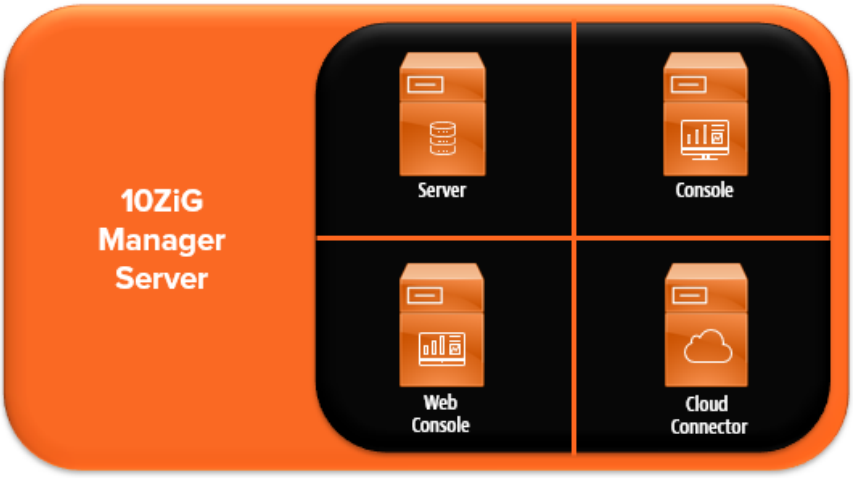


FIGURE 1 COMPONENTS OF THE 10ZIG MANAGER APPLICATION SUITE

The 10ZiG Secure Connector is a component of the 10ZiG Manager application suite, which can be included at installation and used to tunnel the various management protocols between manager and client over a secure HTTPs connection.

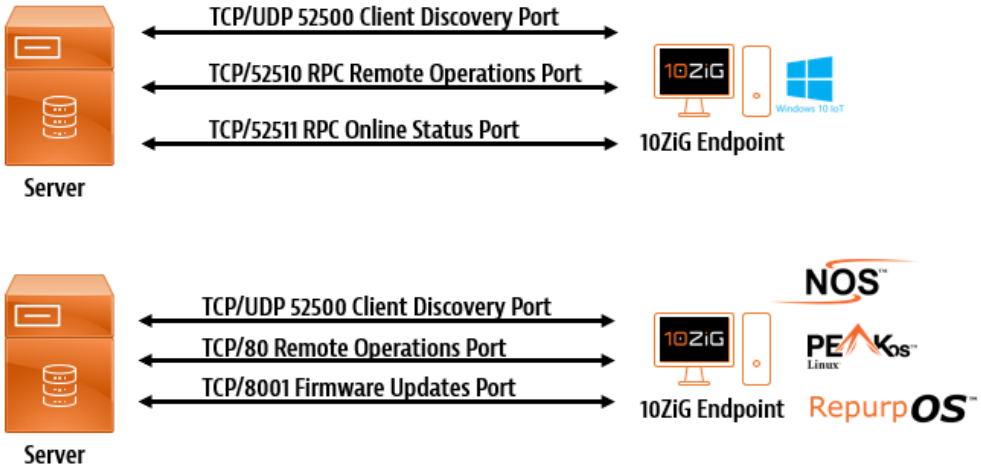


FIGURE 2 SOME OF THE VARIOUS MANAGEMENT PROTOCOLS USED BETWEEN THE MANAGER AND CLIENT OPERATING SYSTEMS.

The Secure Connector is required to be installed when looking to deploy remotely located 10ZiG Thin Clients or devices running the RepurpOS operating system, and where you want them to be managed centrally from either a head office location, Data Center, or Secure environment such as Azure or AWS where the 10ZiG Manager is deployed.

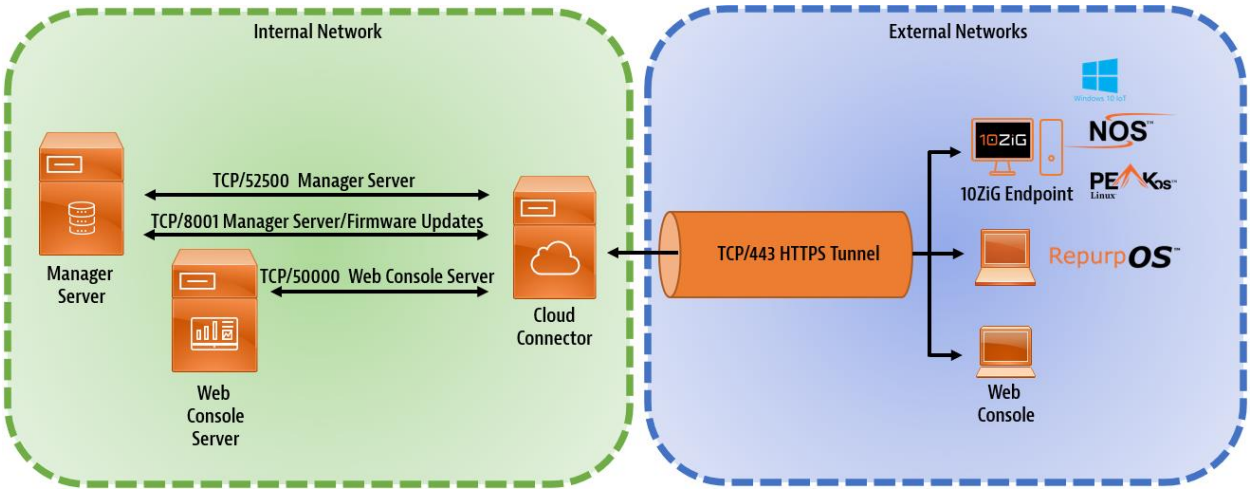


FIGURE 3 MANAGEMENT PROTOCOLS COMMUNICATION CHANNELS WITH SECURE CONNECTOR IN USE.

The Secure Connector could also be deployed for enterprise networks where VLANS or multiple WAN locations are used and networked through security appliances that could potentially block the standard management protocol communication channels being used. Dependent on how these network security appliances are configured, tunneling the traffic through a HTTPs communication channel can help overcome these blockages.

This 10ZiG Manager Secure Connector - Installation Guide for Remote Clients will look at two common deployment scenarios. Other deployment configurations are possible but not covered here.

Deployment Scenario 1 – Internal 10ZiG Manager Server Accessible Externally

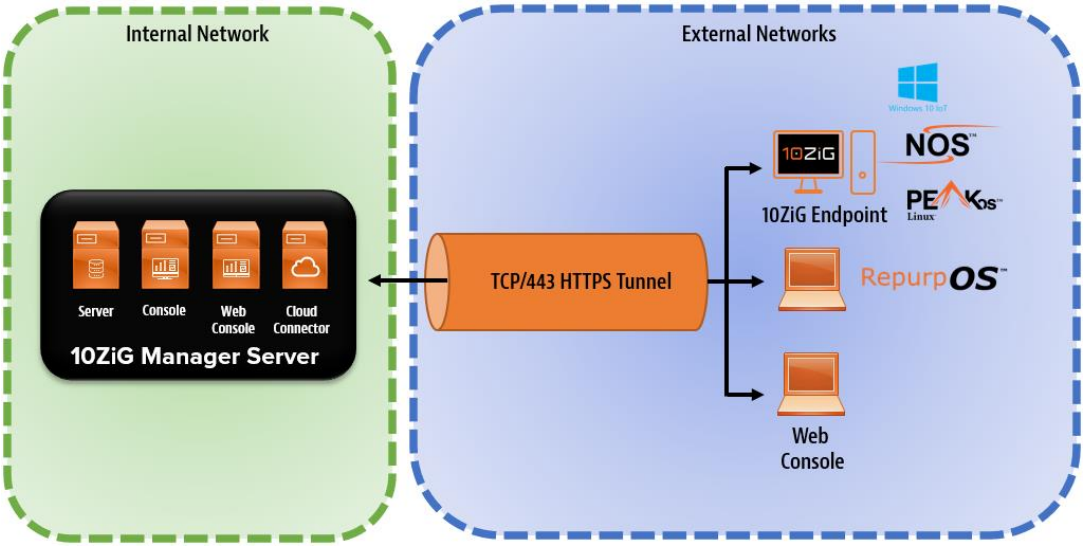


FIGURE 4 INTERNAL 10ZIG MANAGER SERVER ACCESSIBLE EXTERNALLY

Deployment Scenario 2 – Internal 10ZiG Manager Server and DMZ based Secure Connector Accessible Externally

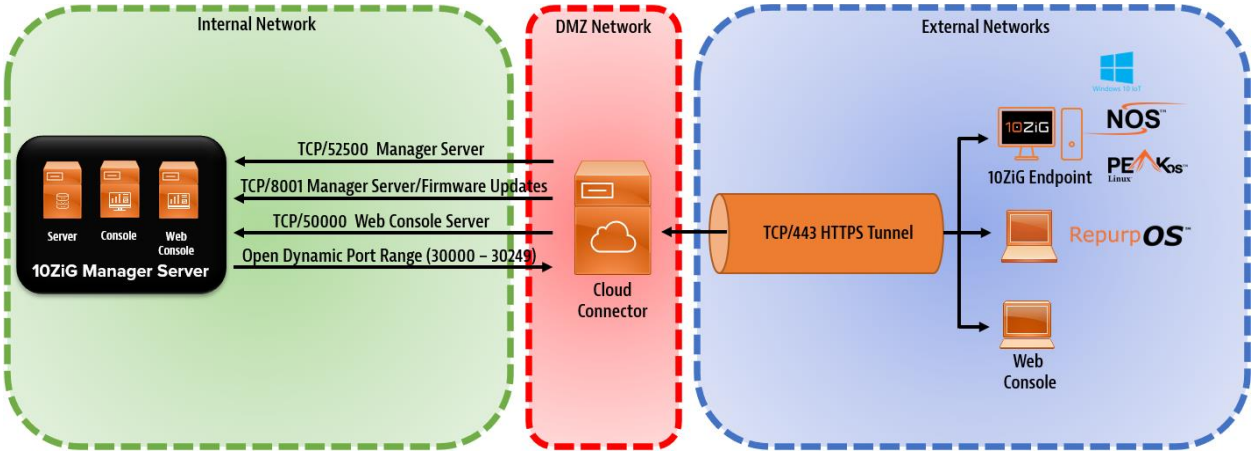


FIGURE 5 INTERNAL 10ZIG MANAGER SERVER AND DMZ BASED SECURE CONNECTOR ACCESSIBLE EXTERNALLY

DEPLOYMENT SCENARIO 1 CONFIGURATION GUIDE

In this deployment, the 10ZiG Manager is installed on a single internal server. The Edge Router/Firewall connected to the Internet from where the externally deployed 10ZiG Clients will connect from, is configured to port forward TCP/443 HTTPs traffic inbound to the 10ZiG Manager Server. No outbound rules are required.

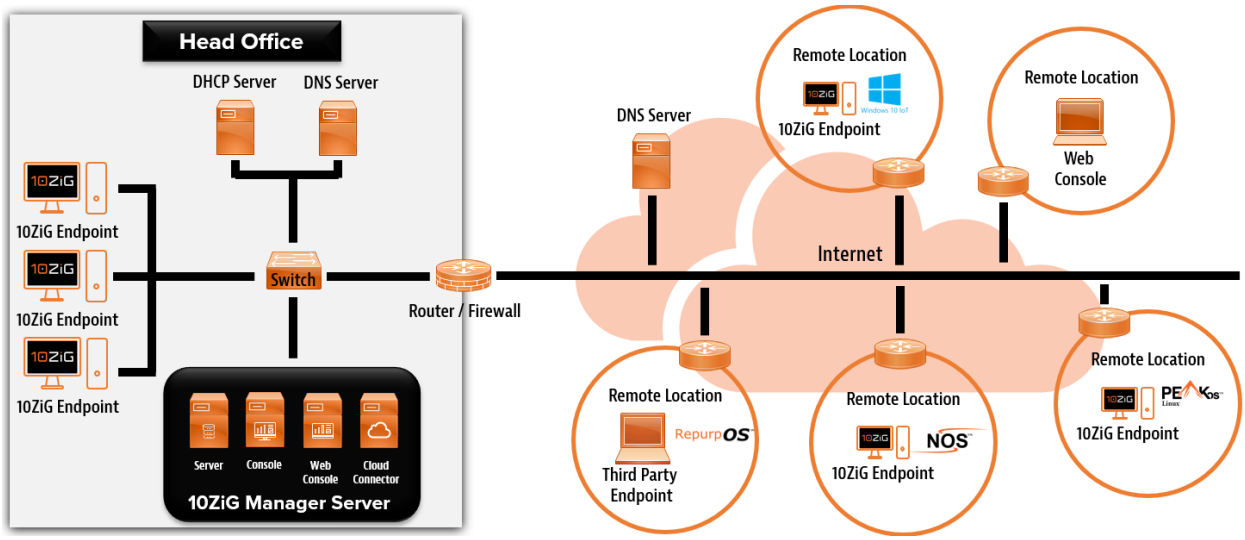
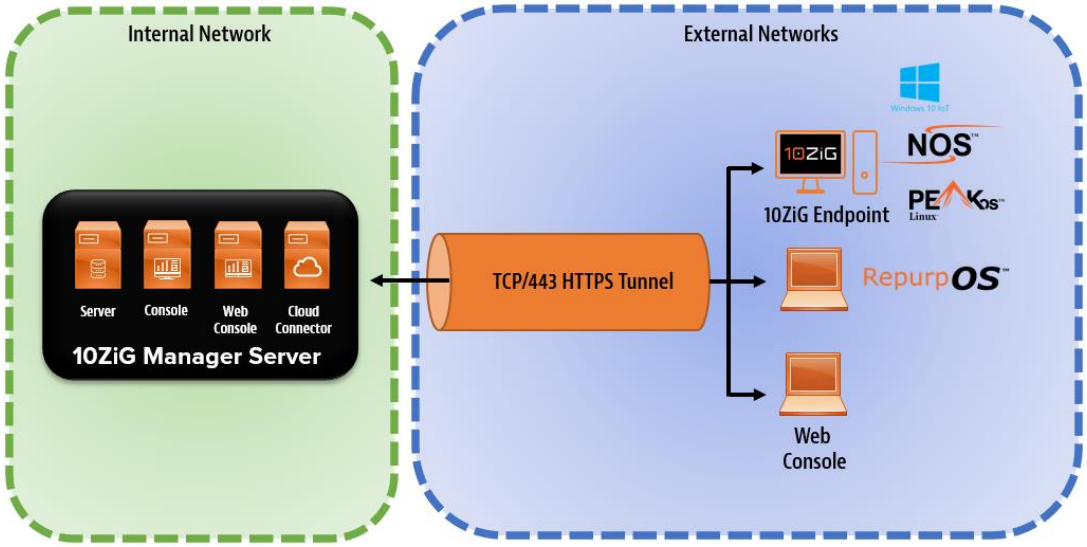


FIGURE 6 DEPLOYMENT SCENARIO 1 EXAMPLE NETWORK DIAGRAM



MANAGER INSTALLATION AND CONFIGURATION

NOTE: If you are using 10ZiG Windows 10 IoT devices with the XTC Agent 2.1.0.0 or newer installed. You will also need to be running the 10ZiG Manager 3.0.5.0 or newer to manage these devices remotely.

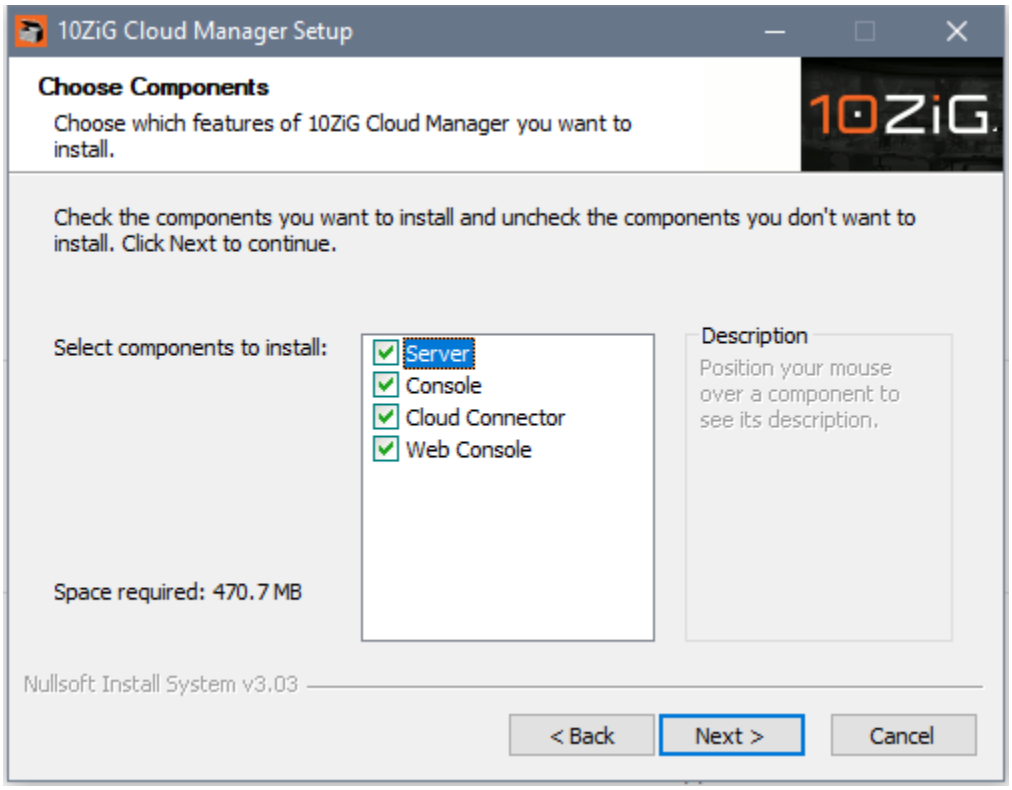
If the 10ZiG Manager is not installed or a supported version, please download the latest version from the 10ZiG website at

https://www.10zig.com/manager

A password is required for installation, please contact 10ZiG support to obtain the password. For 10ZiG Technical Support contact details please refer to the section on TROUBLESHOOTING AND SUPPORT

MANAGER INSTALLATION

1. Run the 10ZiG Manager application suite installer to begin the 10ZiG Secure Manager Setup.
2. When the **Choose Components** screen is displayed, select components **Server**, **Console**, **Secure Connector**, **Web Console** and press **Next** to continue the setup procedure.

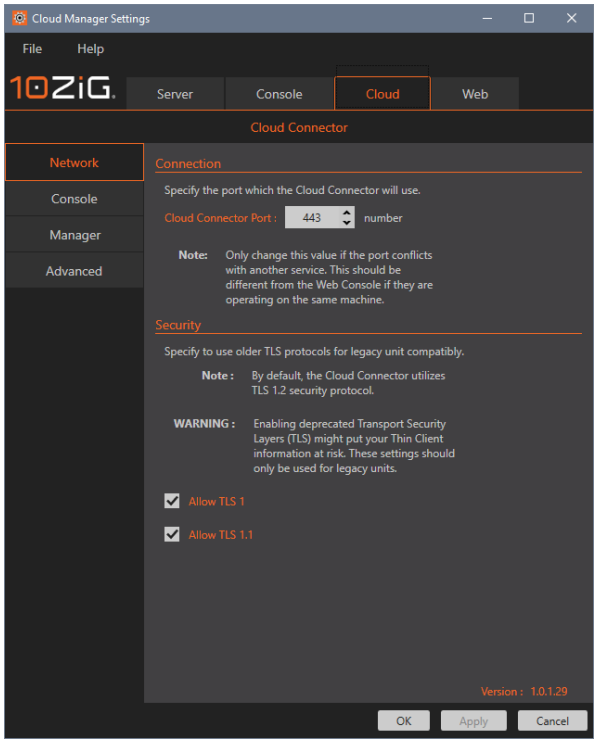


3. Click through the rest of the 10ZiG Secure Manager Setup following the prompts to finish the installation.

MANAGER CONFIGURATION

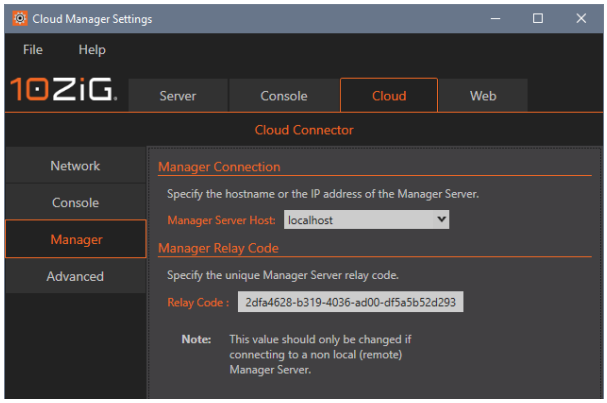
1. Run the **10ZiG Secure Manager Settings** application from **Start > 10ZiG Manager > 10ZiG Cloud Manager Settings**.

2. Switch to the **Cloud Connector** configuration settings. On the **Network** screen the **Cloud Connector Port** is set to **443** by default.



3. Switch to the **Console** configuration tab. The default configuration settings are shown below. If you want to block the relaying of traffic to the Web Console Server to prevent external access to the web-based management tool then enable the option **Disable External Web Console Relaying** to prevent this.

4. Switch to the **Manager** configuration tab. The default configuration settings are shown below.



5. Switch to the **Advanced** configuration tab. The default configuration settings are shown below. For troubleshooting issues, the **Logging Level** can be increased from the default **info** to **debug** and the output viewed using the **10ZiG Syslog Viewer** from **Start > 10ZiG Manager > 10ZiG Syslog**.

6. When you have checked these settings and happy with the configuration press the **OK** button to close the **10ZiG Cloud Manager Settings** application.

NETWORK CONFIGURATION

10ZiG Technology recommends that you have minimum prior knowledge on the following:

- Domain Name System (DNS)
- Network Address Translation (NAT)

10ZiG Manager Cloud Connector Site Recommendations

- A static Public IP address required on the WAN interface.
- Use split DNS with an internal DNS SRV record for 10ZiG Manager Server Hostname resolvable to the 10ZiG Manager Server IP address. And use an external DNS A record for 10ZiG Manager Server Hostname resolvable to the static Public IP Address on the WAN interface.
- A NAT router is required in a typical deployment. Most business grade SOHO routers and above include this function.
- TCP port 443 by default or custom port number configured in 10ZiG Cloud Manager Settings, opened on Firewall from the public internet and forwarded to the 10ZiG Manager Server IP Address.
- You will need administrative access to the WAN router/firewall device. 10ZiG Technology will not provide support in configuration of this device.

External Thin Client Site Recommendations

- A NAT router is required in a typical deployment. Most business grade SOHO routers and above include this function.

- You may need administrative access to the WAN router/firewall device. 10ZiG Technology will not provide support in configuration of this device.

WAN Router/Firewall

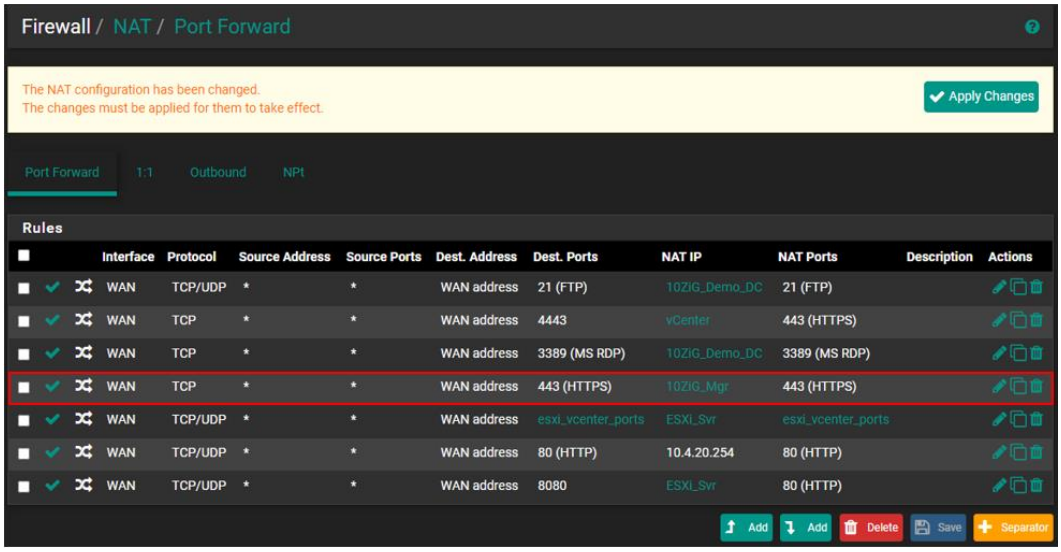
To allow external access to the 10ZiG Manager through the Cloud Connector, NAT Port Forwarding/Firewall rules should be configured on the Edge Router/Firewall.

Default ports that should be opened are described below. Custom port numbers used, will need to be adjusted and opened accordingly within the WAN router/firewall device.

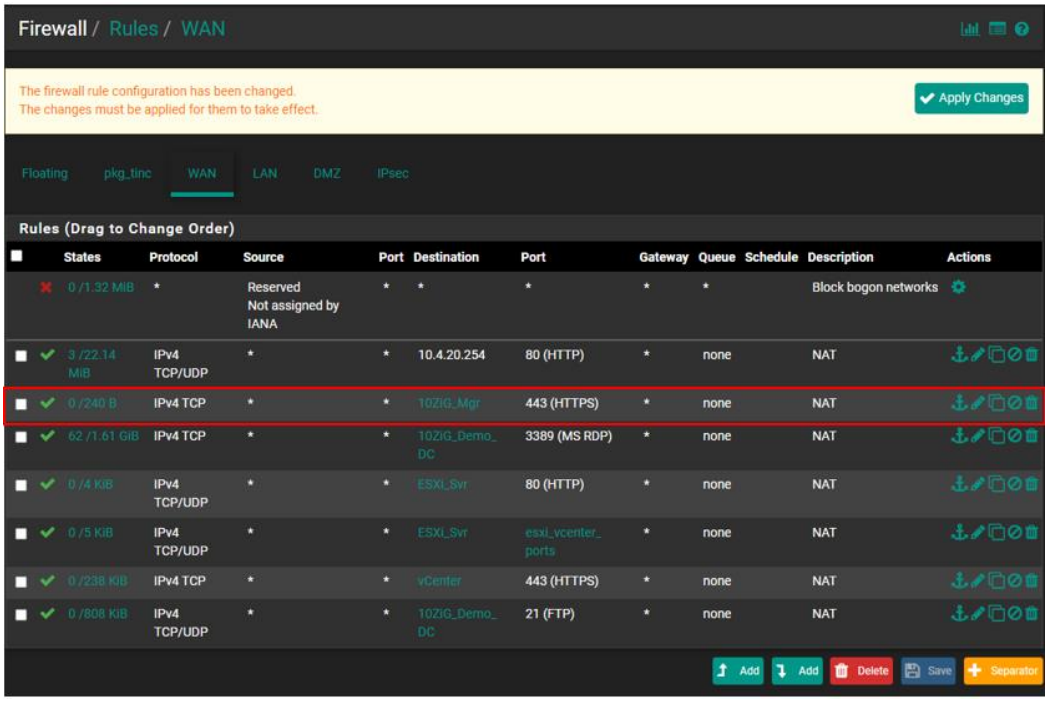
NOTE: Router/Firewall configuration will vary depending on the manufacturer/model of device being used. Refer to the manufacturer's product documentation for further guidance on implementing this.

EXTERNAL > INTERNAL

Interface	Protocol	Source Address	Source Ports	Destination Address	Destination Ports	NAT IP	NAT Ports
WAN	TCP	*	*	WAN IP Address	443	IP Address of the 10ZiG Manager Server	443



Interface	Address Family	Protocol	Source Address	Destination Address	Destination Port	Action
WAN	IPv4	TCP	*	IP Address of the 10ZiG Manager Server	443	PASS


Firewall / Rules / WAN
The firewall rule configuration has been changed.
The changes must be applied for them to take effect.
Apply Changes
Floating
pkg_tinc
WAN
LAN
DMZ
IPsec
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
0 /1.32 MiB
*
Reserved Not assigned by IANA
*
*
*
*
*
Block bogon networks
3 /22.14 MiB
IPv4 TCP/UDP
*
*
10.4.20.254
80 (HTTP)
*
none
NAT
0 /240 B
IPv4 TCP
*
*
10ZiG_Mgr
443 (HTTPS)
*
none
NAT
62 /1.61 GiB
IPv4 TCP
*
*
10ZiG_Demo_DC
3389 (MS RDP)
*
none
NAT
0 /4 KiB
IPv4 TCP/UDP
*
*
ESXi_Svr
80 (HTTP)
*
none
NAT
0 /5 KiB
IPv4 TCP/UDP
*
*
ESXi_Svr
esxi_vcenter_ports
*
none
NAT
0 /238 KiB
IPv4 TCP
*
*
vCenter
443 (HTTPS)
*
none
NAT
0 /808 KiB
IPv4 TCP/UDP
*
*
10ZiG_Demo_DC
21 (FTP)
*
none
NAT
Add
Add
Delete
Save
Separator

DEPLOYMENT SCENARIO 2 CONFIGURATION GUIDE

In this deployment, the 10ZiG Manager is installed on multiple servers. Internally the Manager Server, Console, and Web Console Server are installed. The Edge Router/Firewall connected to the Internet from where the externally deployed 10ZiG Clients will connect from, is configured to port forward TCP/443 HTTPs traffic inbound to the 10ZiG Manager Cloud Connector Server situated in a DMZ. The DMZ is configured to forward the required traffic Internally to the destination 10ZiG Manager Server. Outbound rules from the internal network are required to forward traffic back to the Cloud Connector in the DMZ.

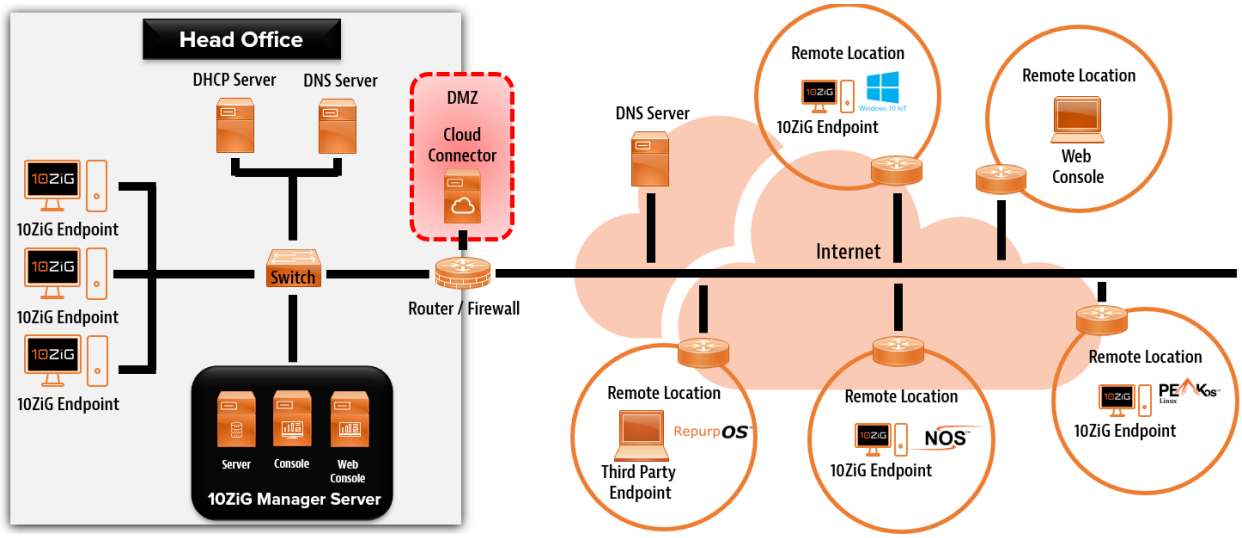
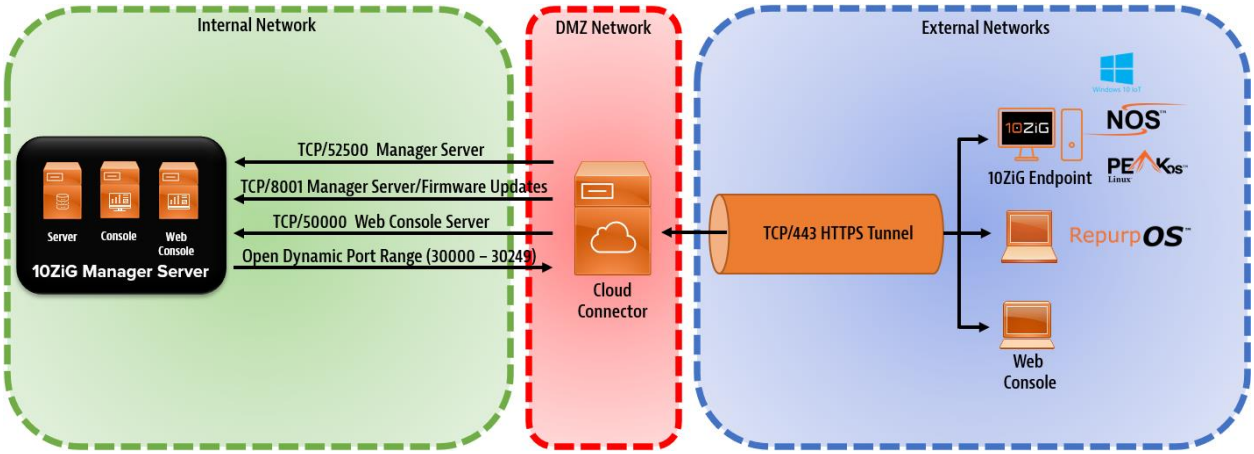


FIGURE 7 DEPLOYMENT SCENARIO 2 EXAMPLE NETWORK DIAGRAM



MANAGER INSTALLATION AND CONFIGURATION

NOTE: If you are using 10ZiG Windows 10 IoT devices with the XTC Agent 2.1.0.0 or newer installed. You will also need to be running the 10ZiG Manager 3.0.5.0 or newer to manage these devices remotely.

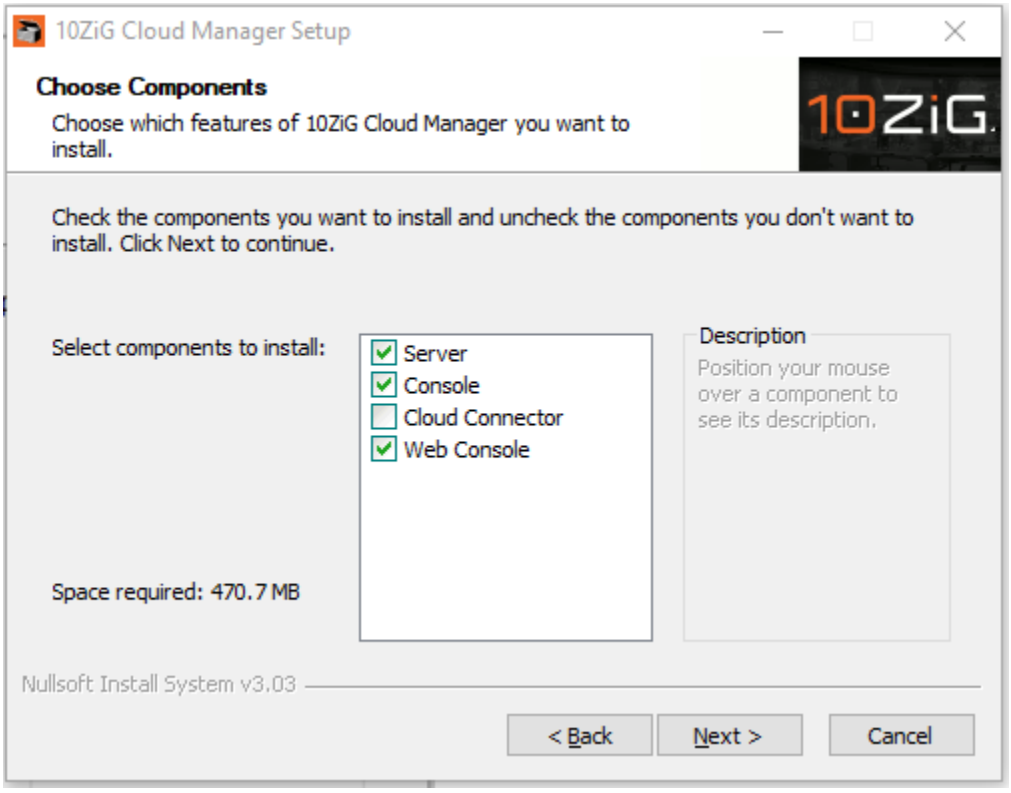
If the 10ZiG Manager is not installed or a supported version, please download the latest version from the 10ZiG website at

https://www.10zig.com/manager

A password is required for installation, please contact 10ZiG support to obtain the password. For 10ZiG Technical Support contact details please refer to the section on TROUBLESHOOTING AND SUPPORT

MANAGER SERVER INSTALLATION (INTERNAL NETWORK)

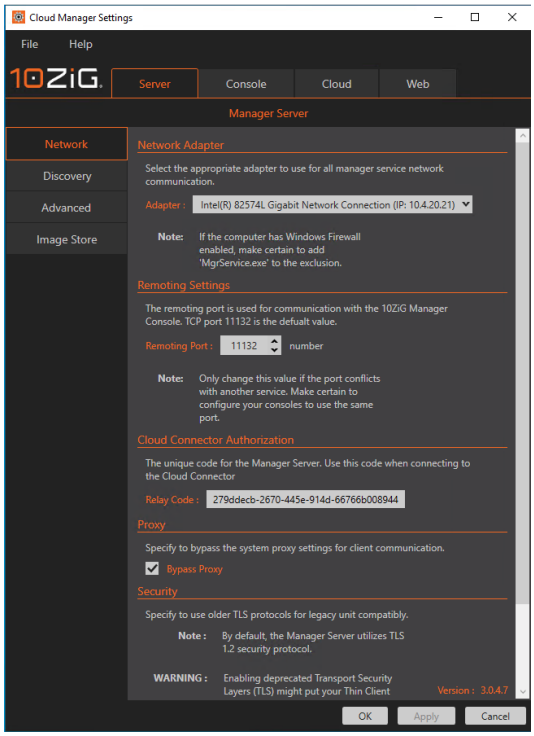
1. Run the 10ZiG Manager application suite installer to begin the 10ZiG Cloud Manager Setup.
2. When the **Choose Components** screen is displayed, select components **Server**, **Console**, **Web Console** and press **Next** to continue the setup procedure.



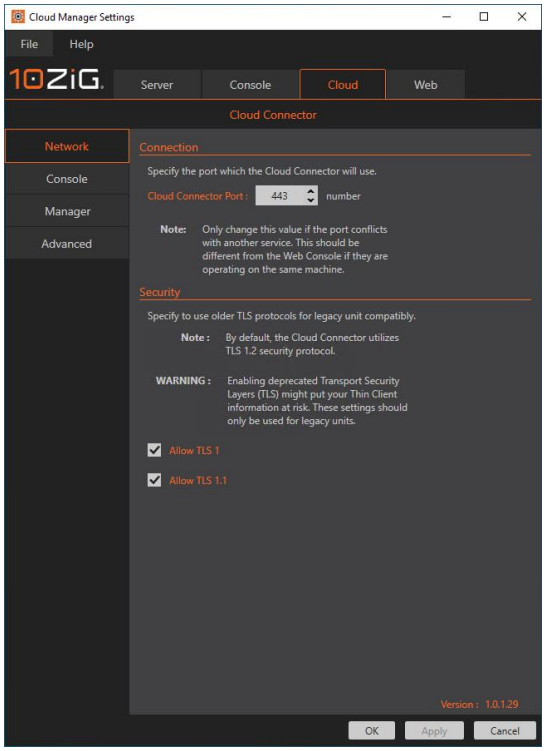
3. Click through the rest of the 10ZiG Cloud Manager Setup following the prompts to finish the installation.

MANAGER SERVER CONFIGURATION (INTERNAL NETWORK)

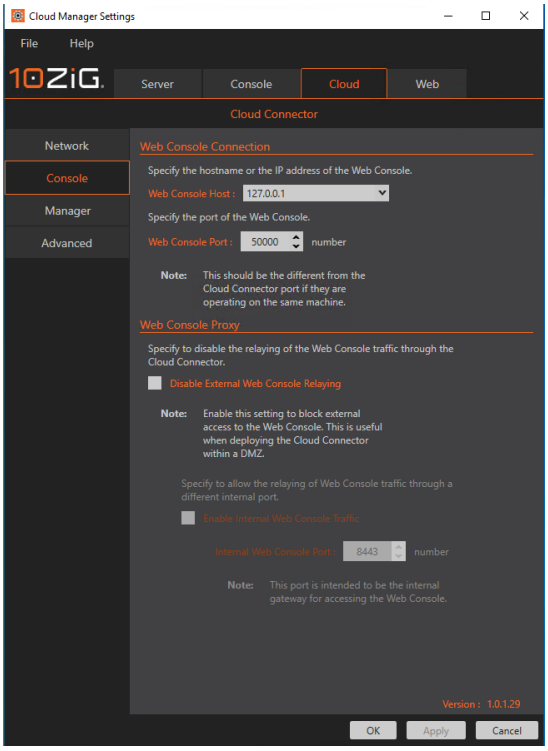
1. Run the **10ZiG Cloud Manager Settings** application from **Start > 10ZiG Manager > 10ZiG Cloud Manager Settings**.



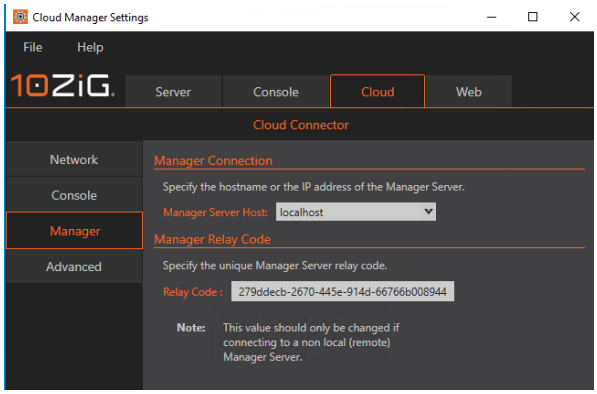
2. Switch to the **Cloud Connector** configuration settings. On the **Network** screen the **Cloud Connector Port** is set to **443** by default.



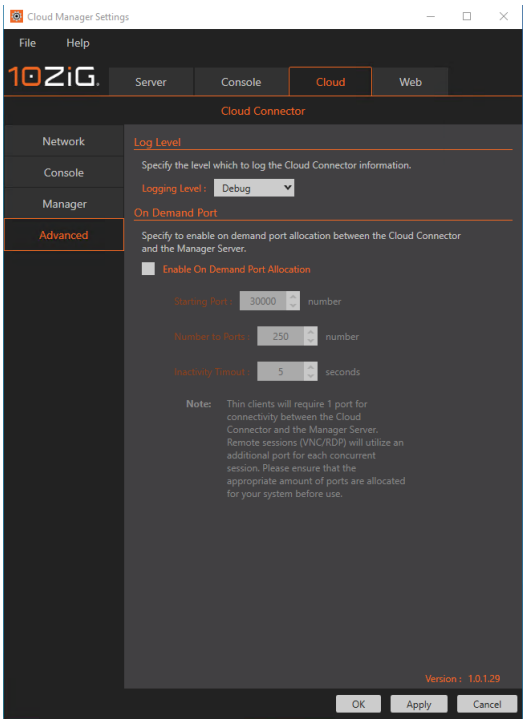
3. Switch to the **Console** configuration tab. The default configuration settings are shown below.



4. Switch to the **Manager** configuration tab. The default configuration settings are shown below. Make a note or copy the **Relay Code** displayed here. This is required to be entered in the **10ZiG Manager Cloud Connector Server** settings.



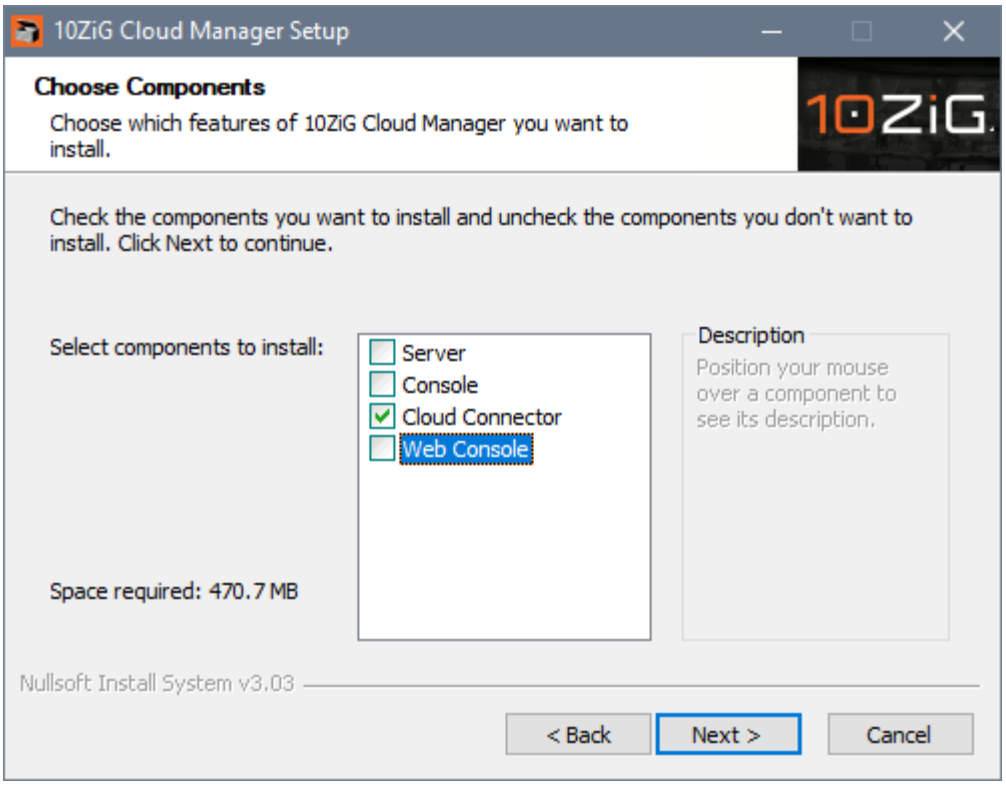
5. Switch to the **Advanced** configuration tab. The default configuration settings are shown below. For troubleshooting issues, the **Logging Level** can be increased from the default **info** to **debug** and the output viewed using the **10ZiG Syslog Viewer** from **Start > 10ZiG Manager > 10ZiG Syslog**.



6. When you have checked these settings and happy with the configuration press the **OK** button to close the **10ZiG Cloud Manager Settings** application.

MANAGER SECURE CONNECTER SERVER INSTALLATION (DMZ NETWORK)

1. Run the 10ZiG Manager application suite installer to begin the 10ZiG Cloud Manager Setup.
2. When the **Choose Components** screen is displayed, select the **Cloud Connector** component, and press **Next** to continue the setup procedure.

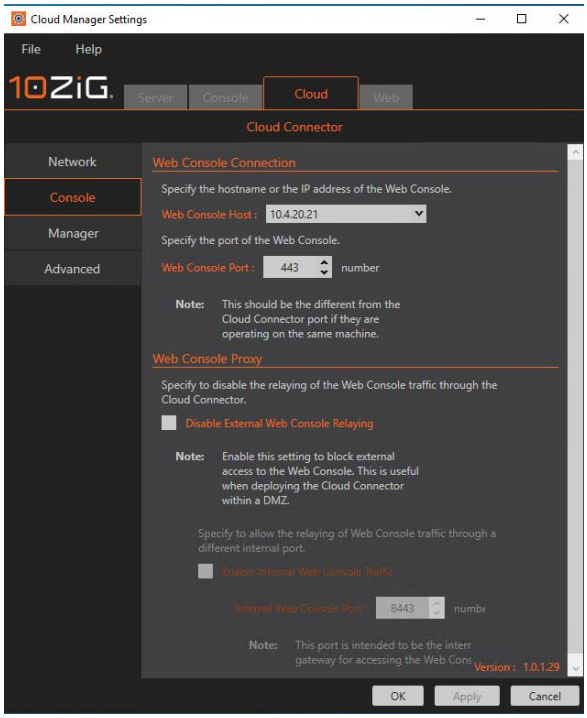


3. Click through the rest of the 10ZiG Cloud Manager Setup following the prompts to finish the installation.

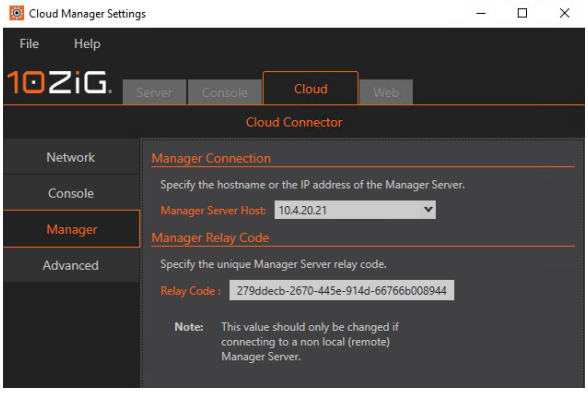
MANAGER SECURE CONNECTOR SERVER CONFIGURATION (DMZ NETWORK)

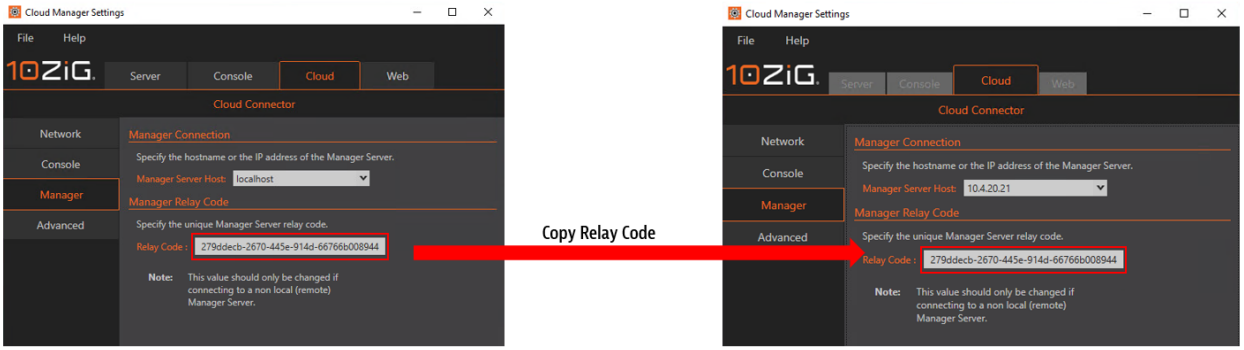
1. Run the **10ZiG Cloud Manager Settings** application from **Start > 10ZiG Manager > 10ZiG Cloud Manager Settings**.
2. Switch to the **Cloud Connector** configuration settings. On the **Network** screen the **Cloud Connector Port** is set to **443** by default.

3. Switch to the **Console** configuration tab. If Web Console access is required externally, then configure the **Web Console Host** value with the **10ZiG Manager (Web Console Server) IP Address**. If you wish to prevent traffic before relayed between the Cloud Connector and Web Console Server, then you can restrict this usage **Enabling** the option **Disable External Web Console Relaying**.



4. Switch to the **Manager** configuration tab. The default configuration settings are shown below. Paste or enter the **Relay Code** from the **10ZiG Manager Server** configured previously here





Manager Server

Manager Cloud Connector Server

5. Switch to the **Advanced** configuration tab. For troubleshooting issues, the **Logging Level** can be increased from the default **info** to **debug** and the output viewed using the **10ZiG Syslog Viewer** from **Start > 10ZiG Manager > 10ZiG Syslog**.
6. **Enable** the option **Enable On Demand Port Allocation**.
7. **Starting Port** can be configured with any port number within the range 1025 – 65535. The default value is starting from port **30000**. If this conflicts with any other applications on the network, it can be changed to a different value.
8. **Number to Ports** by default is set to **250.** The number entered here is determined by the number of remote clients that will be connecting simultaneously.in addition to the number of simultaneous VNC/RDP connections. For example, you have 50 remotely deployed 10ZiG Thin Clients and 4 Desktop Support staff that may be shadowing users via VNC/RDP providing support. Enter a value of 54 should provide the required number of ports (30000 – 30053) to facilitate clients and support sessions. If you stick with the default number of ports **250**, then the port range will be (30000 – 30249).
9. **Inactivity timeout** by default is configured to **5** seconds.

1. When you have checked these settings and happy with the configuration press the **OK** button to close the **10ZiG Cloud Manager Settings** application.

NETWORK CONFIGURATION

10ZiG Technology recommends that you have minimum prior knowledge on the following:

- Domain Name System (DNS)
- Network Address Translation (NAT)

10ZiG Manager Cloud Connector Site Recommendations

- A static Public IP address required on the WAN interface.
- Use split DNS with an internal DNS SRV record for 10ZiG Manager Server Hostname resolvable to the 10ZiG Manager Server IP address. And use an external DNS A record for 10ZiG Manager Server Hostname resolvable to the static Public IP Address on the WAN interface.
- A NAT router is required in a typical deployment. Most business grade SOHO routers and above include this function.
- TCP port 443 by default or custom port number configured in 10ZiG Cloud Manager Settings, opened on Firewall from the public internet and forwarded to the 10ZiG Manager Cloud Connector Server IP Address.
- You will need administrative access to the WAN router/firewall device. 10ZiG Technology will not provide support in configuration of this device.

External Thin Client Site Recommendations

- A NAT router is required in a typical deployment. Most business grade SOHO routers and above include this function.
- You may need administrative access to the WAN router/firewall device. 10ZiG Technology will not provide support in configuration of this device.

WAN Router/Firewall

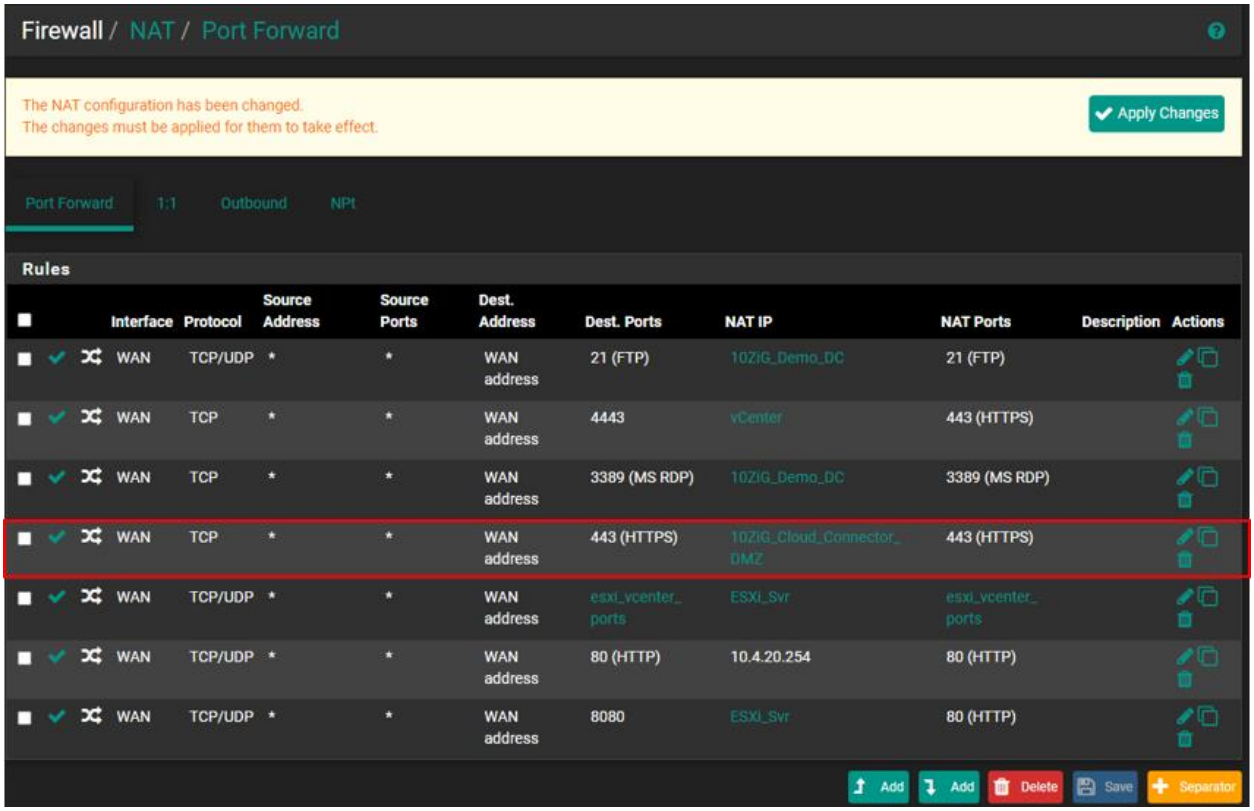
To allow external access to the 10ZiG Manager through the Cloud Connector, NAT Port Forwarding/Firewall rules should be configured on the Edge Router/Firewall.

Default ports that should be opened are described below. Custom port numbers used, will need to be adjusted and opened accordingly within the WAN router/firewall device.

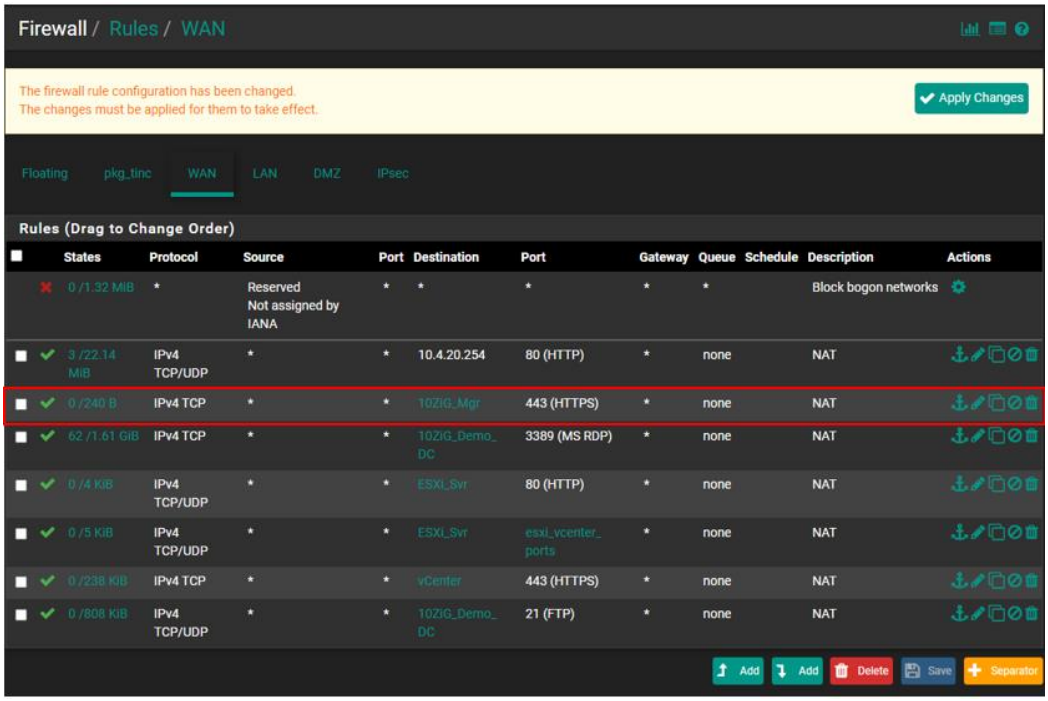
NOTE: Router/Firewall configuration will vary depending on the manufacturer/model of device being used. Refer to the manufacturer's product documentation for further guidance on implementing this.

EXTERNAL > INTERNAL

Interface	Protocol	Source Address	Source Ports	Destination Address	Destination Ports	NAT IP	NAT Ports
WAN	TCP	*	*	WAN IP Address	443	IP Address of the 10ZiG Manager Cloud Connector Server (DMZ)	443

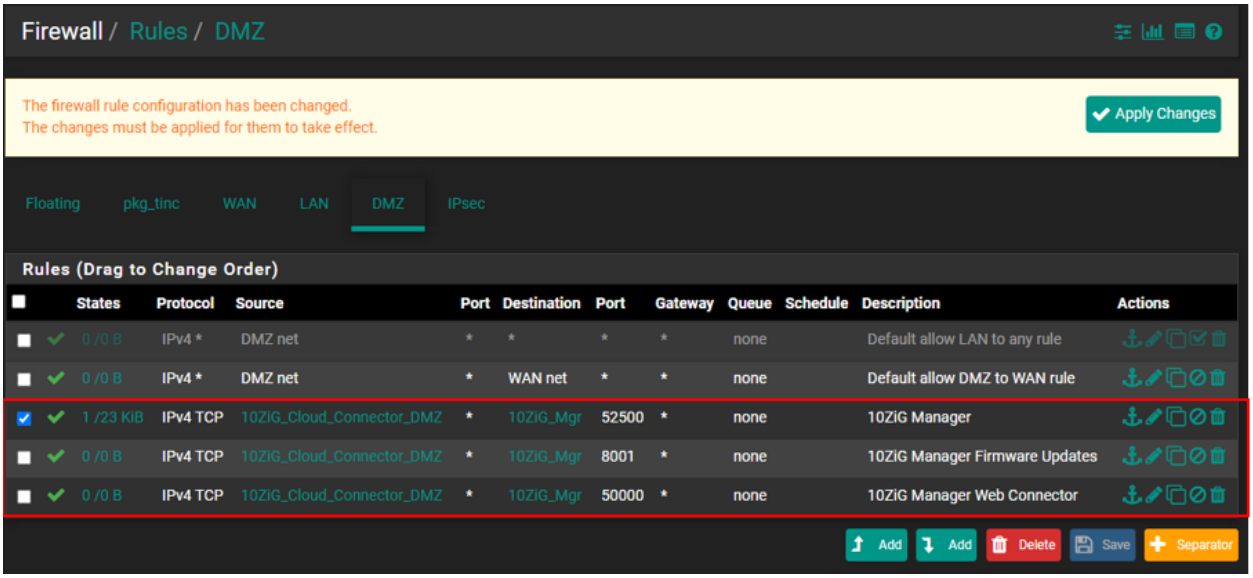


Interface	Address Family	Protocol	Source Address	Destination Address	Destination Port	Action
WAN	IPv4	TCP	*	IP Address of the 10ZiG Manager Cloud Connector Server	443	PASS



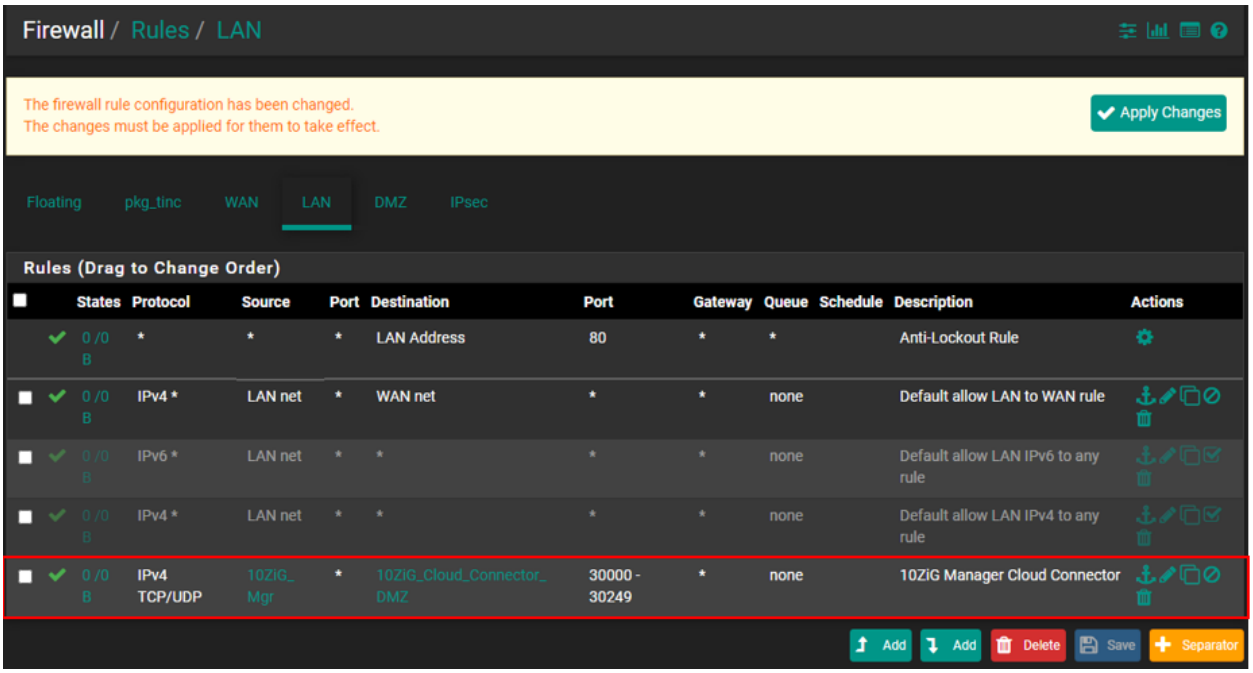
DMZ > INTERNAL

Interface	Address Family	Protocol	Source Address	Destination Address	Destination Port	Action
DMZ	IPv4	TCP	IP Address of the 10ZiG Manager Cloud Connector Server	IP Address of the 10ZiG Manager Server	52500	PASS
DMZ	IPv4	TCP	IP Address of the 10ZiG Manager Cloud Connector Server	IP Address of the 10ZiG Manager Server	50000	PASS
DMZ	IPv4	TCP	IP Address of the 10ZiG Manager Cloud Connector Server	IP Address of the 10ZiG Manager Server	8001	PASS



INTERNAL > DMZ

Interface	Address Family	Protocol	Source Address	Destination Address	Destination Port Range	Action
LAN	IPv4	TCP	* IP Address of the 10ZiG Manager Server	IP Address of the 10ZiG Manager Cloud Connector Server	30000 - 30249	PASS


Firewall / Rules / LAN
The firewall rule configuration has been changed.
The changes must be applied for them to take effect.
Apply Changes
Floating
pkg_tinc
WAN
LAN
DMZ
IPsec
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
0 /0 B
*
*
*
LAN Address
80
*
*
Anti-Lockout Rule
0 /0 B
IPv4 *
LAN net
*
WAN net
*
*
none
Default allow LAN to WAN rule
0 /0 B
IPv6 *
LAN net
*
*
*
*
none
Default allow LAN IPv6 to any rule
0 /0 B
IPv4 *
LAN net
*
*
*
*
none
Default allow LAN IPv4 to any rule
0 /0 B
IPv4 TCP/UDP
10ZiG_Mgr
*
10ZiG_Cloud_Connector_DMZ
30000 - 30249
*
none
10ZiG Manager Cloud Connector
Add
Add
Delete
Save
Separator

SECURE AGENT CONFIGURATION

All 10ZiG Thin Client Operating Systems - NOS, PeakOS, RepurpOS - and Windows 10 IoT clients come pre-installed with a Cloud Manager Agent. This section guides you through configuring the Cloud Manager Agent for remotely deployed 10ZiG Thin Clients.

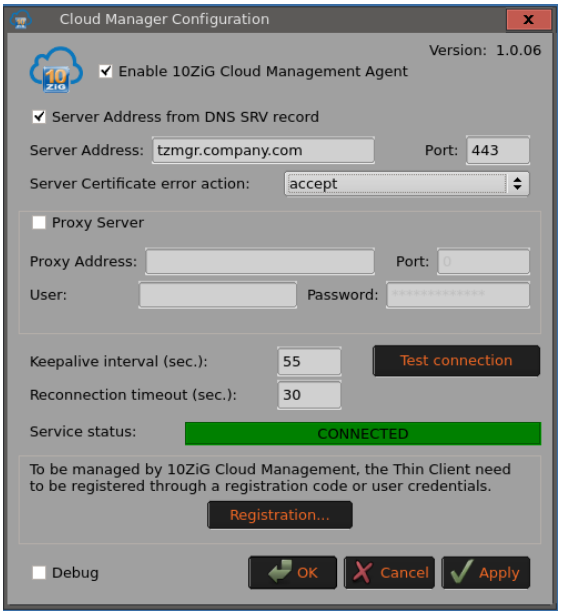
NOTE: 10ZiG Technology offer a service to use a custom configured template provided by the customer, which can be put on ordered Thin Clients during the production phase before shipping. So already pre-configured on arrival to the customer premises. If you are interested in taking advantage of this service, please discuss further with your sales representative.

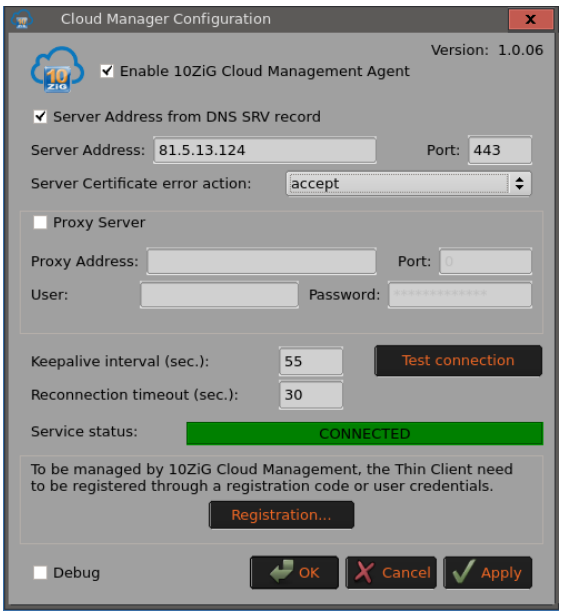
NOS, PeakOS, RepurpOS

NOS CONFIGURATION

1. From the NOS **Control Panel**, select **Cloud Manager**. 

2. Enter the **Hostname (FQDN)** or **Public IP Address** of the **10ZiG Manager Cloud Connector.Server**. This is used as an alternative to the secure agent discovering the secure connector using the 'Server Address from a DNS SRV record'. To leverage this connectivity, refer to Appendix D – Split DNS in Network Environments.





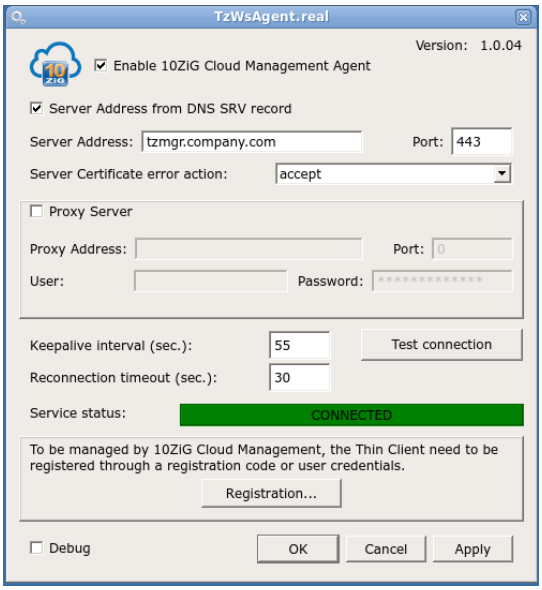
3. If the 10ZiG Manager Server and Cloud Connector are configured and deployed, you can click the **Test Connection** button to check the connection is successful.
4. OPTIONAL: You can click the **Registration…** button and add a **Registration Code** that can be used by the 10ZiG Manager to auto-populate the device into a group configured with a registration code filter for better organization and easier maintenance. Click the **OK** button when you have completed this.

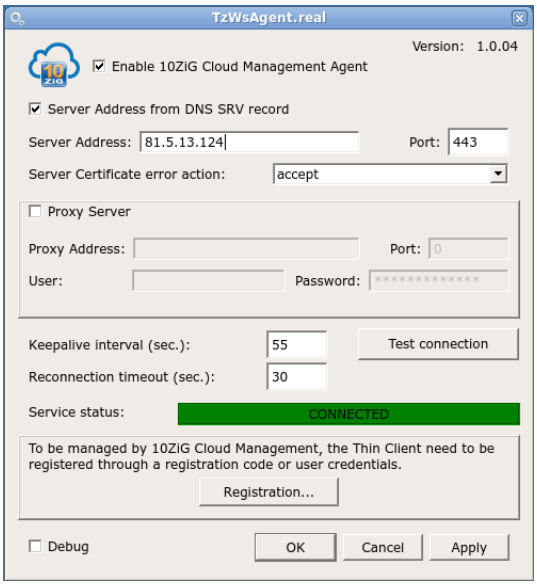
5. When you are happy with the settings on the Cloud Manager Configuration screen you can press the **OK** button to complete this part of the deployment configuration.

PeakOS CONFIGURATION

1. From the PeakOS **Terminal Properties** screen, select **Cloud Manager**.

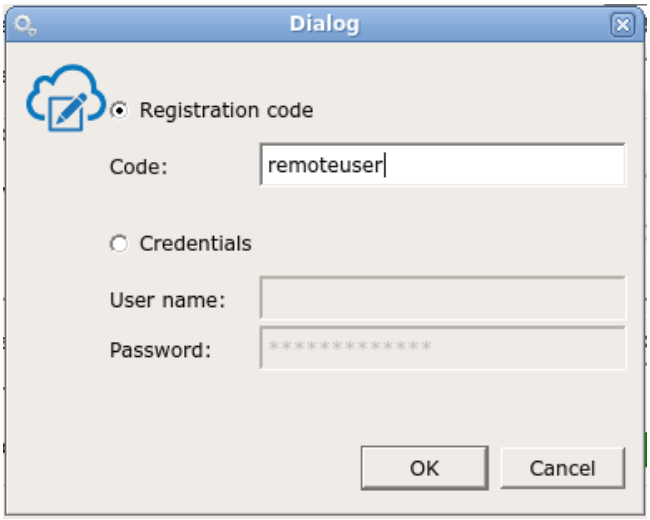
1. Enter the **Hostname (FQDN)** or **Public IP Address** of the **10ZiG Manager Cloud Connector.Server**. This is used as an alternative to the secure agent discovering the secure connector using the 'Server Address from a DNS SRV record'. To leverage this connectivity, refer to Appendix D – Split DNS in Network Environments.





2. If the 10ZiG Manager Server and Cloud Connector are configured and deployed, you can click the **Test Connection** button to check the connection is successful.

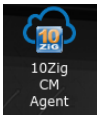
3. OPTIONAL: You can click the **Registration…** button and add a **Registration Code** that can be used by the 10ZiG Manager to auto-populate the device into a group configured with a registration code filter for better organization and easier maintenance. Click the **OK** button when you have completed this.



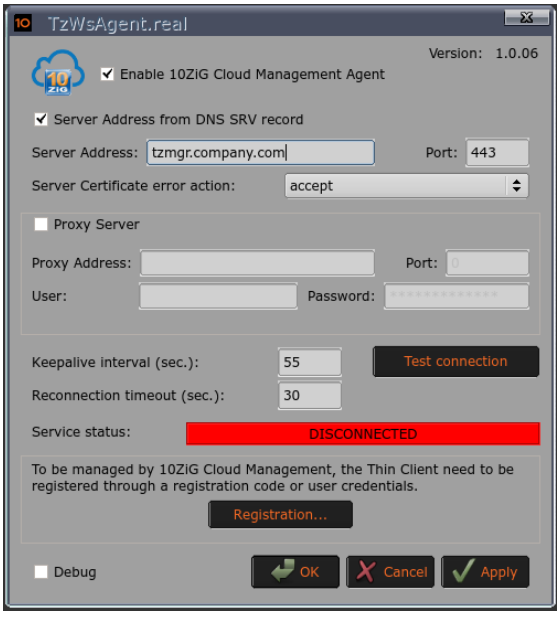
4. When you are happy with the settings on the Cloud Manager Configuration screen you can press the **OK** button to complete this part of the deployment configuration.

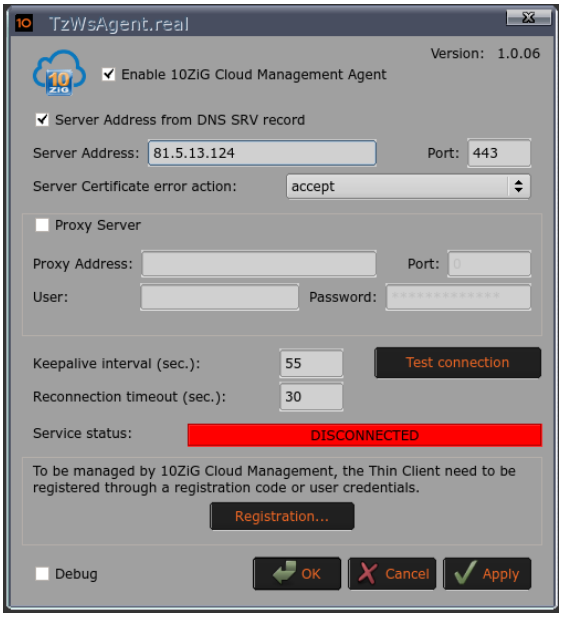
RepurpOS CONFIGURATION

1. From the RepurpOS **Terminal Properties** screen, select **10ZiG CM Agent**.

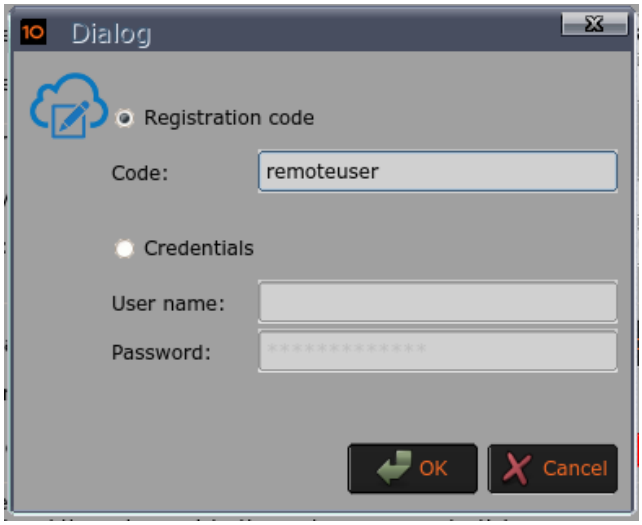


1. Enter the **Hostname (FQDN)** or **Public IP Address** of the **10ZiG Manager Secure Connector Server**. This is used as an alternative to the secure agent discovering the secure connector using the 'Server Address from a DNS SRV record'. To leverage this connectivity, refer to Appendix D – Split DNS in Network Environments.





2. If the 10ZiG Manager Server and Secure Connector are configured and deployed, you can click the **Test Connection** button to check the connection is successful.
3. OPTIONAL: You can click the **Registration…** button and add a **Registration Code** that can be used by the 10ZiG Manager to auto-populate the device into a group configured with a registration code filter for better organization and easier maintenance. Click the **OK** button when you have completed this.

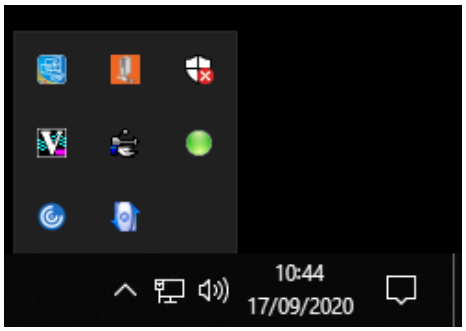


4. When you are happy with the settings on the Registration Code Configuration screen you can press the **OK** button to complete this part of the deployment configuration.

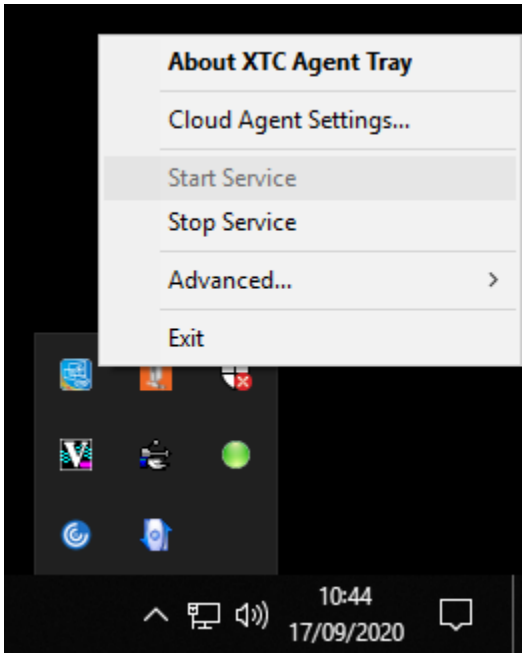
WINDOWS 10 IoT

NOTE: 10ZiG Windows 10 IoT devices must be running 10ZiG XTC Agent 2.1.0.0 or newer to be able to connect remotely using the 10ZiG Manager Secure Connector.

You can check this on your device by right clicking the **XTC Agent Tray** icon  from the Windows system tray.



From the menu displayed, select **About XTC Agent Tray**.



If you do not see this icon  in the system tray, then either the XTC Agent is not installed or not currently running.

If it is not running but installed, go to **Start > All Programs > 10ZiG XTC Agent > XTC Agent Tray** to start the service.

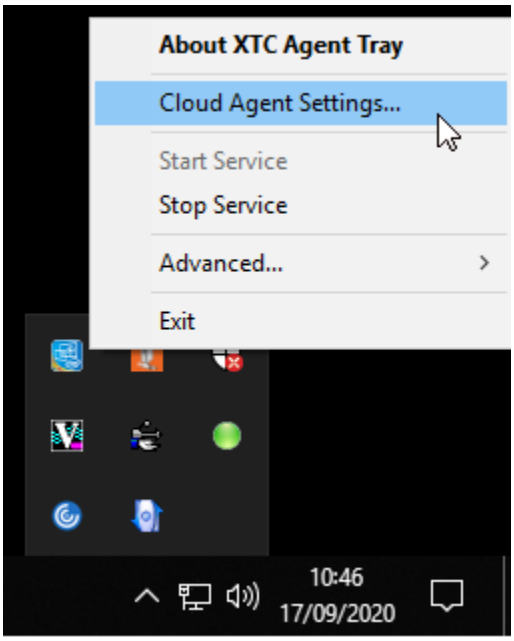
If the XTC Agent tray is not installed or a supported version, please download the latest version from the 10ZiG website at

https://www.10zig.com/manager

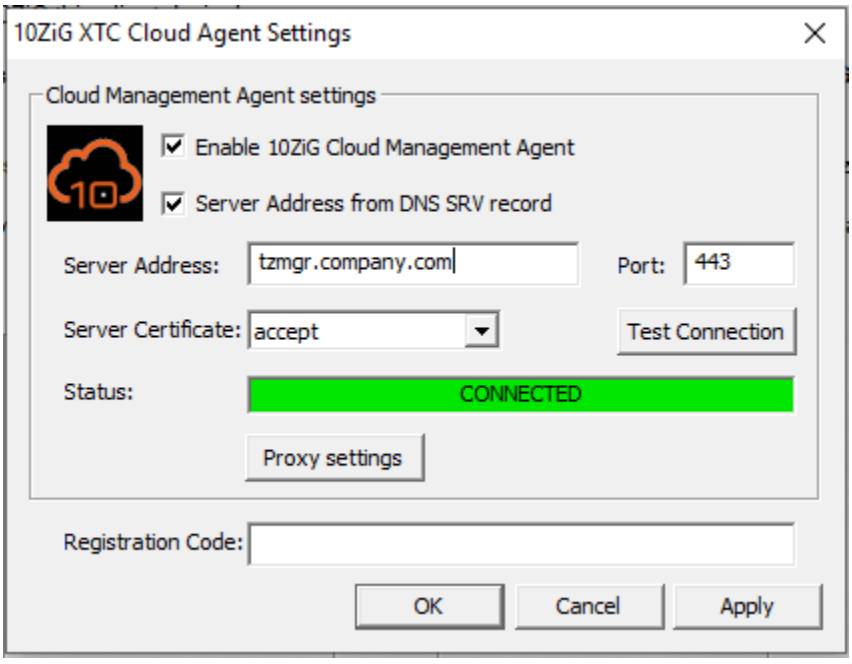
alternatively contact 10ZiG support to obtain the latest version. For 10ZiG Technical Support contact details please refer to the section on TROUBLESHOOTING AND SUPPORT

WINDOWS 10 IoT CONFIGURATION

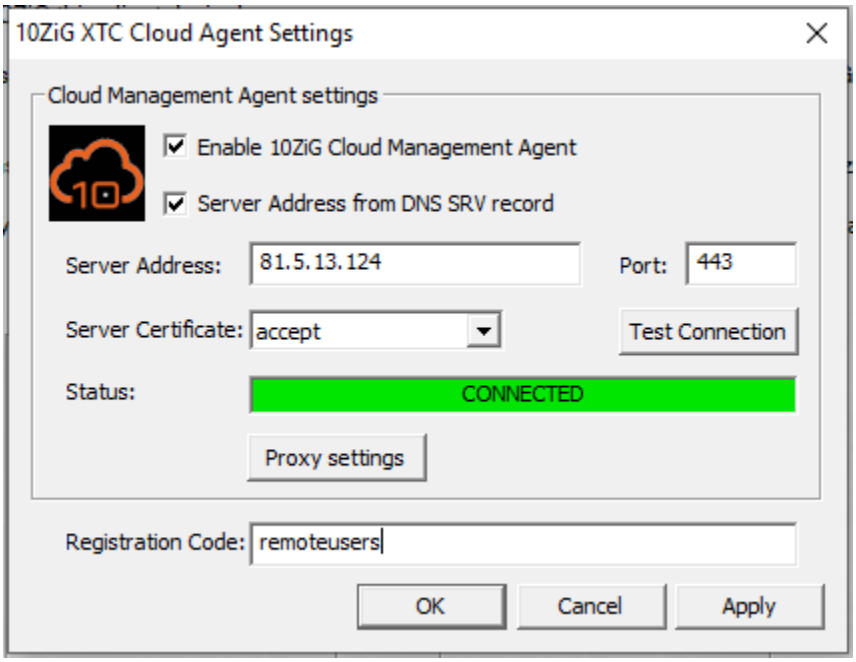
1. Right click the **XTC Agent Tray** icon from the Windows System Tray.
2. From the menu displayed select **Secure Agent Settings...**



3. Enter the **Hostname** or **Public IP Address** of the router with access to the 10ZiG Manager Secure Connector Server.



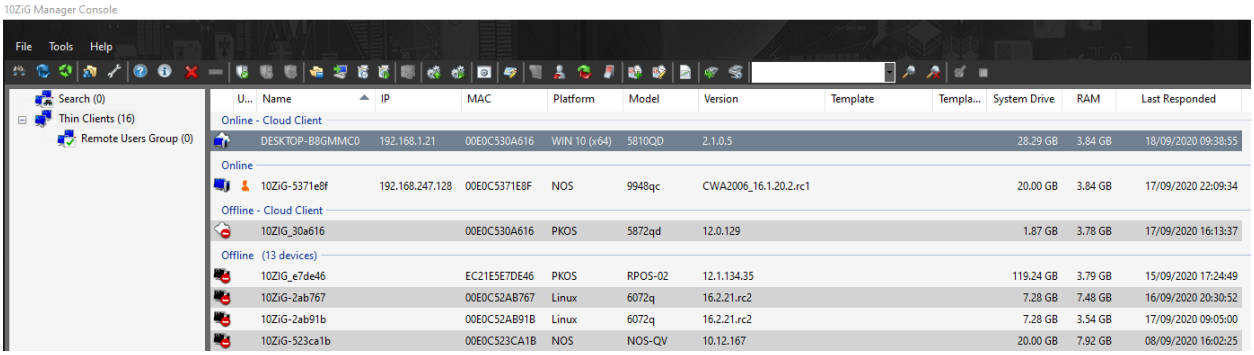
4. OPTIONAL: You can add a **Registration Code** that can be used by the 10ZiG Manager to auto-populate the device into a group configured with a registration code filter for better organization and easier maintenance.



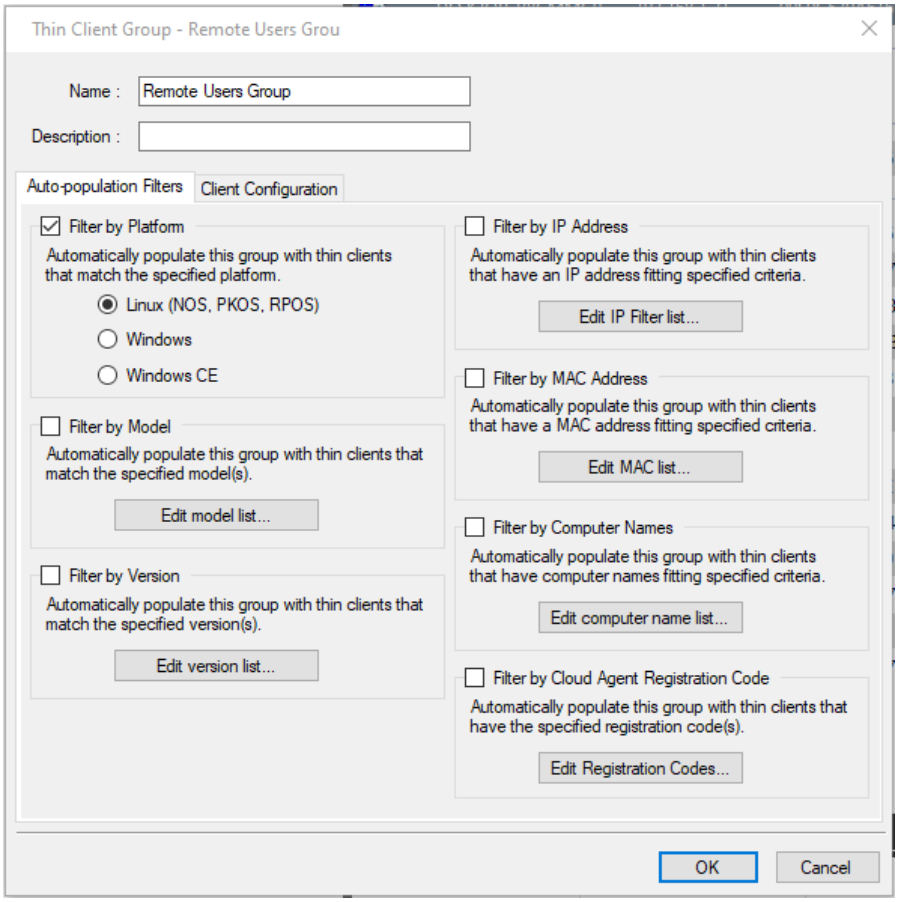
5. When you are happy with the settings on the 10ZiG XTC Secure Agent settings screen you can press the **OK** button to complete this part of the deployment configuration.

10ZiG MANAGER GROUP AUTO-POPULATION FOR SECURE CONNECTED DEVICES

The 10ZiG Manager can automatically populate registered 10ZiG Thin Client devices into groups for easier visibility and administration for implementing firmware and configuration templates.



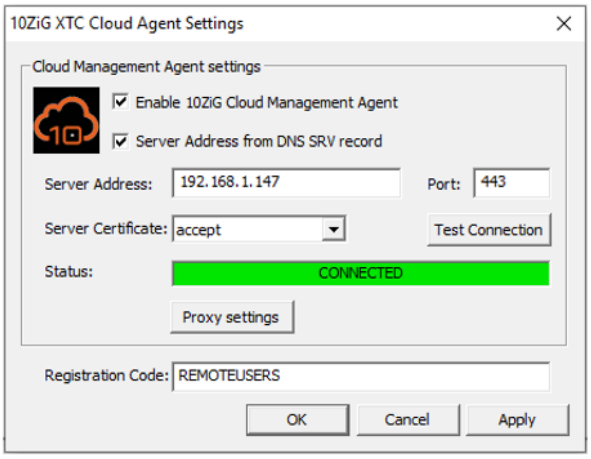
Internal devices are normally easy to filter, as the two most widely used filters implemented are **Filter by Platform** for the device operating system, and **Filter by IP Address**, which can be useful in VLAN and WAN environments where multiple IP subnets are used.



For deployments of remotely located 10ZiG Thin Clients however this is more problematic as they will be seen in the 10ZiG Manager as coming from various public IP addresses assigned to the WAN interface of their Edge Router/Firewall.

The easiest way to auto populate remote devices into groups is to use the **Registration Code** configured in the client Secure Agent. This can be configured before shipping clients to the users or if already done so, once connected to the 10ZiG Manager by sending a configuration file/template to the client with the **Registration Code** configured.

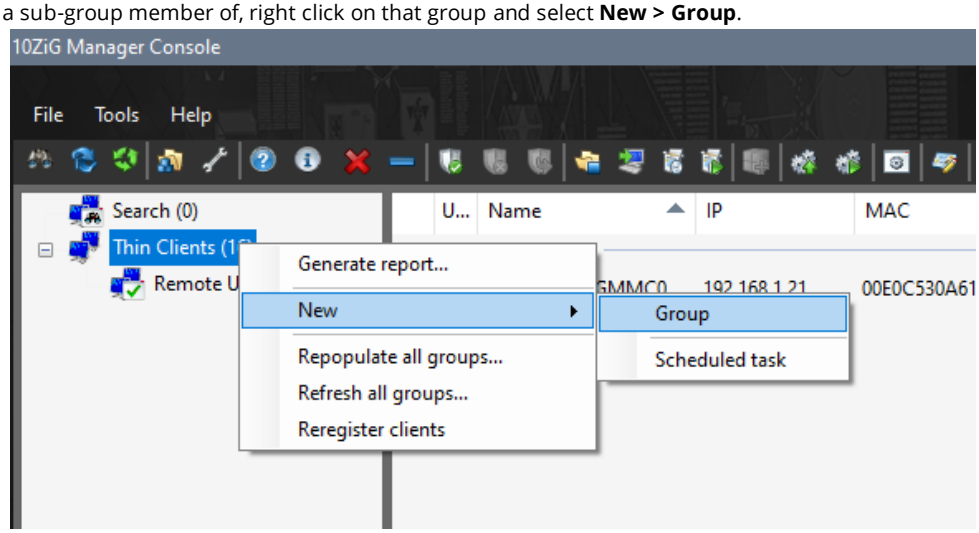
NOS



Windows 10 IoT

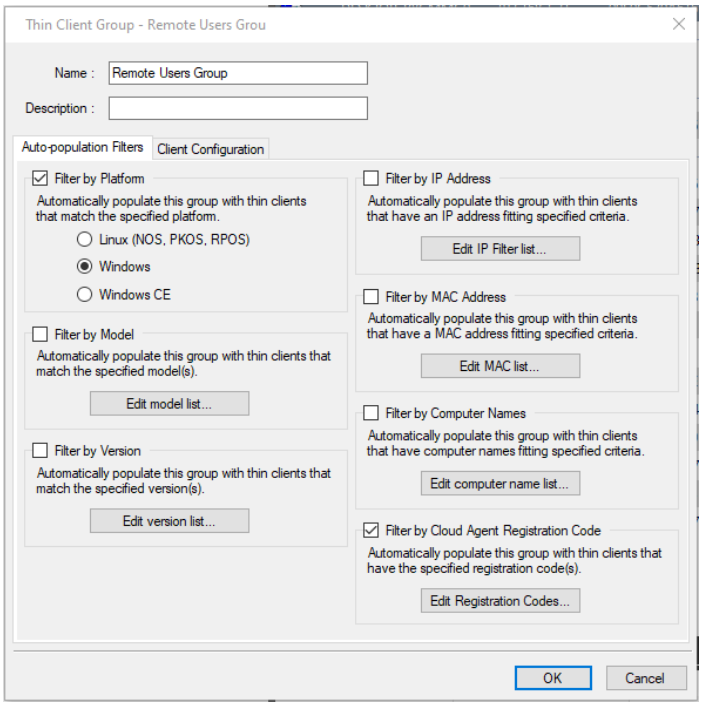
CREATE A GROUP FILTERED BY SECURE AGENT REGISTRATION CODE

1. Open the **10ZiG Manager Console**.
2. Right click the parent **Thin Clients** group or if you already have some child groups you want the new group to become a sub-group member of, right click on that group and select **New > Group**.

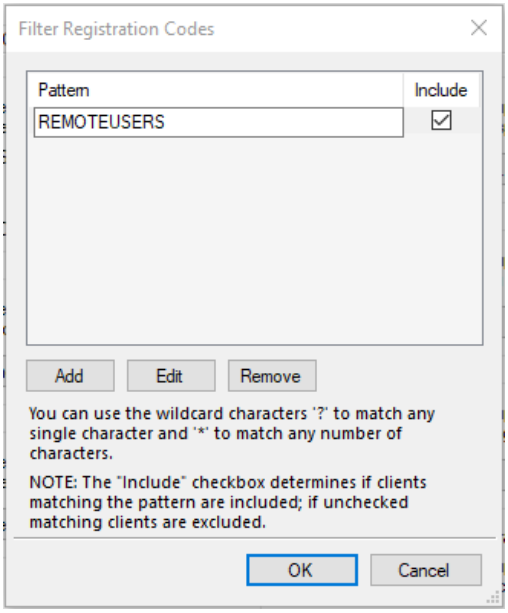


3. At the **Thin Client Group** screen, enter a **Name** for your group and optional **Description**. Under **Auto-population Filters** configure the following:

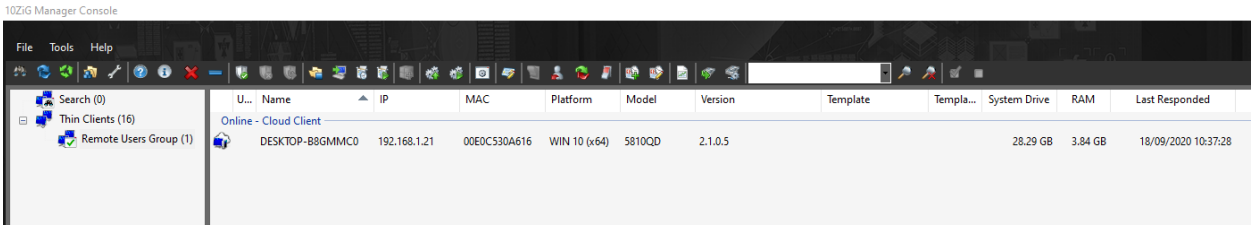
a. Enable **Filter by Platform** and select the **Operating System** family of the remote devices being grouped.
b. Enable **Filter by Secure Agent Registration Code** and click **Edit Registration Codes…**.



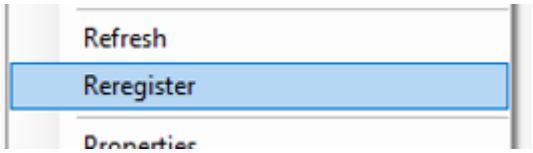
4. Once the **Edit Registration Codes…** button is pressed the **Filter Registration Codes** screen is displayed. Click the **Add** button to create a new pattern and enter the value configured in the 10ZiG Thin Clients Secure Manager Agent **Registration Code** field here.



5. Once you are happy the **Registration Code** patterns are configured correctly. Press the **OK** button to close the Filter Registration Codes screen.
6. Press the **OK** button on the Thin Client Group screen and the new group should appear and be configured ready for devices to auto-populate.



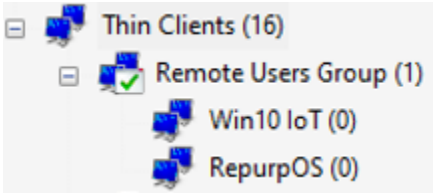
7. If the devices do not auto-populate to the group automatically you can check the following:
   a. Force a Re-Register by selecting the client or client(s) you want to correctly auto-populate and either press the **Re-Register** button on the toolbar  or right click and from the menu displayed select the option Re-Register.



   b. Reboot the client to force it to re-register on boot.
   c. Check the **Registration Code** is correct in both the client **Secure Agent** on the devices and group **Filter by Secure Agent Registration Code** and then attempt the above again.

Unfortunately, it is not possible to filter Linux and Windows 10 IoT devices in the same group, as you can only select either Linux or Windows in the **Filter by Platform** option.

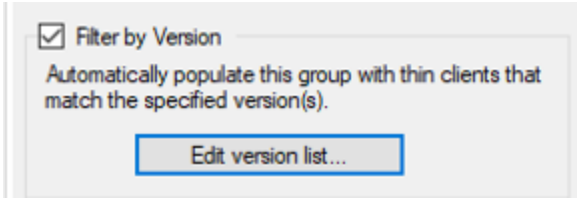
What you can do instead is create a group for the purpose of organizing the devices and then subgroups within that group can be used for splitting the different platforms.



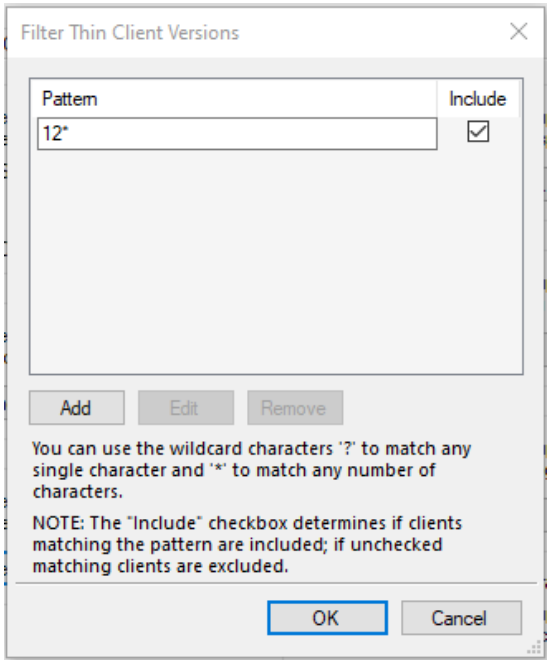
You can have a single group for the Linux platform, which would put any NOS, PeakOS, RepurpOS devices into it. But this could cause issues mixing those devices in the same group further down the road if you want to assign automatic templates to the group, as these differ between the different operating systems and firmware.

It is not an issue if you do not use **Automatic Client Configuration**, or **Auto Update Firmware**. But if you do intend to do this then you want to split the NOS, PeakOS, RepurpOS devices into their own specific groups.

Create the group with the **Filter by Platform** and **Filter by Secure Agent Registration Code** items configured as described above but also configure the **Filter by Version**.



1. Enable **Filter by Secure Agent Registration Code** and click **Edit version list…**.
2. Once the **Edit version list…** button is pressed the **Filter Thin Client Versions** screen is displayed. Click the **Add** button to create a new pattern and enter the prefix value from the below table along with a * (wildcard) to filter that specific operating system.



1. Once you are happy the **Thin Client Version** patterns are configured correctly. Press the **OK** button to close the Filter Thin Client Versions screen.

Operating System	Firmware Version Format	Pattern
NOS (32bit)	10.XX.XXX	10*
NOS (64bit)	16.XX.XXX	16*
PeakOS	12.XX.XXX	12*
RepurpOS	12.XX.XXX	12*

NOTE: RepurpOS and Peak OS use the same Firmware Version numbering so if you come across a situation where both these operating systems are in use and you want to filter these out similar to as shown above, then for the RepurpOS devices group you can also use the **Filter by Model** option and configure the pattern to match the platform name prefix **RPOS***.

TROUBLESHOOTING AND SUPPORT

If your having difficulties with deploying a Secure Connector environment or managing remotely deployed 10ZiG Thin Clients, then contact the Technical Support team covering your region for further assistance.

Please have a MAC address of one of your devices available when contacting the Technical Support teams with new support cases.

10ZiG Technology

North America (Rest of the world): **P: +1(866)865-5250**

E: support@10zig.com

EMEA: **P: +44(0)116 2148661**

E: support@10zig.eu

For further information on the 10ZiG Manager Application Suite, you can also look towards our YouTube channel that hosts videos on this subject and our other available products. Usefull videos to look out for are noted below:

Introduction & Tour – PeakOS, NOS, & Windows Endpoint Management Overview

(https://www.youtube.com/watch?v=Le5lXQv6Jlc)

Installation Deployment Best Practices for Remote Management and Configuration of 10ZiG Thin and Zero Clients

(https://www.youtube.com/watch?v=QPKU69BVry4&t=12s)

PeakOS / NOS Endpoint Deployment, Management and Configuration Best Practices
(https://www.youtube.com/watch?v=Hap5yHmMj4A)

APPENDICES

APPENDIX A – 10ZiG MANAGER MANAGEMENT PROTOCOLS WITHOUT USING THE SECURE CONNECTOR

DESCRIPTION	OPERATING SYSTEM(S)	PROTOCOL	PORT(S)
The Manager Console will register one of the ports within this range for notifications.	-	TCP	1113 – 11147
Discovery port for Thin Clients (Windows & Linux)	WINDOWS LINUX	UDP	52500
Used for querying information from and perform operations on Thin Clients (Linux)	LINUX	TCP	80, 443
Used for publishing firmware updates to Thin Clients (Linux)	LINUX	TCP	8001
RPC port used for performing remote operations and queries on Thin Clients. (Windows)	WINDOWS	TCP	52510
RPC port used to enable the Thin Clients to notify the Manager when they come online / offline (Windows)	WINDOWS	TCP	52511

APPENDIX B – SUPPORTED 10ZiG MANAGER SECURE CONNECTOR FEATURES FOR REMOTE LINUX CLIENTS

FEATURE	SUPPORTED (YES/NO)
IMAGE MANAGEMENT	
BACKUP	NO
RESTORE	NO
SYSTEM OPERATIONS	
REBOOT	YES
SHUTDOWN	YES
CONFIGURATION	
RETRIEVE	YES
SEND	YES
GENERATE TEMPLATE	YES
APPLY TEMPLATE	YES
RESET TO FACTORY DEFAULT SETTINGS	YES
CLIENT AUTOMATIC NAMING	YES
FIRMWARE UPDATES	YES
VNC REMOTE SHADOWING	YES
SCHEDULED TASKS	
POWER ON CLIENT	NO
REBOOT CLIENT	YES
SHUTDOWN CLIENT	YES
UPDATE DEVICE FIRMWARE	YES
APPLT TEMPLATE CONFIGURATION	YES
RESET TO FACTORY DEFAULT	YES

APPENDIX C – SUPPORTED 10ZiG MANAGER SECURE CONNECTOR FEATURES FOR WINDOWS 10 IoT CLIENTS

FEATURE	SUPPORTED (YES/NO)
WRITE PROTECTION	
ENABLE WRITE FILTER	YES
DISABLE WRITE FILTER	YES
IMAGE MANAGEMENT	
CLONE SYSTEM IMAGE	NO
DEPLOY SYSTEM IMAGE	NO
BACKUP	NO
RESTORE	NO
SYSTEM	
LOGOFF CURENT USER	YES
REBOOT	YES
SHUTDOWN	YES
WINDOWS CLIENT ADMINISTRATION	
LOCAL ADMINISTRATOR PASSWORD	YES
AUTOLOGON SETTINGS	YES
MANAGE UPDATES	YES
EXECUTE UPDATES	YES
VNC PROMPT ON CONNECT	YES
CONNECT USING RDP	YES
LOCAL PROCESSES	YES
LOCAL SYSTEM DRIVE	NO
CONFIGURATION	

RETRIEVE	YES
SEND	YES
CLIENT AUTOMATIC NAMING	YES
XTC AGENT UPDATES	YES
VNC REMOTE SHADOWING	YES
SCHEDULED TASKS	
POWER ON CLIENT	NO
LOGOFF ACTIVE USER	YES
REBOOT CLIENT	YES
SHUTDOWN CLIENT	YES
UPDTE XTC AGENT ON CLIENT	YES
DEPLOY SYSTEM IMAGE	NO
EXECUTE UPDATE	YES

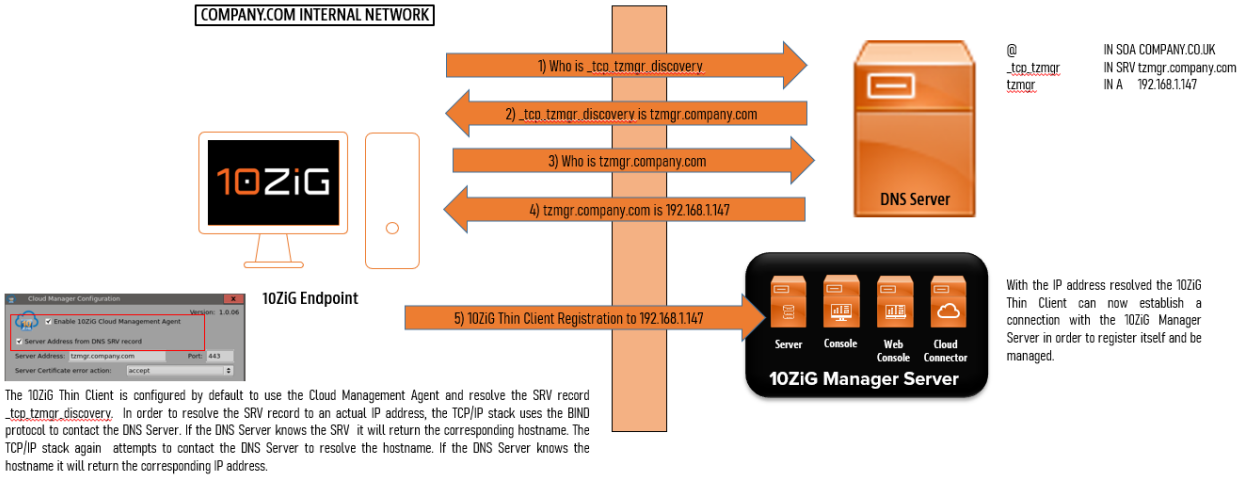
APPENDIX D – SPLIT DNS IN NETWORK ENVIRONMENTS

Split DNS is a useful implementation method that allows for a single hostname to be used and resolve to a Private IP Address when on the internal LAN network and to a different Public WAN IP Address when located externally for remote access.

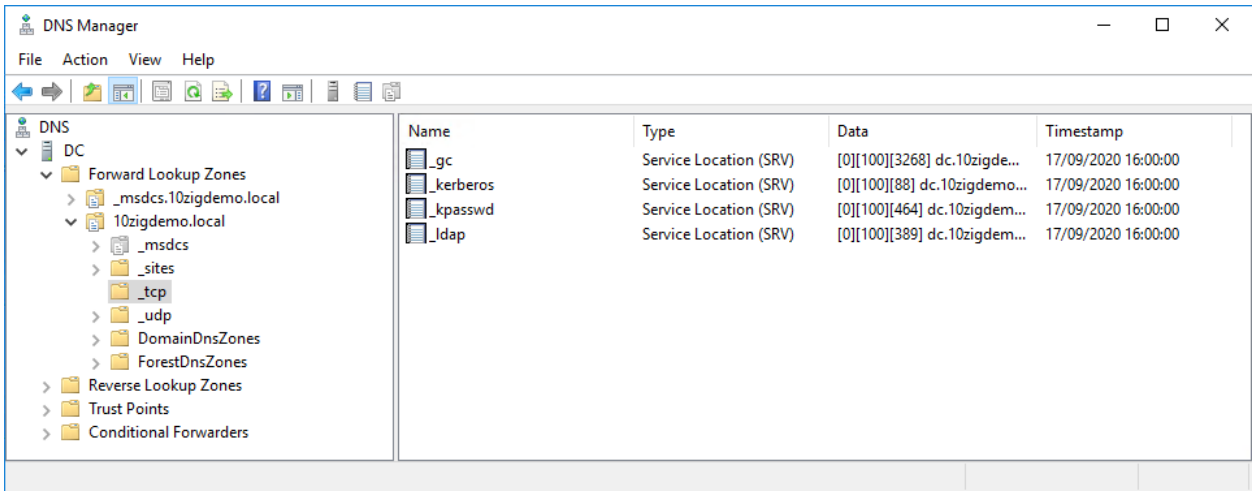
Many client applications such as Microsoft Outlook commonly use a FQDN (Fully Qualified Domain Name) to connect to an application server (i.e. Microsoft Exchange). For 10ZiG Thin Clients this can be used to connect devices to the 10ZiG Manager Server for centralized administration

INTERNAL DNS

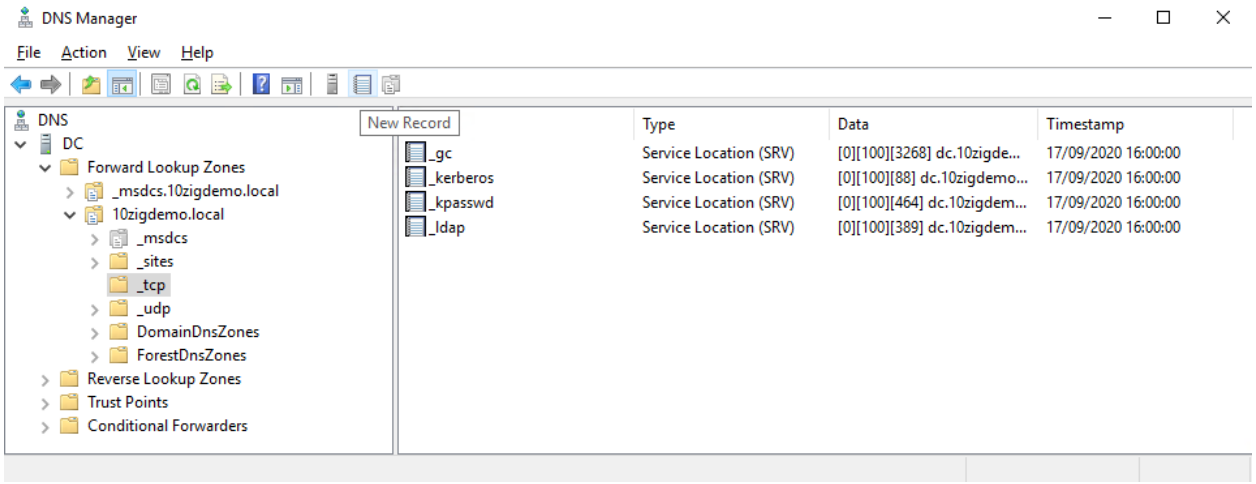
The resolution of the DNS address tzmgr.company.com to the IP address 192.168.1.147 and the subsequent connection between the 10ZiG Thin Client and the 10ZiG Manager Secure Connector will be accomplished as follows.



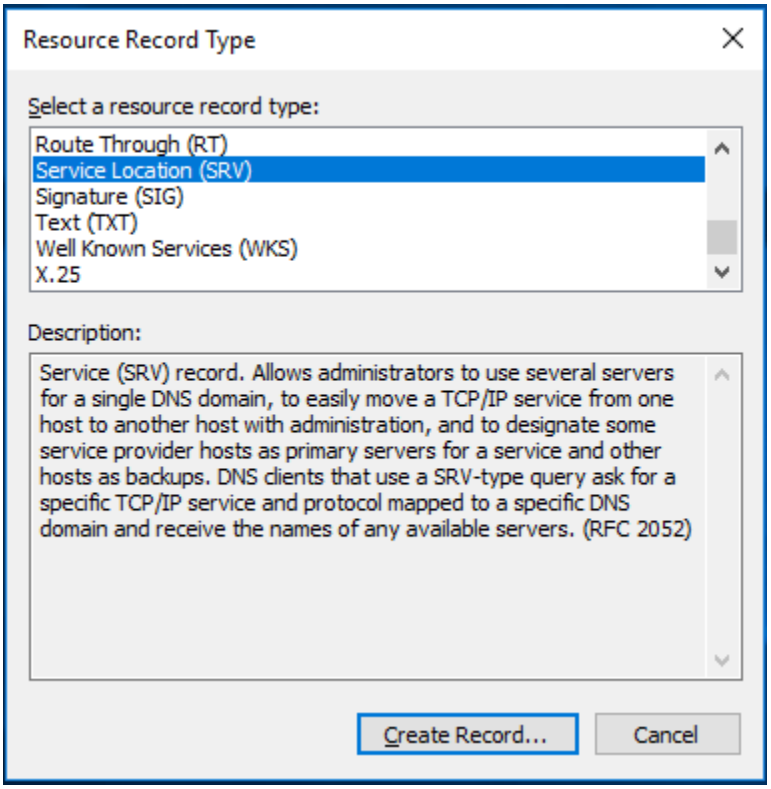
1. Launch the **Microsoft DNS Manager** on your internal DNS Server from the **Administrative Tools** Start menu folder or from the **Server Manager Console**.
2. Expand the DNS domain tree to navigate to navigate to the **_tcp** subdomain in the **Forward Lookup Zones** of your domain as pictured below.



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

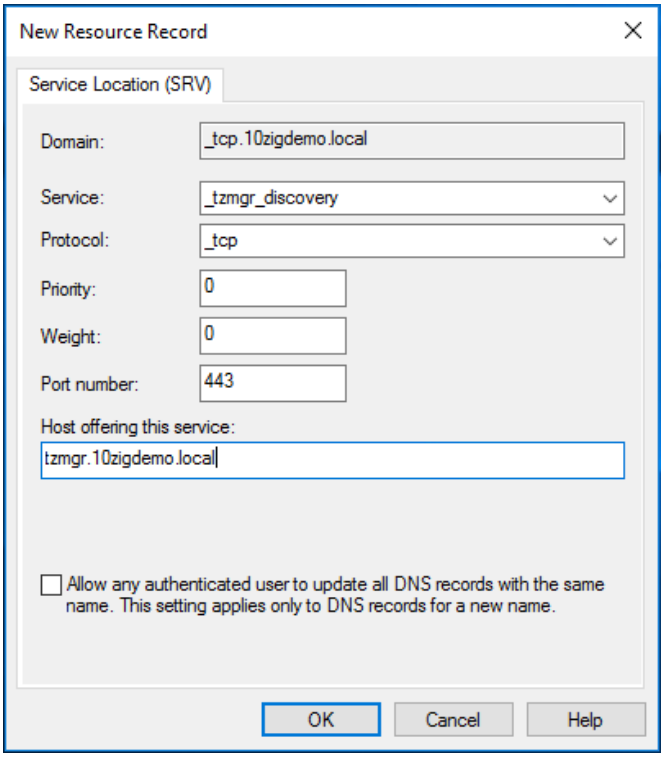


4. The Resource Record Type dialog window will appear. Scroll down list to find and select **Service Location (SRV)**, then click the **Create Record…** button.

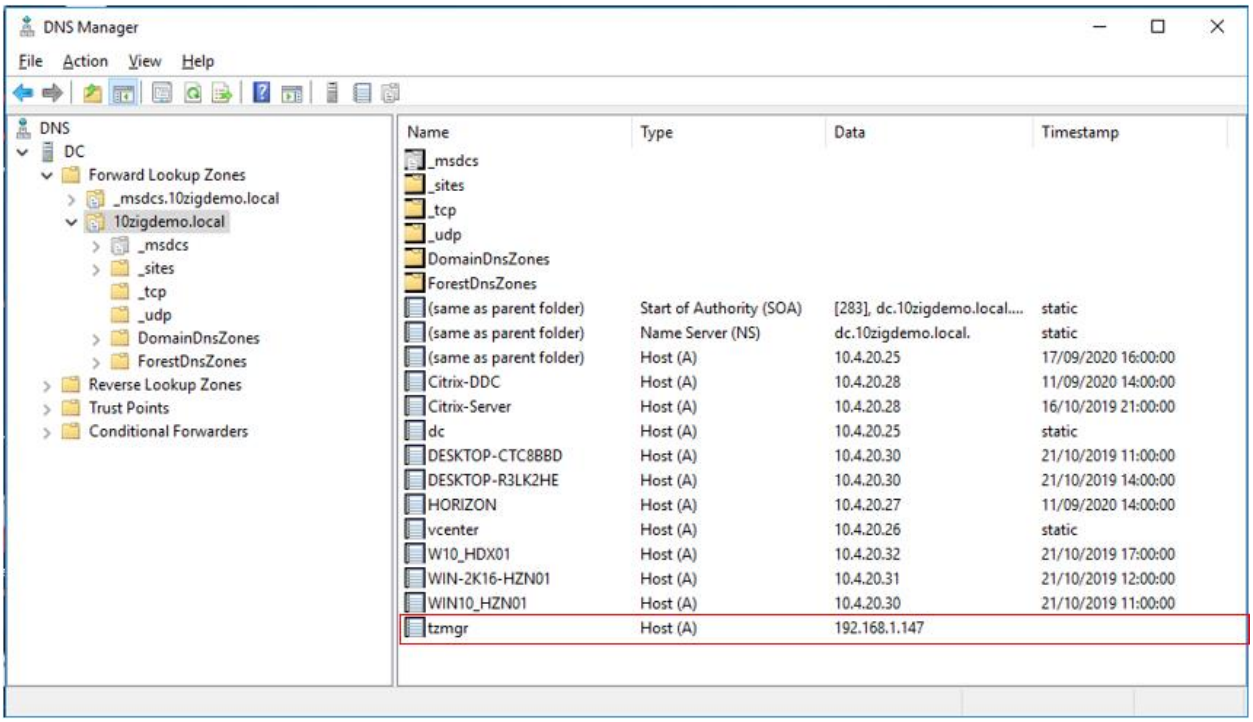


5. Specify the record details as pictured below (adjust for your own domain details and host addressing).
   a. Service: **_tzmgr_discovery**
   b. Protocol: **_tcp**
   c. Port number: Specify the port used by the Secure Connector (default **443**)

d. Host offering this service: Enter the host name of the server where the Secure Connector has been installed.

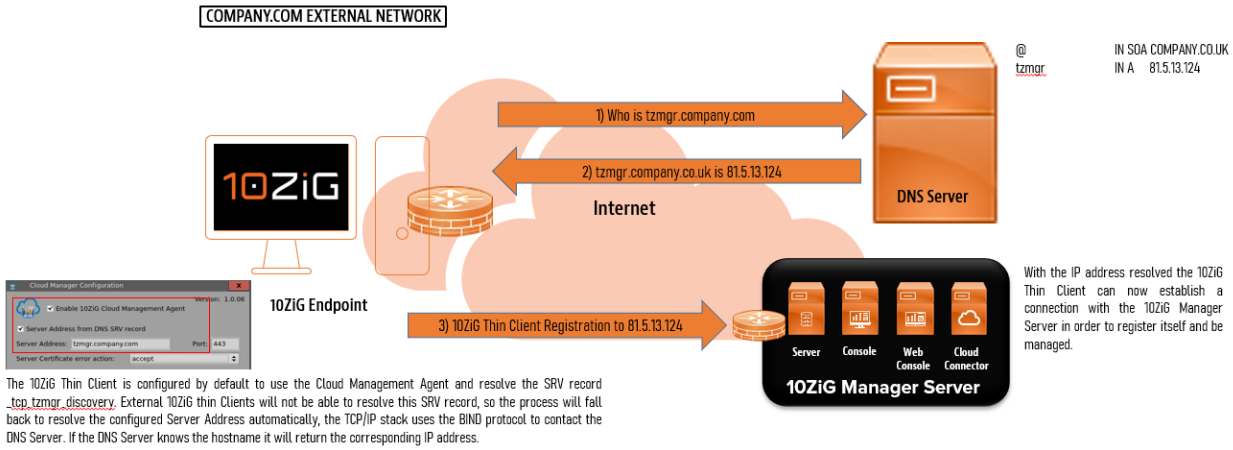


6. When you have completed the configuration press **OK** to close and add the new record.
7. You can then if you wish to check that the host name of the server where the Secure Connector has been installed has the required (A) record created for it. In this example we have one for **tzmgr** that resolves to 192.168.1.147 internally.



EXTERNAL DNS

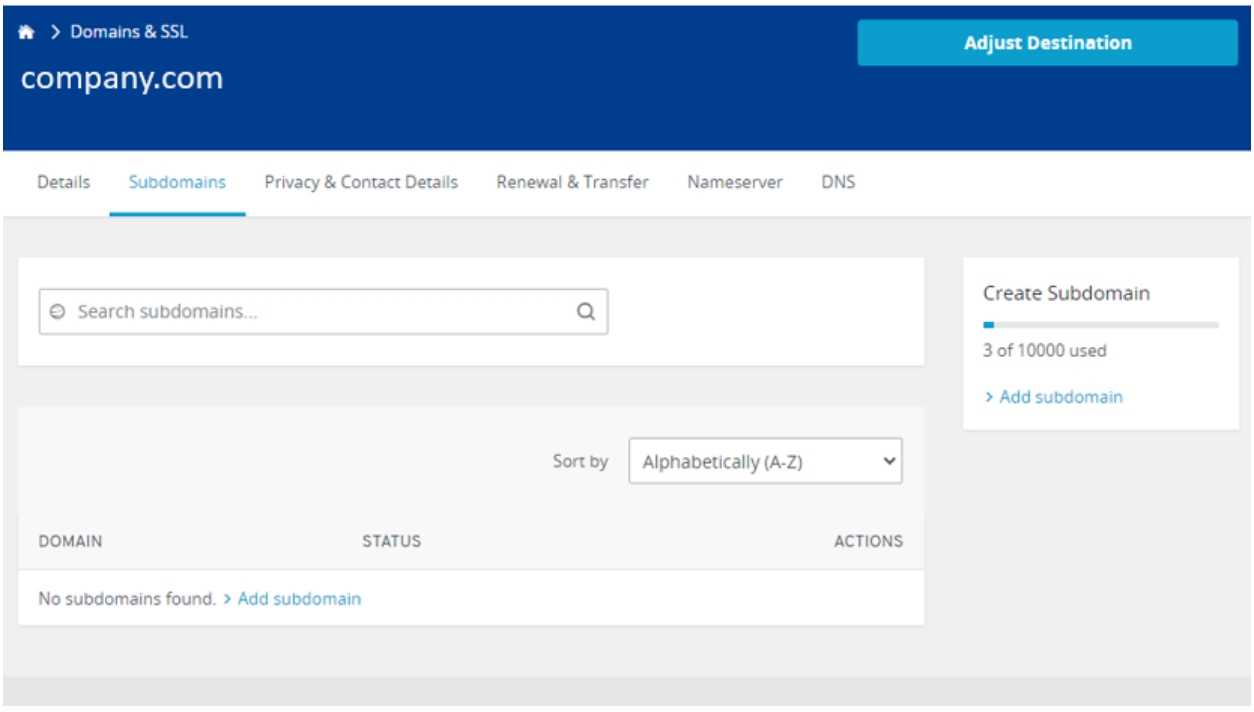
When access is required from a remote location, the connection can no longer be established directly to the 10ZiG Manager Secure Connectors internal IP address. Instead, the DNS address tzmgr.company.com should now resolve to the Public IP address of the WAN router connected to the 10ZiG Manager Secure Connector Server LAN network. This requires that the external Domain Name Server resolves pbx.company.com to the relevant Public IP address.



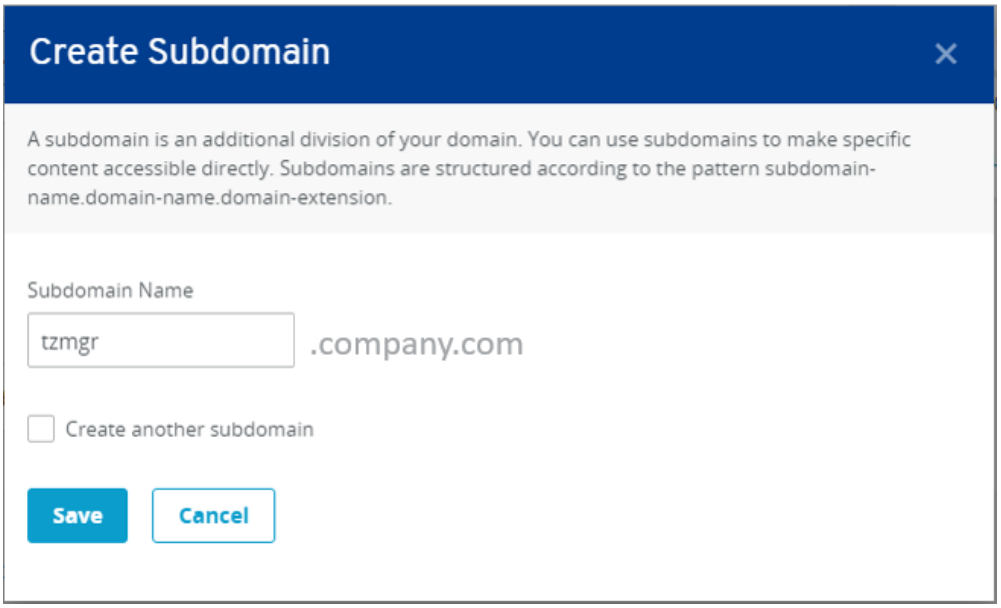
Since the 10ZiG Thin Client and 10ZiG Manager Secure Connector Server are no longer on the same network the connection is established through the WAN Router/Firewall, which will be configured for port forwarding to allow the 10ZiG Thin Client to register with the 10ZiG Manager Secure Connector Server.

CONFIGURE AN EXTERNAL DOMAIN NAME PROVIDER FOR REMOTE CONNECTIVITY

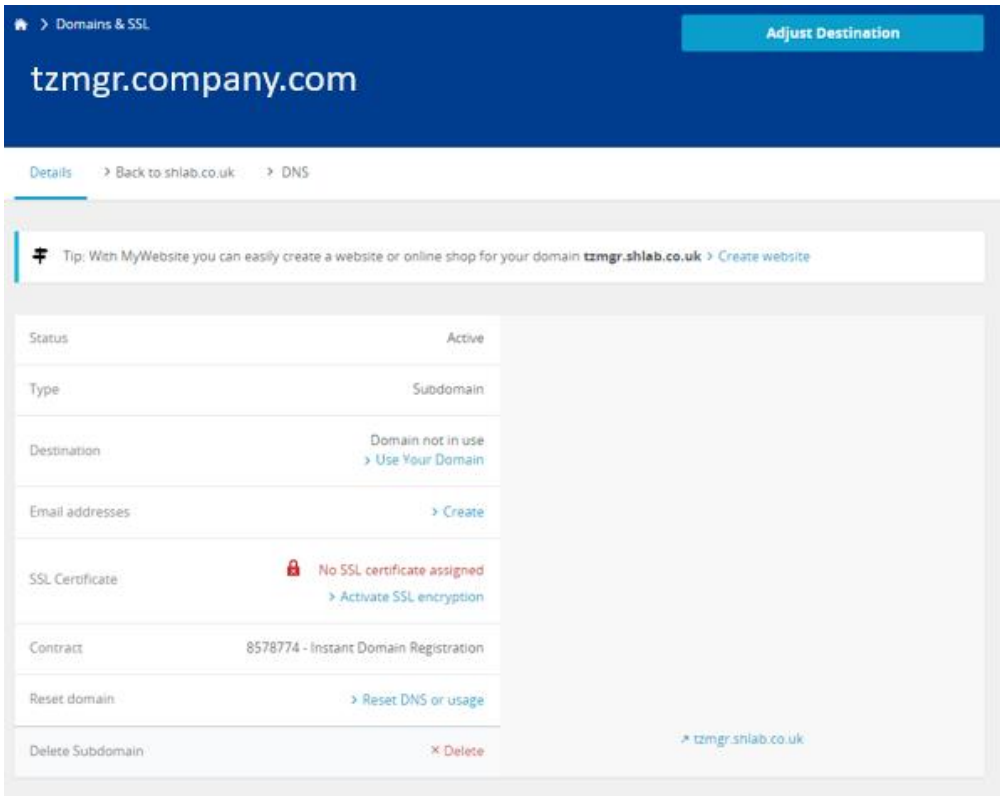
1. Login to your external Domain Name provider.



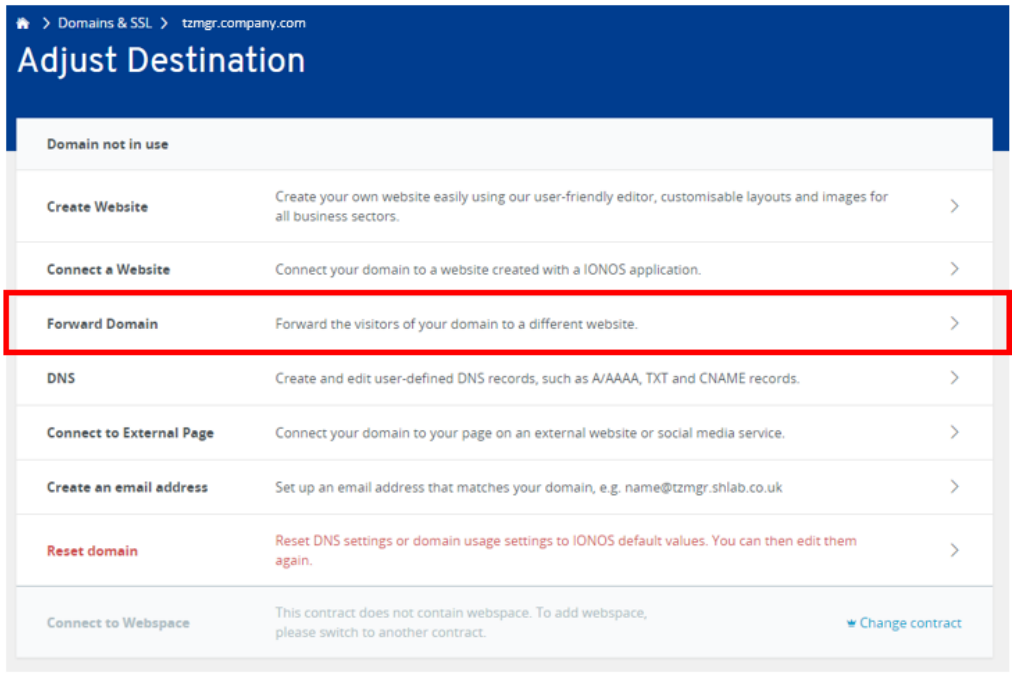
2. Create a Subdomain that will match the Hostname you are using. In this example we are using **tzmgr.company.com**.



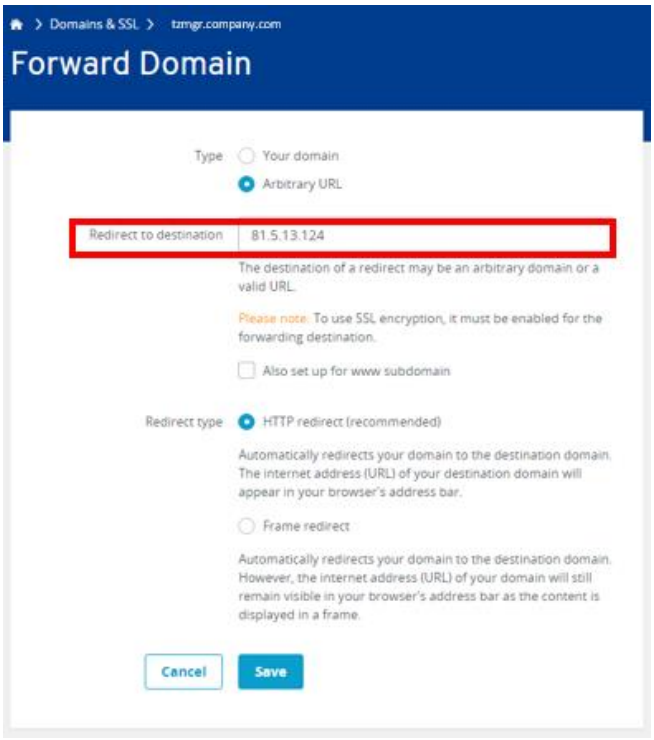
3. Next you will need to re-direct traffic destined for **tzmgr.company.com** to the Public IP Address of the WAN router connected to the 10ZiG Manager Secure Connector Server network.



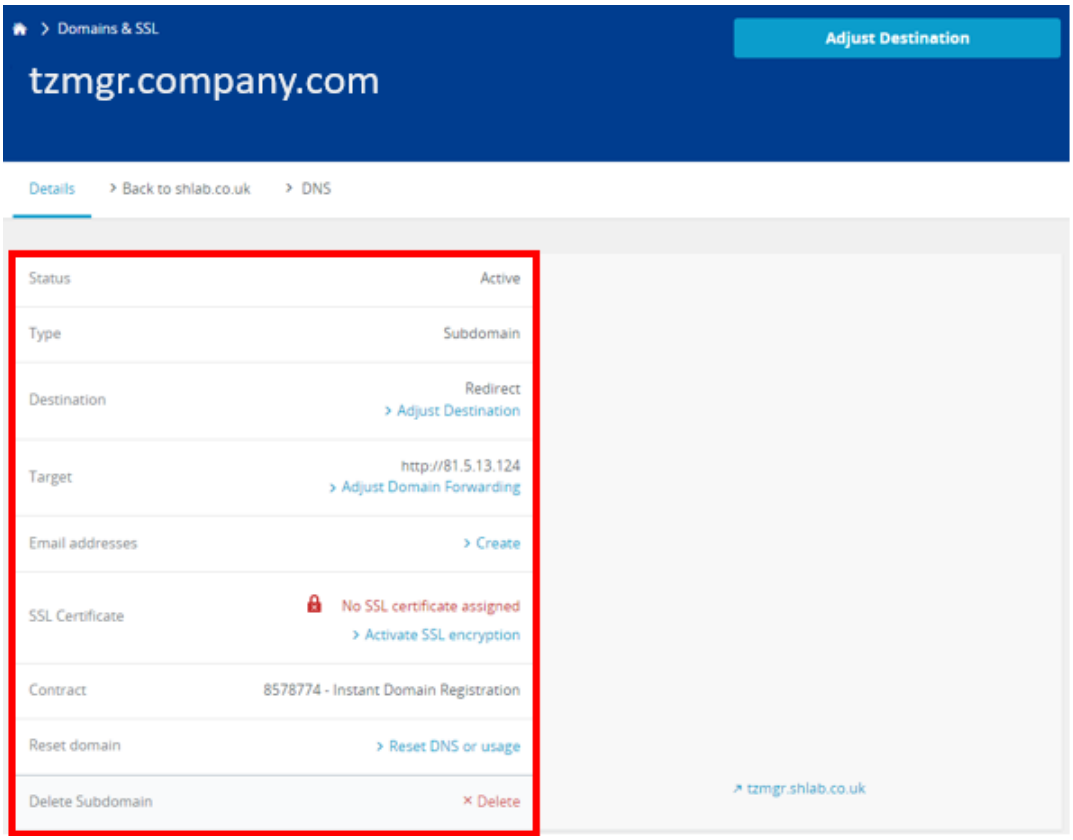
4. Select the option **Forward Domain**.



5. Enter the **Public IP Address of the WAN router** connected to the 10ZiG Manager Secure Connector Server network as the **Redirect Destination**. Press **Save** to update sub-domain destination.



6. The redirection should now be configured. Please note depending on the Domain name provider it may take some time for DNS changes to propagate fully.



NOTE: Configuration of external Domain Name services will vary depending on the provider you are using. Please refer to the providers specific documentation on implementing any of the above if differences in configuration are seen when trying to implement this.

THIS PAGE IS INTENTIONALLY BLANK