TECHNICAL SERIES

WORKLIST INFRASTRUCTURE

Original Software

T. DILLON

NOVEMBER 2021

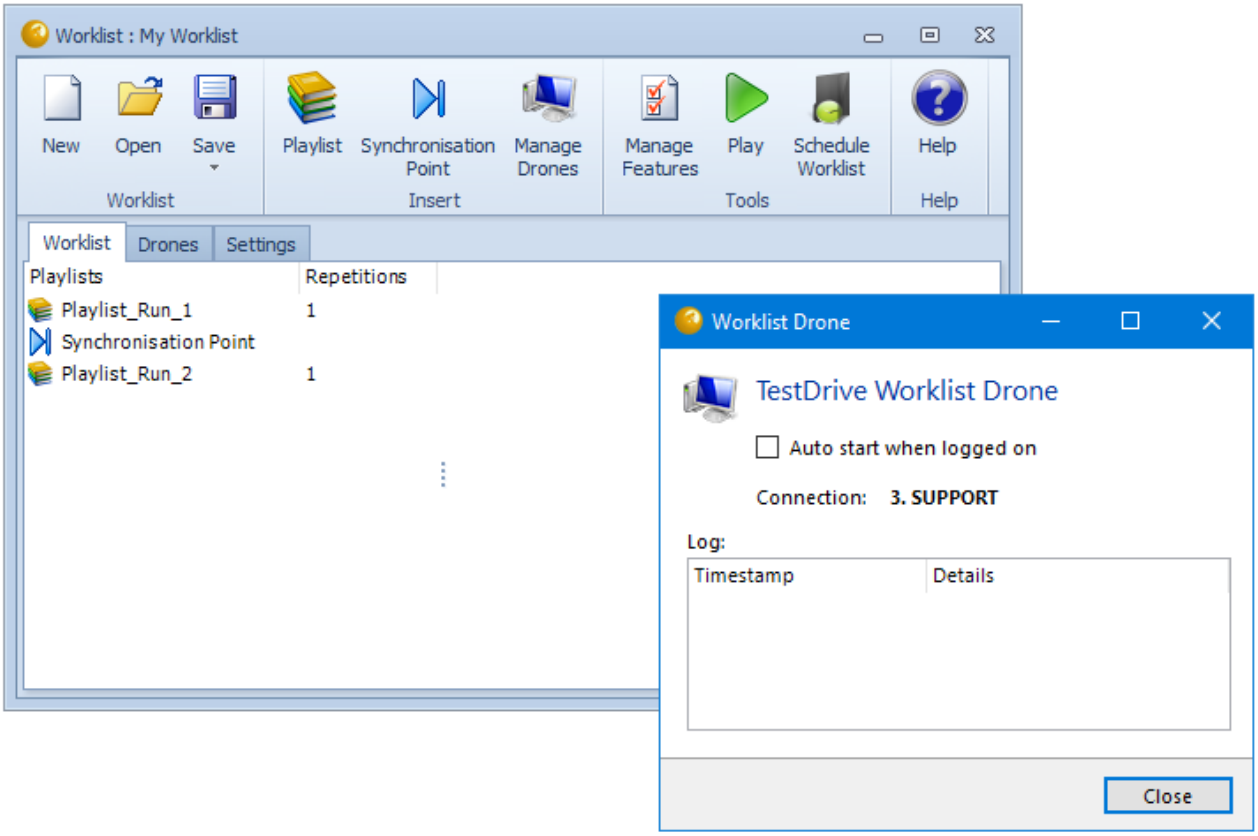
TABLE OF CONTENTS

SYNOPSIS

PURPOSE

The purpose of this document is to provide an overview of the Worklist solution and where possible offer information to assist when setting up the solution in a real-life environment.

Due to the number of potential environmental configurations, Firewalls, Network configurations, Operating systems etc., it is not possible to create a detailed guide that will work in all environments. Instead, the aim of this document is to provide guidelines and tips, advising of the type of things that need to be considered and where to look for potential problems with the implementation.

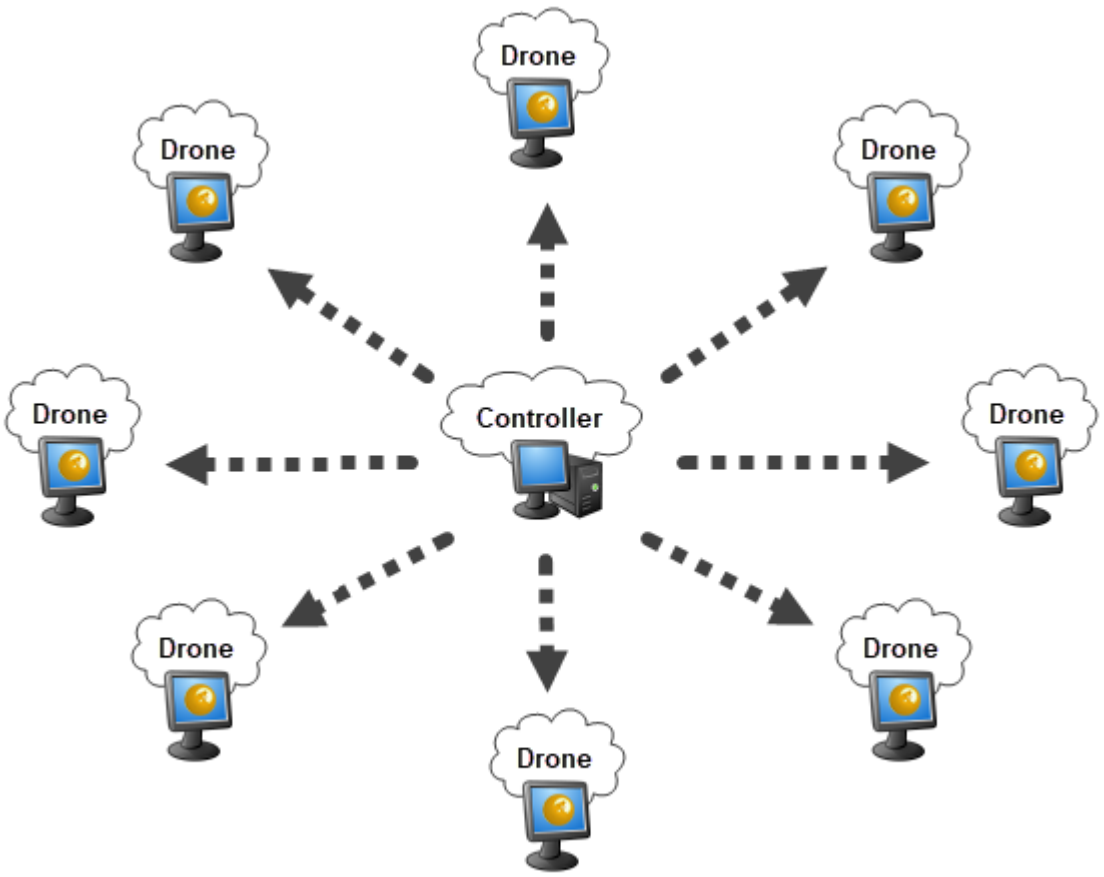


SOLUTION OVERVIEW

UNDERSTANDING WORKLIST

TestDrive is Original Software's solution to the ever-growing Automation requirements of its customer base. As more businesses move towards Agile/quicker to market methodologies, an increasing number of businesses processes will need to be automated. This then necessitates a higher frequency of regression runs and the need for automation and efficiency only grows stronger.

Worklists complement Original Software's UI Automation tool TestDrive and allow a single user to control multiple workstations to concurrently playback automated test cases, against different test environments on multiple client configurations all controlled from a single machine.



TECHNICAL OVERVIEW

WORKLIST MECHANICS

Worklists are executed via a Controller. The Controller is a machine with the Original Software solutions installed and the machine that will be used to execute the Worklist. The Controller communicates down to the Drones. Drones also require the Original Software solutions installed and must have the Drone software running to enable the Controller to recognise the machine as a Drone. Drones are the machines which will used to execute the automated tests.

Communication between Controllers and Drones is done via TCP/IP. TCP/IP communication works by uniquely identifying a machine with a combination of the IP Address and Port number, this means that each Controller and Drone will need a unique IP Address for this solution to work.

WORKLIST PORTS

Original Software uses a range of unassigned network ports for the Worklist solution. It is possible that other custom purpose-built software may be using some of the same ports which can potentially cause conflicts. This is unlikely and only becomes an issue if that software is also installed on the Controllers and Drones due to the way that:

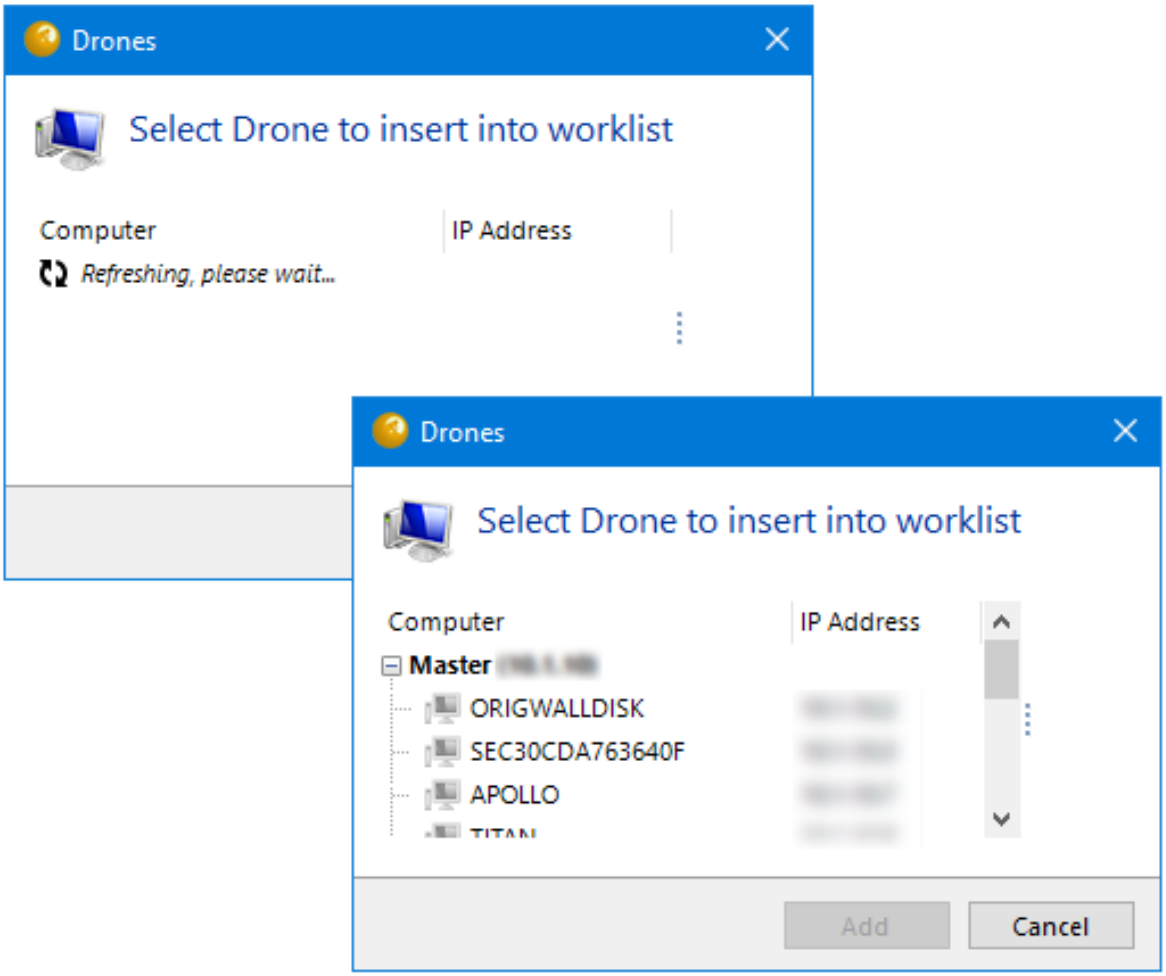
- The Controller opens port **8345** where it receives replies from the Drones.
- Each Drone opens port **8344** and listens for messages from the Controller.
- When playback starts the Controller opens an additional port for each Drone to send information through. These extra ports are **8345**+n where n is the index of the Drone. These additional ports will be closed at the end of playback.

Example for one Controller and five Drones:

As each Drone is started, port **8344** is opened to listen for messages. As the Controller is started, it will open and listen on port 8345. At playback time, the Controller will also open ports **8346**, **8347**, **8348**, **8349** & **8350**.

IP RANGES

When creating a Worklist and assigning Drones, the solution will scan the network within a specified IP range returning all the client machines in that range. The clients are then selected manually, and no further network scan is required. As a result, consideration should be given to assigning a range of IP addresses for the use of Worklists. This is not essential so long as the computer names in the Worklist can resolve to a unique IP.



INFRASTRUCTURE CONFIGURATION

CONFIGURATION GUIDELINES

The key part of using Worklists is ensuring that each Drone can be uniquely identified. As mentioned in the technical overview, this is done via a combination of IP Address and Port number. For a standalone machine this is straight forward to control by using DHCP in your network, however, for Citrix, Virtual Solutions and Terminal Services, this is somewhat a more complicated configuration point, but essential to understand and to get correct for the Worklist solution.

Original Software has other documentation specific to implementation of its product set and their requirements. **This current documentation refers to the use of Worklists only**.

PHYSICAL CLIENTS – RECOMMENDED IMPLEMENTATION

Physical Clients provide the best solution for Worklists. Having a physical client with its own network adapter, receiving its own IP Address from a networks DHCP server removes any dependencies on software. The only cause for conflicts now will be at the network level and much easier for the Infrastructure team to diagnose and resolve.

VDI SOLUTIONS – RECOMMENDED NON-PHYSICAL IMPLEMENTATION

Virtual desktop solutions flood the market with lots of software using the Remote Desktop Protocols. For this document, we will assume the virtual solution being used is VMware.

Consideration should be given to how the Virtual machines will be assigned an IP address. There are multiple ways to configure Virtual Machines with network access and again each will have its own advantages and dis-advantages. The most used methods are listed below:

- Host-Only networking
- Bridged networking
- Network Address Translation (NAT)

Host-Only is not an option for Worklists as this solution tends to assume only a single operating system will be running and therefore shares the Ethernet connection from the host and the IP Address with it. Information on Host-Only can be found below.

- http://www.vmware.com/support/ws55/doc/ws_net_configurations_hostonly.html

NAT means that the VM will obtain an IP from the virtualization software's DHCP server. However, the host IP address is used for connection to the network, so Worklists must rely on the Virtualization software to intercept messages and relay them to the correct VM. This should only be used where the VM's cannot be assigned an IP on the required network. The Controllers and Drones must be on the same network. Information on NAT can be found below.

- http://www.vmware.com/support/ws55/doc/ws_net_configurations_nat.html

Bridged networking allows the VM to obtain its IP Address from your networks DHCP server essentially making it just another LAN pc. This makes it the best solution not just for Worklists but for many other software solutions. Information on Bridged networking can be found below.

- http://www.vmware.com/support/ws55/doc/ws_net_configurations_bridged.html

CITRIX

There are many different methods of delivering through Citrix. Each has their own advantages and dis-advantages. The most common methods are listed below –

- Published Desktops.
- Published Applications.
- Streamed Applications/Desktops.

Whatever methodology of Citrix is being/has been implemented, it will need to be compatible with IP pooling or virtual IP addressing or a similar solution. Some information can be found below on IP pooling. The Citrix knowledge base contains more detailed information on both IP pooling and virtual IP addressing.

- https://docs.citrix.com/en-us/netscaler-gateway/12/vpn-user-config/configure-plugin-connections/ng-plugin-ip-pooling-overview-con/ng-plugin-ip-pooling-config-tsk.html

TERMINAL SERVERS

Terminal Services are common in the workplace. Windows Servers do not currently have a solution to deal with served desktop's requiring unique IP's, at least no added feature to deal with this requirement.

Static IP's must be assigned in the registry of the Server. These IP's are then used for Remote Desktop IP Virtualization and each new served desktop should be assigned one of these upon connection. It may be necessary to ensure that the DHCP server is not assigning the same IP Address's as this may cause network conflicts and cause the Worklist to fail in its attempts to communicate with its Drones.

- https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ee382306(v=ws.10)

ALTERNATE CONSIDERATIONS

PC SECURITY SOFTWARE

There are many different forms of security software, and most are highly configurable. In an enterprise organization it is likely that this software is installed and managed at a global Infrastructure level and not individually per client, so consideration should be given to ensuring that the Controller and Drones will be able to open and communicate through the correct ports. Some software may allow configuration so that a said piece of software can communicate at will across the network without any other configuration required. In others you may need to add specific ports or a port range to allow communications through the network.

WINDOWS FIREWALL

Windows 7/8/10 have a built in Firewall that can stop the communications through the required ports. Specific rules can be configured to allow/block incoming and outgoing communications. It is possible that these rules may need to be configured to allow communications through the specific ports. It is also likely that you will need a local admin account to apply any changes. Again, at an enterprise organization it is likely that these Firewall settings are controlled at a global level by group polices.

Original Software attempts to add the required entries to the Windows Firewall upon opening of the software but this relies upon the connecting user having the access to amend the Firewall.

WORKLIST DRONE CONFIGURATION

WORKLIST (WORKLIST DRONE) SETUP

With the Worklist Infrastructure knowledge understood, you may be looking to setup Worklist (Worklist Drone) and implement into your organization. To achieve this, you will need to refer to the Worklist Drone Configuration document with the other Technical How-To documents.

- https://origsoft.com/pauple_helpie/worklist-drone-configuration/