PC-Duo Remote Control Networking Requirements V11.10.2 through v13.1

PC-Duo Remote Control Editions

The PC-Duo product line includes several different software components that are packaged into (and licensed as) different Editions. The networking requirements for each component are described in the Edition that introduces the component. The requirements are *cumulative*, in that each subsequent Edition discussed includes the features and capabilities – and requirements and limitations – of the earlier Editions.

Workstation Edition

The PC-Duo Workstation edition allows installed Masters to connect to installed Hosts via a direct, peer-to-peer connection.

This scenario requires direct IPv4 or IPv6 connectivity between the machines. UDP is the preferred protocol (which enables polling for Hosts), but TCP can be used if the IP address or DNS name of the target machine is known.

The software installers configure the Windows Firewall to unblock the products; if a different firewall software is used on the machine, it may need to be manually configured to allow access.

The Master starts connections from a dynamically allocated port. The Host listens for connections on a specific port. The default is 1505, but is configurable in Host settings.

Gateway Edition

The PC-Duo Gateway edition allows installed Masters to connect to the Gateway Server, and connect through that server to Hosts which can also communicate with the Gateway server. There is no direct network connection from Master to Host.

This scenario requires direct IPv4 or IPv6 connectivity from every Master and every Host to the Gateway Server only. A variety of protocols are supported (UDP, TCP, SSL, WebSocket (WS), and Secure WebSocket (WSS)). The IP address or DNS name of the Gateway Server must be known to the Masters and Hosts.

The software installers configure the Windows Firewall to unblock the products; if a different firewall software is used on the machine, it may need to be manually configured to allow access.

Connectivity TO the Gateway Server from Master and Host is as follows. The Master starts connections from a dynamically allocated port, and connects to the Gateway Server on its specific port. The Host starts connections either on a dynamically allocated port, or in certain cases, from its configured listening port (default 1505). The Gateway specific port defaults for UDP, TCP, WS is port 2303; for SSL and WSS the default port is 443 (in v12 and earlier); this is changed to default to 8443 in v13. (Obviously, a port other than 443 must be used if PC-Duo Web Console is used or if another application on the server needs HTTPS/443.) All ports can be configured in Gateway settings. This connection requires direct IP connectivity from the Master and/or Host to the Gateway. Although our implementations of WS and WSS are HTTP-compliant, PC-Duo does not implement a full HTTP stack, nor provides a browser engine on the endpoint, so any web proxy, firewall, or SSL VPN solution that requires its own authentication or otherwise doesn't pass the connection straight through will not work. Additionally, the web proxy, firewall, or other network infrastructure must support the WebSocket standard.

There's an additional consideration for Host <-> Gateway connectivity. The minimum requirement is that there is direct connectivity from Host to Gateway. If there is additionally direct connectivity the other way – from Gateway Server to Host, as

would be typical on a LAN – then the Gateway Server can connect to the Host at will, and it does not need to keep a "reverse connection" at all times to maintain connectivity.

Note very well that the determination of whether a reverse connection is needed or not is *not* done by testing connectivity. The Gateway Server must be configured with knowledge of the "local network address ranges" that it can reach directly; the default is all private IP address ranges.

The Gateway Server 13.5 has a limit of 8000 reverse connections (2000 if GWS 13.4 or earlier and 1000 if GWS v12 or earlier is running on a 32-bit edition of Windows Server), so if no Hosts can be directly reached from the Gateway Server, that's the limit on the number of Hosts the Gateway Server can manage. If the Hosts can be directly reached (on the LAN) and no reverse connection is used, the Gateway Server can manage up to 10,000 Hosts.

PC-Duo Web Console

The PC-Duo Web Console pairs the Gateway Server (from the Gateway Edition) with a browser-based administration and access portal called the Web Console. The Web Console also includes a Master replacement called the Connection Window, and a Host replacement called the Host on Demand, which are deployed through Microsoft Click-Once deployment, so no preinstalled software is necessary on the clients.

PC-Duo v13.0 and later: The PC-Duo Server v13 has discontinued the Gateway Edition, and all Server installations are PC-Duo Web Console. That is, a PC-Duo Server v13 installation must include a Gateway Server, a Web Console, and a new component called Identity Manager. That said, all the information in the Gateway Edition description above, regarding the Gateway Server component network connectivity and limitations, remains relevant to the PC-Duo Web Console (which adds the Web Console component, but doesn't change the Gateway Server component.)

Access to the Web Console is always via HTTPS protocol (default 443, but reconfigurable), and because it's browser-based, all web proxy, firewall, SSL VPN, etc. technologies should work and allow access to the Web Console.

However, the Microsoft Click-Once deployment have additional considerations. Specifically, click-once deployment cannot work with an "untrusted" SSL certificate.

PC-Duo v13.0 and later: Because browsers are deprecating support for untrusted SSL certificates, PC-Duo v13 is designed to work primarily with trusted SSL certificates, and does not support serving the On Demand applications over HTTP. Instead, the Gateway > Network page can be used to configure delivery of these from Proxy Networks-provided public cloud web hosting.

PC-Duo v12: To work around the Click-Once requirement, the default Web Console installation provides access to the Connection Window (CW) and Host on Demand (HOD) via HTTP on port 80 (by default). This can be reconfigured to work over the same HTTPS port as the main Web Console, but only if the SSL certificate used there is trusted by all clients that will be accessing these applications. (Typically, this means the certificate is from a trusted third party like Verisign, or it's a corporate CA-issued certificate and all clients are machine that are members of the domain.)

Finally, Host on Demand has an additional consideration. The application files are delivered via click-once deployment, but a configuration file is fetched from the same URL as the applications files were deployed from, once the HOD starts up. Because this runs as a separate process and is not browser-based, web proxy, firewall, and SSL VPN technologies that provide session or cookie-based access will not recognize this as a valid request and will block it, causing HOD to fail to start. An alternative is to use "inline" delivery of Host on Demand settings (a configuration choice in the Web Console); this avoids the additional HTTP/HTTPS request for the Host settings, but means that saved/persisted shortcuts to the HOD will not automatically get the latest settings.

Once any issues with deploying the CW or HOD are resolved, these applications still have the same requirements as the installed Master and installed Host in terms of connecting back to the Gateway Server. Specifically, they need direct connectivity to the Gateway Server on a configurable protocol and port.

PC-Duo v13: This configuration is controlled in the Web Console, Gateway > Network Settings tab, Gateway Server Access sections, with separate configurations for internal and external access.

PC-Duo v12: This configuration is controlled in the Web Console, Gateway > Web Console Settings tab, Application Access sections, with separate configurations for internal and external access.

Additional Network Connectivity Considerations

Active Directory Domain Relationships

The server(s) that the PC-Duo Server software is installed on are typically domain-joined, to allow clients to use their domain credentials to authenticate to the system. The systems that are domain-joined must have appropriate connectivity to a domain controller.

PC-Duo v13.0 and later: PC-Duo v13 supports installing all Server components on a single computer that is not domain-joined, and linking the Identity Manager to Azure AD for client authentication.

PC-Duo v13.0 and later: PC-Duo v13 Server requires a Microsoft SQL Server database instance. This instance can be run on a different server, and can even be in SQL high-availability cluster. However, all Server components (Gateway Server, Web Console, and Identity Manager) must have appropriate connectivity to the SQL Database instance. In v13.0, only Windows Authentication is supported to authenticate to the SQL instance, so the machines must all be domain-joined and the services must be running as domain accounts if SQL is off-box. The only supported non-domain installation choice is to have all services (including SQL) running on the same machine using machine-local accounts.

Intrusion Detection Systems (IDS)

Because the Host software is widely deployed within the network, and all of these machines report status to the central Gateway Server, some intrusion detection systems (IDS) may mistake this network activity for a botnet with a command-and-control server – because at the network transport level, that is what it looks like. These systems can disrupt the network connectivity required for PC-Duo to operate correctly, and cause hard-to-diagnose behaviors. PC-Duo software cannot identify when this happens, because the software only sees unexpected network connectivity problems. The most common symptom of this problem is that Hosts are configured to report to the Gateway Server, but either cannot, or do so erratically. Because it's typically the case that the initial network connection is allowed, but then is disrupted by the IDS, the Host CPL may not report an error – the Host knows it successfully established a connection to the Gateway Server – but errors will appear in the Gateway Server audit logs related to the Host status processing events.

If a network environment is known to have an Intrusion Detection System, this document should be shared with the responsible person(s) to ensure the IDS recognizes and allows legitimate PC-Duo network traffic.

Forward (Client) Web Proxy Support

PC-Duo Master (and other clients) and Host running on Windows can connect to a Gateway Server through a web proxy under specific circumstances. This section describes the requirements for web proxy support to work.

Web proxy support only affects the PC-Duo transport when making a WS or WSS (WebSocket over HTTP or HTTPS) connections – these are the only PC-Duo protocols that are HTTP-compliant and therefore can be tunneled through a web proxy.

PC-Duo Master (and other clients): PC-Duo client software runs as the console user, and obeys Windows settings and configuration applied to that user. Specifically, the system Control Panel > Internet Options > Connections > LAN settings configuration is used, along with the system Web Proxy Auto-Discovery (WPAD) protocol, to determine web proxy settings. To minimize delays in completing connections, PC-Duo simultaneously makes Windows API calls to detect the web proxy settings, while it attempts to make a direct connection to the Gateway Server. If the direct connection fails, the web proxy configuration is used to retry to connection through that web proxy.

PC-Duo Host: The Host software uses the same underlying logic as the Master and other clients, and when run as a Session-based Host on Demand, has identical behavior. However, because the installed Host runs as a service, there is no per-user configuration available, and WPAD is the only effective means of configuring the web proxy.

SQL Server Management Studio

PC-Duo v12 and later use a SQL Server database instance to store critical data, and in PC-Duo v13 and later, it is sometimes helpful to be able to review, or edit, information in the database. Microsoft's SQL Server Management Studio (v17 and later) is now a separate installation from SQL Server. The latest version can be downloaded from https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-2017.

Redirecting HTTP to HTTPS

PC-Duo Web Console must always be accessed via HTTPS for security reasons. On the LAN, especially, users may inadvertently end up at the server via the HTTP protocol (on the default port 80). The default installation of IIS has the "Default Web Site" bound to HTTP port 80, and has a placeholder page that is not useful to end-users. This section discusses two techniques for redirecting users that would otherwise end up on this placeholder page to the actual Web Console application on HTTPS port 443 (or other appropriate port).

No Other Use of HTTP on Server

In PC-Duo v13 and later, and PC-Duo v12 and earlier if using a trusted SSL certificate and configured for all access to be over HTTPS, there is no need for the "Default Web Site" and no use of HTTP. In this case, a recommended configuration change is to repurpose the "Default Web Site" to redirect HTTP connections to the Web Console application.

1. Rename the "Default Web Site" web site to be "Redirect HTTP to HTTPS" for clarity, and as a reminder that that is the functionality of this site.
2. Ensure the site bindings are for HTTP port 80 only. No other bindings should be present.
3. In IIS Manager, select this site, and in the IIS section double click "HTTP Redirect" to configure the redirection.
    a. Check the box "Redirect requests to this destination", and enter the full URL of the Web Console application, e.g. https://server.example.com
    b. Check the box "Redirect all requests to exact destination"
    c. Uncheck the box "Only direct requests to contents in this directory (not subdirectories)"
    d. Set Status code to "Permanent (301)".

This ensures any users reaching the web site via HTTP are redirected to the Web Console landing page.

HTTP Used on Server for WCAPPS Access (PC-Duo v12 and earlier)

In PC-Duo v12 and earlier, the Web Console helper applications (Host on Demand, ClickOnce deployed Connection Window, etc.) may be made available over HTTP. That functionality can be preserved, while still redirecting users who navigate to the web site root on HTTP to the Web Console landing page via HTTPS.

1. Rename the “Default Web Site” web site to be “WCAPPS with Root Redirect” for clarity, and as a reminder that that is the functionality of this site.
2. Ensure the site bindings are for HTTP port 80 only. No other bindings should be present.
3. In IIS Manager, select this site, and in the IIS section double click “HTTP Redirect” to configure the redirection.
    a. Check the box “Redirect requests to this destination”, and enter the full URL of the Web Console application, e.g. https://server.example.com
    b. Check the box “Redirect all requests to exact destination”
    c. Check the box “Only direct requests to contents in this directory (not subdirectories)”. This is very important, and different from the above configuration – this allows the WCAPPS subdirectory to be accessed via HTTP.
    d. Set Status code to “Permanent (301)”.

Important Note Regarding IIS Web Site Configuration

IIS configuration is hierarchical, with global settings established at the server node, and per-web site settings established for each Web Site listed in IIS Manager. Note well that the web site settings are stored in the “web.config” file at the physical path set in the web site “Basic Settings”. The means that if multiple web sites share the same physical path, configuration changes to one site affect the other site. Because this is generally not the intended behavior, do not create additional sites that reference the same physical path. Specifically, the “Default Web Site” normally has a physical path of “C:\inetpub\wwwroot”; that path should not be used if you create an additional site (e.g. for Application Request Routing rewrite rules).

Multiplexing WC and GWS with HTTPSYS (in v13.1 and later)

In PC-Duo v13.1 and later, the Web Console and Gateway Server can share the same port(s), normally port 443, for access. This is possible in PC-Duo v13.1 due to the introduction of HTTPSYS support in the Gateway Server.

This support leverages the “HTTP.SYS” kernel-mode driver in Windows, and allows the Gateway Server to register with this driver to handle Web Socket connections on a specific URL (“/ws/gws/”) that does not conflict with the Web Console. The Gateway Server effectively piggy-backs on the Web Console configuration in IIS, and client connections using the PC-Duo WSS protocol to the port(s) configured for Web Console are routed by the HTTP.SYS driver to the Gateway Server.

This feature is only available when both Web Console and Gateway Server are installed on the same computer. It is configured in the Web Console, on the Gateway > Gateway Settings page, Protocols section. The only configuration is to Enable or Disable the feature; it is enabled by default when WC and GWS are installed on the same machine.

Important Note: Not all versions of PC-Duo Host are compatible with using the WSS protocol to connect to the HTTPSYS protocol support; earlier versions of Host work with the Gateway Server native SSL support, but do not meet the stricter HTTP standard compatibility requirements of the HTTP.SYS kernel driver. As a result, only the following versions of PC-Duo Host can reliably be managed by the Gateway Server when reporting on WSS to the HTTPSYS port:

- Host v13.1 original release and later
- Host v13.0 Hotfix #3 (and later)
- Host v12.0.1 Hotfix #8 (and later)

This support is sufficient to meet the needs of an environment where the only configuration goal is to expose the PC-Duo Server on a single port/point of access. If there are more advanced requirements, including application-layer filtering of the

request/data, then an application layer firewall (acting as a reverse web proxy) may be necessary. The remainder of this document discusses how to configure PC-Duo Server to work with a reverse web proxy.

Multiplexing WC and GWS with a Reverse Web Proxy

In PC-Duo v11.10.2 and later, the Web Console and Gateway Server can share the same port, normally port 443, for access. This is made possible by using a "reverse web proxy" to field the initial connection, and then forward the connection to the correct back-end service. This section briefly provides an overview of this, and the following section describes specifically how to set this up using Microsoft Application Request Routing.

Note that this section discusses a "reverse web proxy" scenario. This scenario is explained on Wikipedia (https://en.wikipedia.org/wiki/Reverse_proxy) reasonably well, and should not be confused with the forward- or client-side proxy scenario. The reverse web proxy scenario involves software (like Microsoft ARR) or an appliance (like an application firewall or load balancer with this functionality) that is placed near the PC-Duo Server to act as a front-end. Clients connect to the reverse web proxy, and the reverse web proxy forwards connections (as appropriate) to the Web Console and Gateway Server services of the PC-Duo Server.

The following requirements must be met for successful operation:

1. The reverse proxy must support HTTPS connections and support the WebSocket standard, including binary WebSocket.
2. The reverse proxy must insert the "X-Forwarded-For" header into the forwarded data stream.
3. All communications with the Gateway Server (from Masters and Hosts) must be via the Secure WebSocket (WSS) protocol. This protocol is HTTP-compliant, and is the only Gateway-supported protocol that can be multiplexed with the Web Console HTTP(S) traffic.
4. The reverse proxy must forward requests with the URL "/ws/gws/" to the Gateway Server. It can do this via HTTPS to whatever port the Gateway Server is listening for SSL connections on, or it can do this via HTTP to whatever port the Gateway Server is listening for TCP connection on (normally 2303). All other requests must be forwarded to the Web Console via HTTPS.
5. The PC-Duo Server must be configured so that the IP address of the reverse proxy is listed in the "Trusted Device list". This allows PC-Duo to trust the "X-Forwarded-For" header and report the actual client addresses in Activity and Analytics views. This list must include the address(es) tha that the reverse web proxy uses to forward traffic to the PC-Duo Server components, and may include both IPv4 and IPv6 addresses.
6. The PC-Duo Server must be configured so that the PIM and WC URLs (in PIM Settings) refer to the reverse web proxy server. The recommended configuration is for all traffic (both internal and external) to the PC-Duo Server to be routed through the reverse web proxy. Other configurations are possible, but are outside of the scope of this document.

Multiplexing with Microsoft ARR

Microsoft provides a feature for Internet Information Services (IIS) called Application Request Routing (ARR). This feature acts as a reverse web proxy, allowing the component to field the initial client connection and then forward the request to different back-end services as appropriate. This can be used to multiplex Web Console and Gateway Server, and have the requests routed to the correct service.

This can be done by using ARR on a separate machine (possibly in a DMZ or other restricted networking environment) to forward WC and GWS connections to other machines, or can be configured entirely on one server.

Requirements

The following requirements must be met:

- Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016 must be used to host IIS with AAR. No earlier versions of Windows are supported. The walkthrough section of this guide was written against Server 2012 R2.
- Microsoft Application Request Routing version 3 or later is required. Earlier versions did not provide support for the WebSocket standard, which the Gateway Server uses.
- PC-Duo Gateway Server v11.10.2 or later must be used.
- All communications with the Gateway Server (from Masters and Host) must be via the Secure WebSocket (WSS) protocol. This protocol is HTTP-compliant, and is the only Gateway-supported protocol that can be multiplexed with the Web Console HTTP(S) traffic.

PC-Duo v13.0 and later: PC-Duo v13 introduces a new component, the PC-Duo Identity Manager. This is a web application that is normally installed co-located with the Web Console, and the installation instructions that follow assume that these are installed on the same machine (along with the PC-Duo Gateway Server). However, configurations where these components are installed on different machines are possible, but would require appropriate changes to the reverse proxy configuration.

PC-Duo v13.0 and later: The Identity Manager component uses URLs that have prefix "pim/". This can be turned into a regular expression URL pattern for an ARR rule as "pim/.*".

Technical Background

The Application Request Routing (ARR) component is a reverse web proxy that is configured with rewrite rules to redirect traffic as appropriate and to provide a single point of entry for the clients.

PC-Duo v13 and later: For both single-server and multiple-server installations, all connections must be HTTPS/SSL, and the SSL certificates in use must be trusted on all machines. The latter is easiest to accomplish with either a third-party trusted certificate, or with a domain-issued certificate in an AD domain environment.

PC-Duo v12 and earlier: For single server installations, and for multiple-server installations where the networking between the servers is fully trusted, the recommended configuration is to have ARR terminate the client HTTPS (SSL) connection, and then make an unencrypted HTTP (TCP) connection to WC or GWS.

For installations where all network traffic should be encrypted, the recommended configuration is to have ARR terminate the client HTTPS (SSL) connection, and then make an encrypted HTTPS (SSL) connection to WC or GWS. This requires the SSL certificates in use must be trusted on all machines.

Single Server Installation – PC-Duo Server Setup

The following steps describe the additional steps necessary to setup and configure ARR on a server along with PC-Duo Server Web Console and Gateway Server. The first phase simply sets up the base machine and PC-Duo.

1. Set up machine with Windows Server 2012, Server 2012 R2, or Server 2016.
2. Join the machine to the domain, if this is a domain environment. WC+GWS can run standalone, but then only local machine accounts can be used for authentication. (**PC-Duo v13:** Azure AD can be used for client authentication as well.)

The next installation steps differ in PC-Duo v13 and later versus PC-Duo v12 and earlier.

For PC-Duo v13:

3. Use the "PC-DuoServerProducts.exe" installer which installs all of the product prerequisites and the PC-Duo Server product itself. Use the following configuration parameters when installing the product:
    a. Bindings: configure Web Console/IIS use 8443, and Gateway Server to use 8444. Do not use port 443; this is reserved for multiplexing.
    b. DNS Name and SSL Certificate: the system should be set up with the name that the ARR installation will use to access the WC and GWS; on a single server installation, this should be the machine name (as a fully-qualified name), even if the system will eventually be accessed by a different name.
4. Recommended but not required: In Server Manager, add or modify the Role "Web Server (IIS)". Under Web Server (IIS) > Web Server, add "Health and Diagnostics > Tracing". This adds diagnostic capabilities that are helpful if the ARR rules don't process as expected. (**PC-Duo v13.1:** this feature is automatically installed by the ServerProducts installer.)

The preceding steps set up the PC-Duo Server v13 for HTTPS access on an alternate port (8443) and Gateway Server for SSL/WSS access on port 8444. Now we can install and configure Application Request Routing. Note in the instructions below, the italicized *machinedns* marker should be replaced with the fully qualified DNS name of the machine that was selected during installation and that matches the SSL certificate in use by WC and GWS.

For PC-Duo v11.10 and PC-Duo v12:

3. Install prerequisites required by PC-Duo and ARR:
    a. Internet Information Services (IIS). In Server Manager, add Role, "Web Server (IIS)". In Web Server Role Services, start with the defaults, and add "Common HTTP Features > HTTP Redirection", "Health and Diagnostics > Tracing", "Security > Basic Authentication", "Security > Windows Authentication", "Application Development > .NET Extensibility 4.5", "Application Development > ASP.NET 4.5" (which adds ISAPI Extensions and ISAPI Features), "Application Development > WebSocket Protocol".
    b. Microsoft SQL Server 2008R2 or later ("Express 2012 sp1 with tools" recommended). In Feature Selection, uncheck "SQL Server Replication", "Client Tools SDK", and "SQL Client Connectivity SDK", as these are not needed.) Install a named instance (e.g. "SQLExpress". Authentication Mode must be Windows authentication mode, and ensure the right user(s) are listed under "Specify SQL Server administrators". Note: the database server can be installed standalone, but you may need the SQL Management Studio installed on another computer to confirm or adjust the SQL Server installation. Installing "with tools" puts the management tools on this computer for convenience.
    c. Note that .NET Framework v4.0 or later is included in the OS install.
4. NOTE WELL: Do *not* use IIS Manager to delete the default web site. Web Console installer will create a virtual "wcapps" directory in the default site to access the click-once applications.
5. Install Gateway Server, running as an appropriate identity (e.g. domain\RemoteControlGateway). Note that no configuration of the GWS is required: the default configuration (listening on UDP 2303 and TCP 2303, with SSL not enabled) is correct.
6. Install Web Console. Log in to establish your account as the "first administrator".
7. Use IIS Manager to reconfigure "PC-Duo Web Console" site to bind to HTTPS on a port other than 443 (recommendation: 8443), and also ADD a binding for HTTP on another port (recommendation: 8080). Reconfigure the default web site to *add* a binding for HTTPS to port 443 (and leave the binding for HTTP port 80).
8. Install a trusted third-party certificate, if desired and available, or install a corporate CA-issued certificate if desired and available. If not, use the self-signed SSL certificate created by IIS. Use IIS Manager to ensure IIS is configured to use the correct/desired certificate on all HTTPS bindings.

9. Configure Web Console Setting: in WC > Gateway > Web Console Settings, enable HOD (if desired), and configure "Remote Desktop URL" in both "Application Access - Internal" and "Application Access – External" to be the correct URL (with appropriate machine name/DNS name for the server, using HTTP if an untrusted certificate is used, or HTTPS if a trusted certificate is used). Configure "Remote Desktop Gateway Protocol" and "Remote Desktop Gateway Specifier" as appropriate, again making the "specifier" the appropriate machine name/DNS name, and "Protocol" either "TCP|2303" for direct access to the GWS or "WSS|443" to multiplex these connections through ARR.

The preceding steps set up Web Console for HTTPS access on an alternate port (8443), and Gateway Server for TCP/UDP on the standard port 2303. Now we can install and configure Application Request Routing.

Single Server Installation – ARR Setup

ARR can be downloaded from Microsoft from: http://www.iis.net/downloads/microsoft/application-request-routing. The Microsoft-recommended installation technique is to use the Web Platform Installer (via the "Install this extension" button on that page), or there are manual installation instructions here: http://blogs.technet.com/b/erezs_iis_blog/archive/2013/11/27/installing-arr-manually-without-webpi.aspx.

The Microsoft documentation set for ARR is at: http://www.iis.net/learn/extensions/planning-for-arr. To understand the URL Rewrite rules (and properties & behaviors), see: http://www.iis.net/learn/extensions/url-rewrite-module/url-rewrite-module-configuration-reference

NOTE WELL: Earlier versions of this document had a significant error in the ARR configuration instructions, regarding the {SERVER_PORT} condition. The pattern was previously specified as "443", but that matched any string that contained the sequence of characters four-four-three, including "8443", which would lead to a loop. This version of the document fixes this by making the pattern "^443$" (caret-four-four-three-dollar), which forces the regular expression to match only the exact value "443" and not other strings (like "8443" or "4430"). Because a regular expression is used in this condition, the "Match URL / Using" value must be set to "Regular Expressions", and not "Exact Match" or "Wildcards", because this setting applies to how both the URL pattern and Conditions are evaluated.

To install and configure ARR, follow these steps.

1. Download and install ARR from the link(s) above. To use the Web Platform Installer to automate the installation, use the search field in the top right to search for "Application Request Routing" and select "Application Request Routing 3.0" and click Add, then Install to install that component.
2. Run IIS Manager. In the root node, you'll see new items in the "IIS" group – Application Request Routing Cache and URL Rewrite (possibly among others).
3. Double-click Application Request Routing, on the right-hand side pick Proxy > Server Proxy Settings… and configure:
    a. "Enable proxy" should be checked, which enables the rest of the page.
    b. Uncheck "Reverse rewrite host in response headers". (Note well: this setting *must* be unchecked in order for Azure AD login to work.)
    c. Uncheck "Enable disk cache" in the Cache Setting section.
    d. The rest of the settings can remain the defaults, as follows:
        i. Proxy Setting section:
            1. HTTP version: pass through
            2. [X] Keep alive
            3. Time out: 120 seconds
            4. [ ] Reverse rewrite host in response headers: (turned off: this is different than default setting)
        ii. Custom Headers section:

1. Custom Headers: Preserve client IP in : X-Forwarded-For
2. [ ] Include TCP port from client IP
3. Forwarding proxy header value: normally blank. However, this may need to be set to "X-Forwarded-For" if there are other proxy servers which may be forwarding requests to ARR/WC/GWS.

iii. Cache Setting section:
1. Memory Cache duration: 60 seconds
2. [ ] Enable disk cache (turned off: this is different than default setting)
3. [ ] Enable request consolidation (not enabled)
4. Query string support: ignore query string

iv. Buffer Setting section:
1. Response buffer: 4096 KB
2. Response buffer threshold: 256 KB

v. Proxy Chain section:
1. Proxy Chain: Proxy Server: <empty>

vi. Proxy Type section:
1. Proxy Type: [ ] Use URL Rewrite to inspect incoming requests

4. Right-click on the Sites node in IIS Manager, and select Add Website. Set Site Name to "URL Rewrite Rules", set physical path to a new, *unique* directory (suggestion: "C:\inetpub\urlrewrite"), and set the binding to HTTPS port 443, and select an appropriate SSL certificate for the site.
5. Select the new Site node in the Sites list. All remaining configuration is done on this site, and all instructions assume the "URL Rewrite Rules Home" features view is selected.
6. Double-click URL Rewrite, and add two rules as described in the next two steps.
7. Add a rule for the Gateway Server as follows.
   a. Click "Add Rule(s)…" on the right hand side.
   b. Select "Inbound Rules > Blank Rule", and click OK.
   c. In Edit Inbound Rule dialog, enter:
      i. Name = "GWS".
   d. In "Match URL" section, enter:
      i. Requested URL = "Matches the Pattern".
      ii. Using = "Regular Expressions".
      iii. Pattern = "ws/gws/". Leave Ignore case checked.
   e. In "Conditions" section, enter:
      i. Logical grouping: "Match All".
      ii. Add a condition with:
         1. Condition input = "{HTTPS}"
         2. Check if the string = "Matches the Pattern"
         3. Pattern = "ON"
         4. Leave "Ignore case" checked.
      iii. Add a condition with:
         1. Condition input = "{SERVER_PORT}
         2. Pattern = ^443$
         3. Leave "Ignore case" checked
   f. In "Action" section, enter:
      i. Action type = "Rewrite"

   ii. **PC-Duo v12:** Action Properties, Rewrite URL = http://localhost:2303/{R:0}
   iii. **PC-Duo v13:** Action Properties, Rewrite URL = https://*machinedns*:8444/{R:0}. Note well that this *must* be the GWS SSL listener port; specifying the HTTPSYS port will allow the connection to be established, but no data flows through ARR and an error is reported.
   iv. Uncheck "Append query string" checked.
   v. Check "Stop processing of subsequent rules"
8. Add a rule for the Web Console application as follows.
   a. Click "Add Rule(s)…" on the right hand side.
   b. Select "Inbound Rules > Blank Rule", and click OK.
   c. In Edit Inbound Rule dialog, enter:
      i. Name = "WC".
   d. In "Match URL" section, enter:
      i. Requested URL = "Matches the Pattern".
      ii. Using = "Regular Expressions".
      iii. Pattern = ".*". (That's dot-star). Leave Ignore case checked.
   e. In "Conditions" section, enter:
      i. Logical grouping: "Match All".
      ii. Add a condition with:
         1. Condition input = "{HTTPS}"
         2. Check if the string = "Matches the Pattern"
         3. Pattern = "ON"
         4. Leave "Ignore case" checked.
      iii. Add a condition with:
         1. Condition input = "{SERVER_PORT}"
         2. Check if the string "Matches the pattern"
         3. Pattern = "^443$"
         4. Leave "Ignore case" checked.
   f. In "Action" section, enter:
      i. Action type = "Rewrite"
      ii. **PC-Duo v12:** Action Properties, Rewrite URL = http://localhost:8080/{R:0}
      iii. **PC-Duo v13:** Action Properties, Rewrite URL = https://*machinedns*:8443/{R:0}
      iv. Leave "Append query string" checked.
      v. Check "Stop processing of subsequent rules"
9. Finally, configure WC+GWS in either WC > Gateway Settings > Network or Gateway Administrator > Gateway Settings > Network to include ARR in the "Trusted Device List". This allows the WC and GWS to use the X-Forwarded-For header provided by ARR to identify the client's actual origin. For a single machine installation, the Trusted Device List should be set to be the machine's IPv4 address, plus the IPv4 loopback address (127.0.0.1), plus the machine's link-local IPv6 address, as well as the IPv6 loopback address (::1) – these four addresses cover the likely addresses that ARR will use to connect to the other services on the machine.

Testing the Configuration

With this portion of the configuration complete, the GWS and WC should be accessible both directly on their alternate ports, and indirectly (through ARR) on port 443. This can and should be tested both on the server machine, and from a remote client. With this configuration the WC should respond on URLs:

- https://*machinedns*/ - landing page, which then allows you to log in
- https://*machinedns*:8443/ - landing page, which then allows you to log in

If the latter works, but the former doesn't, then something's wrong with the ARR configuration. In PC-Duo v13, you may notice that after logging in via the first URL, you're redirected to the second URL. Additional configuration is required in PC-Duo v13 to fix this and complete the setup.

If the URL Rewrite Rules are not working as expected, the recommended diagnostic strategy is to enable "Failed Request Tracing". See this article << http://www.iis.net/learn/extensions/url-rewrite-module/using-failed-request-tracing-to-trace-rewrite-rules >> for instructions, taking note of the fact that if you install Tracing after URL Rewrite, you may need to repair the URL Rewrite installation to be able to trace it. To trace everything, configure:

- What would you like to trace? = All content (*)
- Under which condition(s) should a request be traced = [X] Status code(s) 200-999
- Select Trace Providers = [X] WWW Server

Final Configuration for PC-Duo v13

Because PC-Duo v13 has configured "canonical URLs" for Identity Manager and Web Console, accessing the system via other URLS/ports will redirect to the configured canonical ones. In the configuration so far, the actual listening ports are configured, and the ARR front-end is not the primary access point.

To change that and complete the configuration in PC-Duo v13, we need to configure the PIM/WC/GWS components to use the port 443 entry point to the system, instead of the alternate ports. Make the following configuration changes:

- In Web Console > Gateway > Network, Gateway Server Access – Internal
  - Gateway Server address = *machinedns*
  - Gateway Server protocol and port = WSS|443
- In Web Console > Gateway > Network, Gateway Server Access – External
  - Gateway Server address = *machinedns*
  - Gateway Server protocol and port = WSS|443
- At bottom of Web Console > Gateway > Network page, click the link to go to Identity Manager Settings, and make these changes:
  - Identity Manager URL = https://*machinedns*/pim/
  - Web Console URL = https://*machinedns*/
  - Web Console URL (external network) = https://*machinedns*/

Multiple Server Installation

Installing ARR on one server and WC+GWS on a separate server is a similar configuration, with only a few changes necessary to the instructions for a single server installation. This type of installation may be desirable if, for example, the ARR server is placed in a "DMZ" or restricted area of the network, and forwards requests to the WC+GWS server inside the corporate LAN.

The Web Console and Gateway Server machine is set up exactly as in the previous section. One key difference is that, because ARR will not run on this machine, you can use any Windows Server version & edition supported by your version of PC-Duo WC+GWS.

PC-Duo v12: The steps above configure WC for HTTPS port 8443 and HTTP port 8080, and GWS on TCP/WS 2303.

PC-Duo v13: The steps above configure WC for HTTPS port 8443, and GWS on TCP/WS port 2303 and SSL port 8444.

The ARR configuration is the same as before, except that the URL Rewrite rules must now specify the DNS name of the WC+GWS machine, rather than “localhost” or the name of the combined server.

To encrypt the traffic from ARR to WC+GWS, additional configuration is needed:

1. The WC+GWS machine must have an SSL certificate trusted by the ARR machine, for the exact name by which ARR will refer to that server. This can be a third-party certificate, a corporate CA-issued certificate, or a self-signed certificate which is then imported into the ARR machine to trust it.
2. The GWS must be configured to listen for SSL connections on a specific port (recommendation: 8444), and be configured to use the trusted SSL certificate.
3. The URL Rewrite rules in ARR will now be in the form “https://gws-dns-name:port/{R:0}”, where “gws-dns-name” is the DNS name of the WC+GWS machine (as specified in its certificate), and “port” is the appropriate port for the service (8443 for WC, 8444 for GWS).

Multiplexing with NGINX

Rather than using Microsoft Application Request Routing, any appliance or system that supports reverse web proxy functionality can be used as a front-end to the PC-Duo Server system. This section briefly describes how to set up and configure the Nginx web server on Linux. These instructions set up the Nginx server on one machine (named “support.example.com”), which forwards all PC-Duo traffic to a PC-Duo Server installation (on a machine named “proxypro.example.com”).

1. Install PC-Duo Server software on a machine (in this example, named “proxypro.example.com”). This can be a standard installation of PC-Duo Server with default values, putting PIM+WC on https port 443, and Gateway Server SSL listener on port 8443. A trusted SSL certificate for the machine name (“proxypro.example.com”) should be configure. Proper operation of this installation should be tested before proceeding with the reverse web proxy setup.
2. Setup your Linux server (testing done for this document was done with Ubuntu 18.04), install nginx, and confirm that the installation is working correctly. Instructions for doing this are outside of the scope of this document; search the internet for “nginx setup on Ubuntu” to find an appropriate walkthrough.
3. The nginx server normally has a main configuration file in /etc/nginx/nginx.conf, and it loads additional configuration files from the /etc/nginx/conf.d/ directory. Below is a sample configuration file (reverseproxy.conf) that assumes an SSL certificate (with private key) for the server is located in the /etc/nginx/conf.d/ directory with name “servercertificate.pem”.
4. Once the nginx system is configured, you must adjust the PC-Duo Server configuration so that it points to the reverse web proxy, as described in the section “Final Configuration for PC-Duo v13”, above.

Sample NGINX Configuration Script for Reverse Web Proxy Support

```
server {
  listen 443 ssl;
  listen [::]:443 ssl;

  server_name support.example.com;

  ssl_certificate /etc/nginx/conf.d/servercertificate.pem;
  ssl_certificate_key /etc/nginx/conf.d/servercertificate.pem;

  location /ws/gws/ {
    proxy_pass https://proxypro.example.com:8443/ws/gws;
    proxy_http_version 1.1;
    proxy_buffering off;
    proxy_set_header X-Forwarded-For $remote_addr;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection "Upgrade";
  }

  location / {
    proxy_pass https://proxypro.example.com/;
    proxy_buffering off;
    proxy_set_header X-Forwarded-For $remote_addr;
  }
}
```

Other References and Technical Notes

It's possible to multiplex different PC-DUO installations behind a single reverse web proxy, ideally on different ports, but possibly all via the same port via Server Name Indication (SNI). Anyone interested in how to configure this in Application Request Routing should see this blog post:

http://weblogs.asp.net/owscott/archive/2010/01/26/iis-url-rewrite-hosting-multiple-domains-under-one-site.aspx

Application Request Routing has a number of configuration options; this document describes one configuration that's known to work. For more information about ARR options, including the "Preserve client IP in the following header" setting, see this Microsoft TechNet article:

http://technet.microsoft.com/en-us/library/dd443533(v=ws.10).aspx

The following documentation page is a walkthrough of how to create an outbound rewrite, which is needed for multiplexing multiple server installations. See the article "Reverse Proxy with URL Rewrite v2 and Application Request Routing" at:

http://www.iis.net/learn/extensions/url-rewrite-module/reverse-proxy-with-url-rewrite-v2-and-application-request-routing