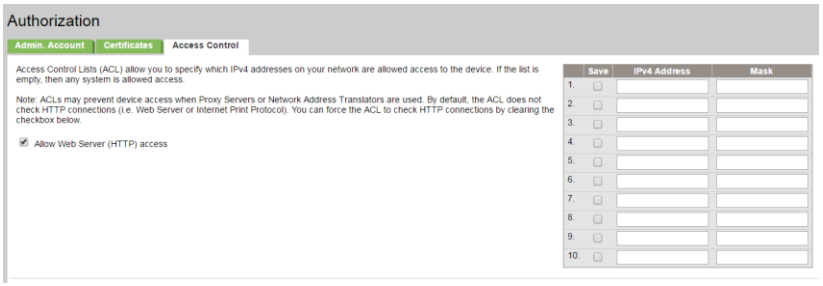
HP Managed Print Services Learning Series

Troubleshooting Guide for DCAs supporting HP MPS agreements

HP Managed Print Services (MPS) contracts rely on remote monitoring of devices using a data collection agent (DCA) which is a minor software application residing on a PC connected to the network. This trouble-shooting guide identifies common issues for each of the two DCAs in use by HP supporting Managed Page or Managed Complete MPS contracts.

Device connectivity issues (both DCAs)

- Verify the device is connected to the network (network cable directly connected to the device)
- Verify SNMP information
  - SNMP v1/2 (port 161/162) is enabled
  - SNMP community name is "public"
    - When using a custom SNMP community name, verify the custom string and configure in DCA
- Devices must be awake during a scan. Check device Auto Shutdown settings by reviewing energy settings in the administrative options of the Embedded Web Server (EWS): Energy Settings>Shutdown
- Device firmware may need to be updated; HP regularly releases new firmware with product enhancements and address known issues
  - Check for HP firmware updates at: http://support.hp.com/us-en/drivers and search/select your device; select OS independent; select updated firmware to download as required
- Review Access Control – some devices have an option to restrict communication to specific IP addresses (Example: Load the EWS > Network > Authorization)



- Verify the DCA client application is running by checking Windows Task Manager for the data collection agent (DCA). If the PC/Server running the DCA is rebooted, the service must be restarted. To enable an automatic restart of the DCA service, add the short cut to the Startup folder or set Windows Control Panel > Administrative Tools > Services console properties > General Startup type to Automatic.

Universal Device Agent (UDA)
UDA supports all HP Managed Page contracts and is the DCA connected to the Express Decision Portal (EDP) providing collected device data.

FMAudit
FMAudit is the DCA used by HP to support Managed Complete contracts and feeds data to our service back-end system.

Providing page counts for non-networked or non-reporting devices
Partners or customers become responsible to report page counts for devices that are non-networked or are non-reporting. The responsible party would provide configuration pages (print/scan or screenshot) for each device and email them to:

pmps-US-Meters@hp.com

Need assistance?
If you need help troubleshooting either a device or a DCA, please email the DCA support team at: pmps-DCA@hp.com

System, network or application issues

UDA

- Verify the following for correct HP UDA client installation (as applicable):
  - Windows Vista, Win78, Server 2008 and 2012 uses .NET 4.5
  - Windows XP / Server 2003 uses .NET 3.5
- Ensure the UDA client application is current. Download most current version: http://hpuda.com/install/HPUDAInstaller.zip
- Open HP UDA client application, ensure the account name is entered and start the service. Verify the application status by selecting Help > Troubleshooting. A green check indicates set-up is correct (see example right).
- If status errors are given, verify the UDA client can communicate:
  - Ensure access to HTTP Port: 80 and HTTPS Port: 443 (outbound)
  - If a proxy server is used to access the Internet and auto-detection is unsuccessful (error message "There was no endpoint listening") stop the UDA service. Go to Tools > Proxy and manually enter the proxy server settings in the UDA client and retest. Alternatively, using Windows Control Panel > Administrative Tools > Services console properties > Log On tab, enter credentials for an account with Internet access.
  - The firewall (local or company) should not block communication from the HP UDA client to the UDA server.
    - Add the URL setting: https://jadcws.jetadvice.com/v2/service1.svc or 23.97.172.77
    - If needed, add an exception to anti-virus software:
      - C:\Program Files (x86)\HP Universal Device Agent\DataCollector
      - C:\ProgramData\HP Universal Device Agent\DataCollector (hidden folder)

- Enter the IP addresses / IP ranges to be scanned by UDA. Ensure the Community name matches.
  NOTE: The number of IP ranges that can be scanned (~1500 max), varies based on network bandwidth/performance. One or more UDA clients can be used to balance the data collection responsibility if needed.
- Check whether the device MAC or HW address changed due to a service event or a transition from a wired to a wireless network (or vice versa). A remapping may be required – contact: l1.edp@hp.com

FMAudit

- Verify the client application is current; run the updater by accessing Program Files (x86)/FMAudit Onsite/Update.exe
- Verify Windows service for FMAudit Onsite is active by checking Windows Services and validating "FMAudit Onsite" is running
- FMAudit Onsite Version 3.0 – 3.6 utilizes .NET 3.5
- Ensure IP Addresses / IP range to be scanned is entered in the application (FMAudit Onsite > Network – see IP Settings)
  - The maximum number of IP addresses that can be scanned, varies based on network speed
    - Based on an SMNP timeout of 1,000 and a pinged response time of <55 milliseconds – allows scanning of ~300k of IP Addresses
- Ensure the following URL is accessible from the host system: https://fmaudit.austin.hp.com Port: 443 (encoded XML)
- Check proxy setting in FMAudit Onsite (Settings > Network > Proxy)
  - Select the "Test" button; you will receive a "Success" or "Failure" notification

4AA7-1028ENUS, September 2017