Technische Vorteile:

- ❖Einfache und schnelle Installation
- ❖Benutzung ist multimandantenfähig
- ❖Managed Ihre Geräteflotte jeder Größe und an jedem Punkt, ob als IT Manager oder Service Dienstleister
- ❖Mietleasing als SaaS und somit geringe Anfangsinvestitionen
- ❖ schreibt Ihre Rechnungen und liefert automatisch Toner
- ❖Keine eigene Server Installation oder Hosting
- ❖Sehr sichere und effiziente Software Architektur
- ❖Integration mit ERP Systemen, Helpdesk oder Service Management Software durch CSV oder XML sehr einfach

My Device Portal
Technische Beschreibung

Übersicht

My Device Portal basiert auf dem **Print Audit Facility Manager PAFM.** Es ist eine zentral gehostete **SaaS** (Software as a Service) zur Fernabfrage von Zählerständen, zum Toner Management, zur Erfassung von Service Informationen und zum Remote Management von Netzwerk Druckern, Faxgeräten und multifunktionalen Geräten.
Print Audit und **OFF SCRIPT** haben vertraglich abgesicherten Zugriff auf die gerätebezogenen Daten der meisten Hersteller dieser Geräte.

My Device Portal Key Features

Nur minimale Software Installation nötig!
Das Device Portal benutzt eine sehr kleine Software (einige 100 KB), die sogenannte **ICE (Information Collection Engine)**, um die Netzwerkumgebung regelmäßig nach technischen Gerätedaten zu scannen. Diese Daten werden auf den zentral gehosteten Device Portal Datenbank Server gesendet.
Es werden außer einem Logfile keine Informationen auf einen lokalen Computer geschrieben!
Die ICE ist kompatibel mit Internet Proxy Servern.
Sicherheit
Es werden keine persönlichen, firmeneigene oder Druckdaten gesammelt oder gesendet. Erfasst und gesendet werden nur:

- Druckername, Hersteller und Typ
- Ort der Aufstellen (falls eingegeben)
- Seriennummer
- IP Adresse
- MAC Adresse
- Seitenzähler (A4, A3, Mono, Colour, Druck, Kopien, Fax, Scan)
- Tonerfüllstand/Tonerwechsel
- Status und Alarmmeldungen (Papier leer, Papierstau, Fehlermeldungen etc.)

Die ICE erzeugt einen Scan File im XML Format, verschlüsselt und komprimiert ihn und sendet ihn dann SSL verschlüsselt zu Device Portal Server
Daten Speicherung

- Der Device Portal Server befindet sich in einem professionellen Hosting Centre mit mit höchstem Sicherheitsstandard, UPS und lückenlosem Sicherheits Backup
- Der Server ist Firewall gesichert und blockiert alle nicht autorisierten Zugriffe. Sein Betriebssystem und die Applikation ist immer auf dem neuesten Stand und mit den letzten Sicherheitsupdates versehen

OFF SCRIPT GmbH, Maternusstr.44, D-41352 Korschenbroich, Geschäftsführer: Maximilian Stottmeister, HRB 15036 AG Neuss, Ust.-ID: DE81569786,
tel. +49 2161 675738, email: info@off-script.com, www.off-script.com

- Die Anzahl der Administratoren ist auf ein Mindestmaß begrenzt und zwar für Update und Maintenance
- Die „My Device Portal“ Anwendung ist die einzige Anwendung auf diesem Server, so dass keine Gefährdungen von anderen Anwendungen ausgehen können

Web Interface

- Jeder Zugriff von außen erfolgt über ein Login mit Benutzernamen und Passwort über eine sichere **https Web Verbindung**
- Der Zugriff ist multi-mandantenfähig und gestattet die Zuweisung von gesonderten Rechten für Mitarbeiter des Händlers/Service Providers und für die Kunden
- Die https Verbindung benutzt eine 128 bit SSL Verschlüsselung

Anforderungen an die IT Umgebung für die ICE

- W2000 oder höheres OS mit Internet Explorer 4.01SP2 oder höher
- TCP/IP Netzwerk
- SNMP fähige Netzwerkdrucker und Netzwerkumgebung

Der Zugriff auf den Device Portal Server kann über Internet Explorer 6 oder höher, Mozilla Firefox 2.0 oder höher und über Apple Safari 4.0 oder höher erfolgen.

Technische Beschreibung des Erfassungsprozesses

Das folgende Kapitel beschreibt, wie die **ICE** die Drucker im Netzwerk entdeckt und die Druckerdaten erfasst. Es richtet sich vornehmlich an IT Personal, das mehr über die Funktionsweise und Auswirkungen der **ICE** auf das Netzwerk wissen will.

Welche Protokolle?

Der RAK benutzt in den meisten Fällen SNMP (Simple Network Management Protocol) zur Datenerkennung. SNMPv2 wird, wann immer möglich, benutzt, um den Traffic(chatter) zu reduzieren, aber es wechselt zu SNMPv1 für solche Geräte, die SNMPv2 nicht unterstützen. Der RAK benutzt auch ICMP (ping) Pakete zur Unterstützung der Geräteerkennung.

Erkennungsprozess

- Die ICE erkennt vom Host Computer die IP Adresse und Subnet, um einen Vorschlag für die IP Scan Range anzeigen zu können. Dann benutzt die ICE ICPM (ping), um festzustellen, ob irgendwelche Geräte mit diesen IP Adressen reagieren. Der Erkennungsscan benutzt dann nur SNMP innerhalb des Netzwerkes (UDP Port 161).
- Die ICE benutzt dafür die sogenannte „unicast transmission“ zu jeder IP Adresse in der konfigurierten IP Scan Range. Es werden keine Broadcast Pakete verschickt.
- Die ICE sendet keine Informationen direkt an die Geräte. Es kann bei Bedarf ein Community String spezifiziert und gesetzt werden.

OFF SCRIPT GmbH, Maternusstr.44, D-41352 Korschenbroich, Geschäftsführer: Maximilian Stottmeister, HRB 15036 AG Neuss, Ust.-ID: DE81569786,
tel. +49 2161 675738, email: info@off-script.com, www.off-script.com

Die ICE durchläuft beim Erkennungsscan folgende Schritte:

1. Die ICE macht einen Ping auf die IP Adresse, um eine gültige Antwort zu erhalten. Es wartet die „ping timeout“ Zeit, die in den erweiterten Settings festgelegt wurde. Wenn keine Antwort erfolgt, wiederholt es den Ping so oft, wie es in den "Ping Retries" festgelegt wurde. Wenn dann immer noch keinen Antwort von der angesprochenen IP Adresse erfolgt, wird die nächste IP Adresse angesprochen.

2. Wenn eine Antwort auf den Ping erfolgt, versucht die ICE, die Standard SNMP Daten des Gerätes zu erhalten. Falls keine Antwort erfolgt, wird so oft wiederholt, wie es in den "SNMP retries" Werten festgelegt wurde. Dies wird für jede Community aus der Community Liste der erweiterten Settings wiederholt. Wird dort auch nichts gefunden, dann stoppt die ICE die Ansprache dieser IP Adresse unter der Annahme, SNMP wird nicht unterstützt.

3. Wenn ein gültiger SNMP Wert als Antwort zurückkommt, dann versucht die ICE die Werte der „public Standard MIB“ des Druckers zu erhalten. Dabei werden die eingestellten "SNMP discovery timeout“ und die "SNMP retries" Werte benutzt. Sollte dabei auch nichts gefunden werden, wird angenommen, dass es sich nicht um einen Drucker oder MFP handelt.

4. Falls hier Informationen gefunden werden, wird die ICE mit den eingestellten "SNMP request" und "SNMP retries" Werten die Daten erfassen.

Datenübertragungsprozess

Nachdem die technischen Daten von den Geräten gesammelt sind, erzeugt die ICE eine verschlüsselte Datei zum Device Portal Server. Folgende Details dazu:

- Die Dateigröße beträgt etwa 5kB pro gescanntem Gerät
- Die ICE verbindet sich mit dem Device Porta Server nur über eine ausgehende Verbindung. Es gibt keine umgekehrten Zugriff vom Server auf die ICE im Kundennetzwerk
- HTTPS ist die Standardverbindungsmethode in der ICE Konfiguration. Dies sichert die verschlüsselte Datenübertragung per Internet Secure Protokoll (128 bit SSL auf TCP Port 443). Wenn HTTPS nicht zur Verfügung steht, wird HTTP (Port 80) benutzt.
- HTTPS ist die gleiche hoho Sicherheitsstufe, wie sie beim Internet-Banking und beim Internet-Shopping etwa bei Amazon benutzt wird.
- Der Device Portal Server sendet lediglich eine Bestätigung, dass er die Daten erhalten hat, sonst nichts. Die Bestätigung ist ebenfalls verschlüsselt.

OFF SCRIPT GmbH Maternusstr.44, D-41352 Korschenbroich, Geschäftsführer: Maximilian Stottmeister, HRB 15036 AG Neuss, Ust.-ID: DE81569786,
tel. +49 2161 675738, email: info@off-script.com, www.off-script.com

Warum könnte die ICE einige meiner Geräte nicht erkennen ?

Sollten einige der Geräte nicht erkannt werden, kann das folgende Ursachen haben:

- Das Gerät ist ausgeschaltet, physikalisch vom Netzwerk getrennt oder in anderer Form offline
- Das Gerät existiert nicht mehr innerhalb dieses Netzwerkes
- Das Gerät hat einen Fehler, welcher die Netzwerkverbindung beeinflusst
- Das Gerät unterstützt nicht SNMP
- Am Gerät ist SNMP nicht aktiviert
- Das Gerät hat eine IP Adresse, die nicht innerhalb des Scan Bereiches des RAK liegt
- Das Gerät ist an einen Print Server angeschlossen (z.B.JetDirect box). Gegenwärtig werden über Network Print Server angeschlossene Geräte nicht erfasst.
- Das Gerät ist ein Fiery Print Server. In einige Fällen liefern Fiery Server nicht genügend Informationen für die ICE.
- Der Community String des Gerätes könnte sich geändert haben.

Falls keiner der Netzwerkdrucker von der ICE gefunden wird, sind dafür folgende Gründe möglich:

- die ICE hat eine falsche IP-Adressen-Bereich Konfiguration
- die ICE Kommunikation im Netzwerk ist behindert, z.B. eine Firewall oder ein Router blockiert SNMP

Was muss ich tun, damit alle meine Geräte gefunden werden?

Falls einzelne Geräte von der ICE nicht gefunden und angezeigt werden, versuchen Sie folgende Schritte zur Fehlersuche:

1. Überprüfung der Gerätekonfiguration, dass es eingeschaltet und mit dem Netzwerk verbunden ist

2. Überprüfung der IP Adresse zur Bestätigung, dass es nicht in ein anderes Subnet oder einen anderen nicht erfassten IP Bereich bewegt wurde. Im Bedarfsfall muss der IP Scan Bereich der ICE dem angepasst werden.

3. Zur Bestätigung die zum Gerät zugehörige Web Site öffen. Es sollte auch überprüft werden, ob der Port 161 nicht blockiert ist.

4. Die IP anpingen, um zu sehen, ob eine Reaktion erfolgt. Wenn nicht, liegt das Problem innerhalb des Netzwerkes und hat nichts mit der ICE zu tun.

Falls keines der Geräte gefunden wird, sollte folgende Fehlersuche erfolgen:

1. Wiederholung der Überprüfung des IP Scan Bereiches und der anderen Settings der ICE

2. Wenn eine Firewall aktiviert ist, sicherstellen, dass nicht SNMP zwischen Gerät und ICE blockiert ist (TCP port 161)

3. Sicherstellen, dass der Community String in der ICE korrekt und identisch zum Gerät gesetzt ist.

OFF SCRIPT GmbH, Maternusstr.44, D-41352 Korschenbroich, Geschäftsführer: Maximilian Stottmeister, HRB 15036 AG Neuss, Ust.-ID: DE81569786,
tel. +49 2161 675738, email: info@off-script.com, www.off-script.com

Ist Network Traffic ein Problem?

Nein, die Pakete sind relativ klein und der Scan läuft nur kurze Zeit.

- Die ICE löst keinen Traffic aus, solange der Scan nicht aktiviert wird
- Wenn der Traffic einmal angestoßen ist, erzeugt die ICE etwa 30-50 KB bidirektionalen Traffic pro Gerät.

Nach dem ersten Descovery Scan macht die ICE Refresh Scans. Der Refresh Scan benutzt dieselben Community Settings und ist deshalb kürzer als ein Discovery Scan. Als Standard erfolgt ein Discovery Scan alle 12 Std. um neue Geräte im Netzwerk zu entdecken.Refresh Scnas erfolgen alle 20 Min oder 60 Min, je nach installierter ICE Version.

Wie kann ich den Network Traffic reduzieren?

Es gibt noch eine Reihe von Maßnahmen, um den Traffic im Erkennungsprozess noch weiter zu reduzieren. Jede der Maßnahmen hat Für und Wieder:

1. Begrenzung der Communities. Solange die Geräte in der Organisation die "public" oder „standard private“ Community nutzen, kann durch erweitertes „Discovery Setting“ mit ein oder zwei Communities ein Traffic Problem vermieden werden. Je mehr Communities vorhanden sind, desto länger dauert ein Scan und desto mehr „SNMP Requests“ werden erzeugt.
2. Verringerung der Anzahl der „SNMP retries“. Es besteht allerdings die Gefahr, dass ein Gerät beim Scann nicht erkannt wird.
3. Hochladen einer Liste spezifischer IP Adressen, die sich auf die vorhandenen Printer beziehen, in das Discovery Scan Fenster. Z.B., wenn 5 Geräte existieren, dann kann der Import der 5 IP Adressen durch File Import oder manueller Eingabe Hunderte von SNMP Request zu anderen IP Adressen einsparen.
4. Wenn einmal der Erkennungsscan beendet ist, sollte im Wiederholungs-falle ein Refresh Scan benutzt werden, um nicht alle IPs noch einmal anzusprechen.

Technischer Support:

Technische Unterstützung oder weitere Informationen erhalten Sie über:
Tel:+49 (0)2161 675738 oder Email: support@off-script.com

Technischer Support in Deutschland, Österreich und Schweiz
Support@off-script.com
Tel. +49 (0)2161 675738