Security

JetAdvice Edge ensures a high degree of data security and confidentiality for every installation of JetAdvice Manager, JetAdvice Connect and JetAdvice Premium.

Bulletproof, end-to-end security is crucial when the software is running on the server, exchanging data over the network.

Technical description

This section describes the technical details about our Connector called JetAdvice Edge and JetAdvice Cloud (our servers).

Network requirements

- Access to the Internet
- SNMP-enabled network

Ports and data

JetAdvice Edge uses HTTPS port 443 (HyperText Transfer Protocol Secure) to secure communication between the Connector and JetAdvice Cloud. You can compare this to browsing the Web with an Internet browser on a standard PC.

The Connector is primarily using Simple Network Management Protocol (SNMP), along with HTTPS, to collect MIB / OID data from the devices on your network. This is done using as few network resources as possible helping to maintain low bandwidth usage.

No user information is ever transmitted – only metadata about device usage, i.e. accounting summary and status information. No print jobs can be reproduced or replicated based on the transmitted data. This ensures a high degree of confidentiality.

By default, the smart collected data is batched together, compressed and submitted to JetAdvice Cloud on a regular basis – or immediately if the collected data has high priority (e.g. low supply levels or hardware alerts).

The Connector is easily configured using JetAdvice Edge UI locally or via the JetAdvice Manager portal from anywhere in the world.

Technologies used

JetAdvice Cloud and JetAdvice Edge are built on the flexible and highly secure .NET Core platform that offers superior performance and scalability.

Requirements

- Windows OS:
  - Microsoft .NET Core Runtime and APS.NET Core Runtime 3.1.1 or higher
  - SNMP version 1, 2 or 3 networks and enabled in the devices
- Linux OS:
  - Raspbian (Jessie, Stretch and Buster) 32bit
  - Debian (v10 LTS) & Ubuntu (v20 LTS) 64bit
  - Microsoft .NET Core Runtime and APS.NET Core Runtime 3.1.1 or higher
  - SNMP version 1, 2 or 3 networks and enabled in the devices

JetAdvice Edge uses very few resources on the computer or server it's installed on.
It runs on all hardware that meets the .Net Core 3.1.1 requirements or higher.

Whitepaper

The main JetAdvice Edge functions

JetAdvice Edge will communicate with JetAdvice Cloud for:

- Authentication
- Configuration
- List of network ranges and SNMP settings
- Updates
- Identify devices
- Discover and Collect phases

JetAdvice Edge scans all defined network ranges, searching for imaging devices (printers, MFPs, label printers, fax machines, etc.) based on specified SNMP settings and credentials. It allows for broad scanning of big ranges – or specific scanning on only individual addresses for full control of which devices it's talking to on the network.

The network scan is flexible and able to collect data from several different network protocols such as IPv4, IPv6 and by Hostname over SNMP v1, 2 & 3. For example, one specific IP address to a full IP range, e.g.: 192.168.99.1 to 192.168.99.254.

The Connector can be configured to automatically stay up-to-date with the latest releases from JetAdvice Cloud. Auto updates can be disabled in the client, with no possibility for JetAdvice Cloud to override this.

JetAdvice Edge uses two phases to retrieve data from an imaging device: Discovery and Collection. The Collection phase is based on state-of-the-art intelligence to reduce unnecessary network traffic.

Discovery phase

The Discover phase is used to look at all IP addresses specified using SNMP. This phase will reveal if the specific IP address holds an imaging device.

First, one SNMP packet is sent to all IP addresses. If JetAdvice Edge gets a reply, a unique set of OIDs is sent to identify the imaging device. When the imaging device is identified for the first time, the Collection phase will start.

Collection phase

Depending on the imaging devices found in the Discovery phase, the type of data requested can vary. The Collection phase is normally processed via SNMP and HTTP for all devices.

The amount of data for small devices, like single-function mono devices, is very limited. Whereas larger multi-function devices typically have a wider data set to be collected.

With our intelligent data collection technology, devices are checked at varying intervals to determine if anything has changed. If the device state or information is altered, a data collection is subsequently carried out. A device is fully collected from and synced with JetAdvice Cloud once every 24 hours – regardless of whether there are any changes or not.

Collecting the IP address, MAC and Hostname of each scanned imaging device is standard. This ensures the accurate identity and location information of each imaging device on the network.

When a device is found, it's matched to a specific model and set of OIDs. Information related to type and model is then collected.

For detailed information see the FAQ: "OID information" https://app.jetadvice.com/FAQ.aspx?FaqID=3417