SHARP

MICAS WHITE PAPER

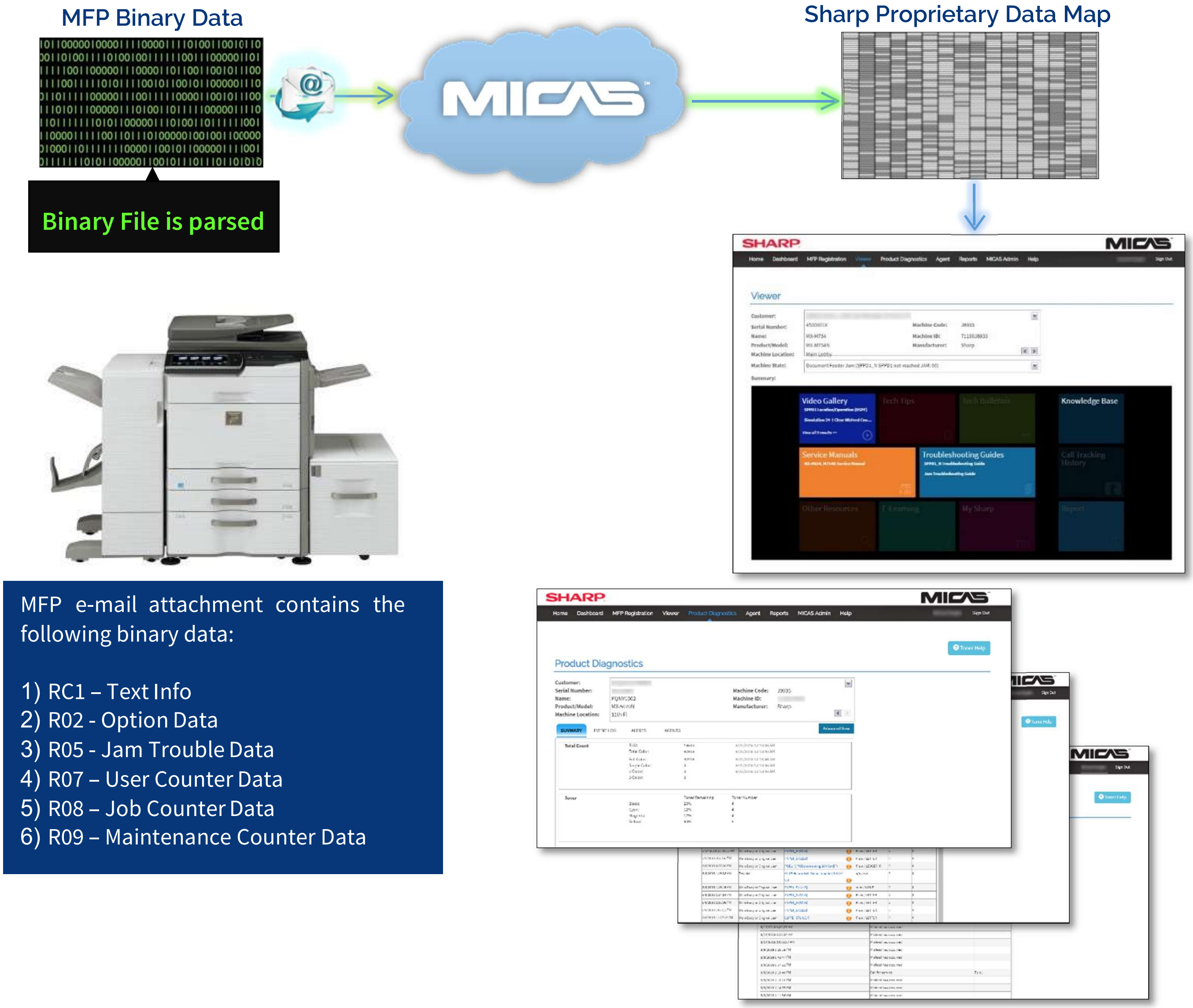
MICAS℠ for Your Business

Contents

1 Introduction

The Machine Intelligence Call Assistance Service (**MICAS**) is a cloud-based service application, as well as a real-time monitoring agent (**MICAS Agent**). MICAS collects and reports information on MFP device status, usage counts, supply levels, errors and alerts, while providing a library of support resources to assist field service technicians. MICAS never collects any personal or sensitive information.

Servicing dealers use MICAS to increase call efficiency, reduce unnecessary service visits, provide proactive support and enhance customer experience.



MFP e-mail attachment contains the following binary data:

1) RC1 – Text Info
2) R02 - Option Data
3) R05 - Jam Trouble Data
4) R07 – User Counter Data
5) R08 – Job Counter Data
6) R09 – Maintenance Counter Data

2 Overview

MICAS can collect data from an MFP fleet using remote email diagnostics (R.E.D.), or the MICAS Agent, or both.

2.1 R.E.D (Remote Email Diagnostics)

Sharp MFPs are configured to send R.E.D data every 24 hours by email. The R.E.D email data attachments are a Sharp proprietary binary format.

2.2 MICAS Agent

The MICAS Agent automatically collects data using SNMP and transmits updates to the MICAS server using HTTP web services. The MICAS Agent also provides device information, troubleshooting and an end-user dashboard. MICAS utilizes request signing for web service calls.

Access to the MICAS Agent user interface can be secured with access control and role-based authorization. It is possible to remotely schedule Agent Device Discovery from the MICAS portal via Remote Commands. This is significant because a technician will no longer need to be on-site to make Device Discovery adjustments to an agent.

2.3 MICAS Web Portal

The **MICAS viewer** provides users with solutions to MFP jams, low toner levels, errors and alerts, and helps dealers to schedule scheduled maintenance.

The **MICAS Dashboard** is used to view summary and detailed data at the dealer fleet or customer level.

The **MICAS MFP Registration** is used to import and maintain customers and devices.

The **MICAS Product Diagnostics** page is used to view details of a single device.

MICAS Reports provide summaries of copy counts, toner levels, trouble codes and preventative maintenance.

3 About MICAS

3.1 MICAS Portal

Sharp utilizes data centers for MICAS web and database servers to ensure continuous operation during most network disruptions. Smaller issues such as minor hardware failures are handled without affecting end users.
Production database servers are configured as active/passive cluster. Either server can fail, with no reduction in performance. Live databases are replicated to Sharp's Disaster Recovery Datacenter throughout the day, significantly reducing the potential loss of production data. Disaster Recovery servers also configured as active/passive cluster. Databases are backed up daily.

Anti-virus Software

Antivirus Software effects the operation of the MICAS Agent. Please ensure you have setup a rule to allow the MICAS agent to access the ports to communicate with the MICAS Cloud Service. Directions for setup are in the agent installation instructions.

3.2 MICAS Data Collection

For Sharp MFPs, dealers can use R.E.D. data collection, the MICAS Agent, or both. For third-party devices, the MICAS Agent must be used.

Remote Email Diagnostics

Sharp MFPs are configured in the MFP control panel to send R.E.D. (**Remote Email Diagnostic**) data to MICAS every 24 hours by email. R.E.D. collects information about paper jams, error codes, toner levels, counters, and MFP configuration. The R.E.D. email contains binary attachments in a proprietary format which MICAS translates into MFP solutions.

Remote SNMP Walk

SNMP Walks for unknown printer models can be initiated from the MICAS Portal, which will then issue a remote command to the agent at that location. The Agent executes the command, sends the walk data to the portal, where it is collected and emailed to the dealer. There is an Agent switch to disable remote SNMP walks. It is included in the Security Settings section.

MICAS Agent

The MICAS Agent uses SNMP to detect devices on the network, and to collect device information on an on-going basis. The MICAS Agent supports SNMP v1 and v3. The Agent queries SNMP data from registered devices:

- 60 seconds after the service starts, it queries individual counter OIDs/job counter/toner levels/supply levels/AQUOS Board™ readings.
- Then every 1 minute afterward, SNMP alerts only.
- Every 60 minutes, it queries everything.

Values are only sent to MICAS if the value has changed since the last time it was queried. Clicking the Refresh button in the devices page, queries and sends SNMP alerts, individual counter OIDs, job counters, toner levels, and other supply levels to MICAS **WITHOUT** checking that the values have changed.

3.3 TCP/UDP Ports

Port	Protocol	Direction	Scope	Purpose
8080	TCP	Out	LAN	MICAS Agent user interface (HTTP). Port 8080 is used for administrator access to the Agent serving the pages that you see on-screen at http://localhost:8080.
80, 443	TCP	Out	Internet	Communication from MICAS Agent to Web\Cloud Server (HTTP and HTTPS) via https://micasagent.sharpamericas.com
5353	UDP	In	LAN	Used by MICAS Agent for device detection on LAN (mDNS).
161*	UDP	Out	LAN	Used by MICAS Agent for device detection and on-going collection of telemetry data (SNMP). ** Ports 161 and 162 are used by all versions of the SNMP protocol.*
162*	UDP	In	LAN	

Ports 80, 443 are enabled by default for Windows®. Ports 5353, 161, 162 and 8080 are automatically opened in Windows firewall as part of the installation process. MFP devices send R.E.D. data using email. Port 25 is the default port used to transmit emails using SMTP.

3.4 MICAS Agent Installation Requirements

Sharp recommends that you install and run the MICAS Agent on a secure in-house server, as opposed to a third-party or outside server. Running the MICAS Agent on an in-house server will help to provide secure, uninterrupted service.

Minimum Windows® Server Requirement:

- Windows 7
- Windows 8 or 8.1
- Windows 10
- Windows Server 2008
- Windows Server 2012 / 2012R2
- Windows Server 2016
- Windows Server 2019

Minimum Microsoft® .NET Framework: .NET Framework 4.5

The MICAS Agent installation file can range in size from 10-20 MB. File size will vary depending upon version number and could increase in size with future releases. The general memory requirement is 4 GB and may vary by operating system and network. Once installed, the MICAS Agent can be accessed on a web browser on the same network, using the host IP address and port number.

MICAS Agent Updates

Download the latest version of the MICAS Agent directly from the Update tab within the Agent page. MICAS Agent version 4 and greater can check for and install available upgrades automatically.

3.5 Impact on Customer Network

The MICAS Agent Installation file can range in size from 10-20 MB. The file size will vary depending upon version number and could increase in size with future release versions.
The following would be a typical usage scenario:

- Check device registration and register machines as required.
- Retrieve table of OIDs to query for each device. OIDs are cached for 12 hours. This would occur twice a day, per device.
- Send OID values back to server, depending upon device usage. Values are sent only if the value has changed since the last time the OID was queried.
- Send toner levels back to server depending upon device usage. Levels are sent only if a toner level has changed since the last time it was queried.

The size of each of these requests or responses will range from 1-20KB.
For example, a MICAS Agent with 5 machines, assuming each request/response is 20KB per day, breaks down as follows:

- 100 registration checks
- Request or response =100KB
- 10 OID list reads
- 400 OID value reports
- 400 toner level reports= approximately 1000 x 20KB = 2MB.

The full download will amount to approximately 5MB. Values are variable and can change per usage and number of machines. The total effect on the network would be negligible.

4 Sharp Corporate Security

Sharp recognizes the need for security and the confidentiality of client data. Sharp works to help protect its clients' information by providing security features on not only the Sharp MFP line, but also within MICAS.

4.1 Corporate Policies and Practices

The following list includes several Sharp policies* designed to protect Sharp, its affiliates, and clients:

- IT Security
- IT Access Control
- IT Change Management
- IT Threat and Risk Assessment
- IT Incident Handling
- IT Disaster Recovery
- IT Records Management

*Due to the confidential nature of the content of these policies, they are not regularly distributed. However, they can be made available for review with Sharp upon execution of a Nondisclosure Agreement.

4.2 Sharp Administrator Access of Data

Sharp IT or Support may occasionally need to access client data in order to provide support on technical issues. For these types of issues, access permissions will be limited to the minimum necessary to resolve the client issue. Sharp administrators are granted role-based permissions in order to uphold data security for the customer, as follows:

- Access by Sharp administrators is always logged.
- MICAS users, business administrators, and dealer administrators have access to items within their scope of authority. System administration is limited to Sharp authorized personnel. Sharp administrators can access only information critical to the operation of the system.

5 Appendices

5.1 Appendix A — Which products are covered/not covered?

A Management Information Base (**MIB**) is a database used for managing entities in a communications network. MIB is most often associated with the Simple Network Management Protocol (**SNMP**). Both Sharp and non-Sharp multifunction printing devices are capable of transmitting status information using the Host Resources MIB (**RFC 2790**) and Printer MIB (**RFC3805**). Based upon MFP model, age, and manufacturer, the quantity of captured data may differ. Sharp MICAS products fall into two categories: those that solely capture R.E.D. alerts and meters (**Diagnostic Support**) and those which provide advanced technical support.

Diagnostic Support Only

AR-300/400/500 (list can vary)

Non-Sharp MFPs and printers*

*Toner and meter reads only

Advanced Technical Support

MX-2610N/3110N/3610N

MX-2615N/3115N

MX-2630N

MX-2616N/3116N

MX-2640N/3140N/3640N

MX-4110N/4111N/5110N/5111N

MX-4140N/4141N/5140N/5141N

MX-6240N/7040N

MX-6500N/7500N

MX-C250

MX-C300P

MX-C301W

MX-C303W/C304W

MX-3050N/3550N/4050N/5050N/6050N

MX-3050V/3550V/4050V/5050V/6050V

MX-3070N/3570N/4070N/5070N/6070N

MX-3070V/3570V/4070V/5070V/6070V

MX-B402

MX-C312

MX-B350P/B450P

MX-B350W/B450W

MX-C402SC

MX-M264N/M314N/M354N

MX-M364N/M464N/M564N

MX-M266N/M316N/M365N

MX-M365N/M465N/M565N

MX-M654N/M754N

MX-M904/M1054/M1204

MX-M1055/M1205

MX-M905

MX-M2630

MX-M3050/3550/4050/5050/6050

MX-M3070/M3570/M4070/M5070/M6070

MX-M65760/M7570

MX-6580N/7580N

MX-7090N/8090N

MX-2651/3051/3551/4051

MX-3071/3571/4071

Devices Not Covered

Dot matrix printers

Some wide format printers

5.2 Appendix B — Firmware

The following MFPs are supported for Agent firmware updates and **do not include** DSK and specialty firmware. The Agent may display that machines with DSK and specialty firmware require an update. This should be confirmed with your service manager.

DX-C310
DX-C400
DX-C311
DX-C401
MX-2300N
MX-2700N
MX-2310U
MX-3111U
MX-2600N
MX-3100N
MX-2610N
MX-3110N
MX-3610N
MX-2615N
MX-2616N
MX-3115N
MX-3116N
MX-2640N
MX-3140N
MX-3640N
MX-3050N
MX-3050V
MX-3550N
MX-3550V
MX-4050N
MX-4050V
MX-5050N
MX-5050V
MX-6050N
MX-6050V
MX-3070N
MX-3070V
MX-3570N
MX-3570V
MX-4070N
MX-4070V
MX-5070N
MX-5070V
MX-6070N
MX-6070V
MX-3500N
MX-3501N
MX-4501N
MX-4100N
MX-4101N
MX-5001N
MX-4110N
MX-4111N
MX-5110N
MX-5111N
MX-4140N
MX-4141N
MX-5140N
MX-5141N
MX-5500N
MX-6200N
MX-7000N
MX-6201N
MX-7001N
MX-6240N
MX-7040N
MX-6500N
MX-7500N
MX-6580N
MX-7580N
MX-B355W
MX-B455W
MX-B400P
MX-B401
MX-B402
MX-B402SC
MX-C301W
MX-C311
MX-C401
MX-C312
MX-C400P
MX-C402SC
MX-M1055
MX-M1205
MX-M283N
MX-M363N
MX-M453N
MX-M503N
MX-M363U
MX-M453U
MX-M503U
MX-M364N
MX-M464N
MX-M564N
MX-M365N
MX-M465N
MX-M565N
MX-M623N
MX-M753N
MX-M623U
MX-M654N
MX-M754N
MX-M1100
MX-M850
MX-M950
MX-M1054
MX-M1204
MX-M904
MX-M905
MX-M2630
MX-M3050
MX-M4050
MX-M3550
MX-M5050
MX-M6050
MX-2651
MX-3051
MX-3551
MX-4051
MX-3071
MX-3571
MX-4071

5.3 Appendix C — References

R.E.D. — **Remote Email Diagnostic** is proprietary through Sharp MFPs and can be configured to send status messages via email. These status messages contain binary data that include MFP maintenance, configuration, and error logs.

MIB — **Management Information Base** is a collection of information organized hierarchically. These are accessed using a protocol such as SNMP. There are two types of MIB's: scalar and tabular. Scalar objects define a single object instance whereas tabular objects define multiple related object instances grouped in MIB tables. The Standard Printer MIB is outlined in a document referred to as RFC 3805.

HTTP — **Hypertext Transfer Protocol** is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web. Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is the protocol to exchange or transfer hypertext.

OID— **OID** stands for Object Identifier which uniquely identifies managed objects in a MIB hierarchy. This can be depicted as a tree, the levels of which are assigned by different organizations. Top level MIB Object Identifiers (**OIDs**) belong to different standards organizations. Vendors define private branches including managed objects for their own products. Here is a sample structure of an OID:

```
1.3.6.1.4.868.2.4.1.2.1.1.1.3.3562.3
```

SNMP — **SNMP** stands for Simple Network Management Protocol and consists of three key components: managed devices, agents, and Network-Management systems (**NMSs**). A managed device is a node that has an SNMP agent and resides on a managed network. These devices can be routers and access servers, switches and bridges, hubs, computer hosts, or printers. An agent is a software module residing within a device. This agent translates information into a compatible format with SNMP. An NMS runs monitoring applications. They provide the bulk of processing and memory resources required for network management.

SSL — **Secure Sockets Layer** is a cryptographic protocol designed to provide communication security over the internet. SSL is in the process of being deprecated.

TLS — **Transport Layer Security** is a cryptographic protocol that provides end-to-end communications security over networks. TLS replaces SSL.

MICAS Agent — **Proprietary Software Application**