SHARP

MICAS℠

for Your Business

Contents

1 Introduction 1

2 Overview 2

2.1 R.E.D (Remote Email Diagnostics) 2

2.2 MICAS Agent 2

2.3 MICAS Web Portal 2

3 About MICAS 3

3.1 MICAS Cloud 3

3.2 MICAS Data Collection 3

3.3 TCP/UDP Ports 4

3.4 MICAS Agent Installation Requirements 4

3.5 Impact on Customer Network 5

4 Sharp Corporate Security 6

5 Appendices 7

5.1 Appendix A - What products are covered/not covered 7

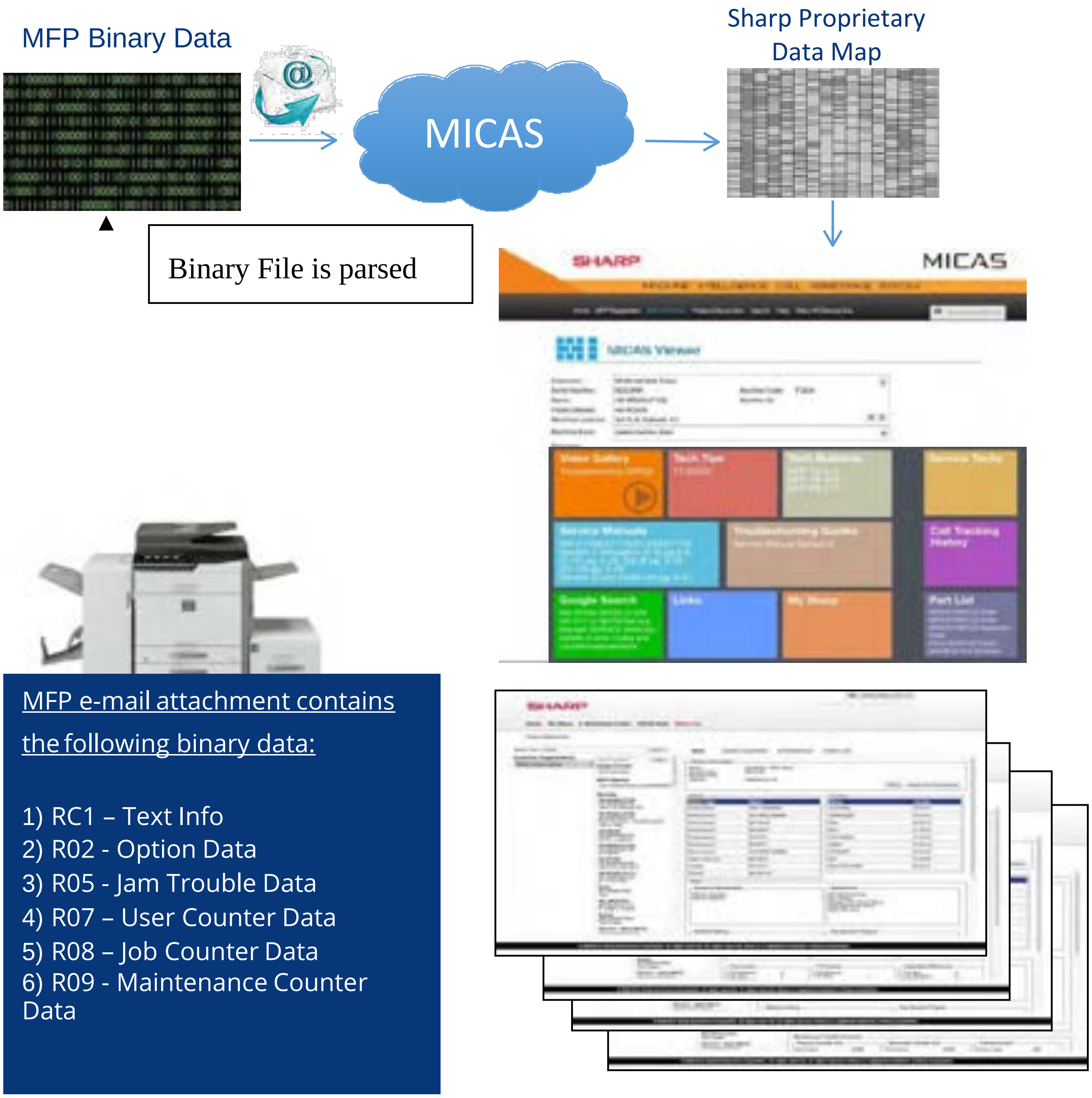
Appendix B - Firmware 7

Appendix C – References 8

1 Introduction

The MICAS Service (“MICAS”) is a cloud-based service application and real-time monitoring agent (“MICAS Agent”) which collects and reports information on MFP device status, usage counts, supply levels, errors and alerts and provides a library of support resources to assist field service technicians.

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 e-mail diagnostics (R.E.D.), the MICAS Agent, or both.

2.1 R.E.D (Remote Email Diagnostics)

Sharp MFPs are configured to send RED data periodically by e-mail. The R.E.D email data attachments are a Sharp proprietary binary format.

2.2 MICAS Agent

The MICAS Agent automatically collects real-time 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 either Windows Authentication, local access control, or role-based authorization.

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 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 Cloud

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 affects 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 remote e-mail diagnostics (R.E.D.) data to MICAS periodically by e-mail. R.E.D. collects information about paper jams, error codes, toner levels, counters, and MFP configuration. The R.E.D. e-mail contains binary attachments in a proprietary format which MICAS translates into MFP solutions.

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 versions 1 and 3.

The Agent queries SNMP data from registered devices:

- 60 seconds after the service starts, it queries OIDs/counter/toner/supply/AQUOS Board readings).
- Then every 1 minute afterward, SNMP alerts only.
- Every 60 minutes, it queries everything (SNMP alerts, OID builder OIDs, job counters, toner levels, other supply levels and AQUOS Board readings)

Data are sent to MICAS only if value have changed since the last time it was queried. Clicking the Refresh button on the Devices page queries the device and sends SNMP alerts, OID builder OIDs, job counters, toner levels, 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 access to the Agent serving the pages that you see on-screen at http://localhost:8080.
80	TCP	Out	Internet	Link to Dealer Graphics Image on Agent. If Dealer graphics uses an HTTPS URL, port 443 is used.
443	TCP	In/Out	Internet	Secure communication between MICAS Agent and Web\Cloud Server https://micas.sharpamericas.com 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 161, 162, 5353 and 8080 are automatically opened in Windows® firewall as part of the installation process. MFP devices send R.E.D. data using e-mail. Port 25 is the default SMTP port used to transmit e-mails.

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® Requirement:

- Windows 10
- Windows 11
- Windows Server 2012 / 2012R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Note that Windows Home Editions are not supported. 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 Agent page. The MICAS Agent 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 dates.
The following would be a typical use scenario:

- Check device registration and register machines as required.
- On each page load, read the banner image. This will typically be cached & would not be re-read more than once every couple of weeks
- Retrieve 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. OID 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 is in the range 1-20KB.

For example: MICAS Agent with 5 machines, assuming each request/response is 20KB per day. Please see below.

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

The full download will amount to about 5MB in total, although this can vary. Totals will change based on 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 client information by providing security features on not only the Sharp MFP line, but also within MICAS.

4.1 Corporate Policies and Practices

MICAS and its attendant systems are ISO/IEC 270001 compliant. Certificate is available upon request.

4.2 Sharp Administrator Access of Data

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

- 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 - What products are covered/not covered

A MIB (Management Information Base) 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 can transmit 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	**Advanced Technical Support**	**Devices Not Covered**
AR-300/400/500 (list can vary). Non-Sharp MFPs and printers	All Sharp MFPs manufactured after 2011	Dot matrix printers Some wide format printers

Appendix B - Firmware

All Sharp MFPs manufactured after 2011 are supported for Agent firmware updates

Appendix C – References

R.E.D. - **Remote Email Diagnostic (R.E.D.)**. Sharp MFPs can be configured to send status messages via e-mail. 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** (**HTTP**) 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.

HTTPS - **Hypertext Transfer Protocol Secure** (**HTTPS**) is a secure application protocol for distributed, collaborative, hypermedia information systems. It is the secure counterpart to HTTP.

OID - **OIDs** or Object Identifiers uniquely identify managed objects in a MIB hierarchy. This hierarchy can be depicted as a tree, the levels of which are assigned by different organizations. Top level MIB object ID's (OID's) belong to different standard 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.

MICAS Agent – Locally-installed application that collects device data and transmits it to the MICAS servers.

Design and specifications are subject to change without notice. Sharp, MICAS, and other related trademarks are trademarks or registered trademarks of Sharp Corporation and/or its affiliated companies. Windows is a registered trademark of Microsoft Corporation. All other trademarks are the property of their respected holders.