SSP ElectraM3

Remote Access

CONFIDENTIALITY STATEMENT

SSP Limited has prepared this document in good faith. Many factors outside SSP Limited's current knowledge or control may affect the recipient's needs and project plans. Errors in the document will be corrected once discovered by SSP Limited. The responsibility lies with the recipient to evaluate the document for applicability. The information in this documentation is proprietary, confidential and an unpublished work and is provided upon recipient's covenant to keep such information confidential. Personal Data supplied in this document may not be used for any purpose other than for which it was supplied. Personal Data may not be transferred to other parties without prior consent of SSP Limited. In no event may this information be supplied to third parties without SSP Limited's prior written consent.

The following notice shall be reproduced on any copies permitted to be made:

SSP Limited Head Office:
Fourth Floor, G MILL, Dean Clough, Halifax, West Yorkshire, HX3 5AX, UK
Registered in England and Wales No. 04234499

T: +44(0)1422 330022
F: +44(0)1422 349130
W: www.ssp-worldwide.com

CONTENTS

INTRODUCTION

With reference to Coronavirus and the questions some of our ElectraM3 customers are raising with SSP in relation to remote access to the ElectraM3 application for their users, we have prepared this document.

As ElectraM3 is not a hosted application / product, the application is not set-up for remote access and access is restricted to each customer's individual network.

Remote access can be achieved, albeit, with restricted functionality.

Remote Access

If an ElectraM3 User needs access to ElectraM3 remotely, our suggested method of connection is via the use of a PC Remote Access Software package, there are number of different packages available that customers can review and select i.e. LogMeIn, GoToMyPC, TeamViewer, etc. Some of these packages offer a limited period free trial.

The customer will be responsible for purchasing, installation, and set-up (each SSP customer would also need to check and take responsibility for the security of the software / connection used).

Once the remote software is installed on a User PC in the office, the product will then allow them to connect via a remote PC / Laptop device, which in turn provides direct access to 'take over' that specific users work PC and in turn, access the ElectraM3 application. The users work PC would have to be left powered on so that access can be established remotely.

Once remote connectivity is set-up, there are restrictions this has, i.e. printing and backups

Printing cannot be directed remotely and will continue to print to the printers in the office.

VPN Connectivity

Some of our customers have advised that they are looking to set-up a VPN connection as an option for their staff to connect to ElectraM3.

Any customer implementing this solution would be expected to take responsibility for setting this up themselves, the ElectraM3 Technical Support Team are available to assist with basic advice and questions or 'hand holding' where they can, but please note it is the customer and/or their IT Professional who will be responsible for completing all of the set-up actions themselves – not SSP.

Where there is limited IT knowledge at the customers' office, we suggest the customer use remote PC access software instead, and set this up as stated above in the Remote Access section.

Recommendations

Printing

Printing via any third party remote access product will only print to the printers installed within the work/office location, i.e. there is no option to print remotely (i.e. from home).

Any ElectraM3 generated documents will continue to print in the same way to office printer's set-up within the ElectraM3 application.

Customers with "SSPD" functionality would be better placed to use this rather that physically printing documents.

Backups

The current standard ElectraM3 Backup routine writes data to a physical tape, which is inserted into the tape drive, a task which is the responsibility of the SSP customer. Without a tape being inserted each day the backup will fail and if tape is not inserted for 5 days the system will lock out all users. We therefore recommend that the customer continues to change the tape daily.

If a daily backup is not completed there is risk of data loss in the event of a system issue / failure, again something the customer needs to be aware of as data backups are their responsibility, this is not SSP's responsibility.

Summary

SSP's recommendation is that one person (if available) visits the office each day to take last night's backup off site and insert a new tape for tonight, while on site checking the printers have enough paper in the trays and sorting the documents printed so that they can place what is needed in the post.

Support Desk

The Service Desk will assist with a level of hand holding but we are not in a position to purchase, install or set any remote access up for any customer and their users but if you have any questions, please log an IM in the usual way and we will do what we can to assist and advice.

Back-up Tapes will need to be changed daily to ensure a data backup is maintained, the customer needs to check the backup status and report any issues/failures to SSP in the normal way