



micros[®] Systems, Inc.

Remote Support Access Policy

A description of the policies and procedures relating to remote access to customer systems by MICROS Systems, Inc. (MICROS) Customer Support personnel. This document also includes MICROS's recommended connection and security methods as well as details on how PCI-DSS, PABP and Sarbanes-Oxley requirements affect how MICROS customers are supported.

Foreword

This document is provided by MICROS Systems, Inc., MICROS-Fidelio, its subsidiaries and affiliates, (collectively MICROS) as a reference guide only and in no way implies that the recommendations described herein will prevent unauthorized access to customer networks or systems. MICROS accepts no responsibility for the security of customer networks, systems, or applications. Please refer to your individual service or support maintenance contract or contact your local MICROS account or support representative for further details.

Additionally, MICROS is not a security company and does not provide PCI-DSS assessments or audits and cannot provide review of or approval for customer network security strategies or policies.

MICROS strongly recommends that its customers comply with the remote access policies described in this document. For MICROS customers who decline to comply, MICROS may, at its discretion, require such customers to sign a disclosure document, which indicates that the customer has been made aware of our remote access policies, has declined to comply with such policies and shall not hold MICROS responsible in the event such non-compliance results in any customer damages.

Table 1: Document Change History

DATE	DESCRIPTION
03.10.08	Initial Draft
05.09.08	Updates Based On Feedback From VeriSign Review
09.23.08	Updates To Approved Applications and Encryption Requirements
04.21.09	Updates To VPN Recommendations
09.09.09	Updates To Approved Remote Support Applications/Solutions
06.09.10	Updates To Approved Remote Support Applications/Solutions
03.09.12	Document Updated To Consolidate USA And International Policies

Document prepared by:

Eric Seaman
 Vice President, Customer Support
 MICROS Systems, Inc.

James Walsh
 Chief Security Officer
 MICROS Systems, Inc.

Uwe Maulhardt
 Chief Security Officer – EAME
 MICROS Systems, Inc.

Table of Contents

Overview	4
Intended Audience.....	4
Reference Documentation.....	4
Executive Summary.....	5
MICROS Recommendations for Secure Remote Support Access	5
MICROS Policies Regarding Secure Remote Support Access	5
Industry Requirements	6
Payment Card Industry Data Security Standard (PCI-DSS).....	6
MICROS Recommendations	7
1. Build and Maintain a Secure Network	7
Firewalls	7
User Accounts and Passwords	7
2. Protect Cardholder Data	8
Database Handling	8
Transport Encryption	8
3. Implement Strong Access Control Measures.....	9
4. Regularly Monitor and Test Networks	9
Track and Monitor All Access to Network Resources and Cardholder Data.....	9
Remote Access and Support Software and Tools	9
1. BOMGAR	10
2. WEBEX Support Center Remote Support.....	10
3. PCAnywhere (V 12.5 or higher, with all Symantec Security Updates Installed)	10
Verification of MICROS Callers.....	11
Not supported or approved	11
Resulting Remote Support Options	12
1. Allowed – without executing MICROS disclosure document:	12
2. Allowed – only after execution of MICROS disclosure document:	12
Explanation VPN-Tunnels & Bomgar Session:.....	13
1. Bomgar-Session:.....	13
2. Site-to-Site-VPN:	13

3. Client-to-Site-VPN: 14

Overview

In order to facilitate security and compliance with certain industry requirements such as the Cardholder Information Security Program (CISP), Payment Card Industry Data Security Standard (PCI-DSS) and Payment Application Data Security Standard (PA-DSS), MICROS has developed standard policies pertaining to methods used to deliver remote support to its customers from the MICROS Customer Support Centers. This document describes the MICROS recommended connectivity and security methods and supported remote access applications and policies. This document also provides details on user account and password management.



Intended Audience

This document is intended for MICROS customers as well as MICROS Support, Implementation, Sales, and Account Management professionals, MICROS VARs and Service Partners and any other audience interested in the remote support policies and procedures used by the MICROS Support Centers.

Reference Documentation

- The Payment Card Industry Security Standards Council (PCI-SSC) web site is available at: <https://www.pcisecuritystandards.org/>
- The latest version of the Payment Card Industry Data Security Standard (PCI-DSS) is available at: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
- A listing of Qualified Security Assessors (QSA's) is available from the PCI-SSC web site at: https://www.pcisecuritystandards.org/qsasv/find_one.shtml
- A copy of the Payment Card Industry (PCI) Self-Assessment Questionnaire from the PCI-SSC is available at: <https://www.pcisecuritystandards.org/saq/index.shtml>
- General information on PCI compliance validation and requirements are available from VISA's web site at http://usa.visa.com/merchants/risk_management/cisp_merchants.html
- MICROS Information Security web site is available at <http://www.micros.com/ServicesAndSupport/InformationSecurity/>

Executive Summary

MICROS Recommendations for Secure Remote Support Access

1. Customers should implement and maintain secure network infrastructure and policies such as firewalls, Network Address Translation (NAT), Access Control Lists (ACL's), individual user-account-based authentication, unique (non-default) user accounts with strong passwords and routine password rotation.
2. Customers are advised to implement secure methods for remote support access that comply with the terms of the PCI-DSS.
3. Customers should implement methods for logging user access to their networks and system(s) consistent with the terms of the PCI-DSS.
4. Remote access applications/tools and user accounts/passwords configured for use by MICROS Support or for any other entity or reason should be enabled only when needed for a specific purpose requiring remote access and should be disabled or removed immediately afterward. For security purposes, MICROS discourages the use of persistent open communications between your MICROS system and any public networks.
5. In addition to standard access controls, user accounts configured for remote access should include only those access rights required for the service/support being provided and should be robustly audited.



MICROS Policies Regarding Secure Remote Support Access

1. MICROS will only provide remote support via solutions that have been tested and approved by MICROS. Solutions not approved and supported by MICROS can be nominated for approval through your MICROS Account Manager or Account Representative. A testing and validation fee may be charged to complete the review/approval process. Additional costs may be included if non-standard or unsupported software is required. MICROS may, at its discretion, provide remote support via a customer-required method or tool that does not comply with MICROS policy or meet the approval of MICROS. In such event, MICROS may require the customer to execute a disclosure document which attests that the customer has been made aware of MICROS' Remote Support Access Policy, has elected not to comply with such policy and will not hold MICROS responsible in the event such non-compliance results in any customer damages.

2. MICROS Customer Support will not store or manage user account information or passwords for customer systems or applications. It is recommended that customers use unique and strong user-based accounts and passwords for network and application access. MICROS Customer Support is unable to provide assistance for issues involving lost or forgotten passwords or user account information.
3. MICROS Customer Support does not provide network configuration, implementation, or consultation services or support.

Industry Requirements

The PCI Security Standards Council (PCI-SSC) was formed in 2006 by Visa, MasterCard, American Express, Discover and JCB to develop industry standards relating to the handling and storage of credit card data and credit card customer information. These standards comprise the Payment Card Industry Data Security Standard (PCI-DSS). The PCI-DSS details specific requirements relating to network security and access control. The following is a summary of those requirements which impact how MICROS provides remote support to its customers. Complete details on PCI-DSS requirements can be found at www.pcisecuritystandards.org and should be reviewed in detail by each customer with their individual PCI-DSS Qualified Security Assessor (QSA). *MICROS is not a security company and does not provide PCI-DSS assessments or audits and cannot provide approval for customer network security strategies or policies.*

Payment Card Industry Data Security Standard (PCI-DSS)

PCI-DSS requirements are applicable to any networks or systems where credit card Primary Account Numbers (PAN's) are stored, processed, or transmitted. Such networks or systems are typically referred to as "cardholder data environments". Customers using MICROS Point-Of-Sale and/or Property Management products equipped with the optional Credit Card (CA/EDC) module, installed and active, are in scope of the PCI-DSS and may be contractually compelled to comply with the terms of the PCI-DSS by their Acquirer or Processor. The PCI-DSS applies to all "system components" that comprise the merchant's cardholder data environment. The PCI Council defines System Components as "... any network component, server, or application that is included in or connected to the cardholder data environment." Please refer to the PCI-DSS for more detail.

The PCI-DSS is comprised of 12 General Requirements grouped in 6 Sections.

SECTION	GENERAL REQUIREMENT
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords or other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

MICROS Recommendations

The following recommendations are provided as a guideline that should be followed to help ensure MICROS' support personnel are able to provide you with remote support assistance without compromising your Information Security Policy.

1. Build and Maintain a Secure Network

Firewalls

MICROS recommends that all customers implement and maintain network access control appliances and/or software to control access to and from customer networks and systems (firewalls). Firewalls should include the use of Network Address Translation (NAT), Packet Filtering, Access Control Lists (ACL) and/or Application-Layer firewalls.

User Accounts and Passwords

All default, shared or generic user accounts and passwords created during the installation and configuration of your MICROS product(s) should be removed, disabled, or changed to comply with the terms of the PCI-DSS. MICROS will *not* maintain or store user account information, including passwords, for your system.

MICROS recommends that unique user accounts with strong passwords are used for all users including any user accounts assigned by the customer for use by the MICROS Support Centers. MICROS customers should not use their own user accounts or passwords to permit the remote access of MICROS Support or another support entity. User accounts provided to MICROS Support or any other support entity for remote support access should be disabled when not in use.

For security purposes, effective July 1, 2010, MICROS will no longer store sensitive customer information such as user access credentials, user account information, remote access information, and passwords on its network. All existing information of this nature will be securely deleted from current secure storage locations within the MICROS networks. MICROS Support will not create or modify any user accounts or account passwords on your system nor does MICROS Support have dedicated user accounts or “back door” accounts available. If a customer is unable to provide a login and password for access (if needed) to the MICROS or Fidelio application, database, or Operating System, MICROS may not be able to provide remote support. Therefore, MICROS strongly recommends that its customers designate someone on their staff to actively manage their user accounts and passwords and to be able to provide access to MICROS in the event that remote support is needed.

2. Protect Cardholder Data

Database Handling

Cardholder data is stored in a highly encrypted format within your PA-DSS Validated MICROS product’s database (sensitive Track Two data is not stored after authorization by MICROS PA-DSS Validated products). From time to time it may be necessary for MICROS Support to obtain a copy of your database for testing or trouble-shooting purposes. In such cases, MICROS will transfer a copy of the database via secure connection to a dedicated test machine within a MICROS Support Center or facility. Once testing and/or trouble-shooting has completed, the database and any data generated from the database (i.e. reports, data exports, etc.) will be securely destroyed.

MICROS Customer Support will not accept databases from its customers via email or unsecure file transfer. Databases can be mailed to MICROS Customer Support only by utilizing a tracking-based shipping method that requires an accepting signature (i.e. FedEx, UPS, DHL, etc.).

Transport Encryption

Connectivity methods provided by customers must be capable of providing at least 128 bit encryption at the transport layer (SSL or IPSEC).

3. Implement Strong Access Control Measures

MICROS recommends that each customer provide remote access to be used by MICROS Customer Support via PCI-DSS compliant methods. Allowing access to your network and/or systems using unsecure methods or methods not conforming to PCI-DSS standards can leave you open to breach and loss of sensitive data as well as fines and other damages.

Implementation and maintenance of customer networks, network configurations, and network security are the responsibility of the customer.

4. Regularly Monitor and Test Networks

Track and Monitor All Access to Network Resources and Cardholder Data

MICROS recommends that customers implement methods for logging user access to their system(s) consistent with the terms of the PCI-DSS. Logging should be enabled both within the MICROS application(s), at the Operating System level and for all components of the cardholder data environment with such access logs, to ensure that all user access can be audited. See the Payment Card Industry Data Security Standard (PCI-DSS) or consult your PCI Consultant or Qualified Security Assessor (QSA) for more information.



Remote Access and Support Software and Tools

Our current remote support policy requires that MICROS employees and contractors only connect to customer's systems using a MICROS-approved remote access tool that requires the customer to tactically grant access each time remote support is needed. This ensures that no MICROS personnel are permitted to connect to any customer systems without their express knowledge and consent. This policy actually exceeds the Payment Card Industry Data Security Standard (PCI-DSS) requirements and provides MICROS customers with a much improved level of security. As previously stated, MICROS may, at its discretion, agree to use a customer-required remote access method or tool that does not comply with this policy. Provided, however, that the customer has first executed a disclosure document which attests that the customer has been advised of our remote support access policy, has elected not to comply with our policy, and will not hold MICROS responsible in the event of any resulting damages. MICROS has listed three approved remote access tools below which do not permit access to customer systems without the knowledge and collaboration of the customer. These are the only MICROS approved remote access tools at this time. Any other remote access tools or applications must be reviewed and approved by MICROS in writing.

1. BOMGAR

MICROS currently utilizes **BOMGAR Secure Remote Support Software** product as its preferred method for all remote support tasks, including the delivery of MICROS Customer Support. BOMGAR is an on-demand, secure, web based, remote access application. A “Support Session” can only be started via a cooperative exchange between the customer and a MICROS Customer Support agent. Once a Support Session is started, the customer must grant access to either the entire system or an individual application(s). Application level access must be provided to the Support Agent by the customer as well. The authentication for the support agent is linked to the MICROS corporate Active Directory domain user database for MICROS staff. The user accounts on the Bomgar system used by MICROS partners will be maintained by authorized MICROS personnel only.

MICROS customers do not need to purchase BOMGAR software or services in order to receive remote support from MICROS using this tool. Nor are MICROS customers required to install any special remote agents or software on their equipment to facilitate remote access using this tool. All that is needed is secure internet access.

2. WEBEX Support Center Remote Support

The WEBEX Support Center Remote Support product works in a manner very similar to the BOMGAR product described above. This product can also be configured in such a manner that it does not permit remote access to a customer system without the knowledge and collaboration of the customer. It also does not require the customer to purchase or install anything on its systems. All that is needed is secure internet access. Although this is not currently the preferred MICROS remote access tool, it is approved for use by MICROS.

3. PCAnywhere (V 12.5 or higher, with all Symantec Security Updates Installed)

PCAnywhere should only be used if the PCAnywhere Host on the customer system has been configured in a secure manner consistent with the recommendations outlined in the document “Secure Setup of PCAnywhere”, which is posted on the MICROS Information Security web site at this link: http://www.micros.com/NR/rdonlyres/948FFEC6-232F-463D-91E1-23350BA3EF2C/0/SECURE_CONFIG_PCANYWHEREJan2010.pdf

The configuration of PCAnywhere specified in this document includes:

- a. Symmetric or Public Key encryption enabled
- b. Logging enabled
- c. Account Lockout enabled
- d. Prompt to Confirm Connection enabled
- e. Use of unique user account and strong password for each support session
- f. PCAnywhere Host must be disabled when not in use

Customers wishing to use PCAnywhere will need to purchase and deploy the PCAnywhere application. This can be acquired from MICROS if desired.

Verification of MICROS Callers

As most communication between MICROS Support and its customers is initiated by MICROS customers, it is typically unnecessary for our customers to verify that the person on the telephone is actually a MICROS representative. However, in cases where MICROS contacts you and requests remote access to your system for a reason that you were previously unaware of, MICROS highly recommends that you verify the legitimacy of the caller before granting access to your network. This can be done by requiring the MICROS representative to provide you with the Clarify CRM support case number for the particular support case he/she is contacting you about. Then, you can contact the appropriate MICROS Customer Support Center to verify the legitimacy of the support case and caller.

Also, all remote connections by MICROS personnel using the BOMGAR Secure Remote Support Software will be made using one of the following domains: customersupport.micros.com or eamesupport.microsdc.com

Remote connections by MICROS-Fidelio partners will be initialized from: eamepartners.microsdc.com

Not supported or approved

- WebEx Remote Access Solution (a.k.a. SMARTech)
- Other Remote Support Solutions like TeamViewer or LogMeIn
- Unsecured/unencrypted direct internet connection (not using a VPN Tunnel) via PCAnywhere versions older than V 12.5, VNC, Microsoft Remote Desktop, DameWare or other remote access tools
- VPN-Tunnels based on PPTP, L2TP
- Any remote access method that does not require the customer to grant access at the time the connection is being made to a system or network (e.g. static IPsec-tunnels).
- Any remote access method which requires the installation of specific client software not usually operated by MICROS support.
- Any remote access method which requires the installation of client software at the customer site.

Resulting Remote Support Options

The following remote support options are currently available:

1. Allowed – without executing MICROS disclosure document:

- Internet access: Bomgar Secure Remote Support Software
- Internet access: PC Anywhere v 12.5 or higher (with secure configuration outlined in the MICROS document “Secure Setup of PCAnywhere” , the latest Symantec security updates installed, and dual-factor authentication)
- Dial-up-Modem access: PC Anywhere v 12.5 or higher (with secure configuration outlined in the MICROS document “Secure Setup of PCAnywhere” , the latest Symantec security updates installed, and dual-factor authentication)
- Internet access: WebEx Support Center Remote Access Solution (Customer specific solution; requirement: WebEx is offered by the customer)
- Internet access: Bomgar Secure Remote Support Software (Customer specific solution; requirement: Bomgar is offered by the customer)

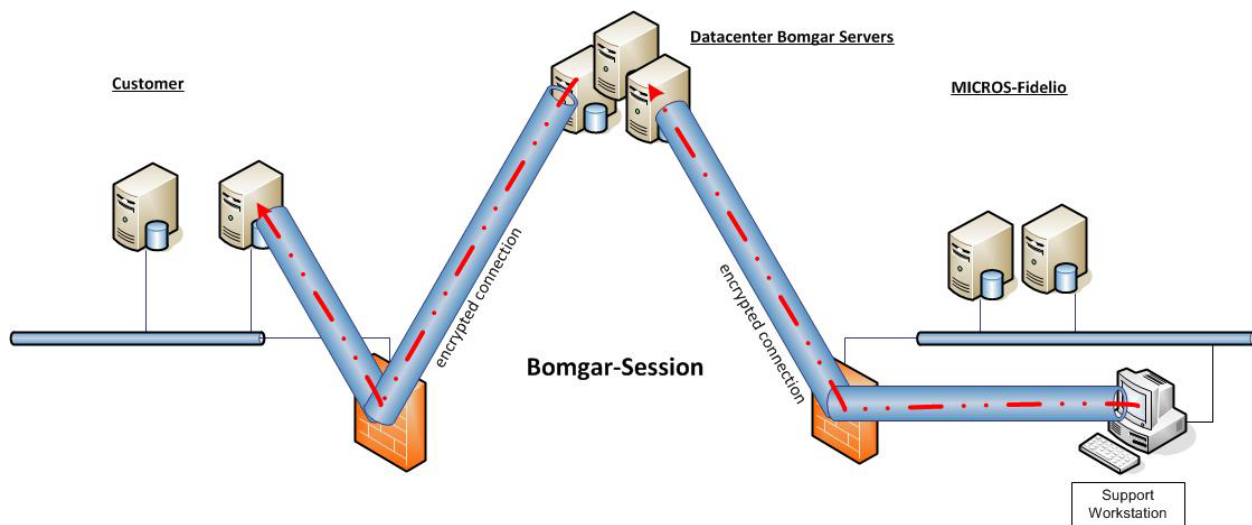
2. Allowed – only after execution of MICROS disclosure document:

- Internet access: VPN-Tunnel (Site-to-site)+ Support Software (RDP, VNC, PC Anywhere version older than 12.5); Connection initiated by MICROS
- Internet Access: VPN-Tunnel (Client-to-site) (i.e. Cisco or Astaro) + Support Software (RDP, VNC, PC Anywhere version older than 12.5); Connection initiated by MICROS- should be migrated in the future
- Other: Customer-required access method which does not conform with MICROS’ policy

Explanation VPN-Tunnels & Bomgar Session:

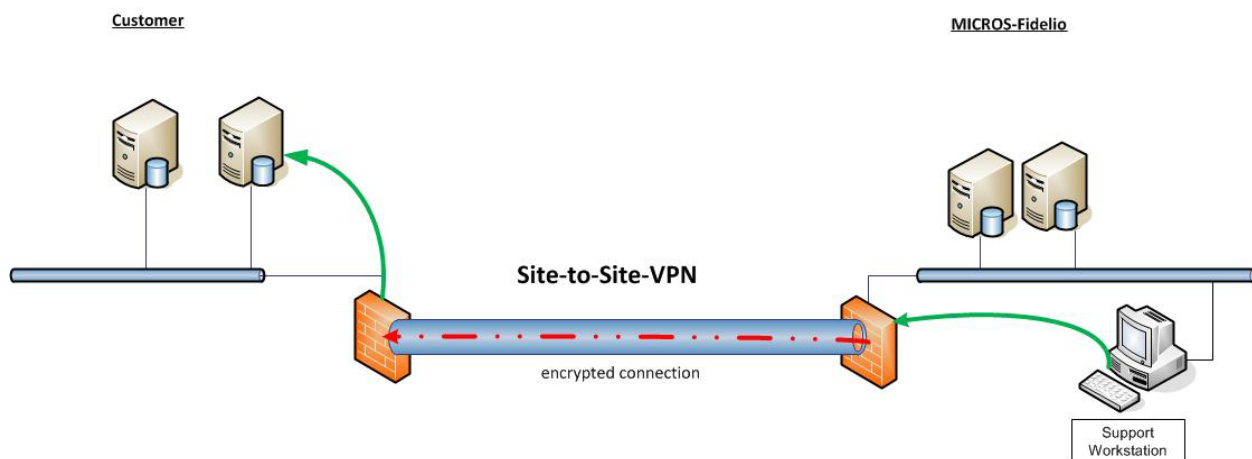
1. Bomgar-Session:

- SSL Encrypted Session (Connection on demand) between MICROS Support-Workstation, MICROS-Datacenter Bomgar Servers and Customer Server/Client
- Connection (on demand) from both sites to central point through establishes tunnel for support-traffic



2. Site-to-Site-VPN:

- VPN-Tunnel (permanent established connection) between two Firewalls
- Connection (on demand) with Remote Support Software from MICROS Support-Workstation to Customer Site through this tunnel



3. Client-to-Site-VPN:

- VPN-Tunnel (Connection on demand) between MICROS Support-Workstation and Customer Firewall.
- Connection (on demand) with Remote Support Software from MICROS Support-Workstation to Customer Site through this tunnel

