

Network Interface Firewall for IBM i

Reduce exposure to open ports and services on your system

IBM Technology Expert Labs Power Delivery Practice is proud to offer the Network Firewall for IBM i Exit Points. The primary purpose of this tool is to restrict access to various remote services on IBM i to only a pre-approved list of users. If the user is not pre-authorized to use that particular service, then they will be blocked. Blocking is done per service, per user and even by IP address, if desired. For example, you could allow user JSMITH access over FTP only if coming from another server.

Network Interface Firewall for IBM i Exit Points

When installed and configured, this tool simplifies managing the addition and removal of exit point definitions for users on IBM i. Exit points are a provision of the IBM i operating system that lets some system functions perform additional checking and validation through user created programs. The tool currently includes programs for managing exit points for FTP, ODBC, JDBC, File Transfer, Host Servers, DRDA/DDM, REXEC, CLI and RMTCMD. This easy-to-use interface lets a security admin define which users are allowed through the exit point, and an audit journal record is created whenever a user accesses it. Besides user enforcement, the tool can be set to only monitor and record whom is access which services, when, and from where. This tool is the perfect jump start to reduce your exposure to remote user access while maintaining a high level of security.

```

2/10/17                               Work with Exit Point Definitions                               10:20:50
Position to: _____ Filter Definitions: _____ ALLOBJ: *NOTUSED
Type options, press Enter.
5=Display 8=Add Exit 9=Remove Exit N=*ON F=*OFF L=*LOGONLY W=WRKREGINF

Opt Definition Exit Point Name Exit Point Description Status
- DRDADDM CHGNETA DRDA/DDM Logon *ADDED2NAT
- DSTPGMC QIBM_QZRC_RMT Distributed Program Call *ADDED2XPT
- DTAQSRVR QIBM_QZHQ_DATA_QUEUE Host Servers DATAQ Server *ADDED2XPT
- FILESRVR QIBM_QPWFS_FILE_SERV Host Servers File Server *ADDED2XPT
- FTPCLNRQ QIBM_QTMF_CLIENT_REQ FTP Client Request Validation *ADDED2XPT
- FTPLOGON QIBM_QTMF_SVR_LOGON FTP Server Logon *ADDED2XPT
- FTPSVRRQ QIBM_QTMF_SERVER_REQ FTP Request Validation *ADDED2XPT
- HSTPRT QIBM_QNPS_ENTRY Host Server Net Print Server *ADDED2XPT
- OJDBC QIBM_QZDA_INIT DB Logon - ODBC/JDBC/File XFR *ADDED2XPT
- OSQL1 QIBM_QZDA_SQL1 DB Server SQL Access *ADDED2XPT
- OSQL2 QIBM_QZDA_SQL2 DB Server SQL Access *ADDED2XPT
- REXECREQ QIBM_QTMX_SERVER_REQ REXEC Request Validation *ADDED2XPT
- RMTCMD QIBM_QZRC_RMT RMTCMD Logon *ADDED2XPT
More...

F3=Exit F5=Refresh F6=Create Definition F9=Command Line
    
```



Implementation Services

Need help securing your IBM i system? Our Expert Labs team is highly trained in the proper way to handle complex security configurations. We can guide you all the way from design to implementation. You don't have to undertake security yourself – allow IBM Expert Labs to be your trusted consultants to ensure a successful project!

Interested in a Quote or Learning More?

If you are interested in purchasing this asset or discussing it further with one of our consultants, please contact Ron Bibby at ronbibby@us.ibm.com! Or visit our website at <https://ibm.biz/IBMiSecurity>.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.