BNS GROUP

msXfax®

ENTERPRISE CLOUD CONNECTOR

WINDOWS SERVER 2016 & EXCHANGE 2016

Interoperability testing Windows Server 2016 & Exchange Server 2016 CU3 with msXfax version 8.1 & Sonus SBC

www.bnsgroup.com.au

msXfax®
ENTERPRISE CLOUD CONNECTOR

BNS GROUP
Secure SMS & FAX Messaging Solutions

CONTENTS

FIGURES

TABLES

No table of figures entries found.

SECTION 1 Interoperability testing

1.1 BNS Group Australia

BNS is a Microsoft Silver Application Development partner specializing in Fax and SMS gateways which run on Windows Server Virtual machines within an enterprise network.

BNS is working with Skype for Business partners to assist them migrate legacy faxing from traditional PBX analog extensions by leveraging session border controllers to carry both voice and fax in a Skype for Business solution. BNS's fax server technology is focused on both on-premises Exchange and native Exchange online support.

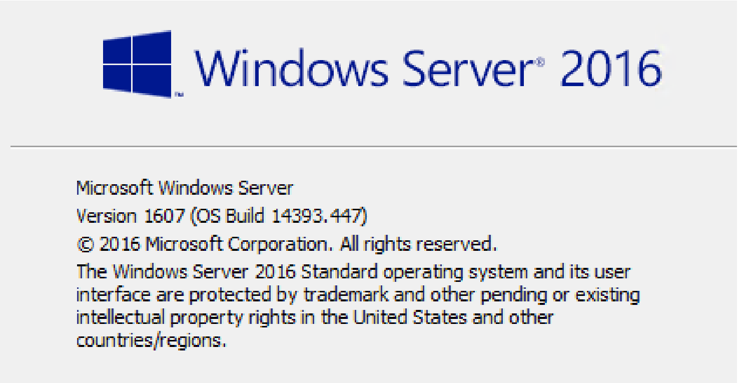
BNS can assist other Microsoft partner provide both FAX and SMS solutions to their customers.

About BNS: http://www.bnsgroup.com.au/bns-group/AboutUs.aspx?a=29&s=49&c=930

Web: www.bnsgroup.com.au

1.2 Purpose

This document outlines successful interoperability testing of msXfax version 8.1 with the following technologies:



Microsoft Windows Server
Version 1607 (OS Build 14393.447)
© 2016 Microsoft Corporation. All rights reserved.
The Windows Server 2016 Standard operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

- Exchange Server 2016 CU3 (built on Windows Server 2016)
- Office 2016 built on Windows 10
- Sonus Session Border Controllers 1000 & 2000 (version 5.x and 6.1 software)
    - ISDN
    - Optus Evolve SIP Trunk service.

BNS Group has ISDN and Optus SIP Trunk service installed in its test lab for the purposes of providing fully tested solutions for its partners and customers.

1.3 msXfax version 8.1

BNS Group's msXfax Enterprise Cloud Connector (Fax Server) runs in a Windows Server 2012R2 or Windows server 2016 virtual machine providing a powerful and flexible fax over IP solution supporting T.38 real time fax over IP and G.711 fax pass through.

The solution connects to Exchange Server on-premises (2007, 2010, 2013, 2016 or better), Office 365, Gmail for business or any other IMAP/SMTP compliant messaging system.

msXfax manages outbound and inbound fax calls, delivering them efficiently to the correct destination.

msXfax is an ideal solution for businesses who understand the importance of maintaining privacy in fax communications with their customers and trading partners.

The connector conforms to the Australian Information Security Manual for network separation and Email Protective Marking checks, audit and compliance.

msXfax incorporates XCAPI fax over IP drivers from TE-Systems Inc.

msXfax supports Windows Servers 2012 R2 or 2016 on any hypervisor platform such as VMWare, Hyper-V, Azure and is also supported on AWS.

1.3.1 Summary msXfax version 8

- Support for Windows Server 2012 R2 or Windows Server 2016
- Virtualisation of the fax server software
- Fully test with Sonus Session Border Controllers. Can co-exist with Skype for Business implementations using Sonus SBCs.
- Designed for compliance with ISM for: network separation, audit, data export controls and protective markings/DLMs.
- Support for Fax over IP to compliant equipment and SIP Trunk providers.
- No requirement for Microsoft Office or Acrobat on the fax server
- Robust Microsoft SQL Server/SQL Express support
- Scalable from 2 to 60 channels per fax server VM.
- Multiple fax server VMs supported on one SIP Trunk.
- Scalable to 1900 fax channels per Optus evolve IP service.
- Scalable across data centers using load balancers
- High availability and redundancy achieved using load balancers, DNS, SMTP Connectors, master slave SIP gateways (T.38/G.711).
- Report Generators for SQL Server offering comprehensive reporting, graphs and dashboards.
- Tested with various Ricoh technologies.
- Open standards SMTP allows easy device and application integration.

1.4 Session border controller (SBC)

BNS Group selected Sonus Networks SBC to perform interoperability testing with the Optus SIP Trunk Service.

Sonus enables and secures real-time communications so the world's leading service providers and enterprises can embrace the next generation of SIP and 4G/LTE solutions including VoIP, video, instant messaging and online collaboration.

With customers in nearly 100 countries and nearly two decades of experience, Sonus offers a complete portfolio of hardware-based and virtualized Session Border Controllers (SBCs), Diameter Signaling Controllers (DSCs), policy/ routing servers and media and signaling gateways.

BNS Group acknowledges the support and co-operation from Sonus Networks Australia.

SECTION 2 Test platform

2.1 Test lab configuration

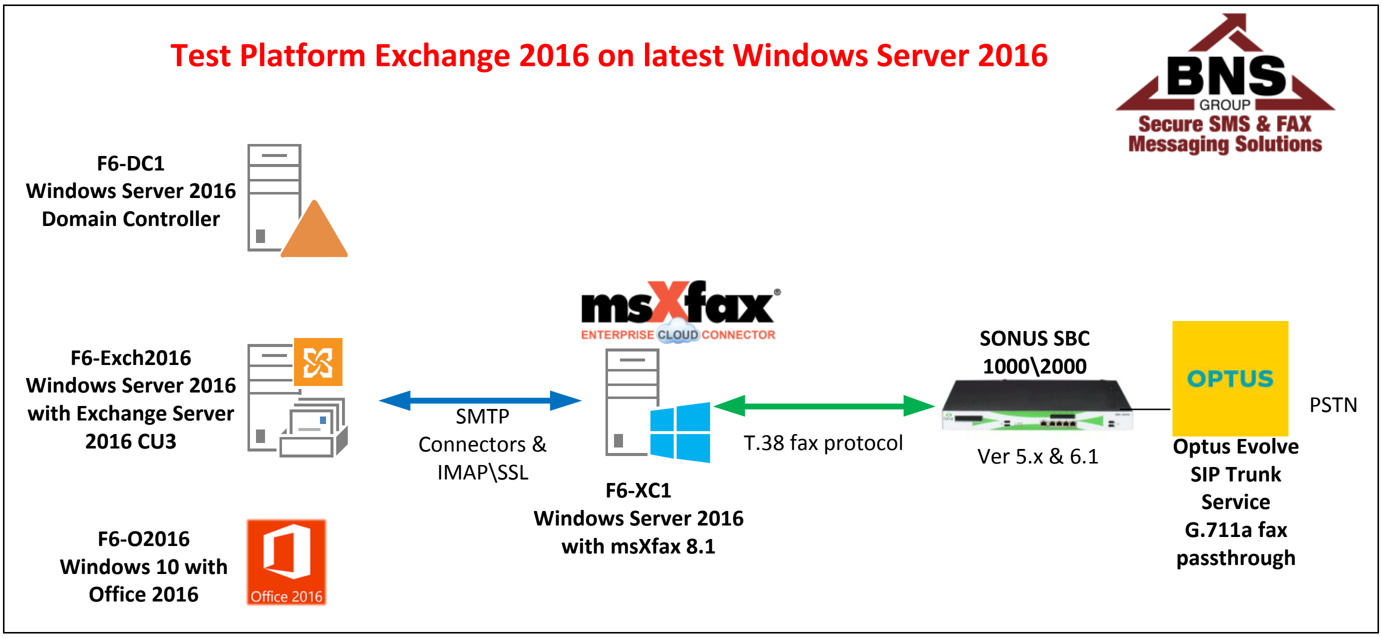


Figure 1 BNS Group Test Lab configuration

- SIP Trunk from Optus: fibre connected service from Optus into the BNS test lab. The service was commissioned on 26 June 2015.
- SBC Sonus 1000 software version 5.0.1 Build 399
- SBC Sonus 2000 software version 6.1.0 build 457 tested in T.38 loopback
- msXfax version 8.1 build 23 with Windows Server 2016 VM 6GB ram 4 x VCPU
- XCAPI 3.6.7
- Microsoft Exchange Server 2016 CU3 with Windows Server 2016 with all updates effective 6 Dec 2016

2.1 Tests conducted

BNS confirms the following tests were performed.

- Connectivity testing using G.711a fax pass through to Optus SIP Trunk to PSTN
- Transcoding from G711a to T.38 on Sonus SBC
- Sending to fax destinations on the PSTN domestic and international
- Receiving faxes from the Optus SIP Trunk Service.
- IMAP\SSL connectivity to Exchange 2016
- SMTP Connectors (send and receive) to Exchange 2016
- Office 2016 on Windows 10 client
- Office 2016 Word, Excel & other document type tests sent via Outlook as attachments to be faxed.
- Load tested with 10,000 faxes 30 channels transmit and 30 channels receive on the 1 Windows server 2016 VM. Sonus SBC used to route SIP to SIP T.38 fax.

SECTION 3 Enterprise faxing

3.1 Reasons why customers do not outsource fax

The following are some of the reasons why fax services are **not** outsourced to the cloud:

- Fax remains one of the few legally recognized forms of electronic document delivery today. Email is not an end to end guaranteed delivery. A fax cloud service provider usually offer SMTP email delivery to a customer. Therefore, if an important legal document is received at your cloud service provider and you fail to receive it via email, the other party would be in a strong position in a legal case.
- The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Privacy Amendment Act) made many significant changes to the *Privacy Act 1988* (Privacy Act). These changes commenced on 12 March 2014.

  The Privacy Regulation 2013, made under the Privacy Act, also commenced on 12 March 2014. Information stored in fax images usually contains sensitive and confidential information which must be secure at all times.
- Some fax service providers only have a point of presence in Australia. The actual fax image is stored in overseas data centers which adds to the complexity and compliance to security. Refer to http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles
- The Australian Privacy Principles (APPs) regulate the handling of personal information by Australian government agencies and some private sector organisations.
- Government Departments and Agencies must follow the ISM and protect material according to its classification. A fax received at a service provider may upon reception be personal, staff-in-confidence, sensitive-legal, contain signatures, bank accounts and other sensitive data. Therefore, organisations who outsource store and forward fax must have measures in place with the fax service provider to provide the same level of security and network classifications as their own networks in addition to providing a guaranteed end to end delivery of the image.
- In Federal Government, outbound fax requests involving email transports must comply with the Email Protective Marking standards. msXfax checks the markings before release to the public switched telephone network.

3.2 Government Security

BNS Group manufactures commercial FAX and SMS messaging software for Corporate and Government customers. msXfax and msXsms Enterprise SMS software focused on meeting the Australian Government Information Security Manual (ISM) requirements published at http://www.dsd.gov.au/infosec/ism/.

msXfax software complies with the Australian Government email protective marking (EPM) standards 2012.3.   msXfax Enterprise Version 8 checks for 2012.3 compliance of the protective marking on email to fax transmissions . Dissemination Limiting Markers (DLMs) are also checked.

EPM standards defines the format of protective markings for Internet email message headers used for messages exchanged within and between Australian Government agencies. A protective marking conveys the protection requirements for information in a message, as defined within the *Australian Government Protective Security Policy Framework*. The protective marking may also contain additional information about the message that tells systems and system users how to appropriately disseminate the information contained in the message.

Many fax products today utilise email as a transport mechanism to send and receive faxes between the fax server and users of the system.

Any Government Department or agency using internal email systems to send faxes via a fax server which communicates to the public switched telephone network, must ensure that gateways and fax servers comply with ISM by implementing Email Protective Marking checking and other security requirements such as network separation, data export controls and audit.

msXfax inspects and checks the SMTP message headers and/or the subject for a compliant marking or DLMs introduced in the ISM 2012.