



## **IPedge Virtual Server Install For R1.7.4 and Later Systems**

# Publication Information

**Toshiba America Information Systems, Inc.  
Telecommunication Systems Division**

## **Publication Information**

Toshiba America Information Systems, Inc., Telecommunication Systems Division, reserves the right, without prior notice, to revise this information publication for any reason, including, but not limited to, utilization of new advances in the state of technical arts or to simply change the design of this document.

Further, Toshiba America Information Systems, Inc., Telecommunication Systems Division, also reserves the right, without prior notice, to make such changes in equipment design or components as engineering or manufacturing methods may warrant.

Version 2, February 2017  
IPedge R1.7.4 and later

Our mission to publish accurate, complete and user accessible documentation. At the time of printing the information in this document was as accurate and current as was reasonably possible. However, in the time required to print and distribute this manual additions, corrections or other changes may have been made. To view the latest version of this or other documents please refer to the Toshiba FYI website.

Toshiba America Information Systems shall not be liable for any commercial losses, loss of revenues or profits, loss of goodwill, inconvenience, or exemplary, special, incidental, indirect or consequential damages whatsoever, or claims of third parties, regardless of the form of any claim that may result from the use of this document.

THE SPECIFICATIONS AND INFORMATION PROVIDED HEREIN ARE FOR INFORMATIONAL PURPOSES ONLY AND ARE NOT A WARRANTY OF ACTUAL PERFORMANCE, WHETHER EXPRESSED OR IMPLIED. THE SPECIFICATIONS AND INFORMATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. ACTUAL PERFORMANCE MAY VARY BASED ON INDIVIDUAL CONFIGURATIONS, USE OF COLLATERAL EQUIPMENT, OR OTHER FACTORS.

## **© Copyright 2014, 2015, 2016, 2017**

This document is copyrighted by Toshiba America Information Systems, Inc. with all rights reserved. Under the copyright laws, this document cannot be reproduced in any form or by any means—graphic, electronic, or mechanical, including recording, taping, photocopying, without prior written permission of Toshiba. No patent liability is assumed, however, with respect to the use of the information contained herein.

## **Trademarks**

Toshiba, IPedge, CIX, CTX, eManager, SoftIPT, Strata, Strata Net, Stratagy, UCedge, are trademarks of Toshiba Corporation or Toshiba America Information Systems, Inc.

Adtran and NetVanta are registered trademarks of Adtran, Inc.

AppCritical is a registered trademark of Apparent Networks, Inc.

Android and Google are trademarks of Google Inc.

Apple is a registered trademark of Apple Inc.

Audacity is a trademark of Dominic M Mazzoni.

Dell is a registered trademark of Dell, Inc.

Linux is a registered trademark of Linus Torvalds.

AudioCodes is Registered trademark of AudioCodes Ltd.

Cisco is a registered trademark of Cisco Technology, Inc.

Mozilla and Firefox are registered trademarks of Mozilla Foundation Corp.

Windows, Outlook, and Microsoft are registered trademarks of Microsoft.

Wireshark is a registered trademark of the WIRESHARK FOUNDATION, INC.

Solarwinds is a trademark of SolarWinds Worldwide, LLC

SonicWALL, TZ100, TZ170, and pro 2040 are registered trademarks of SonicWALL Inc.

VMware is a registered trademark of VMware, Inc.

WhatsUp is a registered trademark of Ipswitch, Inc.

Wi-Fi and Wi-Fi Alliance are registered trademarks of Wi-Fi Alliance.  
GoDaddy is a registered trademark of Go Daddy Operating Company  
Verisign and Thawte are registered trademarks of VeriSign, Inc  
Comodo is a registered trademark of Comodo Security Solutions, Inc  
Trademarks, registered trademarks, and service marks are the property of their respective owners.

## General End User Information

### FCC Requirements

Means of Connection: The IPedge does not connect directly to the telephone network. All direct connections are made to a gateway. Please refer to the gateway manufacturer's documentation

### Radio Frequency Interference

Warning: This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the manufacturer's instruction manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case, the user, at his/her own expense, will be required to take whatever measures may be required to correct the interference.

### Underwriters Laboratory

This system is listed with Underwriters Laboratory (UL). Secondary protection is required, on any wiring from any telephone that exits the building or is subject to lightning or other electrical surges, and on DID, OPS, and Tie lines. (Additional information is provided in this manual.)



### CP01, Issue 8, Part I Section 14.1

Notice: The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee the Equipment will operate to the user's satisfaction.

**Repairs to Certified Equipment** should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

---

**CAUTION!** Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

---

### Important Notice — Music-On-Hold

In accordance with U.S. Copyright Law, a license may be required from the American Society of Composers, Authors and Publishers, or other similar organization, if radio or TV broadcasts are transmitted through the music-on-hold feature of this telecommunication system. Toshiba America Information Systems, Inc., strongly recommends not using radio or television broadcasts and hereby disclaims any liability arising out of the failure to obtain such a license.

**Hearing Aid Compatibility Notice:** The FCC has established rules that require all installed business telephones be hearing aid compatible. This rule applies to all telephones regardless of the date of

manufacture or installation. There are severe financial penalties which may be levied on the end-user for non-compliance.

Regulatory Information		
Area	United States	Canada
Safety	ULn	CSA
Network	FCC CFR 47 Part 68 TIA/EIA/IS-968	IC CS-03
EMC	FCC CFR 47 Part 15	ICES003:2004

### **Emergency Service (911) Warning**

The *IPedge* system must have a constant source of electricity and network connection availability to function. In the event of a power failure or network availability outage the *IPedge* system's SIP service will be disabled. The user understands that in the event of a power or network outage the *IPedge* system will not support 911 emergency services and further, that such services will only be available via user's regular telephone line not connected to the *IPedge* system or gateway. User further acknowledges that any interruption in the supply or delivery of electricity or network availability is beyond Toshiba's control and that Toshiba shall have no responsibility for losses arising from such interruption.

### **Security Warning**

All *IPedge* systems ship with the same default user names and passwords. To help protect your *IPedge* system from unauthorized administrator access change the user names and passwords as described in the new system installation section of the *IPedge* Install manual. An *IPedge* system that is not properly protected may be exposed to toll fraud, denial of service or other attacks.

### **Export Administration Regulation**

This product may not be exported without US Department of Commerce, Bureau of Export Administration authorization. Any export or re-export by the purchaser, directly or indirectly, in contravention of U.S. Export Administration Regulation is prohibited.

# TOSHIBA AMERICA INFORMATION SYSTEMS, INC. ("TAIS")

## Telecommunication Systems Division License Agreement

IMPORTANT: THIS LICENSE AGREEMENT ("AGREEMENT") IS A LEGAL AGREEMENT BETWEEN YOU ("YOU") AND TAIS. CAREFULLY READ THIS LICENSE AGREEMENT. USE OF ANY SOFTWARE OR ANY RELATED INFORMATION (COLLECTIVELY, "SOFTWARE") INSTALLED ON OR SHIPPED WITH A TAIS DIGITAL SOLUTIONS PRODUCT OR OTHERWISE MADE AVAILABLE TO YOU BY TAIS IN WHATEVER FORM OR MEDIA, WILL CONSTITUTE YOUR ACCEPTANCE OF THESE TERMS, UNLESS SEPARATE TERMS ARE PROVIDED BY THE SOFTWARE SUPPLIER. IF YOU DO NOT AGREE WITH THE TERMS OF THIS LICENSE AGREEMENT, DO NOT INSTALL, COPY OR USE THE SOFTWARE AND PROMPTLY RETURN IT TO THE LOCATION FROM WHICH YOU OBTAINED IT IN ACCORDANCE WITH APPLICABLE RETURN POLICIES. EXCEPT AS OTHERWISE AUTHORIZED IN WRITING BY TAIS, THIS SOFTWARE IS LICENSED FOR DISTRIBUTION THROUGH TAIS AUTHORIZED CHANNELS ONLY TO END-USERS PURSUANT TO THIS LICENSE AGREEMENT.

1. License Grant. The Software is not sold; it is licensed upon payment of applicable charges. TAIS grants to you a personal, non-transferable and non-exclusive right to use the copy of the Software provided under this License Agreement. You agree you will not copy the Software except as necessary to use it on one TAIS system at a time at one location. Modifying, translating, renting, copying, distributing, printing, sublicensing, transferring or assigning all or part of the Software, or any rights granted hereunder, to any other persons and removing any proprietary notices, labels or marks from the Software is strictly prohibited except as permitted by applicable law; you agree violation of such restrictions will cause irreparable harm to TAIS and provide grounds for injunctive relief, without notice, against you or any other person in possession of the Software. You and any other person whose possession of the software violates this License Agreement shall promptly surrender possession of the Software to TAIS, upon demand. Furthermore, you hereby agree not to create derivative works based on the Software. TAIS reserves the right to terminate this license and to immediately repossess the software in the event that you or any other person violates this License Agreement. Execution of the Software for any additional capabilities require a valid run-time license.

2. Intellectual Property. You acknowledge that no title to the intellectual property in the Software is transferred to you. You further acknowledge that title and full ownership rights to the Software will remain the exclusive property of TAIS and/or its suppliers, and you will not acquire any rights to the Software, except the license expressly set forth above. You will not remove or change any proprietary notices contained in or on the Software. The Software is protected under US patent, copyright, trade secret, and/or other proprietary laws, as well as international treaties. Any transfer, use, or copying of the software in violation of the License Agreement constitutes copyright infringement. You are hereby on notice that any transfer, use, or copying of the Software in violation of this License Agreement constitutes a willful infringement of copyright.

3. No Reverse Engineering. You agree that you will not attempt, and if you employ employees or engage contractors, you will use your best efforts to prevent your employees and contractors from attempting to reverse compile, reverse engineer, modify, translate or disassemble the Software in whole or in part. Any failure to comply with the above or any other terms and conditions contained herein will result in the automatic termination of this license and the reversion of the rights granted hereunder back to TAIS.

4. Limited Warranty. THE SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, TAIS AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES WITH REGARD TO THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE WARRANTY OF NON-INFRINGEMENT OF THIRD PARTY RIGHTS, THE WARRANTY OF YEAR 2000 COMPLIANCE, AND THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE IS WITH YOU. NEITHER TAIS NOR ITS SUPPLIERS WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. HOWEVER, TAIS WARRANTS THAT ANY MEDIA ON WHICH THE SOFTWARE IS FURNISHED IS FREE FROM DEFECTS IN MATERIAL AND WORKMANSHIP UNDER NORMAL USE FOR A PERIOD OF NINETY (90) DAYS FROM THE DATE OF DELIVERY TO YOU.

5. Limitation Of Liability. TAIS' ENTIRE LIABILITY AND YOUR SOLE AND EXCLUSIVE REMEDY UNDER THIS LICENSE AGREEMENT SHALL BE AT TAIS' OPTION REPLACEMENT OF THE MEDIA OR REFUND OF THE PRICE PAID. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL TAIS OR ITS SUPPLIERS BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, SPECIAL, INCIDENTAL OR INDIRECT DAMAGES FOR PERSONAL INJURY, LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION/DATA, OR ANY OTHER PECUNIARY LOSS OF ANY KIND ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF TAIS OR ITS SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL TAIS OR ITS SUPPLIERS BE LIABLE FOR ANY CLAIM BY A THIRD PARTY.

6. State/Jurisdiction Laws. SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY MAY LAST, OR THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO SUCH LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS LIMITED WARRANTY GIVES YOU SPECIFIC RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE/JURISDICTION TO STATE/JURISDICTION.

7. Export Laws. This License Agreement involves products and/or technical data that may be controlled under the United States Export Administration Regulations and may be subject to the approval of the United States Department of Commerce prior to export. Any export, directly or indirectly, in contravention of the United States Export Administration Regulations, or any other applicable law, regulation or order, is prohibited.

8. Governing Law. This License Agreement will be governed by the laws of the State of California, United States of America, excluding its conflict of law provisions.

9. United States Government Restricted Rights. The Software is provided with Restricted Rights. The Software and other materials provided hereunder constitute Commercial Computer Software and Software Documentation and Technical Data related to Commercial Items. Consistent with F.A.R. 12.211 and 12.212 they are licensed to the U.S. Government under, and the U.S. Government's rights therein are restricted pursuant to, the vendor's commercial license.

10. Severability. If any provision of this License Agreement shall be held to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions hereof shall not in any way be affected or impaired.

11. No Waiver. No waiver of any breach of any provision of this License Agreement shall constitute a waiver of any prior, concurrent or subsequent breach of the same or any other provisions hereof, and no waiver shall be effective unless made in writing and signed by an authorized representative of the waiving party.

12. Supplier Software. The Software may include certain software provided by TAIS suppliers. In such event, you agree that such supplier may be designated by TAIS as a third party beneficiary of TAIS with rights to enforce the Agreement with respect to supplier's software.

YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT AND THAT YOU UNDERSTAND ITS PROVISIONS. YOU AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. YOU FURTHER AGREE THAT THIS LICENSE AGREEMENT CONTAINS THE COMPLETE AND EXCLUSIVE AGREEMENT BETWEEN YOU AND TAIS AND SUPERSEDES ANY PROPOSAL OR PRIOR

AGREEMENT, ORAL OR WRITTEN, OR ANY OTHER COMMUNICATION RELATING TO THE SUBJECT MATTER OF THIS LICENSE AGREEMENT.

**Toshiba America Information Systems, Inc. - Telecommunication Systems Division**

**9740 Irvine Boulevard, Irvine, California 92618-1697, United States of America. DSD 020905**

# **Toshiba America Information Systems, Inc.**

## **Telecommunication Systems Division**

### **End-User Limited Warranty**

Toshiba America Information Systems, Inc., ("TAIS") warrants that this telephone equipment manufactured by Toshiba (except for fuses, lamps, and other consumables) will, upon delivery by TAIS or an authorized TAIS dealer to a retail customer in new condition, be free from defects in material and workmanship for twenty-four (24) months after delivery, except as otherwise provided by TAIS in the TAIS warranty accompanying the products or posted on TAIS's website. Products which are not manufactured by Toshiba but are purchased from Toshiba, will be subject to the warranty provisions provided by the equipment manufacturer, unless TAIS notifies the end-user of any additional warranty provisions in writing.

This warranty is void (a) if the equipment is used under other than normal use and maintenance conditions, (b) if the equipment is modified or altered, unless the modification or alteration is expressly authorized by TAIS, (c) if the equipment is subject to abuse, neglect, lightning, electrical fault, or accident, (d) if the equipment is repaired by someone other than TAIS or an authorized TAIS dealer, (e) if the equipment's serial number is defaced or missing, or (f) if the equipment is installed or used in combination or in assembly with products not supplied by TAIS and which are not compatible or are of inferior quality, design, or performance.

The sole obligation of TAIS or Toshiba Corporation under this warranty, or under any other legal obligation with respect to the equipment, is the repair or replacement of such defective or missing parts as are causing the malfunction by TAIS or its authorized dealer with new or refurbished parts (at their option). If TAIS or one of its authorized dealers does not replace or repair such parts, the retail customer's sole remedy will be a refund of the price charged by TAIS to its dealers for such parts as are proven to be defective, and which are returned to TAIS through one of its authorized dealers within the warranty period and no later than thirty (30) days after such malfunction, whichever first occurs.

Under no circumstances will the retail customer or any user or dealer or other person be entitled to any direct, special, indirect, consequential, or exemplary damages, for breach of contract, tort, or otherwise. Under no circumstances will any such person be entitled to any sum greater than the purchase price paid for the item of equipment that is malfunctioning.

To obtain service under this warranty, the retail customer must bring the malfunction of the machine to the attention of one of TAIS' authorized dealers within the applicable warranty period and no later than thirty (30) days after such malfunction, whichever first occurs. Failure to bring the malfunction to the attention of an authorized TAIS dealer within the prescribed time results in the customer being not entitled to warranty service.

**THERE ARE NO OTHER WARRANTIES FROM EITHER TOSHIBA AMERICA INFORMATION SYSTEMS, INC., OR TOSHIBA CORPORATION WHICH EXTEND BEYOND THE FACE OF THIS WARRANTY. ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND FITNESS FOR USE, ARE EXCLUDED.**

No TAIS dealer and no person other than an officer of TAIS may extend or modify this warranty. No such modification or extension is effective unless it is in writing and signed by the Vice President and General Manager, Telecommunication Systems Division.

## End User License Agreement

### **Preface:**

For users in the following countries, please refer to “TOSHIBA AMERICA INFORMATION SYSTEMS, INC. End User License Agreement” or “TOSHIBA AMERICA INFORMATION SYSTEMS, INC. Contrat de licence de la Division des systèmes de télécommunication.”

- United States of America
- Canada
- Bahamas
- Barbados
- Dominican Republic
- Puerto Rico
- Trinidad

For users in the following countries, please refer to “TOSHIBA CORPORATION End User License Agreement”.

- Australia
- Greece
- Hong Kong
- Indonesia
- Ireland
- Malaysia
- New Zealand
- Saudi Arabia
- Singapore
- South Africa
- Thailand
- United Kingdom

# TOSHIBA AMERICA INFORMATION SYSTEMS, INC.

## End User License Agreement

Toshiba America Information Systems, Inc.  
Telecommunication Systems Division  
9740 Irvine Boulevard  
Irvine, California 92618-1697  
United States of America

**IMPORTANT:** THIS END USER LICENSE AGREEMENT ("EULA") IS A LEGAL AGREEMENT BETWEEN YOU ("YOU") AND TOSHIBA AMERICA INFORMATION SYSTEMS, INC. ("TAIS"). CAREFULLY READ THIS EULA. USE OF ANY PROPRIETARY TOSHIBA AND THIRD PARTY SOFTWARE OR ANY RELATED DOCUMENTATION PRE-INSTALLED ON, OR SHIPPED WITH, A TAIS TELECOMMUNICATION SYSTEMS PRODUCT OR OTHERWISE MADE AVAILABLE TO YOU BY TAIS IN WHATEVER FORM OR MEDIA (COLLECTIVELY, "SOFTWARE"), WILL CONSTITUTE YOUR ACCEPTANCE OF THESE TERMS. IF SEPARATE TERMS ARE PROVIDED BY THE SOFTWARE SUPPLIER, THE TERMS OF THIS EULA THAT ARE NOT INCONSISTENT WITH THOSE SEPARATE TERMS WILL CONTINUE TO BE APPLICABLE. IF YOU DO NOT AGREE WITH THE TERMS OF THIS EULA, DO NOT INSTALL, COPY, OR USE THE SOFTWARE AND PROMPTLY RETURN IT TO THE TAIS AUTHORIZED CHANNEL FROM WHICH YOU OBTAINED IT IN ACCORDANCE WITH APPLICABLE RETURN POLICIES. EXCEPT AS OTHERWISE AUTHORIZED IN WRITING BY TAIS, THIS SOFTWARE IS LICENSED FOR DISTRIBUTION THROUGH AN AUTHORIZED CHANNEL ONLY TO AN END-USER PURSUANT TO THIS EULA. "AUTHORIZED CHANNEL" MEANS TAIS OR A DEALER AUTHORIZED BY TAIS TO PROVIDE TAIS HARDWARE AND/OR SOFTWARE TO END USERS. TAIS IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU OBTAINED THE SOFTWARE FROM AN AUTHORIZED CHANNEL AND ACCEPT ALL TERMS OF THIS EULA. WE MAY CHANGE THESE TERMS AT ANY TIME BY NOTIFYING YOU OF A CHANGE WHEN YOU NEXT START THE SOFTWARE. YOUR CONTINUED USE OF THE SOFTWARE WILL CONSTITUTE YOUR ACCEPTANCE OF SUCH VARIED TERMS.

**1. License Grant.** The Software is not sold; it is licensed upon payment of applicable charges. TAIS grants to you a non-transferable and non-exclusive right to use with a TAIS telecommunication systems product the copy of the Software provided under this EULA that you have obtained from an Authorized Channel. With respect to third party Software, TAIS is only passing along license rights which may be granted by the owner or licensor of the Software and TAIS does not separately license these rights to you. Each copy of the Software is owned by TAIS and/or its suppliers. You agree you will not copy the Software except as necessary to use it on one TAIS system at a time, at one location. Modifying, translating, renting, copying, distributing, printing, sublicensing, transferring, or assigning all or part of the Software, or any rights granted hereunder, to any other persons and removing any proprietary notices, labels or marks from the Software is strictly prohibited except as permitted by applicable law; you agree violation of such restrictions will cause irreparable harm to TAIS and provide grounds for injunctive relief, without notice, against you or any other person in possession of the Software. You and any other person whose possession of the Software violates this EULA shall promptly surrender possession of the Software to TAIS, upon demand. Furthermore, you hereby agree not to create derivative works based on the Software. TAIS reserves the right to terminate this license and to immediately repossess the Software in the event that you or any other person violates this EULA.

**2. Software Support and Upgrade Service.** NOT WITHSTANDING ANY OTHER PROVISION OF THIS EULA, YOU HAVE NO LICENSE OR RIGHT TO ANY SOFTWARE SUPPORT AND UPGRADE SERVICE, UNLESS YOU HOLD A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAVE PAID THE APPLICABLE FEE TO AN AUTHORIZED CHANNEL FOR THE SOFTWARE SUPPORT AND UPGRADE SERVICE. USE OF SOFTWARE SUPPORT AND UPGRADE SERVICE IS LIMITED TO



TAIS TELECOMMUNICATION SYSTEMS PRODUCT SUPPLIED BY AN AUTHORIZED CHANNEL FOR WHICH YOU ARE THE ORIGINAL END USER PURCHASER OR OTHERWISE HOLD A VALID LICENSE TO USE THE SOFTWARE THAT IS BEING UPGRADED.

**3. Copyright.** You acknowledge that no title to the copyright or any other intellectual property rights in the Software is transferred to you. You further acknowledge that title and full ownership rights to the Software and all copies thereof will remain the exclusive property of TAIS and/or its suppliers, and you will not, by this EULA, acquire any rights to the Software or any copies thereof, except the license expressly set forth above. You will not remove or change any proprietary notices contained in or on the Software. The Software is protected under U.S. patent, copyright, trade secret, and/or other proprietary laws, as well as international treaties. Any transfer, use, or copying of the Software in violation of the EULA constitutes copyright infringement. You are hereby on notice that any transfer, use, or copying of the Software in violation of this EULA constitutes a willful infringement of copyright.

**4. Critical Applications.** The Software is not designed or recommended for any "critical applications". "Critical applications" means life support systems, medical applications, connections to implanted medical devices, commercial transportation, nuclear facilities or systems or any other applications where product failure could lead to injury to persons or loss of life or catastrophic property damage. ACCORDINGLY, SHOULD YOU DECIDE TO USE THIS SOFTWARE FOR ANY CRITICAL APPLICATION, TAIS DISCLAIMS, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ANY AND ALL LIABILITY ARISING OUT OF THE USE OF THE SOFTWARE IN ANY CRITICAL APPLICATION. IF YOU USE THE SOFTWARE IN A CRITICAL APPLICATION, YOU, AND NOT TAIS, ASSUME FULL RESPONSIBILITY FOR SUCH USE. Further, you shall indemnify and hold TAIS harmless from any and all damages, liabilities, costs, and expenses, including reasonable attorneys' fees and amounts paid in settlement of third party or government claims, incurred by TAIS as a result of or in any way arising from such use.

**5. No Reverse Engineering.** You agree that you will not attempt, and if you employ employees or engage contractors, you will use your best efforts to prevent your employees and contractors from attempting to reverse compile, reverse engineer, modify, translate or disassemble the Software in whole or in part. Any failure to comply with the above or any other terms and conditions contained herein will result in the automatic termination of this license and the reversion of the rights granted hereunder back to TAIS. Notwithstanding the foregoing, in regard to any conflict between the terms of this Section 5 and any applicable open source license agreements (as referred to herein) for any open source software included in the Software, the terms of the applicable open source license agreement controls.

**6. Limited Warranty.** THE HARDWARE PRODUCT LIMITED WARRANTY IS SET FORTH IN THE TAIS STANDARD LIMITED WARRANTY ASSOCIATED WITH THE HARDWARE PRODUCT, WHICH MAY BE POSTED ON THE TAIS TELECOMMUNICATION SYSTEMS DIVISION INTERNET WEBSITE. TAIS' SOLE OBLIGATIONS WITH RESPECT TO TOSHIBA SOFTWARE IS SET FORTH IN THIS EULA. UNLESS OTHERWISE STATED IN WRITING, ALL TOSHIBA AND THIRD PARTY SOFTWARE ARE PROVIDED ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND BY TOSHIBA. UNLESS THIRD PARTY SOFTWARE MANUFACTURERS, SUPPLIERS OR PUBLISHERS EXPRESSLY OFFER THEIR OWN WARRANTIES IN WRITING IN CONNECTION WITH YOUR USE OF THEIR THIRD PARTY SOFTWARE, SUCH THIRD PARTY SOFTWARE IS PROVIDED ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND BY THE MANUFACTURER, SUPPLIER, OR PUBLISHER OF SUCH THIRD PARTY SOFTWARE. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, TAIS AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES WITH REGARD TO THE SOFTWARE, EITHER EXPRESS OR IMPLIED, OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE WARRANTY OF NON-INFRINGEMENT OF THIRD PARTY RIGHTS, AND THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE IS WITH YOU. NEITHER TAIS NOR ITS SUPPLIERS WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR

ERROR-FREE. HOWEVER, TAIS WARRANTS THAT ANY MEDIA ON WHICH THE SOFTWARE IS FURNISHED IS FREE FROM DEFECTS IN MATERIAL AND WORKMANSHIP UNDER NORMAL USE FOR A PERIOD OF NINETY (90) DAYS FROM THE DATE OF DELIVERY TO YOU. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY TAIS OR A TAIS AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS LIMITED WARRANTY GIVES YOU SPECIFIC RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE/JURISDICTION TO STATE/JURISDICTION.

**7. Limitation of Liability.** TAIS' AND/OR ITS SUPPLIERS' ENTIRE LIABILITY AND YOUR SOLE AND EXCLUSIVE REMEDY UNDER THIS EULA SHALL BE, AT TAIS' OPTION, REPLACEMENT OF THE SOFTWARE OR REFUND OF THE PRICE PAID. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL TAIS OR ITS SUPPLIERS BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES FOR PERSONAL INJURY, LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION/ DATA, OR ANY OTHER PECUNIARY LOSS OF ANY KIND ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, OR OTHERWISE IN CONNECTION WITH ANY PROVISION OF THIS EULA EVEN IF TAIS OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF THE REMEDY FAILS OF ITS ESSENTIAL PURPOSE. IN NO EVENT SHALL TAIS OR ITS SUPPLIERS BE LIABLE FOR ANY CLAIM BY A THIRD PARTY. DATA USAGE RATES MAY APPLY WHEN DATA IS SENT OR RECEIVED WHILE USING THE SOFTWARE. YOU ARE SOLELY RESPONSIBLE FOR ANY SUCH DATA USAGE AND APPLICABLE CHARGES. ASK YOUR WIRELESS PROVIDER FOR FURTHER DETAILS ON RATES THAT MAY APPLY TO YOU.

**8. State/Jurisdiction Laws.** SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY MAY LAST, THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR THE EXCLUSION OF LIABILITY FOR DEATH OR PERSONAL INJURY CAUSED BY NEGLIGENCE, SO SUCH LIMITATIONS OR EXCLUSIONS IN THIS EULA MAY NOT APPLY TO YOU.

**9. Export Laws.** This EULA involves products and/or technical data that may be controlled under the laws of the United States and other countries, including but not limited to the United States Export Administration Regulations, and any other applicable law, regulation or order ("Export Laws"). The products and/or technical data involved with this EULA may not be exported without US Department of Commerce, Bureau of Export Administration authorization. Any export or re-export by you, directly or indirectly, in contravention of any of the Export Laws is prohibited. You shall comply with all Export Laws to assure that the Software is not exported, directly or indirectly, in contravention of the Export Laws.

**10. Governing Law.** This EULA will be governed by the laws of the State of California, United States of America, excluding its conflict of law provisions.

**11. United States Government Restricted Rights.** The Software is provided with RESTRICTED RIGHTS. The Software and other materials provided hereunder constitute Commercial Computer Software and Software Documentation and Technical Data related to Commercial Items. Use, duplication, or disclosure by the United States Government, its agencies and/or instrumentalities is subject to restrictions of this Agreement pursuant to FAR 12.211, FAR 12.212(a), DFARS 227.7202-1, DFARS 227.7202-3(a), and DFARS 252.227.7014(a)(1) as applicable. Without limiting the foregoing, use, duplication, or disclosure by the United States Government, its agencies and/or instrumentalities is subject to restrictions as set forth in subparagraph (c)(1)(ii) of The Rights in Technical Data and Computer Software Clause at DFARS 252.227-7013 (October 1988) or subparagraphs (c)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19, FAR 52.227-19(b)(1) and (2) (DEC 2007), FAR 52.227-14 (DEC 2007) including Alt. III, FAR 52.227-20, and DFARS 252.227-7015 as applicable.

**12. Severability.** If any provision of this EULA shall be held to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions hereof shall not in any way be affected or impaired.

**13. No Waiver.** No waiver of any breach of any provision of this EULA shall constitute a waiver of any prior, concurrent or subsequent breach of the same or any other provisions hereof, and no waiver shall be effective unless made in writing and signed by an authorized representative of the waiving party. To the extent the terms of any TAIS policies or programs for support services conflict with the terms of this EULA, the terms of this EULA shall prevail.

**14. Supplier Software.** The Software may include certain software provided by TAIS suppliers. In such event, you agree that such supplier may be designated by TAIS as a third party beneficiary of TAIS with rights to enforce the EULA with respect to supplier's software.

**15. MIB Download Confidentiality and Non Disclosure.** Upon downloading any management-information-base technical information and data (collectively, "MIB"), you agree that the MIB is for limited use, only for implementation and use in connection with IPedge® or Strata® CIX™. It may not be sold, shared, or distributed by you, but may be shared with your own employees, consultants or third party developer(s) who have a reasonable need to know said information and are bound by the terms and conditions of this EULA. The MIB is considered proprietary and confidential information of TAIS and no rights, title or interest are being transferred hereunder. When the purpose in which the MIB was intended is no longer valid, the information shall be destroyed or returned to TAIS. Any unauthorized distribution, posting, sharing, or publishing of the MIB is strictly prohibited. The obligation to maintain confidentiality of information received hereunder, including code or MIB, will survive the expiration or termination of this agreement by seven (7) years, or three (3) years from the date of the end of production of the product (including succession products), whichever is longer.

**16. Open Source Software.** The Software may contain software files that are subject to certain open source license agreements. The open source software files and additional terms and conditions may be included in the TAIS Telecommunication Systems Division product general description, Internet website or electronically within the product. The open source software files are provided "AS IS" to the maximum extent permitted by applicable law. Please read the open source and third party software terms and conditions carefully for relevant copyright and licensing terms.

YOU ACKNOWLEDGE THAT YOU HAVE READ THIS EULA AND THAT YOU UNDERSTAND ITS PROVISIONS. YOU AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. YOU FURTHER AGREE THAT THIS EULA CONTAINS THE COMPLETE AND EXCLUSIVE AGREEMENT BETWEEN YOU AND TAIS AND SUPERSEDES ANY PROPOSAL OR PRIOR AGREEMENT, ORAL OR WRITTEN, OR ANY OTHER COMMUNICATION RELATING TO THE SUBJECT MATTER OF THIS EULA.

Copyright © 2007-2016 Toshiba America Information Systems, Inc. All Rights Reserved.

## **Contrat de licence d'utilisation**

### **Avant-propos:**

Les utilisateurs résidant dans les pays suivants sont priés de consulter le Contrat de licence d'utilisation intitulé : « TOSHIBA AMERICA INFORMATION SYSTEMS INC., Contrat de licence de la Division des systèmes de télécommunication.

- États-Unis d'Amérique
- Canada
- Bahamas
- Barbade
- République dominicaine
- Porto Rico
- Trinidad

Les utilisateurs résidant dans les pays suivants sont priés de consulter le document intitulé : « TOSHIBA CORPORATION End User Licence Agreement. »

- Australie
- Grèce
- Hong Kong
- Indonésie
- Irlande
- Malaisie
- Nouvelle-Zélande
- Arabie Saoudite
- Singapour
- Thaïlande
- Royaume-Uni

**TOSHIBA AMERICA INFORMATION SYSTEMS, INC.**  
**Contrat de licence d'utilisation**

Toshiba America Information Systems, Inc. Telecommunication Systems Division 9740 Irvine Boulevard  
Irvine, California 92618-1697  
United States of America

**IMPORTANT** : LE PRÉSENT CONTRAT DE LICENCE D'UTILISATION (« CLU ») CONSTITUE UN ACCORD JURIDIQUE ENTRE VOUS (« VOUS ») ET TOSHIBA AMERICA INFORMATION SYSTEMS, INC. (« TAIS »). VEUILLEZ LE LIRE ATTENTIVEMENT. L'UTILISATION DE TOUT LOGICIEL EXCLUSIF ET DE TIERS ET DE TOUTE DOCUMENTATION Y ÉTANT RELIÉE (NOMMÉS COLLECTIVEMENT « LOGICIEL »), LEQUEL EST PRÉINSTALLÉ DANS UN SYSTÈME DE TÉLÉCOMMUNICATION DE TAIS OU EXPÉDIÉ À MÊME CE PRODUIT, OU QUE TAIS MET À VOTRE DISPOSITION DE QUELQUE MANIÈRE OU SOUS QUELQUE SUPPORT QUE CE SOIT (NOMMÉS COLLECTIVEMENT « LOGICIEL »), FAIT FOI DE VOTRE ACCEPTATION DES PRÉSENTES MODALITÉS. LORSQUE CERTAINS FOURNISSEURS INDÉPENDANTS DE LOGICIELS APPLIQUENT DES MODALITÉS DISTINCTES, TOUTES MODALITÉS DU PRÉSENT CLU N'ENTRANT PAS EN CONFLIT AVEC DE TELLES MODALITÉS DISTINCTES S'APPLIQUENT. SI VOUS REFUSEZ D'ACCEPTER LES MODALITÉS DU PRÉSENT CLU, VOUS NE DEVEZ NI INSTALLER, NI COPIER, NI UTILISER LE PRÉSENT LOGICIEL ET DEVEZ LE RETOURNER SANS DÉLAI À L'ENDROIT OÙ VOUS L'AVEZ OBTENU, CONFORMÉMENT AUX POLITIQUES DE RETOUR EN VIGUEUR. À MOINS D'UNE AUTORISATION CONTRAIRE PAR ÉCRIT DE TAIS, LE PRÉSENT LOGICIEL VOUS EST CONCÉDÉ SOUS LICENCE À DES FINS EXCLUSIVES DE DISTRIBUTION AUX UTILISATEURS PAR CIRCUITS DE DISTRIBUTION AUTORISÉS EN VERTU DU PRÉSENT CLU. LE TERME « CIRCUITS AUTORISÉS » SIGNIFIE TAIS OU TOUT CONCESSIONNAIRE AUTORISÉ PAR TAIS À FOURNIR AUX UTILISATEURS ULTIMES DU MATÉRIEL ET/OU DES LOGICIELS DE TAIS. TAIS CONSENT À VOUS OCTROYER UNE LICENCE D'UTILISATION DE CE LOGICIEL UNIQUEMENT À CONDITION QUE VOUS L'AYEZ ACQUIS PAR L'ENTREMISE D'UN CIRCUIT AUTORISÉ ET QUE VOUS ACCEPTIEZ LES MODALITÉS DU PRÉSENT CLU.

**1. Octroi de licence.** Le présent logiciel ne vous est pas vendu; vous êtes autorisé à l'utiliser moyennant le paiement des frais applicables. TAIS vous accorde le droit individuel, non transférable et non exclusif d'utiliser une copie du logiciel fourni en vertu du présent contrat avec tout système de télécommunication TAIS à condition que vous l'ayez acquis par circuit autorisé. En ce qui a trait aux logiciels de tiers, TAIS vous communique uniquement les droits d'utilisation pouvant être accordés par le propriétaire ou le concédant d'une licence du logiciel et TAIS ne vous octroie aucune licence d'utilisation distincte en rapport avec de tels droits. Toutes les copies du logiciel appartient à TAIS et/ou à ses fournisseurs. Vous acceptez de ne pas copier ce logiciel, à moins que ce ne soit nécessaire pour l'utiliser sur un seul système TAIS à la fois et à un seul endroit. Sauf là où la loi l'autorise, il est strictement interdit de modifier, de traduire, de louer, de reproduire, de distribuer, d'imprimer, de transférer ou de céder, en tout ou en partie, les droits accordés en vertu du présent CLU à des tiers, et d'enlever les avis, les étiquettes et les marques privatives de ce logiciel. Vous reconnaissez que toute violation de ces interdictions causera un préjudice irréparable à TAIS et lui fournira les motifs nécessaires à des mesures injonctives, sans préavis, contre vous et toute autre personne ayant le logiciel en sa possession. Vous et toute personne dont la possession du logiciel viole le présent CLU devez rendre le logiciel à TAIS sur demande. Vous acceptez de plus de ne créer aucune oeuvre dérivée du présent logiciel. En cas de violation du présent CLU par vous ou par un tiers, TAIS se réserve le droit de le résilier et de reprendre immédiatement possession dudit logiciel.

**2. Services de soutien et de mise à niveau logicielle.** NONOBTANT LES AUTRES DISPOSITIONS DU PRÉSENT CLU, VOUS NE DISPOSEZ D'AUCUNE LICENCE NI D'AUCUN DROIT À QUELQUE SERVICE DE SOUTIEN ET DE MISE À NIVEAU LOGICIELLE QUE CE SOIT, À MOINS DE DISPOSER D'UNE LICENCE D'UTILISATION VALIDE DU LOGICIEL D'ORIGINE ET D'AVOIR PAYÉ LES DROITS APPLICABLES À UN CIRCUIT AUTORISÉ POUR DE TELS SERVICES DE SOUTIEN ET DE MISE À NIVEAU. L'UTILISATION DES SERVICES DE SOUTIEN ET DE MISE À NIVEAU LOGICIELLE EST

RÉSERVÉE AUX SYSTÈMES ET PRODUITS DE TÉLÉCOMMUNICATION TAIS DONT VOUS ÊTES L'ACHETEUR INITIAL OU POUR LESQUELS VOUS DÉTENEZ UNE LICENCE D'UTILISATION VALIDE DU LOGICIEL DEVANT ÊTRE MIS À NIVEAU.

**3. Les droits d'auteur.** Vous reconnaissez que les droits d'auteur et autres droits à la propriété intellectuelle de ces logiciels ne vous sont nullement cédés. Vous reconnaissez de plus que les titres et les droits à la pleine propriété de ces logiciels et de toutes copies pouvant en découler demeurent la propriété exclusive de TAIS et/ou de ses fournisseurs, et que le présent CLU ne vous cède aucun droit à ces logiciels ou aux copies dudit logiciel, sauf dans les cas expressément indiqués ci-dessus. Vous ne devez supprimer ni modifier les avis privatifs inscrits sur ou dans le présent logiciel. Ce logiciel est protégé par les lois américaines sur les brevets, les droits à la propriété intellectuelle et le secret industriel, par d'autres lois sur la propriété et par des traités internationaux. Tout transfert, usage ou reproduction de ce logiciel en violation du présent CLU constitue une atteinte aux droits d'auteur. Veuillez donc être prévenu que tout transfert, usage ou reproduction du logiciel en violation du présent CLU constitue une atteinte volontaire aux droits d'auteur.

**4. Logiciels d'applications essentielles.** Ce logiciel n'est pas conçu ni proposé à des fins « d'applications essentielles ». Les « applications essentielles » se définissent comme tout système de survie, toutes applications médicales, toutes connexions à des appareils médicaux pour personnes atteintes de déficiences, à des services de transport commerciaux, à des installations nucléaires et à quelques autres applications où une panne du produit risque d'entraîner des blessures, des pertes de vies ou des dommages catastrophiques à la propriété. AINSI, SI VOUS DÉCIDEZ D'UTILISER CE LOGICIEL À TITRE D'APPLICATION ESSENTIELLE, TAIS DÉCLINE ALORS TOUTE RESPONSABILITÉ DÉCOULANT DE L'UTILISATION DE CE LOGICIEL À DES FINS D'APPLICATIONS ESSENTIELLES, QUELLES QU'ELLES SOIENT. SI VOUS UTILISEZ CE LOGICIEL À DES FINS D'APPLICATIONS ESSENTIELLES, VOUS EN ASSUMEREZ SEUL (ET NON TAIS) LA RESPONSABILITÉ À PART ENTIÈRE. Vous devrez de plus indemniser et dédommager TAIS pour tous dommages, pour toutes responsabilités, pour tous les coûts et toutes les dépenses encourues par TAIS, y compris pour les frais raisonnables d'avocats et pour tout montant que TAIS devra payer en guise de règlement à des tiers ou au gouvernement suite à une telle utilisation.

**5. Interdiction de désosser.** Vous consentez à ne pas tenter de décompiler, désosser, modifier, traduire, ni démonter le présent logiciel, en tout ou en partie. Si vous embauchez du personnel ou des entrepreneurs, vous consentez à faire de votre mieux pour empêcher que ces employés et ces entrepreneurs ne décompilent, ne désossent, ne modifient, ne traduisent ou ne démontent ce logiciel, en tout ou en partie. L'inobservation de cette disposition ou de toutes autres modalités et conditions du présent CLU entraînera la résiliation automatique de ce dernier et la réversion à TAIS des droits accordés en vertu de ce contrat. Nonobstant les dispositions précédentes en ce qui a trait aux conflits pouvant exister entre les modalités du présent article 5 et de tout contrat de licence pour logiciel ouvert (dont il est question dans la présente), compris dans le présent Logiciel, les modalités du contrat de licence pour logiciel ouvert l'emporteront sur de telles dispositions.

**6. Garantie limitée.** LA GARANTIE LIMITÉE SUR LE MATÉRIEL EST FORMULÉE DANS LA GARANTIE LIMITÉE COURANTE DE TAIS SUR LE MATÉRIEL, LAQUELLE POURRAIT ÊTRE PUBLIÉE SUR LE SITE INTERNET DE LA DIVISION DES TÉLÉCOMMUNICATIONS DE TAIS. LA SEULE OBLIGATION DE TAIS EN RAPPORT AVEC LA GARANTIE SUR LE LOGICIEL TOSHIBA EST FORMULÉE DANS LE PRÉSENT CLU. SAUF AVIS CONTRAIRE PAR ÉCRIT, TOUS LES LOGICIELS DE TOSHIBA ET DE TIERS SONT FOURNIS « TELS QUELS », SANS AUCUNE GARANTIE DE TOSHIBA. À MOINS QUE LES FABRICANTS, FOURNISSEURS ET ÉDITEURS DE LOGICIELS DE TIERS VOUS OFFRENT EXPRESSÉMENT ET PAR ÉCRIT LEURS PROPRES GARANTIES EN CE QUI A TRAIT À L'UTILISATION DE LEURS LOGICIELS DE TIERS, DE TELS LOGICIELS DE TIERS SONT FOURNIS « TELS QUELS », SANS AUCUNE GARANTIE DES FABRICANTS, FOURNISSEURS OU ÉDITEURS DE TELS LOGICIELS DE TIERS. DANS LA PLEINE MESURE PERMISE PAR LES LOIS APPLICABLES, TAIS ET SES FOURNISSEURS SE DÉSAVOUENT DE TOUTES GARANTIES EXPRESSES OU TACITES À L'ÉGARD DU LOGICIEL, NOTAMMENT LES GARANTIES DE NON-

VIOLATION DES DROITS DES TIERS ET TOUTE GARANTIE IMPLICITE DE COMMERCIALITÉ ET D'ADAPTATION À UN USAGE PARTICULIER. VOUS ACCEPTEZ TOUS LES RISQUES EN CE QUI CONCERNE LA QUALITÉ ET LE RENDEMENT DE CE LOGICIEL. NI TAIS NI SES FOURNISSEURS NE GARANTISSENT QUE LES FONCTIONS DU LOGICIEL RÉPONDENT À VOS EXIGENCES, OU QUE LE LOGICIEL FONCTIONNERA SANS INTERRUPTION NI ERREUR. TAIS GARANTIT CEPENDANT QUE, DANS DES CONDITIONS D'USAGE NORMAL, LES SUPPORTS SUR LESQUELS LE LOGICIEL VOUS EST FOURNI SERONT EXEMPTS DE DÉFECTUOSITÉS MATÉRIELLES ET DE FABRICATION PENDANT QUATRE-VINGT-DIX (90) JOURS DE LA DATE DE LIVRAISON DU LOGICIEL. AUCUNE INFORMATION ET AUCUN CONSEIL QUE TAIS OU SES REPRÉSENTANTS AUTORISÉS POURRAIENT VOUS TRANSMETTRE VERBALEMENT NE CONSTITUENT QUELQUE GARANTIE QUE CE SOIT ET ILS N'AUGMENTENT NULLEMENT LA PORTÉE DE LA PRÉSENTE GARANTIE.

**7. Limitation de la responsabilité.** LE REMPLACEMENT DES SUPPORTS OU LE REMBOURSEMENT DU PRIX DU LOGICIEL, SELON LE CHOIX DE TAIS, CONSTITUE L'UNIQUE RESPONSABILITÉ DE TAIS ET VOTRE SEUL RECOURS EN VERTU DU PRÉSENT CLU. DANS LA PLEINE MESURE PERMISE PAR LES LOIS EN VIGUEUR, TAIS ET SES FOURNISSEURS NE SERONT NULLEMENT TENUS RESPONSABLES DE QUELQUE DOMMAGE CONSÉCUTIF, PARTICULIER, ACCESSOIRE OU INDIRECT QUE CE SOIT EN CAS DE BLESSURES CORPORELLES, DE PERTES DE PROFITS COMMERCIAUX, D'INTERRUPTION DES ACTIVITÉS COMMERCIALES, DE PERTES D'INFORMATIONS OU DE DONNÉES COMMERCIALES OU DE TOUTE AUTRE PERTE FINANCIÈRE QUE CE SOIT DÉCOULANT DE L'UTILISATION OU DE L'IMPOSSIBILITÉ D'UTILISER LE LOGICIEL OU DE TOUTE AUTRE DISPOSITION DU PRÉSENT CLU, MÊME SI TAIS ET SES FOURNISSEURS ONT ÉTÉ AVISÉS DE LA POSSIBILITÉ DE TELS DOMMAGES ET MÊME SI LES MOYENS D'Y REMÉDIER SONT INSATISFAISANTS. NI TAIS NI SES FOURNISSEURS NE PEUVENT EN AUCUN CAS ÊTRE TENUS RESPONSABLES DE RÉCLAMATIONS DÉPOSÉES PAR DES TIERS.

**8. Lois provinciales et territoriales.** CERTAINES PROVINCES ET CERTAINS TERRITOIRES NE PERMETTENT PAS D'EXCLURE LES GARANTIES IMPLICITES, DE LIMITER LA DURÉE D'UNE GARANTIE IMPLICITE NI D'EXCLURE OU DE LIMITER LES DOMMAGES CONSÉCUTIFS OU ACCESSOIRES. IL SE POURRAIT DONC QUE VOUS NE SOYEZ PAS TOUCHÉ PAR DE TELLES EXCLUSIONS OU LIMITATIONS.

**9. Lois sur l'exportation.** Le présent CLU se réfère à des produits et/ou à des données techniques sous contrôle américain et d'autres pays, y compris, mais sans s'y limiter, des règlements de la *United States Export Administration* (administration des exportations des États-Unis) et de toutes autres lois, tout autre règlement ou décret (« Lois sur l'exportation ») applicables. Vous ne devez pas exporter les produits et/ou données techniques dont il est question dans le présent CLU sans l'autorisation du *Department of Commerce, Bureau of Export Administration* (Département du commerce, bureau américain de gestion des exportations). Les exportations directes ou indirectes en violation des règlements des *United States Export Administration Regulations* (administration des exportations des États-Unis), ou de tout autre règlement, loi ou ordonnance applicables, sont interdits. Vous devrez vous conformer à l'ensemble des lois sur l'exportation pour éviter que ce Logiciel ne soit pas exporté, directement ou indirectement, en violation des lois sur l'exportation.

**10. Lois applicables.** Le présent contrat est assujetti aux lois de la Californie (États-Unis d'Amérique), à l'exclusion de ses dispositions sur les conflits de lois.

**11. Droits limités du gouvernement des États-Unis.** Ce logiciel est fourni avec des DROITS LIMITÉS. Ce logiciel et les autres éléments matériels fournis en vertu des présentes constituent le logiciel commercial, la documentation sur le logiciel et les données techniques ayant trait à ces éléments commerciaux. Conformément aux F.A.R. 12.211 et 12.212(a), DFARS 227.7202-1, DFARS 227.7202-3(a) et DFARS 252.227.7014(a)(1) américains, selon le cas, l'utilisation, la reproduction ou la divulgation par le gouvernement américain, ses agences et/ou ses institutions sont soumis, à cet égard, aux

restrictions du présent CLU. Sans restreindre le caractère général de ce qui précède, toute utilisation, reproduction ou divulgation par le gouvernement américain, ses agences et/ou ses institutions sont soumises aux restrictions formulées dans le sous-alinéa (c)(1)(ii) des clauses suivantes : *The Rights in Technical Data and Computer Software Clause at DFARS 252.227-7013 (October 1988) or subparagraphs (c)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19, FAR 52.227-19(b)(1) and (2) (DEC 2007), FAR 52.227-14 (DEC 2007) including Alt. III, FAR 52.227-20, et DFARS 252.227-7015*, selon le cas.

**12. Divisibilité :** Si une disposition quelconque du présent contrat est jugée invalide, illégale ou inexécutable, la validité, la légalité et le caractère exécutoire des dispositions restantes ne seront d'aucune manière touchés, ni compromis.

**13. Aucune renonciation.** Aucune renonciation au droit de résiliation pour violation d'une disposition du présent CLU ne peut constituer une renonciation au droit de résiliation pour violation précédente, coïncidente ou subséquente de la même disposition ou d'autres dispositions. Une renonciation n'est exécutoire que lorsqu'elle est faite par écrit et qu'elle est dûment signée par un représentant autorisé de la partie l'ayant initiée. Dans la mesure où les modalités de toutes politiques ou de tous programmes de TAIS en ce qui a trait aux services de soutien entrent en conflit avec les modalités du présent CLU, les modalités du présent CLU l'emportent.

**14. Logiciels d'autres fournisseurs.** Il se peut que le présent logiciel soit accompagné de logiciels offerts par des fournisseurs de TAIS. Le cas échéant, vous reconnaissez que de tels fournisseurs peuvent être désignés par TAIS à titre de tiers bénéficiaires de TAIS, et qu'ils sont autorisés à faire respecter les modalités du présent contrat en ce qui a trait à de tels logiciels de fournisseurs.

**15. Confidentialité et non-divulgation ayant trait au téléchargement de la BGI.** En téléchargeant les renseignements et les données techniques de la base de gestion d'informations (nommés collectivement « BGI »), vous consentez à utiliser ladite BGI de façon limitée et à des fins uniques de mise en oeuvre sur les systèmes IPedge et Strata CIX. Il vous est interdit de vendre, de partager ou de distribuer de tels renseignements; vous pouvez toutefois les partager avec votre personnel, vos conseillers et réalisateurs de logiciels de tiers qui ont nécessité raisonnable d'accès à de tels renseignements et qui sont alors liées par les modalités du présent CLU. Ce BGI contient des renseignements exclusifs à TAIS et confidentiels et, à cet égard, le présent CLU ne vous cède aucun droit, titre, ni intérêt. Lorsque les fins auxquelles ce BGI était destiné ne sont plus valables, ces données doivent être détruites ou renvoyées à TAIS. Il est strictement interdit de distribuer, d'afficher, de partager ou de publier ce BGI sans autorisation. L'obligation de préserver la confidentialité des données obtenues en vertu du présent CLU, y compris le code et le BGI, survivra à la date d'expiration ou à de résiliation du présent CLU pendant sept (7) ans, ou au terme de la production de ce produit et de produits patrimoniaux pendant trois (3) ans, la plus longue de ces périodes étant prise en considération.

**16. Logiciels ouverts.** Il se peut que le présent logiciel contienne de fichiers soumis à certaines licences de logiciels ouverts. Les fichiers de logiciels ouverts et les autres modalités et conditions y étant reliés pourraient être publiés dans la description générale du produit de la Division des systèmes de télécommunication de TAIS, sur son site Internet ou en format électronique à même le produit. Dans la mesure permise par les lois en vigueur, de tels fichiers de logiciels ouverts vous sont fournis « TELS QUELS ». Veuillez lire attentivement les modalités et conditions ayant trait aux logiciels ouverts et aux logiciels de tiers pour en obtenir les conditions relatives aux droits d'auteurs et à l'octroi de licence.

**17. VOUS RECONNAISSEZ AVOIR LU LE PRÉSENT CONTRAT ET EN COMPRENDRE LES DISPOSITIONS. VOUS CONSENTEZ À ÊTRE LIÉ PAR LES MODALITÉS QU'IL CONTIENT. VOUS RECONNAISSEZ ÉGALEMENT QUE LE PRÉSENT DOCUMENT RENFERME L'ENTENTE INTÉGRALE ET EXCLUSIVE ENTRE VOUS ET TAIS, ET QU'IL REMPLACE TOUTE PROPOSITION OU ENTENTE VERBALE OU ÉCRITE PRÉCÉDENTE, AINSI QUE TOUTE AUTRE COMMUNICATION CONCERNANT L'OBJET DU PRÉSENT CONTRAT.**

© Toshiba America Information Systems, Inc. 2007-2016. Tous droits réservés.



# TOSHIBA CORPORATION

## End User License Agreement

Toshiba Corporation Industrial ICT Solutions Company,  
Global Sales Department  
Smart Community Center  
72-34 Horikawa-cho, Saiwai-ku, Kawasaki 212-8585  
Japan

**IMPORTANT:** THIS END USER LICENSE AGREEMENT (“EULA”) IS A LEGAL AGREEMENT BETWEEN YOU (“YOU”) AND TOSHIBA CORPORATION (“TOSHIBA”). CAREFULLY READ THIS EULA. USE OF ANY PROPRIETARY TOSHIBA AND THIRD PARTY SOFTWARE OR ANY RELATED DOCUMENTATION PRE-INSTALLED ON, OR SHIPPED WITH, A TOSHIBA TELECOMMUNICATION SYSTEMS PRODUCT OR OTHERWISE MADE AVAILABLE TO YOU BY TOSHIBA IN WHATEVER FORM OR MEDIA (COLLECTIVELY, “SOFTWARE”), WILL CONSTITUTE YOUR ACCEPTANCE OF THESE TERMS. IF SEPARATE TERMS ARE PROVIDED BY THE SOFTWARE SUPPLIER, THE TERMS OF THIS EULA THAT ARE NOT INCONSISTENT WITH THOSE SEPARATE TERMS WILL CONTINUE TO BE APPLICABLE. IF YOU DO NOT AGREE WITH THE TERMS OF THIS EULA, DO NOT INSTALL, COPY, OR USE THE SOFTWARE AND PROMPTLY RETURN IT TO THE TOSHIBA AUTHORIZED CHANNEL FROM WHICH YOU OBTAINED IT IN ACCORDANCE WITH APPLICABLE RETURN POLICIES. EXCEPT AS OTHERWISE AUTHORIZED IN WRITING BY TOSHIBA, THIS SOFTWARE IS LICENSED FOR DISTRIBUTION THROUGH AN AUTHORIZED CHANNEL ONLY TO AN END-USER PURSUANT TO THIS EULA. “AUTHORIZED CHANNEL” MEANS TOSHIBA OR A DEALER AUTHORIZED BY TOSHIBA TO PROVIDE TOSHIBA HARDWARE AND/OR SOFTWARE TO END USERS. TOSHIBA IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU OBTAINED THE SOFTWARE FROM AN AUTHORIZED CHANNEL AND ACCEPT ALL TERMS OF THIS EULA. WE MAY CHANGE THESE TERMS AT ANY TIME BY NOTIFYING YOU OF A CHANGE WHEN YOU NEXT START THE SOFTWARE. YOUR CONTINUED USE OF THE SOFTWARE WILL CONSTITUTE YOUR ACCEPTANCE OF SUCH VARIED TERMS.

**1. License Grant.** The Software is not sold; it is licensed upon payment of applicable charges. TOSHIBA grants to you a non-transferable and non-exclusive right to use with a TOSHIBA telecommunication systems product the copy of the Software provided under this EULA that you have obtained from an Authorized Channel. With respect to third party Software, TOSHIBA is only passing along license rights which may be granted by the owner or licensor of the Software and TOSHIBA does not separately license these rights to you. Each copy of the Software is owned by TOSHIBA and/or its suppliers. You agree you will not copy the Software except as necessary to use it on one TOSHIBA system at a time, at one location. Modifying, translating, renting, copying, distributing, printing, sublicensing, transferring, or assigning all or part of the Software, or any rights granted hereunder, to any other persons and removing any proprietary notices, labels or marks from the Software is strictly prohibited except as permitted by applicable law; you agree violation of such restrictions will cause irreparable harm to TOSHIBA and provide grounds for injunctive relief, without notice, against you or any other person in possession of the Software. You and any other person whose possession of the Software violates this EULA shall promptly surrender possession of the Software to TOSHIBA, upon demand. Furthermore, you hereby agree not to create derivative works based on the Software. TOSHIBA reserves the right to terminate this license and to immediately repossess the Software in the event that you or any other person violates this EULA.

**2. Software Support and Upgrade Service.** NOTWITHSTANDING ANY OTHER PROVISION OF THIS EULA, YOU HAVE NO LICENSE OR RIGHT TO ANY SOFTWARE SUPPORT AND UPGRADE SERVICE, UNLESS YOU HOLD A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAVE PAID THE APPLICABLE FEE TO AN AUTHORIZED CHANNEL FOR THE SOFTWARE SUPPORT AND UPGRADE SERVICE. USE OF SOFTWARE SUPPORT AND UPGRADE SERVICE IS LIMITED TO

TOSHIBA TELECOMMUNICATIONS SYSTEMS PRODUCT SUPPLIED BY AN AUTHORIZED CHANNEL FOR WHICH YOU ARE THE ORIGINAL END USER PURCHASER OR OTHERWISE HOLD A VALID LICENSE TO USE THE SOFTWARE THAT IS BEING UPGRADED.

**3. Copyright.** You acknowledge that no title to the copyright or any other intellectual property rights in the Software is transferred to you. You further acknowledge that title and full ownership rights to the Software and all copies thereof will remain the exclusive property of TOSHIBA and/or its suppliers, and you will not, by this EULA, acquire any rights to the Software or any copies thereof, except the license expressly set forth above. You will not remove or change any proprietary notices contained in or on the Software. The Software is protected under applicable patent, copyright, trade secret, and/or other proprietary laws, as well as international treaties. Any transfer, use, or copying of the Software in violation of the EULA constitutes copyright infringement. You are hereby on notice that any transfer, use, or copying of the Software in violation of this EULA constitutes a willful infringement of copyright.

**4. Critical Applications.** The Software is not designed or recommended for any "critical applications". "Critical applications" means life support systems, medical applications, connections to implanted medical devices, commercial transportation, nuclear facilities or systems or any other applications where product failure could lead to injury to persons or loss of life or catastrophic property damage. ACCORDINGLY, SHOULD YOU DECIDE TO USE THIS SOFTWARE FOR ANY CRITICAL APPLICATION, TOSHIBA DISCLAIMS, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ANY AND ALL LIABILITY ARISING OUT OF THE USE OF THE SOFTWARE IN ANY CRITICAL APPLICATION. IF YOU USE THE SOFTWARE IN A CRITICAL APPLICATION, YOU, AND NOT TOSHIBA, ASSUME FULL RESPONSIBILITY FOR SUCH USE. Further you shall indemnify and hold TOSHIBA and its affiliates harmless from any and all damages, liabilities, costs, and expenses, including reasonable attorneys' fees and amounts paid in settlement of third party or government claims, incurred by TOSHIBA and its affiliates as a result of or in any way arising from such use.

**5. No Reverse Engineering.** You agree that you will not attempt, and if you employ employees or engage contractors, you will use your best efforts to prevent your employees and contractors from attempting to reverse compile, reverse engineer, modify, translate or disassemble the Software in whole or in part. Any failure to comply with the above or any other terms and conditions contained herein will result in the automatic termination of this license and the reversion of the rights granted hereunder back to TOSHIBA. Notwithstanding the foregoing, in regard to any conflict between the terms of this Section 5 and any applicable open source license agreements (as referred to herein) for any open source software included in the Software, the terms of the applicable open source license agreement controls.

**6. Limited Warranty.** TOSHIBA'S SOLE OBLIGATIONS WITH RESPECT TO TOSHIBA SOFTWARE IS SET FORTH IN THIS EULA. UNLESS OTHERWISE STATED IN WRITING, ALL TOSHIBA AND THIRD PARTY SOFTWARE ARE PROVIDED ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND BY TOSHIBA. UNLESS THIRD PARTY SOFTWARE MANUFACTURERS, SUPPLIERS OR PUBLISHERS EXPRESSLY OFFER THEIR OWN WARRANTIES IN WRITING IN CONNECTION WITH YOUR USE OF THEIR THIRD PARTY SOFTWARE, SUCH THIRD PARTY SOFTWARE IS PROVIDED ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND BY THE MANUFACTURER, SUPPLIER, OR PUBLISHER OF SUCH THIRD PARTY SOFTWARE. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, TOSHIBA AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES WITH REGARD TO THE SOFTWARE, EITHER EXPRESS OR IMPLIED, OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE WARRANTY OF NON-INFRINGEMENT OF THIRD PARTY RIGHTS, AND THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE IS WITH YOU. NEITHER TOSHIBA NOR ITS SUPPLIERS WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY TOSHIBA OR A TOSHIBA AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. SOME JURISDICTIONS

DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS LIMITED WARRANTY GIVES YOU SPECIFIC RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE/JURISDICTION TO STATE/JURISDICTION.

**7. Limitation of Liability.** TOSHIBA'S AND/OR ITS SUPPLIERS' ENTIRE LIABILITY AND YOUR SOLE AND EXCLUSIVE REMEDY UNDER THIS EULA SHALL BE, AT TOSHIBA'S OPTION, REPLACEMENT OF THE SOFTWARE OR REFUND OF THE PRICE PAID. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL TOSHIBA OR ITS SUPPLIERS BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES FOR PERSONAL INJURY, LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION/ DATA, OR ANY OTHER PECUNIARY LOSS OF ANY KIND ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, OR OTHERWISE IN CONNECTION WITH ANY PROVISION OF THIS EULA EVEN IF TOSHIBA OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF THE REMEDY FAILS OF ITS ESSENTIAL PURPOSE. IN NO EVENT SHALL TOSHIBA OR ITS SUPPLIERS BE LIABLE FOR ANY CLAIM BY A THIRD PARTY. DATA USAGE RATES MAY APPLY WHEN DATA IS SENT OR RECEIVED WHILE USING THE SOFTWARE. YOU ARE SOLELY RESPONSIBLE FOR ANY SUCH DATA USAGE AND APPLICABLE CHARGES. ASK YOUR WIRELESS PROVIDER FOR FURTHER DETAILS ON RATES THAT MAY APPLY TO YOU.

**8. State/Jurisdiction Laws.** SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY MAY LAST, THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR THE EXCLUSION OF LIABILITY FOR DEATH OR PERSONAL INJURY CAUSED BY NEGLIGENCE, SO SUCH LIMITATIONS OR EXCLUSIONS IN THIS EULA MAY NOT APPLY TO YOU.

**9. Export Laws.** This EULA involves products and/or technical data that may be controlled under all applicable export control laws, regulations and orders, including but not limited to United States Export Administration Regulations or any other applicable law ("Export Laws"). The products and/or technical data involved with this EULA may not be exported without appropriate government authorization. Any export or re-export by you, directly or indirectly, in contravention of the Export Laws is prohibited. You shall comply with the Export Laws to assure that the Software is not exported, directly or indirectly, in contravention of the Export Laws.

**10. Governing Law.** This EULA will be governed by the laws of the Japan, excluding its conflict of law provisions.

**11. Severability.** If any provision of this EULA shall be held to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions hereof shall not in any way be affected or impaired.

**12. No Waiver.** No waiver of any breach of any provision of this EULA shall constitute a waiver of any prior, concurrent or subsequent breach of the same or any other provisions hereof, and no waiver shall be effective unless made in writing and signed by an authorized representative of the waiving party. To the extent the terms of any TOSHIBA policies or programs for support services conflict with the terms of this EULA, the terms of this EULA shall prevail.

**13. Supplier Software.** The Software may include certain software provided by TOSHIBA suppliers. In such event, you agree that such supplier may be designated by TOSHIBA as a third party beneficiary of TOSHIBA with rights to enforce the EULA with respect to supplier's software.

**14. Open Source Software.** The Software may contain software files that are subject to certain open source license agreements. The open source software files and additional terms and conditions may be included in the TOSHIBA Telecommunication System product general description or electronically within

the product. The open source software files are provided "AS IS" to the maximum extent permitted by applicable law. Please read the open source and third party software terms and conditions carefully for relevant copyright and licensing terms.

**15. Entire Agreement.** YOU ACKNOWLEDGE THAT YOU HAVE READ THIS EULA AND THAT YOU UNDERSTAND ITS PROVISIONS. YOU AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. YOU FURTHER AGREE THAT THIS EULA CONTAINS THE COMPLETE AND EXCLUSIVE AGREEMENT BETWEEN YOU AND TOSHIBA AND SUPERSEDES ANY PROPOSAL OR PRIOR AGREEMENT, ORAL OR WRITTEN, OR ANY OTHER COMMUNICATION RELATING TO THE SUBJECT MATTER OF THIS EULA.

Copyright © 2007-2016 Toshiba Corporation. All Rights Reserved.

# Contents

---

## Chapter 1 – Server Hardware Installation

SERVER HARDWARE SUPPORT . . . . .	1-1
CREATE A DELL® ACCOUNT . . . . .	1-1
DELL OWNERSHIP TRANSFER . . . . .	1-1
VMWARE® LICENSE . . . . .	1-6
ESXi VERSION . . . . .	1-6
vSphere Installation . . . . .	1-7
CHANGE VMWARE (ESXi) IP ADDRESS . . . . .	1-9
INSTALL vSHPERE CLIENT . . . . .	1-9
UPLOAD THE LICENSE KEY . . . . .	1-11
IP NETWORK CONNECTION . . . . .	1-13
NETWORK TIME PROTOCOL SYNCHRONIZATION . . . . .	1-13
VMware Tools Out of Date . . . . .	1-15
Automatic Startup . . . . .	1-15
VIRTUAL SERVER COMPONENTS . . . . .	1-17
POWER SUPPLY . . . . .	1-17
RACKMOUNT INSTALLATION . . . . .	1-17
IPedge ES Chassis . . . . .	1-17
Optional Rackmount Rails . . . . .	1-17
Dell 7040M Rackmount Shelf . . . . .	1-17
POWER REQUIREMENTS . . . . .	1-18
UPS RECOMMENDATIONS . . . . .	1-18
IPT POWER CONSUMPTION . . . . .	1-19

## Chapter 2 – Network Requirements

License Server Access . . . . .	2-2
ACD IP Address . . . . .	2-2
IPedge FQDN or Public IP Address Configuration . . . . .	2-2
LAN REQUIREMENTS . . . . .	2-2
VoIP Requirements Remote Users . . . . .	2-3
VoIP Requirements Wi-Fi® Users . . . . .	2-3
SUPPORTED BROWSERS . . . . .	2-4

## Chapter 3 – Enterprise Manager

SUPPORTED BROWSERS .....	3-1
LOGIN .....	3-1
START PAGE .....	3-2
VERSION DISPLAY .....	3-3
AUTOMATIC NEW VERSION DETECT .....	3-3
ROLES .....	3-4
Create a New Role .....	3-4
Copy a Role .....	3-4
USERS .....	3-4
Administration User .....	3-4
Phone User .....	3-5

## Chapter 4 – System Installation

INTRODUCTION .....	4-1
SYSTEM IP ADDRESS DEFAULTS .....	4-1
PRE-INSTALLATION REQUIREMENTS .....	4-1
NETWORK NAMES .....	4-2
INSTALLATION .....	4-3
LICENSE DONGLE .....	4-3
VIRTUAL SERVER INSTALLATION PROCEDURE .....	4-3
Login To The IPedge Server .....	4-4
Initial Setup and Network Configuration .....	4-5
Static Route .....	4-6
USB PASS-THROUGH .....	4-7
LICENSING .....	4-8
ON-LINE LICENSING (Virtual Service) .....	4-8
Off-Site Configuration .....	4-9
OFF-LINE LICENSING .....	4-10
Download License File .....	4-10
Upload and Apply License .....	4-10
Display License Information .....	4-11
Off-Line License Off-Site Configuration .....	4-11
IPedge ES LICENSING .....	4-11
ADMINISTRATION NOTIFICATION SETTINGS .....	4-12
On-Line License .....	4-12
Off-Line License .....	4-13
SIP TRUNK WIZARD .....	4-14
CHANGE SYSTEM PASSWORDS .....	4-16
Change FTP Password .....	4-16
Change Admin Password .....	4-16
Change Tech Support Password .....	4-16

CHANGE ROOT PASSWORD .....	4-16
IP ADDRESS CHANGE .....	4-16
DATABASE PREPARATION .....	4-17
Database Setup .....	4-17
CONFIGURE IPedge MESSAGING .....	4-18
Application Server Configuration .....	4-18
IPedge MESSAGING CONFIGURATION .....	4-23
RESTART IPedge SERVER .....	4-28
SYSTEM DATABASE BACKUP .....	4-28
HTTPS CERTIFICATE .....	4-28
ASSIGN MEMBER NODE .....	4-30
ADD MEMBER NODE .....	4-31
ATTACH MEMBER NODE .....	4-31
DETACH A MEMBER NODE .....	4-32
Over Subscribing .....	4-33
REGION CODE .....	4-33
MODEL DATABASE PROCEDURES .....	4-35
Download Model Database .....	4-35
Upload the IPedge Model Database File .....	4-35
Restore the IPedge Model Database File .....	4-35
Restart IPedge Server .....	4-36
SET SYSTEM TIME .....	4-36
NAME THE SERVER .....	4-37
DATABASE SYNCHRONIZATION .....	4-38
ADDING ACD to IPedge VIRTUAL SERVER .....	4-39
Setup ACD .....	4-39

## **Chapter 5 – UCedge® Server Setup**

UCedge SERVER REQUIREMENTS .....	5-1
UCEDGE SERVER SETUP .....	5-1
IPedge FQDN .....	5-1
Public IP Address Only, No FQDN .....	5-2
All IPedge Systems .....	5-2
FQDN Setup .....	5-5
EXTERNAL FEDERATION (Server White-list) .....	5-7
CHAT SERVER SETUP .....	5-9
USER ACCOUNT SETUP .....	5-10
Name to Display .....	5-11
PHONE ONLY USER ACCOUNT .....	5-11
CREATE A RANGE OF STATIONS .....	5-11
UPDATING AN EXISTING SYSTEM .....	5-11

## Chapter 6 – IPedge System Backup

BACULA .....	6-1
BACKUP FILE LOCATION .....	6-2
BACKUP SCHEDULE .....	6-2
Change Backup Schedule .....	6-2
Create a New Backup Schedule .....	6-4
Verify Backup Job Status .....	6-4
RESTORE FROM BACKUP .....	6-4
MANUAL BACKUP .....	6-5
Manual Backup Procedure .....	6-5
Create the Download File .....	6-6
Download Backup File .....	6-6
MANUAL RESTORE .....	6-7
UPLOAD BACKUP FILE .....	6-7
Upload from Administrator PC .....	6-7
RESTORE THE SERVER .....	6-8
ACD BACKUP .....	6-8

## Chapter 7 – HTTPS Configuration

INTRODUCTION .....	7-1
HTTPS SETUP .....	7-2
Wildcard Certificate .....	7-3

## Chapter 8 – IPT Software Update

INTRODUCTION .....	8-1
IP Telephone Hardware .....	8-1
INSTALLATION .....	8-1

## Chapter 9 – MRS, NAT Traversal, Ports, Firewall Setup

INTRODUCTION .....	9-1
MEDIA RELAY SERVER OVERVIEW .....	9-1
MEDIA RELAY SERVER SETUP .....	9-1
IPedge Configuration .....	9-1
IPT Configuration .....	9-2
SIP TRUNK NAT TRAVERSAL .....	9-3
SIP Trunk RTP Routing .....	9-3
FIREWALL SETUP .....	9-5
IPedge PORTS .....	9-5
FIREWALL PORTS TO OPEN .....	9-5
System to System WAN/VPN Ports .....	9-7
INTERNAL SYSTEM PORTS .....	9-9
CALL SIGNALING EXAMPLES .....	9-10
NETWORK SECURITY .....	9-15



SONICWALL . . . . .	9-16
Transparent Mode . . . . .	9-16
Requirements . . . . .	9-16
SONICWALL TZ100 CONFIGURATION . . . . .	9-18
SONICWALL TZ170 . . . . .	9-20
SONICWALL Pro2040 . . . . .	9-22
CISCO . . . . .	9-24
Inspect SIP Commands . . . . .	9-27

## Chapter 10 – SIP Trunk Configuration

INTRODUCTION . . . . .	10-1
REQUIREMENTS . . . . .	10-1
SIP PROVIDERS and SIP GATEWAYS . . . . .	10-1
CAPACITIES . . . . .	10-2
911/E911 CALLS . . . . .	10-2
SIP SIGNALING . . . . .	10-2
SIP TRUNK EXAMPLE . . . . .	10-3
SIP TRUNK GROUP PROGRAMMING . . . . .	10-4
Programming the Incoming Line Group . . . . .	10-4
Programming the Outgoing Line Group . . . . .	10-5
ASSIGN DID TRUNK DESTINATION . . . . .	10-5
OLG FLEXIBLE ACCESS CODE PROGRAMMING . . . . .	10-6
Creating the Channel Group . . . . .	10-6
Service Definition . . . . .	10-6
Service Assignment . . . . .	10-7
Service URI . . . . .	10-7
CALL FORWARD ACTIONS (R1.2 and Later) . . . . .	10-7
Caller ID of Originating Caller Sent . . . . .	10-7
Caller ID Sent by IPedge . . . . .	10-8
Sending Caller ID From Each Station . . . . .	10-8
SIP TRUNK CONFIGURATION PATTERNS . . . . .	10-9
SIP Trunk Configuration Tables . . . . .	10-11
SIP RESPONSE MESSAGES . . . . .	10-19
From the SIP Provider . . . . .	10-19
From the IPedge Server . . . . .	10-19
Other Indicators . . . . .	10-19

## Chapter 11 – Gateways

INTRODUCTION . . . . .	11-1
------------------------	------

## Chapter 12 – Net Server

ADD NET SERVER . . . . .	12-1
SETUP THE I/O PORT . . . . .	12-2
NET SERVER ADMINISTRATION . . . . .	12-2

Survivability .....	12-2
NET SERVER MENU .....	12-2
Status .....	12-3
Setup .....	12-4
LEVEL 2 MENU .....	12-13
Devices Menu .....	12-13
Logging .....	12-15
Dial Rule Menu .....	12-16
Dial Plan .....	12-16
Calling Within My Home Area Code .....	12-17
Calling Outside the Home Area Code .....	12-18
Server Based Call Manager Configuration .....	12-19
Create User Groups .....	12-19
Assign Users to Call Manager Application .....	12-20
Assign Users to User Groups .....	12-22
Server Based Call Manager Upgrade .....	12-26
Installation .....	12-26
Net Server configuration .....	12-28

## Chapter 13 – Messaging

ADD THE MESSAGING APPLICATION .....	13-1
DEFAULT PARAMETERS .....	13-2
SETUP THE I/O PORTS .....	13-2
ASSIGN THE VOICEMAIL SIP STATIONS .....	13-4
IPT Data .....	13-4
ADD STATIONS TO A STATION/HUNT GROUP .....	13-5
Voice Mail Data .....	13-5
PROGRAM MESSAGING .....	13-6
MESSAGING STORAGE ENCRYPTION .....	13-7
RESTART MESSAGING .....	13-7
DISK FULL NOTIFICATION .....	13-9
MESSAGING BACKUP .....	13-10
MANUAL BACKUP .....	13-10
Backup to a Different Directory .....	13-12
Backup to FTP Site .....	13-12
Retrieve Backup to Local PC .....	13-12
Scheduling a Backup .....	13-13
RESTORE .....	13-13
Restore from Directory .....	13-14
Restore from FTP .....	13-14
Upload from Local Directory .....	13-14
MESSAGING FAX PRINTER DRIVER 6.1 .....	13-15
CONFIGURE MESSAGING FAX .....	13-16
PRINT a FAX DOCUMENT .....	13-17

## Chapter 14 – Maintenance

INTRODUCTION . . . . .	14-1
ALARM NOTIFICATION . . . . .	14-1
SYSTEM PROCESSES . . . . .	14-1
Configure Start on Boot . . . . .	14-1
System Reboot/ Shutdown . . . . .	14-2
IPedge APPLICATION SERVER RECOVERY . . . . .	14-3
SERVER FAN REPLACEMENT . . . . .	14-3
SERVER POWER SUPPLY REPLACEMENT . . . . .	14-3
POWER UP SERVER . . . . .	14-3
HOT-SWAP HARD DRIVE . . . . .	14-3
HDD INDICATORS . . . . .	14-3
SYSTEM INITIAL SETUP . . . . .	14-5
QoS TROUBLESHOOTING TOOL . . . . .	14-6

## Chapter 15 – Restore IPedge Software

DEPLOY IPedge OVA TEMPLATE . . . . .	15-1
DEPLOY ACD TEMPLATE . . . . .	15-2
START ACD VM and WINDOWS . . . . .	15-4
IPedge ES SOFTWARE RESTORE . . . . .	15-5
RECOVERY FROM USB FLASH DRIVE . . . . .	15-5
Apply Licenses . . . . .	15-6
Restore Database . . . . .	15-6

## Chapter 16 – System Software Update

PROGRAM UPDATE . . . . .	16-1
Software Version 1.7.0 Systems . . . . .	16-1
Software Version 1.6 and Earlier Systems . . . . .	16-2
Multi-Node Systems . . . . .	16-3
Systems with ACD . . . . .	16-3
UPGRADING ACD on IPedge 1.7.4 . . . . .	16-3
PROGRAM UPDATE PROCEDURE . . . . .	16-5
ONLINE UPDATE . . . . .	16-6
Version check . . . . .	16-7
License Checking . . . . .	16-7
Language Pack . . . . .	16-7
Online Update Page Content . . . . .	16-8
Update Result: . . . . .	16-8
ENHANCED ONLINE UPGRADE . . . . .	16-8
DOWNLOAD RETRIES . . . . .	16-9
Cancel Upgrade Button . . . . .	16-9
Wait to Upgrade . . . . .	16-9

ONLINE UPDATE PROCEDURE . . . . .	16-10
Wait Then Apply Update. . . . .	16-10
Change and Apply Immediately . . . . .	16-11
Wait and Apply Later . . . . .	16-11
Change To Apply Immediately . . . . .	16-12
Change To Wait . . . . .	16-12
Cancel Update . . . . .	16-12
Remove One Server From Upgrade. . . . .	16-13
Add A Server to the Update . . . . .	16-13
Download Then Apply Update . . . . .	16-14
Download and Update Apply Later. . . . .	16-14
Change and Apply Immediately . . . . .	16-15
Load Update Files then Wait . . . . .	16-15
Cancel Update . . . . .	16-16
Remove One Server from the Update . . . . .	16-16
Add a Server to the Update . . . . .	16-17
OFFLINE UPDATE PROCEDURE . . . . .	16-17
LOCAL UPDATE . . . . .	16-17
USB Drive Requirements . . . . .	16-17
Update File Source. . . . .	16-18
Update Procedure . . . . .	16-18
REMOTE UPDATE PROCEDURE . . . . .	16-19
Upgrade Primary Server. . . . .	16-20
Member Server. . . . .	16-20
SYSTEM REBOOT . . . . .	16-21
MESSAGING DCN . . . . .	16-21
Create a Cluster . . . . .	16-22

## Chapter 17 – ESXi Update

REQUIRED ITEMS . . . . .	17-1
DOWNLOAD the ESXi UPDATE FILE . . . . .	17-1
Shut Down Virtual Machines . . . . .	17-1
ESXi Update Installation. . . . .	17-2

## Chapter 18 – IPedge Software Only

SOFTWARE ONLY SERVER . . . . .	18-1
IPedge Requirements. . . . .	18-1
Over Capacity Server. . . . .	18-1
ACD REQUIREMENTS. . . . .	18-2
ACD Software Requirements . . . . .	18-2
ACD Virtual Machine Requirement. . . . .	18-2
ACD License Requirements . . . . .	18-2
VMWARE® LICENSE . . . . .	18-2
ESXi VERSION . . . . .	18-2
INSTALL vSPHERE CLIENT . . . . .	18-2
NETWORK TIME PROTOCOL SYNCHRONIZATION . . . . .	18-2
NETWORK REQUIREMENTS . . . . .	18-3

OVA INSTALL . . . . .	18-3
IPedge SYSTEM LICENSES . . . . .	18-3
OFF-LINE LICENSE DONGLE . . . . .	18-3
IPedge MIGRATION To SOFTWARE ONLY . . . . .	18-4
MULTI-NODE SYSTEMS . . . . .	18-4
BRANDED IPedge SERVER to SOFTWARE ONLY . . . . .	18-4
MIGRATION with SYSTEM SIZE UPGRADE. . . . .	18-5
IPedge VIRTUAL SERVER (DELL Server) TO SOFTWARE ONLY. . . . .	18-5
IPedge SOFTWARE-ONLY LICENSE PART NUMBERS . . . . .	18-6
MAS to IPedge System License Transfer. . . . .	18-9

**Chapter 19 – Upgrade to Off-line Dongle Licence**

TRANSFER LICENSE . . . . .	19-1
USB PASS-THROUGH SETUP . . . . .	19-2
OFF-LINE LICENSING . . . . .	19-3
Download License File . . . . .	19-3
Upload and Apply License . . . . .	19-3
Display License Information . . . . .	19-4

This page is intentionally left blank.

# Chapter 1 – Server Hardware Installation

---

If you are installing an IPedge turn-key system that is not based on a Dell server go to [VMWARE® LICENSE on page 1-6](#).  
For IPedge ES systems go to [VIRTUAL SERVER COMPONENTS on page 1-17](#).

## SERVER HARDWARE SUPPORT

Server hardware is supported by Dell directly. If any issue associated with the hardware is discovered, please contact Dell. Use the following procedure to obtain Dell support.

This section covers the procedures required to setup the Dell server, as a virtual server on the customer's network, to function as an IPedge Virtual Server

## CREATE A DELL® ACCOUNT

In order to transfer the Dell server and register that server for warranty support you must have a Dell account. Use the procedure below to create an account.

1. Go to the following website.  
<http://www.dell.com/support/retail/us/en/04/ownershiptransfer/IdentifySystem>
2. Click on the **My Account** link in the top left corner of the screen.
3. Click on the **Create a Dell.com account** link.
4. Enter the required information.

**Note:** If you know your standardized address used by the U.S. Post Office, please enter it.  
Enter your 9 digit Zip Code (five digit will work).  
Enter your street name and number in the first address line, and any non-address information (Suite, Department, etc.) in the second address line

5. Click on the Confirm Registration button.

**Important!** Record the Dell 'My Account' information for each customer location. A first step to get Dell support for a server hardware issue is to login to this account which is setup for the ownership transfer.

## DELL OWNERSHIP TRANSFER

The Dell servers are registered to Toshiba when shipped. The first steps transfer the server to you and your customer.

1. Locate the Service Tag Number on the Dell server. The number is on the Information Tag on the server front panel. If there is no service tag, such as 9020m servers, use the chassis serial number.

2. Open the following website.  
<http://www.dell.com/support/retail/us/en/04/ownershiptransfer/IdentifySystem>

**Note:** Dell may change the URL at any time. If necessary, look for warranty service on [www.Dell.com](http://www.Dell.com).

3. Enter the **service tag** number and click **Continue**.

### Are you on the system now?

We can look up your computer's Service Tag and Express Service Code for you.

[Automatically detect my service tag](#)

For (10) or more tags, please use the below Bulk transfer files. Please note there is an International and Domestic file and ALL fields must be completed in order to process your request. (Domestic = US to US; Int'l = all other transfer types)

[Domestic Bulk Transfer](#)

[International Bulk Transfer](#)

### If not, look up one or more systems

Service Tag \* [?](#)      Express Service Code [?](#)

[+ Add More](#)



4. Enter the Company Name and Zip code as shown here. Company Name is **Toshiba** and the zip code is **92618**.

The screenshot shows a web form for Dell ownership transfer. At the top, there are three steps: 'Identify System' (completed with a checkmark), 'Previous Owner Information' (current step with a downward arrow), and 'New Owner Information' (not started). Below the steps, the text reads 'Products you are transferring' followed by 'PowerEdge R720 (5RGDH02)'. The 'Previous Owner Information' section contains several input fields: 'First Name', 'Last Name', 'Company Name \*' (containing 'Toshiba'), 'Email', 'Street Address' (with three stacked input boxes), 'Country' (set to 'United States'), 'City', 'State/Prov/Cnty' (a dropdown menu set to 'California'), 'Zip Code \*' (containing '92618'), and 'Phone Number'. The 'Company Name' and 'Zip Code' fields are highlighted with red circles. At the bottom of the form, there is a 'Continue' button and a 'Previous' link.

5. Enter the following information and click on **Continue**.  
Company Name: Use the following format.  
**Toshiba “DEALER NAME” CUSTOMER NAME**  
For example: Toshiba “ABC Communications” XYZ Company  
Email: Your email address

Address: The address where the server is installed (customer location). Dell will use this information when they need to visit the site for warranty support.

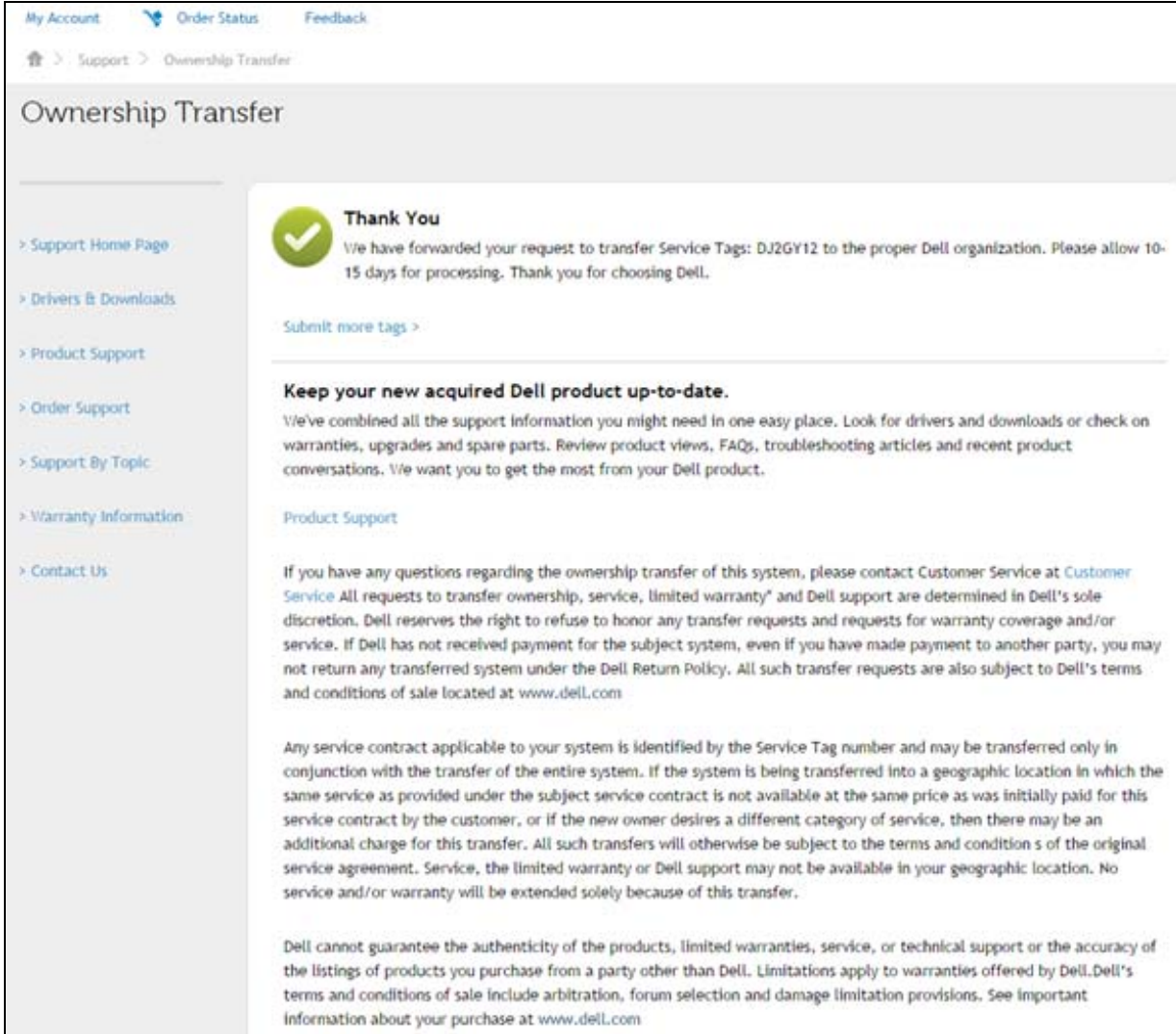
The screenshot shows a four-step progress bar at the top: 'Identify System' (checked), 'Previous Owner Information' (checked), 'New Owner Information' (active), and 'Review' (pending). Below the progress bar, the text reads 'Products you are transferring' followed by 'PowerEdge R720 ( )'. The main section is titled 'New Owner Information' and contains the following fields:

- First Name: John
- Last Name: Smith
- Company Name \*: Toshiba"ABC Comm"XYZ Company
- Email \*: john@abc.com
- Confirm Email \*: john@abc.com
- Street Address \*: 123 Main Street (with a note: PO Boxes are invalid. Please provide a physical address.)  
Suite 312
- Country \*: United States (with a note: If the country you're looking for doesn't appear, please read additional information)
- State/Prov/Cnty \*: Your State
- City \*: Home Town
- Zip Code \*: 99999-9999
- Phone Number: 8885551212
- How will the product be used? \*: Commercial/Office

At the bottom of the form, there is a 'Continue' button and a 'Previous' link.

6. Confirm the information and click on the **Submit** button.

7. The following screen will display. It may take several days for the changes to take effect.



The screenshot shows the Dell Support website interface for an Ownership Transfer. At the top, there are navigation links for 'My Account', 'Order Status', and 'Feedback'. Below that, a breadcrumb trail reads 'Support > Ownership Transfer'. The main heading is 'Ownership Transfer'. On the left, there is a sidebar with navigation links: '> Support Home Page', '> Drivers & Downloads', '> Product Support', '> Order Support', '> Support By Topic', '> Warranty Information', and '> Contact Us'. The main content area features a green checkmark icon and the heading 'Thank You'. The text reads: 'We have forwarded your request to transfer Service Tags: DJ2GY12 to the proper Dell organization. Please allow 10-15 days for processing. Thank you for choosing Dell.' Below this is a link 'Submit more tags >'. A section titled 'Keep your new acquired Dell product up-to-date.' follows, with text: 'We've combined all the support information you might need in one easy place. Look for drivers and downloads or check on warranties, upgrades and spare parts. Review product views, FAQs, troubleshooting articles and recent product conversations. We want you to get the most from your Dell product.' Below this is a link 'Product Support'. The next section is titled 'If you have any questions regarding the ownership transfer of this system, please contact Customer Service at Customer Service'. The text explains that all requests to transfer ownership, service, limited warranty, and Dell support are determined in Dell's sole discretion. It also states that Dell reserves the right to refuse to honor any transfer requests and requests for warranty coverage and/or service. If Dell has not received payment for the subject system, even if you have made payment to another party, you may not return any transferred system under the Dell Return Policy. All such transfer requests are also subject to Dell's terms and conditions of sale located at [www.dell.com](http://www.dell.com). The final section is titled 'Any service contract applicable to your system is identified by the Service Tag number and may be transferred only in conjunction with the transfer of the entire system. If the system is being transferred into a geographic location in which the same service as provided under the subject service contract is not available at the same price as was initially paid for this service contract by the customer, or if the new owner desires a different category of service, then there may be an additional charge for this transfer. All such transfers will otherwise be subject to the terms and conditions of the original service agreement. Service, the limited warranty or Dell support may not be available in your geographic location. No service and/or warranty will be extended solely because of this transfer.' The last section is titled 'Dell cannot guarantee the authenticity of the products, limited warranties, service, or technical support or the accuracy of the listings of products you purchase from a party other than Dell. Limitations apply to warranties offered by Dell. Dell's terms and conditions of sale include arbitration, forum selection and damage limitation provisions. See important information about your purchase at [www.dell.com](http://www.dell.com)'.

8. When warranty service is required, please contact Dell Technical Support through phone, email or chat through the following page.  
<http://www.dell.com/support/contents/us/en/04/category/Contact-Information?ref=opinionlab2>
9. In order to get support, you may need to Login to your Dell account on the My Account page on Dell.com.  
If you do not have an account refer to [CREATE A DELL® ACCOUNT on page 1-1](#).

### VMWARE® LICENSE

The virtual IPedge system requires that the VMware be licensed to the customer (not the dealer). The IPedge Virtual Server ships with a 30-day VMware trial license. If the customer has a VMware license use that license key. If the customer does not already have a VMware license they can use this procedure to acquire a free VMware license.

**Note:** VMware changes their website occasionally. The following steps are a general guide. This was correct when published.

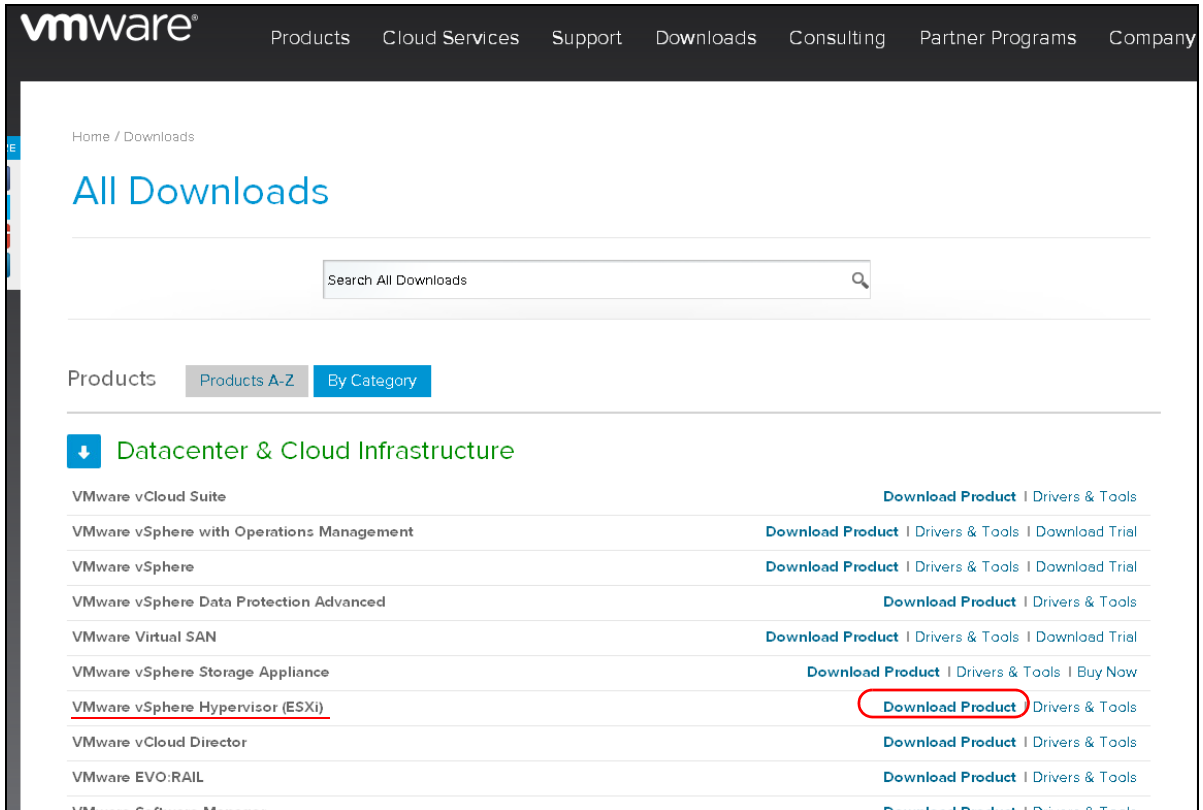
1. Navigate to the VMware website; <http://www.vmware.com>.
2. Click on a My VMware link. You may need to select Login to see the My VMware link.
3. Click on the **Register** link to create an account.
4. Follow the on screen instructions to create your account.
5. When your account has been confirmed by email go to the next step.
6. Browse to <http://my.vmware.com/web/vmware/downloads>.

**Important!** The VMware must be licensed to the end user, not the dealer. The end user's email address is used by VMware to identify to license holder.

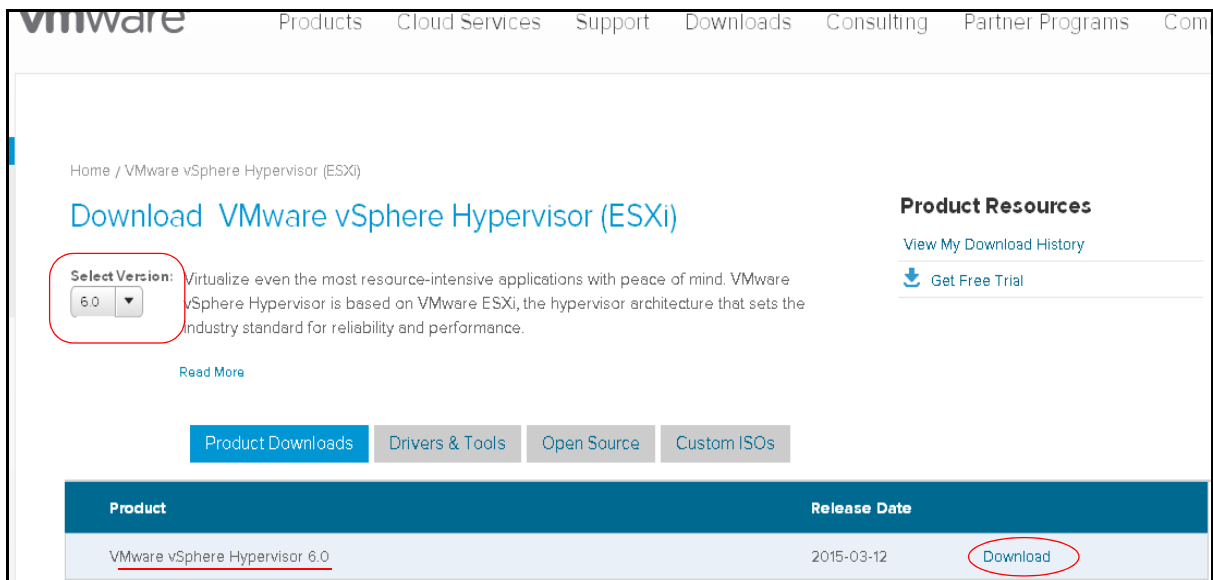
### ESXi VERSION

IPedge Virtual servers run ESXi 5.5 or ESXi 6.0 VMware. For all IPedge systems ensure that you load vSphere for ESXi 6.0.

- vSphere Installation** 1. Select VMware vSphere Hypervisor (ESXi), click on Download Product.



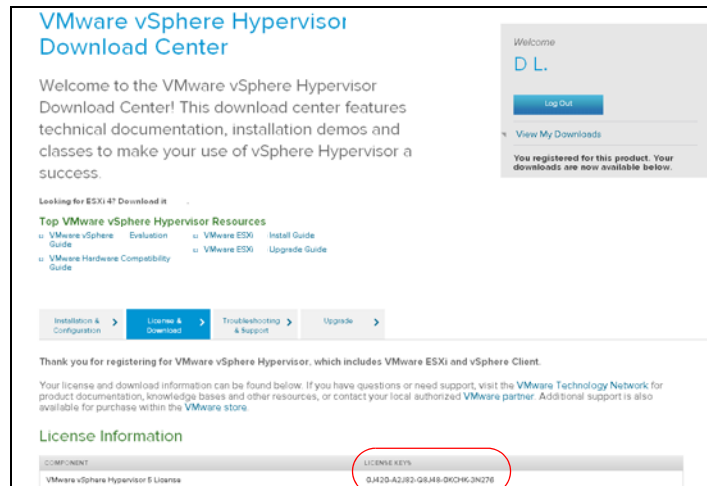
2. Select the Version 6.0 for all IPedge systems in the pull-down list. vSphere 6.0 can be used for systems running ESXi 5.5 and 6.0.



3. Click on **Register**.



- Specify the number of licenses you want. You will need one license for each physical server you install. You can have many virtual servers on one license.
- Copy the License key to a document on your administration PC. The license key will be used in the next procedure.



These next procedures require access to the physical server and connection to a network with internet access.

**CHANGE VMWARE (ESXi)  
IP ADDRESS**

The default address of the ESXi server is 192.168.254.245. To change the network configuration use the system console.

Plug in a monitor and a keyboard to the rear panel connects on the IPedge Virtual server chassis.

1. Press **F2** Customer System/ View Logs.
2. Press **F2** Customize System/ View Logs.
3. Login to user name; **root**. The default password is **password**.

**Note:** If the server is accessible physically and/or on the public network you should change this password. This new password must be retained, there is no way to recover this password.

4. Press **Enter**.
5. Arrow down to select **Configure Management Network** then, press **Enter**.
6. Arrow down to select **IP Configuration** then, press **Enter**.
7. In the IP configuration dialog box:  
Ensure that **Set Static IP address and network configuration** is selected.  
Arrow down to set the **IP Address**.  
Arrow down to set the **Subnet Mask**.  
Arrow down to set the **Default Gateway**.  
Press **Enter**.
8. Arrow down to select **DNS Configuration** then, press **Enter**.  
Arrow down to set the **Primary DNS** IP address.  
Arrow down to set **Alternate DNS** IP address.
9. Leave the hostname at the default value of localhost.
10. Press **Enter**.
11. Press **ESC**
12. Press **ESC**
13. Press **F12** Shut down / Restart.
14. Login. The same as [Step 3](#) above.
15. Press **F11** Restart.
16. Press **Enter** to confirm the restart.

The system will restart. This will take a few minutes.

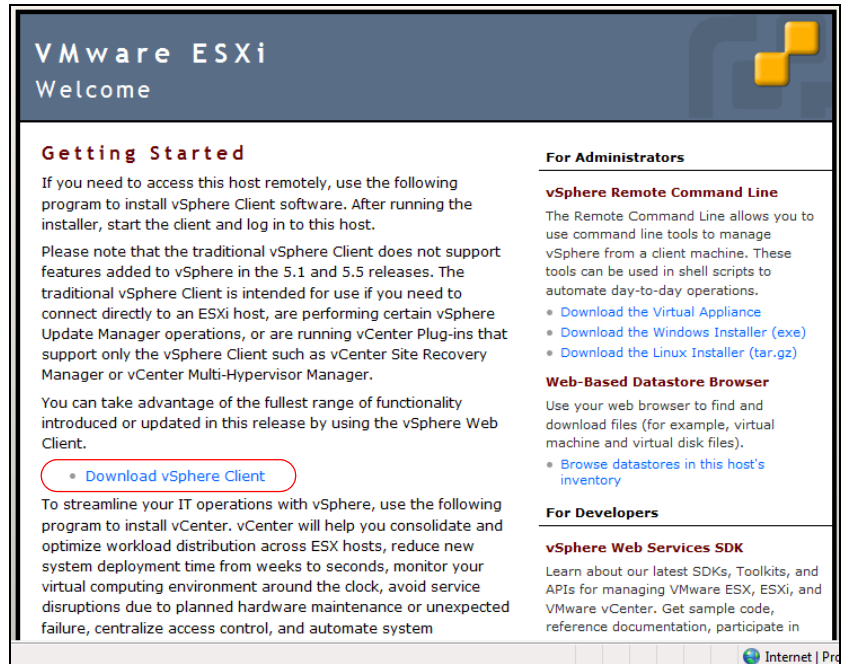
**INSTALL vSHPERE  
CLIENT**

To copy the license key onto the server you must have vSphere Client on you administration PC.

**Note:** The administration PC must have internet access for this vSphere Client download procedure.

1. Ensure that the administration PC is on the same subnet as the IPedge Virtual Server.

2. Launch a browser. Enter the IP address of the ESXi server. The default address is: 192.168.254.245.



**Note:** Ignore any certificate warnings that appear.

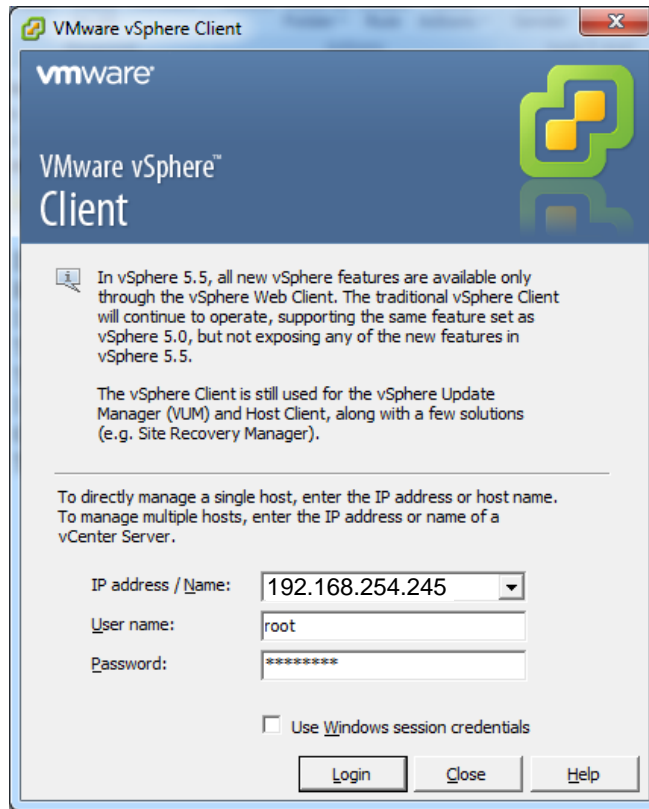
3. The vSphere client will download then launch the installer. Follow the prompts to complete the installation. This will take several minutes.



**UPLOAD THE LICENSE KEY**

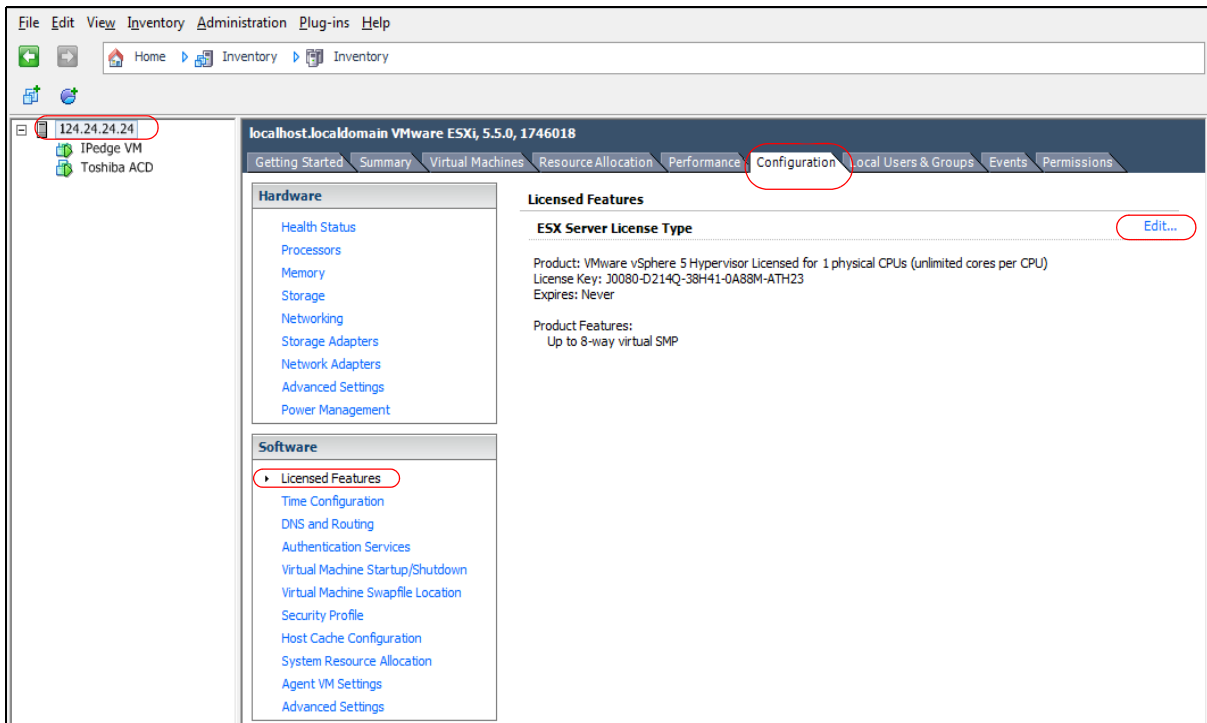
This procedure is used to apply the VMware license key to the server.

1. Launch vSphere Client.



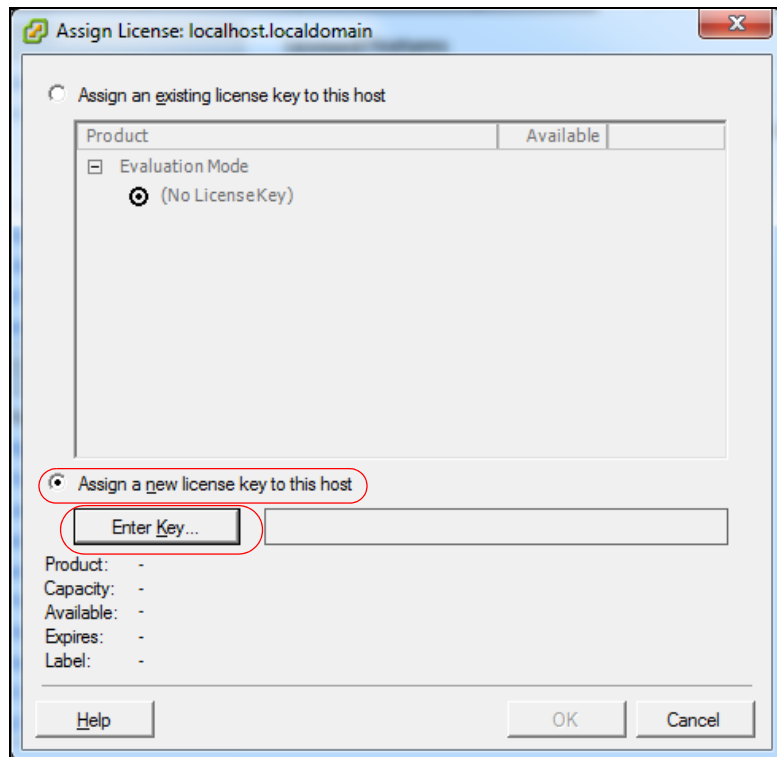
2. Enter the IP address of the IPedge Virtual server.
3. The default user name is; root.  
The default password is: password.
4. Click on the **Login** button.

5. Click on the IP address of the server in the left hand column.

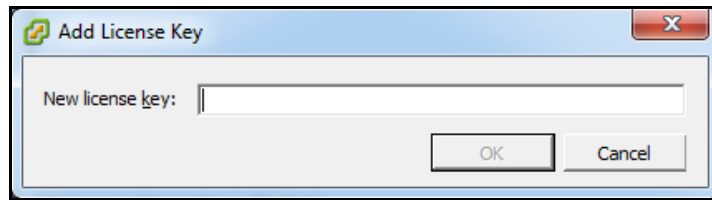


6. Click on the Assign a new license key to the host radio button.

7. Click on **Enter key** button.



- Copy or type the license key into the **New license key** field.



- Click on **OK**.

**Important!** This procedure must be completed within 30 days or the server will stop processing all calls.

## IP NETWORK CONNECTION

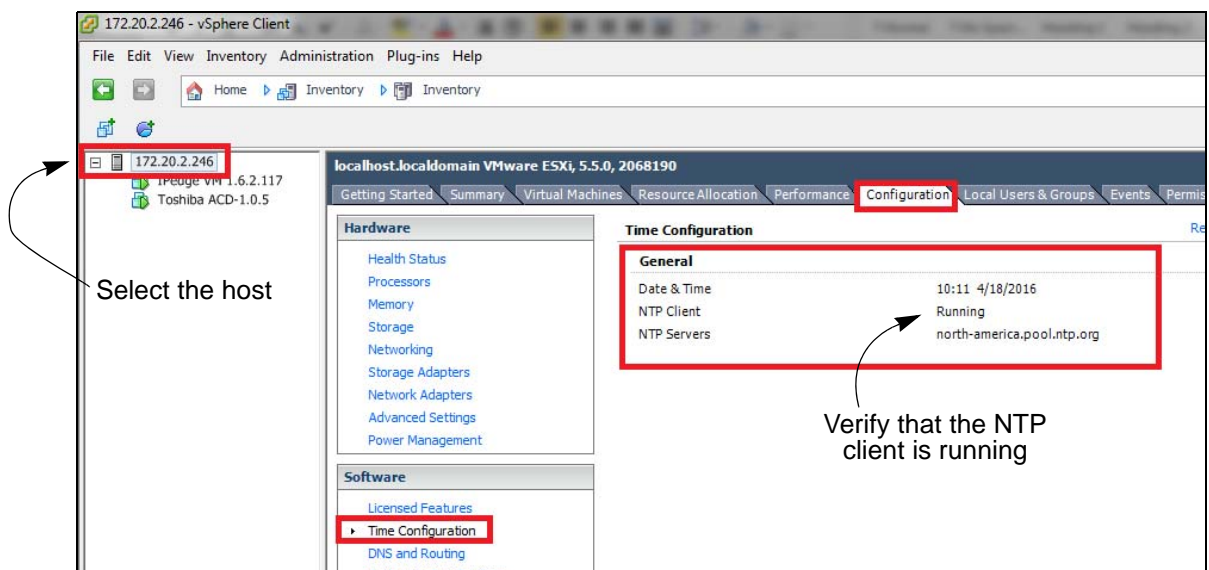
Each IPedge Virtual Server chassis has up to four NIC connectors. The connectors are teamed. The network cable can be plugged into any NIC port. The NIC connectors are teamed by design and must not be altered in any way by the dealer or customer.

## NETWORK TIME PROTOCOL SYNCHRONIZATION

A network time protocol service must be assigned to keep the virtual machines synchronized. The IPedge Virtual Servers will ship with a default NTP service pointer ([north-america.pool.ntp.org](http://north-america.pool.ntp.org)). Toshiba recommends that the VMware be configured with the same NTP service. Note that a time server pool should be referenced, not a single server.

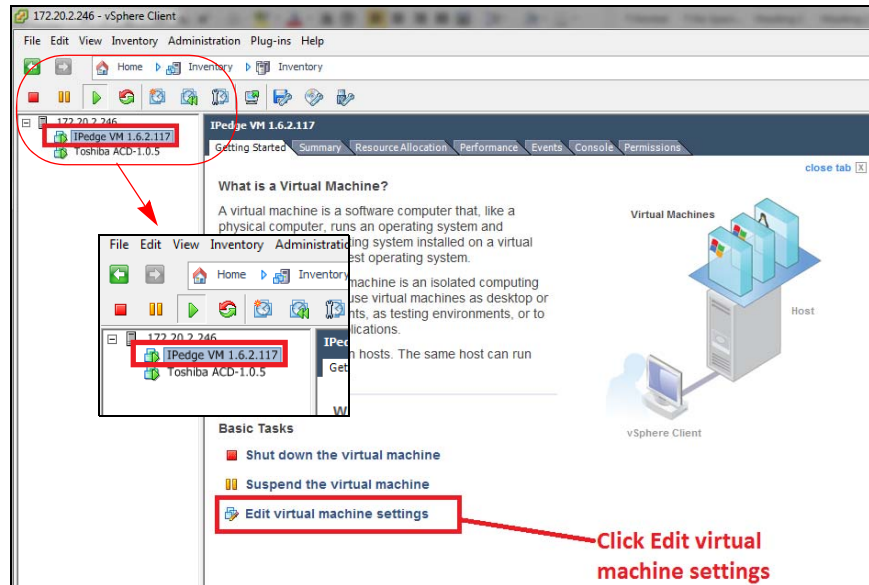
The Network Time Protocol (NTP) is a protocol for synchronizing the server clocks on a data network. NTP uses UDP on port 123 as its transport layer.

- Login to the vSphere Client. Select the host.

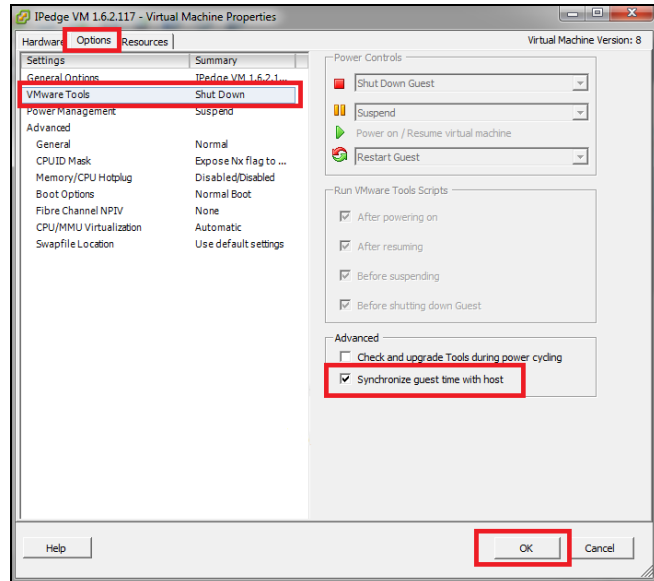


- Select the **Configuration** tab.
- Select **Time Configuration** from the Software section.
- Confirm that the date and time are correct.

5. Verify that the NTP client is running.
6. Select the IPedge guest machine.

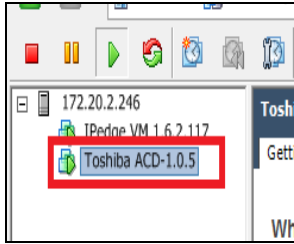


7. Click on **Edit virtual machine settings**.
8. Select the **Options** tab.
9. Select **VMware Tools**. Ensure that **Synchronize guest time with host** is check-marked.



10. Click on **OK** to save the changes.

11. Select the ACD guest if equipped.



12. Click on **Edit virtual machine settings**.
13. Select the **Options** tab.
14. Select VMware Tools.
15. Ensure that **Synchronize guest time with host** is checked.

### VMware Tools Out of Date

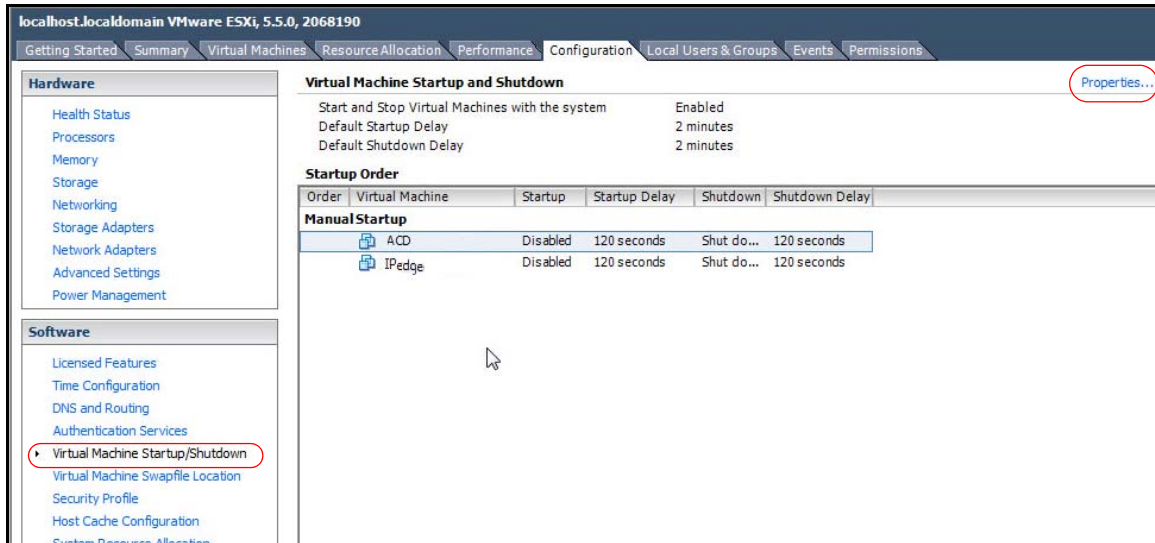
If the VMware tools version are different than the OVA creation system (older or newer) a message that the tools are "Running (Out of date)" will show. This has no effect on system operation. If you wish to update the tools to clear the message use the following procedure. Otherwise go to [Automatic Startup](#).

1. Login to the vSphere client. Select the Summary tab.
2. Right-click on the IPedge VM in the left column. (Notice that the VMware Tools show; Running (Out of date).
3. Select Guest > Install/Upgrade VMware Tools.
4. Click to select Automatic Tools Upgrade then, click on **OK**.
5. VMware Tools will show; Not Running while the Tools upgrade is in process.
6. When the VMware Tools upgrade is complete the display will change to "Running (Current)".

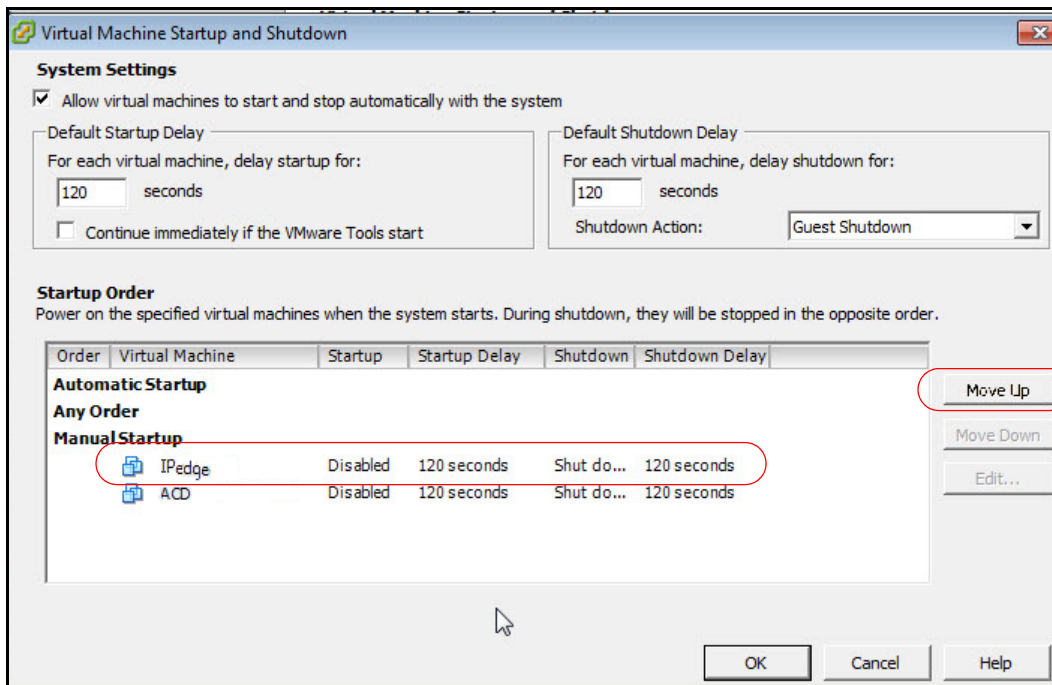
### Automatic Startup

1. Select the virtual machine..
2. Select the **Configuration** tab.
3. Click on **Properties**.

4. Click on **Virtual machine Startup/Shutdown**.



5. Select the IPedge guest machine. Click on the **Move Up** icon until the IPedge machine is listed under **Automatic Startup**.



6. Select the ACD guest machine, if equipped. Click on the **Move Up** icon until the IPedge machine is listed under **Automatic Startup**, under the IPedge machine.
7. Click on **OK**.

## VIRTUAL SERVER COMPONENTS

### POWER SUPPLY

The power supply AC input requirements and heat generated, at maximum load, are shown in [Table 1-1](#).

**Table 1-1 Power Supply Specifications**

Item	9020m/7040m	R220	R430
AC Volts (50 ~ 60 Hz)	100 ~ 240	100 ~ 240	100 ~ 240
(120 V)	NA	4.0	7.4 (single p/s) 6.5 x 2 (redundant p/s)
BTU/Hr (MAX)	NA	1040	2107 (single p/s) 1871 (redundant p/s)
Idle Power (Watts)	65W Adapter	53.30	231.0 (max) 94.1 (typical)

### RACKMOUNT INSTALLATION

The IPedge servers (refer to the IPedge ES exception below) mount into standard 19 inch EIA Universal Spacing racks and cabinets using the optional mounting rails. Order the optional rack-mount rails when ordering the server.

#### IPedge ES Chassis

The Intel NUC processor chassis is 115 mm x 111 mm x 48 mm (4.53 in x 4.37 in. x 1.89 in.). Toshiba does not offer a rackmount option. A wall mount bracket is included with the NUC processor.

#### Optional Rackmount Rails

The optional rackmount rails for Dell servers are not included with any of the server chassis. The optional mounting rails can be ordered from Toshiba. Rail installation instructions are available from [www.DELL.com](http://www.DELL.com).

---

**CAUTION! The servers must only be installed in an equipment rack using the mounting rails. The front panel screws only secure the chassis on the rails. They are not weight bearing.**

---

#### Dell 7040M Rackmount Shelf

The Dell 7040M rack mount shelf allows the server to be mounted in standard 19 inch racks. The 7040M chassis is secured in the box with a screw (included) and the cables secured with cable ties (included) to the slots in the rear edge of the shelf.



Top view



Front view

**POWER REQUIREMENTS**

The IPedge server should have a dedicated AC power circuit. The specific input voltage and current requirements for each server is listed in the specifications for each model.

---

**CAUTION! The Intel NUC and Dell 7040M processors must use the power adapter shipped by the manufacturer.**

---

**UPS RECOMMENDATIONS**

Toshiba recommends an uninterruptible power supply (UPS) with power conditioning for the IPedge Virtual Server.



**IPT POWER CONSUMPTION**

In [Table 1-2](#) the power consumption for IP5000-series telephones and the Add-on modules is shown. Use this information to calculate the Power over Ethernet (PoE) requirements and UPS capacity.

**Table 1-2 IP Telephone and Add-On Module Power Consumption**

Telephone Model <sup>1</sup>	Option		Power Rating (Watts)	Current (A) <sup>2</sup>	Typical (Watts) <sup>3</sup>	Typical Current (A) <sup>4</sup>	IEEE802.3af PD Class
	Model	Qty					
IP5122-SD	none	--	7.4	0.15	6.2	0.13	0
IP5122-SDC	none	--	7.4	0.15	6.2	0.13	0
IP5132-SD	none	--	7.4	0.15	6.2	0.13	0
IP5131-SDL	none	--	7.4	0.15	6.2	0.13	0
IP51xx +	IDM5060	3	10.3	0.21	8.6	0.18	0
IP51xx +	IDM5060	2	9.4	0.20	7.8	0.16	0
IP51xx +	IDM5060	1	8.4	0.18	7.0	0.15	0
IP51xx +	LM5110	2	10.3	0.21	8.6	0.18	0
IP51xx +	LM5110	1	9.4	0.20	7.8	0.16	0
IP51xx +	KM5020	2	8.9	0.19	7.4	0.15	0
IP51xx +	KM5020	1	8.2	0.17	6.8	0.14	0
IP5622-SD	none	--	3.7	0.08	3.0	0.06	1
IP5631-SDL	none	--	4.1	0.08	3.3	0.07	2
IP5631-SDL	IDM5060	3	6.4	0.13	5.4	0.11	2
IP5631-SDL	IDM5060	2	5.6	0.12	4.7	0.10	2
IP5631-SDL	IDM5060	1	4.8	0.10	4.0	0.08	2
IP5631-SDL	LM5110	2	6.4	0.13	5.3	0.11	2
IP5631-SDL	LM5110	1	5.6	0.12	4.7	0.10	2
IP5631-SDL	KM5020	2	5.2	0.11	4.3	0.09	2
IP5631-SDL	KM5020	1	4.6	0.10	3.9	0.08	2
IP5531-SDL	none	--	3.6	0.08	3.0	0.06	2

1. Power ratings are only telephone and option modules consumption. The values do not include LAN cable power loss, and apply to PoE, not local power supplies.
2. Power ratings are only telephone and option modules consumption. The values do not include LAN cable power loss, and apply to PoE, not local power supplies.
3. Typical means that it is only an example and there is no guarantee implied. The "typical" value might be used for a calculation of actual UPS backup time in an average installation
4. Typical Current (A) = Typical Watts / 48 v

This page is intentionally left blank.

# Chapter 2 – Network Requirements

---

The IPedge Virtual Server communication system is an IP system. At each site all of the system components are connected via a LAN. The IPedge Virtual Server, on-site IPTs, gateways, other servers communicate over the site LAN. Other devices connect over a WAN or the Internet.

IPedge systems running release 1.7.4 and later software have two licensing options. The IPedge ES (only) uses a third licensing process.

- On-line virtual licensing - The licensing service requires access to the internet. This access is typically through a firewall / router.
- Off-line dongle based licensing - The license file is uploaded to the IPedge server and the bound dongle must remain plugged into the server at all times. Off-line dongle based licensing is not available on Toshiba branded IPedge servers.

The following list is the IPedge network characteristics required for a successful system implementation.

**Important!** Toshiba recommends a through network assessment using Pathview, AppCritical™ or similar tool. During and after installation setup network monitoring with a tool such as WhatsUp® Gold, Solarwinds™ or, IPSLA.

- The IPedge Virtual Server running in VMware requires a minimum of two static IP addresses. The IPedge ES requires only one address.
  - The IPedge Virtual Server appliance (ESXi) static private IP address.
  - The IPedge server must have a static public IP address. This is typically the public address of the WAN, a router with the ability to translate the public address to a fixed private address.
- Most IPedge systems must have access to the internet to license the system using the Virtual Licensing Service.
  - IPedge systems with On-Line licensing must have internet access
  - IPedge systems with Off-Line dongle based licensing do not require internet access.
  - IPedge ES systems require internet access only for initial licensing, license changes or, software updates.

**License Server Access** For IPedge systems using on-line virtual licensing, the router/firewall the IPedge server connects through to the internet will require access to the IPedge Virtual Licensing service. Allow access to:

- The public domain: toshiba.flexnetoperations.com
- The public domain: fyi.tsd.toshiba.com
- The public domain: opendns.com
- Port: 53
- HTTPS
- Port: 443

**ACD IP Address** The ACD server, if licensed, will require a static IP address

**IPedge FQDN or Public IP Address Configuration** In a single IPedge system UCedge support requires one of two configurations.

- The IPedge server has a FQDN, The IPedge FQDN must be registered and resolve to the public IP address of the IPedge server.  
— OR —
- The IPedge has only a public IP address, no domain name, no FQDN.

- The IPedge system must have a public IP address (your router must have a public IP address and be setup for port forwarding to the IPedge system private IP address.
- The router must be able to translate the public IP address to the private IP address (NAT).
- The router must support 'hairpin' operation such that when an internal device accesses the IPedge public address the router loops the connection back to the private IP address.

**Note:** If ALL of the client devices are on the internal network use the private address of the IPedge in the FQDN field.

The following services must be available to the IPedge Virtual Server.

**DNS** - The enterprise name assigned to the primary node must be registered with the DNS service. Toshiba recommends that the IPedge Virtual Server name(s) be registered with the DNS.

**NTP** - A network time protocol service must be assigned to keep the nodes synchronized. The IPedge Virtual Servers will ship with a default NTP service pointer (north-america.pool.ntp.org). Toshiba recommends that a time server pool be referenced, not a single server.

The Network Time Protocol (NTP) is a protocol for synchronizing the server clocks on a data network. NTP uses UDP on port 123 as its transport layer.

## LAN REQUIREMENTS

Toshiba recommends a through network assessment during and after installation setup.

- Network Reliability (at the server level): 99.99%
- POE for IP telephones is recommended
- Layer 3 voice prioritization strongly recommended
  - Layer 3: DiffServ: Enabled / ToS
  - Type:DSCP / DSCP for Voice: 46
- Layer 2 can also be supported
  - Layer 2: 802.1p/802.1q (VLAN)
- 88kbps (G.711 audio) in each direction per simultaneous call
- Less than 20ms latency
- Jitter: 10ms or less (+/- 5msec)
- Packet Loss: <0.1%.
- Full Duplex and Auto Negotiate on all ports
- Network topology diagram

**VoIP Requirements  
Remote Users**

- Network Reliability – 99.99%
- Layer 3 voice prioritization recommended – Layer 3: DiffServ: Enabled / ToS Type:DSCP / DSCP for Voice: 46
- 88kbps (G.711 audio) in each direction per simultaneous call
  - Note: Media traffic is Peer-to-Peer
- Less than 50 ms latency
- Jitter: 20ms or less (+/- 10msec)
- Packet Loss: < 1%.
- Security: VPN for SoftIPT on PC

**VoIP Requirements Wi-Fi®  
Users**

- VoIP Products and Applications
  - PC's with SoftIPT, Call Manager
  - Polycom 8000 series Wi-Fi phones
  - Motorola TEAM application and phones
  - uMobility on iPhone, Windows Mobile, Android, Blackberry
- QoS
  - 802.11e/WMM recommended
  - Layer 3 DiffServ/DSCP/ToS 46
- VoIP Wi-Fi Device application support
  - SIP Voice
  - Internet Access,
  - Intranet Access
  - eMail/calendar

- Network Reliability: 99.99%
- 88kbps (G.711 audio) in each direction per simultaneous call

**Note:** Media traffic is Peer-to-Peer

- Less than 50 ms latency
- Jitter: 20ms or less (+/- 10msec)
- Packet Loss: < 1%
- Support for 802.11b,g,a & n

A Strata CIX system can be connected to an IPedge Virtual Server via IPedge Net. When the databases, IPedge and CIX, are programmed correctly calls will be processed from one system to the next. This means that an IPedge Virtual Server can also be added to an existing CIX system. An IPedge Virtual Server can also be added to an existing Strata Net IP network.

The Strata CIX system will require a PC with Network eManager for database programming, database backup, and other maintenance operations.

The system administrator must ensure that DN assignments and feature access codes are compatible. There is no communication between Network eManager and Enterprise Manager.

**SUPPORTED BROWSERS** The table below lists the IPedge functions and features and the supported browsers.

#### IPedge System Features and Functions - Browsers Supported

Feature (Browser Mode)	IE 11	Chrome	Firefox
Enterprise Manager General Admin	OK	OK	OK
Enterprise Manager General Admin (HTTPS)	OK	OK	OK
Enterprise Manager - Program Update	OK	NOK	OK
Enterprise Manager - Program Update (HTTPS)	OK	NOK	OK
Enterprise Manager - Station Copy	OK	NOK	OK
Enterprise Manager - Station Copy (HTTPS)	OK	NOK	OK
Enterprise Manager - App Server UC Client User	OK	OK	OK
Enterprise Manager - App Server UC Client User (HTTPS)	OK	OK	OK
Webmin	OK	OK	OK
Webmin (HTTPS)	OK	OK	NOK
ACD Administration	OK	OK	OK

OK = Supported (OK)  
NOK = Not Supported (Not OK)

(Sheet 1 of 2)

**IPedge System Features and Functions - Browsers Supported**

<b>Feature (Browser Mode)</b>	<b>IE 11</b>	<b>Chrome</b>	<b>Firefox</b>
ACD Administration (HTTPS)	OK	NOK	NOK
Netserever Administration	OK	OK	OK
Netserever Administration (HTTPS)	OK	OK	OK
Messaging Administration	OK	OK	OK
Messaging Administration (HTTPS)	OK	OK	OK
Meet-me Audio Conference View/Scheduler/Logs	OK	OK	OK
Meet-me Audio Conference View (HTTPS)	OK	OK	NOK
Meet-me Audio Conference Scheduler (HTTPS)	OK	OK	OK
Meet-me Audio Conference Logs (HTTPS)	OK	OK	NOK
Call Accounting Administration	OK	OK	OK
Call Accounting Administration (HTTPS)	OK	OK	OK
Call Accounting Reports	OK	OK	OK
Call Accounting Reports (HTTPS)	OK	OK	OK
EMPA - Phone Features	OK	OK	OK
EMPA - Phone Features (HTTPS)	OK	OK	OK
EMPA - Messaging	OK	OK	OK
EMPA - Messaging (HTTPS)	OK	OK	OK
EMPA - Call Manager Download	OK	OK	OK
EMPA - Call Manager Download (HTTPS)	OK	OK	OK
Meet-me Web Conference (WebRTC) - HTTPS Only	NOK	OK	NOK
Messaging Fax Printer driver 6.1	OK	OK	OK
Messaging Fax Printer driver 6.1 (HTTPS)	OK	OK	OK
Messaging Fax Printer driver 5.5	OK	NOK	OK
Messaging Fax Printer driver 5.5 (HTTPS)	OK	NOK	OK
Network eManager CIX	OK	NOK	NOK
TASKE Contact	OK	NOK	NOK
OK = Supported (OK) NOK = Not Supported (Not OK)			
(Sheet 1 of 2)			

This page is intentionally left blank.



# Chapter 3 – Enterprise Manager

---

Enterprise Manager is a web browser based application that resides on every IPedge server.

The Administration Terminal is a PC connected to the network, no special software is required. Enterprise Manager is a browser based interface that can be accessed from any computer with network access to the Primary node.

## SUPPORTED BROWSERS

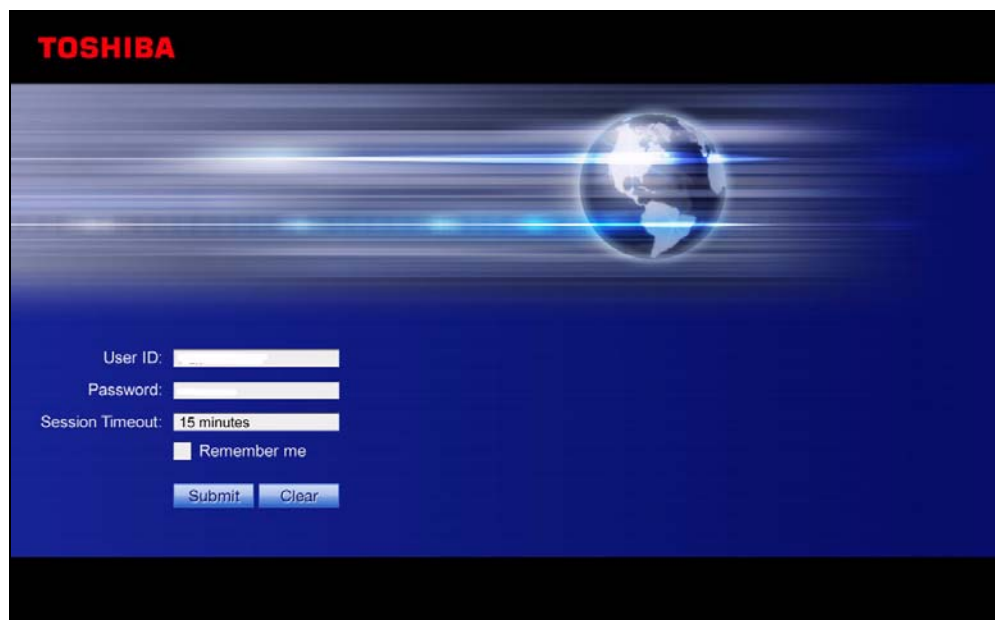
The Enterprise Manager can be accessed using:

- Microsoft™ Internet Explorer version 7 or later
- Mozilla Fire Fox version 5 or later - Must have IE Tabs

Refer to [“SUPPORTED BROWSERS” on page 2 - 4.](#)

## LOGIN

In the address bar of your internet browser enter the IP address of the IPedge server to which you wish to connect, Enterprise Manager uses port 8080.



**Note:** For remote Enterprise Manager access when an IPedge server is installed behind a firewall ports 8080 (Enterprise Manager) and 10000 (Webmin) must be open. When HTTPS is set 443 and 8443 must also be open.

## START PAGE

### START PAGE

After a successful login the Enterprise Manager will display the **Start Page**.

The Start Page will display:

- The name of the administrator logged in (Administrator) to this session.
- The login date and time
- The IPedge software release number (R1.5 and later)
- The Server Name and Server IP address
- The System Summary information

Click on the Toshiba logo on any page to return the this screen.

Click to display maintenance information for all nodes.

New software release is available.

Server Name	Serial Number	Mac Address	Current Version	FYI System #	Expiration Date
Node50	00R4HNP3C9	003048bac6fb	1.6.0.20	72201	11/15/2017
Node51	00R4HXX6BA	00304c3c98be	1.6.0.20	76701	11/15/2017

Click on the Get IPedge server maintenance information link to display:

- Server Name
- Server Serial Number
- Mac Address of the server
- The version of the software on each node
- The FYI System Number of each node
- The Maintenance license expiration date for each server

All of the items listed above are displayed on systems running R1.6.0.2 and later software. When the link is clicked the primary node will request the information from the other connected, nodes. The information is displayed as it is received.

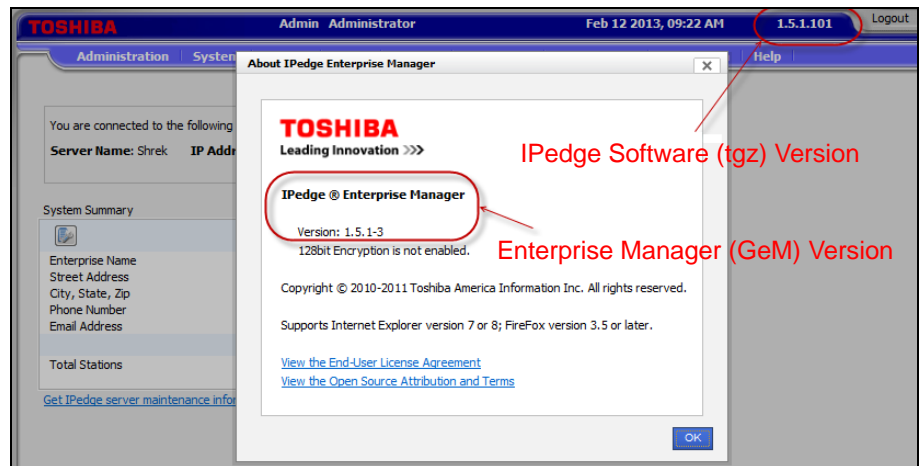
## VERSION DISPLAY

---

### VERSION DISPLAY

IPedge systems running R1.5.1 and later software will display the IPedge system version number on the Enterprise Manager start page. The displayed version will be the IPedge-component tgz version.

The Enterprise Manager version can be displayed in the About Enterprises Manager help. Select **Help > About**. This help menu item is only available on the Primary server. In a multi-node system only the Primary server will have this menu item. The Member server software versions can be displayed in the Program Update pages.



The Enterprise Manager start page will display the software version of the Primary server. Member servers of Multi-Node systems running R1.5.1 or later software will display the software version by using the **Maintenance > System Maintenance > Program Update** screen. A member server that does not have the 1.5.1-1 or later software will be displayed as 'unknown' until it has been upgraded.

### AUTOMATIC NEW VERSION DETECT

Enterprise manager will have the capability to perform IPedge new software release available detection. This is carried as a background service job that gets executed after mid-night. This function requires internet access.

The administrator can manually check if there is any new software available on the TAIS FTP site.

Automatic and manual detection compares the new software FTP site against the primary server only. If no newer software is available then no manifest file is downloaded. If a new version is available the administrator will see a notice on the Enterprise Manager start page. This function requires internet access using FTP (UDP ports 20 and 21).

**ROLES**

There are two types of Enterprise Manager user roles;

- System Administrators
- Telephone Users

Each role is defined as a list of permission items (access rights) that determine the user's access level in Enterprise Manager.

The *IPedge* system has four technician roles and two telephone user roles defined when shipped. These roles cannot be changed. New roles can be added to create custom definitions.

**Create a New Role**

New roles can be configured by adding a new Role and choosing the specific items to include.

1. Select **Administration > Roles**. Click on the **New** role icon.
2. Select the type of role.
3. Enter the name of the new role and a brief description of the new role. Check-mark the items to include in this role.
4. Click on the **Save** icon.

**Copy a Role**

1. Click on a role in the list.
2. Click on the **Copy** icon.
3. Enter a Name and brief description of the new role.
4. Select the items to include in this role.
5. Click on the **Save** icon.

**USERS**

When a **User** is added to the Enterprise Manager that User is assigned a role. The role defines the level of access that user has.

As each **Station** is assigned it is assigned, among other things, a DN and a Telephone User role.

**Administration User**

To add an administration user:

1. Login to Enterprise Manager.
2. Select **Administration > Users** a list of users will display.
3. Click on the **New** user icon.
4. Enter the following parameters. Unless otherwise noted the entries are required.

Login Name - The screen name of the user.

First Name - The user's first name

Middle Name - Optional, this field does not require an entry.

Last Name - The user's last name

Role Name - Select the name of the role that defines the permissions for this user.

Email Address - This entry is required but not used at this time.

5. Click on the **Save** icon.

**Phone User**

To add phone user:

1. Login to Enterprise Manager.
2. Select **Station > Station Assignment**.
3. Add a station or select an existing station and click on the **Edit** icon.
4. Check-mark the **Assign MPM Role** box. MPM refers to My Phone Manager.
5. Select the user role from the **Select Role** pull-down menu.
6. Click on the **Save** icon.

This page is intentionally left blank.

# Chapter 4 – System Installation

---

## INTRODUCTION

This chapter presents a detailed procedure for installing an IPedge system using a Model Database or entering your customer data manually.

The procedures shown below are based on pre-configuring the server before it is moved to the customer site.

## SYSTEM IP ADDRESS DEFAULTS

The default IP addresses of the IPedge Virtual Server, as shipped:

- **IPedge Enterprise Manager:** 192.168.254.250  
The subnet mask is 255.255.255.0. To login to Enterprise Manager enter **http://192.168.254.250:8080/oamp** into the browser address line. The User ID is **Administrator**, the password is **password**. The password is case sensitive. The administrator PC must be in the same subnet as the IPedge server.
- **ACD:** 192.168.254.252 (if equipped)  
The Windows User Name is **Valued Customer**, the password is **toshiba**. The password is case sensitive.
- **ESXi (VMware):** 192.168.254.245 (does not apply to IPedge ES servers)
- **iDRAC7:** 192.168.254.251 (if equipped)

## PRE-INSTALLATION REQUIREMENTS

Refer to the [Server Hardware Installation](#) chapter in this document for power, environment, and UPS requirements. Refer to the LAN Requirements in [Chapter 2–Network Requirements](#) for network performance specifications and measurement tools.

Before starting this procedure the following information is required for each IPedge server.

- Numbers from the Service Tag or the server serial number if there is no service tag. For IPedge ES servers use the serial number on the label attached to the top of the box, not the Intel label on the bottom of the box.
- Physical address where the server will be installed.
- The name and email address of the customer contact (this will be used by Dell for some service contacts).
- The customer will need a VMware license. If the customer does not already have a license, a free license is available. The customer will need to create a VMware account and get a license key. Does not apply to the IPedge ES server.

## NETWORK NAMES

---

- For on-line license systems the name and email address of one or two people to receive notice in the event the IPedge Host ID changes due to public IP address change. Up to five names can be entered for SMS text message notification.  
For off-line license systems the mail box to be sent a message if the license dongle is removed.
- IP Addresses - Refer to [“License Server Access” on page 2-2](#).
  - VMWare® (ESXi) requires one Static private IP address \*
  - VMWare® (ESXi) requires one Static public IP address - that is directed through a router/firewall to the IPedge system \*
  - IPedge Virtual Server requires one Static IP address \*
  - ACD Virtual Server (if equipped) requires one Static IP address
  - iDRAC (if used) requires one Static IP address\* Does not apply to IPedge ES servers
- Subnet mask
- Network Time Protocol source
- Host names
- Default Gateway IP address
- DNS server IP address (Required for Online Update operation)
- Domain name (FQDN) for the IPedge server used for UCedge operation. Refer to [UCedge SERVER REQUIREMENTS](#).
- Domain name (FQDN) for the ACD server (if equipped)  
**Note:** The domain names must be registered with a DNS server to resolve to the IPedge or ACD server public IP addresses. The system firewall or router must resolve the domain names to the private addresses.

## NETWORK NAMES

The network names shown in the table below are assigned during the server installation process.

The names use alpha-numeric characters (A ~ Z, a ~ z and 0 ~ 9) and are case sensitive. For example: NorthTower012

**Note:** Do not attempt to use spaces or special characters in the network names. Descriptive names are recommended. Names could show location by city, campus location or server room and rack location.

**Table 4-1 Network Names**

IPedge Name	Primary Node	Member Node	Notes
Enterprise Name	Required	Recommended	Domain name of this enterprise. Assign the same Enterprise name to all nodes.
Server Name	Required	Required	Unique, descriptive name of the server. Register this name in the DNS server.
Community Name	Required	Required	Unique, descriptive name - Used as authentication by internal processes.
Host Name	Required	Required	Same as the Server name.



## INSTALLATION

---

### INSTALLATION

This list is the system setup that must be complete before starting the install procedure.

- The IPedge server to a network switch.

**Important!** The network cables must be connected to the IPedge server before power is applied.

- Apply power to the IPedge server.
- From a PC login to Enterprise Manager.
- Pop-ups must be enabled on the PC browser.
- Set the system time and assign the NTP source.
- Set the IPedge server IP address.
- The IPedge server requires a static IP address.

### LICENSE DONGLE

The license dongle, if used, **MUST** remain plugged into the server at all times.

**Important!** If the dongle is not connected at system start-up critical functions will not start.

The system will monitor the USB license dongle. If the dongle is removed or replaced with an invalid dongle while the server is running it will continue to function for 24 hours then, the following occurs:

- All new calls (except E911) will be prohibited.
- If ACD is running it will change to 'demonstration' mode.
- New license container files will be rejected.

While the dongle is out:

- Configuration changes are allowed.
- Station registration such as Call Forward, or Do Not Disturbed are allowed.

When the dongle is reconnected normal operation is restored within one minute.

### VIRTUAL SERVER INSTALLATION PROCEDURE

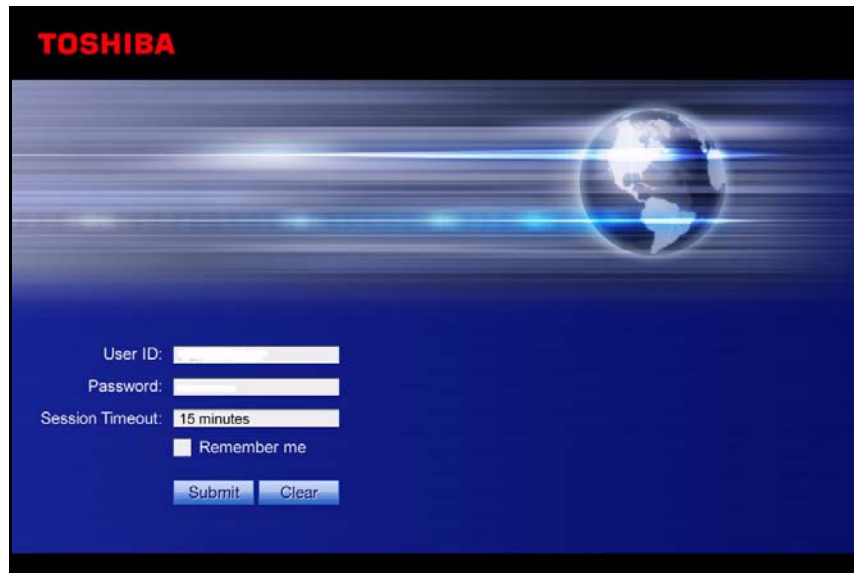
**Important!** Complete the ownership transfer and VMware license procedures in [Server Hardware Installation](#) of this manual before starting this installation process.

**Important!** If you are configuring this system off-site for later transport to the customer's site refer to the IPedge Virtual Licensing Service User Guide.

The following steps include instructions for installation with or without using a Model Database. The instructions also consider on-site system configuration and off-site pre-configuration.

**Login To The IPedge Server**

1. Refer to the [Chapter 1–Server Hardware Installation](#) chapter of this manual to complete the Dell ownership transfer and the VMware licensing.
2. Connect the IPedge server to a network switch.
3. Plug in the power cord(s). If there is a rear panel power switch set it to 1 (on).
4. Press the front panel power button. Initial boot-up will require approximately 5 ~ 8 minutes.
5. Login to Enterprise Manager on the IPedge server using the default IP address, User ID and Password.



6. When the Administrator logs into Enterprise Manager for the first time, Enterprise Manager will detect that the Administrator account password is the default value and it prompts the user to change the password.

The new password should be a 'strong' password with the following:

- At least eight characters, not more than 100 characters
- At least one character should be a capital letter
- At least one character should be a number
- At least one character must be a special character: period (.), underscore (\_), or hyphen (-)

**Note:** The password cannot be; password.

**Important!** This new password cannot be recovered. Once it has been changed, if you lose or forget the password contact Toshiba's Technical Support department.

**Initial Setup and Network Configuration**

When the system administrator logs in, Enterprise Manager checks the Network configuration. If the values are still at default the following screen is presented.

**Figure 4-1 Network Configuration, System Time and Date**

1. Enter the private IP address, Network Mask and Gateway of the IPedge server.

2. Enter the DNS IP addresses in the DNS Server list (shown in red above). The DNS server list must be entered to support Online Update and licensing operation.
3. Enter the Date and Time. Select the local Time Zone for this server.

**Note:** Do not check the ACD box if ACD software is not installed.

**Static Route**

The static route option allows the administrator to configure an alternative network route to access a specific destination.

The static route functionality has been added to IPedge Enterprise Manager System Setup/Network configuration page.

Interface	Network	Netmask	Gateway
bond0	10.10.2.250	255.255.255.0	10.10.2.1

Enterprise Manager will not apply the settings on this page until all data is collected from all initial setup pages and at the end it will show all entered data on a confirmation page where the user can either apply all changes or cancel. The next setup page includes the following:

- Enterprise Information
- IPedge Server Community Name
- IPedge Region

4. Login to Enterprise Manager, it will open to the System Setup page, set the IPedge IP address. This is the private IP address for the IPedge system. The IPedge system will reboot.

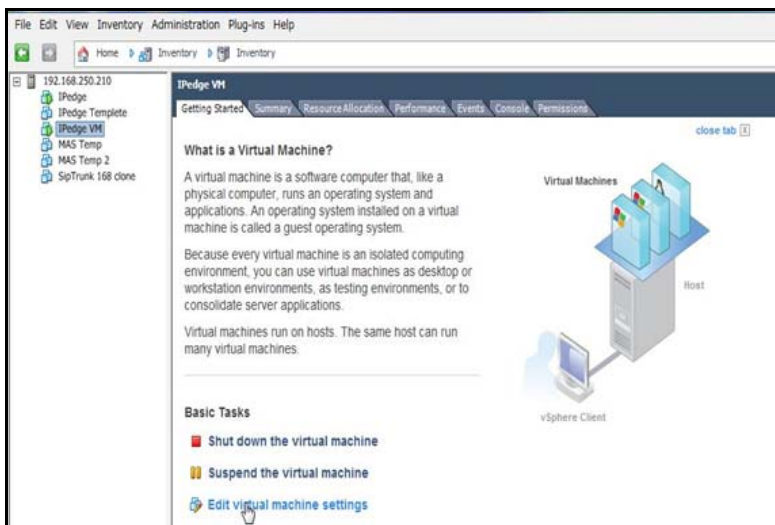
## USB PASS-THROUGH

IPedge virtual servers purchased with on-line virtual licensing have the USB pass-through set up, do to "[LICENSING](#)" on page 4 - 8. Existing IPedge virtual servers using the virtual licensing service that are upgrading to Off-line (dongle based) licensing require USB port pass-through setup. This setup procedure allows the virtual server VMware to recognise the license dongle when it is plugged into a USB port on the server.

1. Launch vSphere client on the administrator PC.
2. Login to the IPedge server.
3. Select the **Getting Started** tab.
4. Select the IPedge server from the list on the left side of the screen.
5. Click on **Shut down the virtual machine**.
6. Plug the license dongle into a USB port on the IPedge server.
7. Wait for the system to shutdown, about 2 minutes.

**Important!** The IPedge virtual machine must be completely shut down. To view the shutdown progress select the **Console** tab.

8. In the Getting started tab click on **Edit virtual machine settings**.



9. Go to the **Hardware** tab then, click on the **Add** button.
10. In the Device Type dialog select **USB Device** then click on the **Next** button.
11. Select **Aladdin Knowledge Sentinel HL**.
12. Click on **Next**.
13. In the Ready to Complete dialog click on **Finish**.

14. In the Hardware screen you will see the New USB Device, click on **OK**.
15. In the **Recent Tasks** at bottom of the screen wait for this task to complete before continuing.
 

**Note:** This procedure maps one USB port for license dongle pass-through. Toshiba recommends that you map all of the USB ports for license dongle use. **Move the USB dongle** to the next available USB port. Repeat [Step 6](#) through [Step 15](#) for each of the USB ports.
16. When all of the USB ports are complete, continue to [Step 17](#).
17. Select **Edit virtual machine settings**.
18. Click on **Edit virtual machine** on the getting started tab in the basic tasks.
19. Click on **Power on the virtual machine**.
20. Allow the IPedge virtual machine to run for two the five minutes to allow all of the processes to startup.

## LICENSING

Licensing is available in two types; On-line using the Toshiba Virtual Licensing service or Off-line using a license dongle. For on-line licensing go to [ON-LINE LICENSING \(Virtual Service\)](#). For Off-Line Licensing go to ["OFF-LINE LICENSING"](#) on page 4 - 10.

## ON-LINE LICENSING (Virtual Service)

1. After the system has restarted, login to Enterprise Manager, the system will display a **Not licensed** message.
2. In System Setup enter the license code sent from the Licensing Service. Click on **Next**.
3. Verify the information on the summary screen is correct then, click on **OK**. If the information is not correct click on Cancel.

**Please confirm**

Please review the information below carefully. Click the OK button to apply the configuration now.

**System Setup / Network Configuration**

<b>Server Name:</b>	IPedge	<b>DNS Server list:</b>	119.119.119.14	<b>System Time Zone:</b>	America/Los_Angeles
<b>Hostname:</b>	IPedge: IPedge-17016		119.119.119.140	<b>System Date:</b>	2015/08/28
	ACD:			<b>SystemTime:</b>	10:25
<b>IP Address:</b>	IPedge: 119.119.119.45			<b>System Time Sync Period:</b>	Daily
	ACD:			<b>System Time Sync Server:</b>	north-america.pool.ntp.org
<b>Network Mask:</b>	255.255.255.0				
<b>Gateway:</b>	159.119.119.1				

**System Setup / Enterprise Region and Licensing**

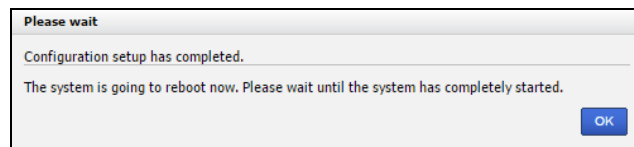
<b>Enterprise Name:</b>	Default Enterprise
<b>Street Address:</b>	123 Enterprise Ctr
<b>City, State, Zip:</b>	Enterprise City, State
<b>Region:</b>	USA

**IPedge License Key:** AES9-AES9-AES9-AES9

**Note:** A system **restart** is required for the configuration changes to be effective. Configuration can be resumed after the system is restarted.

4. When the OK icon is clicked, the IPedge system will contact the virtual licensing server.

5. The IPedge server will complete the licensing process after the database is synchronized, This will take approximately 10 minutes.
6. After the database synchronization the IPedge system will display a series of prompts as licensing is applied to each system database. This process will run for approximately 20 minutes.
7. When these processes are complete the system will display a Configuration complete prompt.
8. Click on **OK**. The system will reboot.

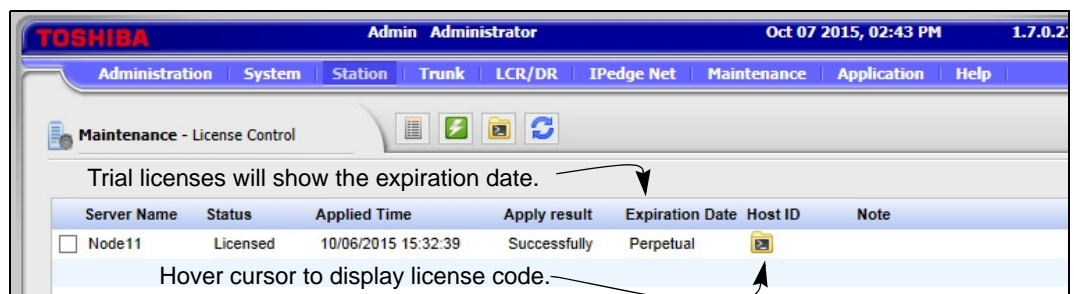


9. When the system has finished the reboot and start up, login to Enterprise Manager. The system will open in the System Setup screen. Apply a model database or skip to system database configuration.

**Note:** The system will not allow login to Enterprise Manager until all of the system services have started.

Verify Media Server

10. Verify that the Media Server is running. In Enterprise Manager select **Maintenance > Call Processing Status**.
11. If the Media Server is running the system has restarted correctly. Go to the next installation process. If the Media Server status is Disabled by fault go to [Step 12](#).
12. Select **Maintenance > System Maintenance > System Processes**, click on the Restart icon.
13. When the system has restarted login to Enterprise Manager then, select **Maintenance > Call Processing Status**.
14. If the Media Server is running the system has restarted correctly. Go to the next installation process. If the Media Server status is Disabled by fault contact Toshiba's Technical Support department
15. Select **Maintenance > License Control**. Trial license expiration dates and license detail information can be displayed.



### Off-Site Configuration

If this system is being configured off-site use the following procedure when the programming is complete.

1. Shut down the IPedge system in preparation for moving the system to the customer's site.
2. Login to the FYI Licensing service.
3. Request a license transfer for this system. Refer to the IPedge Virtual Licensing system user guide for detailed instructions. A new license code will be sent to the listed contacts.
4. At the customer site install the IPedge system.
5. When the systems boots up login to Enterprise Manager. Systems running 1.7.0 software will display a Not Licensed' message. Systems running 1.7.1 or later software will display a 'system will be degraded in 30 days' message.
6. Enter the new license code in the initial setup screen.
7. The system will restart with the licenses applied.
8. Verify that the Media Server is running. In Enterprise Manager select **Maintenance > Call Processing Status**.
9. If the Media Server is running the system has restarted correctly. Go to the next installation process. If the Media Server status is Disabled by fault go to [Step 10](#).
10. Select **Maintenance > System Maintenance > System Processes**, click on the Restart icon.
11. When the system has restarted login to Enterprise Manager then, select **Maintenance > Call Processing Status**.
12. If the Media Server is running the system has restarted correctly. Go to the next installation process. If the Media Server status is Disabled by fault contact Toshiba's Technical Support department.

**OFF-LINE LICENSING**

Licenses are purchased through the Toshiba FYI website. Use the following procedure to update or add new licenses. The license dongle serial number is entered during the license generation process on the FYI website.

**Note:** Off-line, dongle based licensing is not available on Toshiba branded IPedge servers.

**Download License File**

After the licenses have been purchased a license file will be sent to the contact email address. Download the license file to the Administration PC. The file can be saved to any file storage unit on a network that the administration PC and the IPedge server can access. Use the following procedure to apply the license file to the IPedge server.

**Important!** Ensure that the Region code is set to your region before applying licenses.

**Upload and Apply License**

1. Login to the Enterprise Manager on the Primary IPedge server.
2. Select **Maintenance > Licensing > License Control**.
3. Select the server to be licensed.
4. Click on the **Upload License** file icon.



5. Enter the location and name of the license file or click on the Browse button to locate the license file.
6. Click on **OK**.

The license file name, server MAC address and the server name will be displayed. Verify that the MAC address is the correct address for this server. Double click on this line for a detailed list of the licenses.

7. Click to check-mark the uploaded file then, click on the **Apply** icon.
8. After the license is applied, the license result should show "Successful".
9. Then check "**Yes, I want to reboot the system now**" and click on **OK**. Reboot can take several minutes.

### Display License Information

To display the items and quantities licensed on the server.

1. Login to the Enterprise Manager on the Primary IPedge server.
2. Select **Maintenance > Licensing > License Information**.
3. Select the server to display.

To display detailed information about a specific license.

1. Login to the Enterprise Manager on the IPedge server you are going to license.
2. Select **Maintenance > Licensing > License Control**.
3. A list of all the licenses on the server will be displayed.
4. Click to check-mark a license then, click on the **View** icon.
5. After the IPedge server has restarted, login to Enterprise Manager.
6. In Enterprise Manager select **Administration > Enterprise > Servers**.
7. Check the Server Name box and click the **Server Synchronization** icon.
8. The Enterprise - Servers Status screen displays. Check the Table Name box then click on the "**Order database synchronization**" icon.
9. A confirmation dialog window will display. Click on **OK** to start the database synchronization. Wait for the database synchronization to finish. This will take a few minutes.

### Off-Line License Off-Site Configuration

If this system is licensed using the license dongle there are no special procedures required for off-site configuration.

### IPedge ES LICENSING

Licenses are purchased through the Toshiba FYI website The IPedge ES serial number is entered during the license generation process on the FYI website. After the licenses have been purchased a license key will be sent to the contact email address.

1. Ensure that the IPedge system is connected to a LAN with internet access.

2. Power up the server. After the system has started, login to Enterprise Manager, the system will display a **Not licensed** message.
3. Perform the initial system setup including the Network Configuration. The system will reboot.
4. When the reboot is complete login to Enterprise Manager.
5. In the initial system setup confirm the information displayed then press the **Next** icon.
6. In the License Information field enter (copy past) the license string sent to the from the Licensing Service. Press the **Next** icon.
7. Confirm the displayed information, click on the **OK** icon.
8. The system will reboot. The database synchronization will run. This will take several minutes.
9. When the process is complete you will be able to login to Enterprise Manager. The internet connection can be removed at this point.

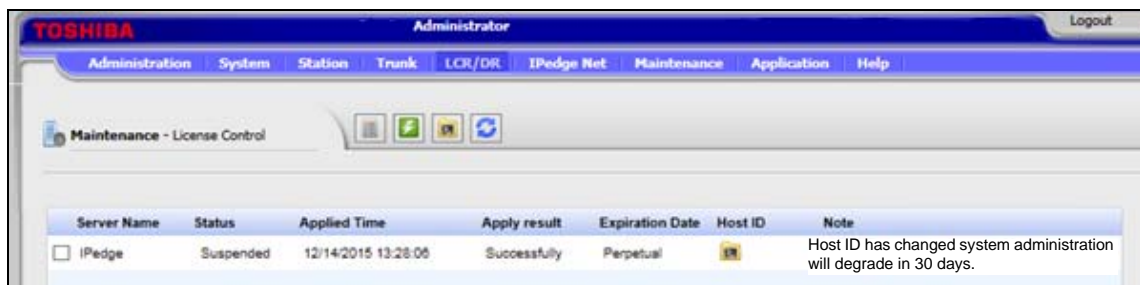
Internet connection will be required for license changes or software updates.

**ADMINISTRATION NOTIFICATION SETTINGS**

IPedge servers running 1.7.4 (or later) software will have one of two licensing systems. On-line virtual licensing requires a connection to the internet and a static public IP address. The dongle based off-line system requires the dongle to be plugged in at all times.

**On-Line License**

When an IPedge system running 1.7.4 or later software with a changed WAN IP address contacts the licensing service the IPedge system will continue to run. Even after a system reboot, the call processing will continue. The Enterprise Manager login page and the License pages will display a changed Host ID message. The administrator will have 30 days to transfer the licenses to the new IP address. If a license transferred to the new Host ID within 30 days the Enterprise Manager access will be degraded. The degraded access will allow only license transfer.



The IPedge system can send an email and text message notification when the public WAN IP Address changes. A list of email addresses and phone numbers for text messages can be configured to receive a notification if the IPedge system detects the public WAN IP address change. In Enterprise Manager select **Administration > Notification Setting**.

**Off-Line License**     The dongle based offline licensing option in eliminates the need for internet access or a static IP address by binding the license to the dongle. Once the license is bound to a dongle, the dongle must be plugged into the IPedge server at all times. If the license dongle is unplugged, a notification voicemail will immediately be sent to the people in the notification list. After 24 hours, all calls, except 911, will be prohibited until the license dongle has been plugged back in

## SIP TRUNK WIZARD

**Note:** SIP trunks must be Toshiba's SIP Trunking I-VoIP Service to use this initial setup SIP trunk wizard.

1. In this screen the administrator can upload a Model Database. Toshiba's SIP Trunking I-VoIP Service SIP trunks can be added using the SIP trunks setup wizard. The SIP URI List must be a CSV file. The URIs are available in the VIPedge portal, where the SIP trunks are ordered, in the DID tab.

The SIP User Name and SIP URI Password are shown in the VIPedge portal in the Customer Services tab as Trunk # and Password respectively.

**TOSHIBA**
System Initial Setup / IPedge Configuration

**IPedge Data Model**

You may upload a standard IPedge data model and apply it now or you may do it later by running Initial Setup again. If you want to do it later, do not change the server name from the IPedge default name.  
**Note:** The Enterprise Name and Address will be overwritten with content from the Data Model.

**Data Model File:**

**Toshiba SIP Trunk Configuration**

The Initial Setup wizard will create the ILG and OLG group #1 for the Toshiba SIP Trunk configuration. If the groups already exist, then they will be deleted and re-created prior creating the Toshiba SIP Trunk. You may also upload a csv file containing the list of URIs for this trunk. If the file is uploaded, then the wizard will configure the URI table as well.

**SIP Trunk Channels:**  **Effective Channel Number:**

**DID Digits:**

**SIP URI List File:**

**SIP URI User Name:**  **SIP URI Password:**

If the SIP URI list is uploaded, then the Initial Setup wizard will create DID configuration from the uploaded SIP URI list. Use the controls below to enter the parameter values for the DID configuration.

**MOH Source:**  **GCO Key Group:**  **Pooled Key Group:**

**DID Destination Selection:**

**VMID Selection:**

- Click on the Apply button to save configuration.



- Verify the data, click on the **OK** button to restart the server.
- Verify Media Server
- Verify that the Media Server is running. In Enterprise Manager select **Maintenance > Call Processing Status**.
  - If the Media Server is running the system has restarted correctly. Go to the next installation process. If the Media Server status is Disabled by fault go to [Step 6](#).
  - Select **Maintenance > System Maintenance > System Processes**, click on the Restart icon.
  - When the system has restarted login to Enterprise Manager then, select **Maintenance > Call Processing Status**.
  - If the Media Server is running the system has restarted correctly. Go to the next installation process. If the Media Server status is Disabled by fault contact Toshiba's Technical Support department
  - Log in to Enterprise Manager.
  - If a Model Database was loaded the System Summary information must be entered. The first screen shown after login is the System Summary. Click on the **Edit** icon. Enter the Enterprise Name and Address for this server. Enter the phone number and an email address. Click on the **OK** button.
 

**Note:** The Enterprise Name and information can be changed at any time.
  - Go to [CHANGE SYSTEM PASSWORDS](#).
 

**Note:** If you wish to change the SIP trunk assignments using the System Initial Setup refer to "[SYSTEM INITIAL SETUP](#)" on [page 14-5](#).

**CHANGE SYSTEM  
PASSWORDS**

For added system security some of the system passwords must be changed from the default settings.

**Change FTP Password**

1. Login to Enterprise Manager.
2. System select the server.
3. Select **Application > Webmin**.
4. In Webmin select **System > Change Passwords**.
5. Click on **ftp**.
6. Enter the **New password**,
7. Click on the **Change** button.
8. Click on **Return to user list**.

**Change Admin Password**

9. Click on **admin**.
10. Enter the **New password**,
11. Click on the **Change** button.
12. Click on **Return to user list**.

**Change Tech Support  
Password**

13. Click on **techsupport**.
14. Enter the **New password**,
15. Click on the **Change** button.

**Important!** Record the new passwords in a safe location. **Do NOT change any other passwords.**

**Important!** This password may be reset to the default after some software restore or upgrades. After each upgrade or restore check the Webmin password.

**CHANGE ROOT  
PASSWORD**

The Linux operating System root password must be changed from the default for added system security.

1. Login to Enterprise Manager.
2. System select the server.
3. Select **Application > Webmin**.
4. In Webmin select **System > Change Passwords**.
5. Click on **root**.
6. Enter the **New password**,
7. Click on the **Change** button.
8. Close the Webmin window.

**Important!** Record the new passwords in a safe location. Do NOT change any other passwords.

**IP ADDRESS CHANGE**

When the IPedge server public IP address changes the Host ID, based in part on the IP address, changes. When a system using on-line virtual

licensing contacts the virtual licensing service the Host ID change will be flagged. This does not apply to systems using off-line (dongle based) licensing. The notice will appear when anyone logs in to Enterprise Manager. If the license is not transferred to the new Host ID within thirty days Enterprise Manager will not allow further database changes. The only change allowed will be to enter a transferred license code. Notification of the public IP address can be sent as an email or text message.

1. Login to Enterprise Manager. Select **Administration > Notification Setting**.
2. Enter names and email addresses.
3. Enter names and cell phone information for text message notification.
4. Click on the **Save** icon.

**DATABASE PREPARATION**

If you have used the System Initial Setup/IPedge Setup and a Model Database go to ["CONFIGURE IPedge MESSAGING"](#) on [Page 4-18](#).

If you have used the System Initial Setup/IPedge Setup and you are not using the Model Database enter the customer's database then, go to ["CONFIGURE IPedge MESSAGING"](#) on [Page 4-18](#).

**Database Setup**

If you are going to use a model database and did not apply it in the System Initial Setup/IPedge Setup change the system name to IPedge (default value) then go to ["MODEL DATABASE PROCEDURES"](#) on [Page 4-35](#).

**CONFIGURE IPedge MESSAGING**

IPedge Messaging can be setup on an IPedge Application server as a voice mail server for Strata CIX systems.

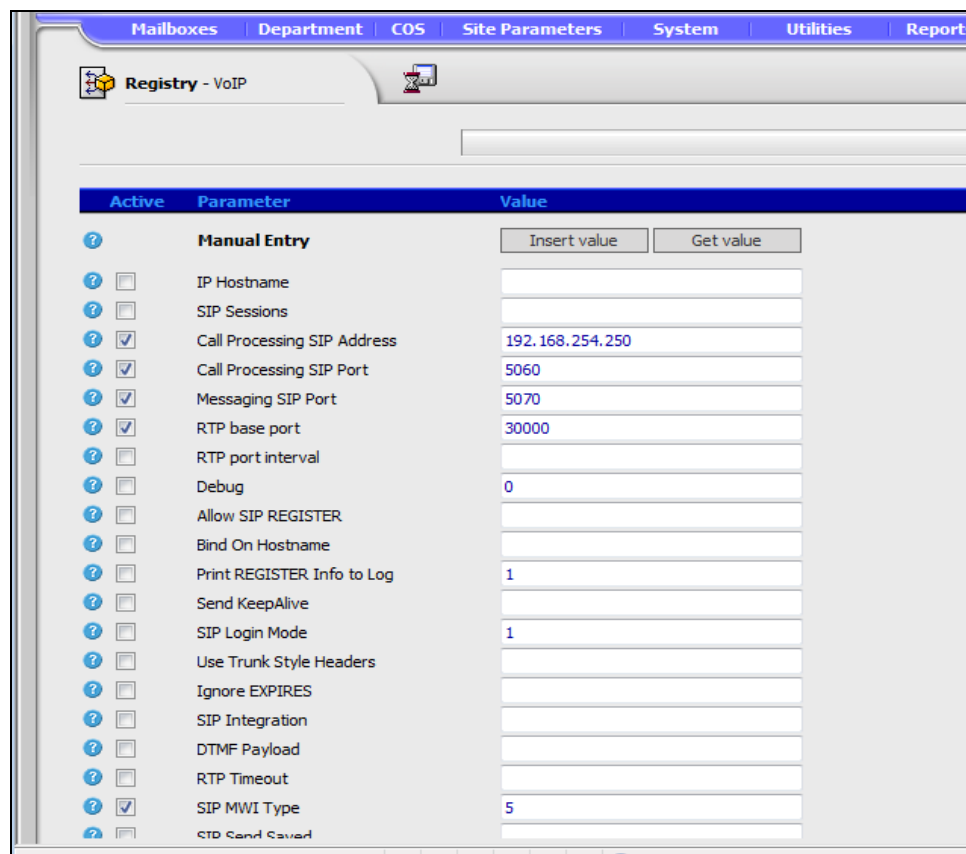
For IPedge server messaging refer to [“IPedge MESSAGING CONFIGURATION” on page 4 - 23.](#)

**Application Server Configuration**

Verify the following parameters before configuring IPedge Messaging:

- Specify number of voice ports and station number.  
Voice port station numbers need to match the Call Processing station numbers.
- Number of voice ports licenses
- Number of voice mailbox licenses  
Ensure that the number of mail box licenses are enough for the number of stations.

1. To configure the Messaging Voice ports login to Enterprise Manager. Select **Application > Messaging**.
2. In the Messaging Administration menu select **Registry > VoIP**.



3. The following parameters must be customized:
  - A. Ensure that IP Hostname is un-checked and the parameter field is blank.

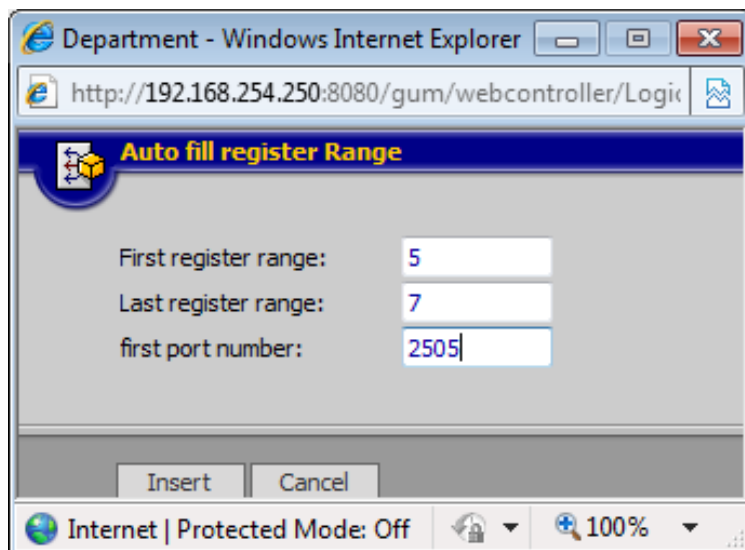


- B. Call Processing SIP Address: Enter the MIPU IP address for an Application server connecting to an IPedge system. Otherwise, enter the IP address of the IPedge server.
- C. Register X: At least four voice port entries will be displayed after you load the model database file. Refer to the example below.

<input type="checkbox"/>	MWI On Prefix		
<input type="checkbox"/>	MWI Off Prefix		
<input checked="" type="checkbox"/>	Register 1	2501:2501:2501	Fill Register range
<input checked="" type="checkbox"/>	Register 2	2502:2502:2502	
<input checked="" type="checkbox"/>	Register 3	2503:2503:2503	
<input checked="" type="checkbox"/>	Register 4	2504:2504:2504	
<input type="checkbox"/>	Register 5		
<input type="checkbox"/>	Register 6		
<input type="checkbox"/>	Register 7		
<input type="checkbox"/>	Register 8		
<input type="checkbox"/>	Register MWI Channel		

- 4. If necessary, add voice ports by using the following steps:
  - A. Click “Fill Register range,” the window shown below will open.
  - B. Specify first range index number in “First register range” field.
  - C. Specify last range index number in “Last register range” field.
  - D. Specify first voice port number in “first port number” field.
  - E. To create, press “Insert” icon.
  - F. Then click “Save” icon.

Creating 2505, 2506 and 2507 voice ports in Register 5 ~7 is shown below as an example.



**Note:** Voice port numbers must be consecutive.

- Configure the Channel definition table. Select **Registry > System > Channel Definition**.

If model database is loaded, some voice ports are assigned.

Enter voice ports in Channel Definition table if necessary.

Enter voice port number in the DN field.

Change "Rec.Calls" field to "Yes"

Any channels which appear on this page but do not have a DN should have **Init Calls** set to **No**.

Click on the **Save** icon.

- If you added voice ports in [Step 4](#) above you must add those ports here.

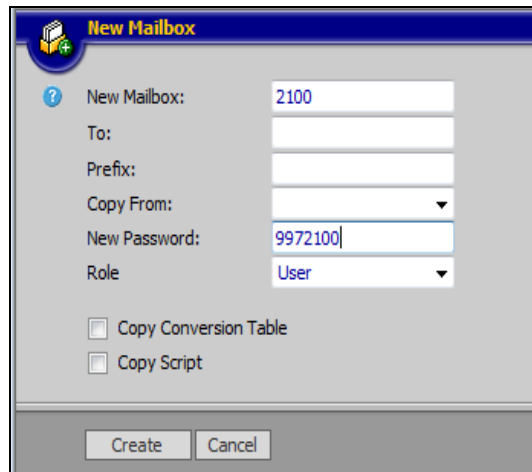
Chnl	DN	Dep.	Rec. Calls	Init. Calls	Mode	Type	PSTN Gateway	Fax Extension
1	2501	1	Yes	Yes	AutoAttend	Primary	0	
2	2502	1	Yes	Yes	AutoAttend	Primary	0	
3	2503	1	Yes	Yes	AutoAttend	Primary	0	
4	2504	1	Yes	Yes	AutoAttend	Primary	0	
5		1	No	Yes	AutoAttend	Primary	0	
6		1	No	Yes	AutoAttend	Primary	0	
7		1	No	Yes	AutoAttend	Primary	0	
8		1	No	Yes	AutoAttend	Primary	0	

7. Program the mailboxes. By default, no mailboxes are created. They must be created manually.

In the Messaging window, select **Mailbox > Properties**.

A range of Mailboxes can be created by entering a value in the **To** field of the New Mailbox screen.

Creating a New Mailbox Click **New Mailbox** icon. The New Mailbox dialog box will open.



Enter mail box number in “New Mailbox” field.

Enter password in “New Password” field.

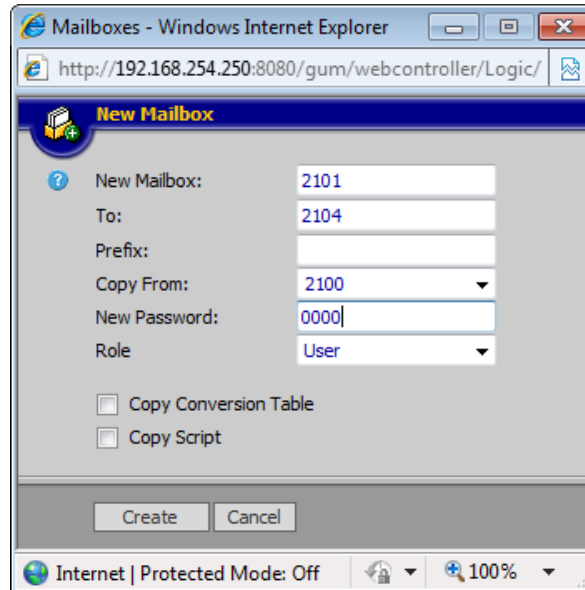
Choose “User” role.

Click “Create” icon.

Click “Save” icon.

8. Customize following parameters, then those parameters will be copied to new mail boxes.
  - Department: default value is 1
  - Class of Service: default value is 1
  - Mailbox Type
  - Wakeup Mode
  - Transfer Mode:
  - MWI
  - Call Record Timer and Mailbox Language
9. To save your configurations, Click “Save” icon

Creating Multiple Mailboxes Use the mailbox copy function. The following example is to copy mail box 2100 to 2101 thru 2104.

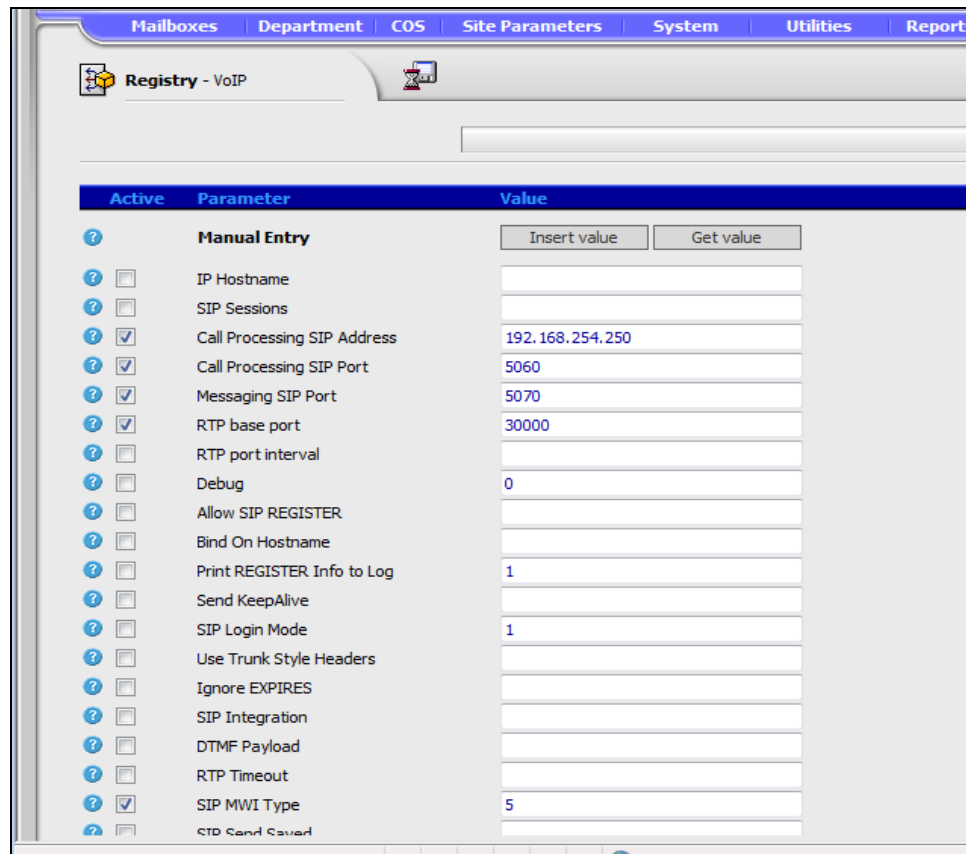


- A. Click on the **New Mailbox** icon.
  - B. Enter mail box number what you make now in the **New Mailbox** field.
  - C. Enter last mail box number in **To** field.
  - D. Enter original mail box number in **Copy From** field.
  - E. Enter password in **New Password** field.
  - F. Click on the **Create** icon to create mailboxes.
  - G. Click the **Save** icon.
10. Customize each mail box configuration.
    - A. First and Last name field.
    - B. Time zone if necessary
  11. Verify voice mail basic functions
    - A. Dial the extension number for each voice port.
    - B. Then you hear "Please enter your password"
    - C. Enter your password then hear "Welcome to voicemail..."
  12. Run data back up for Messaging: **Utilities > Database Maintenance**

## IPedge MESSAGING CONFIGURATION

1. To configure the Messaging Voice ports login to Enterprise Manager. Select **Application > Messaging**.

2. In the Messaging Administration menu select **Registry > VoIP**.



3. The following parameters must be customized:
  - A. Ensure that IP Hostname is un-checked and the parameter field is blank.
  - B. Call Processing SIP Address: Enter the MIPU IP address for an Application server connecting to an IPedge system. Otherwise, enter the IP address of the IPedge server.

- C. Register X: At least four voice port entries will be displayed after you load the model database file. Refer to the example below.

The screenshot shows a configuration window with a list of settings on the left and input fields on the right. The settings are:

- Use US Codes
- MWI On Prefix
- MWI Off Prefix
- Register 1
- Register 2
- Register 3
- Register 4
- Register 5
- Register 6
- Register 7
- Register 8
- Register MWI Channel
- PSTN Gateway 0

The input fields on the right contain the following values:

- Register 1: 380:7Y3h0U5c:380
- Register 2: 381:H3c7F2x6:381
- Register 3: 382:9f0G3o6O:382
- Register 4: 383:W3t4C8f0:383
- Register 5: 384:h1P8j7N4:384
- Register 6: 385:h8T4z7Y3:385
- Register 7: 386:Q8g5N6i7:386
- Register 8: 387:P1m9N0o8:387

A "Fill Register range" button is located to the right of the Register 1 input field.

- 4. If necessary, add voice ports by clicking on New Mailbox.

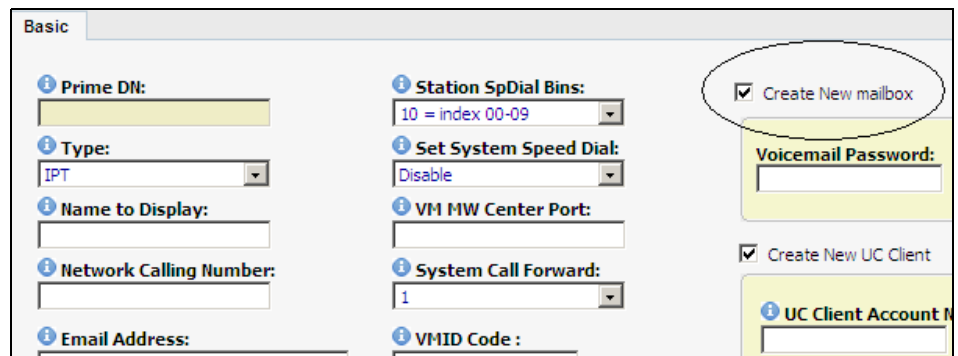
The screenshot shows a "New Mailbox" dialog box with the following fields and options:

- New Mailbox: 2100
- To: (empty)
- Prefix: (empty)
- Copy From: (dropdown menu)
- New Password: 9972100
- Role: User (dropdown menu)
- Copy Conversion Table
- Copy Script

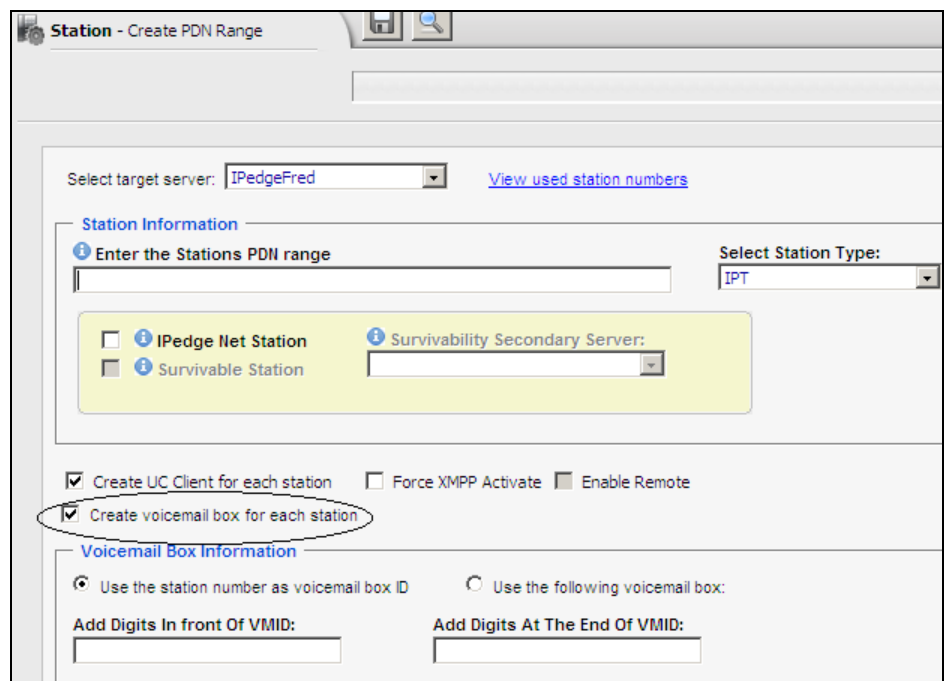
Buttons for "Create" and "Cancel" are at the bottom.

It is, however, usually more efficient to create the mailbox from the

Basic Station Assignment page or the Create PDN Range page in the



IPedge programming.



5. Configure the Channel definition table. Select **Registry > System > Channel Definition**.

If model database is loaded, some voice ports are assigned.

Enter voice ports in Channel Definition table if necessary.

Enter voice port number in the DN field.

Change “Rec.Calls” field to “Yes”

Any channels which appear on this page but do not have a DN should have **Init Calls** set to **No**.

Click on the **Save** icon.



- If you added voice ports in [Step 4](#) above you must add those ports here.

The screenshot shows the 'System - Channel Definition' configuration page in the TOSHIBA IPedge interface. The page includes a navigation menu with options like Mailboxes, Department, COS, Site Parameters, System, Utilities, Reports, and Registry. Below the navigation is a search bar and a table of channel definitions.

Chnl	DN	Dep.	Rec. Calls	Init. Calls	Mode	Type	PSTN Gateway	Fax Extension
1	2501	1	Yes	Yes	AutoAttend	Primary	0	
2	2502	1	Yes	Yes	AutoAttend	Primary	0	
3	2503	1	Yes	Yes	AutoAttend	Primary	0	
4	2504	1	Yes	Yes	AutoAttend	Primary	0	
5		1	No	Yes	AutoAttend	Primary	0	
6		1	No	Yes	AutoAttend	Primary	0	
7		1	No	Yes	AutoAttend	Primary	0	
8		1	No	Yes	AutoAttend	Primary	0	

**RESTART IPedge SERVER**

1. From Enterprise Manager, select **Maintenance > System Maintenance > System Processes**.
2. Click on the **Reboot System** icon.
3. Enter **OK** to confirm the reboot.
4. Click on **OK**.

## Verify Media Server

5. Verify that the Media Server is running. In Enterprise Manager select **Maintenance > Call Processing Status**.
6. If the Media Server is running the system has restarted correctly. Go to the next installation process. If the Media Server status is Disabled by fault go to [Step 7](#).
7. Select **Maintenance > System Maintenance > System Processes**, click on the Restart icon.
8. When the system has restarted login to Enterprise Manager then, select **Maintenance > Call Processing Status**.
9. If the Media Server is running the system has restarted correctly. Go to the next installation process. If the Media Server status is Disabled by fault contact Toshiba's Technical Support department

**Important!**

To complete your customer's database, you can proceed with any other further changes you wish to include. However, before you make any further changes, please do a Call Processing and Messaging backup. Refer to the following sections of the following chapters and sections of this manual.

IPedge System Backup – [“MANUAL BACKUP” on page 6-5](#).

Messaging Backup – [“MESSAGING BACKUP” on page 13-10](#).

Note: The steps that relate to a multi-node system do not apply.

10. Ensure that the system time has been set.

**SYSTEM DATABASE BACKUP**

When the system configuration and database programming is complete backup the Call Processing and Messaging database backup. Refer to [“MANUAL BACKUP” on Page 6-5](#).

**HTTPS CERTIFICATE**

1. If you are going to use https secure connection to the Enterprise Manager create the https certificate. Refer to [Chapter 7–HTTPS Configuration](#) in this manual then go to [“Database Setup” on page 4 - 17](#).
2. If you are not going to use https go to [“Database Setup” on page 4 - 17](#).

**Note:** For an enterprise system with one or more member servers create the HTTPS certificate for the Primary server then, attach the member servers. After the member is attached create the HTTPS certificate for the member.

If this is a single server, stand-alone system you can now begin programming. Refer to the call programming sections in the Features Description manual.

If this is one node of a multi-node system proceed to [“ASSIGN MEMBER NODE” on page 4 - 30.](#)

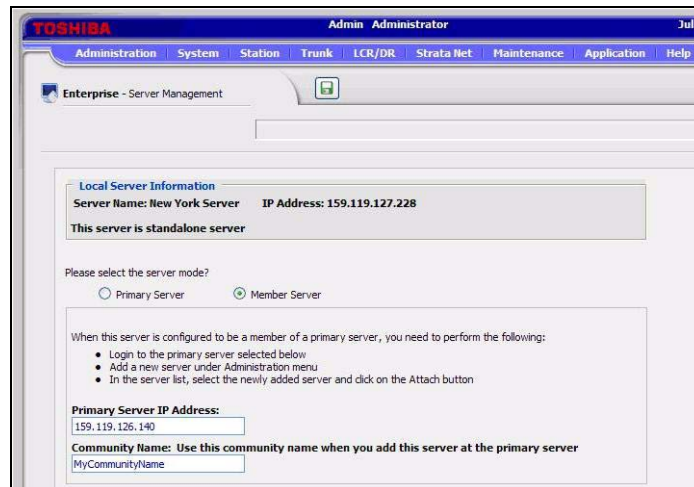
**ASSIGN MEMBER NODE**

The previous procedure sets up each IPedge server as a stand alone system. The following procedure changes a server to a member server and attaches that server to the Primary Node.

This procedure is performed for each member server in an enterprise.

**Important!** Member nodes must be attached one-at-a-time. Complete this procedure for one node. Then, complete this procedure for the next node.

1. Login to Enterprise Manager on the IPedge server that you want to be a member of an enterprise. Use the IP address of the server to access Enterprise Manager on that node.
2. Select **Administration > Enterprise > Server Management**.
3. Click on the **Member Server** radio button.
4. Enter the Primary Server IP address.
5. Enter the Community Name you assigned to this member server earlier.



6. Click on the **Save** icon.
7. The server will stop accepting commands.



- Repeat this process for each Member Node.

**ADD MEMBER NODE**

The following process adds then, attaches the member nodes to the primary node. Toshiba branded IPedge EC and EM servers, and all IPedge virtual servers can be a primary node.

- Login to the primary node Enterprise Manager.
- Select **Administration > Enterprise > Servers**. The first time you enter this screen the Server Name list will be empty.
- Click on the **Add** icon.

The screenshot shows the 'Enterprise - Servers' configuration page in the Toshiba Enterprise Manager. The page has a blue header with the Toshiba logo and navigation tabs: Administration, System, Station, Trunk, LCR/DR, Strata Net, Maintenance, Application, and Help. The main content area contains several input fields: 'Server Name', 'IP Address', 'Community Name', and 'Confirm community name'. Below these is a yellow-highlighted 'Server Information' section with a 'Detect Server Information' button. This section includes dropdown menus for 'System Type' (set to GEMINI) and 'Region' (set to USA), and input fields for 'Version' and 'Mac Address'. At the bottom of the form is a 'Description' text area.

- Enter the Server Name, IP Address and Community Name of the member node to be added.
- Click on **Detect Server Information**. The System Type, Version and Mac Address information will be displayed.
- Enter location and any other useful information into the Description box.
- Click on the **Save** icon.
- Click on the **Search** icon to display the server list.

**ATTACH MEMBER NODE**

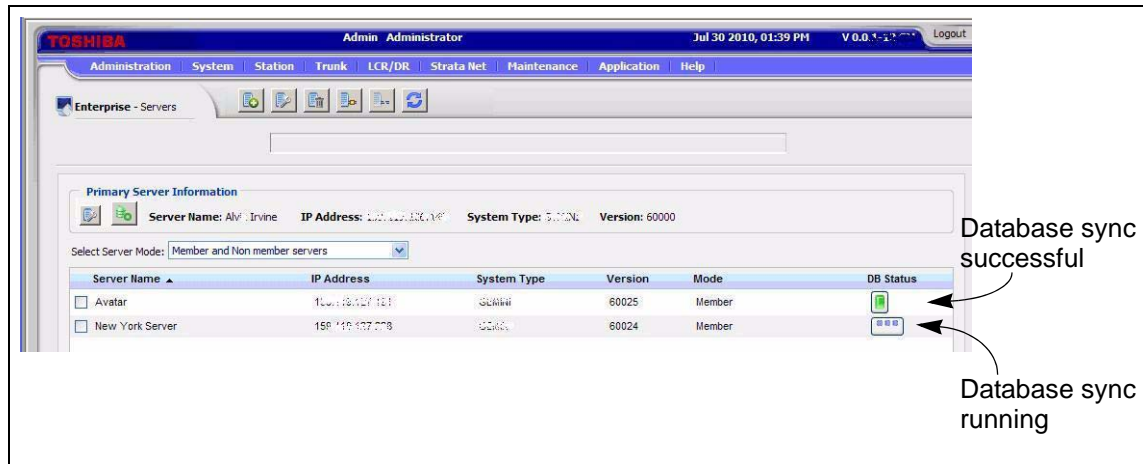
This procedure attaches the member nodes. Part of the attach process is the database synchronization from member to primary node.

- If the server list is not displayed select **Administration > Enterprise > Servers**.
- Click to check-mark the member server to attach.
- Click on the **Attach** icon.

- The primary node will start the database synchronization process. This can take several seconds to a few minutes. The Database Status indicator will change to green when complete. Click on the Reload icon to refresh the status display.

**Note:** The database synchronization can take several minutes.

- You can Add and Attach other member nodes while the database sync process is running.



When the database synchronization is done the node is connected.

## DETACH A MEMBER NODE

The following procedure covers the steps taken to detach a member node from the primary server in an enterprise system. Detaching a node changes that node from a member of an enterprise to stand alone, primary server. After the node is detached it will not accept programming changes from any other node. If the node was a member of an IPedge Network, it will continue to function as a part of the network. Note that any changes made to other nodes in the network that effect network operation will also need to be made to the detached node.

- Toshiba recommends that you perform a full backup of the database on the server you are going to detach before starting this procedure.
- Login to the Primary node.
- Select **Administration > Enterprise > Servers**.
- Click to check-mark the Server Name of the node to be detached.
- Click on the Detach Server icon.
- In the address field of your web browser enter the IP address of the member node you are detaching. Click on **Show local login**.
- Login to the node. Click on the **Server Management** button.
- Click on the **Primary Server** radio button. Then, click on the **Save** icon.
- Click on **OK**.

10. The server is no longer a member of the enterprise. It is now a stand alone system. Select **Administration > Enterprise > Servers**. Notice that the icon in the Primary Server Information section of the screen shows that the database is updating. The Bacula application on this server is creating a backup of the database. Please wait until the backup is complete before making any additional changes.

**Note:** This process may take several minutes, depending on the size of the database. You may logout of Enterprise Manager at this time.

**Note:** If it becomes necessary to re-image the server using the flash drive supplied with the system you must first detach the server if it is part of a multi-node system.

- Backup the server if possible
- Detach the node
- Refer to the OVA Template Restore procedures in this manual.
- Enter (copy and paste) the license code then restore the database
- Attach the node

### Over Subscribing

It is possible to assign more of some system resources than are licensed. This allows the administrator to program stations, or trunk resources at the expected level but only license to the current requirement. The resources in excess of the license will not function until a new license is applied. For example; 250 stations programmed on a system licensed for 200 stations. The first 200 stations to register will operate.

### REGION CODE

The Region is based on the physical location of the IPedge system. The Region must be set before the system licenses are applied. The Region default value is USA.

The Region Code is setup during the Initial setup process. Use this procedure to change the region code.

**Important!** For IPedge systems installed in the USA do not change the Region.

**Note:** Changing the Region after licenses have been installed requires that all of the system data (stations, trunks, etc.) be deleted or the system be re-imaged using an IPedge system recovery ISO image disk. All programming will be lost.

1. Login to Enterprise Manager on the server to be named.
2. Select **Administration > Enterprise > Servers**.

3. Click on the **Edit** icon.
4. Click to check-mark the **Select Region** box.
5. Select the Region from the **Region** pull-down menu.

IP Address:  
127.0.0.1

Community Name: ..... Confirm community name: .....

[Detect Server Information](#)

Server Name:  
NorthTower012

**Server Information:**

**Region:**  
USA  Select Region

**System Type:**  
IPedge

**Version:** 60036 **Mac Address:** 003048bec3c9

**Description:**  
Built-in server record. This record cannot be deleted.

6. Click on the **Save** icon.
- Note:** The system will re-boot.



**MODEL DATABASE PROCEDURES**

The model database can be applied during the Initial Setup. This procedure is used to manually install a model database.

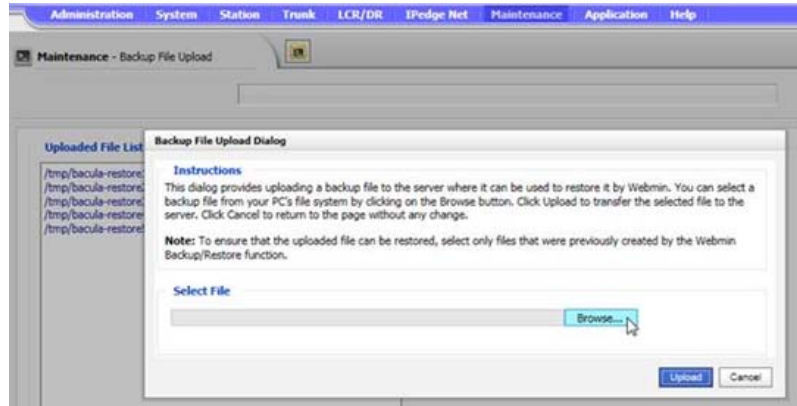
The following steps detail the model database download from the FYI website, upload to the server and restoration to the server database.

**Download Model Database**

1. Download the IPedge Model Database file from Toshiba FYI, select IPedge/VIPedge > Software. Download the correct Model Database for your server. The file name for the databases IPedgeXXModel\_MMDDYYYY.zip where the XX is EC, EM or EP.
2. Save the database to the administrator PC or other location the IPedge server can access.

**Upload the IPedge Model Database File**

1. Login to Enterprise Manager, select **Maintenance > System Maintenance > Backup File Upload**.
2. Click on the **Upload Backup File** icon.
3. In the Backup File Upload Dialog click on the **Browse...** button next the **File to upload** field. Navigate to the backup file (name of file.ZIP).



4. Highlight the backup file then, click on **Open**.
5. The file path will be shown in the Select File field. Click on the **Upload** button.
6. The file name and path will be written in to the Uploaded File List on the IPedge server.

**Note:** Please wait as it may take a few minutes to upload. The Complete screen that says “Successfully uploaded the following files...” displays.

**Restore the IPedge Model Database File**

This process restores the IPedge server.

**Note:** The licenses for the server database that you are about to restore must be applied before you restore the database.

1. Login to Enterprise Manager. Select **Maintenance > System Maintenance > Backup File Upload**.
2. Highlight then copy the backup file path name you want to restore.
3. In Enterprise Manager. Select **Application > Webmin**.

4. If this is a multi-node system select the Primary server.
5. In the Webmin screen select **IPedge > Bacula Backup System**. Click on the **Restore Backup** icon.
6. In the **Restore from Files** tab select the server to restore.
7. Paste the file name (directory name name of file.zip) into the Restore from remote directory, tar, or zip file box.
8. Click on **Restore Now**.
9. Webmin will show the message ... **Done restoring** when the restore is complete. If this is a multi-node system synchronize the database.

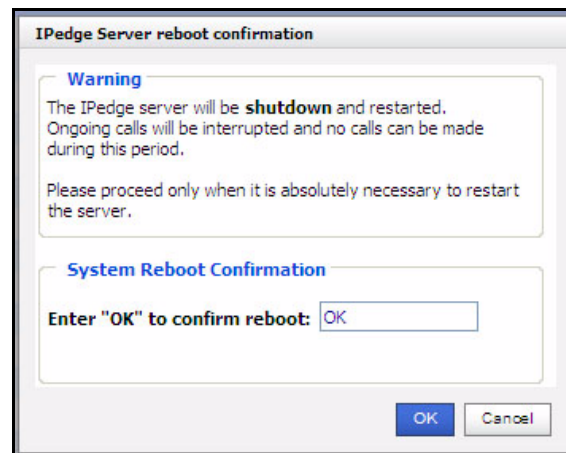
**Restart IPedge Server**

1. From Enterprise Manager, click **Maintenance > System Maintenance > System Processes**.

2. Click on the Reboot System icon



3. Enter **OK** to confirm the reboot.
4. Click on the **OK** button.

**Verify Media Server**

5. Verify that the Media Server is running. In Enterprise Manager select **Maintenance > Call Processing Status**.
6. If the Media Server is running the system has restarted correctly. Go to the next installation process. If the Media Server status is Disabled by fault go to [Step 7](#).
7. Select **Maintenance > System Maintenance > System Processes**, click on the Restart icon.
8. When the system has restarted login to Enterprise Manager then, select **Maintenance > Call Processing Status**.
9. If the Media Server is running the system has restarted correctly. Go to the next installation process. If the Media Server status is Disabled by fault contact Toshiba's Technical Support department
10. After the system has rebooted and has been running for a few minutes start the Messaging configuration.

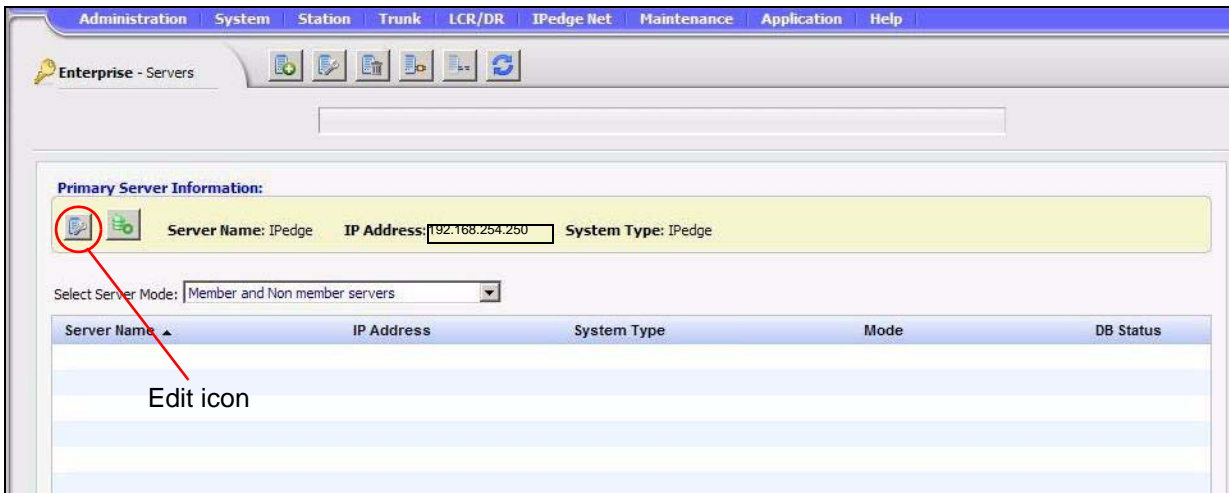
**SET SYSTEM TIME**

The time server is setup during the initial setup process. Use this procedure to change the NTP setup.

## NAME THE SERVER

The IPedge server names are setup during the initial setup process. You can use this procedure to change the name of the server. Assign a unique descriptive name to each IPedge server.

1. Login to Enterprise Manager on the server to be named.
2. Select **Administration > Enterprise > Servers**.
3. Click on the **Edit** icon.



4. Enter the new:
  - Server Name** - A unique descriptive name (same as the Host name for this server) and
  - Community Name** - (default is communityName) this name is use as authentication by some internal processes.

IP Address: 127.0.0.1

Community Name: ..... Confirm community name: .....

[Detect Server Information](#)

Server Name: NorthTower012

**Server Information:**

Region: USA  Select Region

System Type: IPedge

Version: 60036 Mac Address: 003048bec3c9

Description: Built-in server record. This record cannot be deleted.

5. Click on the **Save** icon.

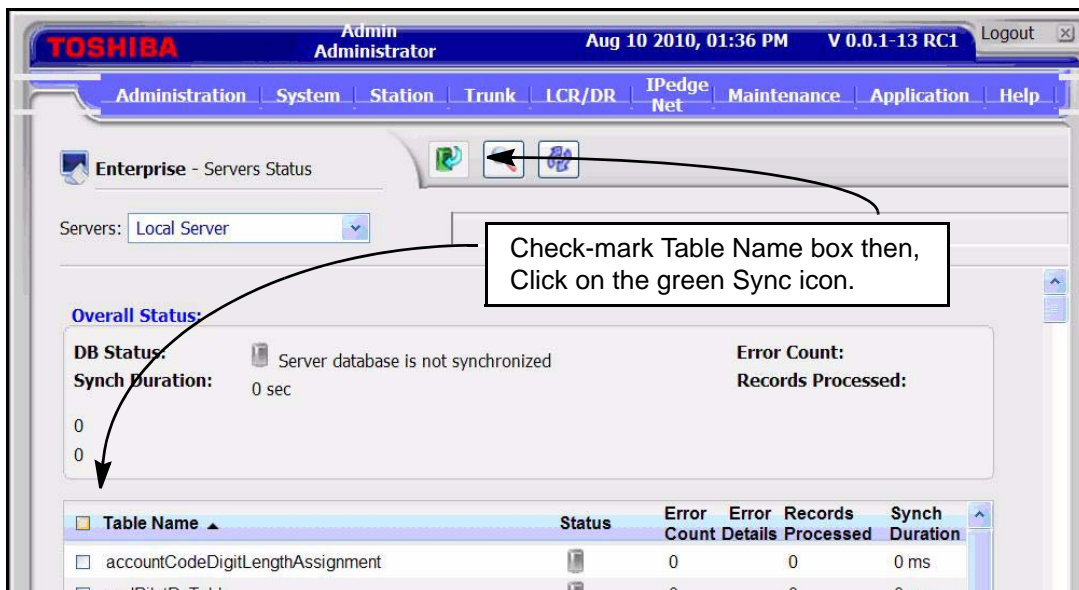
6. Click on **Detect Server Information**.
7. Go to **"DATABASE SYNCHRONIZATION"** on page 4 -38.

**DATABASE SYNCHRONIZATION**

1. Select **Administration > Enterprise > Servers**. Click on the gray database synchronization icon to open the database sync page.



2. Check-mark the **Table Name** box to select all of the tables then, click on the synchronize database icon.



3. Wait for the database synchronization to finish.

**Important!** In multi-node systems wait for the database sync to finish in one node before starting the sync in another node.

4. If you installed a Model Database go to **"HTTPS CERTIFICATE"** on Page 4-28.
5. Go to **"Database Setup"** on page 4 - 17.

**ADDING ACD to IPedge VIRTUAL SERVER**

The purpose of this document is to provide a procedure to add ACD to an existing IPedge Virtual Server. If the server is an “ACD Ready” server the ACD software is already installed but not licensed. Get the license through Toshiba’s FYI website. Apply the license using Enterprise Manager.

If this is an “IPedge only” server it does not have the Windows operating system or the ACD software. Contact Toshiba’s Technical Support department.

**Setup ACD**

1. Get the license through Toshiba’s FYI website.
2. Apply ACD license to the IPedge server as needed. Refer to the New System Install chapter.
3. In Enterprise Manager select **Maintenance > System Initial Setup**. Enter the Host name and IP address of the ACD server.
4. Select **Application > ACD Admin**. Enter the private IP address of the ACD server.
5. Select **Administration > Enterprise > Component Services**, select the **Server Application** tab. Click on the New icon to Add the ACD service.
6. Enter the FQDN of the ACD server. The private IP address can be used instead of the FQDN but this can cause administration access problems.
7. Program the ACD application. Refer to the IPedge ACD Administration manual.

This page is intentionally left blank.

# Chapter 5 – UCedge® Server Setup

---

## UCedge SERVER REQUIREMENTS

UCedge features are available on IPedge and VIPedge systems running R1.6.2 and later software.

- The IPedge server must have a static, public IP address that is directed through a router/firewall to the IPedge system.
- The IPedge server must also have a static, private IP address.
- In a federated (multi-node) system each IPedge system should have a FQDN to support UCedge, refer to the detail information below.

In a single IPedge system UCedge support requires one of two configurations.

- The IPedge server has a FQDN, The IPedge FQDN must be registered and resolve to the public IP address of the IPedge server.

— OR —

- The IPedge has only a public IP address, no domain name, no FQDN.
  - The IPedge system must have a public IP address (your router must have a public IP address and be setup for port forwarding to the IPedge system private IP address (ports listed in [Table 5-1](#)).
  - The router must be able to translate the public IP address to the private IP address (NAT).
  - The router must support 'hairpin' operation such that when an internal device accesses the IPedge public address the router loops the connection back to the private IP address.

**Note:** If ALL of the client devices are on the internal network use the private address of the IPedge in the FQDN field. Refer to page 6-6.

## UCEDGE SERVER SETUP

If the system will be using a FQDN the following applies.

### IPedge FQDN

A public domain name (such as; example.com)

- The IPedge FQDN must be registered. The IPedge system(s) must have a public IP address (your router must have a public IP address and be setup for port forwarding to the IPedge system private IP address (ports listed in [Table 5-1](#)).
- VIPedge systems already have a FQDN (for example: cp2333344.vipedge.com)

- For Strata CIX the MIPU card public IP address can have an FQDN but, it is not required.
- The router connecting the IPedge system WAN must have a static, public IP address. The FQDN resolves to that IP address. Refer to [Figure 5-1](#), [Figure 5-2](#), and [Figure 5-3](#).
- The router must have DNS capability to resolve the FQDN to the private IP address of the IPedge system. Toshiba recommends the Adtran 3120 and 3448.

**Important!** All servers (nodes) must have the same level of sub-domain. For example; If Node 1 is **a.company.com**, the other nodes can be **x.company.com** or **a.company2.com**. Do not use a.b.company.com for any of the nodes.

#### Public IP Address Only, No FQDN

If the IPedge has only a public IP address, no domain name, no FQDN. The IPedge system must have a public IP address (your router must have a public IP address and be setup for port forwarding to the IPedge system private IP address (ports listed in [Table 5-1](#)).

The router must be able to translate the public IP address to the private IP address (NAT) and the router must support 'hairpin' operation where an internal device accesses the IPedge public address and the router loops the connection back to the private IP address.

#### All IPedge Systems

- The router must be setup with port forwarding. Refer to [Table 5-1](#).
- The IPedge system(s) must have a static, private IP address behind the router.
- The UCedge client must be able to access a DNS server to resolve the IPedge or VIPedge FQDN.
 

**Note:** If ONLY Call Manager client is used, a FQDN is not required.
- The UCedge client must be able to access the IPedge server via Wireless access point(s) or a cellular data network.
 

**Note:** The user's cellular data plan charges will apply.
- The stations must be assigned a UCedge Client Account Name in the Basic tab of the Station assignment to be visible in UCedge.
- All of the IPedge systems in a network must have Net Server running for the stations in those node to be visible to all UCedge clients.
- Unifier must be running on the IPedge system for Strata CIX stations to be visible to UCedge clients.



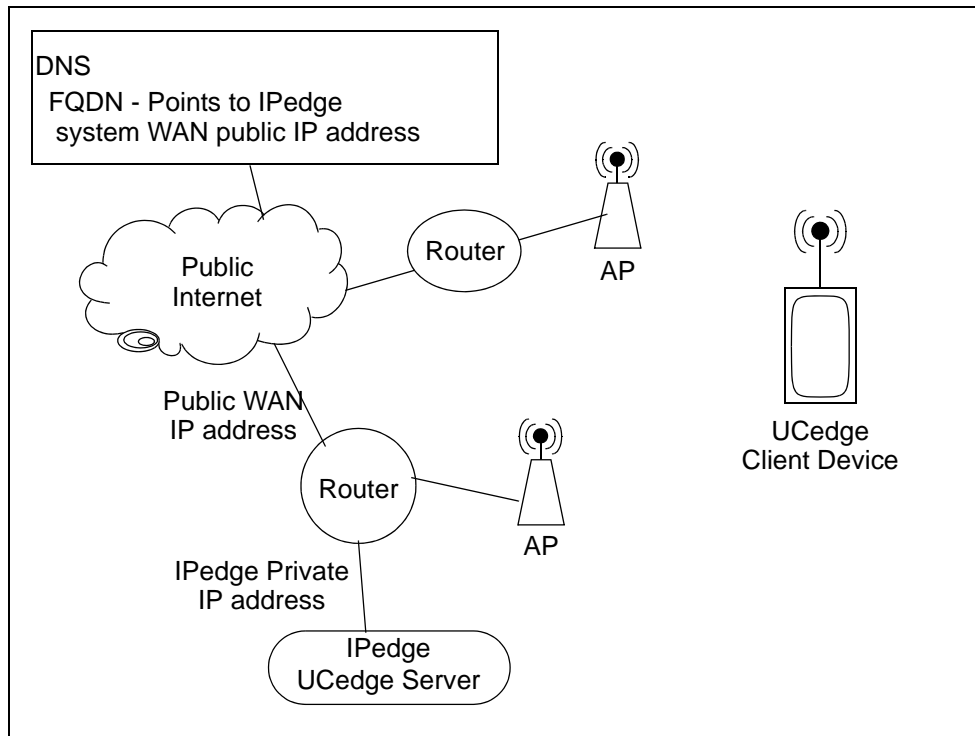


Figure 5-1 Basic IPedge System Network Diagram

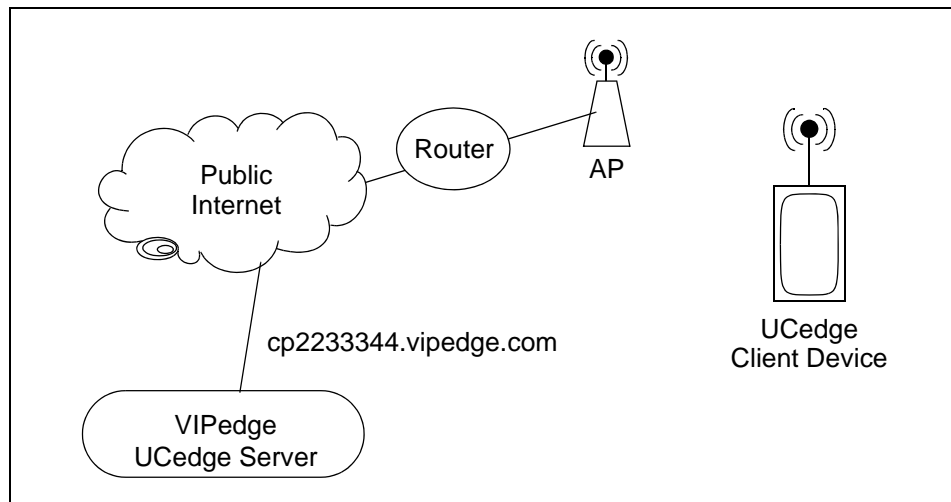


Figure 5-2 Basic VIPedge System Network Diagram

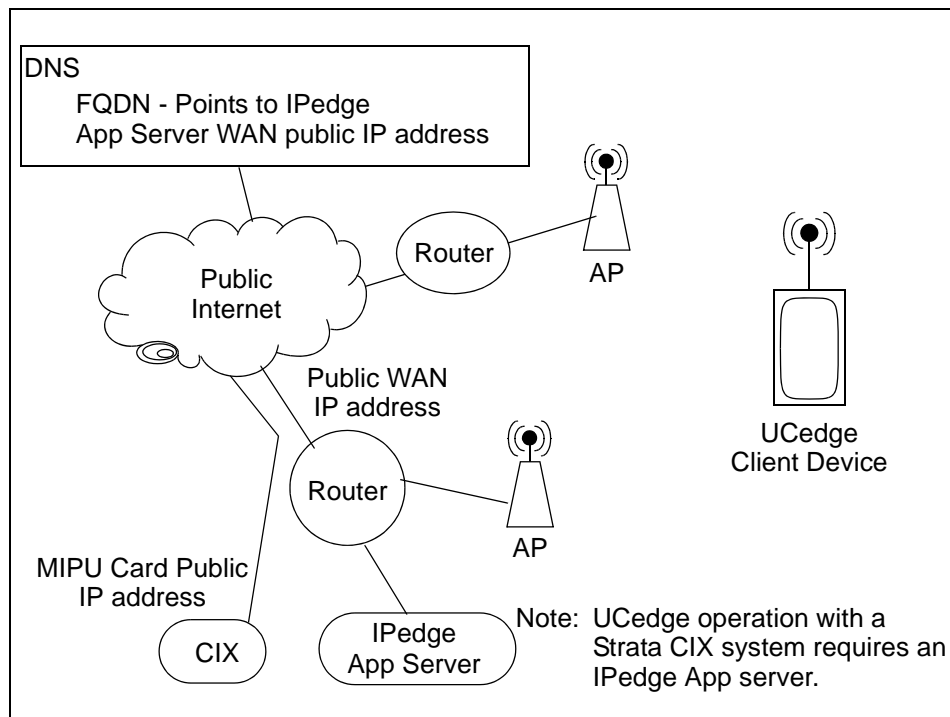
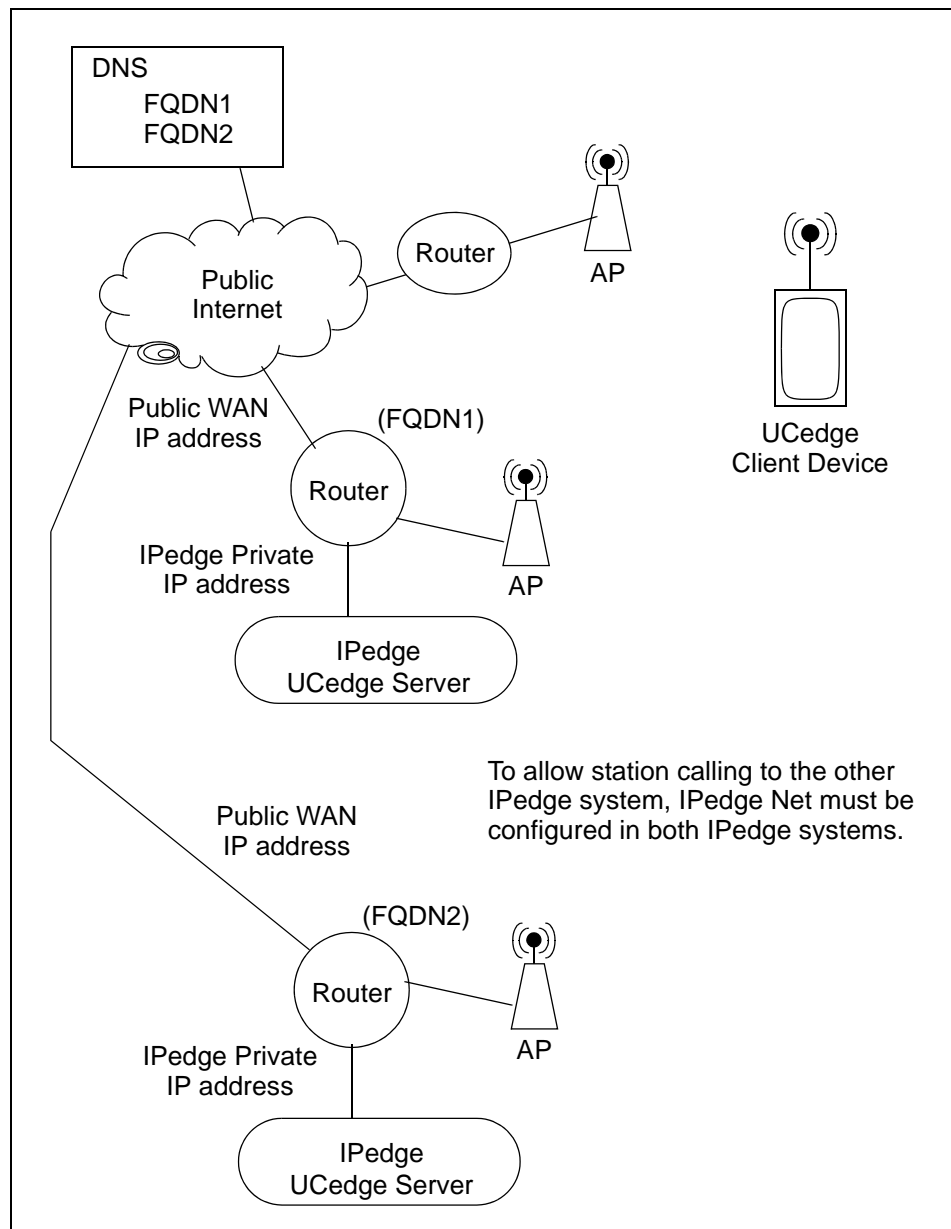


Figure 5-3 Basic Strata CIX System Network Diagram

Table 5-1 Open Router Ports to Allow UCedge Client Access

Function	Type	Use
90	TCP	IPedge Messaging Mobile App Port
1718 ~ 1719	UDP	Remote IP Telephone set registration
2944	TCP	MEGACO
5222	TCP	XMPP Client
5269	TCP	XMPP Server
5280	TCP	XMPP Client
8088	TCP	PhDN and DND features on UCedge clients
8767 and 8768	TCP	Net Server
21000 to 22999	UDP	Remote IP or SIP telephone audio
42507	TCP	Messaging access from UCedge Clients
<b>Note:</b> The ports listed above are used by the UCedge client. Some of these ports are opened while installing the IPedge system with or without UCedge.		



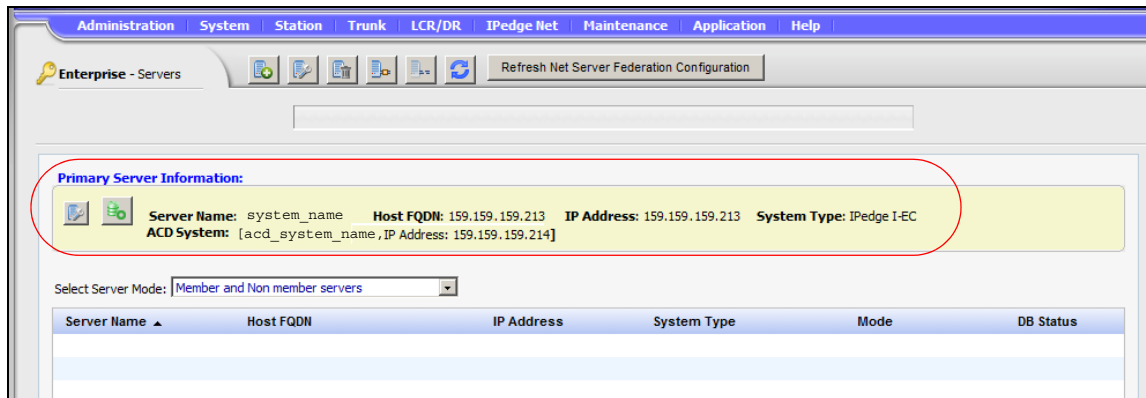
**Figure 5-4 Multi-node System Network Configuration**

The FQDN for the IPedge server must be registered with a DNS service to resolve to the public IP address of the system router, the DNS server on the system network must resolve the FQDN to the private address of the IPedge server. Refer to [Figure 5-4](#).

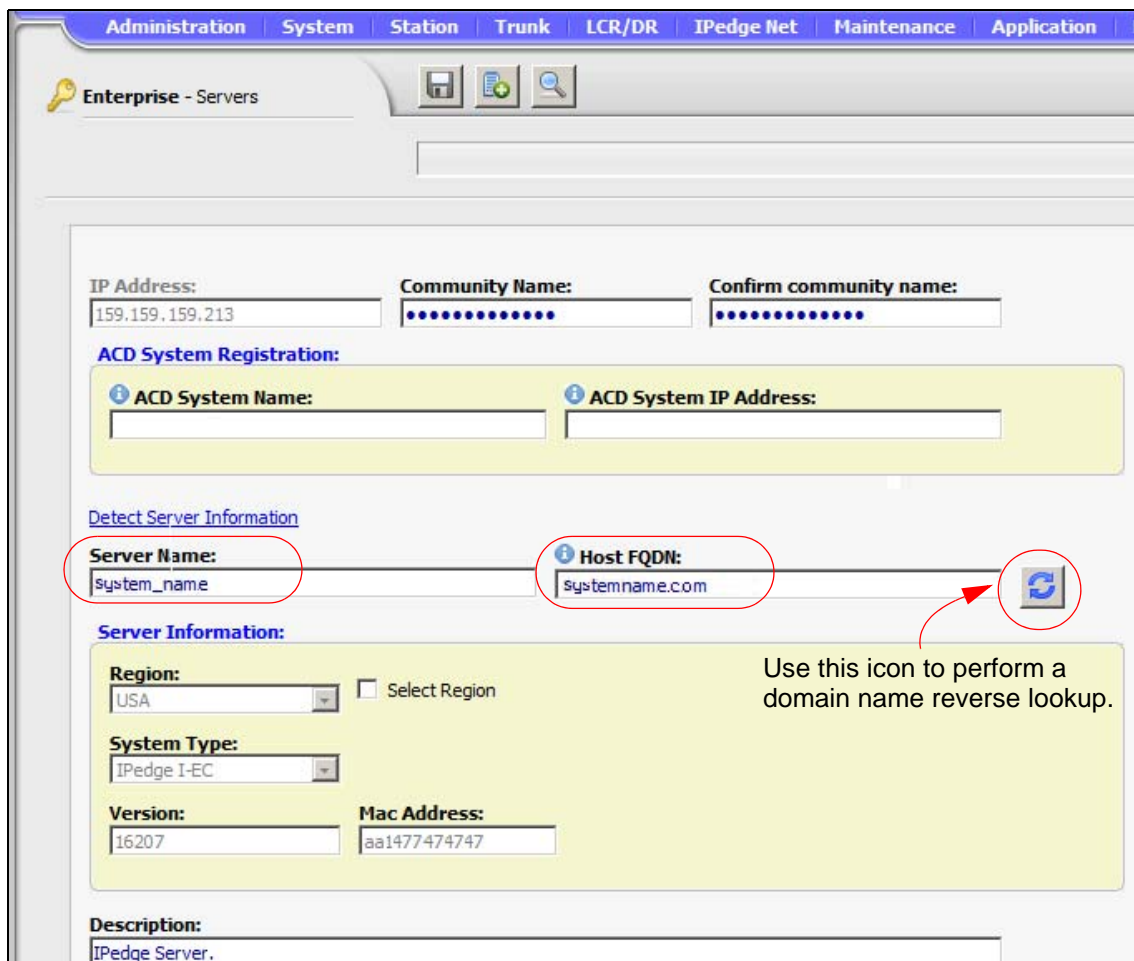
When the DNS service is setup the FQDN must be setup in Enterprise Manager.

- FQDN Setup**
1. Select **Administration > Enterprise > Servers**.
  2. Click on the **Edit** icon.

3. Enter the FQDN in the **Host FQDN** field.



4. Enter the FQDN of the IPedge system in the **Host FQDN** field.



5. When the Save icon is clicked the system will perform an FQDN lookup. If the address returned does not match the address setup during the initial system configuration an error message will be displayed. Typically there is no need to use the Reverse Lookup icon. In some configuration the IPedge server IP address may be used instead of a FQDN. Refer to [UCedge SERVER REQUIREMENTS](#) on

page 5 - 1. Some service providers disable the reverse lookup feature.

The screenshot shows the UCedge Server Setup interface. At the top, there are fields for IP Address (10.10.0.101), Community Name (masked with dots), and Confirm community name (masked with dots). Below this is the ACD System Registration section with fields for ACD System Name and ACD System IP Address. The Detect Server Information section shows Server Name (system\_name) and Host FQDN (system.com). A red box highlights the Host FQDN field with the error message "Host FQDN: Not resolvable." A red arrow points from this error message to a text box below that reads: "Could not be resolved; system.com was entered. The registered FQDN is systemname.com. This host must support XMPP protocol." The Server Information section includes a Region dropdown (USA) and a System Type dropdown (IPedge I-EC).

## EXTERNAL FEDERATION (Server White-list)

UCedge clients can subscribe to external servers to display the presence of UCedge clients in the other server and use the Instant Message feature (Chat) with those clients. Use the procedure shown in the steps below to white-list the servers in a federation.

1. Login to Enterprise Manager in one of the servers.
2. Select **Administration > Enterprise > External Servers**.
3. Click on the **Add** icon.
4. The External Server White-List Entry Properties dialog box will open.
5. In the **Server Name** field enter a friendly name for a server in the federation you wish to add to the white-list. This is the name that will appear in the Domain name pull-down list on the client device when the user selects Subscribes External Contacts.
6. In the **Host FQDN** field enter the FQDN of the other server.

The screenshot shows the "External Server White-List Entry Properties" dialog box. It has two input fields: "Server Name" with the value "headquarters" and "Host FQDN" with the value "yourco.sales.com". There are "OK" and "Cancel" buttons at the bottom right.

**Note:** Enter only the FQDN of the other IPedge or VIPedge system. The VIPedge system have FQDN is the CP address.(for example: cp2333344.vipedge.com).

7. Click on the **OK** button.
8. For IPedge systems running 1.6.2 or later software skip to [Step 13](#).
9. Select **Administration > Enterprise > External Servers**.

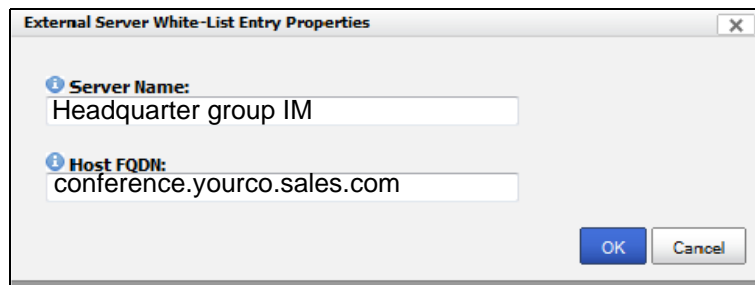
10. Click on the **Add** icon.
11. In the **Server Name** field enter a friendly name for the server added in [Step 5](#) above. In the FQDN field enter **conference.FQDN domain name**, the FQDN domain name from [Step 5](#). (For example: If the FQDN added above was Node3IPedge.com, this entry should be conference.Node3IPedge.com.)

**Note:** Although this name will appear in the Domain name pull-down list on the client device, the user should not select this when setting the External Contacts.

**Important!** The conference FQDN must be registered in the DNS service record for the Host FQDN.

The conference.yourco.com FQDN is only registered in the DNS service account. It does not need to have its own domain.

12. In the **Host FQDN** field enter the conference.FQDN of the other server.



The screenshot shows a dialog box titled "External Server White-List Entry Properties". It has two input fields: "Server Name" with the value "Headquarter group IM" and "Host FQDN" with the value "conference.yourco.sales.com". There are "OK" and "Cancel" buttons at the bottom right.

13. Click on the **OK** button.
14. Repeat Step 1 ~ [Step 13](#) for all of the external servers you wish to white-list.
15. Repeat Step 1 ~ [Step 14](#) in each IPedge server.

**CHAT SERVER SETUP**

Verify the Chat Server is setup in the Net Server application. In Enterprise Manager select **Application > Net Server**. Select the server.

1. In the Net Server administration select **Chat Server > Setup**.
2. In the Domain field enter the FQDN of the IPedge server should appear.



3. If the FQDN does not appear refer to [FQDN Setup on page 5 - 5](#).

**Important!** This screen is for display only. Do NOT change the domain from this menu. Go to the [FQDN Setup on page 5 - 5](#).

**USER ACCOUNT SETUP**

The UCedge Client setup is done on the Station Assignment page in Enterprise Manager. UC Client stations are assigned as IPT stations.

**Important!** When the UCedge client softphone is paired with an IP telephone the IPT must **not** have assigned; Multiple Line appearances, CO Line, Group CO-Line, Pooled Line key, or other features that require feature keys.

UCedge DNs must not be assigned as line appearances on IP telephones.

An IP telephone paired with a client must not have Multiple DNs.

1. In the Basic tab of the Station Assignment check-mark the Create New UC Client box. Refer to [Figure 5-5](#).
2. Select the UC Client Account Name. The client account name can be up to 16 alpha-numeric characters, with no special characters.
  - Copy From Email uses the email account name. This uses the text to the left of the '@' in the email address. (i.e.: first.last@email.com would have first.last as the user name.)
  - Copy from Display Name uses the name entered in the Name to Display field of the station assignment.
  - Use uc+DN use the station DN (i.e.: uc2345 for station DN 2345).
  - Enter my own Account name uses the name you enter into the UC Client Account Name field.

**Note:** Enter the client account name using the First.Last name format.

When the UC Client is assigned it has a default password; DN+997. The system administrator must send the following information to each UC Client user.

- UC Client account name
- The default password
- If the station is assigned to an IPedge or VIPedge system; the system domain name.
- If the station is assigned to a Strata CIX system; the public IP address or FQDN to reach the router to the MIPU card.
- The Security Code if the IP Phone Login Password parameter (in the Enterprise Manager Station Assignment) is set to Enable. Refer to [Figure 5-5](#).

The user can install the UC Client application on a phone or tablet and setup the device as described in the User Guide.

The user can change the account password through the device profile setting.



**Name to Display**

Use only letters, digits, period (.) or, dash (-) in the station name. Using other characters in the Name to Display field will cause an unrecoverable database synchronization failure.

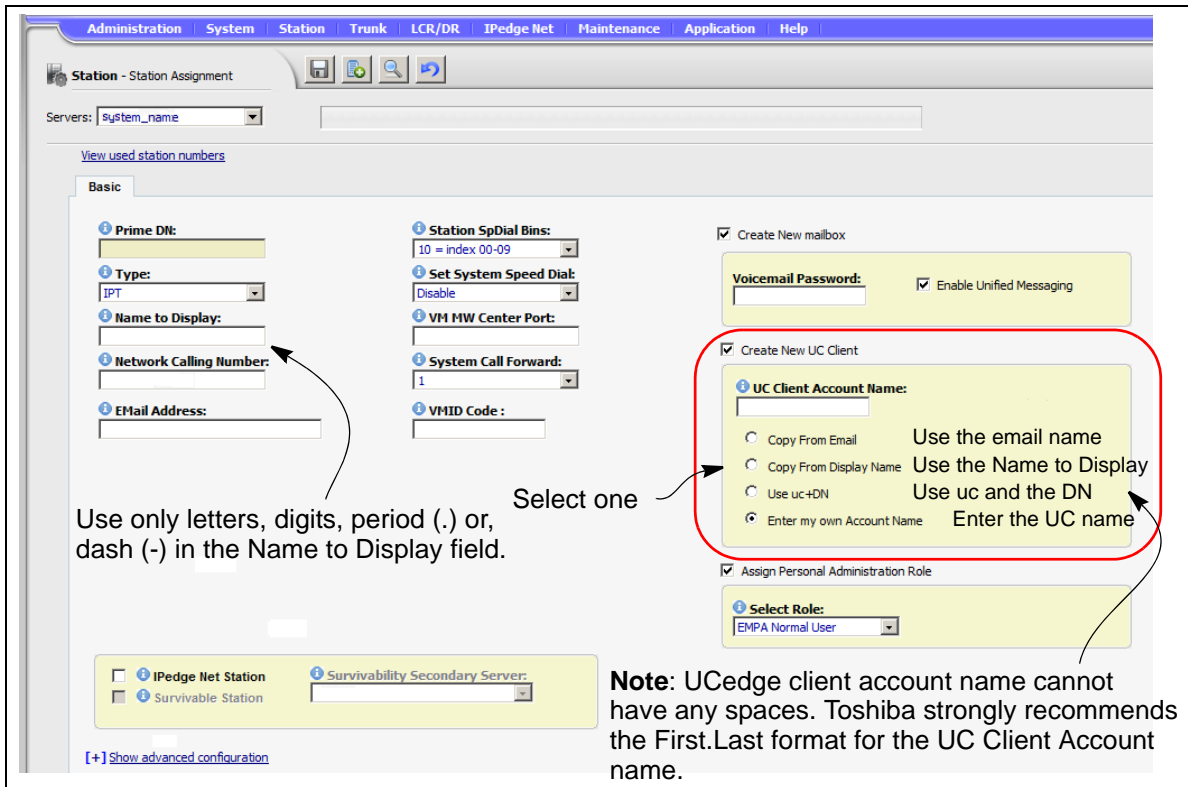


Figure 5-5 UCedge Client Station Assignment

**PHONE ONLY USER ACCOUNT**

A Phone Only account is a station, programmed as a UCedge client, that does not have a client device. The DN, an IPT station, will appear in the UCedge Users list. When a UCedge client subscribes, the phone only user’s presence and availability will be displayed.

The Phone Only user account is programmed using the same procedure as all other UCedge accounts.

**CREATE A RANGE OF STATIONS**

In R1.6.2 and later system software Create New UCedge client is the default action when creating new stations. When a station is created as part of a range it is assigned as a UCedge client. The UCedge account number will be set to uc+DN.

**UPDATING AN EXISTING SYSTEM**

UCedge requires a client password. UCedge does not support spaces or special characters in the user name.

- Spaces in the user name will be changed to a period (.)
- All users with a blank password, no password, will have the default DN+997 password set.

This page is intentionally left blank.

# Chapter 6 – IPedge System Backup

---

## BACULA

To backup the complete IPedge system database three backup and restore procedures are required.

- The IPedge database procedures are covered in this chapter.
- For Messaging backup procedures refer to [“MESSAGING BACKUP”](#) on [page 13 - 10](#).
- For systems with ACD refer to [“ACD BACKUP”](#) on [page 6 - 8](#) for the backup and restore procedures.

**Note:** Enterprise Manager runs correctly with Internet Explorer. Some procedures described in this chapter will not function when another browser is used.

The IPedge system backup process is controlled by Bacula, a Client/Server based backup program. Bacula is a set of programs that manage the backup, recovery, and verification of the IPedge configuration database for a stand alone system or every node on an enterprise network. Bacula runs entirely upon the primary node server. The Bacula application on the Primary node directs all backup processes except Messaging. For the Messaging and Call Accounting backup procedures refer to [“MESSAGING BACKUP”](#) on [page 13 - 10](#).

Bacula is accessed through Enterprise Manager, select **Application > Webmin**. On the Webmin screen select **IPedge > Backup and Restore**. The Bacula Backup System home screen will open.

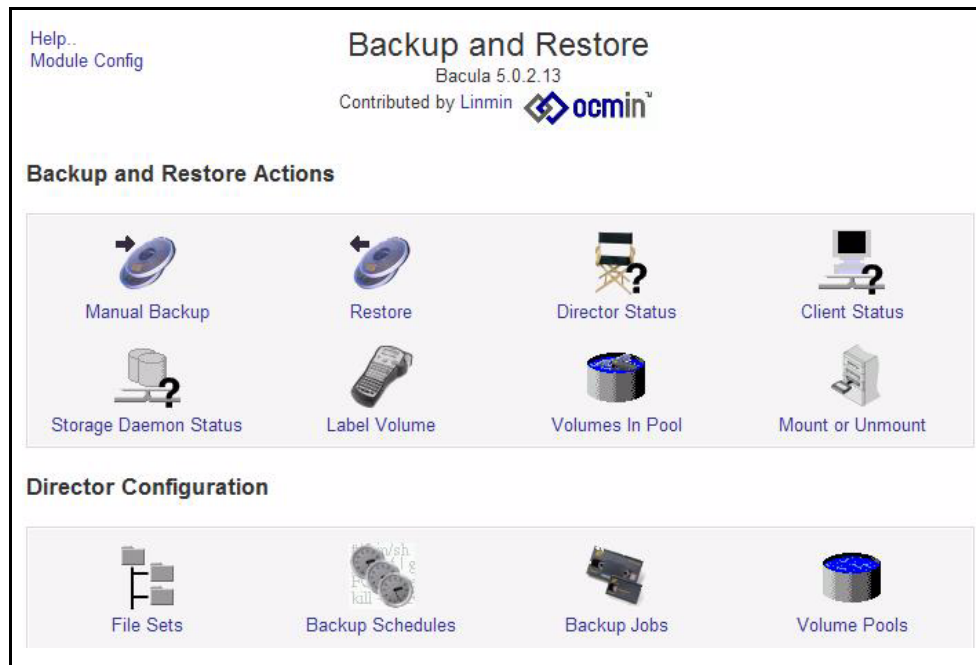


Figure 6-1 Bacula Main Page

**BACKUP FILE LOCATION**

The IPedge system backup files are saved on the system hard disk drive (HDD). Backup files should be saved to a external file server on a regular schedule.

**BACKUP SCHEDULE**

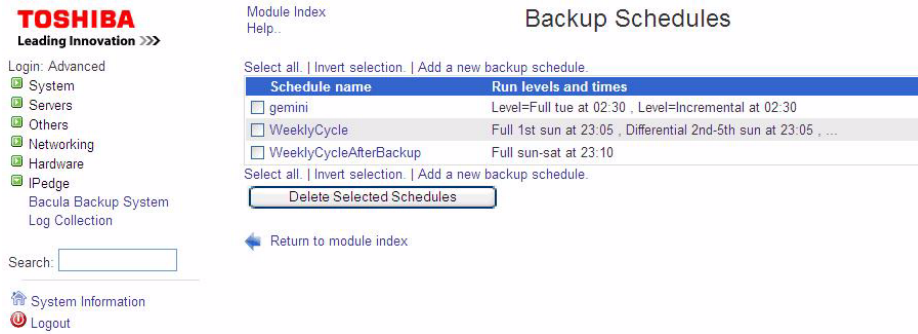
When a system is installed the backup volume, which is the location of the backup files are defined in the default configuration. By default, the backup is run at 3:30 AM (0330 hours) local time. A full backup is performed every Tuesday. An incremental backup is run Wednesday through Monday.

**Change Backup Schedule**

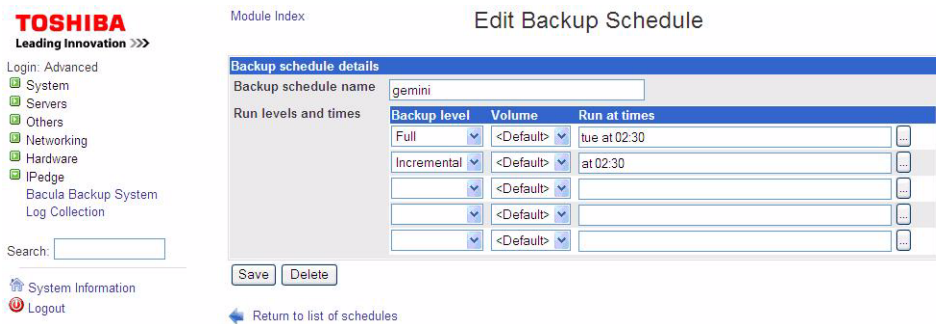
Use the following procedure to change the IPedge backup schedule.

1. Navigate the to the Bacula main screen (Application > Webmin, click on Backup and Restore).
2. Click on the Backup Schedules icon.

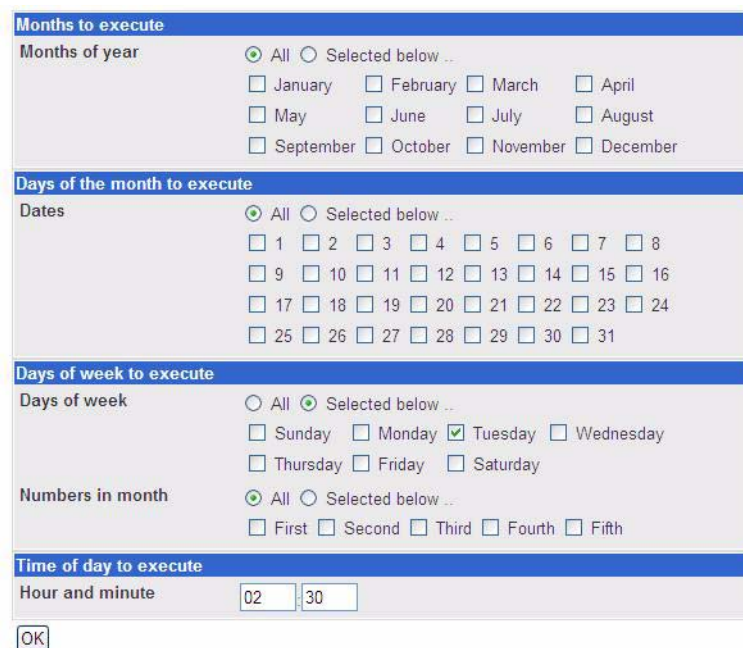
- Click on the gemini backup schedule. Do not check mark the box. Click on the word 'gemini.'



- The Edit Backup Schedule screen will open.



- Click on the ellipses button at the end of the line you wish to change.
- The schedule detail window will open. The window below shows a schedule to run every month, on each Tuesday at 2:30 a.m.

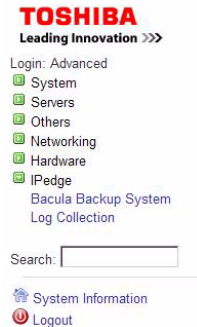


7. Select the schedule you want then, click on the **OK** button.

### Create a New Backup Schedule

Use the following procedure to create a new the IPedge backup schedule.

1. Navigate the Bacula main screen.
2. Click on the Backup Schedules icon.
3. Click on the text; Add a new backup schedule.
4. The Create Backup Schedule screen will open.



Module Index      Create Backup Schedule

**Backup schedule details**

Backup schedule name

Run levels and times	Backup level	Volume	Run at times
	<input type="text" value="&lt;Default&gt;"/>	<input type="text" value="&lt;Default&gt;"/>	<input type="text"/>
	<input type="text" value="&lt;Default&gt;"/>	<input type="text" value="&lt;Default&gt;"/>	<input type="text"/>
	<input type="text" value="&lt;Default&gt;"/>	<input type="text" value="&lt;Default&gt;"/>	<input type="text"/>

[Return to list of schedules](#)

5. Enter a name for the schedule.
6. Select a Backup level.  
Full: Full database backup.  
Differential: Backup all changes since the last full backup.  
Incremental: backup all changes since the previous backup.
7. Select a Volume.
8. Click on the ellipses button at the end of the line to set the schedule.
9. Select the schedule you want then, click on the **Create** button.

### Verify Backup Job Status

1. Navigate the Bacula main screen.
2. Click on the Director Status icon.

### RESTORE FROM BACKUP

Check the following conditions to check before starting the restore procedure.

- **LICENSES** - Apply the licenses for the database you are about to restore before starting the restore.
- **SERVER SIZE** - It is possible to restore an EC-server database to an EM-server. An attempt to restore an EM-server data base to an EC-server will not function correctly.
- **MEMBER / PRIMARY SERVERS** - Restore each database type to a like type server. Restore a Primary database to a Primary server. Attempting to restore a Member server database to a Primary server will fail.

Use this procedure to restore a system from the backup files.

1. Login to Enterprise Manager.
2. Apply the licenses.
3. Sync the databases.
4. Select Webmin.
5. In the Webmin screen select **IPedge > Backup and Restore > Restore**.
6. Select the Restore from Backup tab. In the Options for the source area use the drop-down list in the Restore from Job field select the specific job you wish to restore.
7. In the Options for the Target select the IPedge server to restore.
8. Click on the **Restore** button.

9. Bacula will display an output file that shows the status of the Restore.
10. When the restore is complete reboot the IPedge system.

## MANUAL BACKUP

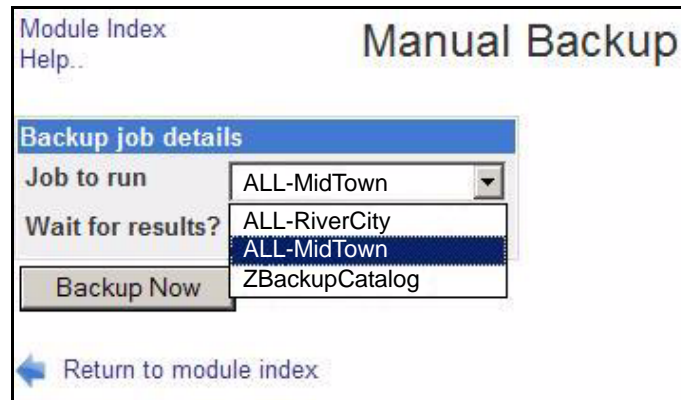
A backup can be run manually any time. Running a manual backup does not effect the automatic backup schedule. Toshiba recommends that you run a backup before making a critical change. The resulting manual backup file can be downloaded to the PC the system administrator is using (Enterprise Manager PC).

### Manual Backup Procedure

This creates a backup as a file in the backup section on the IPedge server.

1. Login to Enterprise Manager. Select **Application > Webmin**.
2. If this is a multi-node system select the Primary server.
3. In the Webmin screen select **IPedge > Bacula Backup System**. Click on the **Run Backup Job** icon.

- In the Job to run pull-down select; All-Server Name. Where ServerName is the server you wish to backup.



- Ensure that **Wait for results** is set to **Yes**. Click on **Backup Now**.
- Wait for the backup to finish. When finished the system will display "... backup complete."

### Create the Download File

This process creates a version of the backup file on the IPedge server that can be downloaded to another location.

- Login to Enterprise Manager. Select **Application > Webmin**.
- If this is a multi-node system select the Primary server.
- In the Webmin screen select **IPedge > Bacula Backup System**. Click on the **Restore Backup** icon.
- In the Restore from Backup tab, select the backup file to restore in the Restore from Job pull-down. The latest file is always shown at the top of the list.
- Click to select **Restore to local (primary server name) directory**.
- Enter a directory name. Use the format: **/NameOfFile**. This will save the backup file in a folder named NameOfFile in the server root directory. The backup file will be zipped. An example of file name is server name and software (TGZ) level. On a version 1.6.1-16 system the file name could be /ALL-MidTown16116.
- Click on the **Restore Now** button.
- Wait for the system to display "... backup complete."
- To download the backup file now click on the **Download** button.
- In the file Download dialog box click on the **Save** button.
- In the Save As screen navigate to the location in which you will save the backup file.

### Download Backup File

This process copies the backup file on the IPedge server to any location the Enterprise Manager PC can access.

- Login to Enterprise Manager. Select **Application > Webmin**.
- If this is a multi-node system select the Primary server.



3. In the Webmin screen select **Others**. Click on **Upload and Download**.
4. In the Download from Server tab click on the ellipsis next the **File download** field.
5. Select the folder name created above (format: **/NameOfFile**). Do not open the folder. Click on **Ok** then, click on the **Download** button.
6. In the dialog box select **Save**. The backup will be a .zip file. The file can be stored in any location the PC can access. The backup file will be copied to the selected location on the Enterprise Manager PC. Do not unzip the file.

## MANUAL RESTORE

The following procedure covers how to upload the manual backup file and restore it to the server. The restore file will be uploaded to the server from which it was saved. During the restore process the file must be restored to the appropriate server.

**Note:** If a member node is detached and then, the database restored, some features may not restore completely. To help ensure a complete restore, attach the member node before restoring the database.

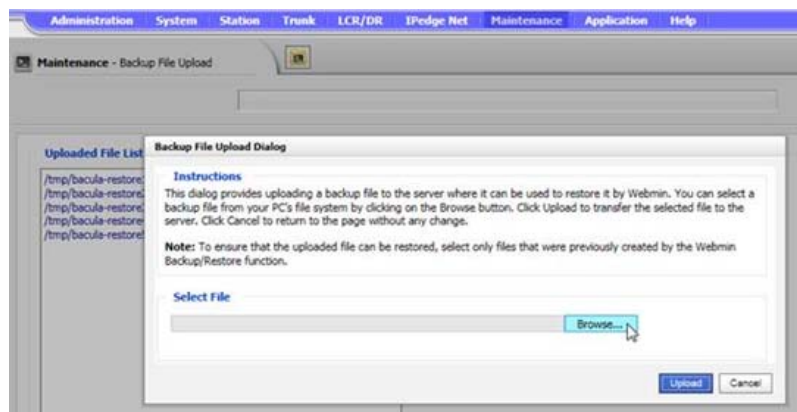
## UPLOAD BACKUP FILE

The restore file can be stored on an IPedge server, the Enterprise Manager PC or any other location. Access to the Backup File Upload is controlled by the User's role.

### Upload from Administrator PC

This process copies the backup file from your storage location to a directory on the IPedge server.

1. Login to Enterprise Manager. Select **Maintenance > System Maintenance > Backup File Upload**.
2. Click on the **Upload Backup File** icon.
3. In the Backup File Upload Dialog click on the **Browse...** button next the **File to upload** field. Navigate to the backup file (name of file.ZIP).



4. Highlight the backup file then, click on **Open**.

5. The file path will be shown in the Select File field. Click on the **Upload** button.
6. The file name and path will be written in to the Uploaded File List on the IPedge server.

**RESTORE THE SERVER**

This process restores the IPedge server.

**Note:** The licenses for the server database that you are about to restore must be applied before you restore the database.

1. Login to Enterprise Manager. Select **Maintenance > System Maintenance > Backup File Upload**.
2. Highlight then copy the backup file path name you want to restore.
3. In Enterprise Manager. Select **Application > Webmin**.
4. If this is a multi-node system select the Primary server.
5. In the Webmin screen select **IPedge > Bacula Backup System**. Click on the **Restore Backup** icon.
6. In the **Restore from Files** tab select the server to restore.
7. Paste the file name (directory name name of file.zip) into the Restore from remote directory, tar, or zip file box.
8. Click on **Restore Now**.
9. Webmin will show the message ... **Done restoring** when the restore is complete. If this is a multi-node system synchronize the database.

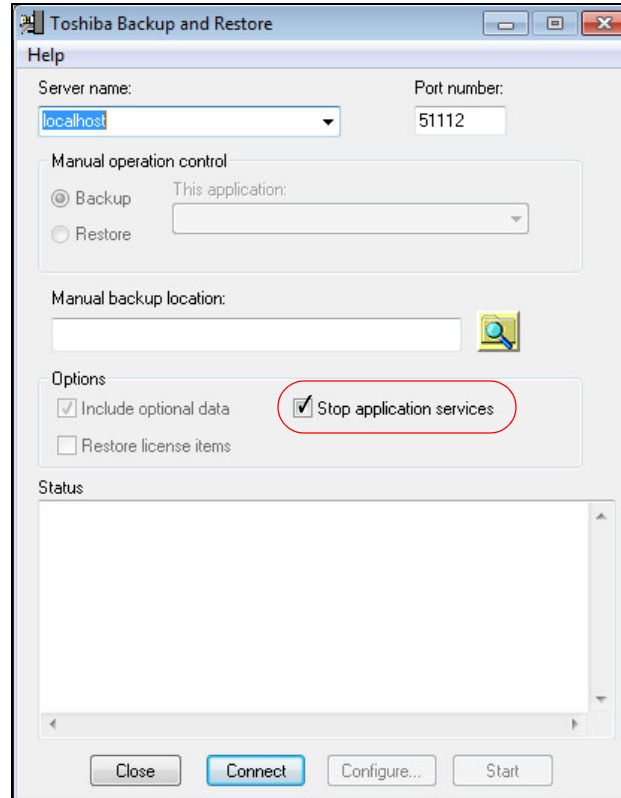
**ACD BACKUP**

The ACD service must be stopped while the backup is running.

**Important!** Schedule the ACD backup during low traffic hours.

1. Use Windows remote desktop or other utility to open a Windows console on the ACD server. The Windows User Name is **Valued**

**Customer**, the password is **toshiba**. Launch the Toshiba Backup And Restore program.



2. Enter or browse to the backup file location.
3. Ensure that the **Stop application services** box is check-marked.
4. Click on **Start**.

**Note:** The ACD service will restart when the backup is complete.

This page is intentionally left blank.

# Chapter 7 – HTTPS Configuration

---

In HTTPS mode all communication between the Administrator's browser and Enterprise Manager is carried over secure tunnel using SSL.

- To setup HTTPS configuration in enterprise systems with more than one IPedge server the Primary Server must be configured first.
- The certificate can be transferred from the primary to the member nodes if a wildcard certificate is used.
- All of the servers in a network must be operating in HTTPS, otherwise some features will fail.
- The IPedge server host names and server names must be configured and registered with a DNS server.

**Important!** When an IPedge server with HTTPS set is installed behind a firewall the following ports must be open:

- 443 - for all systems
- 8444 - for meeting, both HTTP and HTTPS
- 9443 - for Enterprise Manager
- 10000 for Webmin

## INTRODUCTION

IPedge system software release 1.7.4 and later support SSL Certificates from a Certificate Authority (CA). The R1.7.4 and later IPedge systems do not support Self Certification.

Supported Certificate Authorities include:

- GoDaddy®
- Verisign®
- Thawte®
- Comodo®

**Important!** You must have an account with one of the listed Certificate Authorities before starting this process.

The Enterprise Manager (EM) HTTPS page supports the certificate from a CA and notifies the other IPedge system components when a new or updated certificate is available. The CA Certificate tab in the Enterprise Manager HTTPS page is used to manage the CA certificate; loading the private key, the certificate, the chain certificate (if there is one), and the optional CSR file. The certificate must be PEM format. If requested, select a certificate for Apache Tomcat (not Tomcat).

### HTTPS SETUP

All of the HTTPS setup in the following procedure is done on the Primary server. In a multi-node system the CA Certificate can be transferred to the member nodes.

**Important!** For multi-node systems ensure that a **wildcard** certificate is specified.

If using the wildcard certificate go to [“Wildcard Certificate” on page Chapter 7 –3.](#)

1. In Enterprise Manager (EM) select **Maintenance > HTTPS Configuration.**
2. In the **HTTPS Configuration** tab the HTTPS button is selected.
3. Click on the Generate and Download CSR icon.
4. In the pop-up screen complete the form fields.  
**Note:** Enter the IPedge system FQDN in the Common Name field.
5. Click on **OK.**
6. Enterprise Manager will create the Certificate Signing Request (CSR) file.
7. Send the CSR file to your certificate authority. Wait for the CA to return the certification files.
8. When the Certificate file and the Chain file are received save the files to the administrator PC.
9. In the HTTPS configuration page select the **CA Certificate** tab.
10. Check-mark the Use existing server generated private key.
11. Choose the Key file and Certificate file (sent by your CA).  
**Note:** If you used a third party CSR un-check the ‘Use existing file’ box. In addition to the Key and Certificate files there will be a Chain file to choose.
12. Click on the **Save** icon.
13. In the confirmation screen click on **OK.**
14. Wait for the prompt to select the HTTPS tab and select HTTPS On.
15. The server will restart. Wait until Enterprise Manager allows you to login.
16. For multi-node systems use the Transfer CA Certificate icon to send the certificate to each member node.

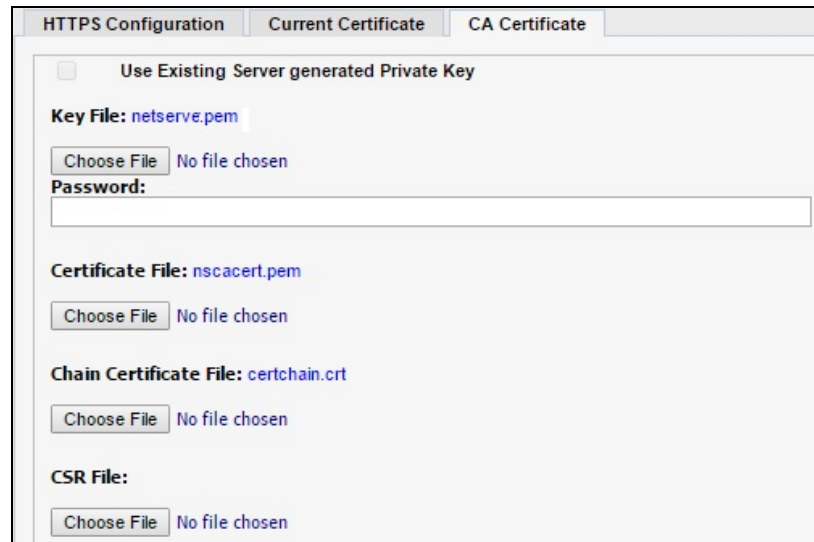
This option allows the administrator to use the certificate in the primary node on a member nodes and/or a Windows ACD server as long as the certificate is a wildcard certificate that covers the member/Windows ACD FQDN.

**Wildcard Certificate**

The wildcard (\*.domain.com) contains three files:

- Key file
- Certificate (for the IPedge server)
- Chain Certificate (for client applications)

1. Un-check the Use existing server certificate (\*.pem) box.
2. Browse to the location of the key file located. This is one of the files sent by your certificate authority (provide the password if needed).
3. Browse to the location of the Certificate file is located (\*.pem) .
4. Browse to the location of the Certificate is located (\*.cert).



The screenshot shows the 'Current Certificate' tab of the 'HTTPS Configuration' dialog. It features a checkbox for 'Use Existing Server generated Private Key' which is unchecked. Below this, there are four sections for file selection, each with a 'Choose File' button and the text 'No file chosen':

- Key File:** netserve.pem
- Certificate File:** nscacert.pem
- Chain Certificate File:** certchain.crt
- CSR File:**

A 'Password:' field is also present below the Key File section.

This page is intentionally left blank.



# Chapter 8 – IPT Software Update

---

## INTRODUCTION

Toshiba IPT5000-series telephones can connect to *IPedge* servers. For the telephones to fully function with the *IPedge* features the telephone software must be updated to the latest version.

The following procedure details the steps to update your existing IPT5000-series telephone software for connection to an *IPedge* server.

### IP Telephone Hardware

The IP Telephone software automatically detects the telephone hardware type. The IP telephone software is common to all IP

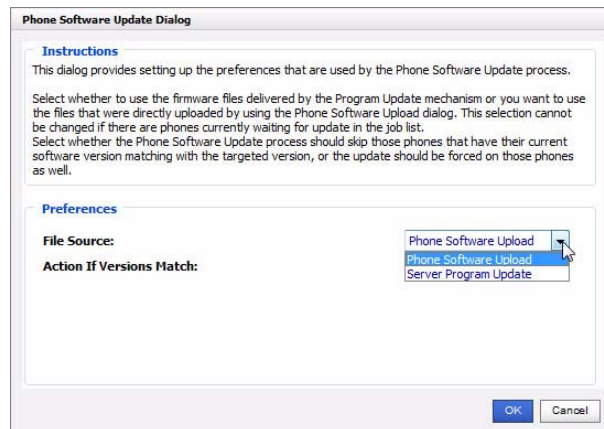
5000, IP5500, and IP5600 series telephones. When the version name is displayed the hardware type is shown.

- IP5000 series telephones are 5Kx-xxxx
- IP5500 and IP5600 series telephones are 5Lx-xxxx

## INSTALLATION

The installation steps for each server, in summary, are:

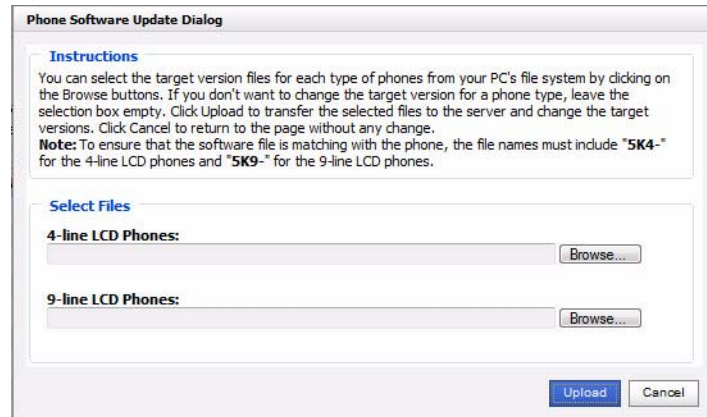
1. Login the Enterprise Manager.
2. Select **Maintenance > Phone Software Update**.
3. Click on the Phone Software Preference icon.
4. Select the File Source, and Action If (phone software) Versions Match then, click on **OK**.



5. If Phone Software Upload was selected click on the Upload Phone Software icon.  
If Server Program Update was selected the update process will use the phone software version included in the last server update file stored in the *IPedge* server.

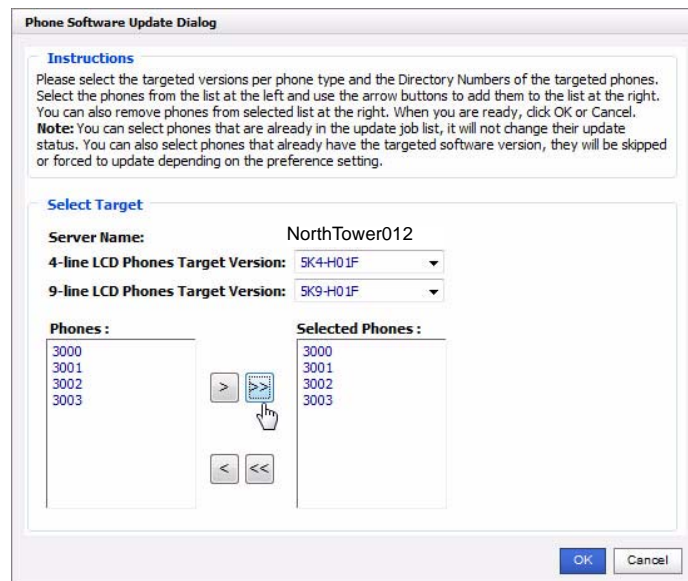
**Note:** The latest software version will always be available on the [Toshiba FYI website](#).

6. Select the 4-line LCD and 9-line LCD software file locations. Use the Browse button to navigate to the files. Then, click on **Upload**.



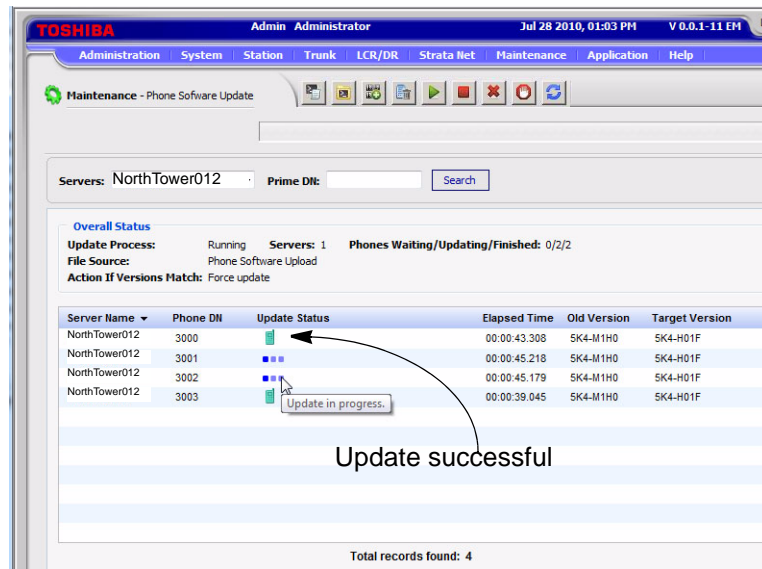
**Note:** If a USB drive plugged into the IPedge server was used to load the update software remove the USB device as soon as the upload is complete. If the USB device is left in the server cannot reboot.

7. Select an IPedge server to update. Click on the Phones to Update icon to select the IP Phones to update on that server. Click on **OK**.

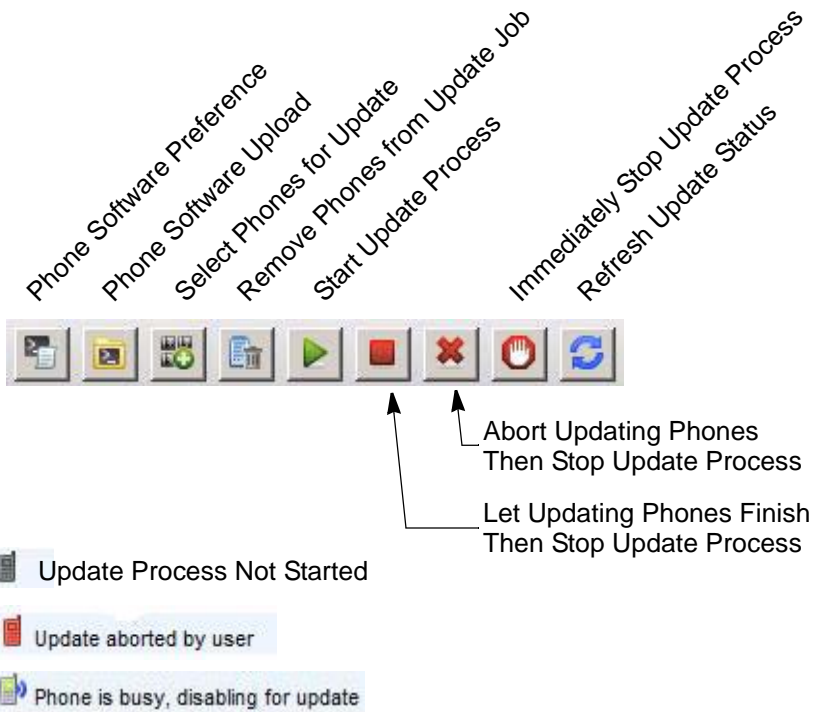


8. You can continue to select servers and IP telephones in those servers.
9. When all of the phones you wish to update have been selected click on the Start Update Process icon.

10. The screen will show the update process status.



The indicators and control icons for the IP Phone software update process are shown below.



This page is intentionally left blank.

# Chapter 9 – MRS, NAT Traversal, Ports, Firewall Setup

## INTRODUCTION

This chapter contains information and setup procedures for the IPedge Media Relay Server, Remote IPTs, SIP NAT Traversal, Firewall Port setup, and Firewall setup.

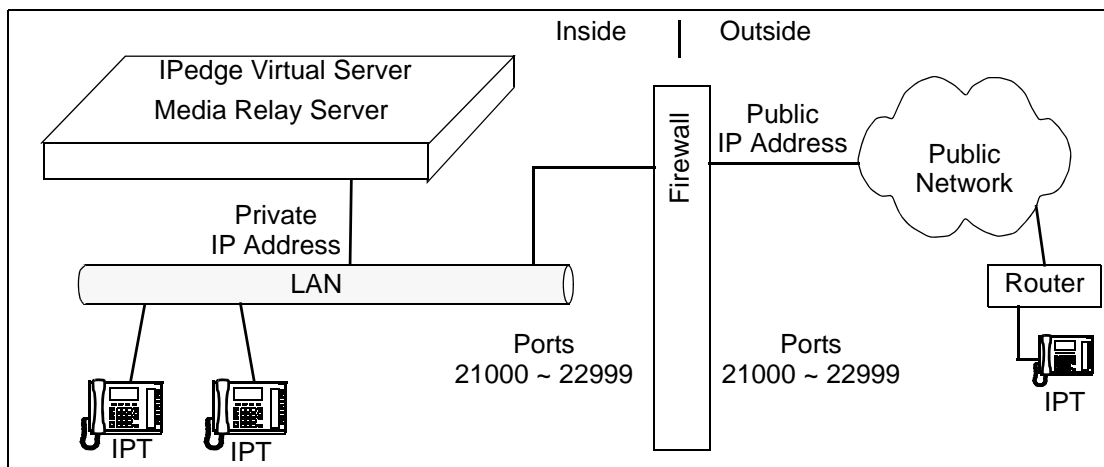
## MEDIA RELAY SERVER OVERVIEW

The IPedge system Media Relay Server (MRS) alters VoIP packets so that remote IPT devices will be instructed to send their RTP (audio) stream to the IPedge system public IP address instead of the unreachable IPedge system private IP address. This can solve one way audio conditions. Without the use of the MRS, the remote IPT will not know the public IP address to which to send its audio stream. Similarly the MRS is also affects SIP Trunk RTP packet routing. However, in a NAT environment use the NAT Traversal capability of the IPedge server (Release 1.3 and later) or a SIP ALG router along with the IPedge MRS.

The MRS is configured by defining the Public IP address of the IPedge server and the port range to be used for calls. Each call requires two UDP ports for the audio streams (one port RTP, one port RTCP).

## MEDIA RELAY SERVER SETUP

Enter the Public IP address of the IPedge server. Enter the port range to be used for calls. Each call requires two UDP ports for the audio streams (one port out bound, one port inbound).



### IPedge Configuration

1. Select **System > Media Relay Server**

Click on the **New** icon

Router Integration = Enable

Media Relay Server Service IDs = 1

Router IP Address = the Public IP Address of the Firewall

2. Click on **OK**
  
3. Select the Port Forwarding Configuration
  - Router Public Port Range Low = Lowest port number
  - Router Public Port Range High = Highest port number
  - Media Relay Server Service ID = 1
  - Media Relay Server Private Port Range Low = Lowest port number
  - Media Relay Server Private Port Range High = Highest port number

**Note:** Typically; the Router Public Port Range values and the Media Relay Server Private Port Range values are the same. The range is within 21000 ~ 22999. For additional information refer to [“IPedge PORTS”](#) on [Page 9 - 5](#).

4. Click on **OK**.
5. Select **Maintenance > System Maintenance > System Processes**.
6. Click to check-mark **Media Relay Server**.
7. Click on the **Send restart action** (double arrow) icon.
8. A dialog box warning that you are about restart the selected service will appear. Click on **OK**.
9. Click to check-mark **Call Processing**.
10. Click on the **Send restart action** icon.
11. A dialog box warning that you are about restart system will appear. Click on **OK**.
12. In the Send Command Parameters dialog box select **Normal start**.

**Important!** The next step will restart the system call processing. All calls will be dropped.

13. Click on **OK**.
14. Wait for the processes to restart.

### **IPT Configuration**

When the "IPT Data Auto Connection to MRS" is set to "Auto," the IPedge system will determine whether the IPT is placed inside NAT or not, and generate appropriate SDP.

If the IPedge system is unable to determine (for example you hear one-way audio) set "IPT Data Auto Connection to MRS" to "Manual." This will ensure that the MRS is used for the IPT connections.

To set the IPT Data Connection to use the Media Relay Server use these steps.

1. In Enterprise Manager select **Station > Station Assignment**.
2. Click to select the DN of the IPT. Select the **IPT** tab.
3. In the **Connection to Media Relay Server** field select **Manual**.
4. Click on the **Save** icon.

**SIP TRUNK NAT TRAVERSAL**

In order to support SIP Trunking on R1.2 and earlier IPedge systems in a NAT environment, the router needs to support an enterprise grade SIP ALG (Application Layer Gateway). In Release 1.3 and later, the IPedge system can support SIP Trunking with routers that do not have a SIP ALG.

When used behind a NAT firewall that does not support a SIP ALG, the IPedge server can still be given a private IP address. The SIP Trunk NAT Traversal capability (Release 1.3 and later) along with the MRS will allow the IPedge server to:

- Use its internal Media Relay Server to route media packets between the WAN and the LAN and
- Apply the correct IP address to SIP signaling messages so that when they are sent out through a NAT firewall, the SIP trunk service provider will be able to send responses to the correct IP address.

Within the NAT router, port forwarding rules will need to be configured, and a range of ports opened for the Media Relay Server.

When used with a NAT firewall that does support an enterprise grade SIP ALG (such as the Cisco ASA5500 product line) the SIP ALG feature needs to be enabled. In this configuration the media packets will be routed directly from the LAN to the WAN and mid-call survivability of a PSTN call is possible.

**SIP Trunk RTP Routing**

For traversal of NAT firewalls without using a SIP ALG, the MRS is enabled and is set to manual, the RTP stream will flow through the IPedge rather than peer to peer. The MRS also changes the IP address and port in the Session Description Protocol (SDP). SDP connection information controls where the RTP stream is sent.

When using a NAT router with the IPedge server's NAT Traversal function disabled (the IPedge Public IP Address and Port for NAT field left blank), the private IP address in the SIP header is not changed. In this configuration a SIP ALG router will be required to change the private IP address to public IP address in fields in the SIP header (such as the contact field). In IPedge systems running R1.3 and later the SIP Trunk NAT Traversal feature can be used instead of the SIP ALG function in a router/firewall.

**Note:** Turning off SIP ALG in the router/firewall is recommended when using the NAT traversal feature.


To set the SIP Trunk Connection to use the Media Relay Server with NAT Traversal capability use these steps.

1. In Enterprise Manager select **Trunk > SIP Trunking**.
2. Click to select the Service Definition tab.
3. Select the **Service Definition** number of the SIP Trunk.

4. Click on **Show advanced configuration**.
5. In the **Connection to Media Relay Server** field select **Manual**.
6. For the **IPedge Public IP Address and Port for NAT** field, enter the public IP address of the WAN interface for the router.
7. Click on the **Save** icon.

[\[-\] Show basic configuration](#)

<p><b>Primary Voice Packet Configuration:</b> 1</p> <p><b>Secondary Voice Packet Configuration:</b> 3</p> <p><b>Registration Period:</b> 3600</p> <p><b>Timer B:</b> 5</p> <p><b>Recovery Timer:</b> 60</p> <p><b>Network Transfer:</b> Enable</p> <p><b>User Agent Header:</b> Disable</p> <p><b>Server Header:</b> Disable</p> <p><b>Protocol Option:</b> Disable</p> <p><b>Session Timer:</b> 1800</p> <p><b>Primary Audio Codec:</b> G.711u</p> <p><b>Secondary Audio Codec:</b> G.729a</p> <p><b>RTCP Support:</b> Enable</p> <p><b>T.38 Support:</b> Disable</p>	<p><b>SIP Server Caches:</b> 10</p> <p><b>Diffserv for Media:</b> Disable</p> <p><b>TOS Field Type for Media:</b> TOS</p> <p><b>TOS Precedence Type for Media:</b> Critical/ESP</p> <p><b>TOS Delay Type for Media:</b> Normal</p> <p><b>TOS Throughput Type for Media:</b> Normal</p> <p><b>TOS Reliability Type for Media:</b> Normal</p> <p><b>DSCP for Media:</b> 0</p> <p><b>Diffserv for Signaling:</b> Disable</p> <p><b>TOS Field Type for Signaling:</b> TOS</p> <p><b>TOS Precedence Type for Signaling:</b> Critical/ESP</p> <p><b>TOS Delay Type for Signaling:</b> Normal</p> <p><b>TOS Throughput Type for Signaling:</b> Normal</p> <p><b>TOS Reliability Type for Signaling:</b> Normal</p>	<p><b>DSCP for Signaling:</b> 0</p> <p><b>Call Release On QoS Failure:</b> Disable</p> <p><b>QoS Failure Notification Timer:</b> 10</p> <p><b>SIP Trunk Service Recovery Time:</b> 60</p> <p><b>SIP Trunk Options Interval:</b> 60</p> <p><b>SIP Trunk Message Option:</b> FQDN</p> <p><b>SIP Trunk Message To Header Option:</b> FQDN</p> <p><b>SIP Trunk Register Message From Header Option:</b> FQDN</p> <p><b>SIP Trunk Register Message To Header Option:</b> FQDN</p> <p><b>Assert Identity:</b> Disable</p> <p><b>Connection To Media Relay Server:</b> Auto</p> <p><b>RFC3311 UPDATE Method Support:</b> Disable</p> <p><b>IPedge Public IP Address And Port for NAT:</b> <input type="text"/></p>
--	---	---

NAT Traversal Function 

8. Configure a port forwarding rule in the NAT firewall to forward packets sent to the 'IPedge Public IP address' and 'Port for NAT', to the IPedge server's local IP address, and to port 5060.



**FIREWALL SETUP**

This section discusses firewall setup.

**Note:** Setup your firewall to ensure that the public WAN IP address is pointed to the IPedge server address.

**IPedge PORTS**

This document details two sets of IPedge port lists. The first is a list of ports to open in a firewall. These include ports used by all IPedge systems and the ports used by specific applications. Refer to [FIREWALL PORTS TO OPEN](#).

The second list shows the ports used by the IPedge system that must not be assigned to any other applications. Refer to [INTERNAL SYSTEM PORTS](#).

**FIREWALL PORTS TO OPEN**

**Note:** Direction “In” implies that the port will be NAT port-forwarded from the firewall WAN IP to the IP address of IPedge.All Systems

The firewall ports shown in [Table 9-1](#) must be open for every system using the IPedge Virtual Licensing Service..

**Table 9-1 IPedge Virtual Licensing**

Port	Type	Direction	Description
443	TCP	Out	Virtual Licensing
53	TCP	Out	Virtual Licensing DNS lookup

**Table 9-2 Remote IPT/UCedge VoIP Client**

Port	Type	Direction	Description
1718 to 1719	UDP	In	Remote IP Telephone set registration
2944	TCP	In	Remote IP Telephone (MEGACO signaling)
21000 to 27999	UDP	In	Remote IPT audio

**Table 9-3 SIP Trunks**

Port	Type	Direction	Description
5060	UDP	In	SIP signaling
21000 - 27999	UDP	In	SIP RTP audio

**Table 9-4 Remote UCedge/IPMobility**

Port	Type	Direction	Description
8767 to 8769	TCP	In	8767 and 8768 for plain text clients, 8769 for encrypted client applications
8088 and 8089	TCP	In	EMPA (RESTful)
90 and 42507	TCP	In	Messaging RESTful Interface for UCedge, IP Mobility, Meet-Me Audio Conference, Web Fax and, other applications.
5222	TCP	In	XMPP Client
5269	TCP	In	XMPP Server
5280	TCP	In	XMPP Client
5281	TCP	In	XMPP over SSL
443	TCP	Out	Google® push notifications/Virtual licensing
7443	TCP	Put	Messaging automatic update of APNS certificate
2195	TCP	Out	Apple APNS push notifications
53	TCP	Out	Virtual Licensing

**Table 9-5 Messaging UM**

Port	Type	Direction	Description
25	TCP	Out	SMTP
465	TCP	Out	SMTP TLS/SSL
587	TCP	Out	SMTP authenticated

**Table 9-6 Messaging Msync**

Port	Type	Direction	Description
443	TCP	Out	Exchange EWS communications
1234	TCP	In	Exchange EWS push notifications

### System to System WAN/VPN Ports

**Table 9-7 IPedge Net**

Port	Type	Direction	Description
4029	TCP	Both	IPedge Net (Connection Request)
12000 to 13791	TCP	Both	IPedge Net (Connection Request)
16000 to 17999	UDP	Both	IPedge Net RTP audio (Node to Node)
18000 to 19999	UDP	Both	IPedge Net RTP audio (Node to IPT)

**Table 9-8 Messaging**

Port	Type	Direction	Description
1000	TCP	Both	Remote node SMDI for centralized VM soft-keys
22	TCP	Both	Messaging DCN initialization
5432	TCP	Both	Messaging DCN database updates
1007 and 1008	TCP	In	Desktop fax driver 5.X
90 and 42507	TCP	In	Messaging RESTful Interface for UCedge, IP Mobility, Meet-Me Audio Conference, Web Fax and, other applications.

**Table 9-9 DSS/BLF**

Port	Type	Direction	Description
3000	UDP	Both	LAN DSS (Call control IPedge Net)
6000	TCP	Both	LAN BLF (Status display IPedge Net)
8766	UDP	Both	DSS Federation in multi-node systems

Table 9-10 shows the port ranges used in different system configurations.

**Table 9-10 End Point Port Range**

IPedge Server Address	End Point IP Address	RTP Port Range for the MRS <sup>1</sup>
Public	Public	27000 ~ 27999 <sup>2</sup>
	Private (NAT)	27000 ~ 27999 <sup>2</sup>
Private	Public	21000 ~ 22999 <sup>3</sup>
	Private behind remote NAT	21000 ~ 22999 <sup>3</sup>
	Private	27000 ~ 27999 <sup>2</sup>
	Private behind local NAT	27000 ~ 27999 <sup>2</sup>
Set the MRS connection mode to Manual during NAT traversal and SIP/SIP Trunk.		21000 ~ 26999 <sup>3</sup>

1. RTP connection as 'seen' from the end point.
2. MRS internal port range is 27000 ~ 27999. This range is fixed.
3. MRS External port range is programmable. The range is 21000 ~ 22999.

**Important!** When the "IPT Data Auto Connection to MRS" is set to "Auto," the IPedge system will determine whether the IPT is placed inside NAT or not, and generate appropriate SDP.

If the IPedge system is unable to determine whether the IPT is placed inside NAT or not, (for example; if you hear one-way audio) set IPT Data Auto Connection to MRS" is set to "Manual." This will ensure that the MRS is used for the IPT connections.

## INTERNAL SYSTEM PORTS

Table 9-11 is a list of ports used by the IPedge system. Do not assign any of these ports to applications such as CSTA.

Table 9-11 Do Not Assign Port List

Port Numbers	Port Numbers	Port Numbers	Port Numbers
20 ~ 23	2020	8080	13000 ~ 19999
25	2944	8100	20023
68	3000 and 3001	8443	20161
90	3306	8444	21000 ~ 26999
110	4003	8445	27000 ~ 29999
111	4029	8767	30000 ~ 30999
123	5060	8768	40000 ~ 40003
143	5070	9101 ~ 9103	40005
161	5280 ~ 5281	9443	40006
162	6000	9999	41088
443	6379	10000	54445
993	6678	10030	(Sheet 4 of 4)
1000	6800	10100 ~ 10103	
1100 ~ 1105	7000 ~ 7009	10200	
1270	7577	10201	
1718 ~ 1720	7583	12000 ~ 13791 (TCP)	
1935	8005	12000 ~ 14511 (UDP)	
1945	8009		
(Sheet 1 of 4)	(Sheet 2 of 4)	(Sheet 3 of 4)	

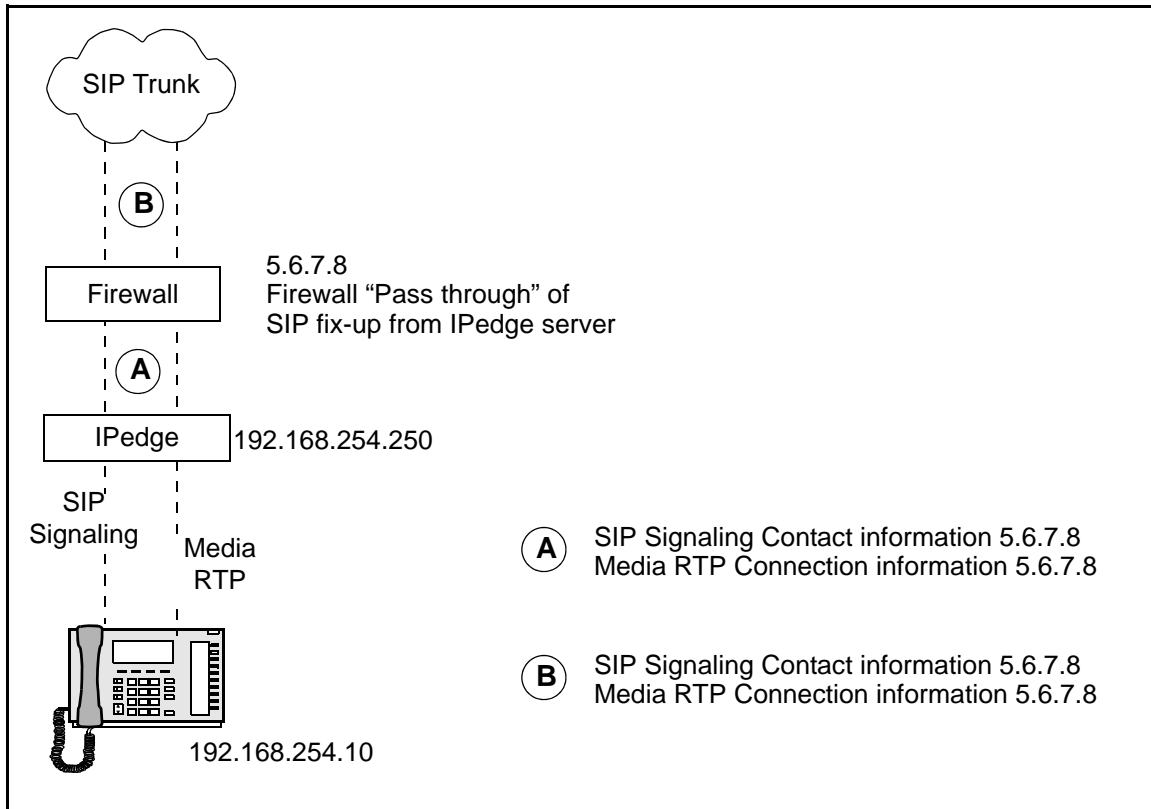
**Notes:** IPedge Net signalling port for originator node should be known to open firewall in advance.

Groups and services list are subject change.

**CALL SIGNALING EXAMPLES**

These are some examples of call flow signaling in different IPedge system topologies.

In the examples the IP address are used to show the changes in the various layers. These example include the IPedge Trunk NAT Traversal function available in IPedge R1.3 and later systems.



**Figure 9-1 Private IP Address with MRS Enabled, With NAT Traversal, No SIP ALG Firewall**

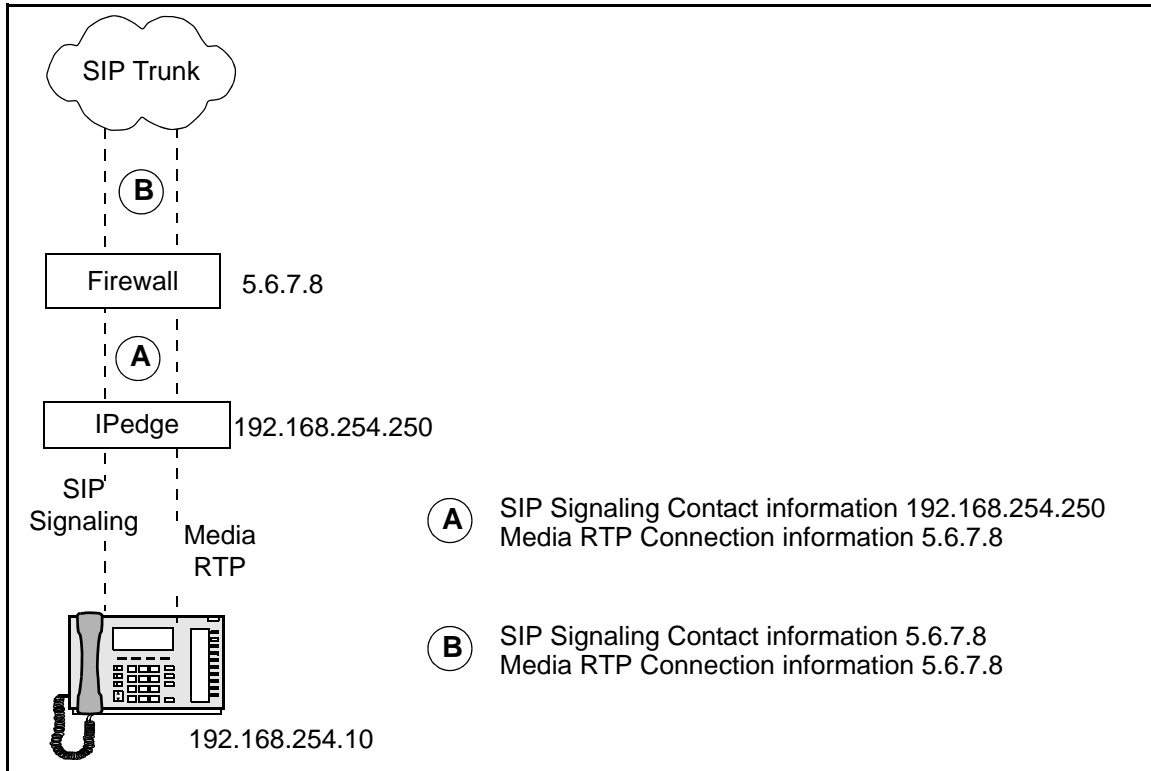


Figure 9-2 Private IP Address, MRS Enabled, No NAT Traversal, With SIP ALG Firewall

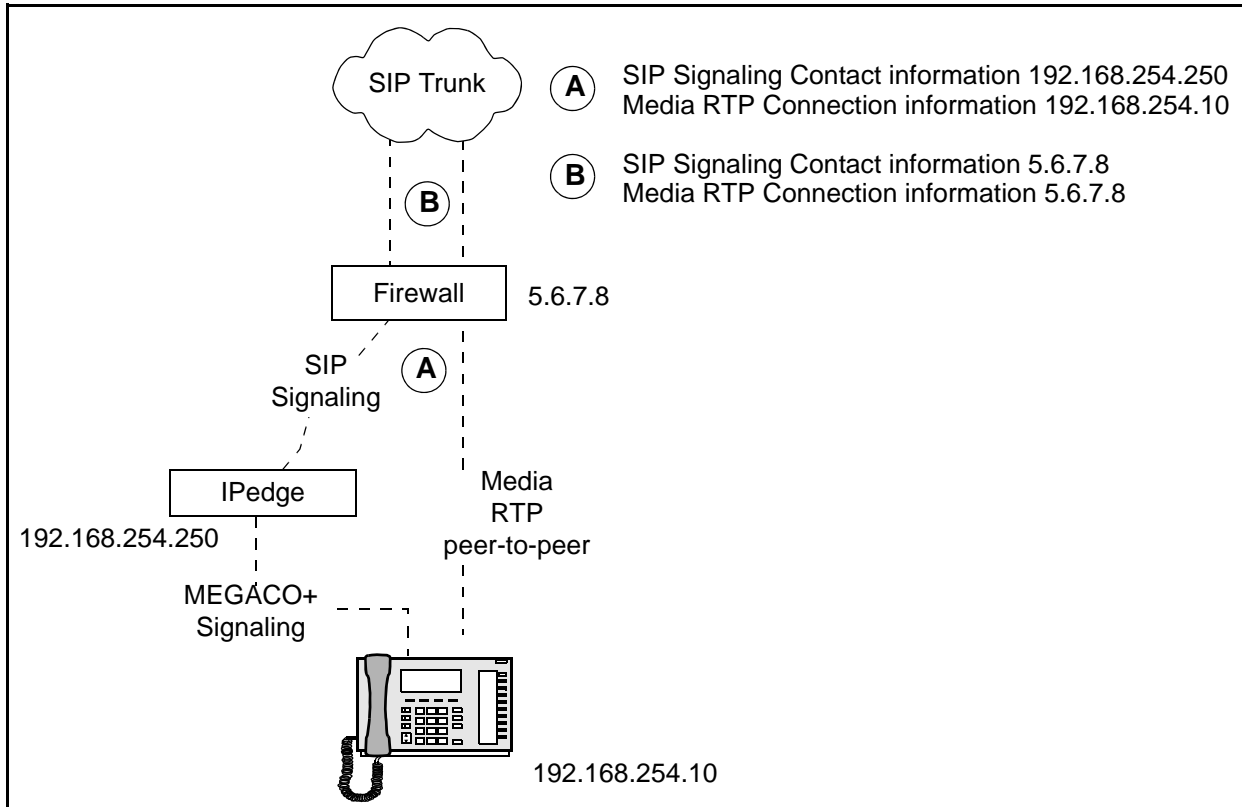
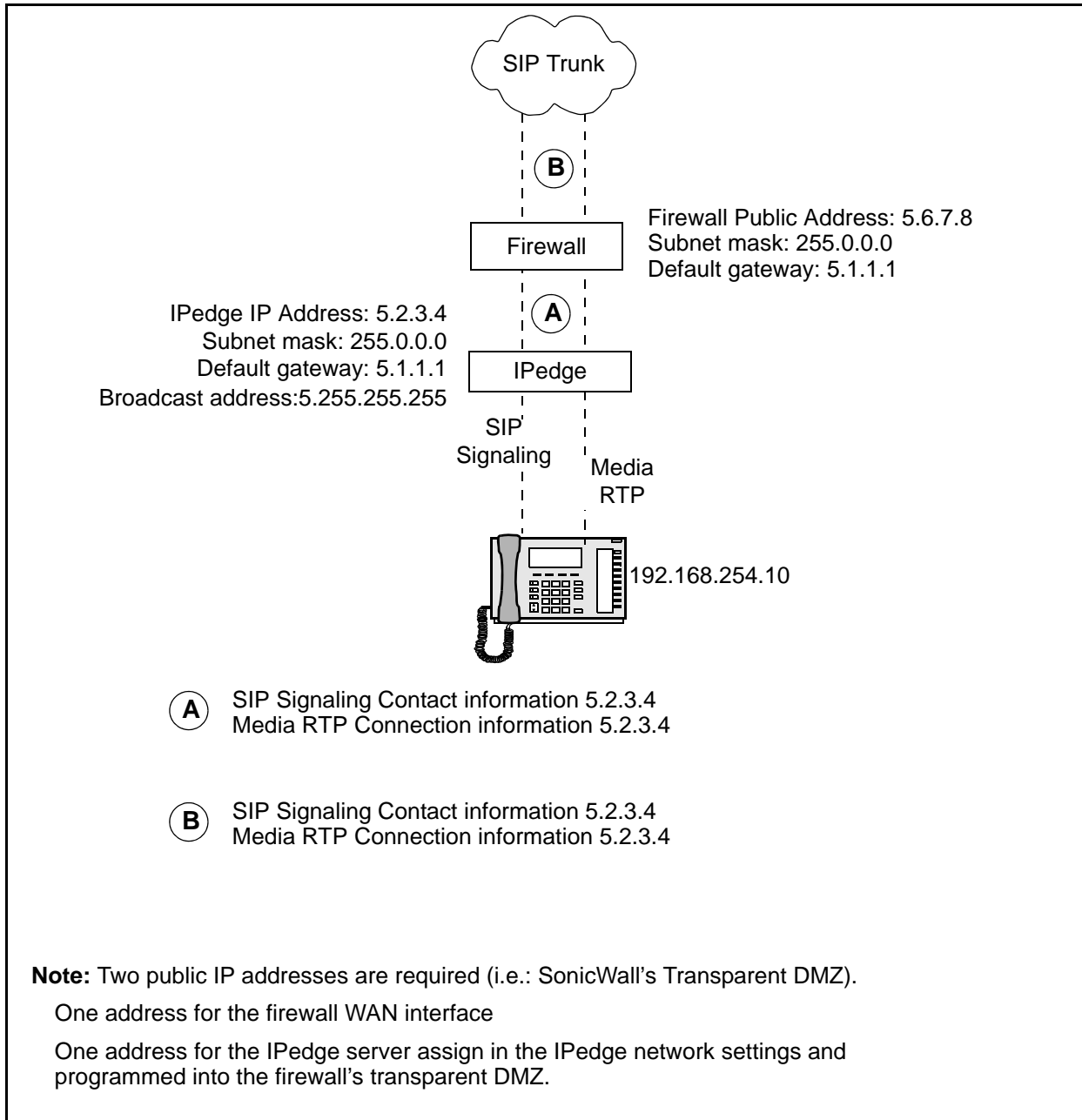


Figure 9-3 Private IP Address, No MRS, No NAT Traversal, With SIP ALG Firewall





**Figure 9-4 MRS Enabled, No NAT Traversal, No SIP ALG Firewall**

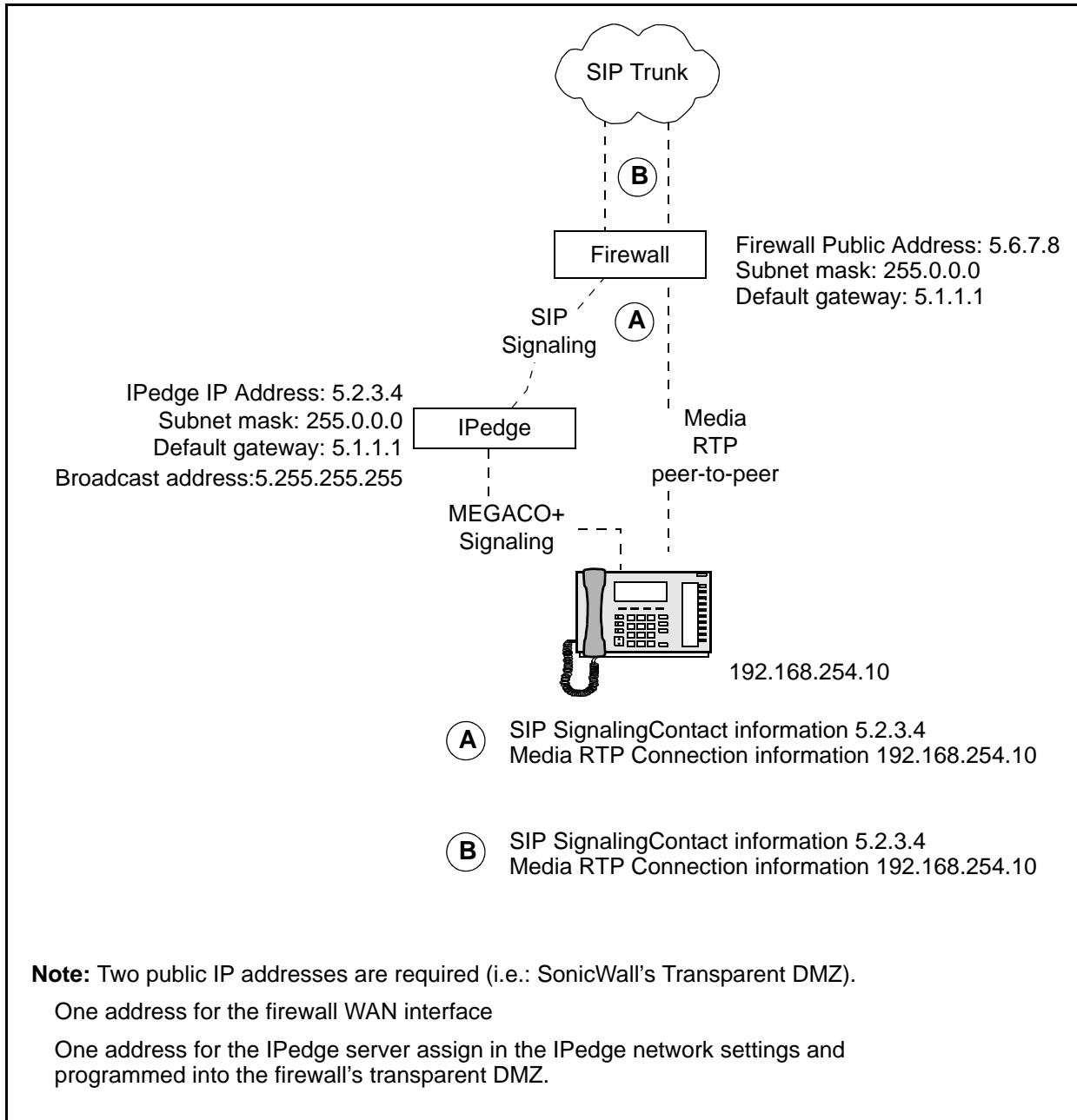


Figure 9-5 Public IP Address, No MRS Enabled, No NAT Traversal, No SIP ALG Firewall

**NETWORK SECURITY**

After the IPedge system is installed, the SIP Trunks and/or Remote IP Telephones working, it is the responsibility of the installer and system user to setup the firewall to help prevent unauthorized access. For example ports used only for specific features, such as remote IPTs, not implemented on your system may be closed.

While this can be accomplished in many ways one basic method is using lists. For example; Cisco devices can be configured using ACL's (Access control lists) and, in SonicWALL by setting up rules to Deny or allow specific IP addresses, or other means in other firewalls.

For example; the firewall configuration could be set to only allow specific IP's. Contact your SIP Provider for a list of the IP's their Signaling and Media will use. For a remote IPT add the static IP to the safe list, if the remote IPT is a dynamic IP you could list a range of IP addresses for use by the IPT, or even better require the use of a hardware VPN for all remote phones and software VPN for softphones that are roaming.

Any specific programming of firewall rules to secure access to the network and IPedge server are the responsibility of the installing dealer and/or customer and vary by the needs and level of protection determined by the customer's IT department. Toshiba technical support does not assume responsibility to provide specific commands or to verify a network or specific IPedge server is secure.

**SONICWALL**

Typical SonicWALL setup:

1. Login to the SonicWALL.
2. Go to the VoIP section.
3. Ensure that the Enable SIP Transformations box is NOT check marked.
4. Open firewall ports as required. Refer to "IPedge PORTS" on [Page 9 - 5](#).
5. Media Relay Server and NAT Traversal may also be required.

**Transparent Mode**

Transparent Mode is usually not required unless a public IP Address for the IPedge server is required. This section covers the configuration of the SonicWALL Router in Transparent Mode for use with the IPedge server.

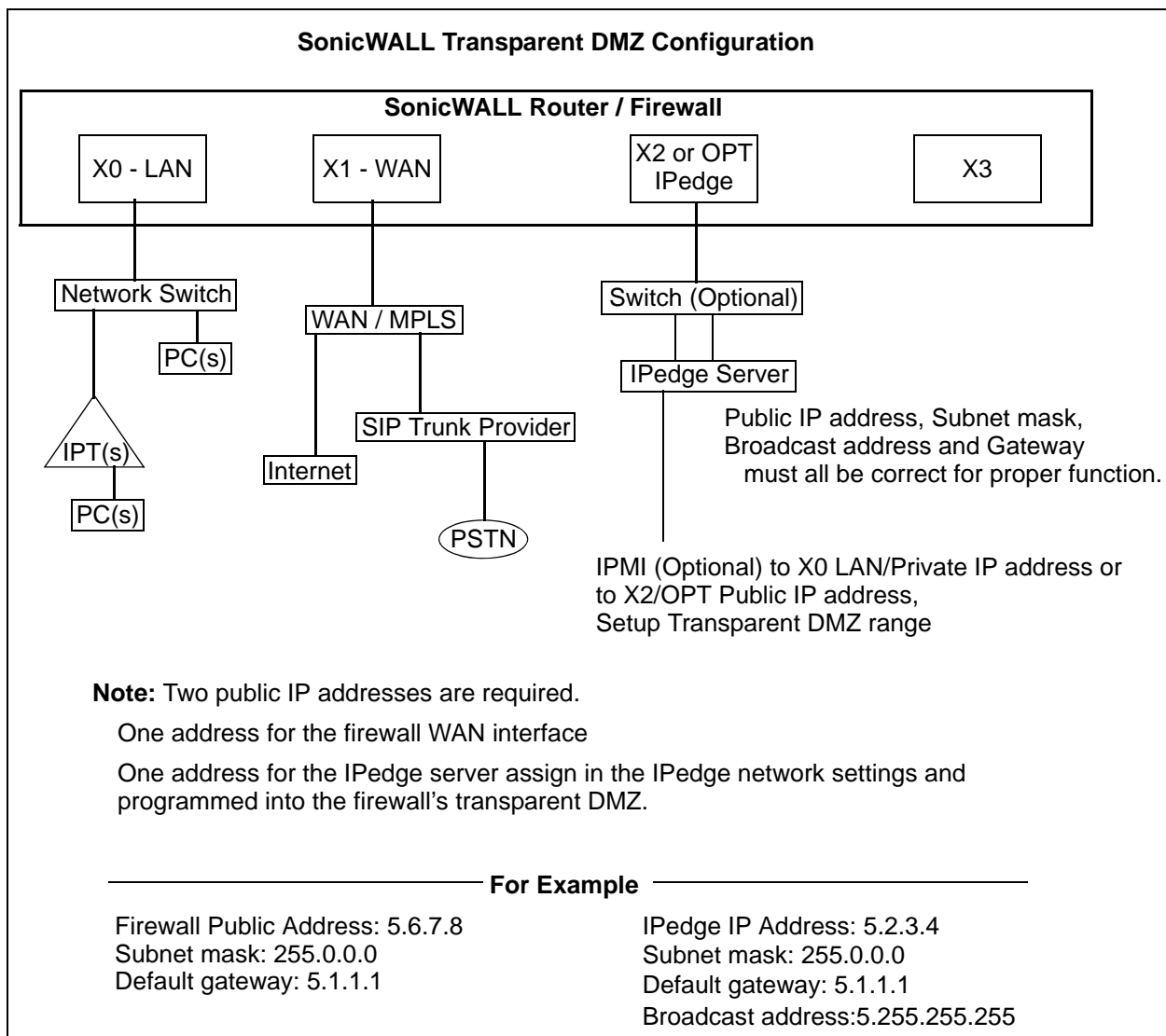
**Requirements**

Before starting this process you must have the following information:

- IP Address of the IPedge server
- Public IP Address of the SonicWALL
- IP Address of all devices on the network

This document is intended as guide to the configuration of your SonicWALL router on your IPedge network.

You are responsible for the security of your network. Open only the port necessary for the operation of your system. Allow only IP addresses you trust. Ensure that all unused ports are DENIED. Refer to [Figure 9-6](#).



**Figure 9-6 SonicWALL Transparent DMZ Configuration**

**SONICWALL TZ100  
CONFIGURATION**

This procedure details the procedure to configure the SonicWALL router WAN interface with the LAN in Transparent Mode.

Transparent Mode requires valid public IP addresses for the IPedge system. Your public WAN IP address is visible to the Internet. X0 is the LAN interface that uplinks to your LAN Switch. The IPTs will be on private IP addresses. An external DHCP server for IPT addresses is alright as long as the phones have the gateway address of the SonicWALL. When using another DHCP server disable the DHCP service in the SonicWALL router.

1. Login to the SonicWALL TZ100.
2. Select **Network > Interfaces**. X1 is WAN with a public IP.
3. Click the **edit** icon next to the X2 interface.
4. Select **DMZ** or create a new Zone. For a new zone setup a Name, security as Public, set member interface to X2. (If you create a new zone name use that name in place of DMZ in the following steps.)
5. Select **Transparent Mode** from the IP address selection.
6. In Transparent range click on **Create New Object** (Select Host for one IPedge system. Select Range for multiple public addresses).
  - A. Name the new object (include the IP address as part of the name).
  - B. Set Zone Assignment = **WAN**
  - C. Type = **HOST**
  - D. IP Address = **IP address** of the IPedge system
  - E. Click on **OK**.
7. Click on **OK**.
8. The WAN and DMZ IP addresses are now identical on the Interface page.
9. Power cycle the SonicWALL unit.
10. Configure the IPedge address as shown in the IPedge Install manual.
11. Connect the IPedge system to the interface configured for Transparent DMZ.
12. Select **Firewall > Access Rules**.
  - A. Set up any allow or deny rules as required. Do not accept "default" settings without verifying. Ensure that you understand what the implications or risks when setting the rules.
    - The SonicWALL default configuration is to DENY DMZ to LAN connections. To allow IPedge to connect to IPTs change this to ALLOW.
    - The SonicWALL default configuration is to ALLOW DMZ to WAN. Ensure that this is set. When the system has passed all installation testing you may want to allow only the IPedge system IP addresses.

- B. The SonicWALL default configuration is to DENY LAN to DMZ. Set LAN to DMZ to ALLOW to allow IPTs on the LAN to connect to the IPedge system.
- C. In the SonicWALL default configuration WAN to DMZ defaults to DENY, set to ALLOW.
  - When the system has passed all installation testing you should only allow certain IP addresses, such as remote IPTs and SIP trunk providers, from WAN to DMZ.
- D. DENY ANY other sources.

13. Enable consistent NAT. Select **VoIP > Settings** then, check mark the box for **Enable consistent NAT**.

**Note:** If IPT users experience one way audio, the IPT user can not hear, you may need to set the "Connection of Media Relay Server" to "Manual" in the IPedge SIP Trunk > Service Definition.

You may additionally or alternatively need to set "Connection of Media Relay Server" to "Manual" in the IPedge Station assignment > Station, in the IPT data tab.

**Note:** Do not set SIP VM ports to "manual" as VM is on the IPedge server.

**Note:** When using Public IP/Transparent DMZ on an IPedge system Ports 27000 ~ 27999 will need to be open in the SonicWall for Remote IPT phones RTP (audio path) on the router in addition to other ports mentioned in the IPedge Install Manual.

**SONICWALL TZ170**

Transparent Mode requires valid public IP addresses for all computers on your network, and allows remote access to authenticated users. Your public WAN IP address is visible to the Internet. The LAN interface uplinks to your LAN Switch, the IPTs will be on the private IP addresses (DHCP is alright as long as the phones have the gateway address of the SonicWALL).

Follow these steps to configure the WAN and LAN interfaces in transparent mode:

1. Login to the SonicWALL TZ170.
2. Select **Network > Interfaces**. WAN has a public IP address.
3. Click the **edit** icon next to the OPT interface.
4. Select **DMZ** or create a new Zone. For a new zone setup a Name, security as Public, set member interface to X2. (If you create a new zone name use that name in place of DMZ in the following steps.)
5. Select **Transparent Mode** from the IP address selection.
6. In Transparent range click on **Create New Object** (Select Host for one IPedge system. Select Range for multiple public addresses).
  - A. Name the new object (include the IP address as part of the name).
  - B. Set Zone Assignment = **WAN**
  - C. Type = **HOST**
  - D. IP Address = **IP address** of the IPedge system
  - E. Click on **OK**.
7. Click on **OK**.
8. The WAN and DMZ IP addresses are now identical on the Interface page.
9. Power cycle the SonicWALL unit.
10. Configure the IPedge address as shown in the IPedge Install manual.
11. Connect the IPedge system to the interface configured for Transparent DMZ.
12. Select **Firewall > Access Rules**.
  - A. Set up any allow or deny rules as required. Do not accept "default" settings without verifying. Ensure that you understand what the implications or risks when setting the rules.
    - The SonicWALL default configuration is to DENY DMZ to LAN connections. To allow IPedge to connect to IPTs change this to ALLOW.
    - The SonicWALL default configuration is to ALLOW DMZ to WAN. Ensure that this is set. When the system has passed all installation testing you may want to allow only the IPedge system IP addresses.



- B. The SonicWALL default configuration is to DENY LAN to DMZ. Set LAN to DMZ to ALLOW to allow IPTs on the LAN to connect to the IPedge system.
- C. In the SonicWALL default configuration WAN to DMZ defaults to DENY, set to ALLOW.
  - When the system has passed all installation testing you should only allow certain IP addresses, such as remote IPTs and SIP trunk providers, from WAN to DMZ.
- D. DENY ANY other sources.

13. Enable consistent NAT. Select **VoIP > Settings** then, check mark the box for **Enable consistent NAT**.

**Note:** If IPT users experience one way audio, the IPT user can not hear, you may need to set the "Connection of Media Relay Server" to "Manual" in the IPedge SIP Trunk > Service Definition.

You may additionally or alternatively need to set "Connection of Media Relay Server" to "Manual" in the IPedge Station assignment > Station, in the IPT data tab.

**Note:** Do not set SIP VM ports to "manual" as VM is on the IPedge server.

**Note:** When using Public IP/Transparent DMZ on an IPedge system Ports 27000 ~ 27999 will need to be open in the SonicWall for Remote IPT phones RTP (audio path) on the router in addition to other ports mentioned in the IPedge Install Manual.

**SONICWALL Pro2040**

Transparent Mode requires valid public IP addresses for all computers on your network, and allows remote access to authenticated users. Your public WAN IP address is visible to the Internet. X0 the LAN interface uplinks to your LAN Switch, the IPTs will be on the private IP addresses (DHCP is ok as long as the phones have the gateway address of the SonicWALL).

1. Login to the SonicWALL Pro2040.
2. Select **Network > Interfaces**. X1 is WAN with a public IP.
3. Click the **edit** icon next to the X2 interface.
4. Select **DMZ** or create a new Zone. For a new zone setup a Name, security as Public, set member interface to X2. (If you create a new zone name use that name in place of DMZ in the following steps.)
5. Select **Transparent Mode** from the IP address selection.
6. In Transparent range click on **Create New Object** (Select Host for one IPedge system. Select Range for multiple public addresses).
  - A. Name the new object (include the IP address as part of the name).
  - B. Set Zone Assignment = **WAN**
  - C. Type = **HOST**
  - D. IP Address = **IP address** of the IPedge system
  - E. Click on **OK**.
7. Click on **OK**.
8. The WAN and DMZ IP addresses are now identical on the Interface page.
9. Power cycle the SonicWALL unit.
10. Configure the IPedge address as shown in the IPedge Install manual.
11. Connect the IPedge system to the interface configured for Transparent DMZ.
12. Select **Firewall > Access Rules**.
  - A. Set up any allow or deny rules as required. Do not accept "default" settings without verifying. Ensure that you understand what the implications or risks when setting the rules.
    - The SonicWALL default configuration is to DENY DMZ to LAN connections. To allow IPedge to connect to IPTs change this to ALLOW.
    - The SonicWALL default configuration is to ALLOW DMZ to WAN. Ensure that this is set. When the system has passed all installation testing you may want to allow only the IPedge system IP addresses.
  - B. The SonicWALL default configuration is to DENY LAN to DMZ. Set LAN to DMZ to ALLOW to allow IPTs on the LAN to connect to the IPedge system.

- C. In the SonicWALL default configuration WAN to DMZ defaults to DENY, set to ALLOW.

When the system has passed all installation testing you should only allow certain IP addresses, such as remote IPTs and SIP trunk providers, from WAN to DMZ.

- D. DENY ANY other sources.

13. Enable consistent NAT. Select **VoIP > Settings** then, check mark the box for **Enable consistent NAT**.

**Note:** If IPT users experience one way audio, the IPT user can not hear, you may need to set the “Connection of Media Relay Server” to “Manual” in the IPedge SIP Trunk > Service Definition.

You may additionally or alternatively need to set “Connection of Media Relay Server” to “Manual” in the IPedge Station assignment > Station, in the IPT data tab.

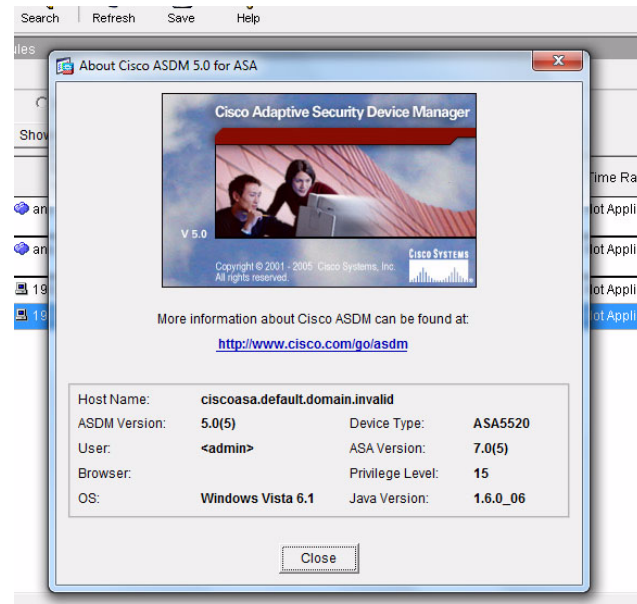
**Note:** Do not set SIP VM ports to “manual” as VM is on the IPedge server.

**Note:** When using Public IP/Transparent DMZ on an IPedge system Ports 27000 ~ 27999 will need to be open in the SonicWall for Remote IPT phones RTP (audio path) on the router in addition to other ports mentioned in the IPedge Install Manual.

For more detail on transparent DMZ visit the SonicWALL website or call SonicWALL for support.

## CISCO

1. Verify that the Cisco firewall software is up to date.

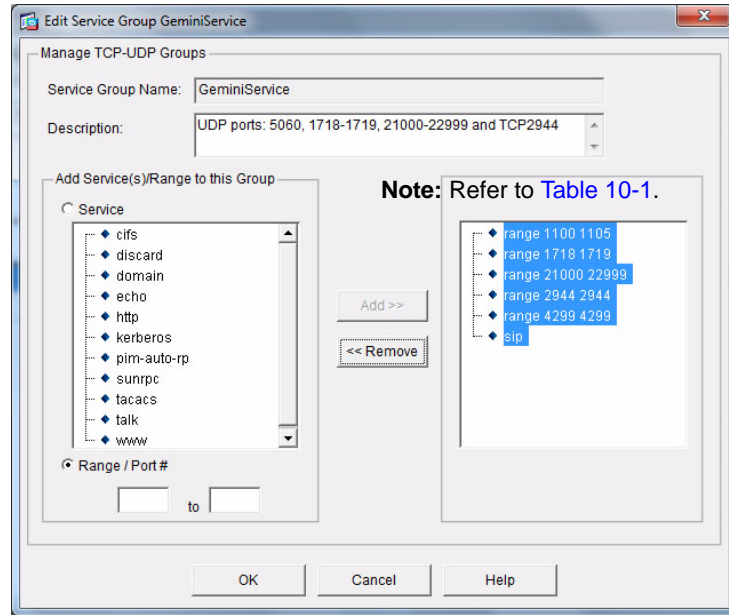


The screen shown above is the Cisco ASDM. This program is available as a download from the Cisco website.

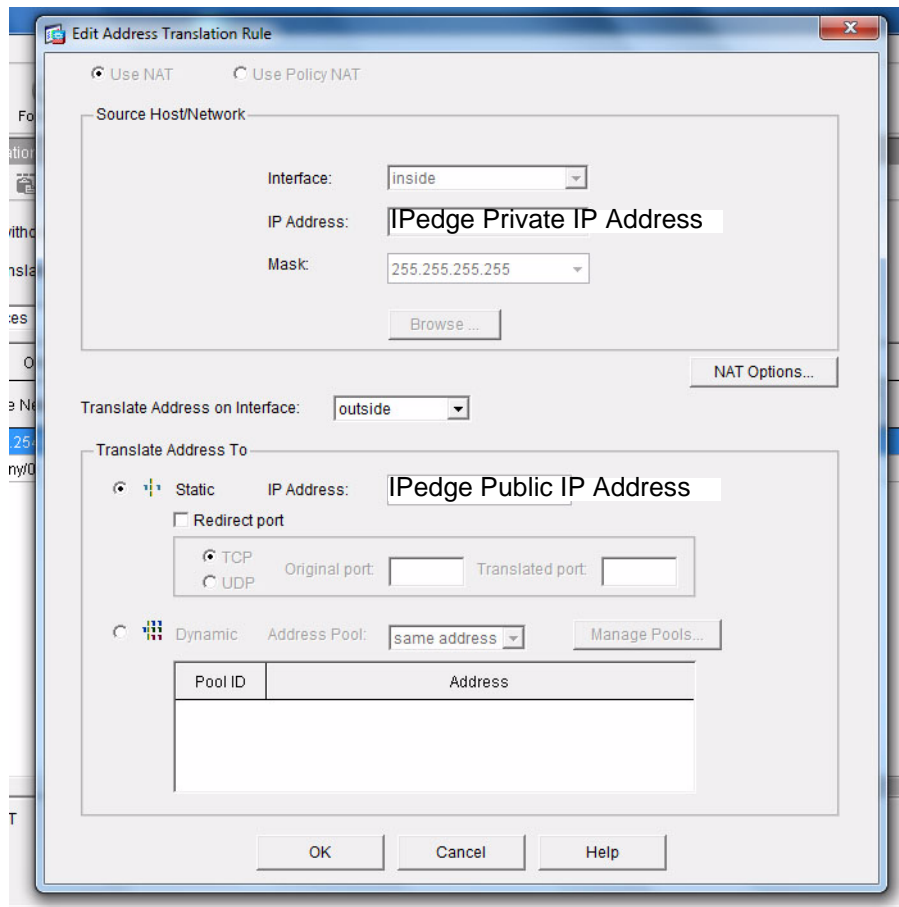
2. Add the TCP and UDP ports to the Manage Ports list. Add the following ports:
  - 1100 to 1105 TCP (Systems connecting with unifier)
  - 1718 to 1719 UDP (Remote IP Telephone set registration)
  - 21000 to 27999 UDP (Remote IP or SIP telephone audio)

**Note:** Refer to [Table 9-10](#).

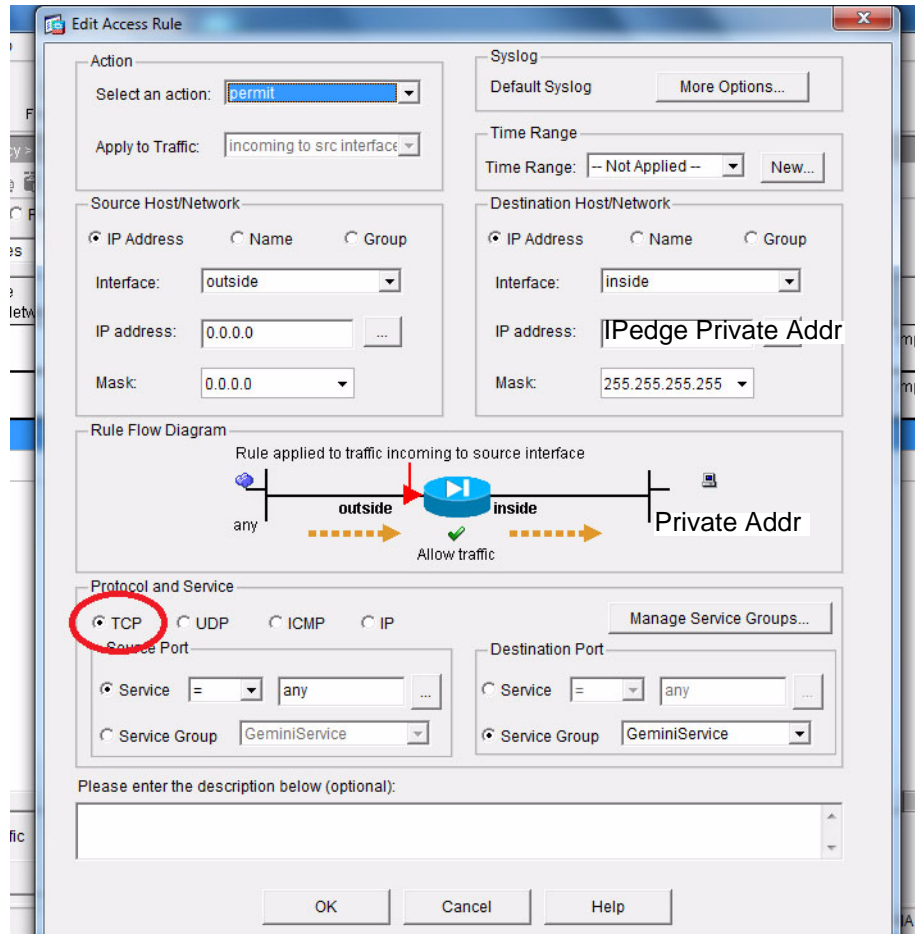
  - 2944 to 2944 TCP (Remote IP Telephone MEGACO signaling)
  - 5060 UDP (SIP trunks or remote SIP telephones)



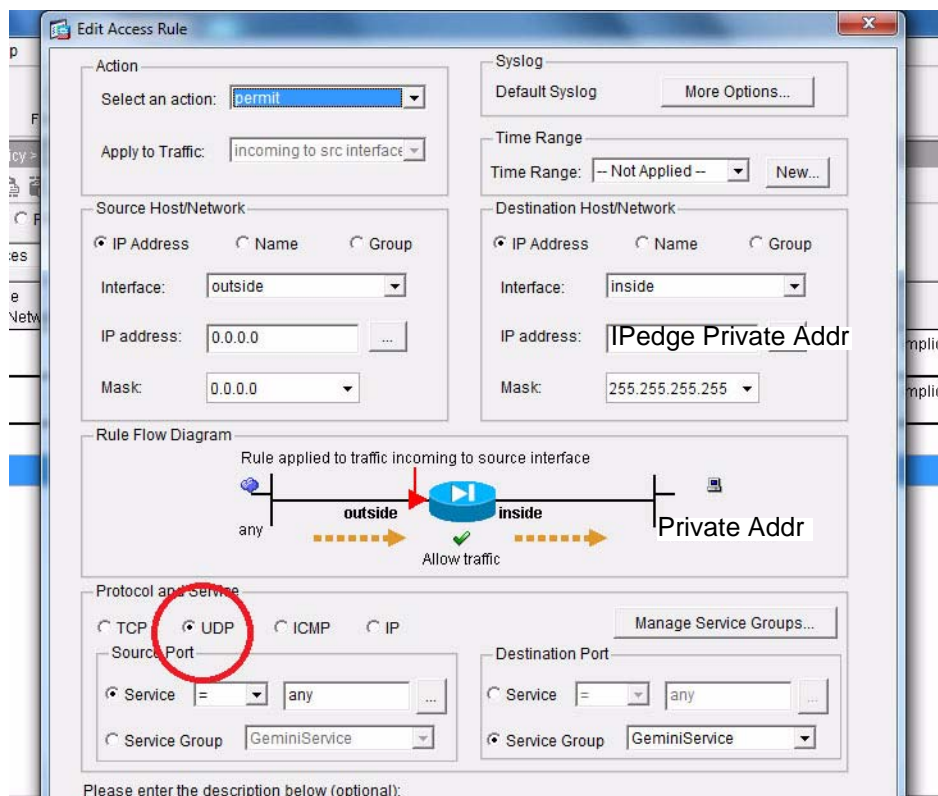
3. In **Configuration > Enable Traffic Through ... > Translation Rules**. Select **Use NAT** the, enter the Inside (IPedge private) Address and the Outside (IPedge public) Address.



4. In the Edit Access Rule dialog Select **permit** as the action, enter the IPedge private IP address as the Destination Host/Network. Under Protocol and Service select **TCP**. Click on **OK**.



- In the Edit Access Rule dialog Select **permit** as the action, enter the IPedge private IP address as the Destination Host/Network. Under Protocol and Service select **UDP**. Click on **OK**.



- If you used the ADSM go to Step 7.  
If you use Command Line Interface (CLI) save the configuration then go to the Inspect SIP Commands in the section below.
- Save the configuration.
- Logout of the Cisco firewall.

### Inspect SIP Commands

The Inspect SIP commands change fields in the SIP messaging from private IP's to public IP's. The paragraph below explains what Inspect SIP commands do.

SIP inspection has a database with indices CALL\_ID/FROM/TO from the SIP payload that identifies the call, as well as the source and destination. Contained within this database are the media addresses and media ports that were contained in the SDP media information fields and the media type. There can be multiple media addresses and ports for a session. RTP/RTCP connections are opened between the two endpoints using these media addresses/ports.

Commands:

- Issue the **policy-map global\_policy** command.  
ASA5510(config)#policy-map global\_policy

2. Issue the **class inspection\_default** command.  
ASA5510(config-pmap)#class inspection\_default
3. Issue the **inspect sip** command.  
ASA5510(config-pmap-c)#inspect sip



# Chapter 10 – SIP Trunk Configuration

---

## INTRODUCTION

Session Initiation Protocol (SIP) is an application layer protocol used for establishing sessions in an IP network. SIP trunks allow the IPedge system to get PRI-like services from an Internet Telephony Service Provider using SIP.

A SIP trunk allows an IPedge system to connect internal voice and private data traffic to the outside public network (PSTN and public data) via IP.

When a user dials a call that will be sent over the PSTN, the call routing is sent over the WAN to the Internet Telephony Service Provider (ITSP) that is providing the SIP trunk. This ITSP will provide a connection to the PSTN through their equipment. The call will be sent from the IPedge system to the SIP provider, who will act as a proxy, and send the call to the dialed destination.

For incoming calls, the SIP trunk acts somewhat like a DID trunk, the dialed number is sent to the SIP provider and then routed over the IP Network to the IPedge system. This routing is based on the URI and associated IP address.

Toshiba's SIP Trunk capabilities allow the IPedge system to communicate with a service provider natively over an IP circuit, which can be used to carry voice and data simultaneously. Inside the IPedge system, voice is converted to data and sent to the service provider along the same circuit as the other data packets. This allows one circuit to be used for voice and data, it also allows data to use all of the bandwidth when no voice is present. Quality of Service (QoS) is managed by the service provider, allowing voice to instantaneously take priority over data.

SIP trunks offer ISDN-like features over a data connection (i.e. a T1 circuit). However, unlike a traditional T1 circuit, a SIP trunk enabled circuit does not have to be physically provisioned and divided to separate the voice channels from the data channels.

## REQUIREMENTS

- Contact the Toshiba Sales Applications Desk for the latest SIP Trunk Service provider list.
- License: I-CP-TRUNK

## SIP PROVIDERS and SIP GATEWAYS

SIP Trunks from the provider - Typically has an IP address not on your LAN

SIP Trunk from a gateway - Typically has an IP address on your LAN

## CAPACITIES

---

### CAPACITIES

The IPedge system can support up to 1000 URI entries. SIP Trunk capacities and IPedge Net Channel capacities are shown in [Table 10-1](#).

**Table 10-1 Trunk Capacities**

Trunks	EC Server	EM Server	EP Server
IPedge Net IP channels	96	440	33
SIP Trunk channels	96	440	33
Total Analog, T1, and ISDN trunk channels connected by gateways.	96	440	33
Channel Groups (One group for SIP trunks and one group for IPedge Net.)	2	2	2

### 911/E911 CALLS

It is imperative to ensure that E911 calls are routed correctly in all cases according to local and state laws.

**Important!** IP Phone users in locations where 911 calls can not be routed to the correct Public Safety Answering Point (PSAP) must maintain a wired land line phone or cell phone in order to make 911 calls to the correct PSAP.

### SIP SIGNALING

IPedge system SIP Trunks will send SIP message 100 trying and 180 ringing in response to Invites, message 183 is not available as a session progress response.

## SIP TRUNK EXAMPLE

### SIP TRUNK EXAMPLE

The example shown in [Figure 10-1](#) is a general system plan. Refer to the specific provider sections of this document. Trunk service from an analog or digital service can be used only through a SIP gateway, refer to [Figure 10-2](#)

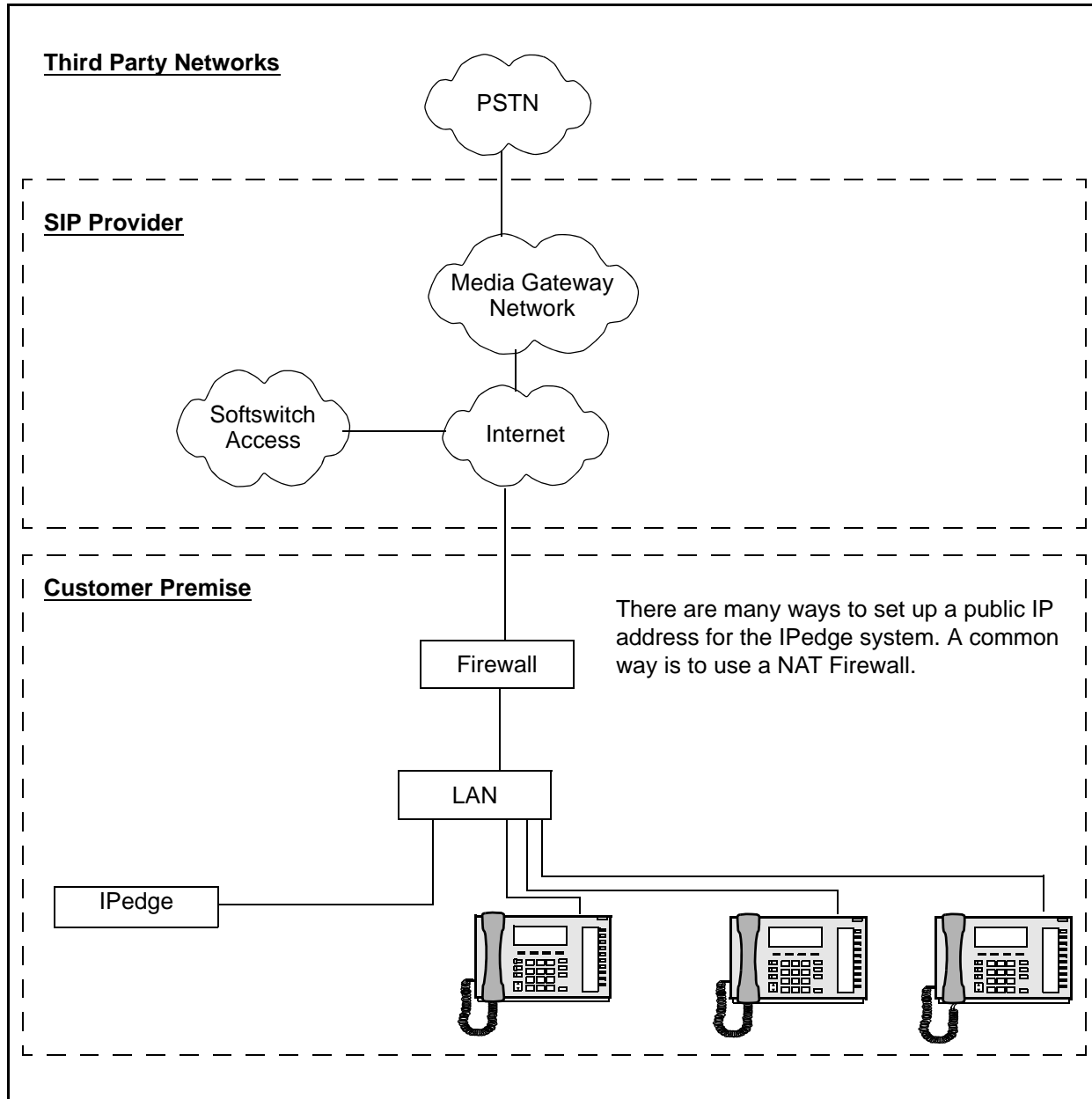


Figure 10-1 IPedge System with SIP Trunking

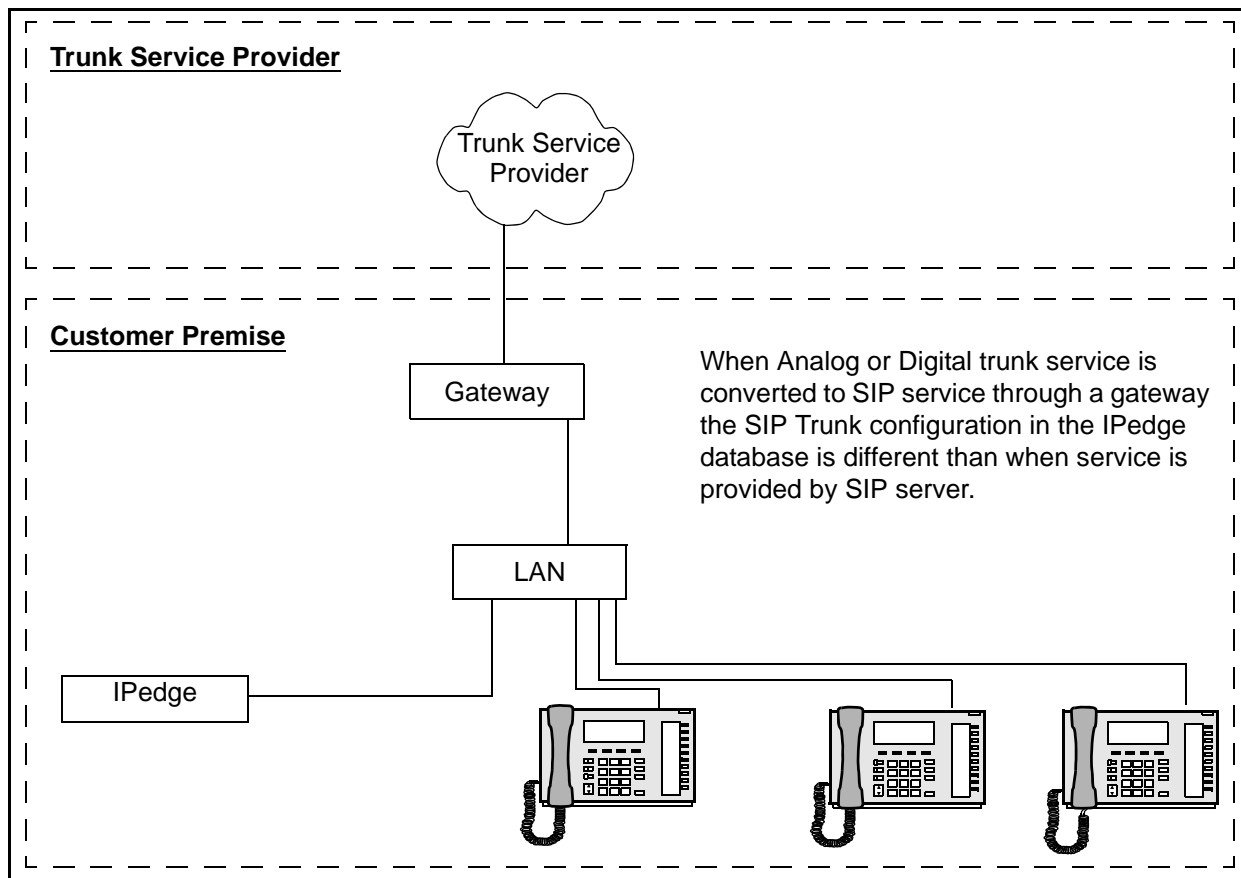


Figure 10-2 IPedge System with SIP Gateway

## SIP TRUNK GROUP PROGRAMMING

The following pages show the general programming and configuration steps to implement a SIP trunk. Specific procedures for each provider are in the linked tables in this document.

**Note:** SIP trunking requires a license for each trunk. No channel group can successfully be programmed without a license.

### Programming the Incoming Line Group

1. Select **Trunk > Trunk Groups**. Click on the **New** icon.
2. Select the server to which to add the trunk group.
3. In the Group Direction pull-down select **Incoming and Outgoing**. then, click on **OK**.
4. In the **Common** tab select a trunk **Group Number** then select **Group Type SIP**. Record this number.

5. On the **Incoming** tab in the **CO Service Type** select DID then, set the number of **DID digits** (Default = 4 digits).

The DID Digits parameter sets how many of the digits received from the SIP Trunk will be used to choose the station to which the call goes. For example; if the SIP provider sends 10 digits, and the DID digits is set to four, only the last four digits are used to route the call. The additional digits will be ignored. All of the received digits must be in the URI table.

6. Click on the **Save** icon.

**Note:** Notice that Incoming and Outgoing trunk group with the same Trunk Group Number have been created.

**Note:** When all of the ILGs and OLGs have been created Toshiba recommends that you enable Intercept and program destination in **Trunk > DID Intercept**.

### Programming the Outgoing Line Group

In the Outgoing tab set the parameters for outgoing calls on this trunk group. Typically the default values are used.

**Note:** An OLG flexible access code must be created for this group.

### ASSIGN DID TRUNK DESTINATION

DID routing must be set up to route incoming SIP calls to their desired destination. This programming is the same as any other trunk group type. If the routing is not set up, incoming Invites will fail instantly.

1. Select **Trunk > DID**.
2. Select the server.
3. Click on the **New** icon.
4. Select the ILG Group Number.
5. Enter the number of DID digits in the **DID Number** field.
6. Select the MOH source.
7. Select the Tenant number (Default = 1).
8. In the DID Audio section: Set Audio Day1 Dst Type, Audio Day2 Dst Type and Audio Night Dst Type to **Dialing Digits**.
9. Set the Dst Digits to the Extension Number to which the DID calls will ring.
10. Leave the DID Data section at default.
11. Leave the remaining parameters blank.
12. Click on the **Save** icon.

**Note:** Least Cost Routing is, by default, programmed to use OLG 1. If SIP trunks are created using a different OLG, adjustments may be required in the LCR > Route Choice Assignments, and Route Definition Assignments.

**OLG FLEXIBLE ACCESS CODE PROGRAMMING**

An access code is required for the OLG that was setup for the SIP Trunks. SIP trunks can also be accessed using LCR.

1. Select **System > Flexible Access Code**.
2. Click on the **New** icon.
3. Enter the Access Code.
4. Select Feature Name; Line Group access code.
5. Select the OLG.
6. Click on the **Save** icon.

**Creating the Channel Group**

**Important!** Complete the Channel Group programming before starting the Service Definition programming.

1. Select **Trunk > SIP Trunking**.
2. In the Channel Group tab select the SIP Trunk Channel Group to be created.

**Note:** Choose a Channel group number that has not been assigned in another section.

When a Channel Group is selected for a SIP trunk that Channel group number cannot be used for IPedge Net.

3. In the SIP Trunk Channels box select the TOTAL number of ports to be dedicated to the SIP trunk channel group.
4. Click on the **Save** icon.

**Service Definition**

1. Click on the Service Definition tab.
2. Click on the **New** icon.
3. Select a Service Definition Index number then, enter the following based on the SIP Trunk Provider:  
Registration Mode - Client or none  
Domain Name - The domain name of the SIP Trunk provider (FQDN) or the IP address.  
SIP Server - The SIP Trunk provider outbound proxy or blank.
4. Enter the ILG and OLG created above.
5. Select the number of trunks/channels provided by this SIP trunk provider as the Effective Channel Number.
6. Click on the **Save icon**.

**Note:** If you experience one-way speech on local IPT to SIP trunk calls; enable the Server in the System Settings then, set Connection to Server to **Manual** in the SIP Trunk service definition.

**Note:** When using a NAT router, the private IP address in the SIP header is not changed. The result is an unsuccessful call.

A SIP ALG router will be required to change the private IP address to public IP address in fields in the SIP header (such as the contact field), MRS is not a SIP ALG. Refer to the NAT Traversal chapter.

- Service Assignment**
1. Click on the Service Assignment tab.
  2. Click on the **New** icon.
  3. SIP trunk Channel Group = Channel Group tab number (Use the Channel group created above.)
  4. Service number = Row number (Enter the digit 1 for the first assignment. Increment for each new assignment.)
  5. Service Definition Index = Value create in service definitions tab.

- Service URI**
- The SIP URI is the Telephone Number (TN) from the SIP trunk provider.
1. Click on the Service URI tab.
  2. Click on the **New** icon.
  3. Service Definition Index: The service index that defines the SIP provider. This is the number assigned in "[Service Definition](#)" on [page 10-6](#).
  4. SIP URI Number: This is the TN of the URI, typically this is the same as the CLID.
  5. SIP URI User Name: Refer to your SIP Trunk provider.
  6. SIP URI password: Refer to your SIP Trunk provider.
  7. SIP URI Attribution: Typically the value is MAIN. If your SIP Trunk provider registers only the Primary number set the remaining numbers to SUB. When SUB is used the URI number cannot be used as the Calling Number.

**Important!** If a SIP URI (TN) is entered into more than one Service Definition Index certain system features may not function as expected. When processing a SIP call the system searches for the URI until the first match is found. If a URI is recorded in two Service Definition Indexes, assigned to two ILGs the SMDR records will only show the calls in one ILG.

**CALL FORWARD ACTIONS (R1.2 and Later)**

When a call, on a SIP trunk, is forwarded out on another trunk, some SIP trunk providers will allow the originating caller's ID to display on the call forward destination phone as the Caller ID, rather than the IPedge URI. However, some providers may not support this.

**Caller ID of Originating Caller Sent**

By default **Number Verification** (Programmed in Enterprise Manager: Trunk > Calling Number > **Calling Number Identification**) is set to **Disable**. If the SIP trunk provider supports this function the call will

forward and the originating caller ID will be sent (The forwarded INVITE will contain the calling phone's PSTN ID in the FROM header). If the SIP provider does not support this function the call will not forward.

**Caller ID Sent by IPedge**

Some SIP Trunk providers require that the IPedge system send a valid, provisioned, calling number. In these cases set the program the IPedge SIP OLG as follows.

In Enterprise Manager or select **Trunk > Calling Number > Calling Number Identification** and set **Number Verification** to **Enable** for the SIP OLG.

The call will forward. The forwarding IPedge system URI will be displayed in the destination phone Caller ID display (The forwarded INVITE will contain the IPedge SIP Trunk URI in the FROM header.).

**Note:** The above discussion is call forward operation not Diversion Headers. IPedge systems do not support diversion header operation or Assert Identity.

**Sending Caller ID From Each Station**

Some SIP trunk providers do not require that the IPedge system send a valid, provisioned, calling number. in these cases set the program the IPedge SIP OLG as follows.

1. In Enterprise Manager select **Trunk > Calling Number > Calling Number Identification** and set **Number Verification** to **Disable** for the SIP OLG.
2. **System > System Data** set Default Calling Number to **Enable**.
3. **Sip Trunking > SIP URI Table** enter the number to be sent as a Main or Sub as determined by the pattern for your SIP provider. Refer to [Table 10-2](#).
4. **Station > Station Assignment** select the **Basic** Tab. Select the station to modify.
5. Enter the same 10-digit calling number used in step 3 above into the **Network Calling Number** field. The value and length of the network calling number must match the SIP URI for each station.

**Note:** If the SIP trunk provider does not support this function the forwarded call will fail.



**SIP TRUNK  
CONFIGURATION  
PATTERNS**

The SIP trunks from service providers typically require IPedge configuration that conforms to one of the patterns shown in [Table 10-4](#) through [Table 10-9](#).

Patterns A and B are the most common. Some SIP trunk providers and the typically used pattern are shown in [Table 10-2](#).

**Table 10-2 SIP Trunks Pattern Reference**

Provider	Pattern	T.38 Support	Notes
123.net	B	Note 1	Enable Network Transfer (Service Def.)
8x8 (Note 2)	Other	Note 1	Contact 8x8 L2 setup for "No Plus"
AccessLine	A	Note 1	
AT&T	Other	Yes	Refer to AT&T IPedge configuration guide
Bright House Networks	B	No	SIP Trunk Option interval must be 0
Broadsoft	Note 3	Note 1	Refer to your SIP Trunk service provider
Broadvox	C	Note 1	Set the SIP URI attribute for additional numbers to SUB. Set the SIP Trunk Option Interval to 180.
Cbeyond (Note 2)	A	No	E911 Emergency destination can not be used on IPedge R1.2 and earlier systems.
Charter	B	Note 1	Contact Charter for a configuration guide.
Firstcomm (Note 2)	B	Note 1	Leave Domain Blank. Enter IP address provided by Firstcomm in SIP Server parameter.
Metaswitch	Note 3	Note 1	Refer to your SIP Trunk service provider
MM Internet	B	Note 1	Enable Network Transfer (Service Def.)
N2Net	B	No	Set the following to the SIP Server IP Address: SIP Trunk Message Option SIP Trunk Register Message From Header Option SIP Trunk Message To Header Option SIP Trunk Register Message to Header Option
Optimum	Other	Note 1	Contact Optimum for a configuration guide
TDS	B	Note 1	
Tierzero	A	Note 1	
Toshiba's SIP Trunking I-VoIP Service	VIPedge SIP Trunk Pattern	No	Refer to <a href="#">Table 10-3</a> . (IPedge systems require software TGZ 1.06.0026 or later)
Twist	A	Yes	
<b>Notes:</b>			
<ol style="list-style-type: none"> <li>1. Check with your SIP service provider about T.38 fax support.</li> <li>2. Field tested</li> <li>3. Refer to your SIP Trunk service provider for the appropriate configuration for this installation. (Sheet 1 of 2)</li> </ol>			
(Sheet 1 of 2)			

**Table 10-2 SIP Trunks Pattern Reference** (continued)

<b>Provider</b>	<b>Pattern</b>	<b>T.38 Support</b>	<b>Notes</b>
Verizon (Note 2)	B	Note 1	Contact Verizon for the configuration guide for settings between IPedge and Acme packets.
Voice Carrier	B	Note 1	Disable Network Transfer (Service Definition)
XO Communications	B	Yes	SIP Trunk Option interval must be 0
<b>Notes:</b> <ol style="list-style-type: none"><li>1. Check with your SIP service provider about T.38 fax support.</li><li>2. Field tested</li><li>3. Refer to your SIP Trunk service provider for the appropriate configuration for this installation. (Sheet 2 of 2)</li></ol> <p style="text-align: center;">(Sheet 2 of 2)</p>			

**SIP Trunk Configuration Tables**

The following tables show the typical SIP trunk configuration patterns. The tables show the data entered in to the IPedge database using Enterprise Manager.

Some SIP Trunk providers may use a trunk number to activate a trunk. That trunk number will be the Main number. All of the rest of the directory numbers will be set to Sub.

**Toshiba's SIP Trunking I-VoIP Service** - The VIPedge SIP trunk portal will provide the Username and Password. Refer to [Table 10-3](#).

**Pattern A - Registration Mode With or Without Authentication** - The SIP provider will typically provide the Username and Password. Refer to [Table 10-4](#).

**Pattern B - No Registration Mode and No Authentication** - The IPedge server requires a static IP address. This address will be used instead of registration. Refer to [Table 10-5](#).

**Pattern C - Registration Mode with or without Authentication** - The SIP provider will typically provide the Username and Password. The Port may be different than 5060 or no SRV records. Refer to [Table 10-6](#).

**Pattern D - No Registration Mode and No Authentication**- The IPedge server requires a static IP address. This address will be used instead of registration. The Port may be different than 5060 or no SRV records. Refer to [Table 10-7](#).

**Pattern E - No Registration Mode With Authentication On** - The SIP provider will typically provide the Username and Password although the provider generally does not require registration. Refer to [Table 10-8](#).

**Other: Different Than Patterns A ~ E** - Consult with your SIP trunk provider and Toshiba's Technical Support group. Refer to [Table 10-9](#).

Table 10-3 Toshiba's SIP Trunking I-VoIP Service Pattern

Parameter	Entry
<b>Trunk &gt; SIP Trunking &gt; Service Definition</b>	
Registration Mode	Client
Domain Name	sip.outbound.vipedge.com
SIP Server	Leave blank
Primary Voice Packet Configuration	1
Primary Audio Codec	G711
Secondary Voice Packet Configuration	1
Secondary Audio Codec	G729
Connection to Server	Manual (IPedge systems)
SIP Trunk Option Interval	60
SIP Trunk Message Option	FQDN (Default)
SIP Trunk Message to Header Option	FQDN (Default)
SIP Trunk Register Message From Header Option	FQDN (Default)
SIP Trunk Register Message To Header Option	FQDN (Default)
<b>Trunk &gt; SIP Trunking &gt; Service URI</b>	
The following values are obtained from the VIPedge SIP Trunk Admin portal.	
<b>Trunk Number</b>	
SIP URI	37412345 (example trunk number)
SIP URI User Name	37412345 (example trunk number)
SIP URI Password	1234 (example trunk password)
SIP URI Attribute	Main
<b>DID Telephone Numbers</b>	
SIP URI	19495833001 (1+10 digits) (TN example)
SIP URI User Name	37412345 (example trunk number)
SIP URI Password	1234 (example trunk password)
SIP URI Attribute	SUB

Table 10-4 Pattern A - Registration Mode With or Without Authentication

Parameter	Entry
<b>Trunk &gt; SIP Trunking &gt; Service Definition</b>	
Registration Mode	Client
Domain Name	SIP Provider IP address or domain name
SIP Server	Use an OutBound proxy if the SIP Provider requires
Primary Voice Packet Configuration	1
Primary Audio Codec	G729 or G711 (Consult your SIP provider.)
Secondary Voice Packet Configuration	1
Secondary Audio Codec	G711 or G729 (Assign the codec not used for as the primary.)
Network transfer	Typically Disabled (Test transfer with on and off to see which works.)
SIP Trunk Option Interval	0
SIP Trunk Message Option	Typically FQDN
SIP Trunk Message to Header Option	Typically FQDN
SIP Trunk Register Message From Header Option	Typically the same as SIP Trunk Message Option
SIP Trunk Register Message To Header Option	Typically the same as SIP Trunk Message to Header Option
<b>Trunk &gt; SIP Trunking &gt; Service URI</b>	
<b>Primary Number</b>	
SIP URI	9495833000 (example only)
SIP URI User Name	9495833000 (example only)
SIP URI Password	1234 (example only)
SIP URI Attribute	Main
<b>Additional Numbers</b>	
SIP URI	9495833001 (example only)
SIP URI User Name	9495833000 (example only)
SIP URI Password	1234 (example only)
SIP URI Attribute (When Reg mode is Client - Use sub if you do not want the number to register)	Main

Table 10-5 Pattern B - No Registration Mode and No Authentication

Parameter	Entry
<b>Trunk &gt; SIP Trunking &gt; Service Definition</b>	
Registration Mode	None
Domain Name	SIP Provider IP address or domain name
SIP Server	Use an OutBound proxy if the SIP Provider requires
Primary Voice Packet Configuration	1
Primary Audio Codec	G729 or G711 (Consult your SIP provider.)
Secondary Voice Packet Configuration	1
Secondary Audio Codec	G711 or G729 (Assign the codec not used for as the primary.)
Network transfer	Typically Disabled (Test transfer with on and off to see which works.)
SIP Trunk Option Interval	60
SIP Trunk Message Option	Typically FQDN
SIP Trunk Message to Header Option	Typically FQDN
SIP Trunk Register Message From Header Option	Typically the same as SIP Trunk Message Option
SIP Trunk Register Message To Header Option	Typically the same as SIP Trunk Message to Header Option
<b>Trunk &gt; SIP Trunking &gt; Service URI</b>	
<b>Primary Number</b>	
SIP URI	9495833000 (example only)
SIP URI User Name	
SIP URI Password	
SIP URI Attribute	Main
<b>Additional Numbers</b>	
SIP URI	9495833001 (example only)
SIP URI User Name	
SIP URI Password	
SIP URI Attribute (When Reg mode is Client - Use sub if you do not want the number to register)	Main

**Table 10-6 Pattern C - Registration Mode with or without Authentication**

The Port may be different than 5060 or no SRV records

Parameter	Entry
<b>Trunk &gt; SIP Trunking &gt; Service Definition</b>	
Registration Mode	Client
Domain Name	IP or domain name
SIP Server	IP or domain name: 5060 (Your SIP provider may use a different port)
Primary Voice Packet Configuration	1
Primary Audio Codec	G729 or G711 (Consult your SIP provider.)
Secondary Voice Packet Configuration	1
Secondary Audio Codec	G711 or G729 (Assign the codec not used for as the primary.)
Network transfer	Typically Disabled (Test transfer with on and off to see which works.)
SIP Trunk Option Interval	0
SIP Trunk Message Option	Typically FQDN
SIP Trunk Message to Header Option	Typically FQDN
SIP Trunk Register Message From Header Option	Typically the same as SIP Trunk Message Option
SIP Trunk Register Message To Header Option	Typically the same as SIP Trunk Message to Header Option
<b>Trunk &gt; SIP Trunking &gt; Service URI</b>	
<b>Primary Number</b>	
SIP URI	9495833000 (example only)
SIP URI User Name	9495833000 (example only)
SIP URI Password	1234 (example only)
SIP URI Attribute	Main
<b>Additional Numbers</b>	
SIP URI	9495833001 (example only)
SIP URI User Name	9495833000 (example only)
SIP URI Password	1234 (example only)
SIP URI Attribute (When Reg mode is Client - Use sub if you do not want the number to register)	Main

**Table 10-7 Pattern D - No Registration Mode and No Authentication**

The Port may be different than 5060 or no SRV records

Parameter	Entry
<b>Trunk &gt; SIP Trunking &gt; Service Definition</b>	
Registration Mode	None
Domain Name	IP or domain name
SIP Server	IP or domain name: 5060 (Your SIP provider may use a different port)
Primary Voice Packet Configuration	1
Primary Audio Codec	G729 or G711 (Consult your SIP provider.)
Secondary Voice Packet Configuration	1
Secondary Audio Codec	G711 or G729 (Assign the codec not used for as the primary.)
Network transfer	Typically Disabled (Test transfer with on and off to see which works.)
SIP Trunk Option Interval	60
SIP Trunk Message Option	Typically FQDN
SIP Trunk Message to Header Option	Typically FQDN
SIP Trunk Register Message From Header Option	Typically the same as SIP Trunk Message Option
SIP Trunk Register Message To Header Option	Typically the same as SIP Trunk Message to Header Option
<b>Trunk &gt; SIP Trunking &gt; Service URI</b>	
<b>Primary Number</b>	
SIP URI	9495833000 (example only)
SIP URI User Name	
SIP URI Password	
SIP URI Attribute	Main
<b>Additional Numbers</b>	
SIP URI	9495833001 (example only)
SIP URI User Name	
SIP URI Password	
SIP URI Attribute (When Reg mode is Client - Use sub if you do not want the number to register)	Main



Table 10-8 Pattern E - No Registration Mode With Authentication On

Parameter	Entry
<b>Trunk &gt; SIP Trunking &gt; Service Definition</b>	
Registration Mode	None
Domain Name	SIP Provider IP address or domain name
SIP Server	Use an OutBound proxy if the SIP Provider requires
Primary Voice Packet Configuration	1
Primary Audio Codec	G729 or G711 (Consult your SIP provider.)
Secondary Voice Packet Configuration	1
Secondary Audio Codec	G711 or G729 (Assign the codec not used for as the primary.)
Network transfer	Typically Disabled (Test transfer with on and off to see which works.)
SIP Trunk Option Interval	60
SIP Trunk Message Option	Typically FQDN
SIP Trunk Message to Header Option	Typically FQDN
SIP Trunk Register Message From Header Option	Typically the same as SIP Trunk Message Option
SIP Trunk Register Message To Header Option	Typically the same as SIP Trunk Message to Header Option
<b>Trunk &gt; SIP Trunking &gt; Service URI</b>	
<b>Primary Number</b>	
SIP URI	9495833000 (example only)
SIP URI User Name	9495833000 (example only)
SIP URI Password	1234 (example only)
SIP URI Attribute	Main
<b>Additional Numbers</b>	
SIP URI	9495833001 (example only)
SIP URI User Name	9495833000 (example only)
SIP URI Password	1234 (example only)
SIP URI Attribute (When Reg mode is Client - Use sub if you do not want the number to register)	Main

Table 10-9 Other: Different Than Patterns A ~ E

Parameter	Entry
<b>Trunk &gt; SIP Trunking &gt; Service Definition</b>	
Registration Mode	Consult with your SIP Trunk provider.
Domain Name	
SIP Server	
Primary Voice Packet Configuration	
Primary Audio Codec	
Secondary Voice Packet Configuration	
Secondary Audio Codec	
Network transfer	
SIP Trunk Option Interval (in a few cases use 0 when reg mode is none)	
SIP Trunk Message Option	
SIP Trunk Message to Header Option	
SIP Trunk Register Message From Header Option	
SIP Trunk Register Message To Header Option	
<b>Trunk &gt; SIP Trunking &gt; Service URI</b>	
<b>Primary Number</b>	
SIP URI	Consult with your SIP Trunk provider.
SIP URI User Name	
SIP URI Password	
SIP URI Attribute	
<b>Additional Numbers</b>	
SIP URI	Consult with your SIP Trunk provider.
SIP URI User Name	
SIP URI Password	
SIP URI Attribute (When Reg mode is Client - Use sub if you do not want the number to register)	

**SIP RESPONSE MESSAGES**

SIP response messages usually come from one of two sources:

- The SIP provider
- The IPedge server

**From the SIP Provider**

The conditions causing these messages may require consultation with the SIP trunk service provider to resolve.

- **401** - Typically a challenge from the SIP service provider. Check the the user name and password set in the IPedge Service URI table.
- **403** - Typically a message that the URI may have an incorrect number of digits set in the IPedge Service URI table or:

SIP Trunk Message options and SIP Trunk Register Message From Header option set in the Service Definition table is incorrect. Sometimes occurs when set to FQDN but should be set to IPU IP address (IPedge server IP address).

- **501** - Typically occurs when the Registration Mode is incorrect (change Client to None).

**From the IPedge Server**

The conditions causing these messages generally indicate incomplete or missing database programming.

- **403** - The DN digits sent by the SIP trunk provider do not match the URI table entries. For example 9495833000 is sent from the SIP trunk provider but this number is not in the URI table or was entered as 5833000.
- **403** (when an Adtran Gateway attempts a call to the IPedge system) - The From Header Host Type must be set to Local. Refer to the Adtran gateway configuration guide.
- **404** - The DID number is missing (Trunk > DID programming).
- **480** - The DID number in the IPedge database is incorrect. Also caused if the destination IPT is: unplugged, set to DND, no System Call Forward is assigned, or is otherwise unreachable.
- **503** - Not enough channels assigned or all channels are in use.

**Other Indicators**

- If a call drops at 32 seconds enable the NAT Transversal and MRS (R1.3 and later) or use a public IP address for the IPedge server (R1.2 and later). Refer to the NAT Traversal chapter.
- If there is no audio on a call check the IPT firmware version.
- If there is no MOH or no 3-way conference check the Media Server configuration.
- Jitter, Echo, Voice Quality issues; check bandwidth, router settings, perform a network assessment.
- SIP Trunks and voicemail were working have stopped working. Check for network security problems.

This page is intentionally left blank.

# Chapter 11 – Gateways

---

## INTRODUCTION

The *IPedge* is an all IP telephony system. To interface with analog telephones or analog CO trunks, PRI or other digital trunks a gateway is required. Refer to the setup and installation instructions for the specific gateway you are installing.

The procedures for manually programming AudioCodes and Adtran gateways are found in the *IPedge Accessories Manual*.

This page is intentionally left blank.

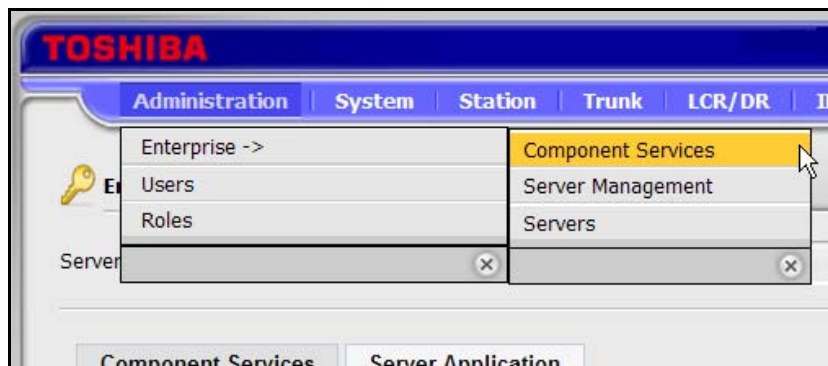
# Chapter 12 – Net Server

---

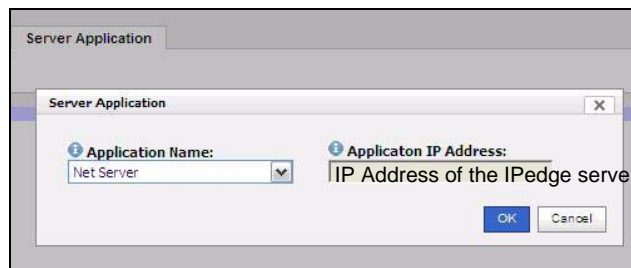
Net Server is pre-installed on the IPedge system and can be activated using IPedge Enterprise Manager. Add Net Server to Enterprise Manager and configure the IO port in the IPedge system. After applying the license, Net Server is ready to be used. If further configuration of Net Server is necessary for server based Call Manager configuration, please see Net Server administration section [page 12-2](#) for details.

## ADD NET SERVER

1. Using your web browser, enter the Enterprise Manager application IP address.
2. Select **Administration > Enterprise > Component Services**.



3. Select the Primary Node Server.
4. Click the **Server Application** tab.
5. Click on the New icon.
6. Select Net Server from the Application Name list (shown below).



7. Add the IP Address of the IPedge server, do not enter 127.0.0.1 as the address.
8. Click on **OK**.
9. For multi-node systems:
  - A. Select a Member node from the Server pull-down list.

**SETUP THE I/O PORT**

- B. Add the Messaging application.
- C. Enter the IP address of the IPedge server that will be running the application.
- D. Repeat A through C for each member node.

1. Using Enterprise Manager, go to **System > I/O Device**.
2. Select the Primary Server.
3. Click the **New** icon.
4. Choose any one of available CTI#0~8 for the Logical Device No.
5. Set the Application Type to Server
6. Server Port No. must be **1100** for Net Server.

**Important!** Do not configure any other application including Attendant Console to use Port 1100.

7. Click the **Save** icon.

**NET SERVER ADMINISTRATION**

Net Server administration allows the administrator to configure the Net Server to control the behavior of Call Manager client application. It is designed to provide the basic operations of Call Manager without any configuration. If the administrator requires the advanced operations such as pushing settings to the clients, Net Server administration needs to be used.

**Survivability**

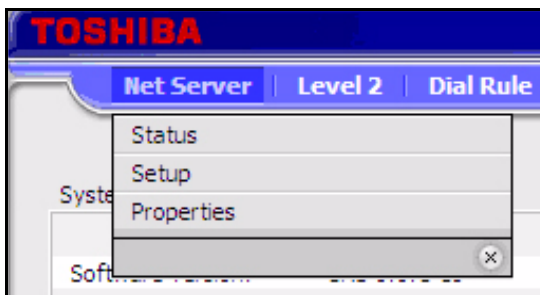
Net Server and Call Manager survivability are described in the IPedge Survivability Feature Description, available on Toshiba's FYI website.

**To access Net Server**

Using Enterprise Manger, go to Application > Net Server menu.

**NET SERVER MENU**

Net Server menu provides access to the basic setup for Net Server application on IPedge server.



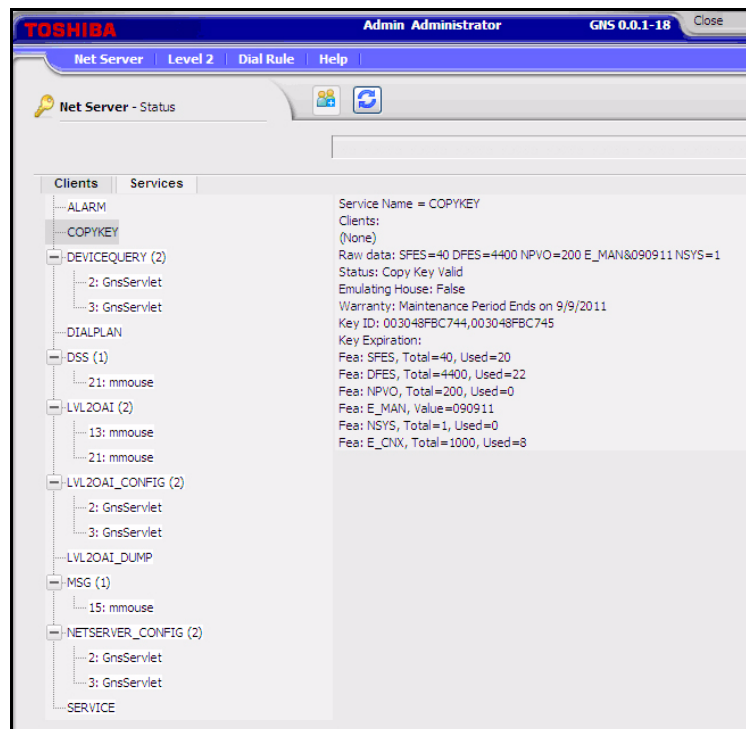


**Status** The Status sub menu provides real time information on the Net Server.

**Clients Tab** Clients tab shows the status of all the client applications that are connected to the Net Server. It includes all the component applications that are parts of Net Server and all the client Call Manager applications that are connected to the Net Server.

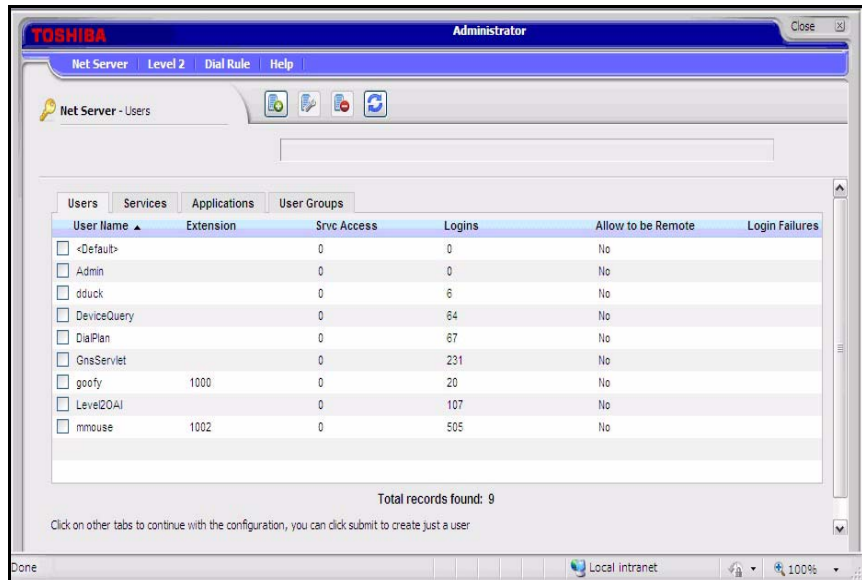


**Services Tab** Services tab shows the real time status of system component services running.



**Setup** Setup sub menu allows the administrator to manage client users, service components, applications, and groups.

Users tab is used to manage the login information of the client applications. Clients can be automatically added or can be added/modified from this tab.

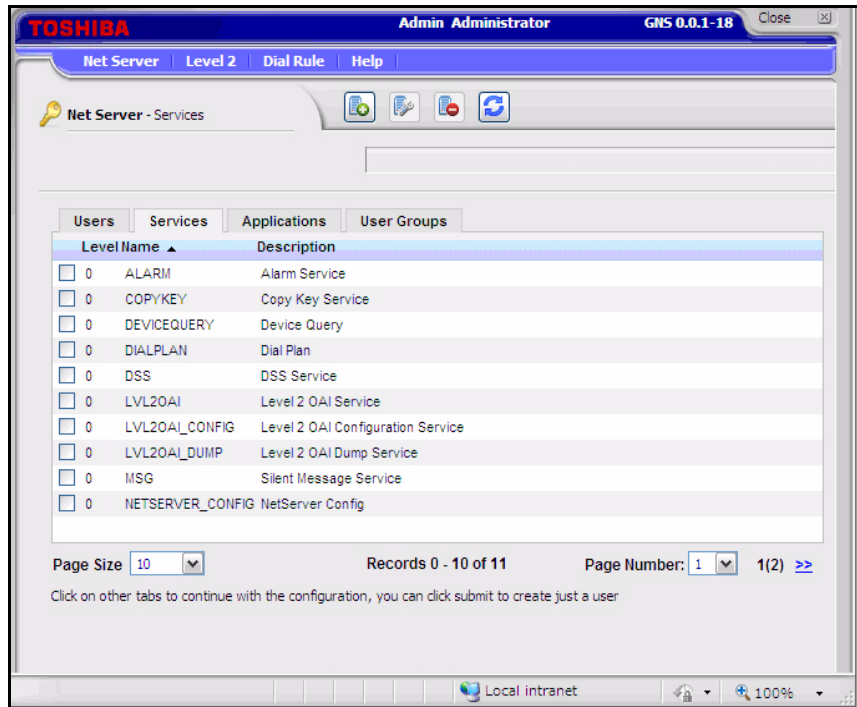


When you Add or Edit a checked entry, data can be entered from the following screen.

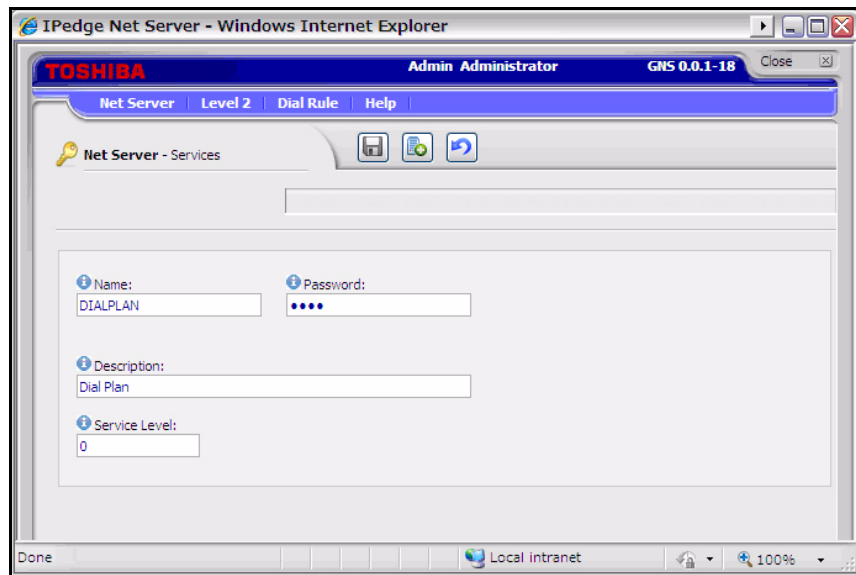
Name	Description
User Name	Name of the user to use for Net Server login
Password	Password used for Net Server login
Extension	Directory Number (DN) of extension that the user controls
Service Access	This is a number that determines which services the client has access to. Each service has a Service Level number, and a client will have access to all services whose Service Level is less than or equal to the client's service level access number.
Logins	Count of logins
Consecutive Login Failures	Count of consecutive login failures. Can be edited to reset the count.
Login Failures	Count of login failures. Can be edited to reset the count.
Last Login Failed on	Date and time of the last login failure
Change Password	Yes to allow the user to change the password
Allow to Remote	Yes to allow the user to connect remotely using the remote port (TCP port:8768)
Group Membership	A list of defined Groups is listed, Placing a check mark in the appropriate Group Name assigns that user to that Group. New Group can be created from User Group tab.

Services Tab Use the Services tab to manage the component services running under Net Server.

It defines which services are on the server and what clients can use them. Services are automatically defined when they are installed, and do not need to be modified.



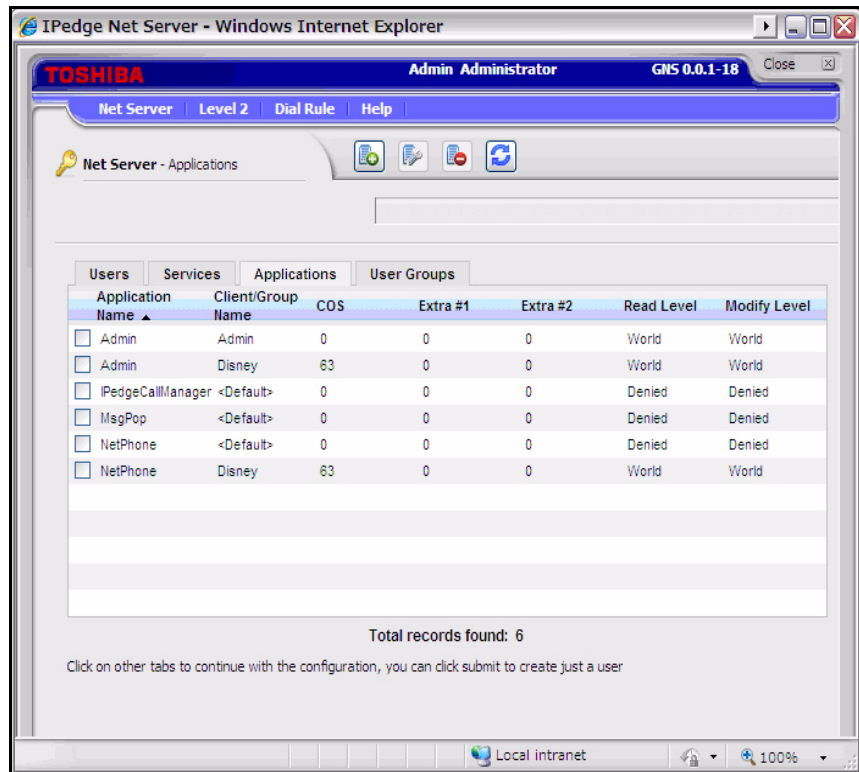
When you Add or Edit a checked entry, data can be entered from the following screen.



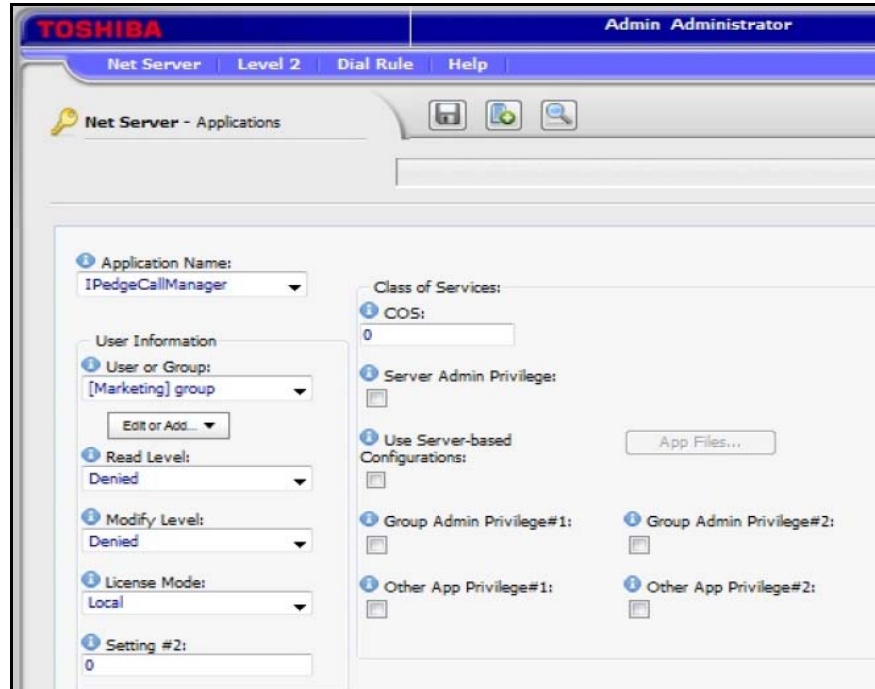
Field	Description
Name	Service name which must be unique in the system
Password	Password for the service to login to Net Server. Typically, it should not be changed.
Description	Description of the service
Service Level	Service Level determines which clients can access this service. Each client has a service level access number, and a client will have access to all services whose Service Level is less than or equal to the client's service level access number.

**Application Tab** The Application tab defines the users for each application and allows you to assign a policy based on the user or the group. Please see Group tab section for the specific information on the group policies.

See the [“Server Based Call Manager Configuration”](#) on page 12-19 for setting up the server based configuration for Call Manager.



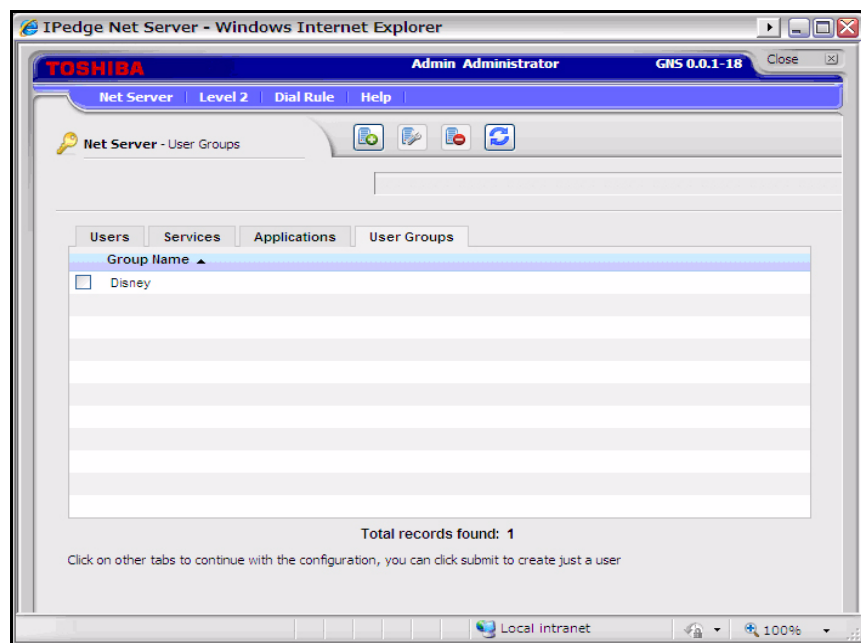
When you Add or Edit a checked entry, data can be entered from the following screen.



Field	Description
Application Name	Name of the application
User or Group	Usually, the client name of the user is shown (see Clients). When it is set to <Default> (or leaving it blank) the settings for the Default User can be defined. It can be used to define the settings of typical users while any additional clients that need settings other than those of the Default User can be defined separately. Each user can be assigned to a group by setting this number (application may use this to standardize settings/features for each group).
Read Level	This defines the access privileges for being able to read information about the application. The settings are Denied, Self, Group, or World.
Modify Level	This defines the access privileges for being able to modify the information about the application. The settings are Denied, Self, Group, or World.
License Mode	Specify the license that users in the group should use: Local – Use Advanced or Standard license specified during the installation. Advanced – Use Advanced license. Standard – Use Standard license. Auto – Try Advanced license first, and if not available, try standard license.
Setting #2	Reserved for future use.
COS	Define a COS number. These options are used to control the user access privileges. COS ranges from 0 to 63 is the sum of values assigned to each privilege shown below.
Server Admin Privilege	Enables the user to do administration of server configuration files. (value: 1)

Field	Description
Use Server-based Configuration	When enabled, user will get the program configuration settings from the server specified by application files. If this is disabled, the user will get configuration settings from the local PC. (value: 2)
Group Admin Privilege#1/2	Determines if this user can perform functions for the group (unique to each application). (value: 4/8)
Other App Privilege#1/2	Determines if this user can perform other functions (unique to each application). (value: 16/32)

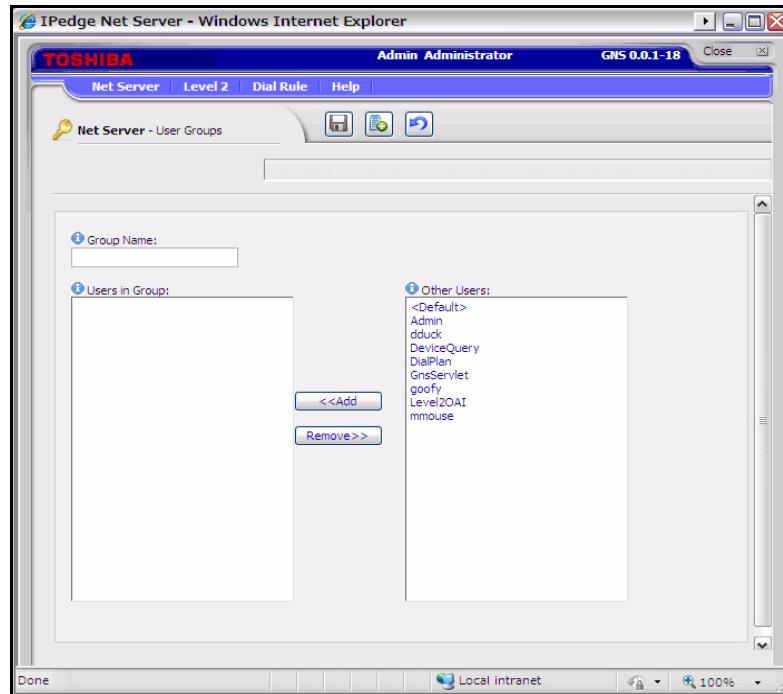
User Groups Tab      User Groups tab defines the group of users to apply the common settings to multiple users.



When you Add or Edit a checked entry, data can be entered from the following screen.

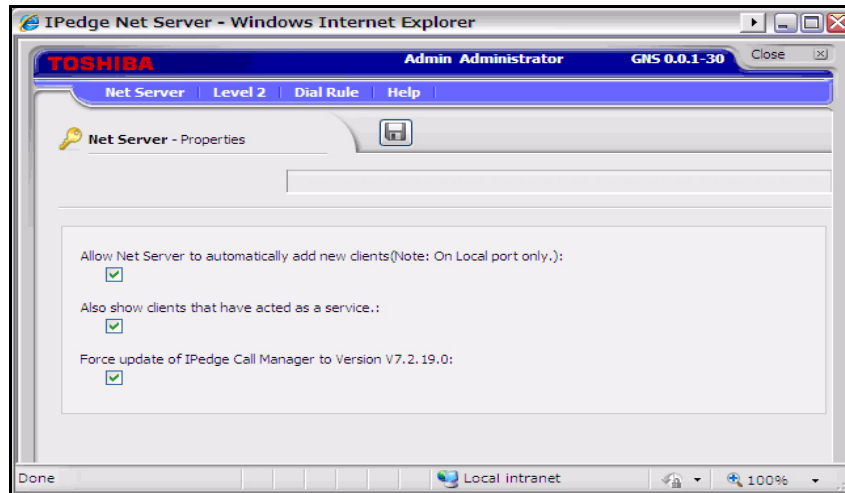
For an example refer to [“Create User Groups” on page Chapter 12 –19](#)





Field	Description
Group Name	Name of the group
Users in Group	List of users that are currently included in the group. A user can be removed from the group by selecting the user and clicking Remove.
Other users	List of users that are not currently in the group. A user can be added by electing the user and clicking Add.

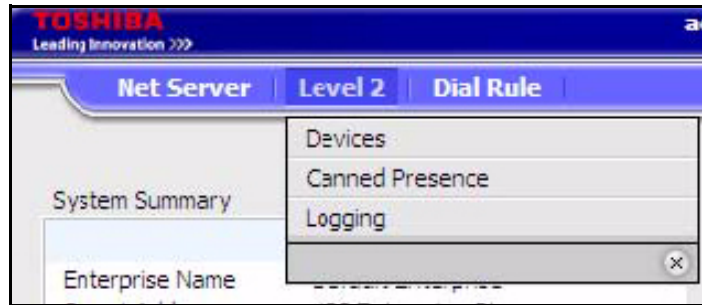
Properties Tab Properties tab is used to configure the Net Server.



Item	Description
Allow Net Server to automatically add new clients (Note: On local port only)	Check this to automatically add users when they connect to the Net Server first time. It is primarily intended to allow Call Manager users to create a user name and password in the system when they login the first time. The user will take on the default parameters for a user of that application. Do not enable this option if the administrator should control the access for each user, this option should not be enabled. To manually create or modify users go to the "Clients Tab".
Also show clients that have acted as a service	Control whether to show a component that is acting as a server in the client list. When checked, the Net Server Administrator / Users tab will show the main services running like Dial Plan, Level2OAI. When un-checked, it only shows the Call Manager Users, and Admin Accounts.
Force update of IPedge Call Manager to Version Vx.x.x.x	Whether to upgrade the Call Manager installed on the client with the one in the server. Version shows the actual version number of the Call manager on the server. Please see Server Based Call Manager Upgrade section.

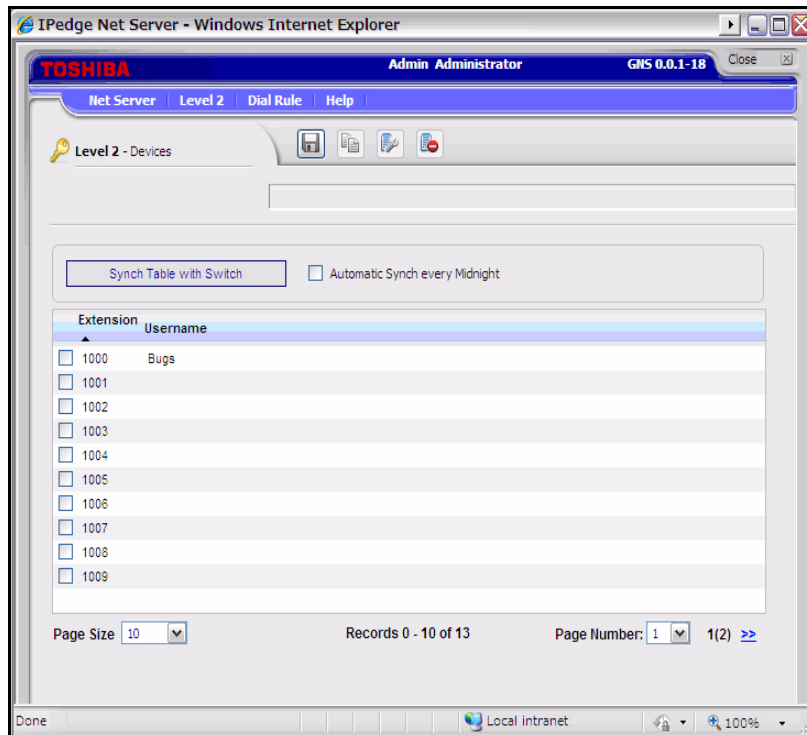
LEVEL 2 MENU

Level2 menu allows the administrator to configure various items managed by Level2 which processes the Computer Telephony Integration with the IPedge system.



Devices Menu

Device menu manages the device table which provides an Extension Directory for Call Manager.



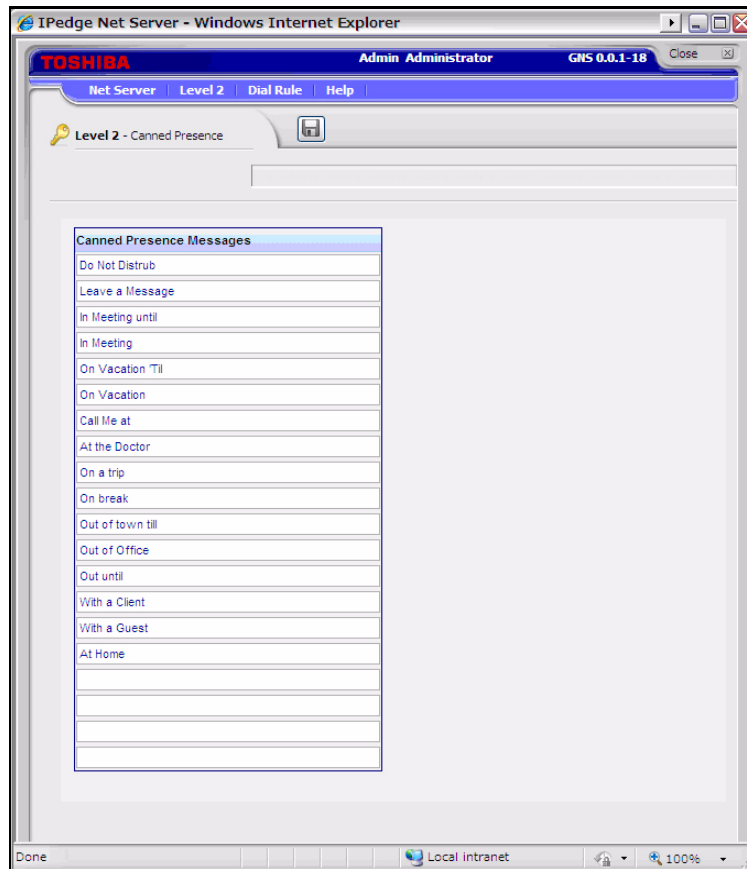
Device Table

Device table can be created manually by creating or copying an entry, or it can be automatically populated by using Synch Table with Switch.

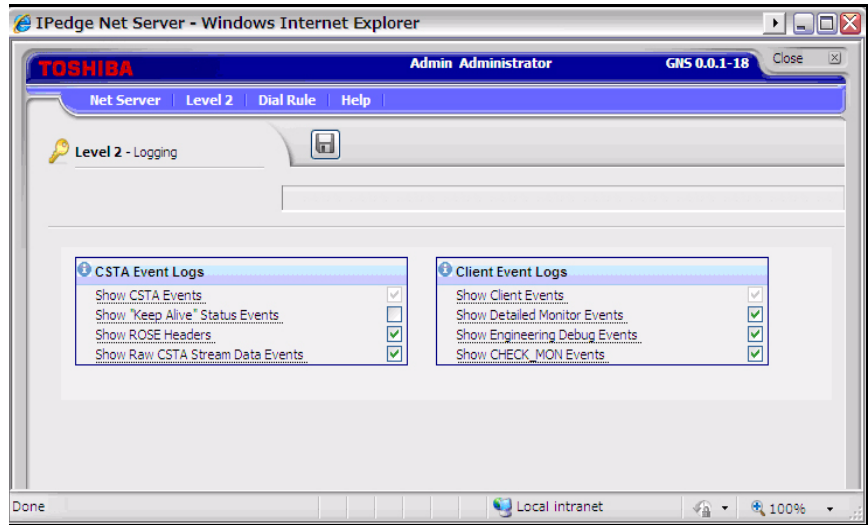
It is also possible to automatically update every midnight by checking Automatic Synch Every Midnight check box.

Canned Presence (Message)

Canned Presence (Message) menu enables the administrator to define messages used by Call manager for the additional information on the presence status. System standard default messages are defined, and the administrator can change them. Twenty different messages are possible.



Logging      Logging menu can control the level of trace information for the problem investigation. All items are checked by default and do not have to be changed unless instructed to so by Toshiba Technical Support.

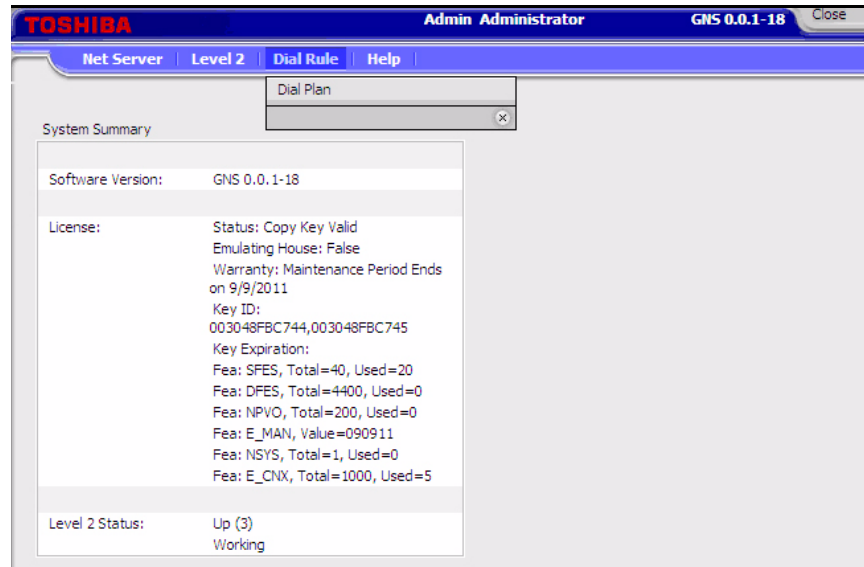


**Dial Rule Menu**

Dial Rule Menu allows the administrator to define the dialing rule to be applied automatically when the application such as Call Manager makes a call.

**Dial Plan**

Dial Plan sub menu defines how the system interprets the dialing string. When the Use SERVER Dial Plan is checked in the Preference in Call Manager, dialing digits from Call Manager are interpreted based on the rule defined in the Dial Plan.



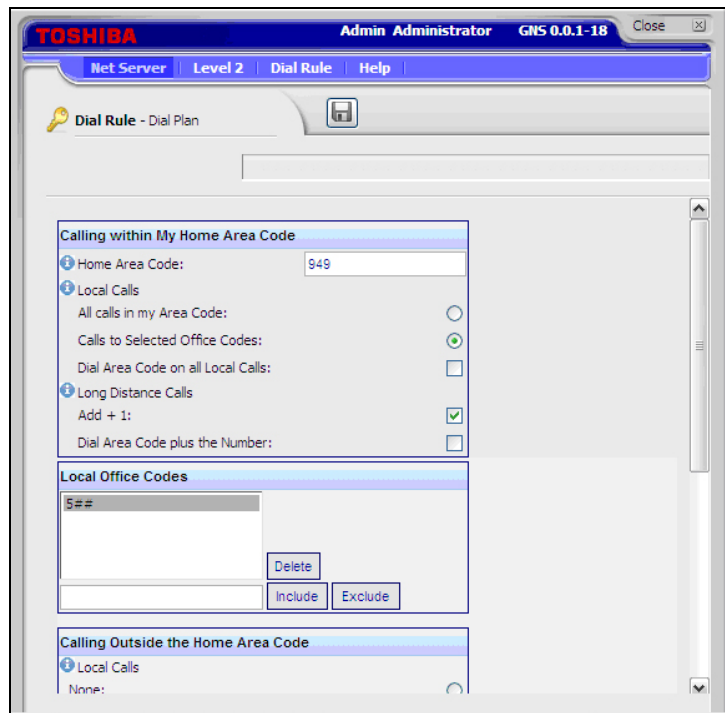
Each area of the US uses a different set of rules for determining which calls are local or long distance calls. The opening pages of your phone book are a good source for how to dial different numbers in your area. Your System Administrator will also need to define access codes for reaching outside lines. These pages generally define how to dial different areas and provide a listing of prefix codes for the local calling areas.

Three typical examples are:

- Phoenix, AZ – all calls within the “602”, “480”, and “623” area codes are considered to be local calls, while all calls outside those area codes are considered long distance.
- Santa Fe, NM – calls to some office codes within the “505” area code are considered to be local calls, while other calls to the “505” area code are considered long distance.
- Atlanta, GA – all calls to area codes “770” are considered to be local calls while some calls to the “404” and “678” area codes are also considered to be local calls.

**Calling Within My Home Area Code**

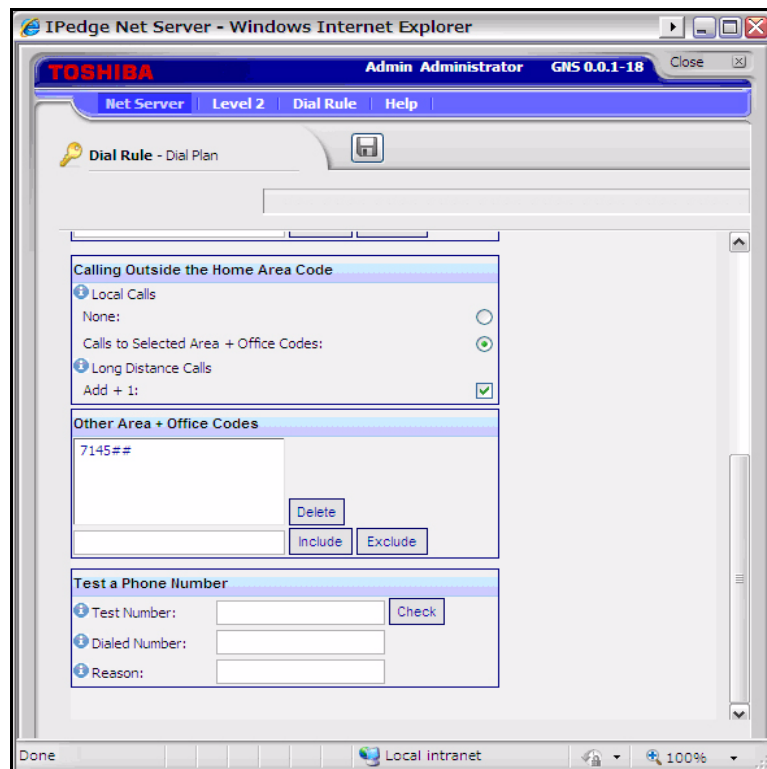
- Home Area Code – Set this to the Area code where the phone is located. This will be used by Call Manager to determine which dialed calls are within your home area code and when searching a contact manager (reverse screen-pop) the dialed number will need the area code included, i.e. Microsoft Outlook.
- All calls in my Area Code – Select All Calls in my Area Code if all calls with the same area code can be considered as local calls.
- Calls to Selected Office Codes – Select Calls to Selected Office Codes when only certain office codes in the same area code are considered to be local calls. If this option is selected, the following office code entry screen is displayed.
  - To Add Local Prefix Codes – Enter the prefix code and click Include. The wild card character # can be entered at the end of a prefix code entry to represent a range of codes. For example, 75# would represent all codes 750 to 759; and 7## would represent codes 700 to 799. If certain numbers need to be excluded from the wild card range, specify the number and click Exclude.
  - To Delete Local Prefix Codes – Highlight a prefix entry and click Delete. The delete button removes the entire entry from the list, therefore if the entry has a wild card, then it removes all codes represented by the wild card.
- Dial Area Code on Local Calls – Enable this feature in areas such as Atlanta, where full 10 digit number must always be used (include the area code) even when the call is local. Most areas of the US, local calls do not include the area code and dial only 7 digit numbers for local calls. Any number dialed from another program or hot key dialing will be down to its base 7 digits by removing the Home Area Code before it is dialed.



- Add+1 – Check the box if you need to dial a leading 1 before the number for calls within your Home Area Code.
- Dial Area Code Plus the Number – Check the box when the home area code is also to be dialed.

### Calling Outside the Home Area Code

- Local calls
  - Select None when a different area code is always a long distance call.
  - Select Calls to Selected Area+Office codes when certain area codes are considered to be the local call area. If this is selected, the following area code entry screen is displayed.
    - To Add Local Area+Prefix Codes – Enter the six digit area+prefix code, then click Add. The wild card character # can be entered at the end of a prefix code entry to represent a range of codes. For example, 602### would represent all prefix codes in area code 602. If certain numbers need to be excluded from the wild card range, enter the number and click Exclude.
    - To Delete Local Area+Prefix Codes – Highlight a prefix entry, then click Delete. The delete button removes the entire entry from the list, therefore if the entry has a wild card, then it removes all codes represented by the wild card.





- For Long Distance Calls add +1 – Check the box when you need to have a leading one (1) added when making long distance calls outside your home area code.
- Click Save when done.

#### Test a Phone Number

Test a Phone Number – Dialing plans can become complex. Use these boxes to enter different telephone numbers and check to see the number that will be dialed. The dialed number should be identical to what you need to dial when using your phone to manually dial.

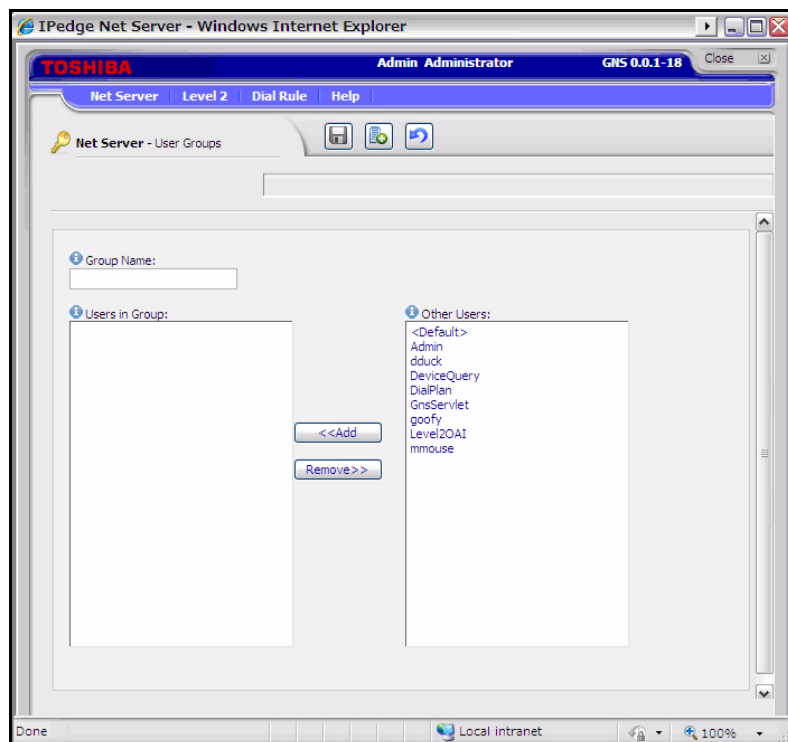
### Server Based Call Manager Configuration

Creating a Server-based Class of Service for Call Manager begins in the group creation of Net Server administration, followed by creating your configuration on the Call Manager Admin, then publishing the configuration files to the Net Server.

The steps below show an example of creating two user groups, users and administrators, and assigning a class of service to each. Multiple groups can be assigned, each with its own configuration created by the Administrator common to that group.

#### Create User Groups

1. Use Net Server > Setup and click User Groups tab.
2. Click Add button
3. Type in a group name to represent the Call Manager administrator (CallManager Admin in this example) and click Save.

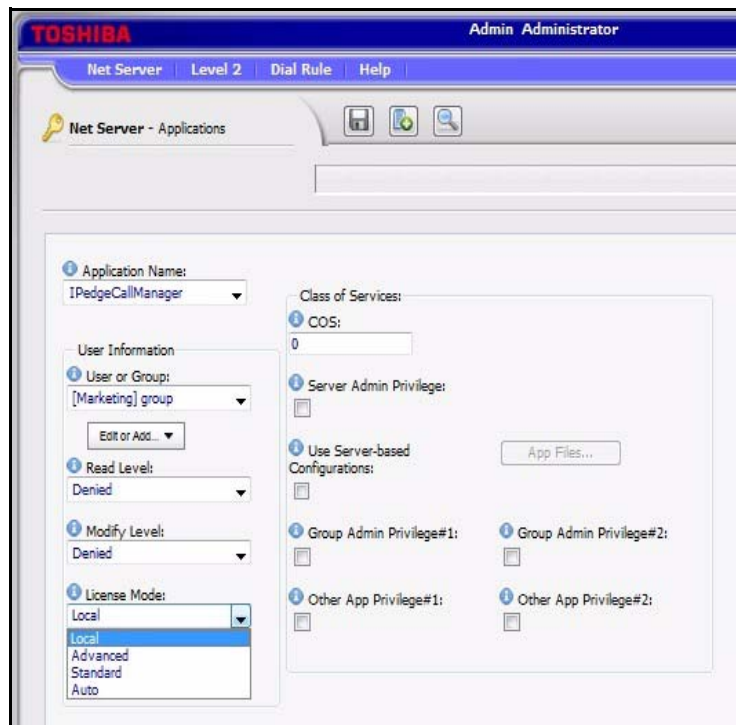


4. Click Add button again, and this time, type in a name to represent the Call Manager Users' group (Call Manager User in this example).
5. Repeat above steps for other groups if necessary.

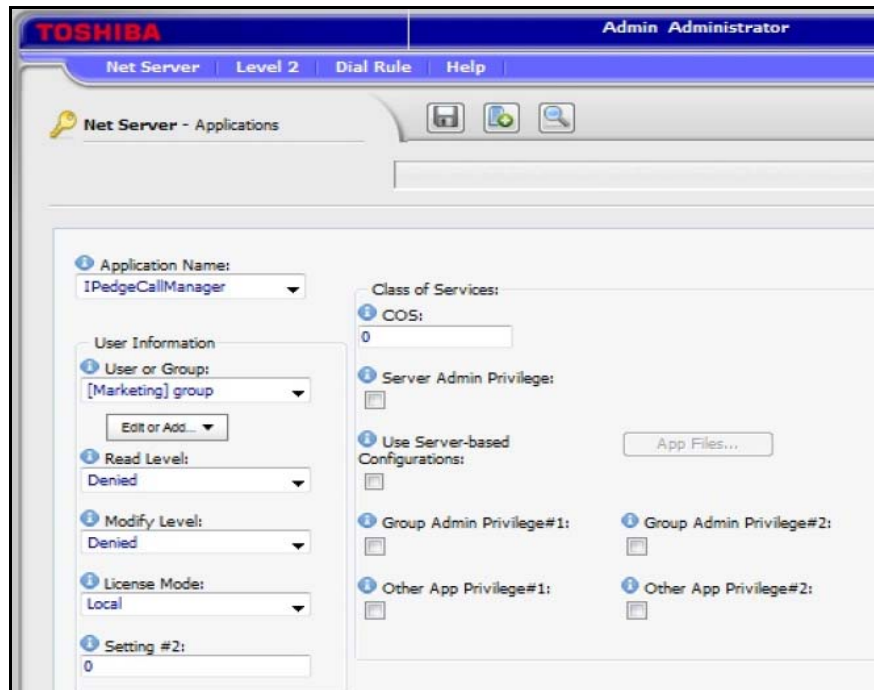
**Assign Users to Call Manager Application**

By assigning Groups to the Call manager application enables you to assign a common “Class of Service” and “Configurations” for all users in a group. Individuals that are not part of a group can also be assigned as a Call Manager application user.

1. Select the Applications tab, and click Add icon.
2. Select the Call Manager in Application Name drop down.
3. Select the administrator group (ex. Call Manager Admin) from the drop down menu for User or Group.
4. Select World for both Read Level and Modify Level from their respective drop-down boxes.
5. Place a checkmark in the Server Admin Privilege checkbox.
6. Select the License Mode.
7. Click Save icon.



8. Click Add icon.
9. Select the Call Manager in Application Name drop down.
10. Select the Call Manager User Group created previously from the User or Group drop-down box.
11. Select Denied for both the Read Level and Modify Level from their respective drop-down boxes.
12. Uncheck the Server Admin Privilege checkbox.
13. Select the License Mode.
14. Place a checkmark in the Use Server-based Configurations checkbox.
15. Click Save icon.

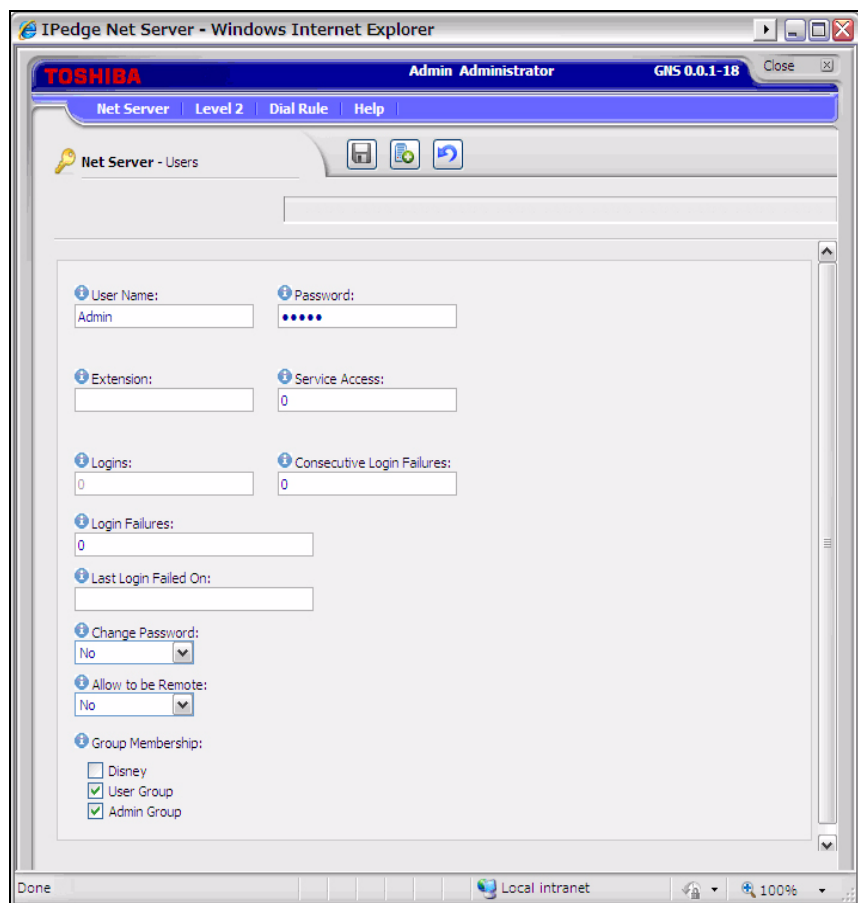


16. Repeat the preceding steps to add any remaining Call Manager user groups.
17. Default in User or Group can be used to setup the default settings for all users that are not included in any group or individual.
18. To exclude certain users from the Default, choose an individual user.

## Assign Users to User Groups

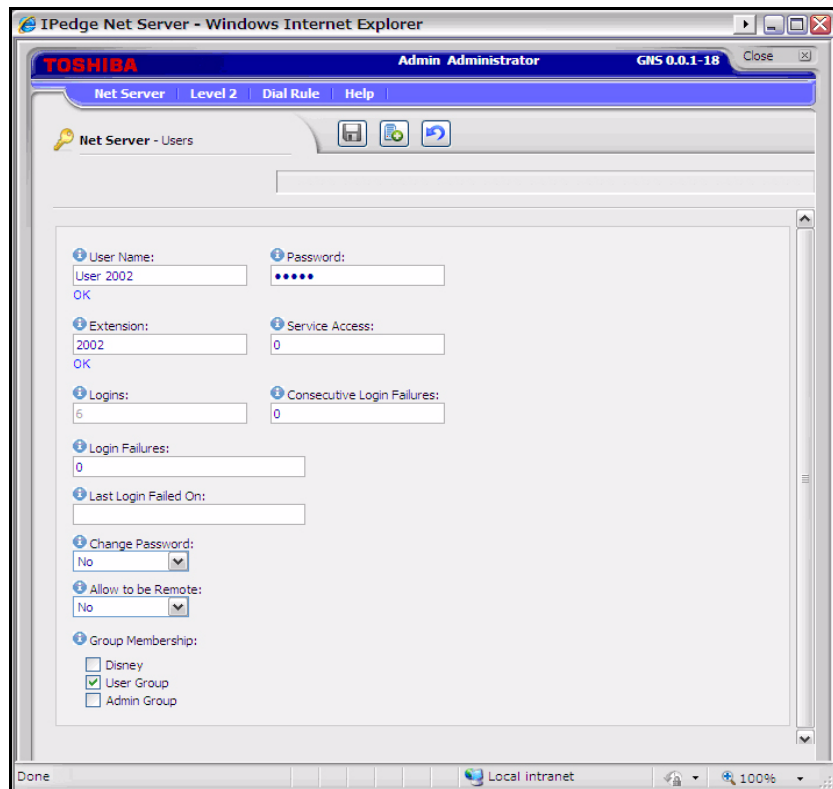
### To Assign Users as Call Manager Administrators

1. Use Net Server menu > Setup, then Users tab.
2. Check the user who needs to be a Call manager administrator and click Edit icon.
3. Place a checkmark in both the Admin and Users groups as is shown in the screen below.
4. Click Save icon.
5. Repeat for other Call Manager users to be assigned as Administrators.



**To assign Users as Call manager Users**

1. Check the user who is a Call Manager user and click Edit icon.
2. Place a checkmark in the User group only as is shown in the following screen:
3. Click Save icon.
4. Repeat for other Call Manager users to be assigned as Users.

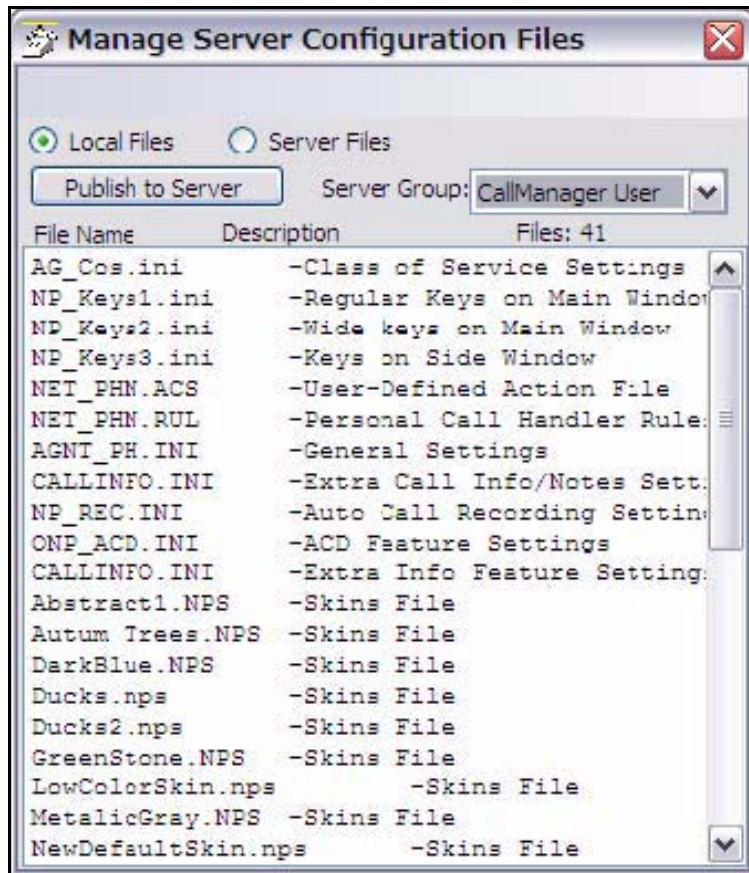


Create Configuration Files using Admin Call Manager

1. Restart the Administrator's Call manager if it is running
2. Set up the buttons, Call Handler rules, skins, etc. as you would like the users' Call Manager to be configured. Use the Call Manager User's Guide as needed for how to configure Call Manager. To access the user guide click on the SCM button in the Call Manager banner and select **Help**.

### To Change the COS Configuration

1. Once the configuration is done, using Call Manager, select Tools > Publish.
2. Select the Server Group: Call manager User (the group created in Net Server).



3. Left-click on the file name "AG\_COS.INI" to highlight it.
4. Right-click on the highlighted file and choose Edit. The following window is shown. Change each value from =Y to =N that should be set and controlled from the Server. Any items left using the =Y setting will allow the user to change and keep those settings on that local PC. The file from the server will not be downloaded.
5. Click File > Save to save the changes. Close the "AG\_COS.INI" file.



The image shows a Notepad window titled "AG\_COS.INI - Notepad". The window contains the following configuration text:

```
[[cos]
Chg_Actions=Y
Chg_Rules=Y
Chg_StdKeys=Y
Chg_PgmKeys=Y
Chg_BotKeys=Y
Chg_MainSet=Y
Chg_OutLookSet=Y
Chg_TnfSet=Y
Chg_Recording=Y
Chg_ACD=Y
Chg_ACD_Viewer=Y
ShowMaintOnSplash=N
Chg_AppKeys=Y
Chg_Docking=Y
UserExit=Y
Chg_Profiles=Y
Chg_XtraKeys1=Y
Chg_XtraKeys2=Y
Chg_XtraKeys3=Y
Chg_XtraKeys4=Y
Chg_XtraKeys5=Y
Chg_XtraKeys6=Y
Chg_XtraKeys7=Y
Chg_XtraKeys8=Y
Chg_XtraKeys0=Y
```

**Server Based Call Manager Upgrade**

When the new Call Manager is released, it is possible to install the upgrade on the server so that it can be downloaded to the client. If the server based upgrade is configured, the Call Manager user will be prompted to upgrade the software when the Call Manager is launched.

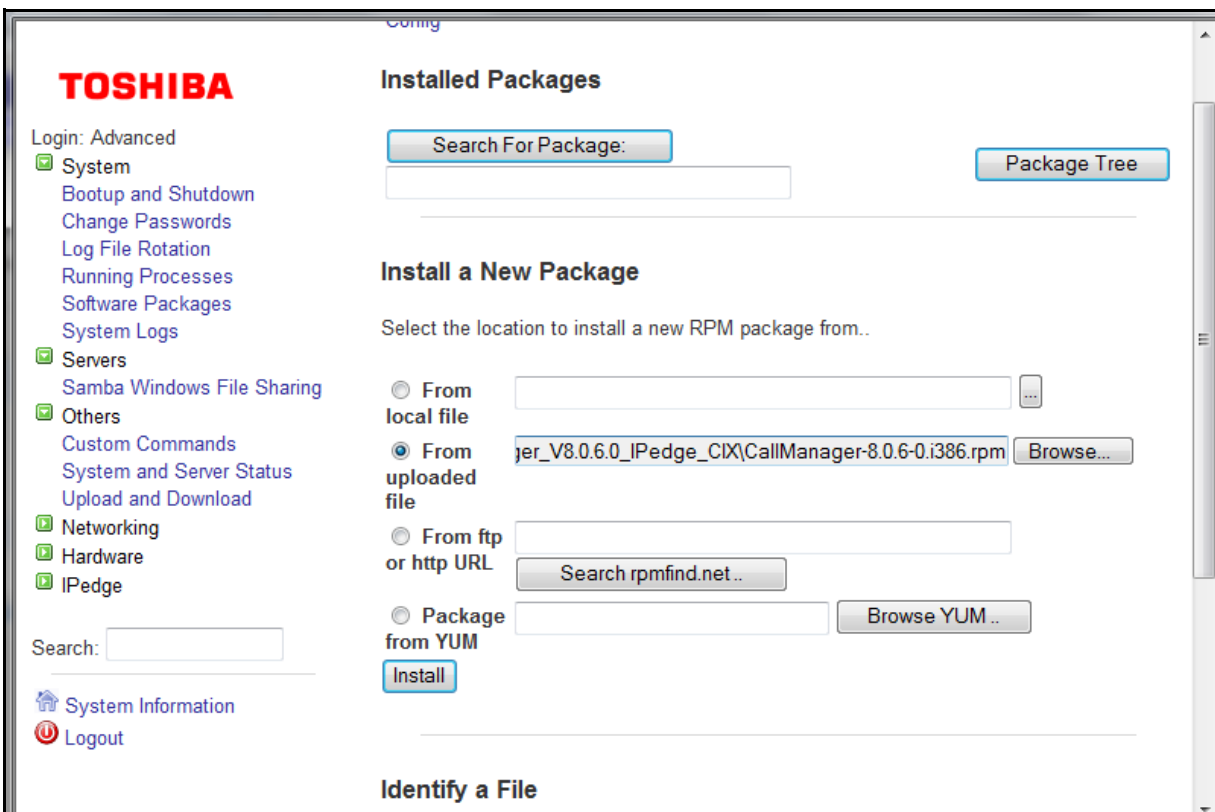
The steps below show how to install the Call Manager upgrade to the server and how to configure the Net Server to upgrade the Call Manager client.

**Note:** When the system software is updated to 1.6.2 and later, the Call Manager Server upgrade is included, these instructions are not necessary.

**Installation**

The Call Manager upgrade software is provided as an rpm file from Toshiba FYI, and it needs to be stored in the PC that can connect to IPedge through Webmin from Enterprise Manager.

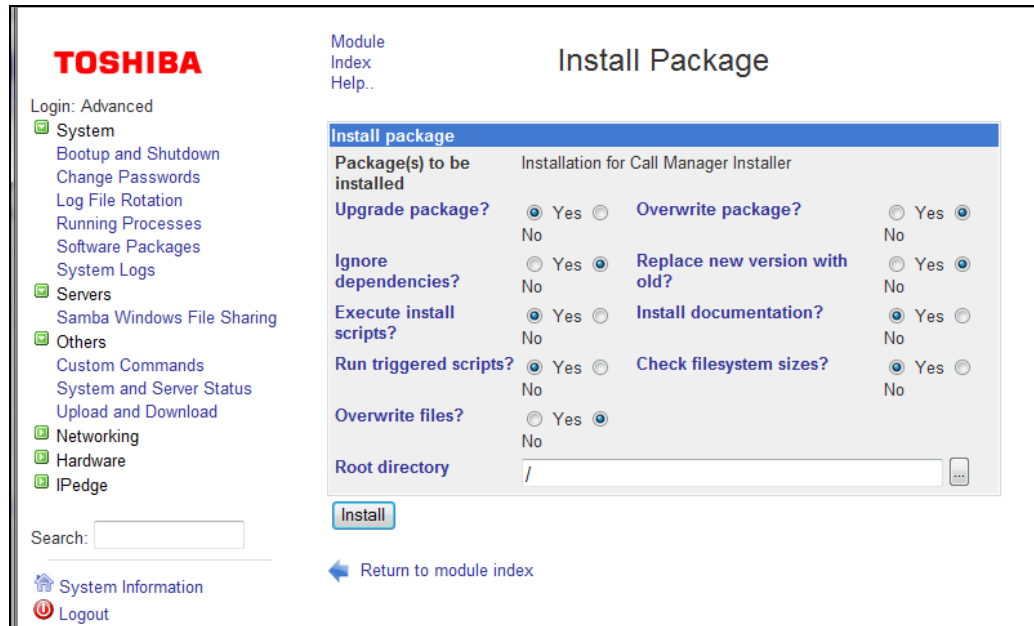
From the PC, launch Enterprise Manager and run Webmin. In the Webmin, select Software Packages menu under System menu. Then, select From uploaded file, and click Browse to specify the Call Manager upgrade software file. Then click Install.



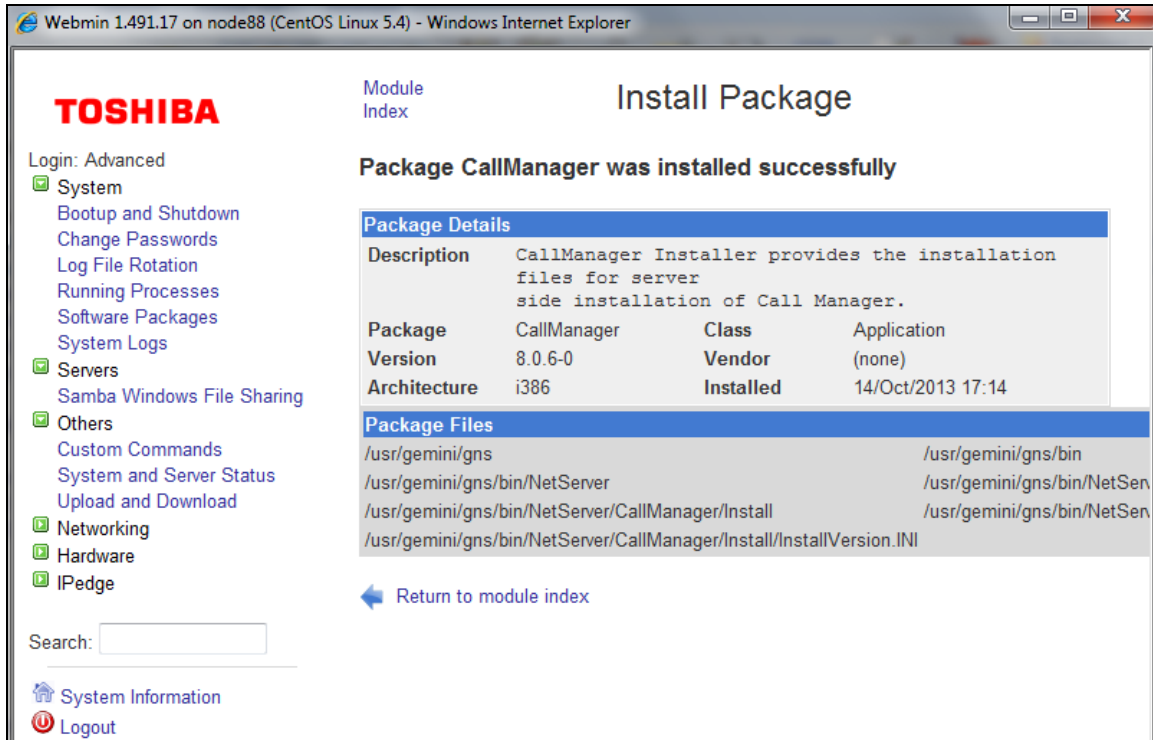


After clicking install, a progress bar is shown to indicate the progress of the file upload to the server.

When the upload is completed, the following screen displays. Please use the default value for all the settings. Click Install to start installing the Call Manager software upgrade to the server.



After the successful installation, the following screen will be shown. Then the user starts the Call Manager next time, the user will be prompted to install the newer version. The user can proceed or cancel the upgrade.



**Net Server configuration**

After the upgrade software is installed on the server, the administrator can choose whether to enable or disable the Server Based Call Manager upgrade.

In the Net Server admin screen, select Properties menu from Net Server tab. Then, check "Force update of IPedge Call Manager to version Vxxx" and click Save to enable the Server Based Call Manager upgrade. To disable the Server Based Call Manager upgrade, deselect it and click Save. Note that the version number is the actual Call Manager version installed on the IPedge server.

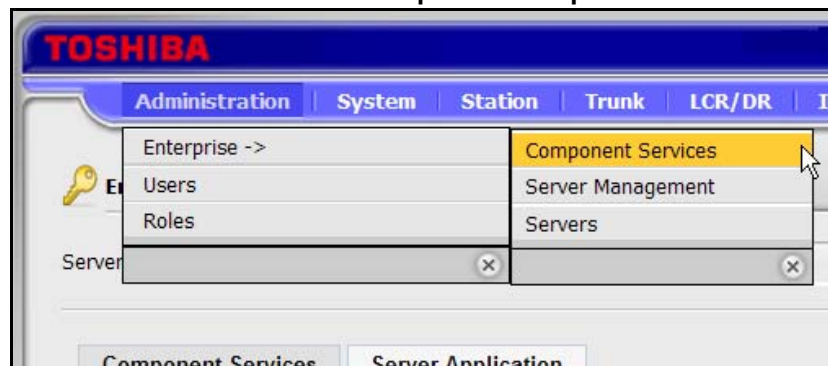
# Chapter 13 – Messaging

---

Messaging is pre installed on the IPedge system and can be activated using IPedge Enterprise Manager. Once the Messaging license is activated, add the Messaging application to Enterprise Manager and then Messaging, then configure the application using the Application menu in Enterprise Manager.

## ADD THE MESSAGING APPLICATION

1. Using your web browser, enter the Enterprise Manager application IP address.
2. Select **Administration > Enterprise > Component Services**.



3. Select the Primary Node Server.
4. Click the **Server Application** tab.
5. Click on the New icon.
6. Select Voice Mail from the list (shown above).
7. Add the IP Address of the IPedge server, do not enter 127.0.0.1 as the address.
8. Click on **OK**.
9. For multi-node systems:
  - A. Select a Member node from the Server pull-down list.
  - B. Add the Messaging application.
  - C. Enter the IP address of the IPedge server that will be running the application.
  - D. Repeat A through C for each member node.

## DEFAULT PARAMETERS

### DEFAULT PARAMETERS

The following table shows the IPedge system default parameter values.

Menu	Item	Default Value	Comments
Registry > Parameters	Mobile App Port	90	
	NetServer Follow me Handoff Application	80	
	NetServer Address	127.0.0.1	
	NetServer User	GUM	
	NetServer User password	GUM	
	NetServer User Extension	Omitted	This field is not necessary
	TCP SMDI Port	1000	Matching port is automatically configured in IPedge Call Processing.
	NetServer Port	Blank	Messaging uses 8767 if the field is blank.
Registry > VoIP	Call Processing SIP Port	5060	
	Messaging SIP Port	5070	
	Specified Caller Number Access Code	#888	
	RTP base port	30000	
Registry > Security	Default Password	0000	If 0000 is specified, Messaging will use the extension number + 997 and the password.
System > Parameters	Outbound Calls Prefix	9	
	Dial Second Line	9	
Site Parameters > Fax Settings	Outbound Calls Prefix	9	

### SETUP THE I/O PORTS

IPedge systems running R1.6.1 and later software, or with the Model Database installed will already have the I/O Ports setup. Use the steps below to verify or change the setup.

1. Using Enterprise Manager, go to **System > I/O Device**.
2. Select the Primary Server.
3. Click the **New** icon.
4. Configure the I/O SMDI#0 for the Logical Device No.
5. Set the Application Type to Client
6. The Client IP address is the address entered in [Step 7](#) of the Add Application procedure above.
7. Client Port No. is **1000**.

## SETUP THE I/O PORTS

---

8. Click the **Save** icon.

System - I/O Device

Servers: South Doc Campus

Logical Device No.: SMDI#0

LAN Port Index No.: 2

Data Flow: Asynchronization

Client IP: 158.128.138.148

Protocol: TCP

Application Type: Client

Server Port No.: 0

Client Port No.: 1000

Read Retry No.: 1

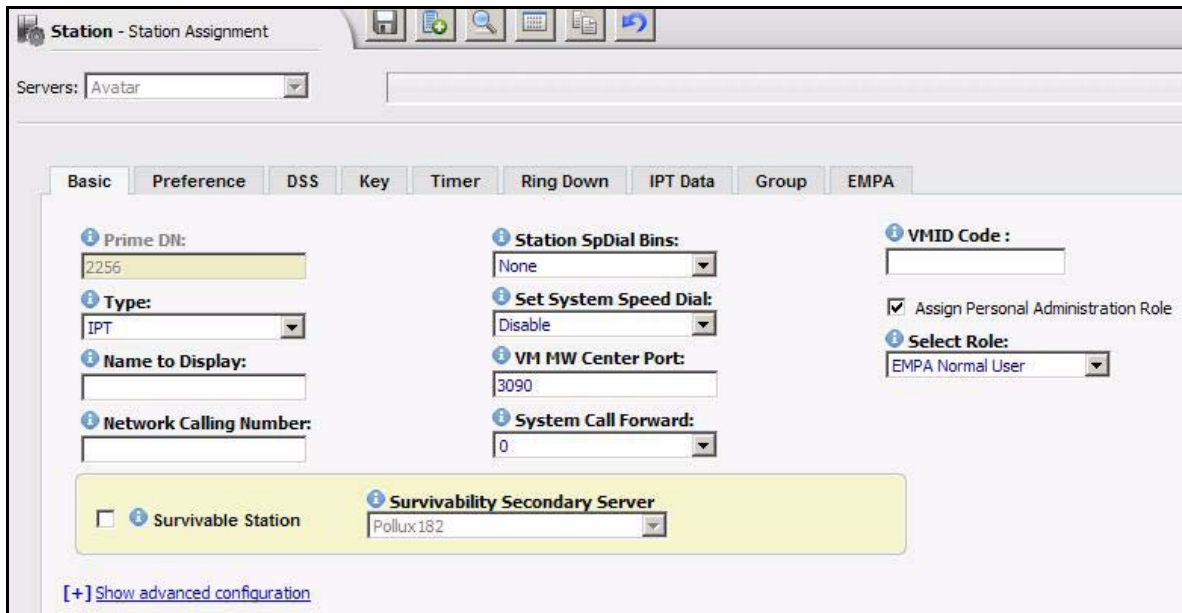
Write Retry No.: 1

CallerName Set To CSTA: No

9. For multi-node systems:
  - A. Select a Member node from the Server pull-down list.
  - B. Add the Messaging application.
  - C. Enter the IP address of the IPedge server that will be running the application.
  - D. Repeat A through C for each member node.

**ASSIGN THE VOICEMAIL SIP STATIONS**

1. From the **Station** menu, select **Station Assignment**.
2. Click the **New** icon.
3. Enter the Prime DN that matches the appropriate numbering plan.
4. Set the **Type** to SIP VM
5. **Name to display** – Optional for SIP VM station to display a name (used during Supervised Transfer).
6. **Display DN** - enter the Pilot DN of the voice mail group.
7. Un-check the **Create New mailbox** check box.
8. VMID Code - leave blank
9. Un-check the Asslgn Personal Administration Role box.
10. Un-check the **Enable Unified Messaging** box.
11. Click on the **Save** icon.



**IPT Data** After the SIP-VM station has been saved, the system will create the SIP URI and SIP password for this station. These values are also saved in the Messaging Registry.

**ADD STATIONS TO A STATION/HUNT GROUP**

1. Using Enterprise Manager, add the voicemail ports to the Hunt Groups by going to **Station > Station Groups**.

2. Click on the **New** icon.  
Make the following selections:  
**Hunt Method** is Distributed.  
**Pilot Number** should be the one used in the Numbering scheme  
Example: When the Message button is pressed, it dials 3090.  
**Multiple DN Hunt** is set to Disable  
Auto Campon is an option.
3. Click on the **Save** icon.
4. Click the members tab, then click the **Add Members** icon. Hold the Shift key to select multiple or hold Control and select the members, then click on **OK**.
5. Click on the **Save** icon.

**Voice Mail Data**

1. Go to **System > Voicemail Data**. Enter the Pilot number in the Hunt group to the Central Voicemail Callback field. Keep all the other defaults.

Enable Output of CLASS / ANI and DNIS to receive Caller ID in SMDI (automatically done in systems running R1.6.1).

SMDI Time Stamp Packet should always be set to Disable.

Transfer Direct to Voicemail DN: should be set to the same Pilot number.

2. Click on the **Save** icon.

3. Assign the Message Center by going to **Station > Station Assignment**, then select an individual DN and enter the Pilot # into the VM MW Center Port.
4. Set up one station and then copy the others.

## PROGRAM MESSAGING

1. Using Enterprise Manager, select **Application > Messaging**.
2. Select the server then, click on **OK**.
3. Systems running R1.6.1 automatically perform steps 4 through 13. For R1.6.1 and later systems go to [Step 12](#).
4. From the main menu, click **Registry > Parameters**.
5. Ensure that **Default IPedge** is check-marked. The IP address should be the IP address of the IPedge server. Do not enter 127.0.0.1.  
For multi-node systems, enter the IP address of the server running Messaging that the stations in this node will access.
6. Click the **Save** icon.
7. Click **Registry > VOIP**.
8. Ensure that the **Call Processing SIP Address** box is check-marked. Enter the IP address of the IPedge server, not 127.0.0.1.
9. Assign SIP PBX Address with <IPedge system IP address>. Assign SIP PBX Port as 5060 (default setting).
10. Assign VM SIP Port as 5070 (default setting). Click Save.
11. Restart Messaging.  
See ["RESTART MESSAGING"](#) on page 13-7.
12. Click on **System > Channel Definition**.  
Enter the DNs of the Messaging Hunt Group stations in the DN column.  
Received calls should be set to Yes.

Chnl	DN	Dep.	Rec. Calls	Init. Calls	Mode	Type	PSTN Gateway	Fax Extension
1	2601	1	Yes	Yes	AutoAttend	Primary	0	
2	2602	1	Yes	Yes	AutoAttend	Primary	0	
3	2603	1	Yes	Yes	AutoAttend	Primary	0	
4	2604	1	Yes	Yes	AutoAttend	Primary	0	
5	2605	1	Yes	Yes	AutoAttend	Primary	0	
6	2606	1	Yes	Yes	AutoAttend	Primary	0	
7	2607	1	Yes	Yes	AutoAttend	Primary	0	
8	2608	1	Yes	Yes	AutoAttend	Primary	0	

13. Restart Messaging again.



**MESSAGING STORAGE ENCRYPTION**

IPedge Messaging provides an option to encrypt all voicemail and fax messages stored in IPedge systems running software release 1.7.4 and later. The system wide option is provided to enable or disable the encryption. When enabled, the voicemail or the fax mail messages are encrypted and stored in the system when a message is stored.

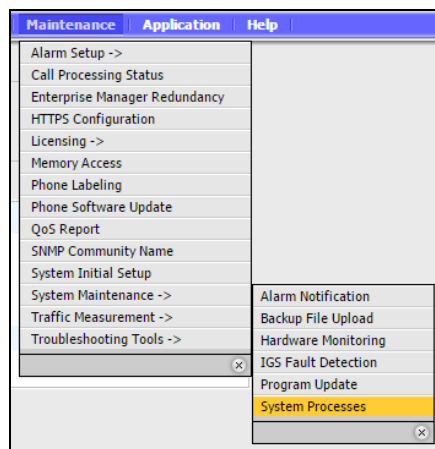
The system administrator can enable or disable the encryption. When it is changed, IPedge Messaging will restart and automatically encrypt or decrypt all of the stored voicemail and fax messages. When encryption is enabled, voicemail and fax messages in the backup data are also encrypted. If the encrypted data is restored to the system which disables the encryption, IPedge Messaging will automatically decrypt and restore the data (refer to the note). If the data is restored to the system which enables the encryption, it is automatically encrypted when it is restored.

Only the stored voicemail and Fax messages are encrypted, and the operation is transparent to users when leaving a message or playing back.

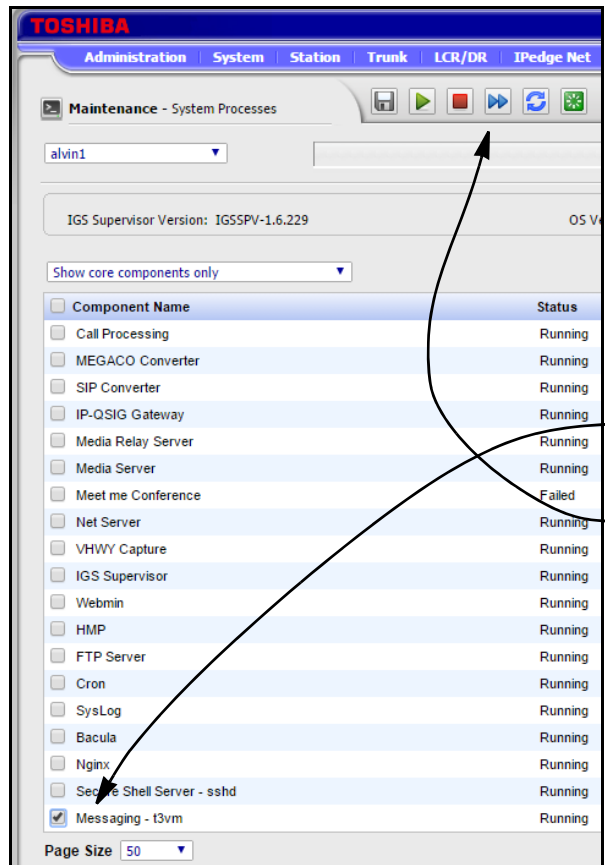
**Note:** Disabling the encryption and/or restoring the data to the system with encryption disabled requires the encryption key. The administrator must retain the key which is provided when enabling the encryption. If the key is missing the encrypted data cannot be decrypted.

**RESTART MESSAGING**

1. Go to Enterprise Manager **Maintenance > System Maintenance > System Processes**.



2. Click to check-mark the **Messaging -t3vm** box.



Check-mark Messaging-t3vm  
then,  
Click on the restart icon.

3. Click on the **Restart** icon left.

**DISK FULL NOTIFICATION**

Under some conditions the server disk can become full. Use the following procedure to setup an email alert to the system administrator when the disk is 80% full.

1. Using Enterprise Manager, select **Applications > Messaging**. In the Messaging administration screen select **Registry > Alerts**.

Active	Parameter	Value
<b>Administration</b>		
<input checked="" type="checkbox"/>	Mail Server	192.168.254.1
<input checked="" type="checkbox"/>	SysAdmin1	admin@xyzco.company.com
<input type="checkbox"/>	SysAdmin2	
<b>Channel Alerts</b>		
<input type="checkbox"/>	Channel Time	
<input type="checkbox"/>	Repeat Channel Time	
<input type="checkbox"/>	Channel Time Message	
<input type="checkbox"/>	Percent of busy channels	
<input type="checkbox"/>	% Busy Channels Message	
<b>Maximum Disk Usage Alert</b>		
<input checked="" type="checkbox"/>	HD Used	80
<input checked="" type="checkbox"/>	HD Used Repetitions	5
<b>Database Errors</b>		
<input checked="" type="checkbox"/>	Database Error Message	%s

2. Under Administration, enter the name or the IP address of the Mail Server.
3. Enter the email address for the administrator where the alerts should be sent.
4. Under Maximum Disk Usage Alert, ensure that HD Used is checked and set at 80 for the Administrator to receive an email notification when the hard disk is 80% full (default setting).
5. HD Used Repetitions – Enter the number of times for the Administrator is to be notified via email.
6. Check Database Error Message. Enter the value %s (default setting).

**MESSAGING BACKUP**

The Messaging database backup is saved to separate files using procedures separate from the IPedge system configuration and call processing database. Messaging must be backed up using the following procedures. The Messaging files can be backed up to a remote drive on the network or to a FTP server.

By default, Messaging runs a nightly back up routine, saving the customer mailbox database, names, greetings and messages into an assigned directory on the IPedge system hard disk drive. These backup files can be automatically forwarded to a FTP server.

**Note:** If the IPedge system has Call Accounting, that database is also sparate from the IPedge anr and Messaging databases. However, Call Accounting database backup to FTP uses the same FTP configuration as the Messaging application. Refer to the Call Accounting feature description document.

Backups can also be manually created on demand.

**MANUAL BACKUP**

Use this procedure to configure the backup utility for Messaging.

**Important!** Once the backup is started the browser must stay open and untouched until the operation completes. If the browser is interrupted the browser will stop responding. The backup will complete but the browser will require that you close then restart the browser. The backup process requires approximately 15 minutes for each 100 hours of messages.

1. Login to Enterprise Manager then, select **Application > Messaging**. Select the server.

- In Messaging Administration select **Utilities > Database Maintenance**.

The screenshot displays the 'Utilities - Database Maintenance' web interface. At the top, there are navigation tabs: Mailboxes, Department, COS, Site Parameters, System, Utilities, and Reports. The main content area is titled 'Utilities - Database Maintenance' and contains three primary sections:

- Backup:** This section allows setting a backup directory to '/tmp/t3backup' and includes buttons for 'Backup to Directory' and 'Retrieve Backup to Local PC'.
- Run Backup:** This section configures the backup schedule, including 'Day' (set to Daily), 'Time' (03:00 AM), and 'Script' (Smbbackup).
- Define FTP Backup:** This section sets up an FTP backup location with fields for 'FTP Name or IP' (172.16.2.225), 'Username' (admin), 'Password', and 'Path' (/tmp/dcn).
- Restore:** This section shows the 'Last Backup available' as 'Fri Jun 27 03:02:45 PDT 2014' and provides options to restore from the directory or FTP location, each with a 'Restore Key' checkbox.

- Click on the **Backup to Directory** button. This will copy all the system files to a backup location (the default backup location is /usr/SM/backup).

The system will remain active while the backup procedure is executed. At the end of the process a message will be displayed. The backup data includes the following:

- VERSION - contains the version of the vm at the time of backup
- KEYINFO - contains the license information at the time of backup
- key.cf - the actual license file
- vmdat.tgz - the system configuration files
- vmuser.tgz- the vm database, including mailboxes, departments, scripts, etc.

- messages.tgz - the messages files
- mailbox.tgz - the mailbox files (including names, greetings)
- The backup also contains voice board configuration files, if applicable
- DATE - the time and date of the backup

### Backup to a Different Directory

To save the data in a directory other than the standard backup directory, you can specify a path to a different directory (on the same disk or any other disk mounted on the system). To change the backup file location enter the directory path in the field then, click on the Save button.

### Backup to FTP Site

The system can backup then, send the data, using FTP transfer to a remote location. Configure the FTP settings, using the following procedure. Enter the following parameters:

1. In Define FTP Backup enter:

FTP Name or IP: the IP address or the qualified name of the FTP server.

Username: the user name that will allow access to the path on the FTP server.

Password: the password for the user name that will allow access to the path on the FTP server.

Path: - the full path name in which you want the data to be stored.

2. To verify the information is correct and the FTP server is accessible, click on the **Test FTP Location** button. A message will be displayed detailing the result of the test.
3. To manually execute a backup to the FTP server, press the **Backup to the FTP Location** button. This will copy the last database backup file on the IPedge server to the FTP server. The resulting file on the FTP site is called vmbackup\_latest.tgz. Every time the system performs a backup to the FTP site, it will move the vmbackup\_latest.tgz file to a sub-directory called rotation. and rename it to r1.tgz and rename the previous backup file to r2.tgz. Up to 4 backup files are stored in the rotation directory (r1.tgz, r2.tgz, r3.tgz and r4.tgz) in addition to vmbackup\_latest.tgz.

Once the FTP server information has been saved, the system will automatically backup and upload during the housekeeping procedure, programmed on the **Site Parameters > Settings** page in the Run Backup parameters. Refer to the Scheduling a Backup section below.

### Retrieve Backup to Local PC

The retrieve to local PC will retrieve the last backup performed by the system. It does not perform backup itself. If you wish to get a current backup of the system, first click on the **Backup to Directory** button. The retrieved file may be used in conjunction with the Upload file and Restore option.

1. Login to Enterprise Manager then, select **Application > Messaging**. Select the server.

2. In the Messaging monitor select **Utilities > Recovery**.
3. Click on **Retrieve Backup to Local PC** to retrieve the latest backup (vmbackup\_latest.tgz) file to a drive of your choosing on your local PC. This action may take several minutes to complete (while it is compressing the backup files) before you will be prompted to save the file to a local destination.

### Scheduling a Backup

Set a schedule to program automatic backups.

1. Login to Enterprise Manager then, select **Application > Messaging**. Select the server.
2. In the Messaging monitor select **Utilities > Database Maintenance**.
3. On the Settings page and enter the timing for the backup, (e.g. daily, weekly, etc. and the time of day for when the backup will be performed).

The screenshot shows two configuration panels. The top panel, titled 'House Keeping', has a blue information icon. It contains four rows: 'Day' with a dropdown menu set to 'Daily', 'Time' with two dropdown menus set to '02' and '00' and a third dropdown set to 'AM', 'Purge Reports' with a dropdown set to '2' and the text 'Months', and 'Script' with the text 'house1\_script'. The bottom panel, titled 'Run Backup', has a blue question mark icon. It contains three rows: 'Day' with a dropdown menu set to 'None', 'Time' with two dropdown menus set to '03' and '30' and a third dropdown set to 'AM', and 'Script' with an empty text box.

**Day:** Select from the drop-down list box which day the Run-backup script will occur. By default Messaging is backed up on a daily basis.

**Time:** Select from the drop-down list box the time the Run-backup script will occur. By default Messaging is backed up at 3:00 am.

**Script:** (Leave at default)

**Important!** There is a parameter box for entering in a name of a file that contains a script for special instructions for the backup. By default the entered script file name is Smbbackup. This entry should not be changed, unless directed by Toshiba.

### RESTORE

The restore process will reinstate all the data from a backup file. It requires a fully installed system (including Operating System and VM software files) of the same version as the backup files or later. Version 10.4.5 and above can automatically restore a backup file from version 10.3 and 10.4. Version 10.5.x can automatically restore a backup file from version 10.3, 10.4 and 10.5.

To restore a system from a backup file, you have the following options:

**Restore from Directory** Press **Restore from Directory** - this will restore the backup saved in the Backup Directory (on the system itself), the time and date of which appear in the Last Backup available field.

**Restore from FTP** Press **Restore from FTP** - this will restore the “vmbackup\_latest.tgz” file from the FTP Backup directory specified in the backup to FTP site procedure.

**Upload from Local Directory** Press the **Browse** button to select a backup file stored on your PC or network. This file must be a tarred backup file containing all the sub-files specified in the Manual Backup section. Once selected, press the **Upload File and Restore** button to complete the restore process.

**Note:** The maximum file size for this method is 2GB. If the backup file size is greater than 2GB, use the Restore from FTP option.

For any of these options, you may check the Restore Key option to restore the key file from the backup file. A confirmation message will be displayed once the restore process is complete.

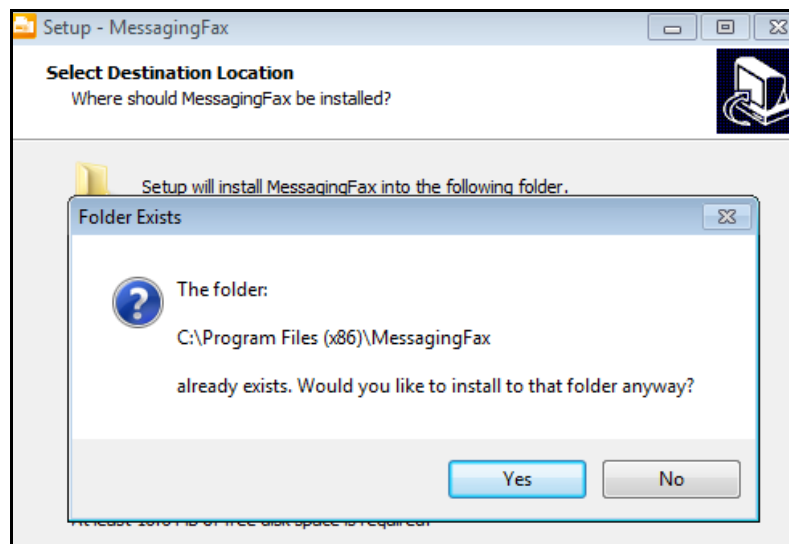


**MESSAGING FAX  
PRINTER DRIVER 6.1**

The following steps are used to install the FAX driver 6.1 onto client PCs. The printer driver allows users to send a document via the IPedge system as a fax. The fax printer driver 6.1 is compatible with IPedge systems running software release 1.7.3 and later.

**Note:** If the previous version (5.0 or 5.5) of Messaging Fax is installed on the client PC, you must first uninstall it.

1. If needed, uninstall Messaging FAX 5.0 or 5.1
2. Download MessagingFax 6.1 from Toshiba's FYI website.
3. Right click MessagingFaxSetup\_6.1.exe and select Run as Administrator.
4. If the Windows User Account Control **Setup** dialog box appears, click **Yes** to continue.
5. Read the License Agreement, select **I accept the agreement** then, click on **Next**.
6. Accept the Destination Location. Click on **Next**.
7. If a previous version (5.0/5.5) was installed the following message will be displayed. Click on **Yes**.

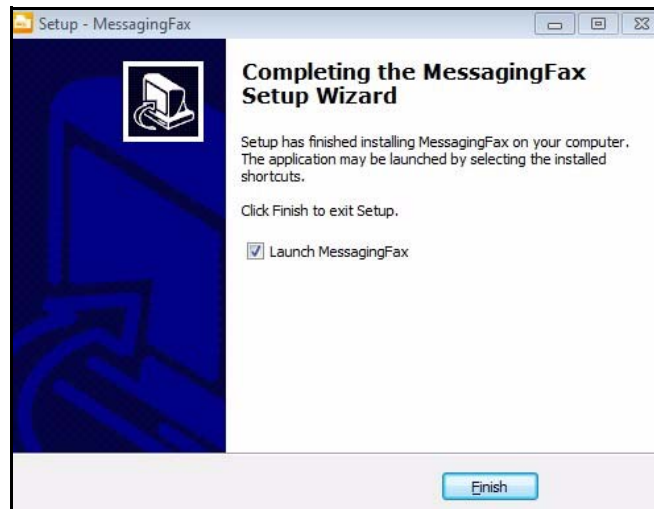


8. In the Select Additional Tasks dialog check-mark the **Create a desktop shortcut** box then, click on **Next**.
9. Review the Ready to install dialog. Click on **Install**.
10. If a Microsoft Visual C++ dialog box appears, select **Repair** then click **Next**. Otherwise go to [Step 12](#).
11. When the Setup is Complete click on Finish.
12. You may be prompted to restart the computer. If this prompt appears close all open windows on this computer, select **Yes, restart the**

**computer now** then, click on **Finish**. If this prompt does not appear go to [Step 13](#).



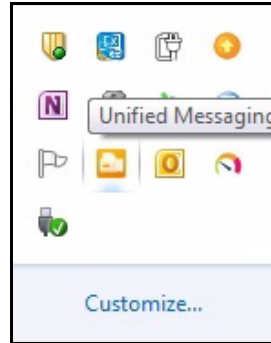
13. If the Completing the Messaging Fax Setup Wizard dialog appears ensure that Launch MessagingFax is checked click **Finish**.



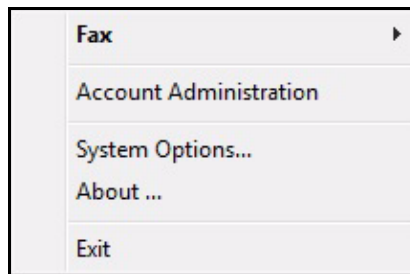
## CONFIGURE MESSAGING FAX

1. To configure Messaging Fax, double click the desktop icon or click **Start > All Programs > MessagingFax > MessagingFax**.

2. Right click the Messaging Fax icon in the Task bar. You may need to click on the Show Hidden Icons button.



3. Click on **System Options...** to begin configure.



4. The System Options dialog box appears. Enter the FQDN or the IP address of the IPedge Messaging server in the Server Path field.
5. Enter the Mailbox and Mailbox password to be used to send FAXes from this client PC.

**Notes:**

1. If the IPedge Messaging server is behind a NAT router ports 90 and 42507 must be allowed by the firewall.
2. If using HTTPs either the Enterprise Manager Certificate or the Messaging generated Certificate is required.

**PRINT a FAX DOCUMENT**

To print a fax received by the IPedge Messaging application use the following procedure.

1. Open the file you wish to send as a fax message. Select File > Print.
2. Select the fax printer as the printer.

- When Messaging Fax is selected to print a document the following FaxMain web page will be displayed.

**Recipient**

<b>Name:</b>	<b>Fax Number / Email:</b>	<b>Company:</b>	
<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	<input type="button" value="Remove"/>

**My Info**

<b>From:</b>	<input style="width: 90%;" type="text" value="Road Runner"/>
<b>Company:</b>	<input style="width: 90%;" type="text" value="Road Run Labs"/>
<b>My Phone Number:</b>	<input style="width: 90%;" type="text" value="949-555-6205"/>
<b>My Fax:</b>	<input style="width: 90%;" type="text" value="800-555-8205"/>
<b>My E-mail:</b>	<input style="width: 90%;" type="text" value="dan.dorvicna@hibachi.com"/>
<b>Date:</b>	Now <input checked="" type="radio"/> Later <input type="radio"/> <input style="width: 90%;" type="text" value="07-28-2016 2:19:08 PM"/>
<b>Number Of Pages:</b>	<input style="width: 90%;" type="text" value="1"/>
<b>User ID:</b>	<input style="width: 90%;" type="text" value="6205"/>
<b>Password:</b>	<input style="width: 90%;" type="password" value="*****"/>
<b>Keep user settings on this computer:</b>	<input checked="" type="checkbox"/>

**Options**

<b>Cover message:</b>	<div style="border: 1px solid gray; height: 80px; width: 100%;"></div>
<b>Send cover page:</b>	<input type="checkbox"/>
<b>Fax Quality:</b>	<input style="width: 90%;" type="text" value="Fine"/>
<b>Account Code:</b>	<input style="width: 90%;" type="text"/>
<b>Billing Code:</b>	<input style="width: 90%;" type="text"/>
<b>Request CSID:</b>	<input style="width: 90%;" type="text"/>

- Click on **Send FAX**.

# Chapter 14 – Maintenance

---

## INTRODUCTION

The Toshiba IPedge system is an all IP telephone system running on an IP network. When troubleshooting consider that problems may be with the network as well as with the server.

Use the following as a check list to help identify voice quality problems.

1. Run a network assessment while the trouble is occurring.
2. Collect Wireshark logs during the issue
3. Document the time, Day, the extension involved in the call.
4. Document any functions performed. (i.e. User pressed the conf/trans key, poor voice quality while reviewing voicemail, etc.)
5. Document whether the call was internal (station-to-station) or external (station-to-trunk).
6. Check managed switch and/or logs for errors.
7. If over WAN, MPLS, or P2P check for any carrier errors.
8. Check IPedge logs.
9. Check any gateways involved in the call for issues.
10. Provide database of gateway if requested by Technical Services.
11. Provide the system logs from the gateway if requested by Technical Services.

## ALARM NOTIFICATION

The IPedge Virtual Server can generate messages in response to specified alarm conditions. To implement any of these function refer to [www.Dell.com](http://www.Dell.com) for iDRAC7 documentation.

## SYSTEM PROCESSES

The status of system processes can be viewed, stopped, started and, set to start on reboot.

1. Select **Maintenance > System Maintenance > System Processes**.
2. The system processes will be displayed.
3. Check-mark a component.
4. Click on the appropriate icon (Configure Start on Boot, Stop, Start, etc.)

### Configure Start on Boot

1. Check-mark a Component.
2. Click on the 'Configure Start on Boot' icon.

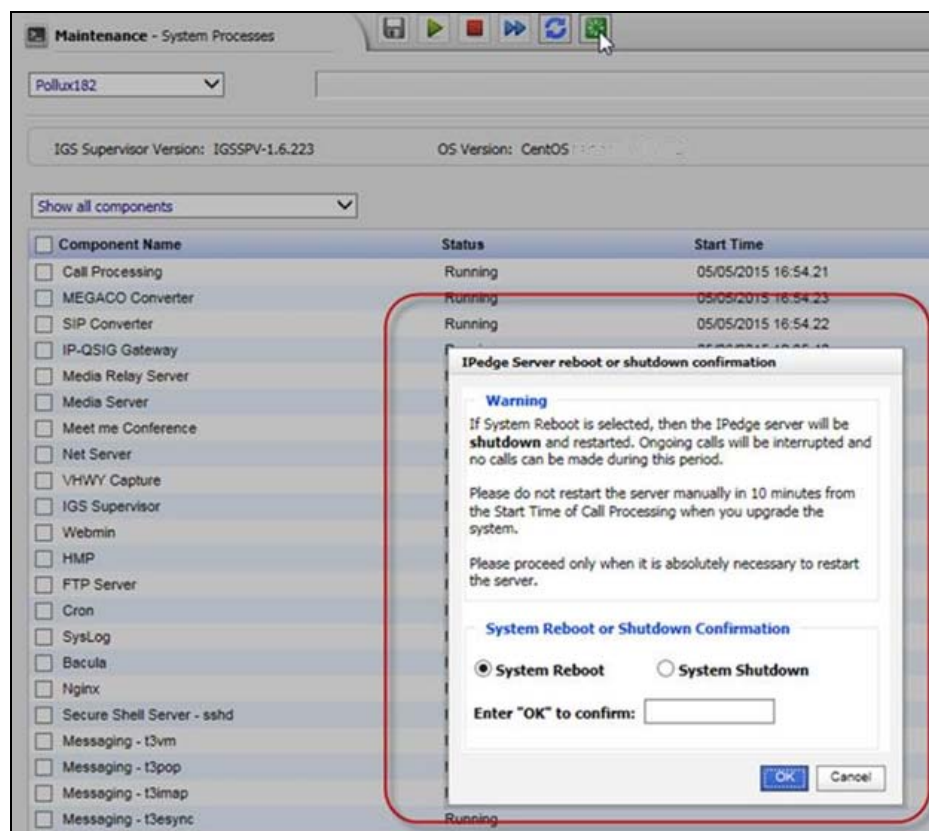
3. A Component Configuration Dialog will open. The current configuration will be shown.
4. To exit without changing the settings click on the **Cancel** button. To change the setting go to the next step.
5. Select the Action parameters then, click on the **OK** button.

### System Reboot/ Shutdown

Some program update procedures require that the System Administrator reboot the system.

1. In the System Processes screen, click on the Reboot / Shutdown icon.
2. Select System Reboot or System Shutdown.
3. Type **OK** in the confirmation field.
4. Click on the **OK** button.

**Note:** A system reboot or startup may take several minutes. Wait for the database synchronization to complete before making programming changes.



**Important!** Allow the system to run for at least 20 minutes before starting a program update.

- Verify Media Server
5. Verify that the Media Server is running. In Enterprise Manager select **Maintenance > Call Processing Status**.
  6. If the Media Server is running the system has restarted correctly. Go to the next installation process. If the Media Server status is Disabled by fault go to [Step 7](#).
  7. Select **Maintenance > System Maintenance > System Processes**, click on the Restart icon.
  8. When the system has restarted login to Enterprise Manager then, select **Maintenance > Call Processing Status**.
  9. If the Media Server is running the system has restarted correctly. Go to the next installation process. If the Media Server status is Disabled by fault contact Toshiba's Technical Support department

### IPedge APPLICATION SERVER RECOVERY

If the hard disk drive(s) (HDD) in the IPedge Virtual server is damaged or corrupted contact Dell Technical Support.

### SERVER FAN REPLACEMENT

Each server contains several cooling fans. Refer to the Dell owner's guide for replacement instructions.

### SERVER POWER SUPPLY REPLACEMENT

You must shut down the system to replace a power supply module on the R220, R420 and the EC class R430 servers. The R430 EM class (R430 with dual power supplies) and the R720 server has redundant power supplies. Replace with the same model and power rating.

Refer to the Dell owner's manual for power supply replacement instructions.

### POWER UP SERVER

1. Connect the AC Power cords.
2. Set the rear panel switches to ON.
3. **Wait one minute** then, press the front panel Power Switch.

### HOT-SWAP HARD DRIVE

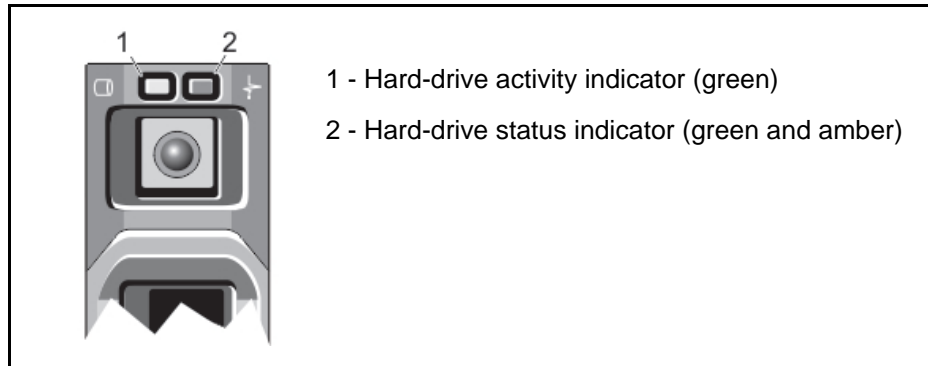
The R420 server with RAID, the R430 and the R720 servers used as IPedge Virtual Servers are equipped with hot-swap Hard Disk Drives (HDD). In the event that a HDD fails it can be replaced without shutting down or restarting the server. The replacement HDDs are ordered directly from Dell.

### HDD INDICATORS

The HDD indicators are two LEDs on each drive, visible from the front of the system. Refer to the Systems Owner's documentation for more information.

**Note:** When a single HDD in a RAID server fails that HDD can be replaced with no loss of data. Note the following:

- Replace only one HDD. Remove the failed drive, insert a new HDD. Allow the system to rebuild the new drive. This rebuild can take up to several hours.
- DO NOT change the position of the HDDs in a RAID server.



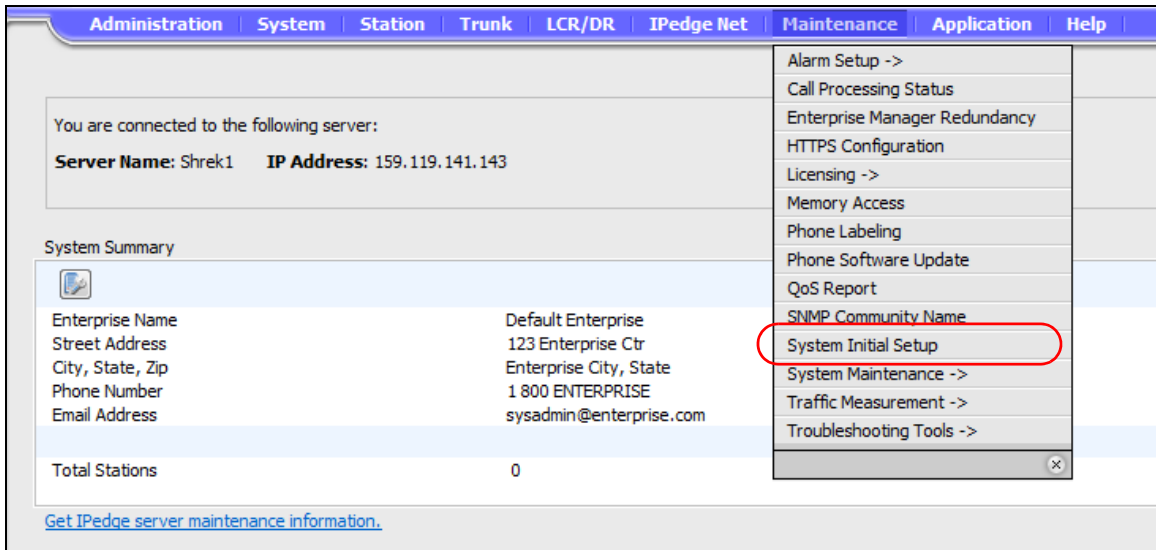
**Table 14-1 RAID HDD Indicators**

Drive-Status Indicator Pattern (RAID Only)	Condition
Blinks green two times per second	Identifying drive or preparing for removal
Off	Drive ready for insertion or removal <b>NOTE:</b> The drive status indicator remains off until all hard drives are initialized after the system is turned on. Drives are not ready for insertion or removal during this time.
Blinks green, amber, and off	Predicted drive failure
Blinks amber four times per second	Drive failed
Blinks green slowly	Drive rebuilding
Steady green	Drive online

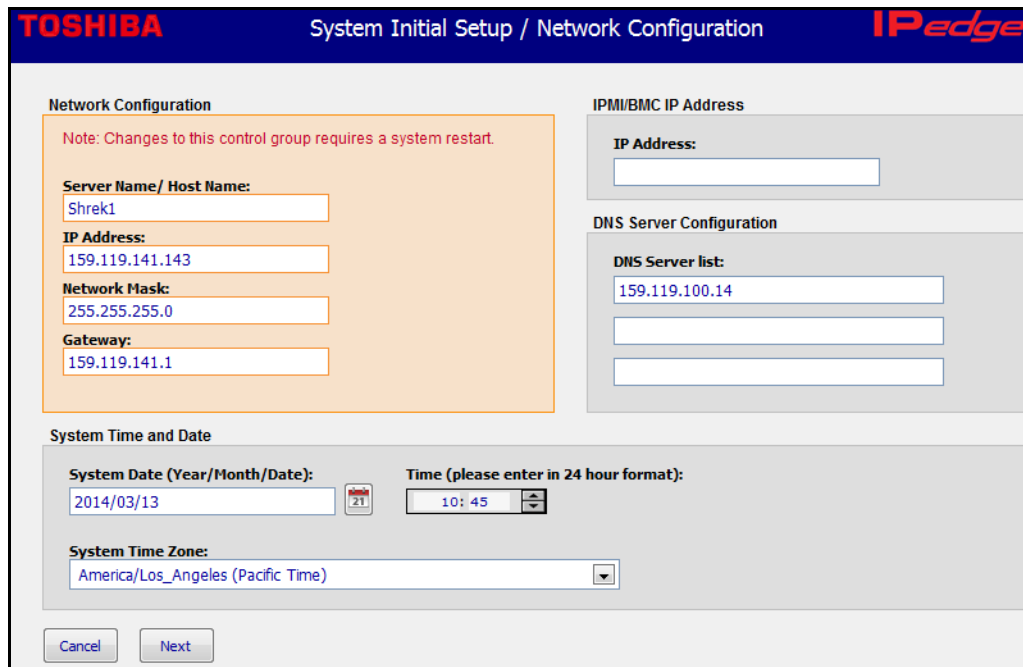


SYSTEM INITIAL SETUP

The System Initial Setup function in the Maintenance menu allows the administrator to startup the same initial response as the startup that runs when a new system is powered up.



This function is commonly used when a system that has configured by the dealer technician before shipping to the customer location needs a new IP address. This System Initial Setup can be use to change the IPedge server IP address. This process is used instead of using the Webmin network assignments.



**Important!** If any SIP trunks have been programmed or a model database has been installed the SIP Trunk Service Definition 1 must be deleted before starting a System Initial Setup. Select **Trunk > SIP Trunk** then the **Service Definition** tab. Delete Service Definition 1.

**QoS TROUBLESHOOTING  
TOOL**

IPedge systems running release 1.7.4 and later software can display a completed call's MOS score (Mean Opinion Score) to assist the technician in troubleshooting call quality issues.

The QoS report also provides a Search option to easily filter the report to target and find specific calls based on any of the column names. The QoS report can be downloaded as a CSV file. The file can be viewed and sorted using a spreadsheet program such as Microsoft® Excel®.

**Quality Of Service Values**

Range	User Experience
4.3 or above	Very Satisfied
4.0 – 4.2	Satisfied
3.6 – 3.9	Some users Dissatisfied
3.1 – 3.5	Many users Dissatisfied
2.6 – 3.0	Nearly all users Dissatisfied
1.0 – 2.5	Not recommended for use

**Note:** The maximum achievable score for G711 is 4.4.  
The maximum achievable score for G729 is 4.1.

For every finished call, the technician will be able to view valuable metrics such as:

- Source and Destination ports
- Packets Sent and Received
- Jitter
- Delay
- Packet Loss
- CODEC

Administration System Station Trunk LCR/DR IPedge Net Maintenance Application Help

Maintenance - QoS Report

Servers:  Source Device:  Search Advanced

QoS Report Download

Alarm	Protocol	Timestamp	Source Device	Source RTP	Destination Device	Destination RTP	Packets Sent	Packets Recv	Jitter	Delay MS	Packet Loss	Codec Type	Call Duration	QoS
	IPT	10/18 19:20:08	2410	49154	2411	49154	14904	14788	0	0	0	G.711M	00:04:56	4.4
	IPT	10/18 19:20:08	2411	49154	2410	49154	14809	14808	0	0	0	G.711M	00:04:56	4.4
	IPT	10/18 19:20:11	2411	49154	2410	49154	40	40	0	0	0	G.711M	00:00:00	4.4
	IPT	10/18 19:20:11	2410	49154	2411	49154	50	46	0	0	0	G.711M	00:00:01	4.4
	IPT	10/18 19:20:32	2109	49154	2503	30004	5924	267	0	0	0	G.711M	00:01:58	4.4
	IPT	10/18 19:20:33	2411	49154	2410	49154	349	349	0	1	0	G.711M	00:00:06	4.4
	IPT	10/18 19:20:33	2410	49154	2411	49154	355	347	0	1	0	G.711M	00:00:07	4.4
	IPT	10/18 19:20:37	2411	49154	2410	49154	44	44	0	0	0	G.711M	00:00:00	4.4
	IPT	10/18 19:20:37	2410	49154	2411	49154	50	42	0	0	0	G.711M	00:00:01	4.4
	IPT	10/18 19:21:09	2108	49154	2504	30006	5919	261	0	0	0	G.711M	00:01:58	4.4
	IPT	10/18 19:21:36	2411	49154	2410	49154	2886	2886	0	1	0	G.711M	00:00:57	4.4
	IPT	10/18 19:21:38	2410	49154	2411	49154	2892	2885	0	1	0	G.711M	00:00:57	4.4
	IPT	10/18 19:22:32	2109	49154	2505	30008	5930	323	0	0	0	G.711M	00:01:58	4.4
	IPT	10/18 19:23:09	2108	49154	2506	30010	5934	316	0	0	0	G.711M	00:01:58	4.4
	IPT	10/18 19:24:16	2411	49154	2410	49154	1049	1048	0	1	0	G.729	00:00:41	4.1
	IPT	10/18 19:24:16	2410	49154	2411	49154	1045	1045	0	1	0	G.729	00:00:41	4.1
	IPT	10/18 19:24:32	2109	49154	2507	30012	5929	320	0	0	0	G.711M	00:01:58	4.4
	IPT	10/18 19:25:09	2108	49154	2508	30014	5932	313	0	0	0	G.711M	00:01:58	4.4
	IPT	10/18 19:26:32	2109	49154	2509	30016	5931	279	0	0	0	G.711M	00:01:58	4.4
	IPT	10/18 19:27:09	2108	49154	2510	30018	5934	320	0	0	0	G.711M	00:01:58	4.4

Page Size 20 Records 1 - 20 of 20 Page Number: 1(1)

Administration System Station Trunk LCR/DR IPedge Net Maintenance Application Help

Maintenance - QoS Report

Servers:  Source Device:  Search Advanced

QoS Report Download

Alarm	Protocol	Timestamp	Source Device	Source RTP	Destination Device	Destination RTP	Packets Sent	Packets Recv	Jitter	Delay MS	Packet Loss	QoS
	IPT	07/08 15:56:14	2301	49154	2302	49154	26742	26723	0	0	0	4.4
	IPT	07/08 16:52:02	2301	49154	2302	49154	38	33	0	0	0	4.4
A	IPT	07/08 16:52:09	2301	49154	159.119.141.213	13096	327	298	11	0	32	4.0
	IPT	07/12 09:52:09	2301	49154	2302	49154	55	54	0	0	0	4.4
	IPT	07/12 09:52:40	2301	49154	159.119.141.213	13098	1501	1482	1	0	0	4.4

Page Size 20 Records 1 - 5 of 5 Page Number: 1(1)

This page is intentionally left blank.

# Chapter 15 – Restore IPedge Software

---

This section covers the procedures to Restore IPedge and/or ACD image on the IPedge Virtual Server.

**Important!** Backup the database before starting the OVA deploy process. The database of the virtual machine (IPedge or ACD) will be lost when the new OVA is deployed.

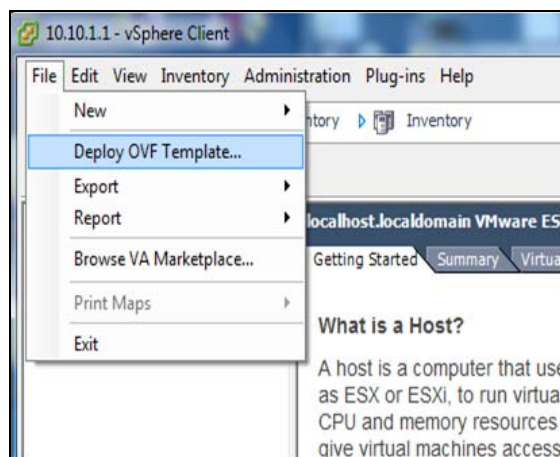
**Note:** Before starting an IPedge EM OVF deployment ensure that the host server has at least 250 GB of disk space available.

**Note:** Ensure that the IPedge Virtual Machine (virtual machine) images (\*.ova) are in one folder.

IPedge EC, EM and EP Virtual Server software is restored by deploying an [OVA template](#). IPedge ES software is restored by loading an ISO file from the [IPedge ES recovery](#) flash drive.

## DEPLOY IPedge OVA TEMPLATE

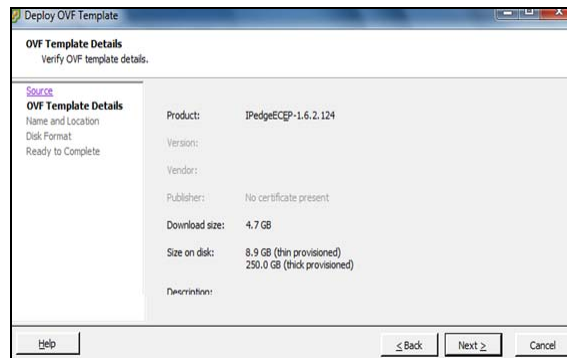
1. Launch the vSphere Client on your PC. Connect to the IPedge Virtual server.
2. Delete the old IPedge OVA file to make room for the new IPedge file.
3. Select **File > Deploy OVF Template**.



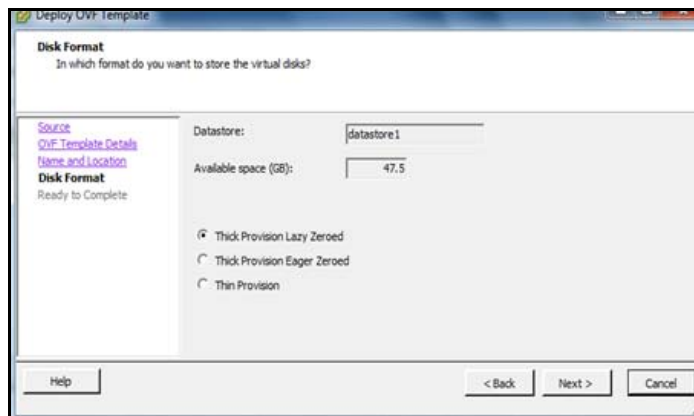
4. Browse to the OVA file on the recovery USB flash drive.



5. In the Template Details screen click on **Next**.



6. Enter a unique name for the IPedge virtual machine then (the file name on the USB drive can work), click on **Next**.
7. Check-mark the **Thick Provision Lazy Zeroed** box.

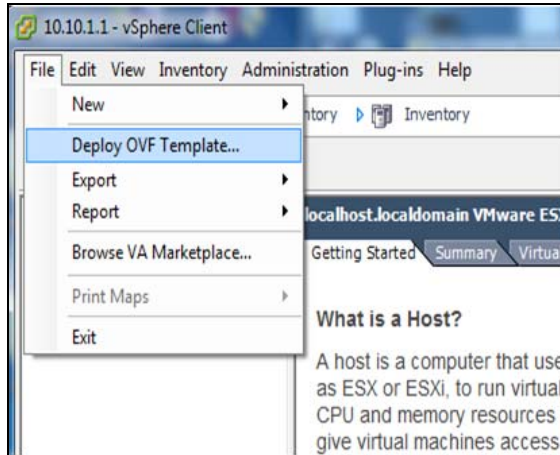


8. Click through to **Finish**. The deployment will take approximately 35 to 110 minutes, depending on file sizes.

## DEPLOY ACD TEMPLATE

1. Before the deployment of an ACD OVA file:
  - A. Backup the ACD database.

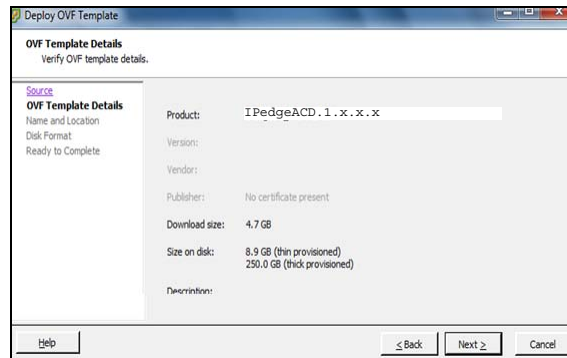
- B. If the server is configured for HTTPS you must turn off HTTPS. Refer to the HTTPS Configuration chapter of this manual.
2. Delete the old ACD OVA file.
3. Select **File > Deploy OVF Template**.



4. Browse to the OVA file on the recovery USB memory.

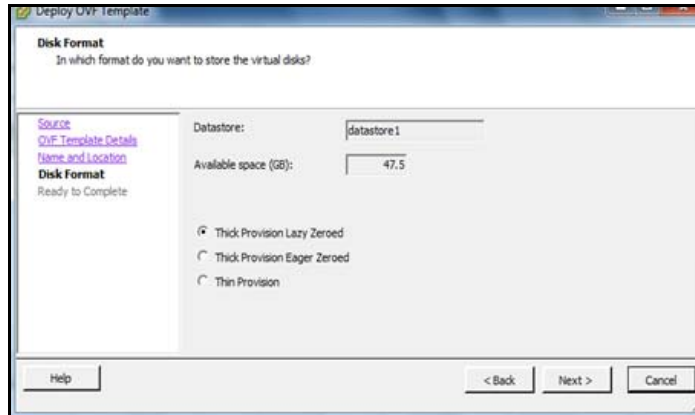


5. In the Template Details window click on **Next**.



6. Enter a unique name for the ACD virtual machine or use the file name on the USB recovery drive then, click on **Next**.

7. Check-mark the **Thick Provision Lazy Zeroed** box.



8. Click through to **Finish**. The deployment will take approximately 10 to 12 minutes.
9. Click to **Power on the virtual machine**.
10. Wait for Windows to start - Click on console tab
11. Follow the Windows registration steps.

## START ACD VM and WINDOWS

After the OVA has been deployed the virtual machine must be started and and the Windows operating system setup.

1. Click on the ACD virtual machine in the left column of the vSphere client screen.
2. Click on the **Power On** icon.
3. Click on the **Console** tab.
4. The Windows operating system setup will launch. This start up will take a few minutes.
5. In the Setup Windows dialog box click on **Next**.
6. Enter the Windows Product Key. Click on **Next**.
7. Read and accept the license terms. Click on **Next**.
8. **Click on Use recommended settings**. Click on **Next**.
9. Set the date and local date. Click on **Next**.
10. Select **Work network**. Click on **Next**.
11. Windows will configure your settings. Select the Console tab to see the Windows operation system startup.
12. When the Windows operating system restarts, select Start > Control Panel > Network and Sharing Center.
13. Click on **Local Area Connection**.
14. In the Local Area Connection Status dialog box click on **Properties**.



15. Click on **Internet Protocol Version 4 (TCP/IP v4)**. Click on the **Properties** button.
16. Change the:
  - IP address to 192.168.254.252
  - Subnet to 255.255.255.0
  - Gateway to 192.168.254.1
17. Save this configuration.
18. Log out of the vSphere client.
19. If the system was configured for HTTPS refer to the HTTPS Configuration chapter of this manual.

The Virtual Machines are now running on the host. The IPedge and ACD servers are reset to the factory defaults, Refer to the install procedures in the IPedge Virtual Server Installation manual, in the System Installation chapter.

### IPedge ES SOFTWARE RESTORE

The following procedure details the IPedge ES server recovery using the IPedge Recovery USB Drive.

**Important!** Before starting the recovery process ensure that the IPedge ES server is connected to a LAN.

**Important!** Use the Manual backup procedure to create a database backup and store the backup files off the server.

**WARNING!** If this is a member of a multi-node system, detach this node before starting this procedure.

### RECOVERY FROM USB FLASH DRIVE

Use this procedure to install the IPedge server recovery software image. This procedure requires that the IPedge server be connected to a network with internet access and the following hardware.

- USB Keyboard
- Monitor (HDMI or VGA)
- USB recovery flash drive shipped with the IPedge ES server.

1. Power down the IPedge ES server.
2. Connect the IPedge server to a network (internet access is not required).
3. Connect the keyboard, monitor and the USB flash drive to the IPedge ES server.
4. Power on the IPedge server.
5. To select the boot device while the boot menu is displayed, on the keyboard press the **F10** key.

6. Use the keyboard cursor keys to highlight the "USB" option then, press the **Enter** key.
7. When the **Welcome to CentOS...** screen appears press the **Enter** key or wait for the count-down clock to time out.
8. The system will re-format the disk drive then restore the IPedge system software.

This process will require approximately 30 ~ 45 minutes.

9. After recovery procedure is successfully done a **CentOS Installation is complete** message is displayed. There will be a **Reboot** icon in the lower right corner.
20. Press the keyboard **Enter** key. to reboot the system.
21. The IPedge ES system will reboot.

**Important!** The system has been returned to its as-shipped condition. Remember that the IP addresses, User Names and Passwords are reset to their default values.

22. When the system boot-up is complete remove the USB flash drive.
23. Refer to the initial system setup procedures in this manual.

### Apply Licenses

The system has been returned to its as-shipped condition. The licenses must be applied before restoring the database.

1. The IPedge ES requires a connection to the internet to apply the licenses.
2. Refer to the IPedge Virtual License Service User Guide and the IPedge Virtual Server Install manual.

### Restore Database

If a backup file is available use the following outline.

1. Refer to the procedures required to set the server name and IP addresses.
2. Apply the licenses.

**Note:** Connection to the internet is required for loading the license file.

3. Restore the database. Refer to the Manual Restore section in the backup and restore section.
4. Synchronize the database.

# Chapter 16 – System Software Update

---

## PROGRAM UPDATE

IPedge systems running 1.7.0 or earlier software can be upgraded to 1.7.4 software. Before starting an upgrade insure that the Software Support and upgrade Service (SUS) is current.

---

**CAUTION!** After a system update from R1.5.1 to R1.6.x wait 30 minutes, do nothing with or to the system during this wait.

**Do not restart, login to, or power down the system. The system is converting and rebuilding databases during this time period. If the system is stopped, restarted or otherwise altered during this process the software can become corrupted. The telephones will be unavailable during this process.**

---

**Important!** After a system update from R1.5.1 to R1.6.x all voice mailbox passwords will reset to 0000. Login to each mailbox to change the password.

---

**CAUTION!** For systems using Messaging DCN, the DCN must be disabled on all nodes before upgrading. Refer to [“MESSAGING DCN”](#) on [Page 16-21](#)

---

## Software Version 1.7.0 Systems

If the existing system is running IPedge 1.7.0 software the upgrade is available on Toshiba’s FYI website.

IPedge Servers running IPedge 1.7.0 software can be upgraded using the on-line update process.

**Note:** Do not delete the ACD OVA file. The WebACD software is available on Toshiba’s FYI website.

### Stop ACD Services

1. Backup the IPedge and ACD databases.
2. Login to Enterprise Manager then select **Application > ACD**.
3. In the ACD Main screen click on the **Service** link under the Quick Link section.
4. In the Service Status screen select and shut-down all services.
5. When all of the ACD services have shut down close the ACD Admin screen.

6. The upgrade software file, TGZ 1.7.4.110 is available on Toshiba's FYI website for local update. Refer to the IPedge Install manual for software upgrade instructions.

**Note:** If it is necessary to re-image an 1.7.0 IPedge branded server use the 1.7.4 ISO available on the FYI website. To re-image an IPedge virtual server to IPedge 1.7.4 the IPedge OVA file is available on Toshiba's FYI website in the IPedge Software section. Refer to the IPedge Virtual Server Install manual for detailed instructions.

7. When an IPedge virtual server is re-imaged refer to the IPedge Virtual Licensing Service User Guide for license transfer instructions.

Restore the IPedge database (it is not necessary to restore the ACD database).

### Software Version 1.6 and Earlier Systems

1. Systems running 1.6 and earlier software must first be upgraded to **1.6.2.359** then backup the IPedge and ACD databases.

**Important!** Login to Toshiba's Virtual Licensing Service to create the customer site then, transfer the license(s) for this system before starting the next step. **Do not start the system re-image to release 1.7.4 software until you have received the License String from the licensing service.** Note that some licenses require manual transfer by your Customer Support representative. Refer to the Virtual Licensing Service User Guide, available on Toshiba's FYI website.

### Stop ACD Services

2. Store the backup files on another server, not on the IPedge server.
3. Login to Enterprise Manager then select **Application > ACD**.
4. In the ACD Main screen click on the **Service** link under the Quick Link section.
5. In the Service Status screen select and shut-down all services.
6. When all of the ACD services have shut down close the ACD Admin screen.

**Note** Do not delete the ACD OVA file. The WebACD software is available on Toshiba's FYI website.

7. Load the 1.7.4 OVA file onto the IPedge server. The IPedge 1.7.4 IPedge OVA file is available from the FYI website. Refer to [Chapter 15 – Restore IPedge Software](#) for the detailed process.

**Note:** The restore process removes the pre-configured Meet-Me Audio Conference script mailbox (9998). To use Meet-Me Audio Conference the system administrator must create the script mailbox. Refer to the Meet-Me Audio Conference feature description, programming section. The Toshiba IPedge system must be running R1.5.1 TGZ 107 or later software before the system can be upgraded to R1.6 or later software. If your server is already R1.5.1, TGZ 107, or later use the procedures in this chapter. If not contact Toshiba Technical Support.

8. Restore the IPedge database (it is not necessary to restore the ACD database). Refer to the IPedge Install manual for details.

**Multi-Node Systems**

For all multi-node systems; all of the nodes must first be detached. While detached each node is upgraded to 1.71. software separately. When all of the systems are upgraded to 1.7.4 software attach the nodes to the primary node.

**Systems with ACD**

WebACD must be upgraded to version 1.0.2-2 software for all IPedge systems and IPedge App Servers with ACD. The WebACD software is available on Toshiba's FYI website. To download the software login to the FYI website then select; **IPedge/VIPedge > Software**.

**UPGRADING ACD on IPedge 1.7.4**

- Important!** Backup the ACD database before starting this procedure.  
**Important!** ACD functions will not be available during this procedure.  
**Important!** Do NOT delete the ACD OVA file.

**Note:** You will need to know the ACD service IP address, refer to Step 5.

**Note:** It is not necessary to backup the ACD database to upgrade the ACD software. However Toshiba recommends performing the backup before starting this procedure.

**Important!** IPedge EP systems running on Dell R220 servers use the IPedge EC OVA file. These servers require a license change. Contact your Sales Engineer before starting the upgrade process.

1. Log into IPedge Enterprise Manager.
2. From the Menu bar, select **Application > ACD Admin**.
3. In the ACD Main screen, click the **Service** link located under the Quick Link section.
4. From the ACD Service – Status screen, select and shut-down all services.
5. When all of the ACD Services have shut-down close the ACD Admin screen.

To use the Windows® Remote Desktop you must know the ACD system IP address. To find the current ACD system IP address login to Enterprise Manager. Select **Maintenance > Initial Setup**. In the ACD Config section, the ACD IP address will be displayed.

6. Log into the Windows® 7 operating system Desktop using a Windows Remote Desktop connection.
7. Download the "ToshibaACD-1.0.19.zip (03/17/16)" zip file from the FYI website. Login to the FYI website. Select IPedge / VIPedge > Software. Scroll to WebACD for Windows Virtual Machine (required for IPedge 1.7.4) section. Click on the ToshibaACD link to the zip file.

The ACD files must be extracted to the Windows operating environment on the IPedge server. If a high speed internet connect from the IPedge server is not available Toshiba recommends that you download the zipped file from the FYI website onto a USB drive. The files can be extracted from the USB drive onto the IPedge server.

8. Unzip the "ToshibaACD-1.0.19.zip (03/17/16)" file on the Window 7 System to retrieve the following files;

- Strata Unifier Vxxzip
- Toshiba\_ACD\_Vx\_Setup.zip
- Toshiba\_Call\_Router\_Vx\_Setup.zip
- Toshiba\_DbAssist\_Vx\_Setup.zip
- Toshiba\_Email\_Vx\_Setup.zip
- Toshiba\_TTS\_Vx\_Setup.zip
- Toshiba\_VA\_Editor\_Vx\_Setup.zip
- Toshiba\_VA\_Vx\_Setup\_HMP.zip
- Toshiba\_WebACD\_Vx\_Setup.zip

**Note:** Use the latest version available on the FYI website.

9. Unzip each ACD Component file listed above. The following files will be used to start the upgrade process;

- Strata Unifier Vx.exe
- Toshiba\_ACD\_Vx\_Setup.exe
- Toshiba\_Call\_Router\_Vx\_Setup.exe
- Toshiba\_DbAssist\_Vx\_Setup.exe
- Toshiba\_Email\_Vx\_Setup.exe
- Toshiba\_TTS\_Vx\_Setup.exe
- Toshiba\_VA\_Editor\_Vx\_Setup.exe
- Toshiba\_VA\_Vx\_Setup\_HMP.exe
- Toshiba\_WebACD\_Vx\_Setup.exe

10. To run an upgrade .exe file, right-click a file and select **Run as Administrator** from the file option menu list. From the listed upgrade executable files below, perform the ACD Software component upgrade in the following order.

1. Toshiba\_WebACD\_Vx\_Setup.exe
2. Toshiba\_ACD\_Vx\_Setup.exe
3. Toshiba\_VA\_Editor\_Vx\_Setup.exe
4. Toshiba\_VA\_Vx\_Setup\_HMP.exe
5. Strata Unifier Vx.exe
6. Toshiba\_Email\_Vx\_Setup.exe
7. Toshiba\_Call\_Router\_Vx\_Setup.exe
8. Toshiba\_DbAssist\_Vx\_Setup.exe

## 9. Toshiba\_TTS\_Vx\_Setup.exe

**Note:** It is highly recommended to re-boot the Windows 7 system if the ACD Software components ask you to re-start the system during or after the installation process.

11. After all of the ACD Software components have been upgraded, Toshiba recommends that you reboot the Windows 7 system, to finalize all the upgrade process.
12. After the reboot, login into IPedge Enterprise Manager. Select **Application > ACD Admin**.
13. From the ACD Main screen, click the **Service** link located under the Quick Link section.
14. From the ACD **Service – Status** screen, select and start all of the required and licensed ACD Software component services.  
These are the **ACD, MIS, TKI, VA Host** (Voice Anounce Host) and, **Email Assitant** services
15. Once all ACD Services are running the upgrade process is complete. Wait for the status of each to be; **running**.

**PROGRAM UPDATE PROCEDURE**

The IPedge program update process is controlled through Enterprise Manager. The software update can be performed using three different methods.

- **Online Update** — IPedge systems running R1.5.1 and later can use the online update to download the needed file from a FTP server maintained by Toshiba. Connection to the Internet and permission to access and use an FTP server is required.
- **Remote Update** — The update files are downloaded to the Administrator's PC or saved onto the Primary IPedge server in a multi-node system.
- **Local Update** — The update files are loaded onto a USB flash drive. This process requires the administrator to plug the flash drive into the IPedge server.

---

**CAUTION! The IPedge system must be running for at least 20 consecutive minutes before starting a program update process.**

---

---

**CAUTION! Remove Enterprise Manager Redundancy, if configured before upgrading the system software.**

---

A **Local Program Update** is performed while on site, with physical access to the IPedge server. Local means that the update files are on a USB drive connected to the IPedge server. Program Update can update

the IPedge core software, the Linux operating system and the Media Library. The program update file can be accessed from a USB drive connected to the IPedge server.

**Note:** The IPedge system must be running for at least 20 consecutive minutes before starting a program update process.

A **Remote Program Update** means the administrator may not be on site. The update files are loaded on an IPedge server in the network or loaded on the administration PC.

**Important!** Perform a manual database backup using the **Webmin > IPedge > Backup and Restore** tool before the software update. This backup file will be used in the event you choose to roll back the update. Store the backup file off of the IPedge server.

## ONLINE UPDATE

IPedge systems running R1.6.1 and later software have a program update mechanism called Online Program Update. New software updates will be available on an FTP server. The IPedge server checks the FTP server each night for new software files. When a later version software file is found the system administrator will see a notice the next time Enterprise Manager is logged into.

 [New version of software is available for upgrade.](#)

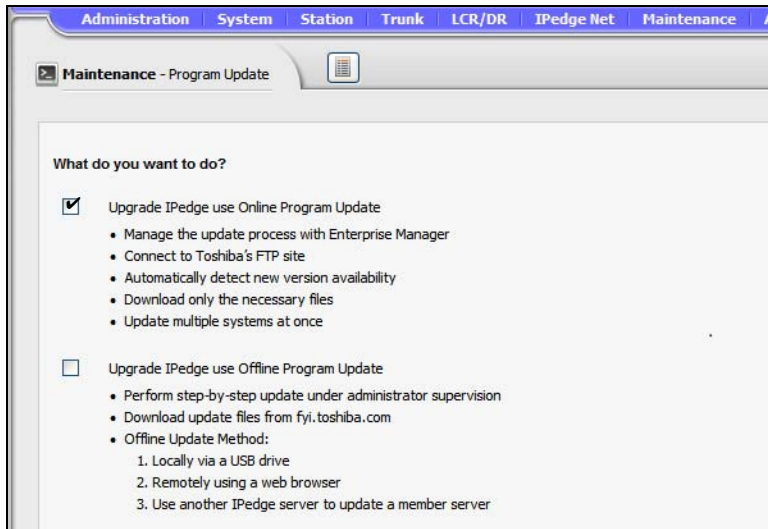
**Note:** The IPedge system must have access to the internet and be allowed FTP server access for the Online Update feature to function.

The administrator can view the update files and decide whether to run the update.

The IPedge software in the form of an RPM file can be uploaded to a predefined directory on the IPedge server. In addition to RPMs, a manifest file is provided that describes the IPedge software release. This manifest file is in xml format and contains information about the software release, release version, RPM files and release date. In Enterprise

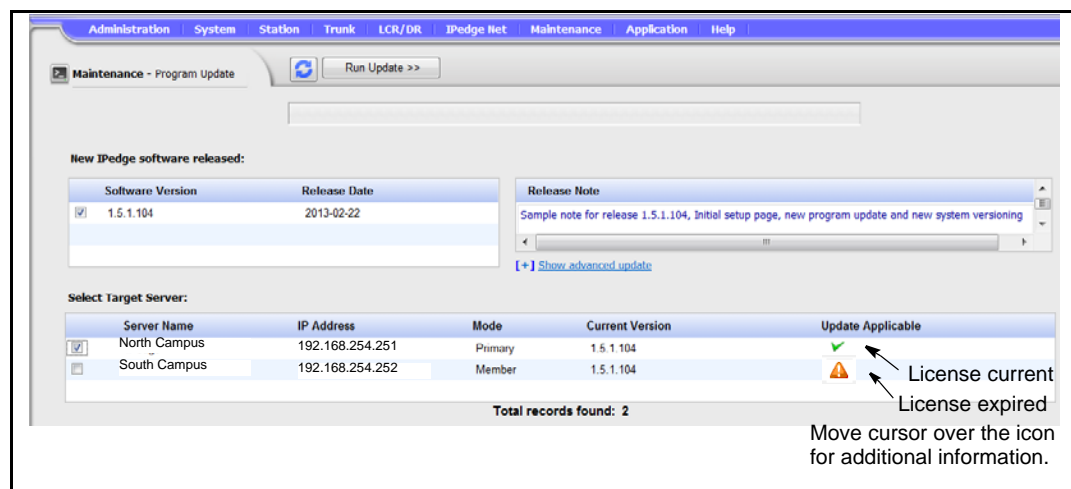


Manager select **Maintenance > System Maintenance > Program Update.**



**Version check** Enterprise Manager verifies the version when the administrator selects software upgrade. The system will allow an upgrade to be applied when the new version is the same or newer. A multi-node system Member server can only upgrade to a version the is the same or newer than the Primary server. A member server that does not have the 1.5.1-1 or later software will be displayed as 'unknown' until it has been upgraded.

**License Checking** The Online Program Update checks for a valid license before the user can select the server. If license failed on validation such as no license or maintenance license expired, the check box will be disabled.



**Language Pack** The language pack is under advanced update section. The administrator must click on the option to expand it. The default is not expanded and all languages are not checked.

The en\_US (US english language pack) is checked and disabled just for display purpose. The English language pack is always the default. Enterprise Manager will compare the langPack version and always download the latest one regardless which software the user selected.

- Software list section – List available version of software that is same or newer than local version.
- Release note display – Display the text that is in the manifest xml file.
- Server list section – List of master and member servers. It indicates license status and validates version compatibility.

Systems running R1.5.1 and later software will check the maintenance license prior to starting a program update.

All results will be logged into a history file in xml format on the IPedge server. A report viewer can display detail status of each rpm.

**Online Update Page Content**

Online program update supports multiple nodes. Multiple servers can be upgrading in parallel with the same version of selected software.

Each server in a multi-node system will download its own rpm files and will handle its own update. The Primary server will be in a waiting state while the member servers are updating. The Primary server will start its own update when all of the selected members have finished the updates.

**New IPedge software released:**

Software Version	Release Date
<input type="checkbox"/> 1.5.1.206	2012-08-25
<input checked="" type="checkbox"/> 1.5.1.207	2012-10-28

**Release Note**  
Release Note For 1

[\[+\] Show advanced update](#)

**Select Target Server:**

Server Name	IP Address	Mode	Current Version	Update Applicable
<input type="checkbox"/> North Campus	192.168.254.251	Primary	1.5.1.09	✓
<input type="checkbox"/> South Campus	192.168.254.253	Member	1.5.1.201	⚠

Total records found: 2

The current software version is same or newer than selected version.

**Update Result:** The process status will display the update process; starting, downloading, updating, and update complete.

Program update is completed. See Program Update History report for detail information.

**Program Update Process Status:** Updating to version 1.3.1.99

Server Name	IP Address	Mode	Current Version	Process Status
North Campus	192.168.254.251	Primary	1.5.1.09	⚠ Update Failed
West Campus	192.168.254.252	Member	1.5.1.201	⚠ Update Failed
Warehouse	192.168.254.253	Member	1.5.1.207	✓ Successfully Completed

Total records found: 3

- The log files reside in each server.
- Each update job creates one log file. The administrator selects the server and log file to see the summary.

**ENHANCED ONLINE UPGRADE**

IPedge systems running R1.6 and later software have an enhanced Online Program Update process. The added enhancements are:

- Re-try while downloading files from the Toshiba FTP site
- Download files and 'Wait to upgrade'
- 'Cancel' download or check download status later

**DOWNLOAD RETRIES**

If an error occurs during the upgrade files download the IPedge system will wait 30 seconds after the transfer failure then try the download again. The files successfully loaded will not need to be reloaded. The retry will continue until it completes or it is canceled by the user.

If the download is taking longer than anticipated the user can cancel the download or check the progress of the update later.

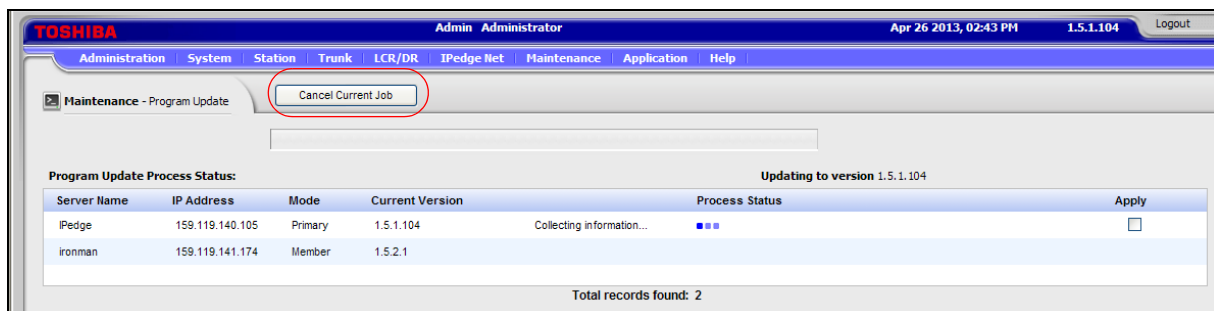
The technician can select the update to begin immediately after the download is finished or wait for a manual start command. This allows the user to do a download only then, run update when user is ready.

**Note:** When the update process is complete the IPedge server will reboot.

**Cancel Upgrade Button**

When the user starts an upgrade the **Cancel Current Job** button is visible. On a multiple server update, the cancel applies to all servers.

- This cancel button stops current running tasks.
- If server is downloading upgrade files the task is stopped immediately. All files already downloaded will be cached in the IPedge server. When the download is run again only the remaining files will be processed.
- If server is processing the call processing data back-up, the task will continue until the backup cycle is finished.
- The Cancel button cannot stop an upgrade on a server that is in the upgrading state. The server that is in upgrading state will continue its update process.



**Figure 16-1 Program Upgrade Screen**

**Wait to Upgrade**

The online program update provides an option to apply the update immediately after download or wait for customer action. The default action is download software and wait to upgrade. The user can download the upgrade files and be able to run upgrade at a later time. The user check

marks the Apply box to have the upgrade start immediately after the file download.

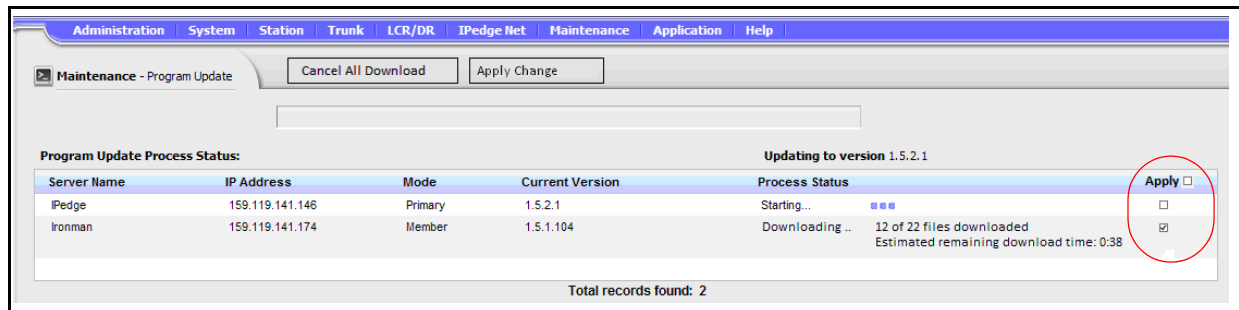


Figure 16-2 Download Then Upgrade

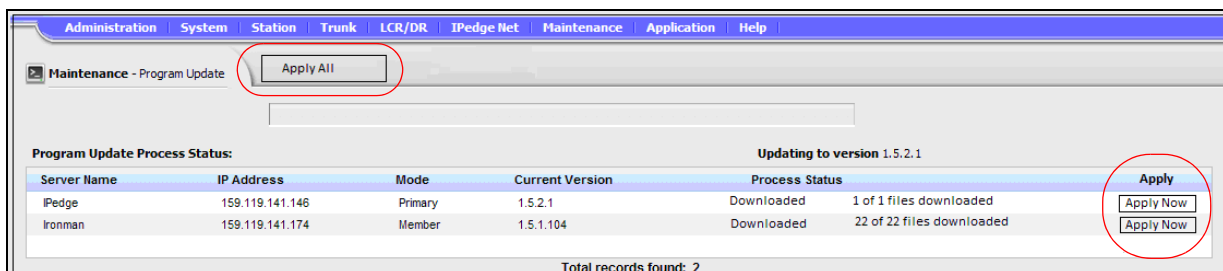
Once started, the upgrade files will continue downloading even if user is not logged into Enterprise Manager.

The option to 'Apply immediately' or 'Wait' can be changed while the file update is starting, downloading and in the waiting state.

Once a server starts upgrading the software it will continue its update process. At this point the Cancel button will be disabled.

The **Apply All** button will cause all of the servers in a multi-node system to update.

If the user choice is download and wait, there will be two reports generated for this update. One report for the download status and one for the update status.



**ONLINE UPDATE PROCEDURE**

The following procedures detail some of the upgrade files download and system upgrade processes that IPedge systems running R1.6 and later software can run.

**Wait Then Apply Update**

1. Login to Enterprise Manager.
2. Navigate to **Maintenance > System Maintenance > Program Update**.

3. Select **Online Program Update**.
4. Select software version.
5. Select target server(s).
6. Click on **Run**. The server will download the upgrade files.
7. When the server has finished the file download click on **Apply Now** to update.

**Notes:**

- A. The online update feature will only download the required update files.
- B. If the download fails Enterprise Manager will retry the download until is successful or the administrator cancels the download.
- C. When upgrading multiple servers the data connection is shared by all of the servers.
- D. The time required to download the upgrade files and complete the upgrade process varies by server type and the size of the update file(s).
- E. In locations with low bandwidth it may be more efficient to upgrade one server at a time.

**Change and Apply Immediately**

This procedure is used to download updates and apply the updates immediately.

1. Login to Enterprise Manager.
2. Navigate to **Maintenance > System Maintenance > Program Update**.
3. Select **Online Program Update**.
4. Select software version.
5. Select target server(s).
6. Click on **Run**. The server will download the upgrade files.
7. Click to check-mark the **Apply** box next to each server.
8. When the server has finished the file download the upgrade will begin.

**Wait and Apply Later**

1. Login to Enterprise Manager.
2. Navigate to **Maintenance > System Maintenance > Program Update**.
3. Select **Online Program Update**.
4. Select software version.
5. Select target server(s).
6. Click on **Run**. The server will download the upgrade files.
7. User log out or navigate to other page.
8. When ready to start the upgrade, Navigate to **Maintenance > System Maintenance > Program Update**.

9. The server upgrade status will be displayed. (as Illustration 3)
10. Click on **Apply Now]** to start the upgrade.

**Change To Apply Immediately**

The default update condition is download files then wait for a manual upgrade start. This procedure changes the system to start the upgrade as soon as the download is complete.

1. Login to Enterprise Manager.
2. Navigate to **Maintenance > System Maintenance > Program Update**.
3. Select **Online Program Update**.
4. Select software version.
5. Select target server(s).
6. Click on **Run**. The server will download the upgrade files.
7. Click to check-mark the **Apply** box.

**Change To Wait**

This procedure changes the system from 'start the upgrade as soon as the download is complete' to download and wait.

1. Login to Enterprise Manager.
2. Navigate to **Maintenance > System Maintenance > Program Update**.
3. Select **Online Program Update**.
4. Select software version.
5. Select target server(s).
6. Click on **Run**. The server will download the upgrade files.
7. Click the **Apply** check box. This step set the system to start the upgrade as soon as the file download is complete.
8. Commit changes.
9. Anytime before the upgrade starts uncheck the **Apply** check-box.
10. Commit changes.

**Cancel Update**

1. Login to Enterprise Manager.
2. Navigate to **Maintenance > System Maintenance > Program Update**.
3. Select **Online Program Update**.
4. Select software version.
5. Select target server(s).
6. Click on **Run**. The server will download the upgrade files.
7. Anytime before the software upgrade starts click on **Cancel All Download**.

8. Click on **Yes** to confirm.
9. The server upgrade will abort. **Note:** If the server is in the update state, the update job will continue.

**Remove One Server From Upgrade**

When an upgrade on a multi-node system has been started, one, or more, of the nodes can be removed from the upgrade.

1. Login to Enterprise Manager.
2. Navigate to **Maintenance > System Maintenance > Program Update**.
3. Select **Online Program Update**.
4. Select software version.
5. Select target server(s). For example; A, B and C.
6. Click on **Run**. The servers will download the upgrade files. For example: A=5/10, B=6/10 and C=1/10.
7. Click on **Cancel All Download**.
8. Click on **Yes** to confirm.
9. Downloads for all servers are aborted.
10. Select software version
11. Select target server(s). For example; A and B.
12. Click on **Run**. The servers will download the upgrade files. For example: A=6/10, B=7/10.

**Add A Server to the Update**

1. Login to Enterprise Manager.
2. Navigate to **Maintenance > System Maintenance > Program Update**.
3. Select **Online Program Update**.
4. Select software version.
5. Select target server(s). For example; A and B.
6. Click on **Run**. The servers will download the upgrade files. For example: A=5/10 and B=6/10.
7. Click on **Cancel All Download**.
8. Click on **Yes** to confirm.
9. Downloads for all servers are aborted.
10. Select software version
11. Select target server(s). For example; A, B and C.
12. Click on **Run**. The servers will download the upgrade files. For example: A=6/10, B=7/10, and C starts from 0/10.

**Note:** When the software upgrade starts the Cancel button will be disabled.

13. The update results will be displayed.

The screenshot shows the 'Maintenance - Program Update' window. At the top, there is a navigation menu with 'Administration', 'System', 'Station', 'Trunk', 'LCR/DR', 'IPedge Net', 'Maintenance', 'Application', and 'Help'. Below the menu, the title is 'Maintenance - Program Update' with a 'Back' button. A 'Servers:' dropdown menu is set to 'VoiceCustomer1'. Below this is a date and time stamp: 'Wed Mar 13 16:07:36 PDT 2013'. A 'Result Summary' section contains a table with update statistics. Below that is a 'Downloaded RPM List' table with columns for the package name and the result.

Result Summary (Click for individual rpm result)		
Update Type: Online	System Old Version: 1.5.1.105	System Updated Version: 1.5.1.106
Update result:	true	Successfully Completed
Total number of files to download: 7	Successful: 7	Failed: 0
Total number of files to update: 5	Successful: 5	Failed: 0

Downloaded RPM List	Result
Cell-1.5.1.4-036.rpm	true
ipedge-langpack-en_US-packages-1.1.1.305-1.noarch.rpm	true
ipedge-components-packages-1.5.1.106-1.noarch.rpm	true
ipedge-gum-10.5.4.24-036.rpm	true
igs-libsip-1.5.17-1.036.rpm	true
ipedge-media-libraries-packages-1.5.1.106-1.noarch.rpm	true
ipedge-ssl-firmware-packages-1.5.1.106-1.noarch.rpm	true

### Download Then Apply Update

This procedure is used to download updates then, apply the updates.

1. Navigate to **Maintenance > System Maintenance > Program Update**.
2. Select **Online Program Update**.
3. Select the software version.
4. Select the target server(s).
5. Click on **Run**.
6. The server will download the update files.
7. When the server has finished the download click on **Apply Now** to start the update.

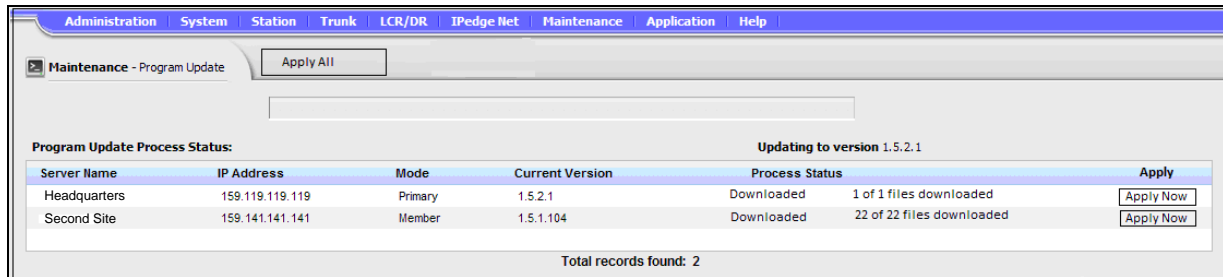
### Download and Update Apply Later

This procedure is used to download updates then, apply the updates at a later time.

1. Navigate to **Maintenance > System Maintenance > Program Update**.
2. Select **Online Program Update**.
3. Select the software version.
4. Select the target server(s).
5. Click on **Run**.
6. The server will download the update files.
7. The administrator can log out or navigate to another page.
8. When you want to update the system login to Enterprise Manager, and navigate to **Maintenance > System Maintenance > Program Update**.



9. The server status will be displayed.

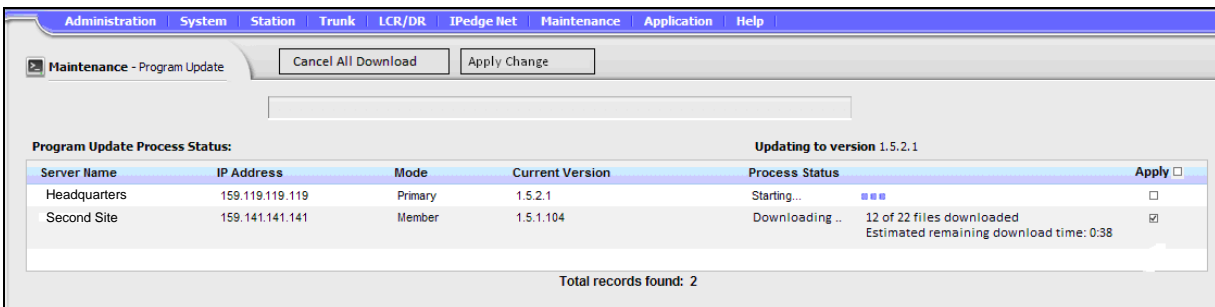


10. Click on **Apply Now** to update.

**Change and Apply Immediately**

This procedure is used to download updates and apply the updates immediately.

1. Navigate to **Maintenance > System Maintenance > Program Update**.
2. Select **Online Program Update**.
3. Select the software version.
4. Select the target server(s).
5. Click on **Run**.
6. The server will download the update files. Apply check-boxes will be displayed.



7. Click to check-mark the **Apply** box.
8. The update will begin as soon as the download is complete.

**Note:** If the Apply check-box is un-checked before the update starts the system will wait until you click on the Apply Now button. Once the update starts it cannot be canceled.

**Load Update Files then Wait**

1. Navigate to **Maintenance > System Maintenance > Program Update**.
2. Select **Online Program Update**.
3. Select the software version.
4. Select the target server(s).
5. Click on **Run**.

6. The server will download the update files.
7. Click to mark the **Apply** check box and the system will start the update as soon as the all files are downloaded.
8. Uncheck the **Apply** check-box before the download is finished for the system to wait after loading the update files. Click on the **Apply Now** button or the **Apply All** button start the update.

**Cancel Update**

Steps 1 through 5 start the update file download process. The download can be canceled anytime before it is complete, step 7. Any update files that were downloaded before the Cancel was clicked will be retained. When the update is attempted later these files will not need to be downloaded again.

1. Navigate to **Maintenance > System Maintenance > Program Update**.
2. Select **Online Program Update**.
3. Select the software version.
4. Select the target server(s).
5. Click on **Run**.
6. The server will download the update files.
7. Click on the **Cancel All Download** button.
8. Confirm (yes) the cancelation.
9. The download for that server will be aborted. If a server is in the update state, the update job continue.

**Remove One Server from the Update**

To remove a server from the update process all of the downloads are canceled then, the update is started with the appropriate servers selected.

1. Navigate to **Maintenance > System Maintenance > Program Update**.
2. Select **Online Program Update**.
3. Select the software version.
4. Select the target server(s) you wish to remove from the update process.
5. Click on **Run**.
6. Enterprise Manager will display the download progress for the selected servers (i.e.: downloading files. A=5/10, B=6/10 and C=1/10).
7. Click on the **Cancel All Download** button. Confirm the cancelation.
8. The incomplete downloads will be canceled.

**Finish the Download for the Other Servers**

9. Select software version
10. Select the servers you want to update.
11. Click on **Run**.

12. The selected servers will finish downloading the update files.

### Add a Server to the Update

To add a server to the update process all of the downloads are canceled then, the update is started with the appropriate servers selected.

1. Navigate to **Maintenance > System Maintenance > Program Update**.
2. Select **Online Program Update**.
3. Select the software version.
4. Select the target servers, the servers that are downloading update files.
5. Click on **Run**.
6. Servers that are downloading files will be displayed.
7. Click on **Cancel All Downloads**. Confirm the cancelation.
8. The downloads will be aborted.
9. Select software version.
10. Select target servers.
11. Click on **Run**.
12. The servers will download the required files.

#### Notes:

- The update file download can be canceled anytime. All files that had finished loading will be retained. On the next file download those files will not download again.
- The server update process can not be stopped once it has started.

### OFFLINE UPDATE PROCEDURE

The offline update uses files loaded on a USB flash drive or onto one of the IPedge servers in the same network as the server being updated.

### LOCAL UPDATE

The local update process requires the system administrator to load the update files to a prepared USB flash drive and be present on site during the update process. In Enterprise Manager select **Maintenance > Program Update** then check-mark **Upgrade IPedge use Offline Program Upgrade**.

### USB Drive Requirements

The following are the USB drive requirements for successful IPedge Program Update:

- The USB drive must be Linux mountable. Some USB drives on the market contain an auto\_start feature or custom driver which is not Linux compatible.
- The USB drive recommended capacity is 4G Byte or more
- Supported file format FAT, FAT32 ISO9660

- The update folder must be created in the USB then, the update programs are written into this folder.

**Important!** The update files must be loaded into a folder named **update** on the root directory of the USB drive.

### Update File Source

Update files can be downloaded from the Toshiba FYI website or the Toshiba TSD Technical Support website. The update files are TGZ format.

**Important!** Before starting this procedure use a PC to perform a virus test on the USB flash drive.

1. Download the compressed update file from a Toshiba website to your PC.
2. Create a folder named **update** on the root of the USB drive.
3. Copy the files to the update folder on a USB drive. Do not extract (un-compress) the files.

The update file can then be loaded onto:

- The IPedge server (update target server) or
- Another IPedge server

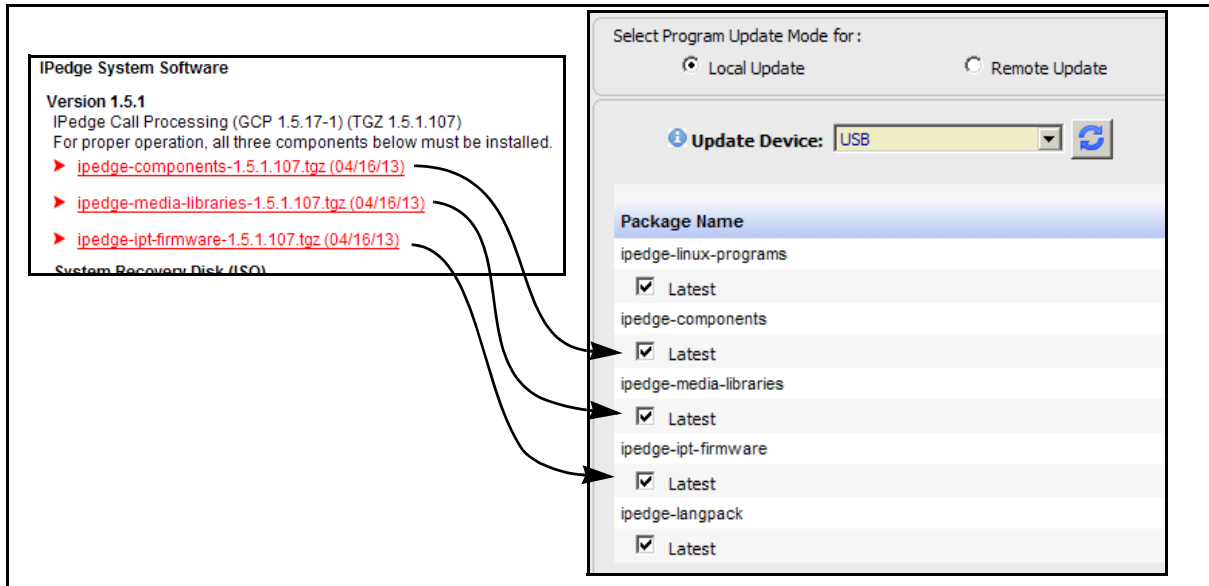
### Update Procedure

1. In Enterprise Manager select **Maintenance > System Maintenance > Program Update**.
2. In the Select Target Server screen click to check-mark the server you will update then click on the **Next** button.

Select the update mode.

- **Local Update** - The update file is in the update folder on a USB drive connected to the IPedge server. Go to [Step 3](#).
  - **Remote Update** - The update file is on the PC used to connect to the IPedge server. Refer to "[REMOTE UPDATE PROCEDURE](#)" on [page 16-19](#).
3. When Local Update is selected, select USB in the Update Device menu.

4. Check-mark the boxes with the same names as the tgz files downloaded from the FYI website.



5. If the update files are already extracted click on the **Skip** button to skip the extract process and start the file update process.  
— OR —  
Select the files to be used then, click on the **Extract** button. The extract button will extract the compressed file and copy it to the target IPedge server.

**Note:** The file will only extract if it is newer than a file already on the server.

6. When the file extraction is complete the **Run update** button will appear. Click to run the update then, go to [Step 8](#). If the update file is not a newer file than what is already on the IPedge server the Run update button will not appear.

7. Select the IPedge server that has the extracted update files available.

**Note:** If the target server is already running the same software version of the download, Enterprise Manager will advise that no update is necessary and the Run update button will not appear.

8. Some updates will cause a system restart. If this occurs Enterprise Manager will logout. If the server does not restart the update complete screen will be displayed.

**Important!** Remove any USB device except the license dongle from the server before the reboot. **DO NOT** remove the license dongle.

9. Login to Enterprise Manager.

10. Synchronize the database.

**REMOTE UPDATE PROCEDURE**

A Remote Program Update can preformed from anywhere. Remote means that the update files are loaded on an IPedge server in the

network or on the PC used to access Enterprise Manager. Program Update can update the IPedge core software, the Linux operating system and the Media Library. The program update file can be accessed from a USB drive connected to the IPedge server.

**Important!** Perform a manual database backup using the **Webmin > IPedge > Backup and Restore** tool before the software update. This backup file will be used in the event you choose to roll back the update.

### Upgrade Primary Server

1. In Enterprise Manager select **Maintenance > System Maintenance > Program Update**.
2. Select **Upgrade IPedge using Offline Program Update**.
3. Click **Next**.
4. In the Select Target Server screen click to check-mark the server you will update (the **Primary** server) then click on the **Next** button then, select **Remote Update** mode.
5. Select the IPedge server that has the extracted update files available. Check-mark **From other IPedge server** then, select the server from the pull-down list. Go to [Step 7](#).  
- OR -  
From the Primary IPedge server only; Check-mark **From Client computer** then, **Click to upload files**. Click to **Browse** to the update file.
6. Click to **Extract** the file(s) then go to [Step 9](#).
7. Click on the **Download File** button.
8. When the file download is complete the **Run update** button will appear.
9. Click on the **Run update** button to start the update process.

**Note:** If the target server already has updates Enterprise Manager will advise that no update is necessary and the Run update button will not appear.

10. Some updates will cause a system restart. If this occurs Enterprise Manager will logout. If the server does not restart the update complete screen will be displayed.
11. If a manual reboot is required you will be prompted to reboot the server.

### Member Server

1. In Enterprise Manager select **Maintenance > System Maintenance > Program Update**.
2. Select **Upgrade IPedge using Offline Program Update**.
3. Click **Next**.
4. In the Select Target Server screen click to check-mark the server you will update (a **Member** server) then click on the **Next** button then, select **Remote Update** mode.

5. The **From other IPedge server** will be selected, select the server from the pull-down list. Go to [Step 7](#).
6. Click on the **Download File** button.
7. When the file download is complete the **Run update** button will appear.
8. Click on the **Run update** button to start the update process.

**Note:** If the target server already has updates Enterprise Manager will advise that no update is necessary and the Run update button will not appear.

9. Some updates will cause a system restart. If this occurs Enterprise Manager will logout. If the server does not restart the update complete screen will be displayed.
10. If a manual reboot is required you will be prompted to reboot the server.

## SYSTEM REBOOT

Some program update procedures require that the System Administrator reboot the system.

**Important!** Remove any USB device except the license dongle from the server before the reboot. DO NOT remove the license dongle.

1. Select **Maintenance > System Maintenance > System Processes**.
2. Select the target server from the pull-down list.
3. Click on the **Reboot system** icon.

## MESSAGING DCN

This procedure is for systems using Messaging DCN. DCN must be disabled on all nodes before upgrading to R1.6.

1. Backup the messaging database in the primary node.

**Important!** Store the backup file to a location that is not on the IPedge server.

2. Use the **Utilities > Push Mailbox** menu to set the home node for all users to **0** (not blank).

**Note:** If this parameter is not changed before DCN is disabled message waiting lights will not function after the upgrade to R1.6 software, until the DCN cluster is re-created.

3. Disable DCN in **Registry > Parameters**:
  - A. **Dbsync** - uncheck and clear the value.
  - B. **Node number** - uncheck and clear the value.
  - C. Click on **Save**.

- D. Delete the DCN nodes on each server in the cluster.
- E. Select **Site Parameters > Cluster**. Check-mark in the Delete column Next to each Node.

**Note:** If this is a Primary / Member configuration each Member must be configured under **Administration > Component Services > Server Application > Messaging** with the actual IP address of the Member Node.

Access each messaging node individually **Application > Messaging** <select node from the drop down box> and repeat Step 3E.

- F. Click on the **Save** icon.
- G. Restart the Messaging service using Webmin.

4. Stop Messaging in each node.
  - A. In Enterprise Manager select **Application > Webmin**, select the server as needed.
  - B. In Webmin select **System > Bootup and Shutdown**.
  - C. Scroll down, check-mark the **t3vm** box then, scroll to the bottom of the screen to click on the **Stop** button.
5. When Messaging has stopped in all nodes, start Messaging in each node.
  - A. In Enterprise Manager select **Application > Webmin**, select the server as needed.
  - B. In Webmin select **System > Bootup and Shutdown**, scroll down, check-mark the **t3vm** box.
  - C. Scroll to the bottom of the screen to click on the **Restart** button.
6. Backup the messaging database in each of the nodes after Messaging has started up.

**Important!** Store the backup file to a location that is not on the IPedge server.

**Create a Cluster** Use the Create Cluster wizard to create the cluster in the IPedge Primary node only.

- First Node
1. In Enterprise Manager select **Applications > Messaging**.
  2. Select the Primary node.
  3. in the Messaging menu select **Site Parameters > Cluster**.
  4. Click on the **Start Cluster Wizard** icon.
  5. In the Node ID field enter the DCN node number.
    - For 10.5.4.x systems the first node ID is always 1. Remaining Nodes must be in sequence. For example; 2, 3.
    - For 10.6.1.x system the node ID's do not have to be in sequence. For example; 11, 15, 17 etc.



- 
- Add a Node
6. In the IP Address field enter the IP address of the node you identified in step 5.
  7. Click on **Next**.
  8. Enter the next DCN node number.
  9. Enter the IP address of this IPedge node.
  10. Enter the IPedge username 'admin'.
  11. Enter the password for the account 'admin' (the factory default password should have been changed during IPedge server installation (see chapter 4 in the IPedge Install manual). Confirm the admin password.
  12. Enter the admin password for this node.
  13. Enter the password for the account 'root' (the factory default password should have been changed during IPedge server installation (see chapter 4 in the IPedge Install manual). Confirm the root password.
  14. Click on **Next**.
  15. If there is another node go to [Step 8](#). If this was the last node click on **Finish**.
  16. The wizard will display a list of the nodes and their IP addresses. If the list is correct click on **Create Cluster**. If there is an error click on **Back**.
  17. When the cluster has been created the wizard will display a Cluster created successfully message.
  18. Restart Messaging service.

**Note:** Once the DCN wizard has been run on one of the nodes in the network, it cannot be run on any other nodes in the network. The DCN wizard can only be run again on the same node where the wizard was first run.

This page is intentionally left blank.

# Chapter 17 – ESXi Update

---

## REQUIRED ITEMS

- Update ISO file, one file per CD
- External USB CD / DVD drive (if the server does not have one)
- Monitor and keyboard

## DOWNLOAD the ESXi UPDATE FILE

Download the VMware ESXi (Hypervisor) update version specific to your hardware from the [www.Dell.com](http://www.Dell.com) website to your computer. This will be an ISO image file. Burn the ISO file to a CD or DVD.

To determine the required ISO file you must know the server service tag number and the version of ESXi running on that server. To determine the ESXi version launch the vSphere client on your PC and login to the server. The ESXi version is displayed on most screens.

1. Navigate to [www.Dell.com](http://www.Dell.com).
2. Select **Support > Support by Product**
3. Enter the service Tag number of the server, click on **Submit**.
4. Verify that the correct server model is displayed. Click on **Drivers & downloads**.
5. Click on **Change OS**. Note; you may need to click on the Find it myself tab under Optimize your system with drivers and updates, to reveal the Change OS link.

**Note:** If the list of operating systems does not include ESXi contact Toshiba's Technical Support department.

6. Select VMware ESXi version your server is running (5.5 or 6.0 )
7. Click on **Enterprise Solutions**.
8. Download the latest update.

## Shut Down Virtual Machines

1. Login to vSphere Client.
  - A. If ACD is running, click on the IP address in the left column to select the virtual machine.
  - B. In the right side of the screen click on **Shutdown virtual machine**.
  - C. Wait for the option; **Power on** to appear in the Basic Tasks list. This indicates that the virtual machine has stopped. Do not select power down.
  - D. Select the IPedge virtual machine, click on the IP address in the left column.

- E. In the right side of the screen click on **Shutdown virtual machine**. Do not select power down.
- F. Wait for the option; **Power on** to appear in the Basic Tasks list. This indicates that the virtual machine has stopped. This may take a few minutes.

- 2. Plug in the monitor and keyboard. Refer to the IPedge Virtual Server Install manual.

**Note:** If the system does not have a built in CD/DVD ROM drive, such as the Dell R220 series, you will need an external USB CD/DVD drive.

- 3. Ensure that the CD with the update ISO file is in the CD ROM drive and the drive is connected to the server.
- 4. When the virtual machine(s) have shutdown go the monitor and keyboard. Press the **F12** key.

**Note:** If the message **Forcefully terminating running VMs** appears return to the vSphere display to ensure that the virtual machines have shut down. Do not 'forcefully' terminate the virtual machines.

- 5. When prompted enter the user name and password.
- 6. When prompted, press **F11** to restart. The screen will display a restart message.

**Note:** The vSphere connection will be lost.

- 7. When the F11 for Boot Manager prompt is displayed press the **F11** key.
- 8. For servers with a CD/DVD drive ensure that the Optical Drive selection is highlighted. then press **Enter**.

For other servers Arrow down to highlight the (one shot) BIOS manager. Then, press the **Enter** key.

- 9. Ensure that Optical Device is highlighted, press the **Enter** key.
- 10. Update on CD should be highlighted, the boot process will start automatically in a few seconds.

**ESXi Update Installation**

- 11. The screen will display a Welcome to the VMware ESXi Installation message. Press the **Enter** key to continue.
- 12. Read and accept the EULA then, press the **F11** key.
- 13. Select a disk to install.  
For servers running VMware on an internal SD select the Dell IDSDM then, press **Enter**.  
For servers running VMware on the Hard Disk Drive select the HDD then, press **Enter**.
- 14. At the ESXi found prompt arrow to select **Upgrade** then press the **Enter** key.
- 15. At the confirm Upgrade prompt press **F11**.
- 16. When the upgrade is complete remove the CD ROM then, press the **Enter** key to reboot.

17. Login to the vSphere client. Select the Summary tab.
18. Right-click on the IPedge VM in the left column. (Notice that the VMware Tools show; Running (Out of date).
19. Select Guest > Install/Upgrade VMware Tools.
20. Click to select Automatic Tools Upgrade then, click on **OK**.
21. VMware Tools show; Not Running while the Tools upgrade is in process.
22. When the VMware Tools upgrade is complete the display will change to Running (Current).

End of ESXi upgrade procedure.



# Chapter 18 – IPedge Software Only

---

## SOFTWARE ONLY SERVER

Toshiba's IPedge Software-only product integrates Toshiba's IPedge phone system application with a VMware Virtualized server architecture in a customer's VMware infrastructure. IPedge Software-only is compatible with VMware 5.5 and 6.0. The IPedge OVA software package can be downloaded from the Toshiba public FTP server. Also, with the purchase of a Software-only package, a USB drive containing the IPedge OVA file will be shipped.

### IPedge Requirements

IPedge Software-only can be installed on any VMware-certified hardware, such as, Dell and HP servers, that meets the specifications for each IPedge system class (EP/EC/EM) requirement below. Login to vSphere Client to check the CPU speed (CPU Available Capacity) and Memory Available Capacity in the server ESXi **Resource Allocation** tab to determine whether the IPedge virtual machine can be deployed.

IPedge Class	vCPU <sup>1</sup>	CPU Speed <sup>2</sup>	Reserved CPU Speed <sup>3</sup>	Memory	Reserved Memory <sup>4</sup>	Disk Speed	Disk Space
EP	4	5 GHz	3 GHz	3.6 GB	3.6 GB	80MB/s	250 GB
EC	4	6.5 GHz	4 GHz	3.6 GB	3.6 GB	80MB/s	250 GB
EM	8	12 GHz	8 GHz	11.6 GB	11.6 GB	80MB/s	250 GB

1. The number of virtual CPUs (CPU cores).
2. Available Capacity (CPU) must be greater than the Reserved CPU Capacity. (vCPU number) x (clock speed per CPU core) must be greater than CPU Speed requirement.
3. This is the CPU speed that will be reserved when the OVA is deployed.
4. Memory "Available Capacity" must be larger than "Reserver Memory."  
Memory "Total Capacity" must be larger than "Memory."

### Important!

If equipped, ACD requires an additional 3.6 GB of reserved memory, 4 GHz reserved CPU speed and 250 GB of disk space. Refer to [ACD REQUIREMENTS on page 18-2](#).

### Over Capacity Server

IPedge Software-only removes the restriction that prevented lower capacity IPedge software from running on higher end hardware, for example:

- Apply EP License to an EC or EM capable server
- Apply EC license to an EM capable server

**ACD REQUIREMENTS**

In order to ensure correct operation, ACD software installation must be done by the Toshiba Technical Support group. Please purchase TECHSUPT-ACDVM and arrange the installation schedule with Technical Support.

**ACD Software Requirements**

Customers need Windows Server 2012 R2 Standard Edition operating system installed on their server. A Client Access License (CAL) is required for each ACD administrator and/or TASKE supervisor.

**ACD Virtual Machine Requirement**

The list below shows the **minimum** requirement for virtual machine resource allocation to run ACD. Toshiba recommends allocating 8 GB of memory, especially when TASKE is used in a high traffic environment.

Reserved CPU Speed	Reserved Memory <sup>1</sup>	Disk Speed	Disk Space
4 GHz	4 GB	80MB/s	250 GB

1. Toshiba recommends allocating 8GB of memory, especially when TASKE is used in a high traffic environment.

**ACD License Requirements**

In order to run Toshiba ACD on the virtual machine the I-ACD-SYS-VS ACD system license is required. All other optional ACD licenses including Unifier license can be applied. When TASKE is necessary, please purchase TASKE dongle (H-TASKE-LICKEY) and necessary TASKE license parts.

**VMWARE® LICENSE**

The VMware must be licensed to the customer. If the customer VMware is not licensed the IPedge system software will not run or may stop running.

**ESXi VERSION**

IPedge Virtual Servers use ESXi VMware 5.5 or 6.0 based on system type.

- IPedge Virtual EP servers run ESXi 6.0 VMware,
- IPedge Virtual EC and EM servers run ESXi 5.5 VMware.

**INSTALL vSPHERE CLIENT**

To copy the license key onto the server you must have vSphere Client on your administration PC.

Refer to [VMWARE® LICENSE on page 1-6](#), [ESXi VERSION on page 1-5](#) and [vSphere Installation on page 1-7](#) for VMware and vSphere installation instructions if VMware is not installed on your server.

**NETWORK TIME PROTOCOL SYNCHRONIZATION**

A network time protocol service must be assigned to keep the virtual machines synchronized. The IPedge Virtual Servers will ship with a default NTP service pointer (north-america.pool.ntp.org). Toshiba recommends that the VMware be configured with the same NTP service. Note that a time server pool should be referenced, not a single server.



The Network Time Protocol (NTP) is a protocol for synchronizing the server clocks on a data network. NTP uses UDP on port 123 as its transport layer.

Refer to [NETWORK TIME PROTOCOL SYNCHRONIZATION on page 1-13](#) for the NTP synchronization procedure if you do not have your VMware NTP setup. If you are using a different NTP source change the IPedge setting.

**NETWORK REQUIREMENTS**

Refer to [Network Requirements on page 2-1](#) for the network requirements. IP addresses required, access to public domains and open port requirements are covered.

**OVA INSTALL**

Refer to [Deploy OVA Template on page 15-1](#) for the IPedge OVA deployment. Contact Toshiba's Technical Support department for IPedge and ACD OVA installation.

**IPedge SYSTEM LICENSES**

The IPedge server must be licensed using Toshiba's on-line Virtual Licensing Server or the off-line, dongle based license. For on-line licensing refer to the IPedge Virtual Licensing Service User Guide available on Toshiba's FYI website.

**OFF-LINE LICENSE DONGLE**

If you are installing a system using the off-line, dongle based licensing refer to [USB PASS-THROUGH on page 4-7](#).

**IPedge MIGRATION To SOFTWARE ONLY**

This section covers the requirements and processes to migrate from a turnkey IPedge branded server or Dell server based IPedge system to the Toshiba Software Only solution.

IPedge virtual systems running on branded servers and IPedge virtual servers running on Dell machines can be migrated to a software-only solution.

Toshiba's ACD application and the TASKE™ system can also be moved as a software only solution into the customer's VMware environment.

The migration can be like to like, EP to EP, EC to EC or EM to EM. The migration can be combined with a server upgrade such as IPedge EP branded server to IPedge EC software only. Upgrades to a different class (i.e.: IPedge EC to IPedge EM) requires a manual transfer by Customer Service. Contact Toshiba's Sales Application Desk or your Toshiba Sales Engineer for a quote.

IPedge systems must be running IPedge 1.6.2-359 or later software to migrate to a Software-only solution.

Ensure that the customer's VMware environment can support the IPedge software and, as needed, the ACD application. Refer to [SOFTWARE ONLY SERVER on page 18-1](#).

In order to transfer licenses, all systems be current in the maintenance program. If not, the SUS coverage must be extended before the transfer.

**MULTI-NODE SYSTEMS**

Each node of a multi-node system must be detached, updated as needed then, migrated. Once the migration is complete the nodes can be attached.

**BRANDED IPedge SERVER to SOFTWARE ONLY**

IPedge branded systems must be running software release 1.6.2-359 (or later) in order to transfer the IPedge database to a Software Only system environment.

**Note:** The system must have current maintenance coverage.

1. For IPedge systems running 1.6.2-359 or later go to [Step 2](#).

Systems running IPedge 1.6 or earlier release software must first upgrade to 1.6.2-359. Refer to the IPedge Virtual Server install manual for the procedure or use the database conversion service offered by Toshiba's Technical Support department.

2. Backup all of the system databases.
  - IPedge
  - Messaging
  - ACD (if equipped)
3. Move the backup files to a location that is not on the IPedge server.

4. For systems running 1.7 or later software go to the next step. For systems running 1.6.2 software refer to the IPedge Virtual Licensing User manual, use the “System Upgrade to Virtual Licensing” procedures.
5. Deploy the IPedge Software-Only OVA to the customer’s machine.
6. If the customer has ACD or TASKE on an App Server, MAS, or an ACD stand alone system and would like to transfer the license, consult a Toshiba Sales Engineer. Systems with ACD will require Toshiba Technical Support for the ACD deployment. Contact Technical Services to schedule the ACD deployment.
7. In the IPedge Virtual Licensing Service, preform the IPedge license transfer to the new server. Contact a Customer Service representative to transfer the ACD license.
8. If necessary connect the TASKE license dongle to the software only server. The dealer must return the branded (native) server to Toshiba as scrap. Refer to [Table 18-2](#) on [page 18-8](#).
9. Apply the license key from the Licensing Service, and restore the databases.

**Important!** After the upgrade to Software Only the IPedge branded systems running 1.6.1 (or earlier) and 1.7 (or later) software must be returned to Toshiba for scrap. Refer to [Table 18-1](#) on [page 18-7](#).

**Important!** After the upgrade to Software Only the IPedge systems running 1.6.2 software on a Dell server; the license dongle must be returned to Toshiba for scrap. Refer to [Table 18-1](#) on [page 18-7](#).

### MIGRATION with SYSTEM SIZE UPGRADE

Preparation for migration with a system size upgrade is much the same as a migration without upgrade. The databases are prepared in the same manner. Contact your Toshiba Sales Engineer or the Toshiba Sales Application Desk to quote the licensing cange.

### IPedge VIRTUAL SERVER (DELL Server) TO SOFTWARE ONLY

The IPedge turn-key systems running on Dell servers were initially released with 1.6 IPedge software and used a license dongle.

1. When upgrading to a software only system the license dongle must be returned to Toshiba as scrap. If the license dongle is not returned the dealer will be charged full system license fees for that dongle. Refer to [Table 18-1](#) on [page 18-7](#).
2. For IPedge systems running 1.7 or later there is no license dongle and no need to return the Dell server. Refer to [Table 18-1](#) on [page 18-7](#).
3. Backup all of the system databases.
  - IPedge

- Messaging
  - ACD (if equipped)
- Move the backup files to a location that is not on the IPedge server.
4. For systems running 1.7 or later software go to the next step. For systems running 1.6.2 software refer to the IPedge Virtual Licensing User manual, use the “System Upgrade to Virtual Licensing” procedures.

**Important!** Dell server based IPedge systems running 1.6 software used a license dongle. The dongle must be returned to Toshiba when the licenses are transferred to the virtual license service.

5. Deploy the IPedge Software-Only OVA to the customer’s server.
6. Systems with ACD will require Toshiba Technical Support for the ACD software deployment. Contact Technical Services to schedule the software deployment.
7. Systems that include TASKE will require a TASKE license dongle. Upgrades from IPedge systems running 1.6.2 software will require a new TASKE license dongle. Contact your Toshiba Customer Service representative for a new TASKE license dongle. Upgrades from IPedge systems running 1.7 software have a TASKE license dongle. This can be used on the upgraded system. Refer to [Table 18-2 on page 18-8](#).
8. In the IPedge Virtual Licensing Service preform the IPedge and ACD license transfer to the new server.
9. Apply license key, and restore databases.
10. The Dell server can be retained for other use.

**Note:** IPedge license dongles must be returned to Toshiba. Failure to return the dongle will result in full license fees being charged to the customer.

**IPedge SOFTWARE-ONLY LICENSE PART NUMBERS**

**IPedge License Part Numbers for Software-only**

Part Number	Description
I-EP-SW	IPedge EP Software Only includes: IPedge system license: 6-users, 3-trunks, 6-UCedge Essentials, 6- mailboxes, 4-messaging channels, 4-port audio conference and a recovery USB.
I-EC-SW	IPedge EC Software Only includes: IPedge system license: 24-users, 12-trunks, 24-UCedge Essentials, 24- mailboxes, 6-messaging channels, 4-port audio conference and a recovery USB.
I-EM-SW	IPedge EM Software Only includes: IPedge system license: 32-users, 16-trunks, 32-UCedge Essentials, 32-mailboxes, 8-messaging channels, 4-port audio conference and a recovery USB.

**IPedge App Server License Part Numbers for Software-only**

Part Number	Description
I-ASEP-SW	IPedge App Server EP Software Only includes: IPedge App Server system license: 6-UCedge Essentials, 6- mailboxes, 4-port audio conference, 1-CSTA/ACD license for IPedge and CIX and a recovery USB.
I-ASEC-SW	IPedge App Server EC Software Only includes: IPedge App Server system license: 24-UCedge Essentials, 24- mailboxes, 4-port audio conference, 1-CSTA/ACD license for IPedge and CIX and a recovery USB.
I-ASEM-SW	IPedge App Server EM Software Only includes: IPedge App Server system license: 32-UCedge Essentials, 32- mailboxes, 4-port audio conference, 1-CSTA/ACD license for IPedge and CIX and a recovery USB.

**Note:** The CSTA/ACD license does not include ACD software or all of the licenses required for ACD operation. Refer to [ACD REQUIREMENTS](#).

**Table 18-1 Migration from IPedge Turn-key to Software Only**

Start	System Type	Action Required	Notes
IPedge 1.7 and later	Dell Server	License Transfer using Toshiba Virtual License Service (online)	Keep the server hardware
IPedge 1.7 and later	Branded IPedge Server	License Transfer using Toshiba Virtual License Service (online)	Return the server <sup>1</sup>
IPedge 1.6.2 <sup>2</sup>	Dell Server	Process a system upgrade to 1.7.x.	Return the IPedge dongle <sup>1</sup>
IPedge 1.6.2 <sup>3</sup>	Branded IPedge Server	Process a system upgrade to 1.7.x	Return the IPedge server <sup>1</sup>
IPedge 1.6.1 and earlier <sup>2</sup>	Branded IPedge Server	Process a system upgrade to 1.7.x	Return the server

1. A scrap fee is charged for returned hardware.
2. IPedge databases must be updated to 1.6.2-359 (minimum) before the system is upgraded to 1.7. The IPedge 1.6.2-359 (minimum) server can be upgraded directly to Software Only. Refer to the IPedge Virtual Server Install manual for upgrade procedures. A database upgrade service is available from Toshiba's Technical Support department.
3. IPedge databases must be updated to 1.6.2-359 (minimum) before the system is upgraded to 1.7. The IPedge 1.6.2-359 (minimum) server can be upgraded directly to Software Only. Refer to the IPedge Virtual Server Install manual for upgrade procedures. A database upgrade service is available from Toshiba's Technical Support department.

**Table 18-2 ACD and TASKE Migration to Software Only**

Application	System Type	Action Required	Notes
ACD	Dell Server	Use Toshiba Virtual License Service to process a system upgrade	
ACD	MAS <sup>1</sup>	Requires Sales App or Sales Engineer quote. Customer Server Rep will manually transfer licenses	Transfer Fee required
ACD	Stand Alone PC	Requires Sales App or Sales Engineer quote. Customer Server Rep will manually transfer licenses	Transfer Fee required
TASKE	MAS <sup>1</sup>	Requires Sales App or Sales Engineer quote. Customer Server Rep will manually transfer licenses.	A new TASKE dongle is required
TASKE	Stand Alone PC	Requires Sales App or Sales Engineer quote. Customer Server Rep will manually transfer licenses	Return old ACD dongle - a new TASKE dongle is required <sup>2</sup>
TASKE	IPedge R1.6.2 Virtual Server	Customer Server Rep will manually transfer licenses	A new TASKE dongle is required
TASKE	IPedge 1.7 and later IPedge Server	Move the TASKE dongle to the new system and reapply the existing TASKE license.	Use the existing TASKE dongle

1. Any transfer from a MAS to Software Only requires a quote from Toshiba’s Sales Application Desk or Sales Engineer. Refer to the MAS License Transfer section below.

2. A scrap fee is charged for returned hardware.

**MAS to IPedge System License Transfer**

The list of licenses that can be transferred from a MAS to the IPedge system is shown here.

All ACD licenses can be transferred:

- Enhanced ACD Agents
- Voice Assistance Channels
- Call Router
- IVR/Database Assistance
- Web Callback
- WebChat
- UCedge Essentials/Call Manager Standard
- UCedge/Call Manager Advanced
- UCedge/Call Manager Softphone VoIP plug-in
- TASKE Contact
- TASKE Reporter (non-promotional)
- TASKE Essentials

The licenses that CANNOT be transferred from a MAS to the IPedge system are shown here.

- Free TASKE Reporter promotion
- Insight
- VCS
- Stratagy ES

This page is intentionally left blank.



# Chapter 19 – Upgrade to Off-line Dongle Licence

---

To change existing IPedge systems to Dongle licensing the server must be upgraded to IPedge release 1.7.4 software. The IPedge software release 1.7.4 dongles are blue in color. License transfer from a Toshiba branded server to a virtual server using a license dongle will not be available until early March 2017.

This procedure is for installed IPedge systems with a virtual license. For new systems that have not been licensed refer to the IPedge Virtual Server install manual.

**Important!** Order the license dongle **before starting this process**. You must have the license dongle to complete the license upgrade procedure.

**Important!** The IPedge server must have internet access for this procedure.

## TRANSFER LICENSE

1. Login to Toshiba's FYI website
2. Select **License Codes > IPedge Virtual Licensing**.
3. Enter the System Number of the installed system.
4. Select the **Customer Name**.
5. The sites and system names for this customer will be listed.
6. Click on the **Create New System** button. You are adding a new system to this customer.
7. Complete all of the required fields (\*) to create the new system. Use a unique name for the new system This will be the new name of the installed system. Click the **Submit** button.
8. The new system name is added to the list of systems for this customer.
9. Select **License Codes > System Upgrade** then, click on **Create New**.
10. On the System Upgrade Quote page, complete all of the required fields.  
Use the pull-down list to specify the Target System (select a -V Dongle)  
For the Serial #/System # field enter the new system number created in Step 6.

The Virtual Dongle ID is the number of the license dongle that was ordered for this upgrade.

11. Click on the **Continue** button. on the new system upgrade quote screen the new customer number (created in Step 6) will show as the **Target System #**.
12. In the Source System field use the pull-down list to select the existing system.
13. In the Source Serial #/System # field enter the system number of the existing system.
14. In the Process Disposition field select **Keep (Non-branded)**.
15. Click on **Continue**.
16. Verify that the licenses and quantities are correct, click on **Continue**.
17. Check-mark the **I Agree** to the above ... box then, click on the **Finalize** button.
18. The EULA will be sent to the customer contact email address.
19. When the EULA has been accepted the license BIN file to be generated then sent to the dealer contact email address.
20. If the license dongle number was not entered in Step 10 an error message dialog will open. click on Continue, go to Step 10, enter the dongle number, follow the remaining steps to finish.

## USB PASS-THROUGH SETUP

Existing IPedge virtual servers using the virtual licensing service that are upgrading to Off-line (dongle based) licensing require USB port pass-through setup. This setup procedure allows the virtual server VMware® to recognize the license dongle when it is plugged into a USB port on the server.

1. Ensure that the IPedge server has a connection to the internet.
2. Launch vSphere client on the administrator PC.
3. Login to the IPedge server.
4. Select the **Getting Started** tab.
5. Select the IPedge server from the list on the left side of the screen.
6. Click on **Shut down the virtual machine**.
7. Plug the license dongle into a USB port on the IPedge server.
8. Wait for the system to shutdown, about 2 minutes.

**Important!** The IPedge virtual machine must be completely shut down. To view the shutdown progress select the **Console** tab.

9. In the Getting started tab click on **Edit virtual machine settings**.
10. Go to the **Hardware** tab then, click on the **Add** button.
11. In the Device Type dialog select **USB Device** then click on the **Next** button.
12. Select **Aladdin Knowledge Sentinel HL**.

13. Click on **Next**.
14. In the Ready to Complete dialog click on **Finish**.
15. In the Hardware screen you will see the New USB Device, click on **OK**.
16. In the **Recent Tasks** at bottom of the screen wait for this task to complete before continuing.

**Note:** This procedure maps one USB port for license dongle pass-through. Toshiba recommends that you map all of the USB ports for license dongle use. Move the USB dongle to the next available USB port. Repeat Step 7 through Step 16 for each of the USB ports.

17. When all of the USB ports are complete, continue to Step 18.
18. Select **Edit virtual machine settings**.
19. Click on **Edit virtual machine** on the getting started tab in the basic tasks.
20. Click on **Power on the virtual machine**.
21. Allow the IPedge virtual machine to run for two the five minutes to allow all of the processes to startup.
22. Login to Enterprise Manager on the IPedge server.
23. Select **Maintenance > Licensing > License Control**. The system will show **Not licensed**.

## OFF-LINE LICENSING

Licenses are purchased through the Toshiba FYI website. Use the following procedure to update or add new licenses. The license dongle serial number is entered during the license generation process on the FYI website.

### Download License File

After the licenses upgrade is complete a license file will be sent to the contact email address. Download the license file to the Administration PC. The file can be saved to any file storage unit on a network that the administration PC and the IPedge server can access. Use the following procedure to apply the license file to the IPedge server.

### Upload and Apply License

1. Plug in the license dongle.
2. Login to the Enterprise Manager on the Primary IPedge server.
3. Select **Maintenance > Licensing > License Control**.
4. Select the server to be licensed.
5. Click on the **Upload License** file icon.
6. Enter the location and name of the license file or click on the Browse button to locate the license file.
7. Click on **OK**.  
The license file name, server MAC address and the server name will

be displayed. Verify that the MAC address is the correct address for this server. Double click on this line for a detailed list of the licenses.

8. Click to check-mark the uploaded file then, click on the **Apply** icon.
9. After the license is applied, the license result should show "Successful".
10. Then check "**Yes, I want to reboot the system now**" and click on **OK**. Reboot can take several minutes.

### Display License Information

To display the items and quantities licensed on the server.

1. Login to the Enterprise Manager on the Primary IPedge server.
2. Select **Maintenance > Licensing > License Information**.
3. Select the server to display.

To display detailed information about a specific license.

1. Login to the Enterprise Manager on the IPedge server you are going to license.
2. Select **Maintenance > Licensing > License Control**.
3. A list of all the licenses on the server will be displayed.
4. Click to check-mark a license then, click on the **View** icon.
5. After the IPedge server has restarted, login to Enterprise Manager.
6. In Enterprise Manager select **Administration > Enterprise > Servers**.
7. Check the Server Name box and click the **Server Synchronization** icon.
8. The Enterprise - Servers Status screen displays. Check the Table Name box then click on the "**Order database synchronization**" icon.
9. A confirmation dialog window will display. Click on **OK** to start the database synchronization. Wait for the database synchronization to finish. This will take a few minutes.

## MICROSOFT SOFTWARE LICENSE TERMS

### WINDOWS 7 ULTIMATE FOR EMBEDDED SYSTEMS

### WINDOWS 7 PROFESSIONAL FOR EMBEDDED SYSTEMS (ALL VERSIONS)

---

These license terms are an agreement between you and *Toshiba America Information Systems*. Please read them. They apply to the software included on this device. The software also includes any separate media on which you received the software.

The software on this device includes software licensed from Microsoft Corporation or its affiliate.

The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those terms apply.

If you obtain updates or supplements directly from Microsoft, then Microsoft, and not *Toshiba America Information Systems*, licenses those to you.

**As described below, using the software also operates as your consent to the transmission of certain computer information for Internet-based services.**

**By using the software, you accept these terms. If you do not accept them, do not use the software. Instead, contact *Toshiba America Information Systems* to determine its return policy for a refund or credit.**

---

**If you comply with these license terms, you have the rights below.**

#### 1. OVERVIEW.

- a. **Software.** The software includes desktop operating system software. This software does not include Windows Live services. Windows Live services are available from Microsoft under a separate agreement.

#### 2. USE RIGHTS.

- a. **Use.** The software license is permanently assigned to the device with which you acquired the software. That device is the "licensed device". You may use the software on the licensed device.
- b. **Processor Limit.** You may use the software with no more than two processors at any one time.
- c. **Alternative Versions.** You may only use the version of the software that is installed on the licensed device. You may not change it to any other version (such as the 32-bit or 64-bit version, or another language version).

#### 3. ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.

- a. **Specific Use.** *Toshiba America Information Systems* designed the licensed device for a specific use. You may only use the software for that use.
- b. **Other Software.** You may use other programs with the software as long as the other programs
  - directly support the specific use for the licensed device, or

- provide system utilities, resource management, or anti-virus or similar protection.

Software that provides consumer or business tasks or processes may not run on the licensed device. This includes email, word processing, spreadsheet, database, scheduling and personal finance software. The licensed device may use terminal services protocols to access such software running on a server.

**c. Device Connections.** You may not use the software as server software. In other words, more than one device may not access, display, run, share or use the software at the same time. You may allow up to twenty other devices to access the software to use

- File Services,
- Print Services,
- Internet Information Services, and
- Internet Connection Sharing and Telephony Services.

The twenty connection limit applies to devices that access the software indirectly through “multiplexing” or other software or hardware that pools connections. You may use unlimited inbound connections at any time via TCP/IP.

**d. Remote Access Technologies.** You may access and use the software remotely from another device using remote access technologies as follows.

Remote Desktop. The single primary user of the licensed device may access a session from any other device using Remote Desktop or similar technologies. A “session” means the experience of interacting with the software, directly or indirectly, through any combination of input, output and display peripherals. Other users may access a session from any device using these technologies, if the remote device is separately licensed to run the software.

Other Access Technologies. You may use Remote Assistance or similar technologies to share an active session.

Other Remote Uses. You may allow any number of devices to access the software for purposes other than those described in the Device Connections and Remote Access Technologies sections above, such as to synchronize data between devices.

**e. Font Components.** While the software is running, you may use its fonts to display and print content. You may only

- embed fonts in content as permitted by the embedding restrictions in the fonts; and
- temporarily download them to a printer or other output device to print content.

**f. Icons, images and sounds.** While the software is running, you may use but not share its icons, images, sounds, and media.

**4. POTENTIALLY UNWANTED SOFTWARE.** The software includes Windows Defender. If Windows Defender is turned on, it will search this device for “spyware,” “adware” and other potentially unwanted software. If it finds potentially unwanted software, the software will ask you if you want to ignore, disable (quarantine) or remove it. Any potentially unwanted software rated “high” or “severe,” will be automatically removed after scanning unless you change the default setting. Removing or disabling potentially unwanted software may result in

- other software on your computer ceasing to work, or

- your breaching a license to use other software on
- this device.

By using this software, it is possible that you will also remove or disable software that is not potentially unwanted software.

**5. SCOPE OF LICENSE.** The software is licensed, not sold. This agreement only gives you some rights to use the software. *Toshiba America Information Systems* and Microsoft reserve all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the software that allow you to use it only in certain ways. For more information, see the software documentation or contact *Toshiba America Information Systems*. You may not:

- work around any technical limitations in the software;
- reverse engineer, decompile or disassemble the software;
- make more copies of the software than specified in this agreement;
- publish the software for others to copy;
- rent, lease or lend the software; or
- use the software for commercial software hosting services.

Except as expressly provided in this agreement, rights to access the software on this device do not give you any right to implement Microsoft patents or other Microsoft intellectual property in software or devices that access this device.

- **INTERNET-BASED SERVICES.** Microsoft provides Internet-based services with the software. Microsoft may change or cancel them at any time.
- a. **Consent for Internet-Based Services.** The licensed device may contain one or more of the software features described below. These features connect to Microsoft or service provider computer systems over the Internet. In some cases, you will not receive a separate notice when they connect. For more information about these features, visit [go.microsoft.com/fwlink/?linkid=104604](http://go.microsoft.com/fwlink/?linkid=104604).

**By using these features, you consent to the transmission of this information.**

Microsoft does not use the information to identify or contact you.

Computer Information. The following features use Internet protocols, which send to the appropriate systems computer information, such as your Internet protocol address, the type of operating system and browser, and the name and version of the software you are using. Microsoft uses this information to make the Internet-based services available to you. *Toshiba America Information Systems* has elected to turn on the following features in the licensed device.

- Plug and Play and Plug and Play Extensions. You may connect new hardware to your device. Your device may not have the drivers needed to communicate with that hardware. If so, the update feature of the software can obtain the correct driver from Microsoft and install it on your device.
- Web Content Features. Features in the software can retrieve related content from Microsoft and provide it to you. Examples of these features are clip art, templates, online

training, online assistance and Appshelp. You may choose not to use these web content features.

- Digital Certificates. The software uses x.509 version 3 digital certificates. These digital certificates confirm the identity of users sending information to each other and allow you to encrypt the information. The software retrieves certificates and updates certificate revocation lists over the Internet.
- Auto Root Update. The Auto Root Update feature updates the list of trusted certificate authorities. You can switch off this feature.
- Windows Media Digital Rights Management. Content owners use Windows Media digital rights management technology (WMDRM) to protect their intellectual property, including copyrights. This software and third party software use WMDRM to play and copy WMDRM-protected content. If the software fails to protect the content, content owners may ask Microsoft to revoke the software's ability to use WMDRM to play or copy protected content. Revocation does not affect other content. When you download licenses for protected content, you agree that Microsoft may include a revocation list with the licenses. Content owners may require you to upgrade WMDRM to access their content. Microsoft software that includes WMDRM will ask for your consent prior to the upgrade. If you decline an upgrade, you will not be able to access content that requires the upgrade. You may switch off WMDRM features that access the Internet. When these features are off, you can still play content for which you have a valid license.
- Windows Media Player. When you use Windows Media Player, it checks with Microsoft for
  - compatible online music services in your region;
  - new versions of the player; and
  - codecs if your device does not have the correct ones for playing content.

For more information, go to: [go.microsoft.com/fwlink/?linkid=104605](http://go.microsoft.com/fwlink/?linkid=104605).

- Malicious Software Removal/Clean On Upgrade. Before installation of the software, the software will check and remove certain malicious software listed at [www.support.microsoft.com/?kbid=890830](http://www.support.microsoft.com/?kbid=890830) ("Malware") from your device. When the software checks your device for Malware, a report will be sent to Microsoft about any Malware detected or errors that occurred while the software was checking for Malware. No information that can be used to identify you is included in the report.
- Network Awareness. This feature determines whether a system is connected to a network by either passive monitoring of network traffic or active DNS or HTTP queries. The query only transfers standard TCP/IP or DNS information for routing purposes. You can switch off the active query feature through a registry setting.
- Windows Time Service. This service synchronizes with [www.time.windows.com](http://www.time.windows.com) once a week to provide your computer with the correct time. The connection uses standard NTP protocol.

**b. Use of Information.** Microsoft may use the computer information, error reports, and Malware reports to improve our software and services. We may also share it with others, such



as hardware and software vendors. They may use the information to improve how their products run with Microsoft software.

- c. **Misuse of Internet-based Services.** You may not use these services in any way that could harm them or impair anyone else's use of them. You may not use the services to try to gain unauthorized access to any service, data, account or network by any means.

## 6. VALIDATION.

- a. Validation verifies that the software has been activated and is properly licensed. It also verifies that no unauthorized changes have been made to the validation, licensing, or activation functions of the software. Validation may also check for certain malicious or unauthorized software related to such unauthorized changes. A validation check confirming that you are properly licensed, permits you to continue to use the software, certain features of the software or to obtain additional benefits. **You are not permitted to circumvent validation.** This is to prevent unlicensed use of the software. For more information, see [go.microsoft.com/fwlink/?Linkid=104610](http://go.microsoft.com/fwlink/?Linkid=104610).
- b. The software will from time to time perform a validation check of the software. The check may be initiated by the software or Microsoft. To enable the activation function and validation checks, the software may from time to time require updates or additional downloads of the validation, licensing or activation functions of the software. The updates or downloads are required for the proper functioning of the software and may be downloaded and installed without further notice to you. During or after a validation check, the software may send information about the software, the computer and the results of the validation check to Microsoft. This information includes, for example, the version and product key of the software, any unauthorized changes made to the validation, licensing or activation functions of the software, any related malicious or unauthorized software found and the Internet protocol address of the computer. Microsoft does not use the information to identify or contact you. By using the software, you consent to the transmission of this information. For more information about validation and what is sent during or after a validation check, see [go.microsoft.com/fwlink/?Linkid=104611](http://go.microsoft.com/fwlink/?Linkid=104611).
- c. If, after a validation check, the software is found to be counterfeit, improperly licensed, or a non-genuine Windows product, or if it includes unauthorized changes, then the functionality and experience of using the software will be affected. For example:

Microsoft may

- repair the software, and remove, quarantine or disable any unauthorized changes that may interfere with the proper use of the software, including circumvention of the activation or validation functions of the software; or
- check and remove malicious or unauthorized software known to be related to such unauthorized changes; or
- provide notice that the software is improperly licensed or a non-genuine Windows product;

and you may

- receive reminders to obtain a properly licensed copy of the software; or
- need to follow Microsoft's instructions to be licensed to use the software and reactivate;

and you may not be able to

- use or continue to use the software or some of the features of the software; or
- obtain certain updates or upgrades from Microsoft.

d. You may only obtain updates or upgrades for the software from Microsoft or authorized sources (including *Toshiba America Information Systems*). For more information on obtaining updates from authorized sources see [go.microsoft.com/fwlink/?Linkid=104612](http://go.microsoft.com/fwlink/?Linkid=104612).

**7. PRODUCT SUPPORT.** Contact *Toshiba America Information Systems* for support options. Refer to the support number provided with the device.

**8. MICROSOFT .NET BENCHMARK TESTING.** The software includes one or more components of the .NET Framework (".NET Components"). You may conduct internal benchmark testing of those components. You may disclose the results of any benchmark test of those components, provided that you comply with the conditions set forth at [go.microsoft.com/fwlink/?LinkID=66406](http://go.microsoft.com/fwlink/?LinkID=66406).

Notwithstanding any other agreement you may have with Microsoft, if you disclose such benchmark test results, Microsoft shall have the right to disclose the results of benchmark tests it conducts of your products that compete with the applicable .NET Component, provided it complies with the same conditions set forth at [go.microsoft.com/fwlink/?LinkID=66406](http://go.microsoft.com/fwlink/?LinkID=66406).

**9. BACKUP COPY.** You may make one backup copy of the software. You may use it only to reinstall the software on the device.

**10. DOCUMENTATION.** Any person that has valid access to your computer or internal network may copy and use the documentation for your internal, reference purposes.

**11. UPGRADES.** To use upgrade software, you must first be licensed for the software that is eligible for the upgrade. Upon upgrade, this agreement takes the place of the agreement for the software you upgraded from. After you upgrade, you may no longer use the software you upgraded from.

**12. PROOF OF LICENSE.** If you acquired the software on the device, or on a disc or other media, a genuine Certificate of Authenticity label with a genuine copy of the software identifies licensed software. To be valid, this label must be affixed to the device, or included on or in *Toshiba America Information Systems's* software packaging. If you receive the label separately, it is not valid. You should keep the label on the device or packaging to prove that you are licensed to use the software. To identify genuine Microsoft software, see <http://www.howtotell.com>.

**13. TRANSFER TO A THIRD PARTY.** You may transfer the software only with the device, the Certificate of Authenticity label, and these license terms directly to a third party. Before the transfer, that party must agree that these license terms apply to the transfer and use of the software. You may not retain any copies of the software including the backup copy.

**14. NOTICE ABOUT THE H.264/AVC VISUAL STANDARD, THE VC-1 VIDEO STANDARD, THE MPEG-4 VISUAL STANDARD AND THE MPEG-2 VIDEO STANDARD.** This software may include H.264/AVC, VC-1, MPEG-4 Part 2, and MPEG-2 visual compression technology. If the software includes those visual compression technologies MPEG LA, L.L.C. requires this notice:

THIS PRODUCT IS LICENSED UNDER ONE OR MORE VIDEO PATENT PORTFOLIO LICENSES SUCH AS, AND WITHOUT LIMITATION, THE AVC, THE VC-1, THE MPEG-4 PART 2 VISUAL, AND THE MPEG-2 VIDEO PATENT PORTFOLIO LICENSES FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE ABOVE STANDARDS ("VIDEO STANDARDS") AND/OR (ii) DECODE VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE VIDEO UNDER SUCH PATENT PORTFOLIO LICENSES. NONE OF THE LICENSES EXTEND TO ANY OTHER PRODUCT REGARDLESS OF WHETHER SUCH PRODUCT IS INCLUDED WITH THIS PRODUCT IN A SINGLE ARTICLE. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

- 15. NOT FAULT TOLERANT.** The software is not fault tolerant. *Toshiba America Information Systems* installed the software on the device and is responsible for how it operates on the device.
- 16. RESTRICTED USE.** The Microsoft software was designed for systems that do not require fail-safe performance. You may not use the Microsoft software in any device or system in which a malfunction of the software would result in foreseeable risk of injury or death to any person. This includes operation of nuclear facilities, aircraft navigation or communication systems and air traffic control.
- 17. THIRD PARTY PROGRAMS.** The software contains third party programs. The license terms with those programs apply to your use of them.
- 18. NO WARRANTIES FOR THE SOFTWARE.** The software is provided “as is”. You bear all risks of using it. Microsoft gives no express warranties, guarantees or conditions. Any warranties you receive regarding the device or the software do not originate from, and are not binding on, Microsoft or its affiliates. When allowed by your local laws, *Toshiba America Information Systems* and Microsoft exclude implied warranties of merchantability, fitness for a particular purpose and non-infringement.
- 19. LIABILITY LIMITATIONS.** You can recover from Microsoft and its affiliates only direct damages up to two hundred fifty U.S. Dollars (U.S. \$250.00), or equivalent in local currency. You cannot recover any other damages, including consequential, lost profits, special, indirect or incidental damages.

This limitation applies to:

- anything related to the software, services, content (including code) on third party internet sites, or third party programs, and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if Microsoft should have been aware of the possibility of the damages. The above limitation may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

- 20. EXPORT RESTRICTIONS.** The software is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the software. These laws include restrictions on destinations, end users and end use. For additional information, see [www.microsoft.com/exporting](http://www.microsoft.com/exporting).
- 21. ENTIRE AGREEMENT.** This agreement, additional terms (including any printed-paper license terms that accompany the software and may modify or replace some or all of these terms), and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the software and support services.
- 22. APPLICABLE LAW.**
- a. United States.** If you acquired the software in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.
  - b. Outside the United States.** If you acquired the software in any other country, the laws of that country apply.

## MICROSOFT SOFTWARE LICENSE TERMS

### MICROSOFT WINDOWS SERVER 2012 R2 STANDARD (2 CPU)

---

These license terms are an agreement between you and:

- the server manufacturer that distributes the software with the server; or
- the software installer that distributes the software with the server.

Please read them. They apply to the software included on this server, which includes the media on which you received the software.

The terms also apply to any Microsoft:

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those terms apply. If you obtain updates or supplements directly from Microsoft, Microsoft, and not the manufacturer or installer, licenses those to you. Printed paper license terms, which may come with the software, take the place of any on-screen license terms.

**By using the software, you accept these terms. If you do not accept them, do not use the software. Instead, contact the manufacturer or installer to determine its return policy for a refund or credit.**

**As described below, using some features also operates as your consent to the transmission of certain standard computer information for Internet-based services.**

---

**If you comply with these license terms, you have the rights below for each software license you acquire.**

#### **1. OVERVIEW.**

**a. Software.** The software includes:

- server software; and
- additional software that may only be used with the server software.

**b. License Model.** The software is licensed based on:

- the number of instances of server software that you run;
- the number of devices and users that access instances of server software;
- the server software functionality accessed; and
- the number of processors in the physical hardware.

**c. Licensing Terminology.**

- **Instance.** You create an "instance" of software by executing the software's setup or install procedure. You also create an instance of software by duplicating an existing instance. References to software in this agreement include "instances" of the software.
- **Run an Instance.** You "run an instance" of software by loading it into memory and executing one or more of its instructions. Once running, an instance is considered to be running (whether or not its instructions continue to execute) until it is removed from memory.
- **Operating System Environment.** An "operating system environment" is:
  - (i) all or part of an operating system instance, or all or part of a virtual (or otherwise emulated) operating system instance that enables separate machine identity (primary computer name or similar unique identifier) or separate administrative rights, and
  - (ii) instances of applications, if any, configured to run on the operating system instance or parts identified above.

There are two types of operating system environments: physical and virtual. A physical operating system environment is configured to run directly on a physical hardware system. The operating system instance used to run hardware virtualization software (e.g., Microsoft Virtual Server or similar technologies) or to provide hardware virtualization services (e.g., Microsoft virtualization technologies) is considered part of the physical operating system environment. A virtual operating system environment is configured to run on a virtual (or otherwise emulated) hardware system.

A physical hardware system can have either or both of the following:

- (i) one physical operating system environment, and

(ii) one or more virtual operating system environments.

**Server.** A server is a physical hardware system or device capable of running server software. A hardware partition or blade is considered to be a separate physical hardware system.

**Assigning a License.** To assign a license means simply to designate that license to one device or user.

## 2. USE RIGHTS.

**a. Licensing a Server.** The manufacturer or installer has determined a certain number of server software licenses and assigned those licenses to the server with which the software was distributed. Before you run instances of the server software on the server, you must determine the number of software licenses required as described below. You must ensure that you received the appropriate number of licenses with the server. Certificate of Authenticity label(s) may be found affixed to the server and/or in the manufacturer's or installer's software packaging.

**b. Determining the Number of Licenses Required.** This license covers up to two physical processors. In order to determine how many licenses you need for each server, you must count the number of physical processors on the server, divide that number by two, and round up to the nearest whole number.

**c. Assignment of the Required Number of Licenses to the Server.** The software license is permanently assigned to the server with which you acquired the software. That server is the licensed server for such license. A hardware partition or blade is considered to be a separate server. You may not assign the same license to more than one server.

### **d. Running Instances of the Server Software.**

i. You may run, at any one time:

· one instance of the server software in one physical operating system environment, and

· for each license assigned to the server, up to two instances of the server software in virtual operating system environments (only one instance per virtual operating system environment).

ii. If you run all permitted instances at the same time, the instance of the server software running in the physical operating system environment may be used

only to:

- run hardware virtualization software,
- provide hardware virtualization services,
- run software to manage and service operating system environments on the licensed server.

**e. Server Repartitioning.** You may reassign licenses when you:

- reallocate physical processors from one licensed hardware partition to another;
- create two or more partitions from one licensed hardware partition;
- create one partition from two or more licensed hardware partitions

as long as (i) prior to repartitioning, each hardware partition is fully licensed, and (ii) the total number of licenses and physical processors remains the same.

**f. Running Instances of the Additional Software.** You may run or otherwise use any number of instances of additional software listed on the website specified below in physical or virtual operating system environments on any number of devices. You may use additional software only with the server software. For a list of additional software, visit <http://go.microsoft.com/fwlink/?LinkId=290987>.

**g. Creating and Storing Instances on Your Servers or Storage Media.** For each software license you acquire, you may create and store any number of instances of the software on any of your servers or storage media. This may be done solely to exercise your right to run instances of the software under any of your licenses as described in the applicable use rights (e.g., you may not distribute instances to third parties).

**h. Included Microsoft Programs.** The software contains other Microsoft programs. These license terms apply to your use of those programs.

**i. Processor Rights.** You may use the server software with up to two processors of the server at any one time.

### **3. ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.**

**a. Specific Use.** The manufacturer designed this server for a specific use. You may only use the software for that use.

You may not use the software to support additional software programs or functions, other than utilities or similar software used solely for administration, performance enhancement, and/or preventative maintenance of this server.

**b. Windows Server 2012 Client Access Licenses (CALs).**

- i.** You must acquire and assign the appropriate CAL to each device or user that accesses your instances of the server software directly or indirectly. A hardware partition or blade is considered to be a separate device.
  - You do not need CALs for any of your servers licensed to run instances of the server software.
  - You do not need CALs for up to two devices or users to access your instances of the server software only to administer those instances.
  - You do not need CALs for any instance running in a physical operating system environment used solely to:
    - run hardware virtualization software;
    - provide hardware virtualization services;
    - run software to manage and service operating system environments on the licensed server.
  - Your CALs permit access to your instances of earlier versions, but not later versions, of the server software. If you are accessing instances of an earlier version, you may also use CALs corresponding to that version.
- ii.** Some server software functionality requires additional CALs, as listed below.
  - Windows Server 2012 R2 Remote Desktop Services: Windows Server 2012 Remote Desktop Services CAL
  - Windows Server 2012 R2 Active Directory Rights Management Services: Windows Server 2012 Active Directory Rights Management Services CAL
- iii. Types of CALs.** There are two types of CALs: one for devices and one for users. Each device CAL permits one device, used by any user, to access instances of the server software on your licensed servers. Each user CAL permits one user, using any device, to access instances of the server software on your licensed servers. You may use a combination of device and user CALs.
- iv. Reassignment of CALs.** You may:



- permanently reassign your device CAL from one device to another, or your user CAL from one user to another; or
- temporarily reassign your device CAL to a loaner device while the first device is out of service, or your user CAL to a temporary worker while the user is absent.

- v. Windows Server 2012 R2 Remote Desktop Services.** In addition to a Windows Server 2012 CAL, you must acquire a Windows Server 2012 Remote Desktop Services CAL for each user or device that (i) directly or indirectly accesses the Remote Desktop Services functionality or (ii) directly or indirectly accesses the server software to host a graphical user interface (using the Windows Server 2012 R2 Remote Desktop Services functionality or other technology). For more information about Windows Server 2012 Remote Desktop Services CALs, visit <http://go.microsoft.com/fwlink/?LinkId=294095>.
- vi. Windows Server 2012 Active Directory Rights Management Services CALs.** In addition to a Windows Server 2012 CAL, you must acquire a Windows Server 2012 Active Directory Rights Management Services CAL for each user or device that directly or indirectly accesses the Windows Server 2012 R2 Active Directory Rights Management Services functionality.
- vii.** The server software can be used in either “per device or per user” mode or “per server” mode. In “per device or per user” mode, you need a Windows Server 2012 CAL for each device or user that directly or indirectly accesses instances of the server software on your licensed servers. In “per server” mode, you need and must dedicate exclusively to an instance of the server software as many Windows Server 2012 CALs as the greatest number of devices and users that may directly or indirectly access that instance at the same time. You may change the mode only one time, from “per server” to “per device or per user.” If you do, you will retain the same number of Windows Server 2012 CALs.
- c. Multiplexing.** Hardware or software you use to:
- pool connections,
  - reroute information,
  - reduce the number of devices or users that directly access or use the software,
  - reduce the number of devices or users the software directly manages,
- (sometimes referred to as “multiplexing” or “pooling”), does not reduce the number of

licenses of any type that you need.

- d. Font Components.** While the software is running, you may use its fonts to display and print content. You may only:
  - embed fonts in content as permitted by the embedding restrictions in the fonts; and
  - temporarily download them to a printer or other output device to print content.
- d. Icons, images, and sounds.** While the software is running, you may use but not share its icons, images, sounds, and media. The sample images, sounds, and media provided with the software are for your non-commercial use only.
- e. No Separation of Server Software.** You may not separate the server software for use in more than one operating system environment under a single license, unless expressly permitted. This applies even if the operating system environments are on the same physical hardware system.
- f. Additional Functionality.** Microsoft may provide additional functionality for the software. Other license terms and fees may apply.
- g. Maximum Instances.** The software or your hardware may limit the number of instances of the server software that can run in physical or virtual operating system environments on the server.

**4. MANDATORY ACTIVATION.** Activation associates the use of the software with a specific device. During activation, the software will send information about the software and the device to Microsoft. This information includes the version, language, and product key of the software, the Internet protocol address of the device, and information derived from the hardware configuration of the device. For more information, see [www.microsoft.com/piracy/](http://www.microsoft.com/piracy/). By using the software, you consent to the transmission of this information. If properly licensed, you have the right to use the version of the software installed during the installation process up to the time permitted for activation. **The manufacturer should have activated the software for you. Unless the software is activated, you have no right to use the software.** This is to prevent its unlicensed use. **You are not permitted to bypass or circumvent activation.** If the device is connected to the Internet, the software may automatically connect to Microsoft for activation. You can also activate the software manually by Internet or telephone. If you do so, Internet and telephone service charges may apply. Some changes to your computer components or the software may require you to reactivate the software. **The software will remind you to activate it until you do.**

## **5. VALIDATION.**

- a. If the manufacturer activated the software for you, you may not be asked to activate the software when you first use it. The software will from time to time validate the software and update or require download of the validation feature of the software. Validation verifies that the software has been activated and is properly licensed. Validation also permits you to use certain features of the software or to obtain additional benefits. For more information, see <http://go.microsoft.com/fwlink/?linkid=39157>.
- b. During a validation check, the software will send information about the software and the device to Microsoft. This information includes the version and product key of the software, and the Internet protocol address of the device. Microsoft does not use the information to identify or contact you. By using the software, you consent to the transmission of this information. For more information about validation and what is sent during a validation check, see <http://go.microsoft.com/fwlink/?linkid=69500>.
- c. If, after a validation check, the software is found not to be properly licensed, the functionality of the software may be affected. For example, you may:
  - need to reactivate the software, or
  - receive reminders to obtain a properly licensed copy of the software,or you may not be able to:
  - use or continue to use some of the features of the software, or
  - obtain certain updates or upgrades from Microsoft.
- d. You may only obtain updates or upgrades for the software from Microsoft or authorized sources. For more information on obtaining updates from authorized sources, see <http://go.microsoft.com/fwlink/?linkid=69502>.

**6. INTERNET-BASED SERVICES.** Microsoft provides Internet-based services with the software. It may change or cancel them at any time.

**Consent for Internet-Based Services.** The software features described below and in the Windows Server Privacy Highlights connect to Microsoft or service provider computer systems over the Internet. In some cases, you will not receive a separate notice when they connect. You may switch off these features or not use them. For more information about these features, visit <http://go.microsoft.com/fwlink/?LinkID=280262>. **By using these features, you consent to the transmission of this information.** Microsoft does not use the information to identify or contact you.

- Computer Information. The following features use Internet protocols, which send to the appropriate systems computer information, such as your Internet protocol address, the type of operating system, browser, the name and version of the software you are using, and the language code of the device where you run the software. Microsoft uses this information to make the Internet-based services available to you.
- Windows (or Microsoft) Update Feature. You may connect new hardware to the device where the software is installed. Your device may not have the drivers needed to communicate with that hardware. If so, the update feature of the software can obtain the correct driver from Microsoft and install it on your device. You can switch off this update feature.
- Web Content Features. Features in the software can retrieve related content from Microsoft and provide it to you. To provide the content, these features send to Microsoft the type of operating system, name, and version of the software you are using, type of browser and language code of the device where you run the software. Examples of these features are clip art, templates, online training, online assistance, and Appshelp. You may choose not to use these web content features.
- Digital Certificates. The software uses digital certificates. These digital certificates confirm the identity of Internet users sending X.509 standard encrypted information. They also can be used to digitally sign files and macros to verify the integrity and origin of the file contents. The software retrieves certificates and updates certificate revocation lists using the Internet, when available.
- Auto Root Update. The Auto Root Update feature updates the list of trusted certificate authorities. You can switch off the Auto Root Update feature.
- Windows Media Digital Rights Management. Content owners use Windows Media Digital Rights Management Technology (WMDRM) to protect their intellectual property, including copyrights. This software and third-party software use WMDRM to play and copy WMDRM-protected content. If the software fails to protect the content, content owners may ask Microsoft to revoke the software's ability to use WMDRM to play or copy protected content. Revocation does not affect other content. When you download licenses for protected content, you agree that Microsoft may include a revocation list with the licenses. Content owners may require you to upgrade WMDRM to access their content. Microsoft software that includes WMDRM will ask for your consent prior to the upgrade. If you decline an upgrade, you will not be able to

access content that requires the upgrade. You may switch off WMDRM features that access the Internet. When these features are off, you can still play content for which you have a valid license.

- Windows Media Player. When you use Windows Media Player, it checks with Microsoft for:

- compatible online music services in your region;
- new versions of the player; and
- codecs if your device does not have the correct ones for playing content.

You can switch off this last feature. For more information, visit [www.microsoft.com/windows/windowsmedia/player/12/privacy.aspx](http://www.microsoft.com/windows/windowsmedia/player/12/privacy.aspx).

- Network Awareness. This feature determines whether a system is connected to a network by either passive monitoring of network traffic or active DNS or HTTP queries. The query only transfers standard TCP/IP or DNS information for routing purposes. You can switch off the active query feature through a registry setting.
- Windows Time Service. This service synchronizes with [time.windows.com](http://time.windows.com) once a week to provide your computer with the correct time. You can turn this feature off or choose your preferred time source within the Date and Time Control Panel applet. The connection uses standard NTP protocol.
- IPv6 Network Address Translation (NAT) Traversal service (Teredo). This feature helps existing home Internet gateway devices transition to IPv6. IPv6 is a next-generation Internet protocol. It helps enable end-to-end connectivity often needed by peer-to-peer applications. To do so, each time you start up the software, the Teredo client service will attempt to locate a public Teredo Internet service. It does so by sending a query over the Internet. This query only transfers standard Domain Name Service information to determine if your computer is connected to the Internet and can locate a public Teredo service. If you:
  - use an application that needs IPv6 connectivity, or
  - configure your firewall to always enable IPv6 connectivity

by default, standard Internet Protocol information will be sent to the Teredo service at Microsoft at regular intervals. No other information is sent to Microsoft. You can change this default to use non-Microsoft servers. You can

also switch off this feature using a command line utility named "netsh".

- Windows Server 2012 R2 Active Directory Rights Management Services. The software contains a feature that allows you to create content that cannot be printed, copied, or sent to others without your permission. You must connect to Microsoft to use this feature for the first time. Once a year, you must re-connect to Microsoft to update it. For more information, visit [www.microsoft.com/rms](http://www.microsoft.com/rms). You may choose not to use this feature.

- Accelerators. When you click on or move your mouse over an Accelerator in Internet Explorer, any of the following may be sent to the service provider:

- the title and full web address or URL of the current webpage,
- standard computer information, and
- any content you have selected.

If you use an Accelerator provided by Microsoft, the information sent is subject to the Microsoft Online Privacy Statement, which is available at <http://go.microsoft.com/fwlink/?linkid=31493>. If you use an Accelerator provided by a third party, use of the information sent will be subject to the third-party's privacy practices.

- 7. DATA STORAGE TECHNOLOGY.** The server software includes data storage technology called Windows Internal Database. Components of the server software use this technology to store data. You may not otherwise use or access this technology under this agreement.
- 8. MICROSOFT .NET BENCHMARK TESTING.** The software includes one or more components of the .NET Framework (".NET Components"). You may conduct internal benchmark testing of those components. You may disclose the results of any benchmark test of those components, provided that you comply with the conditions set forth at <http://go.microsoft.com/fwlink/?LinkID=66406>. Notwithstanding any other agreement you may have with Microsoft, if you disclose such benchmark test results, Microsoft shall have the right to disclose the results of benchmark tests it conducts of your products that compete with the applicable .NET Component, provided it complies with the same conditions set forth at <http://go.microsoft.com/fwlink/?LinkID=66406>.
- 9. SCOPE OF LICENSE.** The software is licensed, not sold. This agreement only gives you some rights to use the software. The manufacturer or installer, and Microsoft reserve all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the software that only allow you to use it in certain ways. For more information, see the software documentation. You may not:

- work around any technical limitations in the software;
- reverse engineer, decompile, or disassemble the software, except and only to the extent that applicable law expressly permits, despite this limitation;
- use the software's files and components within another operating system or application running on another operating system;
- make more copies of the software than specified in this agreement or allowed by applicable law, despite this limitation;
- publish the software for others to copy;
- rent, lease or lend the software; or
- use the software for commercial software hosting services.

Rights to access the software on any device do not give you any right to implement Microsoft patents or other Microsoft intellectual property in software or devices that access that device.

- 10. BACKUP COPY.** You may make one backup copy of the software media. You may use it only to create instances of the software.
- 11. DOCUMENTATION.** Any person that has valid access to your computer or internal network may copy and use the documentation for your internal, reference purposes.
- 12. DOWNGRADE.** If the software version installed on the server is a version prior to MICROSOFT WINDOWS SERVER 2012 FOR EMBEDDED SYSTEMS R2 STANDARD, you may store and use such earlier version of the software. This agreement applies to your use of the earlier version of the software; for the avoidance of doubt, by using the downgrade you will not have the right to store or use a greater number of instances of the software than are permitted under this agreement . If the earlier version includes different components not covered in this agreement, the terms that are associated with those components in the earlier version of this edition applies to your use of it.
- 13. PROOF OF LICENSE.** If you acquired the software on the server, a disc, or other media, your proof of license is the genuine Certificate of Authenticity label that comes with the server. To be valid, this label must be affixed to the server or appear on the manufacturer's or installer's software packaging. Certificate of Authenticity labels for additional licenses will be affixed to packaging by the manufacturer or installer. If you receive the label in any other manner, it is invalid. You should keep the label on the server or retain any labels on the packaging to prove that you are licensed to use the software. To identify genuine Microsoft

software, see [www.howtotell.com](http://www.howtotell.com).

**14. TRANSFER TO A THIRD PARTY.** You may transfer the software only with the licensed server, all Certificate of Authenticity label(s), any additional licenses included with the server, and this agreement, directly to a third party. Before any permitted transfer, the other party must agree that this agreement applies to the transfer and use of the software. You may not retain any instances of the software unless you also retain another license for the software.

**15. NOTICE ABOUT THE H.264/AVC VIDEO STANDARD AND THE VC-1 VIDEO STANDARD.** This software includes H.264/ AVC and VC-1 visual compression technology. MPEG LA, L.L.C. requires this notice:

THIS PRODUCT IS LICENSED UNDER THE H.264/AVC AND THE VC-1 VIDEO PATENT PORTFOLIO LICENSES FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE ABOVE STANDARDS ("VIDEO STANDARDS") AND/OR (ii) DECODE H.264/AVC AND VC-1 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE SUCH VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE.

If you have questions about the Video Standards, further information may be obtained from MPEG LA, L.L.C.; see [www.mpegla.com](http://www.mpegla.com).

**16. EXPORT RESTRICTIONS.** The software is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the software. These laws include restrictions on destinations, end users, and end use. For additional information, see [www.microsoft.com/exporting](http://www.microsoft.com/exporting).

**17. SUPPORT SERVICES.** Contact the manufacturer or installer for support options. Refer to the support number provided with the software. For updates and supplements obtained directly from Microsoft, Microsoft provides support as described at [www.support.microsoft.com/common/international.aspx](http://www.support.microsoft.com/common/international.aspx).

**18. RESTRICTED USE.** The Microsoft software was not designed for systems that require fault-tolerant performance. You may not use the Microsoft software in any device or system in which a failure or fault of any kind of the software could reasonably be seen to lead to death or serious bodily injury of any person, or to severe physical or environmental damage.

**19. ENTIRE AGREEMENT.** This agreement (including the warranty below), and the terms for supplements, updates, and Internet-based services and support services that you use, are



the entire agreement for the software and support services.

**20. APPLICABLE LAW.**

- a. United States.** If you acquired the software in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.
- b. Outside the United States.** If you acquired the software in any other country, the laws of that country apply.

**21. LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your state or country. You may also have rights with respect to the party from whom you acquired the software. This agreement does not change your rights under the laws of your state or country if the laws of your state or country do not permit it to do so.

**22. NO WARRANTIES FOR THE SOFTWARE. The software is provided "as is". You bear all risks of using it. Microsoft gives no express warranties, guarantees, or conditions. Any warranties you receive regarding the device or the software do not originate from, and are not binding on, Microsoft, or its affiliates. When allowed by your local laws, the manufacturer and Microsoft exclude implied warranties of merchantability, fitness for a particular purpose and non-infringement.**

**23. LIMITATION ON AND EXCLUSION OF DAMAGES. You can recover from Microsoft and its affiliates only direct damages up to two hundred fifty U.S. Dollars (U.S. \$250.00), or equivalent in local currency. Except for any refund the manufacturer or installer may provide, you cannot recover any damages, including consequential, lost profits, special, indirect, or incidental damages.**

This limitation applies to:

- anything related to the software, services, content (including code) on third-party Internet sites, or third-party programs; and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if:

- repair, replacement, or a refund for the software does not fully compensate you for any losses; or

- the manufacturer or installer, or Microsoft knew or should have known about the possibility of the damages.

Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. They also may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential, or other damages.

- 24. FOR AUSTRALIA ONLY.** Our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure.

Goods presented for repair may be replaced by refurbished goods of the same type rather than being replaced. Refurbished parts may be used to repair the goods.

For further information regarding this warranty and to claim expenses in relation to the warranty (if applicable), please contact the manufacturer or installer; see the contact information provided in the system packaging.

- 25. APPROVED ADDITIONAL TEXT IF EMBEDDED SYSTEM IS AUTHORIZED TO BE LEASED UNDER THE OEM LICENSE AGREEMENT:**

**LEASED HARDWARE.** If you lease the server from the manufacturer the following additional terms shall apply: (a) you may not transfer the software to another user as part of the transfer of the server, whether or not a permanent transfer of the software with the server is otherwise allowed in these license terms; (b) your rights to any software upgrades shall be determined by the lease you signed for the server; and (c) you may not use the software after your lease terminates, unless you purchase the server from the manufacturer.

**THIS IS THE LAST PAGE OF THE DOCUMENT.**

