

IP *edge*[®]

Virtual Application Server for
Strata[®]

CIX[™]

Installation Manual

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 1, November 2014

Strata CIX R5 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 web site.

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

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, VCS, eManager, SoftIPT, Strata, Strata Net, Stratagy, Net Phone, SmartMedia, and SD (Secure Digital) 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.

Audacity is a trademark of Dominic M Mazzone.

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.

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

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 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 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 United States and other countries, including but not limited to United States Export Administration Regulations or 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 U.S. Export Administration Regulation 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 CIX Strata. 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 Agreement. 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 © 2007-2014 Toshiba America Information Systems, Inc. All Rights Reserved.

TOSHIBA AMERICA INFORMATION SYSTEMS, INC. Contrat de licence de la Division des systèmes de télécommunication

IMPORTANT : LE PRÉSENT CONTRAT DE LICENCE (« CONTRAT ») CONSTITUE UN ACCORD JURIDIQUE ENTRE VOUS (« VOUS ») ET TAIS. VEUILLEZ LE LIRE ATTENTIVEMENT. L'UTILISATION DE TOUT LOGICIEL ET DE TOUT RENSEIGNEMENT S'Y RAPPORTANT (ENSEMBLE, « LOGICIELS ») INSTALLÉ DANS UN PRODUIT NUMÉRIQUE OU EXPÉDIÉ À MÊME CE PRODUIT, OU QUE TAIS MET À VOTRE DISPOSITION DE QUELQUE MANIÈRE OU SOUS QUELQUE FORME QUE CE SOIT, FAIT FOI DE VOTRE ACCEPTATION DES PRÉSENTES MODALITÉS, À MOINS QUE LE FOURNISSEUR DU LOGICIEL NE PRÉSENTE DES MODALITÉS DISTINCTES. À DÉFAUT D'ACCEPTER LES MODALITÉS DU PRÉSENT CONTRAT, VOUS NE DEVEZ PAS INSTALLER, COPIER NI UTILISER LE PRÉSENT LOGICIEL ET DEVEZ LE RETOURNER SANS DÉLAI À L'ENDROIT D'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 OCTROYÉ À DES FINS EXCLUSIVES DE DISTRIBUTION PAR VOIES AUTORISÉES AUX UTILISATEURS.

1. Octroi de la licence : Ce 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. Vous consentez à ne pas copier le logiciel, sauf si nécessaire aux fins d'utilisation sur un seul système TAIS à la fois et dans un même endroit. Il vous est strictement interdit de modifier, de traduire, de louer, de reproduire, de distribuer, d'imprimer, de sous-louer, de transférer ou de céder ce logiciel, en tout ou en partie, ni de céder les droits accordés en vertu du présent contrat à des tiers ou d'enlever les avis, les étiquettes et les marques privatifs du logiciel, sauf dans la mesure permise par les lois en vigueur. Vous reconnaissez que la violation de l'une ou l'autre de ces interdictions fera un tort irréparable à TAIS et lui fournira les motifs nécessaires à l'adoption de mesures injonctives, sans préavis, contre vous et toute autre personne ayant le logiciel en sa possession. Toute personne dont la possession du logiciel viole le présent contrat doit, sur demande, le rendre à TAIS dans les plus brefs délais. Vous consentez à ne créer aucune œuvre dérivée du présent logiciel. En cas de violation du présent contrat par vous ou par des tiers, TAIS se réserve le droit de le résilier et de reprendre immédiatement possession du logiciel. L'exécution du présent logiciel à d'autres fonctions exige un permis d'exécution valide.

2. Propriété intellectuelle : Vous reconnaissez que le titre du logiciel ne vous est nullement cédé, que le titre et les droits de pleine propriété du logiciel demeurent la propriété exclusive de TAIS et/ou de ses fournisseurs, et vous n'acquerrez aucun droit au logiciel, sauf les droits accordés en vertu de la présente licence. Vous ne devez supprimer ni modifier les avis privatifs inscrits sur ou dans ce logiciel. Ce logiciel est protégé par les lois américaines sur les brevets, les droits d'auteur et le secret industriel et/ou par d'autres lois sur la propriété et des traités internationaux. Tout transfert, utilisation ou reproduction du logiciel en violation du présent contrat constitue une violation du droit d'auteur. Sachez que tout transfert, usage ou reproduction du logiciel en violation du présent contrat constitue une atteinte volontaire au droit d'auteur.

3. Interdiction de désosser : Vous acceptez de ne pas essayer de décompiler, de désosser, de modifier, de traduire ou de démonter le logiciel, en tout ou en partie. Si vous embauchez des employés ou des entrepreneurs, vous devez mettre tout en œuvre pour empêcher que ces employés et entrepreneurs ne décompilent, ne désossent, ne modifient, ne traduisent ou ne démontent le logiciel, en tout ou en partie. L'inobservation de cette disposition ou d'autres modalités du présent contrat entraînera la résiliation automatique de ce dernier et la restitution à TAIS des droits accordés en vertu du présent contrat.

4. Garantie limitée : LE PRÉSENT LOGICIEL EST FOURNI « TEL QUEL », SANS GARANTIE DE QUELQUE NATURE QUE CE SOIT. DANS LA PLEINE MESURE PERMISE PAR LES LOIS EN VIGUEUR, TAIS ET SES FOURNISSEURS DÉSAVOUENT TOUTES LES GARANTIES EXPRESSES OU TACITES À L'ÉGARD DU LOGICIEL, NOTAMMENT LES GARANTIES DE NON-VIOLATION DES DROITS DE TIERS ET DE CONFORMITÉ À L'AN 2000, ET LA GARANTIE IMPLICITE DE QUALITÉ MARCHANDE ET D'ADAPTATION À UN USAGE PARTICULIER. VOUS ACCEPTEZ TOUS LES

RISQUES EN CE QUI A TRAIT À LA QUALITÉ ET AU RENDEMENT DU 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. CEPENDANT, TAIS GARANTIT QUE, DANS DES CONDITIONS D'USAGE NORMAL, LES MÉDIAS SUR LESQUELS LE LOGICIEL EST FOURNI SERONT EXEMPTS DE DÉFECTUOSITÉS MATÉRIELLES ET DE FABRICATION PENDANT 90 JOURS À COMPTER DE LA DATE DE LIVRAISON DU LOGICIEL.

5. Limitation de la responsabilité : LE REMPLACEMENT DES MÉDIAS 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 CONTRAT. 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, MÊME SI TAIS ET SES FOURNISSEURS ONT ÉTÉ AVISÉS DE LA POSSIBILITÉ DE TELS DOMMAGES. NI TAIS NI SES FOURNISSEURS NE PEUVENT EN AUCUN CAS ÊTRE TENUS RESPONSABLES DE RÉCLAMATIONS DÉPOSÉES PAR DES TIERS.

6. 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 LIMITES. LA PRÉSENTE GARANTIE RESTREINTE VOUS DONNE DES DROITS SPÉCIFIQUES; IL SE PEUT QUE VOUS EN AYEZ D'AUTRES ET QUE DE TELS DROITS VARIENT D'UNE PROVINCE OU D'UN TERRITOIRE À L'AUTRE.

7. Lois sur l'exportation : Le présent contrat se réfère à des produits et/ou à des données techniques pouvant être contrôlés en vertu des règlements des United States Export Administration Regulations (administration des exportations des États-Unis) et, le cas échéant, une autorisation du United States Department of Commerce (département du commerce américain) pourrait être nécessaire avant de pouvoir les exporter. 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 interdites.

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

9. Droits limités du gouvernement des États-Unis : Ce logiciel est fourni avec des droits limités. Ce logiciel et les autres éléments matériels fournis avec les présentes constituent le logiciel commercial, la documentation sur le logiciel et les données techniques reliés à ces éléments commerciaux. Conformément aux F.A.R. 12.211 et 12.212, le gouvernement américain les utilise sous licence et les droits du gouvernement américain à cet égard sont restreints, conformément à la licence commerciale du revendeur.

10. Divisibilité : Si une disposition 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.

11. Aucune renonciation : Aucune renonciation au droit de résiliation pour violation d'une disposition du présent contrat ne peut constituer une renonciation au droit de résiliation pour une 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 par un représentant autorisé de la partie l'ayant initiée.

12. Logiciels fournisseurs : Ce logiciel pourrait être 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 fournisseurs.

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. Telecommunication Systems Division 9740 Irvine Boulevard
Irvine California 92618-1697 United States of America

DSD 020905

Copyright © 2007-2014 Toshiba America Information Systems, Inc. All Rights Reserved.

TOSHIBA CORPORATION

End User License Agreement

Toshiba Corporation Cloud & Solutions Company,
Global Sales & Marketing Department 2
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 © 2007-2014 Toshiba Corporation. All Rights Reserved.

Contents

Chapter 1 – Introduction

- INTRODUCTION..... 1-1
- APPLICATION SERVER ADMINISTRATION..... 1-2
- IPedge SERVER APPLICATIONS 1-2
 - Enterprise Manager Single View, Single Page..... 1-2

Chapter 2 – Server Hardware Installation

- SERVER HARDWARE SUPPORT..... 1-1
- CREATE A DELL ACCOUNT..... 1-1
- DELL OWNERSHIP TRANSFER..... 1-1
- VMWARE® LICENSE..... 1-4
- CHANGE VMWARE (ESXi) IP ADDRESS..... 1-7
- INSTALL VSHPERE CLIENT..... 1-8
- UPLOAD THE LICENSE KEY..... 1-9
- DONGLE PORT..... 1-11
- IP NETWORK CONNECTION..... 1-11
- POWER SUPPLY..... 1-11
- PHYSICAL..... 1-12
- SERVER CHASSIS INSTALL..... 1-12
- DELL DELL R420 SERVER..... 1-13
- DELL R720 SERVER..... 1-15
- HARD DISK DRIVE INDICATORS..... 1-18
- RACKMOUNT INSTALLATION..... 1-19
- POWER REQUIREMENTS..... 1-19
- UPS RECOMMENDATIONS..... 1-19

Chapter 3 – Network Requirements

- LAN REQUIREMENTS..... 2-2
 - VoIP Requirements Remote Users..... 2-2
 - VoIP Requirements Wi-Fi® Users..... 2-2

Chapter 4 – App Server Installation

- INTRODUCTION..... 3-1

| | |
|---|------|
| SYSTEM IP ADDRESS DEFAULTS | 3-1 |
| PRE-INSTALLATION REQUIREMENTS | 3-1 |
| NETWORK NAMES | 3-2 |
| VIRTUAL SERVER INSTALLATION PROCEDURE | 3-3 |
| Login To The IPedge Server | 3-3 |
| Initial Setup and Network Configuration | 3-4 |
| SIP TRUNK WIZARD | 3-7 |
| CHANGE SYSTEM PASSWORDS | 3-7 |
| Change FTP Password | 3-7 |
| Change Webmin Password | 3-7 |
| Change Webmin After Initial Setup | 3-8 |
| CHANGE ROOT PASSWORD | 3-8 |
| DATABASE PREPARATION | 3-9 |
| Database Setup | 3-9 |
| CONFIGURE IPedge APPLICATION SERVER MESSAGING | 3-9 |
| RESTART IPedge SERVER | 3-16 |
| SYSTEM DATABASE BACKUP | 3-16 |
| HTTPS CERTIFICATE | 3-16 |
| LICENSES | 3-17 |
| Download License File | 3-17 |
| Upload and Apply License | 3-17 |
| Display License Information | 3-17 |
| Over Subscribing | 3-18 |
| REGION CODE | 3-18 |
| MODEL DATABASE PROCEDURES | 3-20 |
| Download Model Database | 3-20 |
| Upload the IPedge Model Database File | 3-20 |
| Restore the IPedge Model Database File | 3-20 |
| Restart IPedge Server | 3-21 |
| SET SYSTEM TIME | 3-21 |
| Real Time Clock Hardware | 3-23 |
| NAME THE SERVER | 3-23 |
| DATABASE SYNCHRONIZATION | 3-25 |
| ADDING ACD to IPedge VIRTUAL SERVER | 3-26 |
| Setup ACD | 3-26 |

Chapter 5 – UCedge Service Setup

| | |
|-----------------------------------|-----|
| UCEDGE SETUP | 4-1 |
| USER ACCOUNT SETUP | 4-5 |
| Station Assignments | 4-5 |
| PHONE ONLY USER ACCOUNT | 4-5 |

Chapter 6 – Enterprise Manager

| | |
|------------------------------------|-----|
| SUPPORTED BROWSERS | 5-1 |
| LOGIN | 5-1 |
| START PAGE | 5-2 |
| VERSION DISPLAY | 5-3 |
| AUTOMATIC NEW VERSION DETECT | 5-3 |
| ROLES | 5-4 |
| Create a New Role | 5-4 |
| Copy a Role | 5-4 |
| USERS | 5-4 |
| ADMINISTRATION USER | 5-4 |

Chapter 7 – Webmin

| | |
|------------------------|-----|
| STOP SERVICES | 6-1 |
| START SERVICES | 6-1 |
| RESTART SERVICES | 6-1 |
| REBOOT SYSTEM | 6-1 |
| SHUTDOWN SYSTEM | 6-2 |

Chapter 8 – Application Server Backup

| | |
|------------------------------------|-----|
| BACULA | 7-1 |
| BACKUP SCHEDULE | 7-2 |
| Change Backup Schedule | 7-2 |
| Create a New Backup Schedule | 7-3 |
| Verify Backup Job Status | 7-4 |
| RESTORE FROM BACKUP | 7-4 |
| MANUAL BACKUP | 7-5 |
| Manual Backup Procedure | 7-5 |
| Create the Download File | 7-5 |
| Download Backup File | 7-6 |
| MANUAL RESTORE | 7-6 |
| Upload Backup File | 7-6 |
| Restore the Server | 7-7 |
| ACD BACKUP | 7-8 |

Chapter 9 – HTTPS Configuration

| | |
|---------------------------------|-----|
| HTTPS CONFIGURATION | 8-1 |
| Create New Certificate | 8-1 |
| Root Certificate Download | 8-2 |
| Trust the Certificate | 8-2 |
| TURN HTTPS OFF | 8-2 |

Chapter 10 – Meeting

| | |
|--|-----|
| IPedge MEETING INITIAL CONFIGURATION | 9-1 |
| Meeting IP Address and Hostname | 9-1 |
| ASSIGN MODERATORS | 9-5 |
| Setup a Meeting | 9-5 |
| Email Summary Settings | 9-5 |

Chapter 11 – Net Server

| | |
|--|-------|
| ADD NET SERVER | 10-1 |
| SETUP THE CIX SYSTEM I/O PORT | 10-2 |
| NET SERVER LEVEL 2 CONFIGURATION | 10-2 |
| NET SERVER MENU | 10-2 |
| Status | 10-3 |
| Setup | 10-4 |
| LEVEL 2 MENU | 10-13 |
| Devices Menu | 10-13 |
| Logging | 10-15 |
| Dial Rule Menu | 10-16 |
| Dial Plan | 10-16 |
| Calling Within My Home Area Code | 10-17 |
| Calling Outside the Home Area Code | 10-18 |
| Server Based Call Manager Configuration | 10-19 |
| Create User Groups | 10-19 |
| Assign Users to Call Manager Application | 10-20 |
| Assign Users to User Groups | 10-22 |
| Server Based Call Manager Upgrade | 10-26 |
| Installation | 10-26 |
| Net Server configuration | 10-28 |

Chapter 12 – Messaging

| | |
|--|------|
| ADD THE MESSAGING APPLICATION | 11-1 |
| SETUP THE I/O PORTS | 11-1 |
| ASSIGN THE VOICEMAIL SIP STATIONS | 11-3 |
| ADD STATIONS TO A STATION/HUNT GROUP | 11-3 |
| System Voice Mail Data | 11-4 |
| Stations | 11-4 |
| PROGRAM MESSAGING | 11-4 |
| DISK FULL NOTIFICATION | 11-5 |
| MESSAGING BACKUP | 11-6 |
| MANUAL BACKUP | 11-6 |
| Backup to a Different Directory | 11-7 |
| Backup to FTP Site | 11-7 |
| Retrieve Backup to Local PC | 11-8 |
| Scheduling a Backup | 11-8 |

| | |
|-----------------------------------|------|
| RESTORE..... | 11-9 |
| Restore from Directory | 11-9 |
| Restore from FTP..... | 11-9 |
| Upload from Local Directory | 11-9 |

Chapter 13 – Fax

| | |
|---|-------|
| FAX MAIL SYSTEM | 12-1 |
| FAX FEATURE DESCRIPTION | 12-1 |
| Fax Mail | 12-1 |
| Fax-on-Demand | 12-2 |
| SOFTWARE REQUIREMENTS for FAX..... | 12-2 |
| HARDWARE REQUIREMENTS for FAX | 12-2 |
| FAX PART NUMBERS | 12-3 |
| NETWORK CONFIGURATION for FAX | 12-3 |
| FAX INSTALLATION..... | 12-3 |
| CIX PROGRAMMING | 12-3 |
| MESSAGING PROGRAMMING | 12-7 |
| Retrieving Faxes..... | 12-9 |
| FAX ON DEMAND | 12-9 |
| FAX-ON-DEMAND SCRIPT FUNCTIONS | 12-10 |
| Script Functions | 12-10 |
| Get Phone No..... | 12-10 |
| Trans. Fax | 12-10 |
| FAX CONTACTS | 12-12 |
| FAX LOG..... | 12-12 |
| FAX QUEUE | 12-12 |
| AUDICODES INSTALLATION | 12-14 |
| LOAD AUDICODES TEMPLATE | 12-14 |
| CONFIGURE THE AUDICODES FAX GATEWAY | 12-15 |
| CLIENT INSTALLATION..... | 12-19 |
| FAX PRINTER DRIVER | 12-19 |
| FAX PRINTER DRIVER CONFIGURATION..... | 12-19 |
| WEB CONTROLLER MAILBOX FAX OPTIONS | 12-20 |
| Fax Settings | 12-20 |
| Incoming Faxes | 12-20 |
| Fax Confirmation | 12-20 |
| Auto Print | 12-21 |
| Fax Contacts | 12-21 |
| Fax Log..... | 12-21 |
| Fax Queue | 12-21 |
| Cover Information..... | 12-21 |
| Fax Confirmation | 12-21 |
| AUTO PRINT | 12-21 |

| | |
|--|-------|
| AUTOPRINT SERVICE. | 12-22 |
| AutoPrint on Windows Vista and Windows 7 | 12-23 |
| Printer Configuration. | 12-24 |

Chapter 14 – Maintenance

| | |
|--|------|
| INTRODUCTION. | 13-1 |
| ALARM NOTIFICATION | 13-1 |
| IPedge VIRTUAL APPLICATION SERVER RECOVERY. | 13-1 |
| SERVER FAN REPLACEMENT | 13-2 |
| SERVER POWER SUPPLY REPLACEMENT | 13-2 |
| POWER UP SERVER. | 13-2 |
| HOT-SWAP HARD DRIVE | 13-2 |
| HDD INDICATORS | 13-2 |

Chapter 1 – Introduction

INTRODUCTION

The IPedge Virtual Application Server for the Strata CIX System is an advanced communications server.

Each IPedge Application Server has multiple applications running on the server. These applications include Messaging, Meeting, Call Manager, Webmin, Bacula and Enterprise Manager. Some applications are extra cost options.

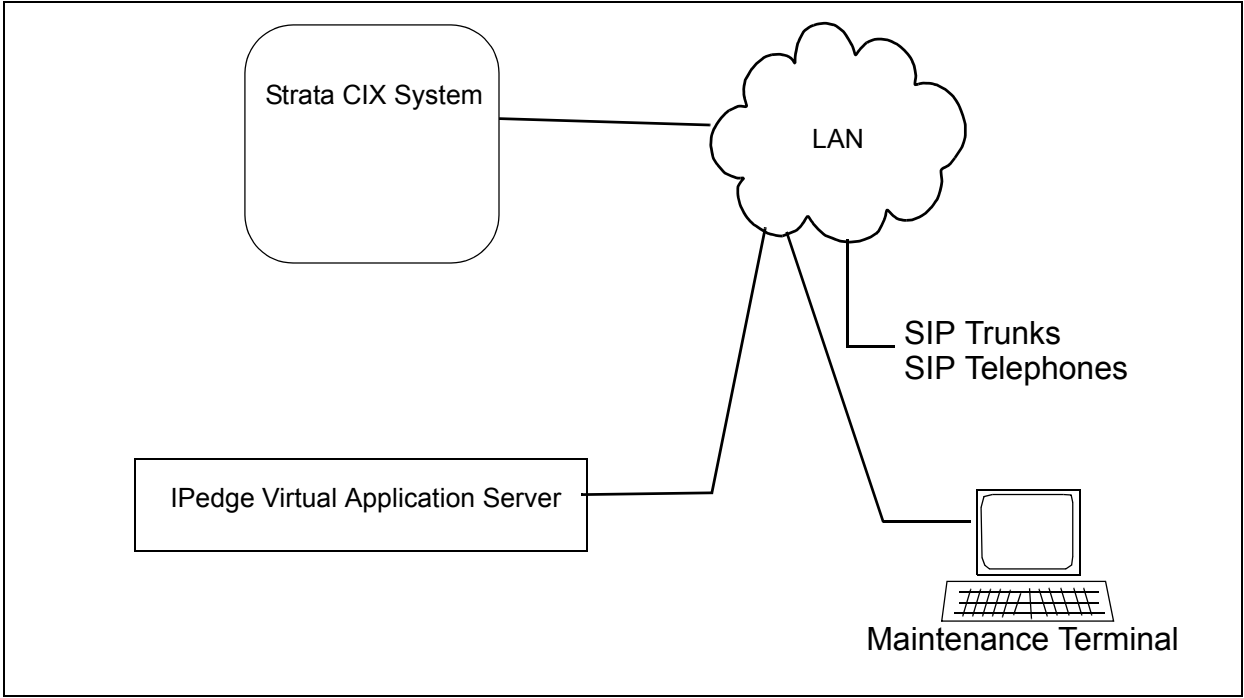


Figure 1-1 IPedge Application Server For Strata CIX System

APPLICATION SERVER ADMINISTRATION

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

The Enterprise Manager can be accessed using:

- Microsoft™ Internet Explorer version 8 or later
- Mozilla® Firefox® version 12 or later - Must have IE Tabs

The system can be administered remotely over the internet.

Important! The Strata CIX system administration requires Network eManager running on your PC.

IPedge SERVER APPLICATIONS

The IPedge server in each node is referred to as the Integrated IPedge server. This server includes these IPedge Applications:

- IPedge Messaging
- Call Manager
- IPedge Meeting
- IPedge Enterprise Manager

The IPedge Application Server also includes:

- WebMin
- Bacula
- Call Manager (Client)

Enterprise Manager Single View, Single Page

All of the IPedge Application Server functions are accessed through Enterprise Manager.

Chapter 2 – Server Hardware Installation

SERVER HARDWARE 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 Application Server

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

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.

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. Refer to [Figure 2-1](#), [Figure 2-1](#), or [Figure 2-3](#).
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.

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**.

Identify System Previous Owner Information New Owner Information

Products you are transferring
PowerEdge R720 (5RGDH02)

Previous Owner Information

First Name

Last Name

Company Name *

Email

Street Address

Country

City

State/Prov/Cnty

Zip Code *

Phone Number

[Previous](#)

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 web form for transferring ownership. At the top, a progress bar has four steps: 'Identify System' (checked), 'Previous Owner Information' (checked), 'New Owner Information' (current step, highlighted with a blue triangle), and 'Review' (empty). 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: 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.

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

My Account Order Status Feedback

Support > Ownership Transfer

Ownership Transfer

> Support Home Page

> Drivers & Downloads

> Product Support

> Order Support

> Support By Topic

> Warranty Information

> Contact Us

Thank You

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.

[Submit more tags >](#)

Keep your new acquired Dell product up-to-date.

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.

[Product Support](#)

If you have any questions regarding the ownership transfer of this system, please contact Customer Service at [Customer Service](#). All requests to transfer ownership, service, limited warranty* and Dell support are determined in Dell's sole discretion. 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

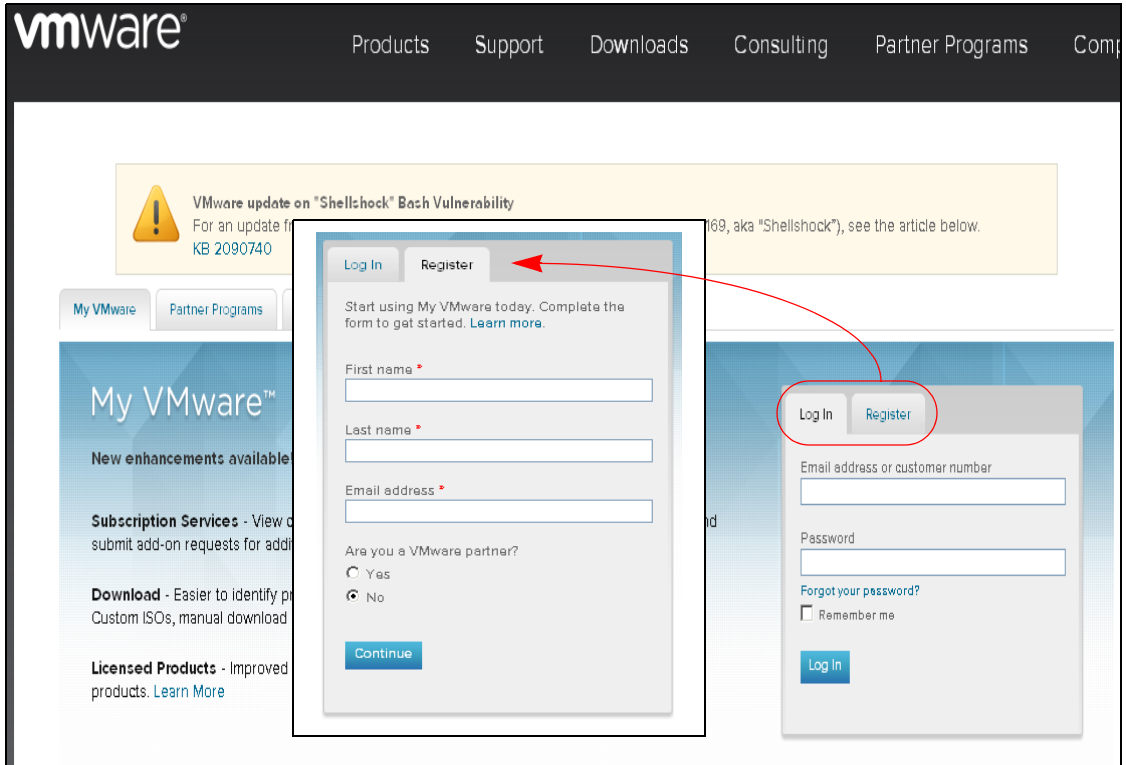
Any service contract applicable to your system is identified by the Service Tag number and may be transferred only in conjunction with the transfer of the entire system. If the system is being transferred into a geographic location in which the same service as provided under the subject service contract 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.

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

- 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>
- 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 2-1.

does not already have a VMware license they can use this procedure to acquire a free VMware license.

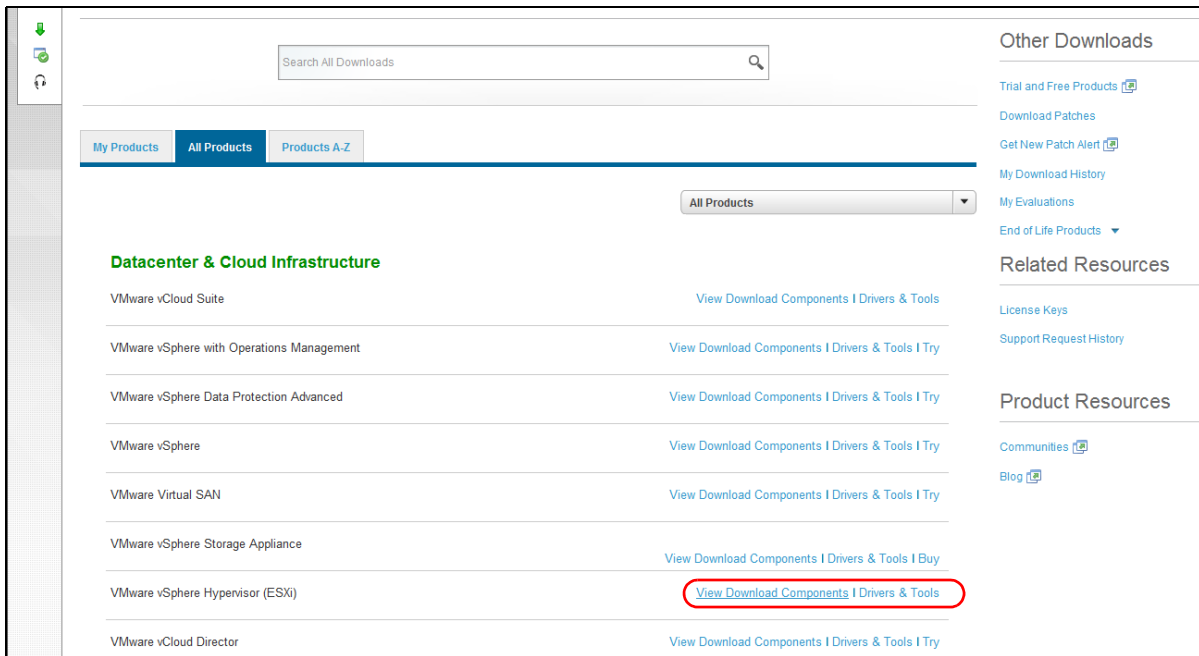
1. Navigate to the VMware website; <http://www.vmware.com>.
2. Click on the Register tab to create an account.



3. Follow the on screen instructions to create your account.
4. When your account has been confirmed by email go to the next step.
5. Browse to <http://vmware.com/products/vsphere-hypervisor>. Click on **Download**.

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.

6. Select VMware vSphere Hypervisor (ESXi).



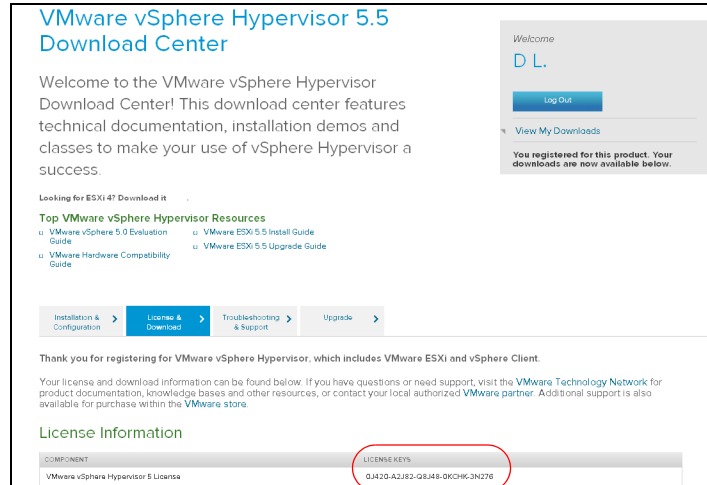
7. Click on Register.



8. 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.

CHANGE VMWARE (ESXi) IP ADDRESS

9. 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. Refer to [Figure 2-1](#), [Figure 2-2](#), or [Figure 2-4](#).

1. Press **F2** Customer System/ View Logs.
2. Press **F2** Customise System/ View Logs again.
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**.

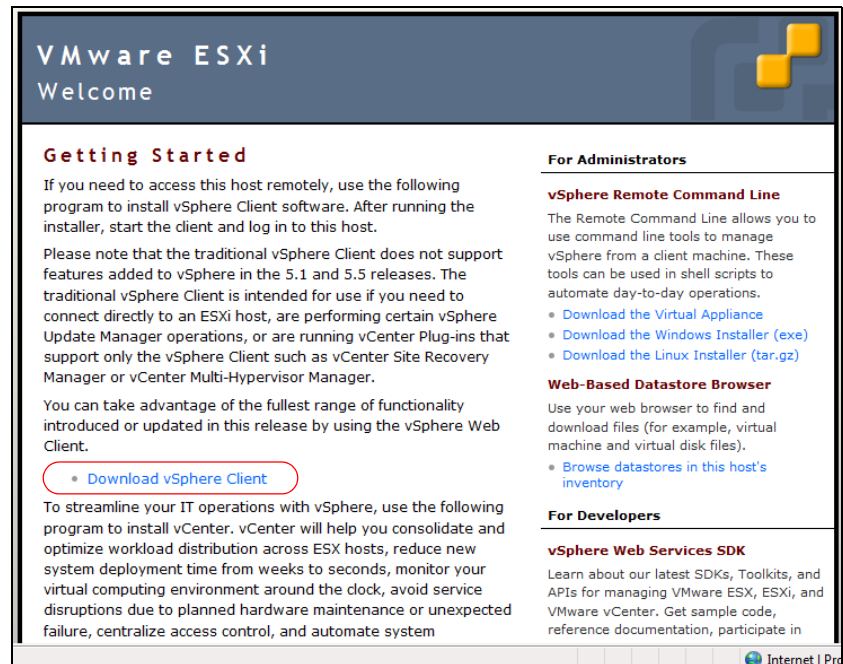
8. Arrow down to select **DNS Configuration** then, press **Enter**.
Arrow down to set the **Primary DNS** IP address.
Arrow down to set **Alternate DNS** IP address.
 9. Leave the hostname at the default value of localhost.
 10. Press **Enter**.
 11. Press **ESC**
 12. Press **ESC**
 13. Press **F12** 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 your administration PC. If you already have vSphere on your PC skip to [UPLOAD THE LICENSE KEY on page 2-9](#).

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.

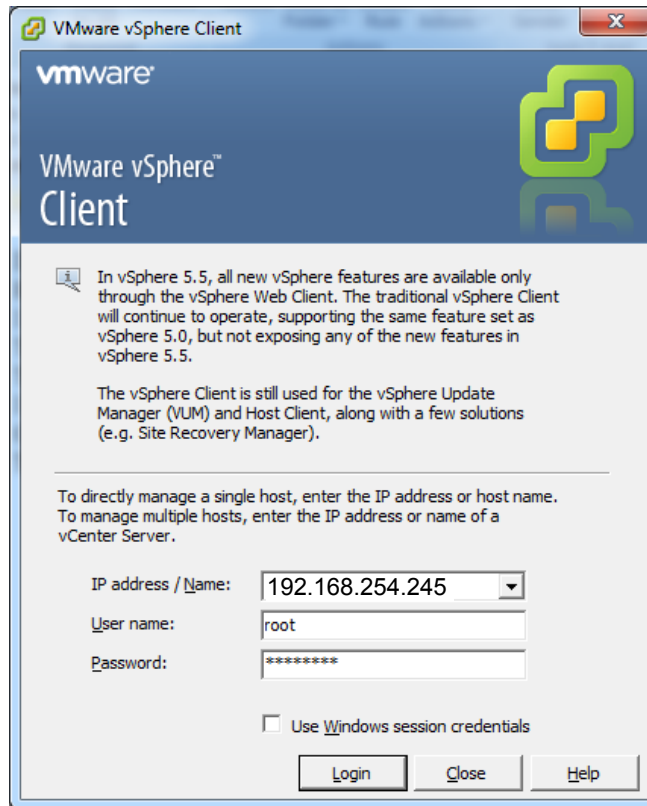
3. The vSphere client will download then launch the installer. Follow the prompts to complete the installation. This will take several minutes.

UPLOAD THE LICENSE KEY

UPLOAD THE LICENSE KEY

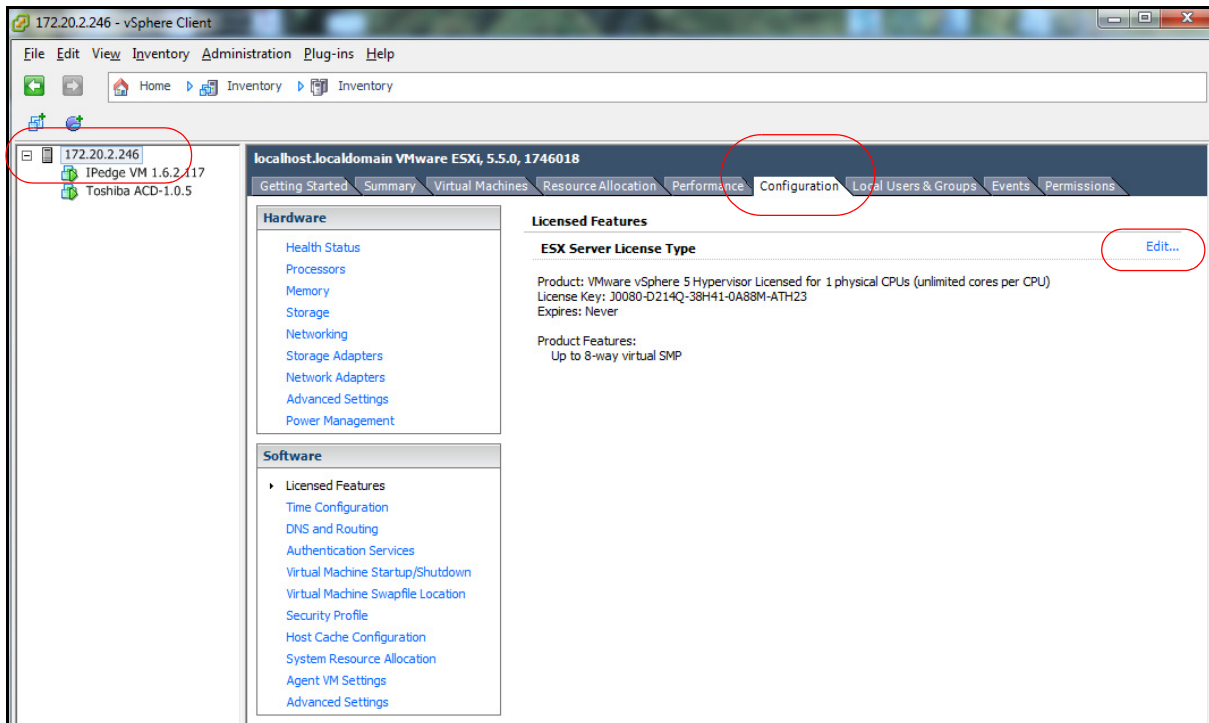
This procedure is used to apply the VMware license key to the server.

1. Launch vSphere Client.

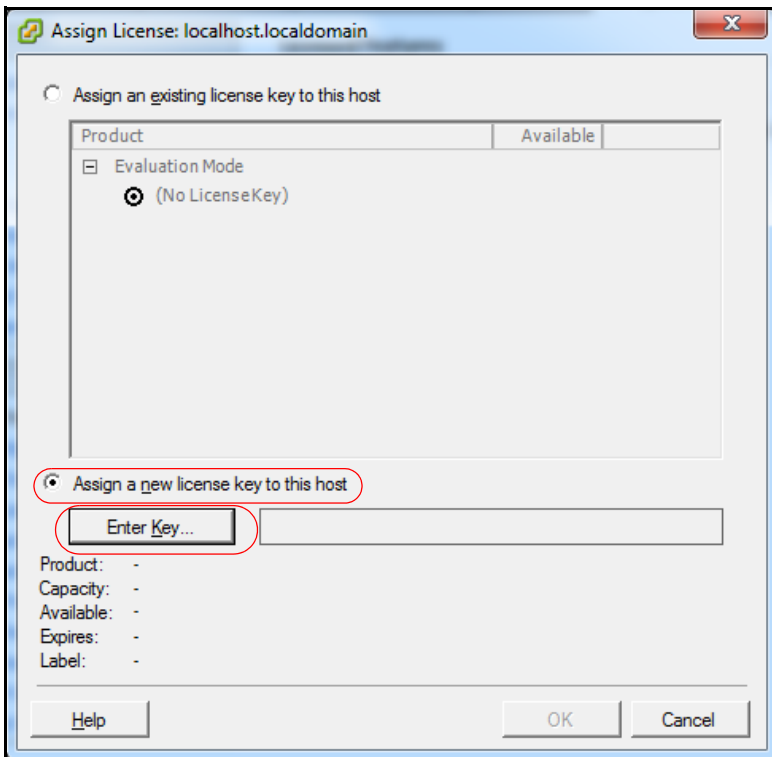


2. Enter the IP address of the IPedge Virtual server.
3. The default user name is; root.
The default password is: password.
4. Click on the **Login** button.

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

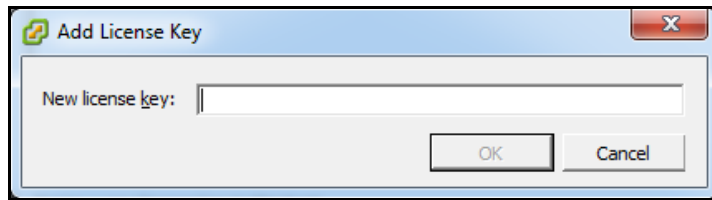


6. Click on the Assign a new license key to the host radio button.
7. Click on **Enter key** button.



DONGLE PORT

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



- Click on **OK**.

Important! This procedure must be completed within 60 days or the server will stop processing.

DONGLE PORT

The license dongle **MUST** remain plugged into the server at all times. The systems monitors the dongle.

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.

IP NETWORK CONNECTION

Each IPedge Virtual Server chassis has from two to four NIC connectors. The connectors are teamed. The network cable can be plugged into any NIC port.

POWER SUPPLY

The power supply AC input and heat generated, at maximum load, are shown in [Table 2-1](#)

PHYSICAL

Table 2-1 Power Supply Specifications

| Item | R220 | R420 | R720 |
|-----------------------|-----------|-----------|----------------|
| AC Volts (50 ~ 60 Hz) | 100 ~ 240 | 100 ~ 240 | 100 ~ 240 |
| Current AMPs (120 V) | 4.0 | 7.4 | 6.5 (3.25 x 2) |
| Maximum Power (Watts) | 100.00 | 174.5 | 605 |
| BTU/Hr (MAX) | 1040 | 2315 | 1908 |
| Idle Power (Watts) | 53.30 | 85.6 | 287.9 |

PHYSICAL

The physical size, weight, and power requirements are shown in [Table 2-2](#).

Table 2-2 IPedge Virtual Server Physical Specifications

| Item | R220 | R420 | R720 |
|----------------------------|-------------------------|-------------------------|------------------------|
| Height | 42.8 mm (1.68 in.) (1U) | 42.8 mm (1.68 in.) (1U) | 87.3mm (3.44 in.) (2U) |
| Width with rack latches | 482.4 mm (18.99 in.) | 482.4 mm (18.99 in.) | 482.4 mm (18.99 in.) |
| Depth (excludes bezel) | 393.7 mm (15.5 in) | 607.0 mm (23.9 in) | 755.8 mm (29.75 in) |
| Weight (maximum) | 8.058 kg max (17.73 lb) | 19.9 kg (43.87 lb) | 29.5 kg (65.03 lb) |
| Width without rack latches | 434.0 mm (17.08 in.) | 434.0 mm (17.08 in.) | 444.0 mm (17.48 in.) |
| Maximum Power (Watts) | 100.00 | 174.5 | 605 |
| Idle Power (Watts) | 53.30 | 85.6 | 287.9 |

SERVER CHASSIS INSTALL

Refer to the DELL instructions to install the chassis rackmount rails and to install the chassis in the rack. When the chassis is installed in the rack use the following procedure.

1. Plug the license dongle into a USB connector on the chassis.
2. Plug the network cable into any server NIC.
3. Plug the AC power cord(s) into the server power supplies.
4. Plug the AC power cords into the AC power source.
5. Set the power supply switches, if equipped, to ON.
6. Use the front panel switch to power up the server.

DELL DELL R420 SERVER The PowerEdge R420 is a 1.68 inch (1U) rack-mount server. The R420 server has a single power supply (P/S) with one 115 V AC, 15 AMP power cord.

The R420 without the RAID option has one HDD. The R420 with RAID1 has two HDDs. The server cannot have the RAID option added after shipping.

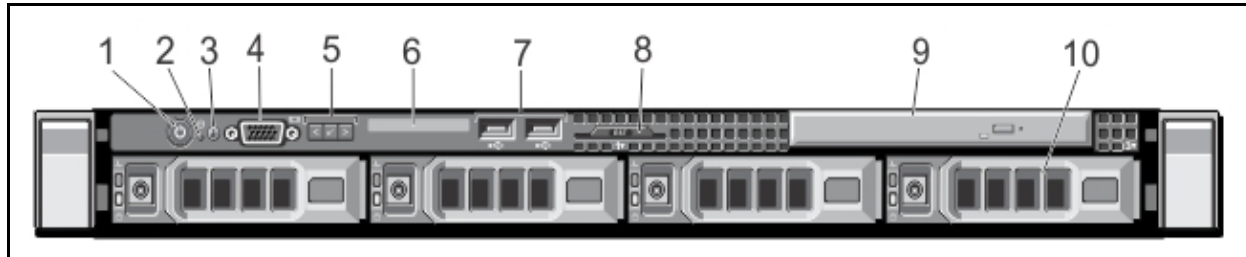


Figure 2-1 R420 Server Front Panel

Table 2-3 R420 Server Front Panel

| Label | Item | Description |
|-------|----------------------------------|---|
| 1 | Power-on indicator, power button | The power-on indicator lights when the system power is on. The power button controls the power supply output to the system. NOTE: On ACPI-compliant operating systems, turning off the system using the power button causes the system to perform a graceful shutdown before power to the system is turned off. |
| 2 | NMI button | Used to troubleshoot software and device driver errors when running certain operating systems. This button can be pressed using the end of a paper clip. Use this button only if directed to do so by qualified support personnel or by the operating system's documentation. |
| 3 | System identification button | The identification buttons on the front and back panels can be used to locate a particular system within a rack. When one of these buttons is pressed, the LCD panel on |
| 4 | Video connector | Allows you to connect a VGA display to the system. |
| 5 | LCD menu buttons | Allows you to navigate the control panel LCD menu. |
| 6 | LCD panel | Displays system ID, status information, and system error messages. The LCD lights blue during normal system operation. The LCD lights amber when the system needs attention, and the LCD panel displays an error code followed by descriptive text. NOTE: If the system is connected to a power source and an error is detected, the LCD lights amber regardless of whether the system is turned on or off. |
| 7 | USB connectors (2) | Allows you to connect USB devices to the system. The ports are USB 2.0-compliant. |

(Sheet 1 of 2)

Table 2-3 R420 Server Front Panel

| Label | Item | Description (continued) |
|-------|--------------------|---|
| 8 | Information tag | A slide-out label panel which allows you to record system information such as Service Tag, NIC, MAC address and so on as per your need. |
| 9 | Optical drive slot | Not equipped |
| 10 | Hard drives | Up to four 2.5 inch hot-swappable hard drives |

(Sheet 2 of 2)

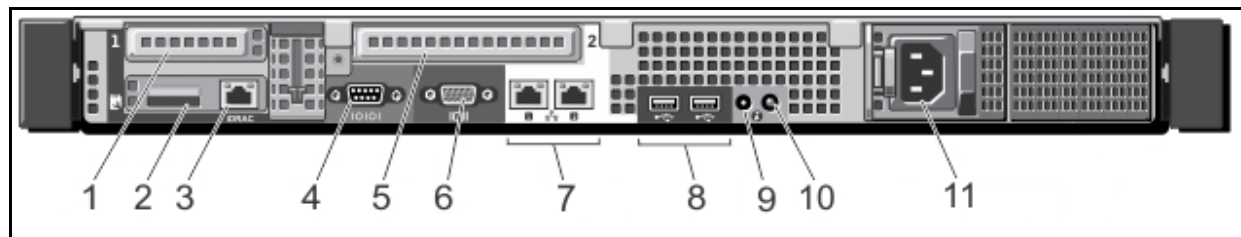


Figure 2-2 R420 Server Rear Panel

Table 2-4 R420 Server Rear Panel

| Label | Item | Description |
|-------|--|---|
| 1 | PCIe expansion card slots, low-profile | Not used. |
| 2 | vFlash card slot | Accepts a vFlash media card. Not used. |
| 3 | iDRAC7 Enterprise Port | Dedicated management port. |
| 4 | Serial connector | Serial device connection. |
| 5 | PCIe expansion card slots, low-profile | Not used. |
| 6 | Video connector | VGA display connection. |
| 7 | Ethernet connectors | Two integrated 10/100/1000 Mbps NIC connectors |
| 8 | USB connectors (2) | Allows you to connect USB devices to the system. The ports are USB 2.0-compliant. |
| 9 | System Identification Connector | Connects the optional system status indicator assembly through the optional cable management arm. |
| 10 | System identification button | The identification buttons on the front and back panel can be used to locate a particular system within a rack. When one of these buttons is pressed, the LCD panel on the front and the system status on the back flashes until one of the buttons is pressed again. |
| 11 | Power supply | AC power input plug |

DELL R720 SERVER

The PowerEdge R720 is a 2.5 inch (2U) rack-mount server. The server includes two power supplies. Refer to [Figure 2-3](#) and [Figure 2-4](#).

The R420 without the RAID option has one HDD. The R420 with RAID1 has two HDDs. The server cannot have the RAID option added after shipping.HDD - Two (RAID1) or Four (RAID5)

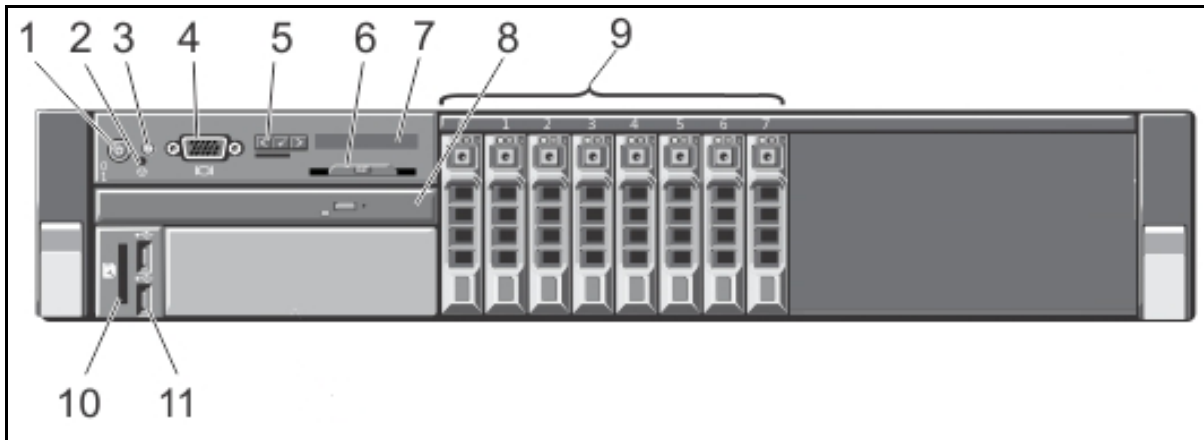


Figure 2-3 R720 Front Panel

Table 2-5 R720 Server Front Panel

| Label | Item | Description |
|----------------|----------------------------------|--|
| 1 | Power-on indicator, power button | The power-on indicator lights when the system power is on. The power button controls the power supply output to the system. NOTE: On ACPI-compliant operating systems, turning off the system using the power button causes the system to perform a graceful shutdown before power to the system is turned off. |
| 2 | NMI button | Used to troubleshoot software and device driver errors when running certain operating systems. This button can be pressed using the end of a paper clip. Use this button only if directed to do so by qualified support personnel or by the operating system's documentation. |
| 3 | System identification button | The identification buttons on the front and back panels can be used to locate a particular system within a rack. When one of these buttons is pressed, the LCD panel on |
| 4 | Video connector | Allows you to connect a VGA display to the system. |
| 5 | LCD menu buttons | Allows you to navigate the control panel LCD menu. |
| (Sheet 1 of 2) | | |

Table 2-5 R720 Server Front Panel

| Label | Item | Description (continued) |
|-------|------------------------|---|
| 6 | Information tag | A slide-out label panel which allows you to record system information such as Service Tag, NIC, MAC address and so on as per your need. |
| 7 | LCD panel | Displays system ID, status information, and system error messages. The LCD lights blue during normal system operation. The LCD lights amber when the system needs attention, and the LCD panel displays an error code followed by descriptive text. NOTE: If the system is connected to a power source and an error is detected, the LCD lights amber regardless of whether the system is turned on or off. |
| 8 | Optical drive slot | Not equipped |
| 9 | Hard drives | Up to up to four 2.5 inch hot-swappable hard drives. |
| 10 | vFlash media card slot | Accepts a vFlash media card. Not used. |
| 11 | USB connectors (2) | Allows you to connect USB devices to the system. The ports are USB 2.0-compliant. |

(Sheet 2 of 2)

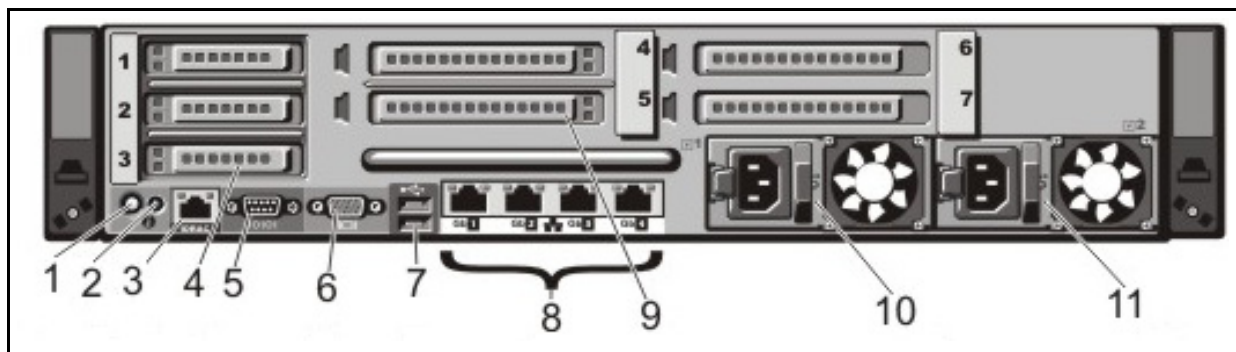


Figure 2-4 R720 Rear Panel

Table 2-6 R720 Server Rear Panel

| Label | Item | Description |
|-------|--|--|
| 1 | System identification button | The identification buttons on the front and back panel can be used to locate a particular system within a rack. When one of these buttons is pressed, the LCD panel on the front and the system status on the back flashes until one of the buttons is pressed again. |
| 2 | System Identification Connector | Connects the optional system status indicator assembly through the optional cable management arm. |
| 3 | iDRAC7 Enterprise Port | Dedicated management port. |
| 4 | PCIe expansion card slots, low-profile (3) | Not Used |
| 5 | Serial connector | Serial device connection. |
| 6 | Video connector | VGA display connection. |
| 7 | USB connectors (2) | Allows you to connect USB devices to the system. The ports are USB 2.0-compliant. |
| 8 | Ethernet connectors | Four integrated 10/100/1000 Mbps NIC connectors or Four integrated connectors that include: Two 10/100/1000 Mbps NIC connectors Two 100 Mbps/1 Gbps/10 Gbps SFP+/10 GbE T connectors |
| 9 | PCIe expansion card slots full height | Not used |
| 10 | Power supply (PSU1) | AC power input plug shown |
| 11 | Power supply (PSU2) | |

HARD DISK DRIVE INDICATORS

HARD DISK DRIVE INDICATORS

The HDD indicators are shown in [Figure 2-5](#) and [Table 2-7](#).

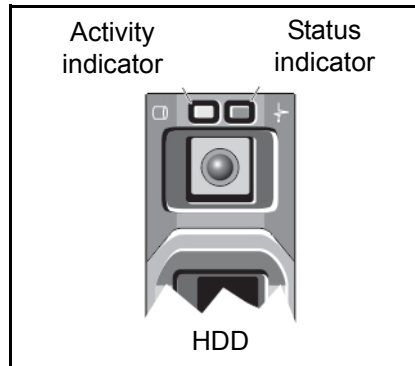


Figure 2-5 HDD Indicator

Table 2-7 RAID Hard Disk Drive Indicators

| Status Indicator Pattern | Condition |
|---|---|
| Flashes green two time per second | Identifying drive or preparing for removal (RAID only) |
| Off | Drive is ready for removal. The status indicator will remain off until all of the HDDs are initialized after the system is turned on. HDDs are not ready for insertion or removal during this time. |
| Flashes; green, amber, off. | Predicted HDD failure. |
| Flashes amber four times per seconds | HDD failed |
| Flashes green slowly | HDD rebuilding |
| Steady green | HDD is online |
| Flashes green three seconds, amber three seconds, and off six seconds | HDD rebuild aborted |

RACKMOUNT INSTALLATION

RACKMOUNT INSTALLATION

The IPedge servers 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.

Table 2-8 Rack Mount Rail Kits

| Part Number | Description |
|---------------|--|
| DELL-770-BBIF | R220 standard size rail kit – 1U/2U Static Rails for 2-Post and 4-Post Racks, Customer Kit (770-BBIF) |
| DELL-770-BBIG | R220 short rail kit – 1U/2U Static Rails for 2-Post and 4-Post Racks, Short, Customer Kit (770-BBIG) |
| DELL-331-5460 | R420 static rail – Ready Rails Static Rails for Select 1U systems, Universal 2-Post/4-Post, Customer Install (331-5460) |
| DELL-331-5463 | R420 sliding rail kit – Ready Rails Sliding Rails Without Cable Management Arm for 1U Systems, Customer Kit (331-5463) |
| DELL-330-8149 | R720 static rail kit – Ready Rails Static Rails for select 2U systems, Univ 2-Post/4-Post, Customer Install (330-8149) |
| DELL-331-4436 | R720 sliding rail kit – Ready Rails Sliding Rails for 2U PowerEdge Systems, Customer Kit (331-4436) |

The optional rackmount rails are not included with the server chassis. The optional mounting rails can be ordered from Toshiba. Refer to the [Table 2-8](#) for the Rail Kit part numbers. Rail installation instructions are available from 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.

POWER REQUIREMENTS

The IPedge Application 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.

UPS RECOMMENDATIONS

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

This page is intentionally left blank.

Chapter 3 – Network Requirements

The IPedge Virtual Server requires static IP addresses.

- The IPedge Virtual Server static IP address.
- The IPedge server static IP address.
- If the ACD server is licensed it will require a static IP address
- To support ACD; a public domain name (such as; acd-example.com)
 - The ACD server FQDN must be registered. The ACD server system must have a public IP address (your router must have a public IP address and be setup for port forwarding to the ACD server system private IP address (ports are listed in the System Ports Feature Description).
- To support UCedge; a public domain name (such as; example.com) for the IPedge server is required.
 - The IPedge server FQDN must be registered. The IPedge server 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 are listed in the System Ports Feature Description).
 - The router connecting the IPedge server WAN must have a static, public IP address. The FQDN resolves to that IP address.
- The router on the IPedge Virtual server network must have DNS capability to resolve the FQDN to the private IP address of the IPedge server. Toshiba recommends the Adtran 3120 and 3448.

At each site all of the system components are connected via a LAN. The IPedge Virtual Application Server, gateways and, other servers communicate over the site LAN. Other devices connect over a WAN or the Internet.

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 What's up Gold, Solarwinds or, IPSLA.

The following servers 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. If equipped, the IPedge Meeting names must 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 (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

This page is intentionally left blank.

Chapter 4 – App Server Installation

INTRODUCTION

This chapter presents a detailed procedure for installing an IPedge Virtual Application server.

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
- **ESXi (VMware):** 192.168.254.245
- **iDRAC7:** 192.168.254.251

PRE-INSTALLATION REQUIREMENTS

Refer to the [IPedge Power Requirements and Server Hardware Installation](#) chapter in this document for power, environment, and UPS requirements. Refer to the LAN Requirements chapter 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 on the server front panel.
- 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.
- IPedge Virtual Server license dongle serial number (required to license the system)
- IP Addresses:
 - VMWare® (ESXi) requires one Static IP address
 - 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
- Subnet mask
- Network Time Protocol source

NETWORK NAMES

- Host names
- Default Gateway IP address
- DNS server IP address (Required for Online Update operation)
- Domain name (FQDN) for the IPedge Virtual Application server required for UCedge operation
- 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 Application server 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.

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 - This will be also used be for the Meeting server. |

Descriptive names are recommended. Names could show location by city, campus location or server room and rack location.

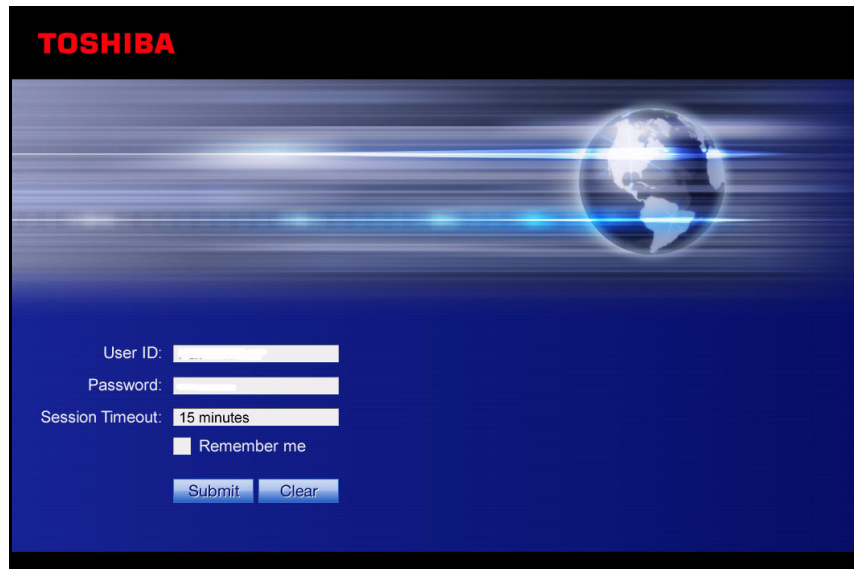
**VIRTUAL SERVER
INSTALLATION
PROCEDURE**

The following steps include instructions for installation. The instructions also consider on-site system configuration and off-site pre-configuration.

Important! The IPedge Virtual Server must have the License Dongle plugged in and a LAN connection BEFORE connecting the power. The dongle can be plugged into any USB connector on the server and the LAN cable can be plugged into any NIC on the server.

**Login To The IPedge
Server**

1. Plug the license dongle into any USB connector on the server.
2. Connect the IPedge server to a PC through 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 DNS IP addresses in the DNS Server list (shown in red above). The DNS server list must be entered to support Online Update operation.

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:

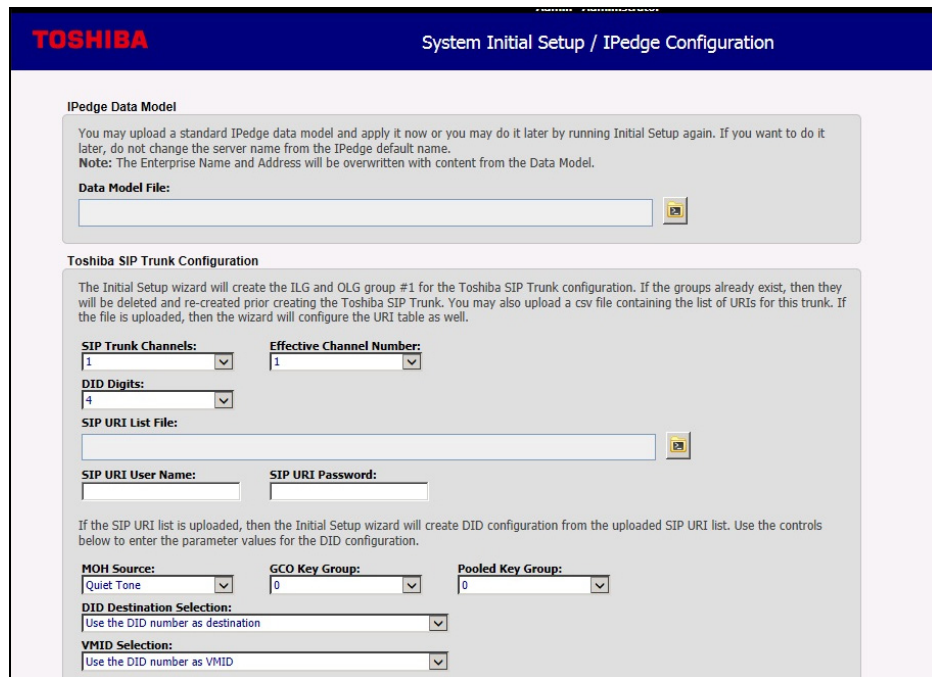
- Enterprise Information
 - IPedge Server Community Name
 - IPedge Region
 - License File Information
2. The administrator can Apply changes, go Back to change information or Cancel. Click on Next, to open the next screen, click on Back to return to the previous screen.

Any change this parameter in this area will cause a system reboot.

Figure 4-2 Initial Setup In Enterprise Information and License Screen

3. Upload the 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 IPedge

portal in the Customer Services tab as Trunk # and Password respectively.



4. Click on the Apply button to save configuration.



5. Verify the data, click on the **OK** button to restart the server.

6. Log in to Enterprise Manager.

SIP TRUNK WIZARD

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

7. 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.

8. 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 16-41.

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

Change Webmin
Password

1. Login to Enterprise Manager.
2. Select the server.
3. Select **Application > Webmin**.
4. The Webmin window will open. Click on **Logout** on the left side of the screen.
5. In the login dialog enter **Administrator** as the user name and **password** as the password.
6. If this is the first time anyone has logged into Webmin you will be prompted to change the password.

7. Enter the current password (**password**)
Enter the new password: Toshiba recommends that you use a strong password made up of alpha characters (upper and lower case) and numeric characters (0~ 9)
8. Confirm the password.
9. The password is changed. Record the new password in a secure location.

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

10. Go to [CHANGE ROOT PASSWORD](#).

Change Webmin After Initial Setup

This procedure is used to change the Webmin User Name and Password after the initial setup. If you are not prompted to change the password after logging into Webmin directly use this procedure.

1. Login to Enterprise Manager.
2. Select the server.
3. Select **Application > Webmin**.
4. The Webmin window will open. Click on **Webmin Users**.
5. Click on **Webmin user Administrator**.
6. In the Webmin user access rights, select the Password drop-down list. Change from "don't change" to **set to**.
7. Enter the **New password** into the box.
8. Scroll down to click on **Save**.

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.

9. Click on **root**.
10. Enter the **New password**,
11. Click on the **Change** button.
12. Close the Webmin window.

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

DATABASE PREPARATION

If you have used the System Initial Setup/IPedge Setup and a Model Database go to [“CONFIGURE IPedge APPLICATION SERVER MESSAGING”](#) on Page 4-9.

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 APPLICATION SERVER MESSAGING”](#) on Page 4-9.

Database Setup

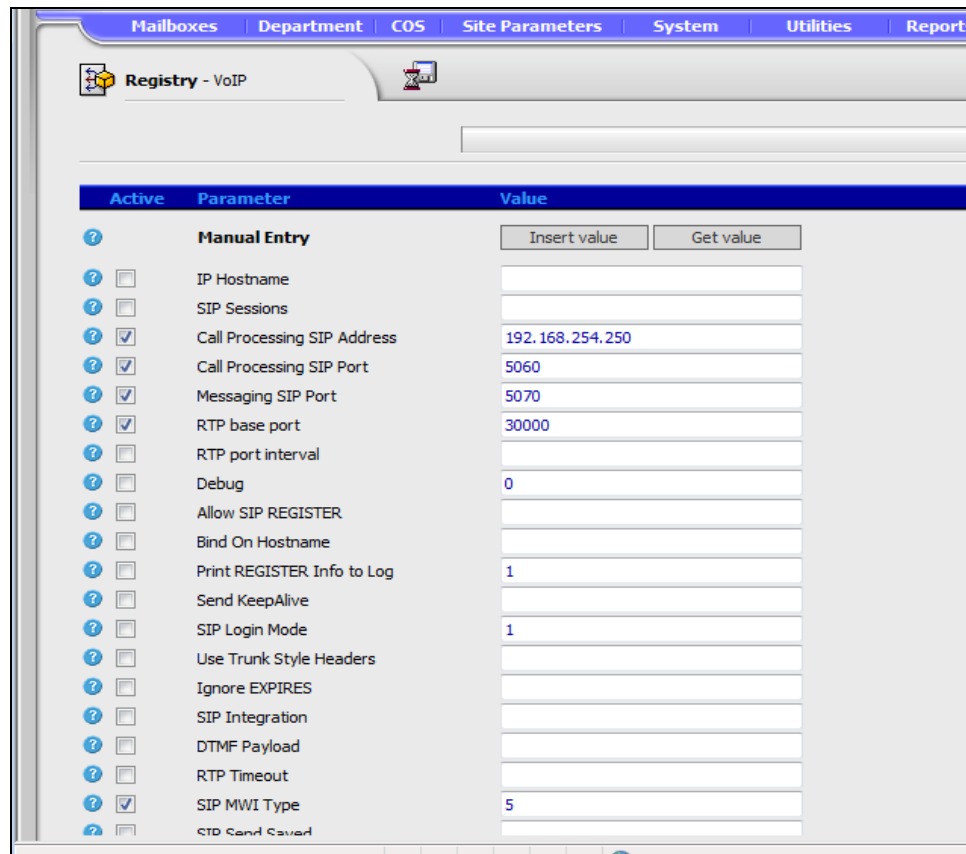
If you are going to use a model database and did not apply it in the System Initial Setup/IPedge Setup change the system name to IPedge (default value) then go to [“MODEL DATABASE PROCEDURES”](#) on Page 4-20.

CONFIGURE IPedge APPLICATION SERVER MESSAGING

Verify the following parameters before configuring IPedge Messaging:

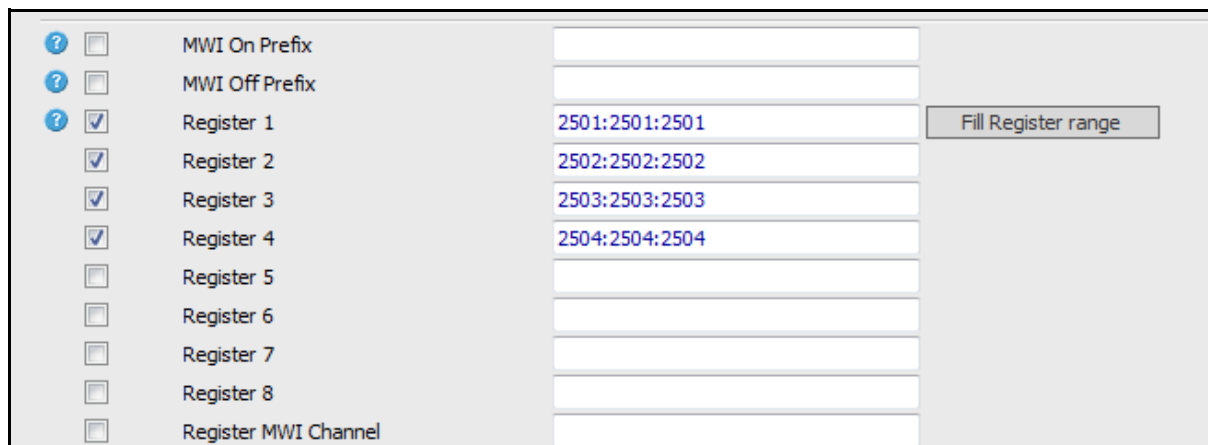
- Specify number of voice ports and station number.
Voice port station numbers need to match the Call Processing station numbers.
 - Number of voice ports licenses
 - Number of voice mailbox licenses
Ensure that the number of mail box licenses are enough for the number of stations.
1. To configure the Messaging Voice ports login to Enterprise Manager. Select **Application > Messaging**.

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



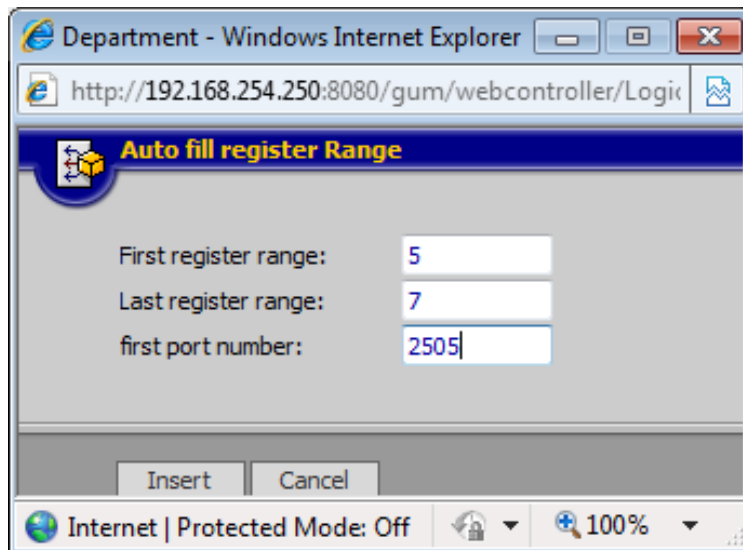
3. The following parameters must be customized:

- A. Ensure that IP Hostname is un-checked and the parameter field is blank.
- B. Call Processing SIP Address: Enter IPedge server or MIPU IP address.
- C. Register X: At least four voice port entries will be displayed after you load the model database file. Refer to the example below.



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.

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 | |

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

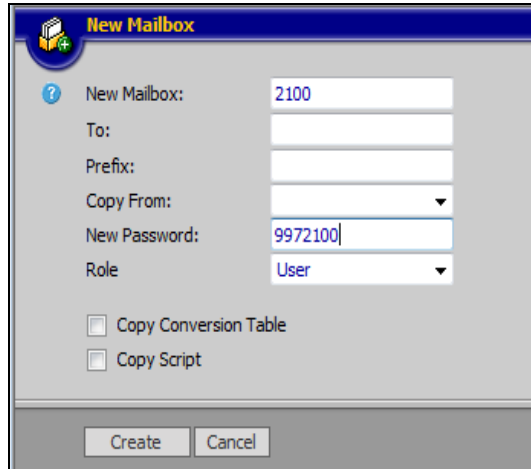
In the Messaging window, select **Mailbox > Properties**.

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

The screenshot displays the 'Mailbox - Properties' configuration window. At the top, there is a navigation bar with tabs for Mailboxes, Department, COS, Site Parameters, System, Utilities, Reports, and Registry. Below the navigation bar, there is a search field with the number '100' and a 'Go' button. The main configuration area is divided into several sections:

- Mailbox is not locked** (indicated by a green checkmark)
- MWI:** Radio buttons for A (selected), B, R, and N.
- MWI2:** Radio buttons for A (selected), B, R, and N.
- Optional:** An empty text input field.
- Special MWI:** Checkboxes for Active, Saved, Email, and Fax. The 'Active' checkbox is checked. 'On:' and 'Off:' fields are present.
- MWI Counters:** Checkboxes for Saved, Email, and Fax.
- Use:** Radio buttons for Mailbox and Extension (selected) with the text 'when sending mwi'.
- Home Node:** A dropdown menu set to '0'.
- Additional MWI DNS:** An 'Edit' button.
- Department:** A dropdown menu set to '1'.
- Class of Service:** A dropdown menu set to '1'.
- Mailbox Type:** A dropdown menu set to 'Admin.'.
- Mailbox Role:** A dropdown menu set to 'User'.
- Time Zone:** A dropdown menu set to 'America/Los_Angeles' with '(GMT-8:00)' next to it.
- First Name:** An empty text input field.
- Last Name:** An empty text input field.
- Password:** A masked text input field (dots) and a 'Change PWD' button.
- Ext. 1:** A text input field containing '100'.
- Ext. 2:** An empty text input field.
- Ext. 3:** An empty text input field.

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.

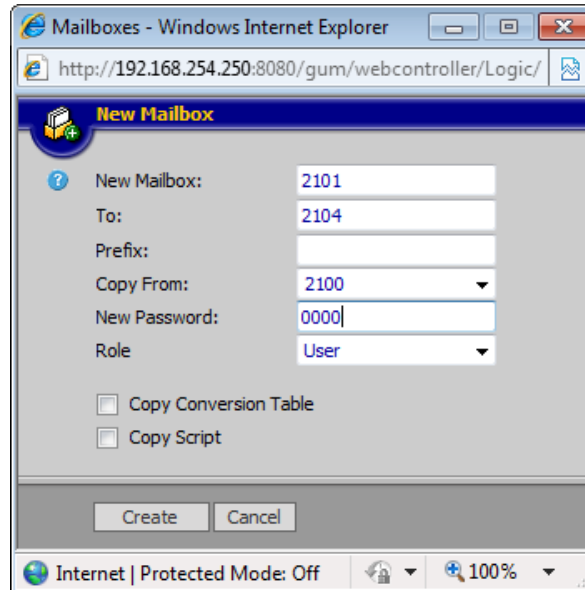
Choose “User” role.

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**

RESTART IPedge SERVER

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

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 7-5](#)

Messaging Backup – [“MANUAL BACKUP” on page 15-11](#)

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

5. Go to [“SET SYSTEM TIME” on Page 4-21](#).

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 7-5](#).

HTTPS CERTIFICATE

1. If you are going to use https secure connection to the Enterprise Manager create the https certificate. Refer to [Chapter 8–HTTPS Configuration](#) in this manual then go to [“Database Setup” on page 4 - 9](#).
2. If you are not going to use https go to [“Database Setup” on page 4 - 9](#).

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.

LICENSES

Licenses are purchased through the Toshiba FYI web site. Use the following procedure to update or add new licenses.

Download License File

After the licenses have been purchased, download the license 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.
10. Go to “[DATABASE PREPARATION](#)” on page 4 - 9.

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.

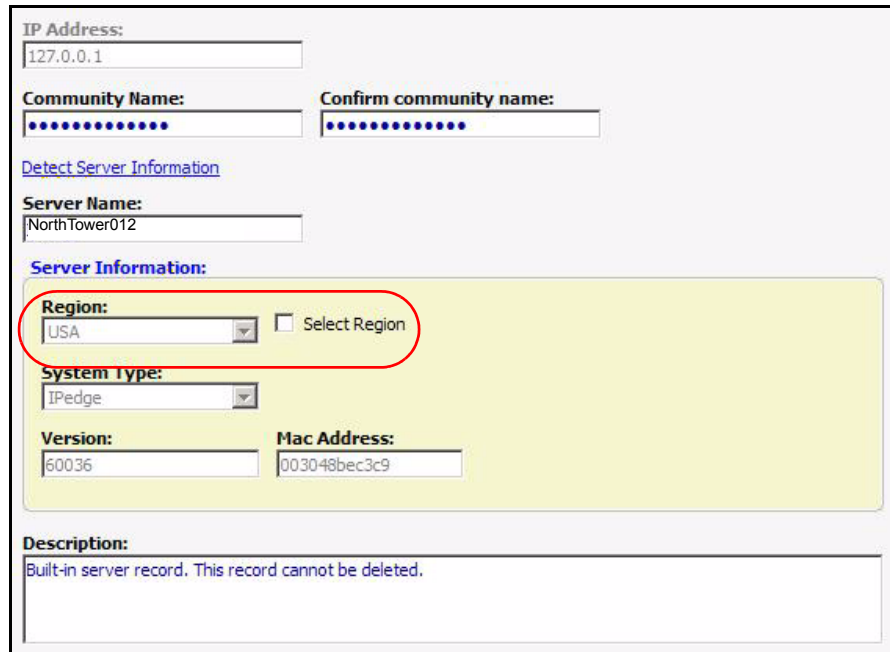
The Region Code is setup during the Initial setup process. Use this procedure to change the region code.

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.

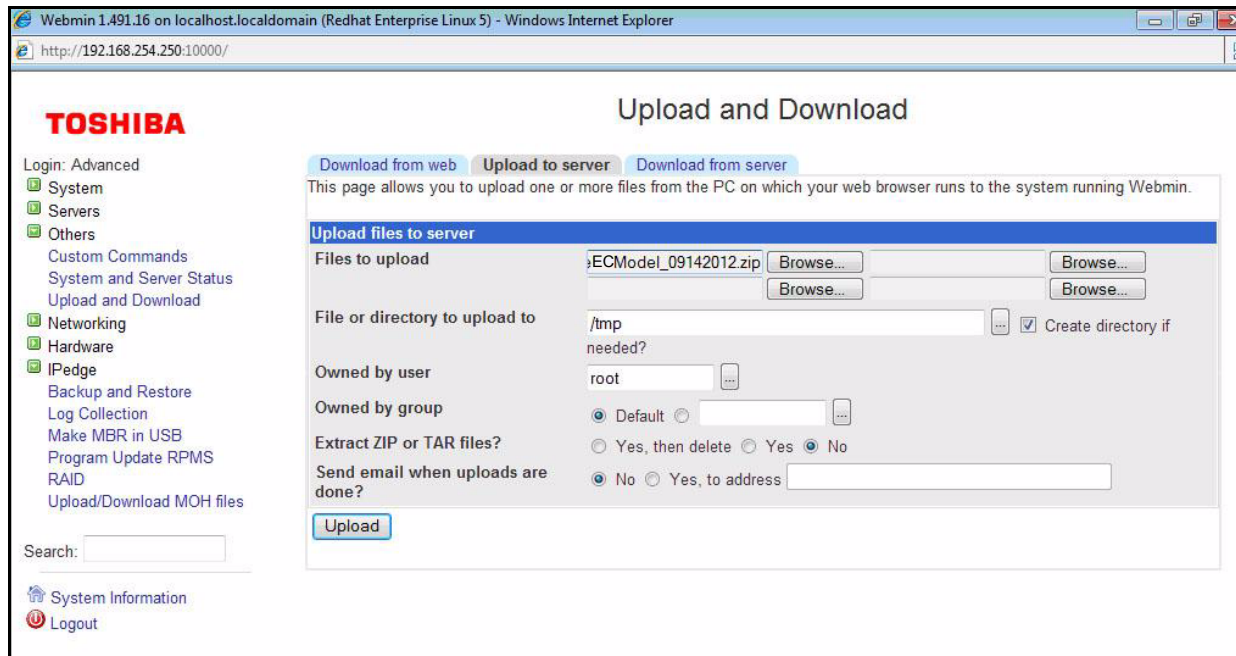
The following steps detail the model database download from the FYI website, upload to the server and restoration to the server database.

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. Login to Enterprise Manager.

Upload the IPedge Model Database File

1. Login to Enterprise Manager, select **Application > Webmin**.
2. Select **Application > Webmin > Others > Upload and Download**.
3. Select the “**Upload to Server**” tab.
4. Use the Browse button next to the ‘Files to upload’ field to find the model database (IPedgeXXModel_MMDDYYYY.zip) on your computer.
5. Enter **/tmp** in the ‘File or directory to upload to’ field.
6. Click to check mark the ‘Create Directory if needed?’ box. Leave the rest of the screen at default as shown below.
7. Click on **Upload**.

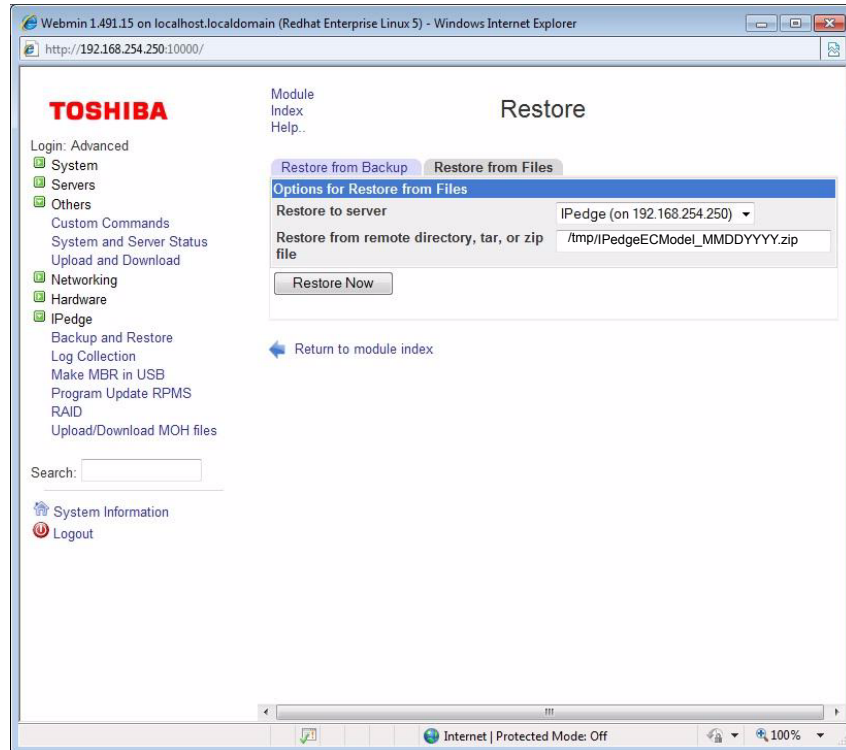


Note: Please wait as it may take a few minutes to upload. The Complete screen that says “Successfully uploaded the following files:...” displays.

Restore the IPedge Model Database File

1. From Enterprise Manager, click **Application > Webmin > IPedge > Backup and Restore** click on the **Restore** icon.
2. Select the ‘Restore from Files’ tab.

3. In the “Restore from remote directory, tar, or zip” field, enter the correct directory name and model database file name and extension (example, /tmp/IPedgeXXModel_MMDDYYYY.zip).
4. Click on the **Restore Now** button (as shown below). The restoration screen displays. This process may take about 5 to 8 minutes.



5. The Call Processing restoration screen displays. Wait for the screen to display --Done Restoring--.

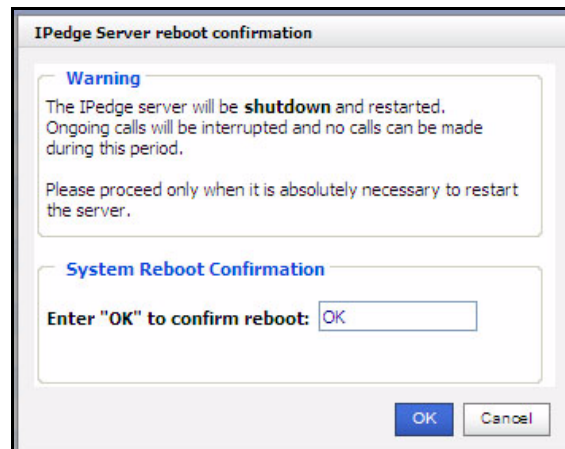
Restart IPedge Server

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

2. Click on the Reboot System icon



3. Enter **OK** to confirm the reboot.
4. Click on the **OK** button.
5. After the system has rebooted and has been running for a few minutes start the Messaging configuration.



SET SYSTEM TIME

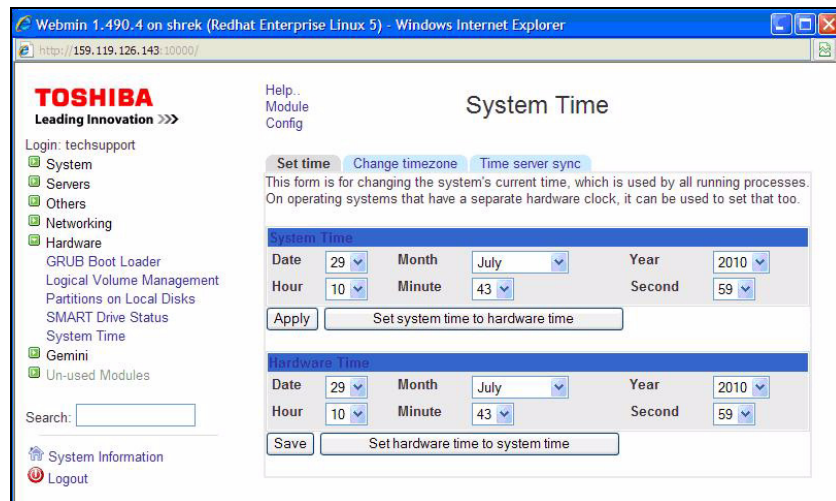
The time server is setup during the initial setup process. Use this procedure to change the NTP setup.

The following steps set the system time and assign the Network Time Protocol server pool. An NTP pool provides access to several NTP servers. This helps ensure that one or more servers is always available.

Toshiba recommends that all IPedge systems use an NTP server to set the system time.

All of the nodes in a multi-node system should synchronize to the same NTP pool. It is critical the time in each node is the same, within several seconds, as the other nodes.

1. Login to Enterprise Manager. Select **Application > Webmin**.
2. Select **Hardware > System Time** then, click on the **Set time** tab. Set the system time to the current correct time. This must be within a few minutes of the local correct time. A cell phone is an easy way to display the current time.



3. Click on **Apply**.
4. Click on the **Set hardware time to system time** button. Verify the Hardware time is the same as the System time you just entered.
5. Click on **Save**.
6. In the **Change timezone** tab set the local time zone.
7. In the **Time server sync** tab enter the Timeserver hostname. Use an NTP pool. Toshiba recommends that the system sync to an NTP pool once each day. In the example below a local region NTP pool (north-

america.pool.ntp.org). has been assigned and the system is set to synchronize everyday at midnight.

TOSHIBA Help... Module Config **System Time**

Set time Change timezone **Time server sync**

This form is for configuring the system to automatically synchronize the time with a remote server. Synchronization will be done using the Unix `ntp` protocol or NTP, depending on which commands are installed and what the remote system supports.

Time Server

Timeserver hostnames or addresses

Set hardware time too

Synchronize on schedule? No Yes, at times below ..

Simple schedule .. Daily (at midnight) Times and dates selected below ..

| Minutes | | | | | Hours | | Days | | | Months | | | Weekdays | | |
|--------------------------------------|-----------------------------------|----|----|----|--------------------------------------|-----------------------------------|--------------------------------------|-----------------------------------|----|--------------------------------------|-----------------------------------|-----------|--------------------------------------|-----------------------------------|--|
| <input checked="" type="radio"/> All | <input type="radio"/> Selected .. | | | | <input checked="" type="radio"/> All | <input type="radio"/> Selected .. | <input checked="" type="radio"/> All | <input type="radio"/> Selected .. | | <input checked="" type="radio"/> All | <input type="radio"/> Selected .. | | <input checked="" type="radio"/> All | <input type="radio"/> Selected .. | |
| 0 | 12 | 24 | 36 | 48 | 0 | 12 | 1 | 13 | 25 | January | February | March | Sunday | Monday | |
| 1 | 13 | 25 | 37 | 49 | 1 | 13 | 2 | 14 | 26 | April | May | June | Tuesday | Wednesday | |
| 2 | 14 | 26 | 38 | 50 | 2 | 14 | 3 | 15 | 27 | July | August | September | Thursday | Friday | |
| 3 | 15 | 27 | 39 | 51 | 3 | 15 | 4 | 16 | 28 | October | November | December | Friday | Saturday | |
| 4 | 16 | 28 | 40 | 52 | 4 | 16 | 5 | 17 | 29 | | | | | | |
| 5 | 17 | 29 | 41 | 53 | 5 | 17 | 6 | 18 | 30 | | | | | | |
| 6 | 18 | 30 | 42 | 54 | 6 | 18 | 7 | 19 | 31 | | | | | | |
| 7 | 19 | 31 | 43 | 55 | 7 | 19 | 8 | 20 | | | | | | | |
| 8 | 20 | 32 | 44 | 56 | 8 | 20 | 9 | 21 | | | | | | | |
| 9 | 21 | 33 | 45 | 57 | 9 | 21 | 10 | 22 | | | | | | | |
| 10 | 22 | 34 | 46 | 58 | 10 | 22 | 11 | 23 | | | | | | | |
| 11 | 23 | 35 | 47 | 59 | 11 | 23 | 12 | 24 | | | | | | | |

Note: Ctrl-click (or command-click on the Mac) to select and de-select minutes, hours, days and months.

8. Close the Webmin window.

Real Time Clock Hardware

If there is a system failure before the real time clock hardware updates the system time will need to be reset.

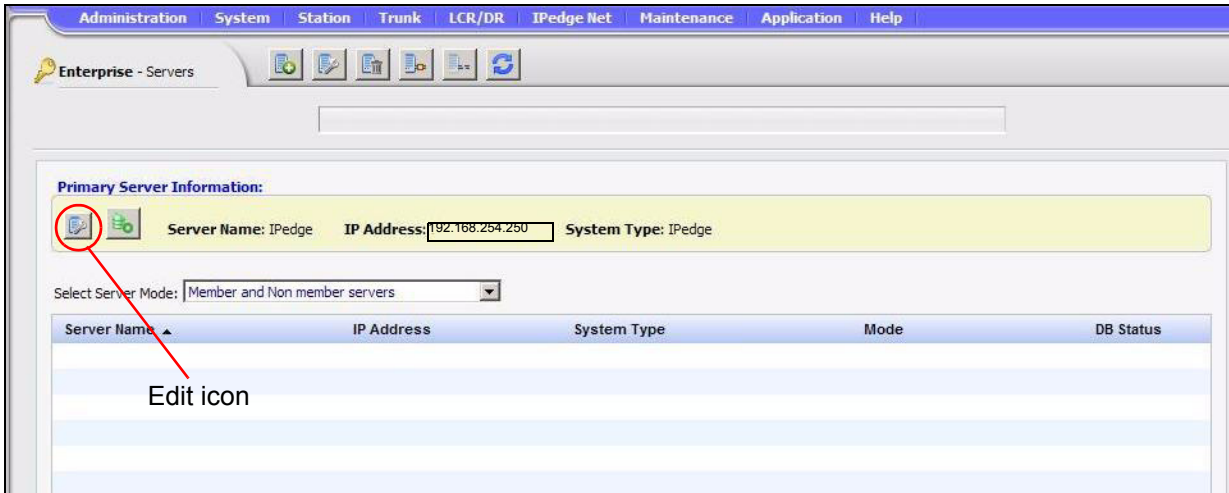
Important! Ensure that the Set hardware time too button is not checked.

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.

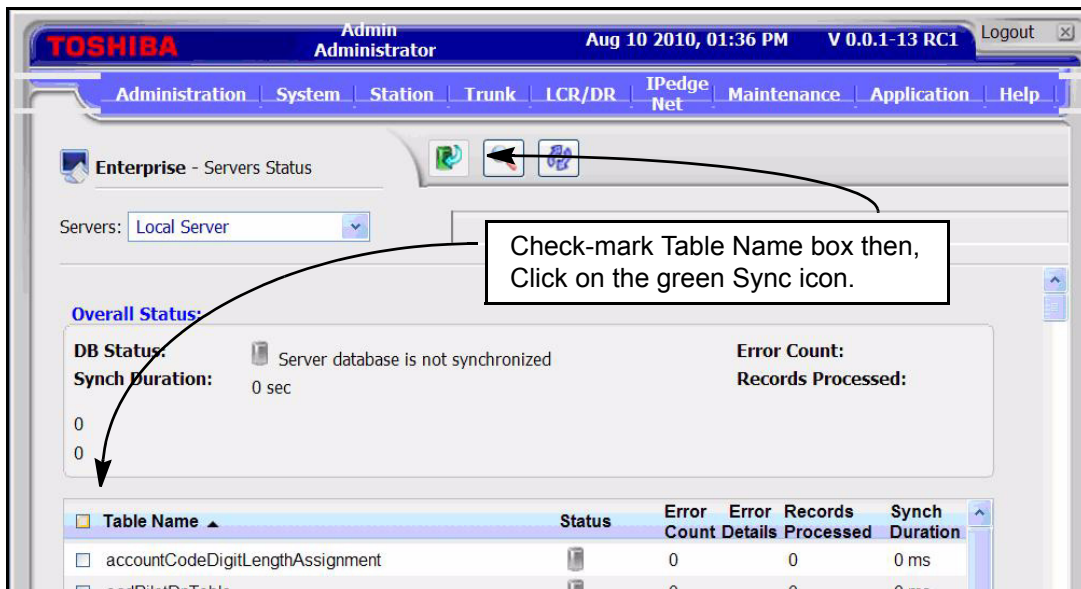
5. Click on the **Save** icon.
6. Click on **Detect Server Information**.
7. Go to "[DATABASE SYNCHRONIZATION](#)" on page 4 -25.

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 4-16](#).
5. Go to **"Database Setup"** on [page 4 - 9](#).

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 web site. 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. Apply ACD license to the IPedge server as needed. Refer to the New System Install chapter.
2. Select Application > ACD.
3. Program the ACD application. Refer to the IPedge ACD Administration manual.

Chapter 5 – UCedge Service Setup

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

UCEDGE SETUP

System:

- 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](#).
- 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.

- The router must be setup with port forwarding
 - 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.

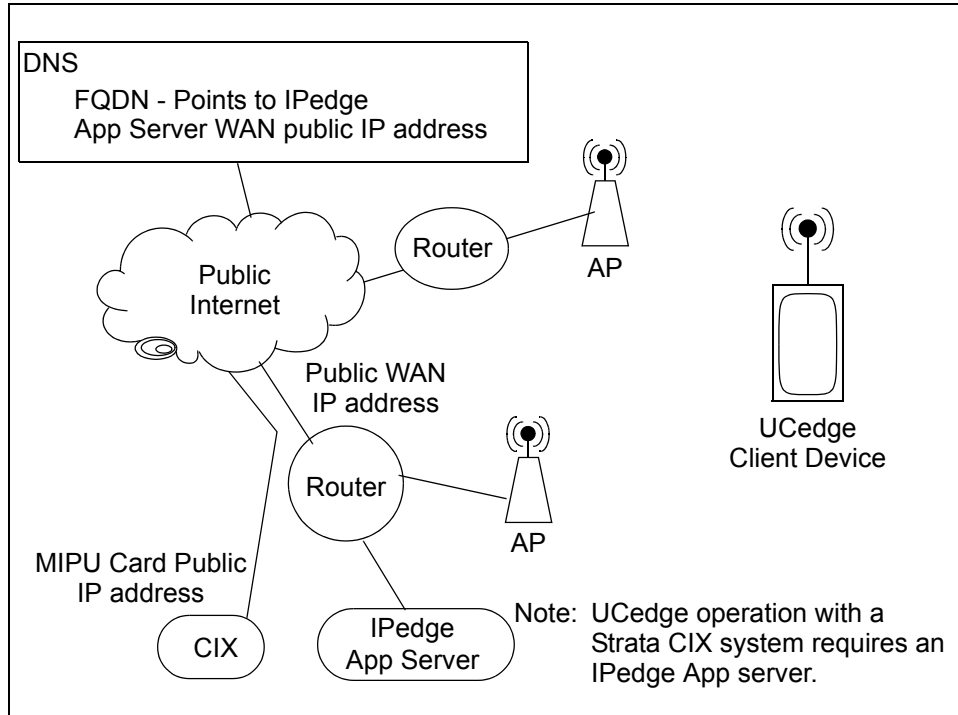


Figure 5-1 Basic Strata CIX System Network Diagram

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

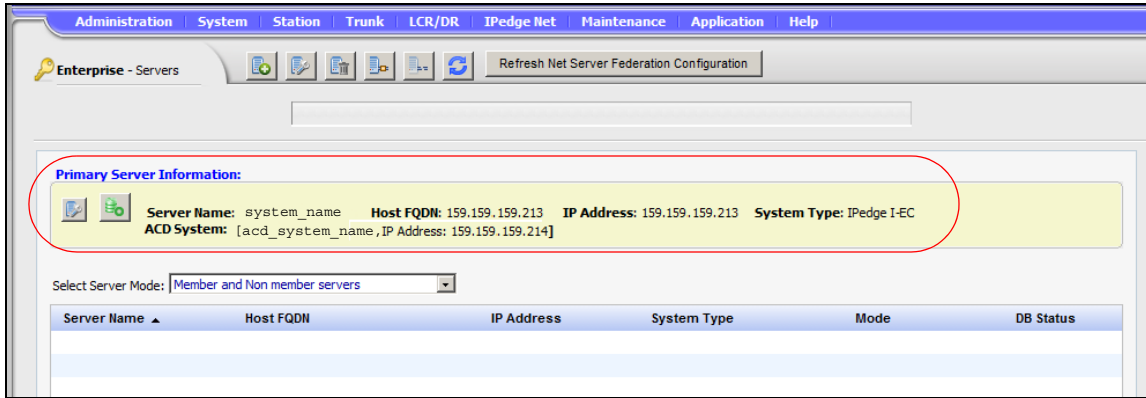
| Function | Type | Use |
|----------------|------|--------------------------------------|
| 90 | TCP | IPedge Messaging Mobile App Port |
| 1718 ~ 1719 | UDP | Remote IP Telephone set registration |
| 2944 | TCP | MEGACO |
| 5222 | TCP | XMPP Client |
| 5269 | TCP | XMPP Server |
| 5280 | TCP | XMPP Client |
| 8767 and 8768 | TCP | Net Server |
| 21000 to 22999 | UDP | Remote IP or SIP telephone audio |

Note: 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.

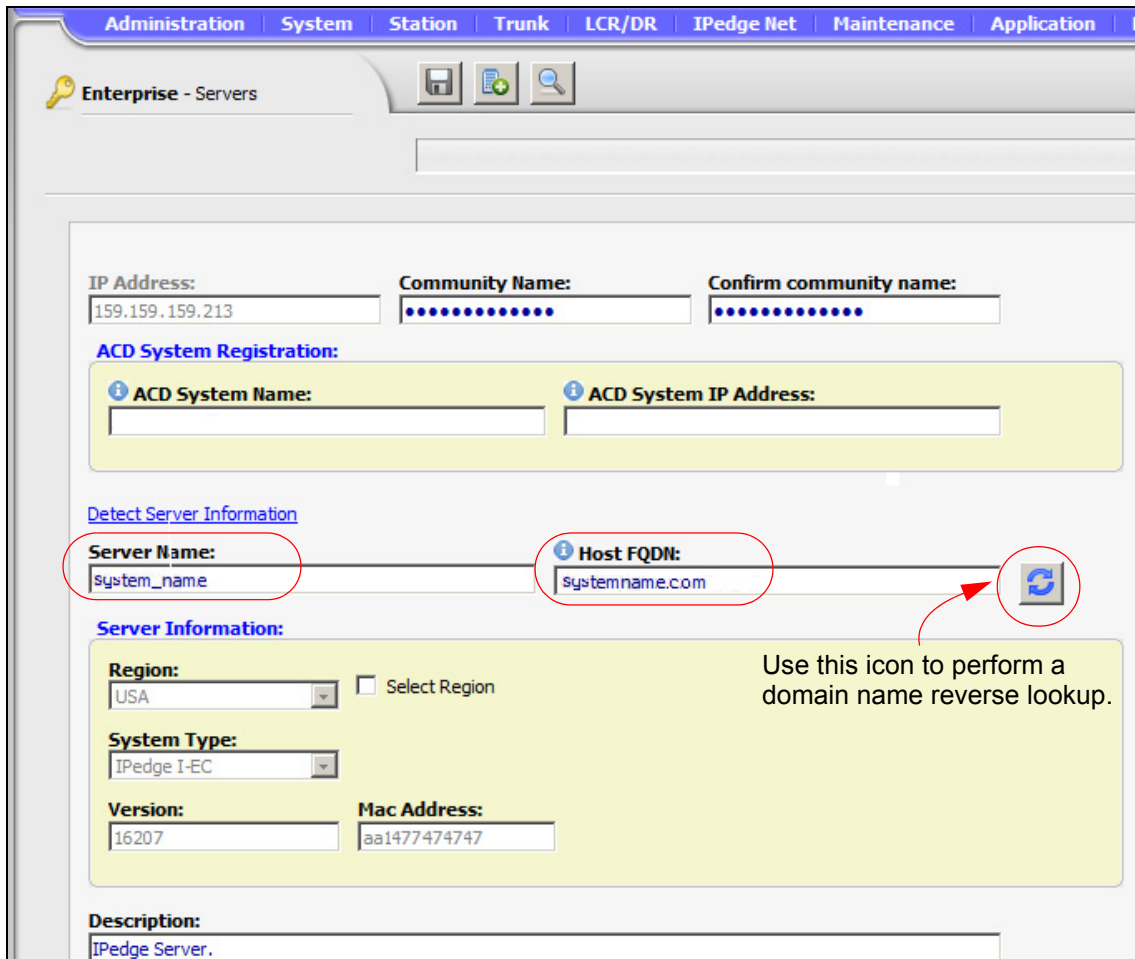
The FQDN for the IPedge server must be registered with a DNS service to resolve to the public IP address of the system router, the DNS server on the system network must resolve the FQDN to the private address of the IPedge server.

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

1. Select **Administration > Enterprise > Servers**.
2. Click on the **Edit** icon.
3. Enter the FQDN in the **Host FQDN** field.

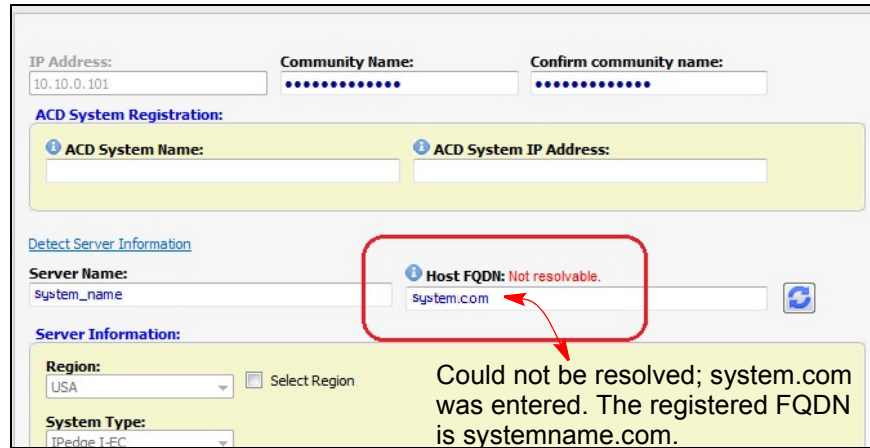


4. Enter the FQDN of the IPedge system in the **Host FQDN** field.



-
- 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. Some service providers disable the reverse lookup feature.



The screenshot displays a configuration interface with the following sections:

- IP Address:** 10.10.0.101
- Community Name:** [Redacted]
- Confirm community name:** [Redacted]
- ACD System Registration:**
 - ACD System Name: [Redacted]
 - ACD System IP Address: [Redacted]
- Detect Server Information:**
 - Server Name: system_name
 - Host FQDN: system.com (highlighted with a red box and error message)
- Server Information:**
 - Region: USA (with a "Select Region" checkbox)
 - System Type: IPedge T-EC

Error Message: Host FQDN: Not resolvable. Could not be resolved; system.com was entered. The registered FQDN is systemname.com.

USER ACCOUNT SETUP

The UCedge Client setup is started in the the Station Assignment page in Network eManager. 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; PhDN, 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.

Station Assignments

1. Login to Network eManager.
2. In Station Assignment create the stations.
3. When all of the stations are assigned export the station data.
4. Use a a spread sheet program to edit the CSV file.
Enter :
 - UC Client Account Name. The client account name can be up to 16 alpha-numeric characters, with no special characters.
 - Email address for each station
 - Display Name - use the First name. Last name format (for example; John.Doe)
 - The Security Code if the IP Phone Login Password parameter (in the Enterprise Manager Station Assignment) is set to Enable.

Note: The edited file must be saved as a CSV file.

5. Login to Enterprise Manager on the Application Server.
6. Import the CSV file into the Application Server.

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.

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.

This page is intentionally left blank.

Chapter 6 – Enterprise Manager

Enterprise Manager is a web browser based administration application that resides on every IPedge Application Server.

Enterprise Manager is a browser based interface that can be accessed from any computer with network access to the Primary node.

Note: Enterprise Manager is used for the initial application server setup and to administer Messaging. Network eManager is required for Strata CIX system administration.

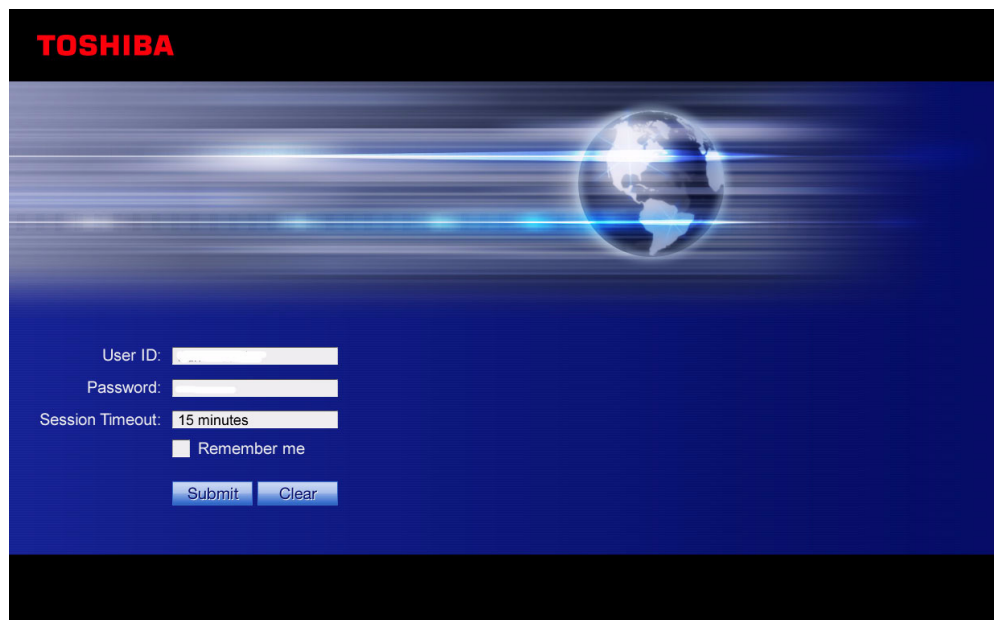
SUPPORTED BROWSERS

The Enterprise Manager can be accessed using:

- Microsoft™ Internet Explorer version 7 or later
- Mozilla Fire Fox version 5 or later

LOGIN

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



TOSHIBA

User ID:

Password:

Session Timeout:

Remember me

Note: When an IPedge Application 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

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:

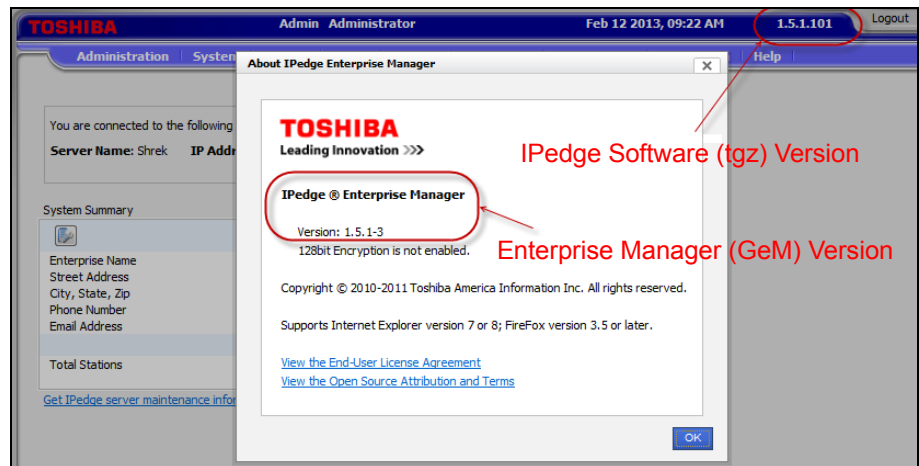
- Server Name
- Server Serial Number
- Mac Address of the server
- The version of the software on each node
- The FYI System Number of each node
- The Maintenance license expiration date for each server

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

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.

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.

ROLES

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

The IPedge Application Server has four technician 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.

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.

Chapter 7 – Webmin

Webmin is a graphical user interface used to simplify Linux operating system management. Webmin lets you perform these tasks through a web interface, and it automatically updates all of the required configuration files.

Webmin is accessed through Enterprise Manager, select **Application > Webmin**.

Although Webmin is accessed through Enterprise Manager it is not part of Enterprise Manager. When accessing Enterprise Manager through a fire wall you must have ports 8080 (Enterprise Manager) and port 10000 (Webmin) open.

STOP SERVICES

1. Select **Application > Webmin**.
2. In the Webmin screen select **System > Bootup and Shutdown**.
3. Check-mark the service(s) to stop.
4. Click on the **Stop** button.

START SERVICES

1. Select **Application > Webmin**.
2. In the Webmin screen select **System > Bootup and Shutdown**.
3. Check-mark the service(s) to start.
4. Click on the **Start** button.

RESTART SERVICES

1. Select **Application > Webmin**.
2. In the Webmin screen select **System > Bootup and Shutdown**.
3. Check-mark the service(s) to restart.
4. Click on the **Restart** button.

REBOOT SYSTEM

1. Select **Application > Webmin**.
2. In the Webmin screen select **System > Bootup and Shutdown**.
3. Click on the **Reboot** button.

SHUTDOWN SYSTEM

1. Select **Application > Webmin**.
2. In the Webmin screen select **System > Bootup and Shutdown**.
3. Click on the **Shutdown System** button.

Important! Do not change the start **At boot** flag for any service.

Chapter 8 – Application Server Backup

BACULA

Note: This procedure will backup and restore the IPedge database only. For ACD backup and restore procedure refer to “[ACD BACKUP](#)” on [page 8 - 8](#).

The IPedge Application Server 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 Application Server configuration database for a stand alone system or every node on an enterprise network. The Bacula application directs all backup processes except Messaging. For the Messaging backup procedures refer to “[MESSAGING BACKUP](#)” on [page 11 - 6](#).

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 8-1 Bacula Main Page

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 Application Server backup schedule.

1. Navigate to the Bacula main screen (Application > Webmin, click on Backup and Restore).
2. Click on the Backup Schedules icon.
3. Click on the gemini backup schedule. Do not check mark the box. Click on the word 'gemini.'

TOSHIBA
Leading Innovation >>>

Login: Advanced

- System
- Servers
- Others
- Networking
- Hardware
- IPedge
 - Bacula Backup System
 - Log Collection

Search:

System Information
Logout

Module Index
Help..

Backup Schedules

Select all. | Invert selection. | Add a new backup schedule.

| Schedule name | Run levels and times |
|---|---|
| <input type="checkbox"/> gemini | Level=Full tue at 02:30 , Level=Incremental at 02:30 |
| <input type="checkbox"/> WeeklyCycle | Full 1st sun at 23:05 , Differential 2nd-5th sun at 23:05 , ... |
| <input type="checkbox"/> WeeklyCycleAfterBackup | Full sun-sat at 23:10 |

Select all. | Invert selection. | Add a new backup schedule.

Delete Selected Schedules

Return to module index

4. The Edit Backup Schedule screen will open.

TOSHIBA
Leading Innovation >>>

Login: Advanced

- System
- Servers
- Others
- Networking
- Hardware
- IPedge
 - Bacula Backup System
 - Log Collection

Search:

System Information
Logout

Module Index

Edit Backup Schedule

Backup schedule details

Backup schedule name: gemini

| Run levels and times | Backup level | Volume | Run at times |
|----------------------|--------------|-----------|------------------|
| | Full | <Default> | tue at 02:30 ... |
| | Incremental | <Default> | at 02:30 ... |
| | <Default> | <Default> | |
| | <Default> | <Default> | |
| | <Default> | <Default> | |

Save Delete

Return to list of schedules

5. Click on the ellipses (...) button at the end of the line you wish to change.

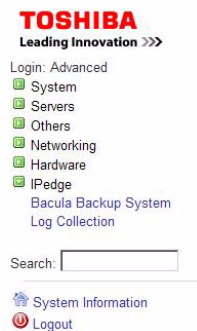
- The schedule detail window will open. The window below shows a schedule to run every month, on each Tuesday at 2:30 a.m.

- 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 Application Server backup schedule.

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



- Enter a name for the schedule.
- 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.
- 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 a smaller server database to a larger server, for example 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.

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 Application Server to restore.
8. Click on the **Restore** button.

Module Index Help.. **Restore**

Restore from Backup Restore from Files

Options for the Source

Restore from Job 35 - ALL-IPedge (2010-12-21 03:30:00) ▼

Restore from storage device File ▼

Options for the Target

Restore to server IPedge (on 159.119.127.154) ▼

Restore to local (IPedge) directory /tmp/bacula-restores

Restore Now

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

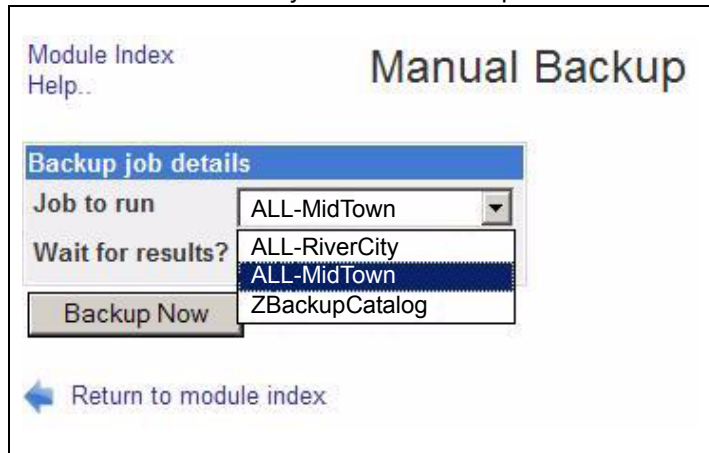
MANUAL BACKUP

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.

Manual Backup Procedure

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

1. Login to Enterprise Manager. Select **Application > Webmin**.
2. In the Webmin screen select **IPedge > Backup and Restore**. Click on the **Manual Backup** icon.
3. In the Job to run pull-down select; All-Server Name. Where ServerName is the server you wish to backup.



4. Ensure that **Wait for results** is set to **Yes**. Click on **Backup Now**.
5. 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 Application Server that can be downloaded to another location.

1. Login to Enterprise Manager. Select **Application > Webmin**.
2. In the Webmin screen select **IPedge > Backup and Restore**. Click on the **Restore** icon.
3. In the Restore from Backup tab, select the backup file to restore in the Restore from Job pull-down. The list always shows the latest file at the top of the list.
4. Click to select **Restore to local directory**.
5. 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.
6. Click on the **Restore Now** button.
7. Wait for the system to display "... backup complete."

Download Backup File

This process copies the backup file on the IPedge Application Server to any location the PC the administrator is using can access.

1. Login to Enterprise Manager. Select **Application > Webmin**.
2. In the Webmin screen select **Others**. Click on **Upload and Download**.
3. In the Download from Server tab click on the ellipsis next the **File download** field.
4. Select the folder name created above (format: **/NameOfFile**). Do not open the folder. Click on **Ok** then, click on the **Download** button.
5. The backup file will be copied to the Enterprise Manager PC. 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.

MANUAL RESTORE

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

Upload Backup File

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

1. Login to Enterprise Manager. Select **Application > Webmin**.
2. Select the sever to which the backup will be restored.
3. In the Webmin screen select **Others**. Click on **Upload and Download**.
4. In the Upload to Server tab click on the Browse... button next the **File to upload** field. Navigate to the backup file (name of file.ZIP).
5. Check-mark the **Create** box next to the File or directory to upload to.
6. Enter a folder name.
7. Ensure the following:
Owned by user = root
Owned by group = Default
Extract ZIP or TAR files? = No
Send email when uploads are done? = No
8. Click on **Upload**.
9. When the upload is complete highlight the file name (directory name\name of file.zip) and copy (keyboard command: Ctrl + C).

Restore the Server

This process restores the IPedge Application Server database.

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

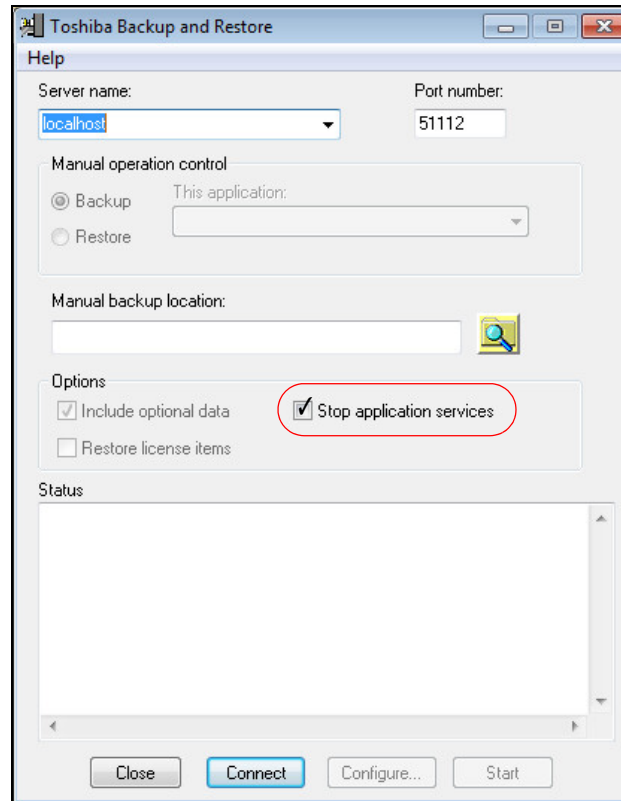
1. Login to Enterprise Manager. Select **Application > Webmin**.
2. In the Webmin screen select **IPedge > Backup and Restore**. Click on the **Restore** icon.
3. In the **Restore from Files** tab select the server to restore.
4. Paste the file name (directory name name of file.zip) into the Restore from remote directory, tar, or zip file box.
5. Click on **Restore Now**.
6. 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. 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.

Chapter 9 – HTTPS Configuration

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

- All of the servers in a network must be operating in HTTPS, otherwise some features will fail.
- The IPedge Application Server host names and server names must be configured and registered with a DNS server.

Important! When an IPedge Application Server with HTTPS set is installed behind a firewall ports 443 and 8443 must be open.

HTTPS CONFIGURATION

The IPedge Application Server can create a server SSL certificate.

Create New Certificate

The following steps create a new SSL certificate and change the system to https operation.

Note: The first time you create a certificate the system will create a Root certificate and a Server certificate. If a new certificate is created the system will create a new Server certificate. The root certificate will remain.

1. In Enterprise Manager select the server to configure. Select **Maintenance > HTTPS Configuration**.
2. In the HTTPS Configuration tab click to select **HTTPS On**.
3. Click on the **Create New Certificate** icon.
4. In the Create New Certificate dialog box enter all of the required information then, click on **OK**. Use descriptive names in the certificate fields.
5. Click on the Save icon.

Note: Changing the HTTPS configuration requires restarting the web server. Please wait several minutes for the web server to restart before logging back to the IPedge Application Server.

6. After the restart, login to the server using the same URL. The web server will automatically redirect to the HTTPS login.
For Example:
http://serverName:8080/oamp will be redirected to
https://serverName:8443/oamp, please observe the changes in bold

-
7. The server is using a self signed certificate, the browser will open a warning dialog box. Click on **Continue to this website (not recommended)** to proceed to the Enterprise Manager login screen.

Important! If the IPedge Application Server IP address is changed a new certificate must be created.

Root Certificate Download

To avoid this warning message the root certificate must be trusted. Download the root certificate onto your PC.

The following steps apply to Internet Explorer only.

1. In Enterprise Manager select the server to configure. Select **Maintenance > HTTPS Configuration**.
2. Select the Current Certificate to display the security certificate.
3. Select the **HTTPS Configuration** then, click on the Download Primary Server Root Certificate icon.
4. In the File Download dialog box click on Save. Save the file to your PC. When the download is complete close the dialog box.

Trust the Certificate

1. Using the browser menu, click on **Tools > Internet Options**.
2. In the **Content** tab click on the **Certificates** button.
3. In the certificates dialog, select the **Trusted Root Certification Authorities** tab.
4. Click on the **Import** button and follow the on screen prompts to import the primary server root certificate.
5. When completed close all browser windows.
6. Launch the browser, the IPedge Application Server certificate is now trusted on this PC. Login to Enterprise Manager as usual.

Note: The browser will be diverted to:
https://Server_address:8443/oamp

TURN HTTPS OFF

1. In Enterprise Manager select the server to configure. Select **Maintenance > HTTPS Configuration**.
2. Click on the **HTTPS Off** radio button.
3. Click on the Save icon.

Note: All servers in the network must be configured in the same manner. When HTTPS is turned off, remember to use the proper URL when accessing Enterprise Manager. The default is: <http://serverName:8080/oamp>.

Chapter 10 – Meeting

IPedge MEETING INITIAL CONFIGURATION

The Meeting server, installed on the IPedge Application platforms, requires a license to operate. Use this procedure to configure the Meeting server to run in your system environment.

Note: Steps 1 through 3 should have been done during the initial Application server setup as covered in Chapter 4 of this manual. If the IPedge server hostname is already assigned skip to Step 4.

Meeting IP Address and Hostname

1. Login in to Enterprise Manager, select **Applications > Webmin**. In **Webmin** select **Networking > Network Configuration** then, select **Hostname and DNS Client**.

Ensure that the **Search Listed** radio button is selected. Enter the Hostname - This is the host name you assigned to the IPedge Application Server System.

The screenshot shows the 'Hostname and DNS Client' configuration page in Webmin. The page has a sidebar on the left with the TOSHIBA logo and a navigation menu. The main content area is titled 'Hostname and DNS Client' and contains a 'DNS Client Options' form. The form has the following fields and values:

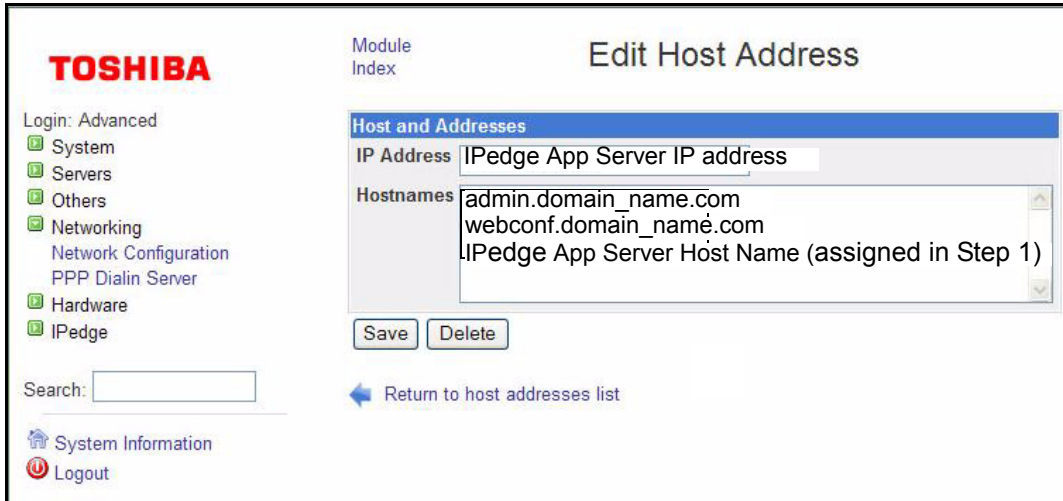
- Hostname: IPedge App Server Host Name
- Update hostname in host addresses if changed?:
- Resolution order: Hosts, DNS, [empty]
- DNS servers: 4.2.2.1, 4.2.2.2
- Search domains: None, Listed ..
- Search domains text box: IPedge App Serv domain_name.com

At the bottom of the form area, there is a 'Save' button and a 'Return to network configuration' link.

2. In the Search Domains box enter the Domain Name where the IPedge is located.
3. Click on the **Save** button.
4. Select **Networking > Network Configuration**. Click on **Host Addresses**.

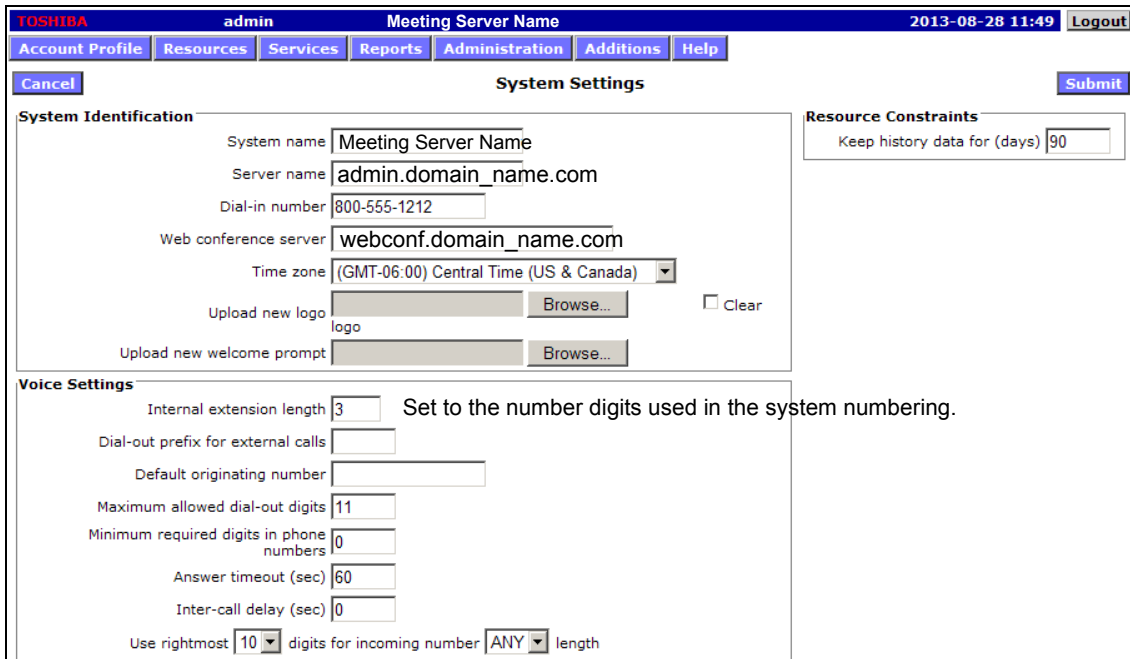
Note: IP Address 127.0.0.1 is the local host address for the IPedge Application Server. DO NOT edit this entry. If this entry is changed, edited or deleted the system may come inoperable and require the disk to be re-imaged.

- Click on the IP Address for the IPedge Application Server to edit the entries. Enter the hostnames for Meeting Admin, Webcon and, the IPedge. The entries will be in this format: admin.domainname.domaintype. For example: admin.yourcompanydomain.com



Note: The admin and webconf host addresses must be entered in the order shown. Any other host names or DNS entries must be entered below these. Click on the **Save** button.

- After the system restarts login to Enterprise Manager. Select **Application > Meeting**.
- Select **Administration > System Settings**. Ensure that the Server Name and Web Conference Web Server entries are the same as entered into the IPedge Hostname setup in [Step 4](#).



8. Click on the **Submit** button.
9. Under **Administration**, select **Circuit Groups**.

| TOSHIBA | | admin | | IPedge Conferencing Server | | 2013-08-28 13:51 | | Logout | |
|-----------------|-------------------------|---------------------|------------|----------------------------|--------------------------|------------------|--|----------------|--|
| Account Profile | | Resources | | Services | | Reports | | Administration | |
| Additions | | Help | | | | | | | |
| Add | | Circuit Groups | | | | | | Delete | |
| No. | Circuit Group | Address | Type | Options | Select | | | | |
| 1 | Strata CIX SIP Stations | MIPU CardIP Address | SIP Phones | N/A | <input type="checkbox"/> | | | | |

10. Click on the **Add** button to open the Add Circuit Group Page. To change circuit group; click on the group then click on **Edit**.
11. Enter the IP address of the MIPU card IP Address in the **Circuit Group Address** and **Realm fields**. Do not enter 127.0.0.1 or the words 'local host.'

Note: When configuring a CIX with the Application Server for Strata CIX, these values for Realm and Circuit Group Address will be the IP address of the CIX MIPU card on which the SIP stations are configured. If spanning more than one MIPU, assign additional Circuit Groups for each additional MIPU.

12. Enter the IPedge SIP station DNs to be used by the Meeting service. Assign the same number of stations as there are Meeting licenses assigned.
 The range of stations assigned as IN are used when meeting attendees call into a meeting.
 The OUT stations are used by moderators to dial out to invite and join a person into the current conference. If a moderator attempts to call out when there are no Out stations available or reserved, the system will use an idle IN station. Stations assigned as OUT stations can only be used for outgoing calls. Typically, the OUT stations do not need to be reserved unless there is a consistent need for moderator to dial out during a conference to invite participant.

| TOSHIBA | | admin | | Gemini Conferencing Server | | 2013-08-28 11:54 | | Logout | |
|------------------------|--|---|--|--|--|------------------|--|----------------|--|
| Account Profile | | Resources | | Services | | Reports | | Administration | |
| Additions | | Help | | | | | | | |
| Cancel | | Add Circuit Group | | | | | | Submit | |
| Circuit Group Settings | | | | | | | | | |
| Circuit Group Name | | Strata CIX SIP stations | | | | | | | |
| Circuit Group Type | | SIP Extensions | | | | | | | |
| Circuit Group Address | | (Meeting) MIPU card IP address | | Authentication Settings Realm: IP address of the (Meeting) MIPU card User Name: <input type="text"/> Password: <input type="password"/> | | | | | |
| Phone Numbers | | In: <input type="text"/> - <input type="text"/> | | Out: <input type="text"/> - <input type="text"/> | | | | | |

The stations are assigned in the Strata CIX system database as follows:

- Assigned station type is SIP
- DNs must be consecutive
- COS allows dialing out with a trunk access code or through LCR

- Stations are members of a distributed hunt group. The Meeting dial-in DID number routes to the Pilot DN of this hunt group.

13. Reboot the IPedge Application Server.
14. Ensure that the domain name of your system is registered with the Domain Service company.
15. Ensure that the following ports are open in the firewall the IPedge server is operating behind.

| Service Groups | | | | Items 1 |
|--|--------------------|----------|------------|----------|
| View Style: <input checked="" type="radio"/> All Services <input type="radio"/> Custom Services <input type="radio"/> Default Services | | | | |
| <input type="checkbox"/> # | Name | Protocol | Port Start | Port End |
| <input type="checkbox"/> | 18 IPedge Services | | | |
| <input type="checkbox"/> | ▶ HTTP | TCP | 80 | 80 |
| <input type="checkbox"/> | ▶ HTTPS | TCP | 443 | 443 |
| <input type="checkbox"/> | ▶ IPedge MMC 1935 | TCP | 1935 | 1935 |
| <input type="checkbox"/> | ▶ IPedge MMC 1945 | TCP | 1945 | 1945 |
| <input type="checkbox"/> | ▶ IPedge MMC 8444 | TCP | 8444 | 8444 |
| <input type="checkbox"/> | ▶ IPedge Web 8080 | TCP | 8080 | 8080 |

End of Meeting Application Installation Procedure

ASSIGN MODERATORS

Moderators are system users that can setup meetings.

1. Login to Enterprise Manager.
2. Select **Application > Meeting**. Select the server with the Meeting Application you are going to set up. Click on **OK**.
3. In the Meeting administration screen select **Resources > Accounts** from the Menu.
4. In the Accounts screen click on **Add**.
5. Enter the information about the Moderator.

Notes:

- Enter a **First Name** and **Last Name**. This will be used by the meeting application.
- Enter the Moderator's DN (extension number) as the **Primary Phone** and the **Login**.
- Check-mark the **Service Privileges** and **Service Defaults**.

6. Click on **Submit**.
7. Repeat steps 4 ~ 7 for each Moderator.

Setup a Meeting

To setup a meeting the moderator must login to the Enterprise Manager Personal Administration.

Email Summary Settings

To setup summary emails:

1. Select **Administration > Service Settings**.
2. In the Basic Settings area check-mark **Send summary emails to moderators**.
3. Click on **Submit**.
4. Select **Resources > Accounts**.
5. For each Moderator, in the Email Settings check-mark the **Send email summary reports** box.

Note: The Email Settings will not be visible unless the Service Settings have been setup (Steps 1 ~ 3).

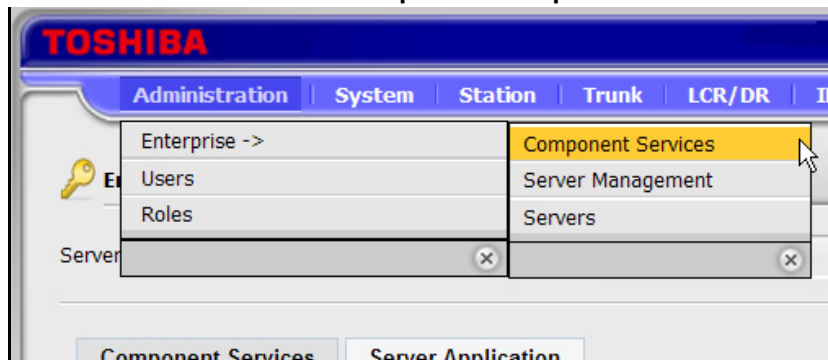
This page is intentionally left blank.

Chapter 11 – Net Server

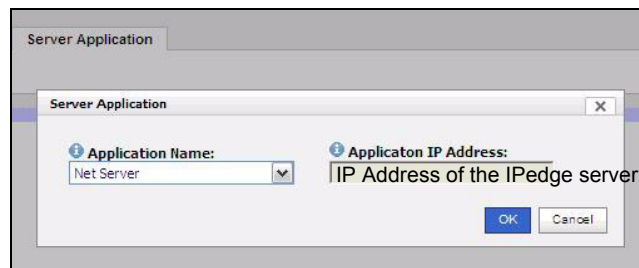
Net Server is pre-installed on the IPedge Application Server and can be activated using Enterprise Manager. Add Net Server to Enterprise Manager and configure the IO port in the IPedge Application Server. After applying the license, Net Server is ready to be used. If further configuration of Net Server is necessary for server based Call Manager configuration, please see Net Server administration section [page 11-2](#) 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**.

SETUP THE CIX SYSTEM I/O PORT

1. Using Network eManager, go to **System > I/O Device**.
2. In the (00) **Logical Device Number** field select **200 CTI #0 ~ 8** (select an unused value 0 to 8).
3. In the (01) **Device Connection** field select **LAN** from the dropdown
4. Choose an unused **Port Index Number** (recommend 10).
5. CTI#0 ~ 8 for the Logical Device No.
6. Click the **Submit** button.
7. Select the **LAN Device** tab.
8. Set (02) **Application Type** to Server.
9. In the (05) **Client IP** field enter the IP address of the IPedge Application Server.
10. Set the (06) **Client Port No.** to 1100.

Important! Do not configure any other application, including the Attendant Console, to use Port 1100.

11. Leave all other settings at their default values.
12. Click on the **Submit** button.

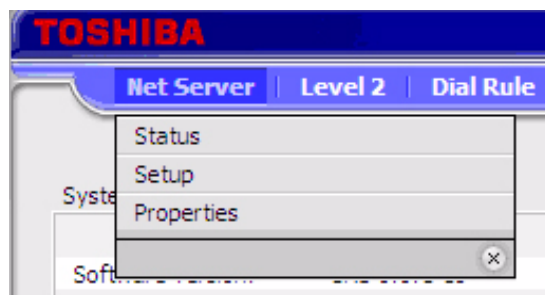
NET SERVER LEVEL 2 CONFIGURATION

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.

Using Enterprise Manager, select **Application > Net Server** menu. Select **Level 2 > Switch Settings**, enter the IP address of the Strata CIX **processor** into the Hostname field.

NET SERVER MENU

Net Server menu provides access to the basic setup for Net Server application on IPedge Application Server.

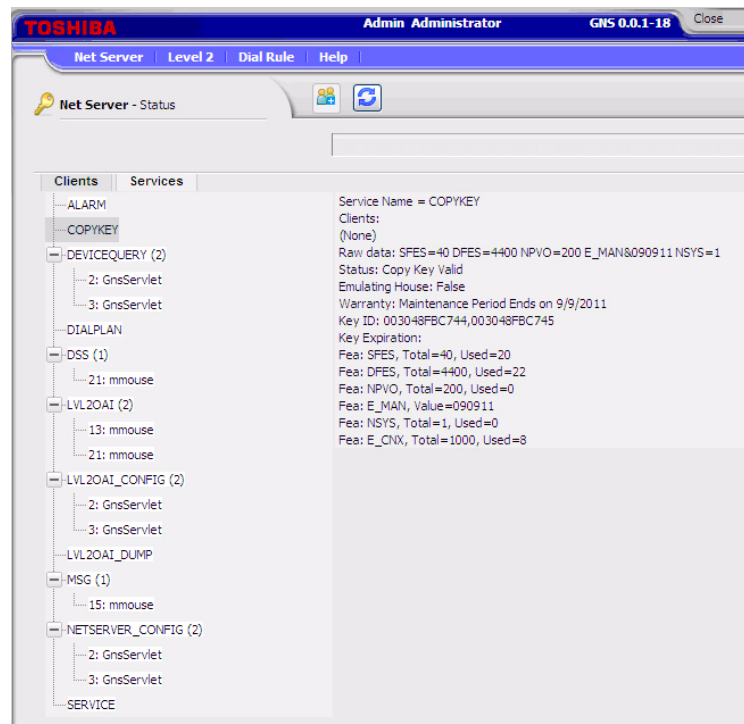


Status The Status sub menu provides real time information on the Net Server.

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.

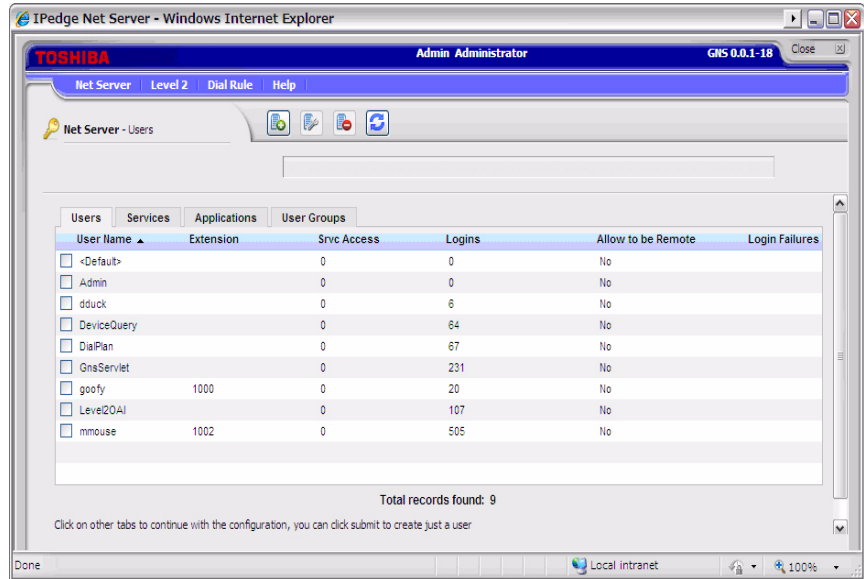


Services Tab Services tab shows the real time status of system component services running.

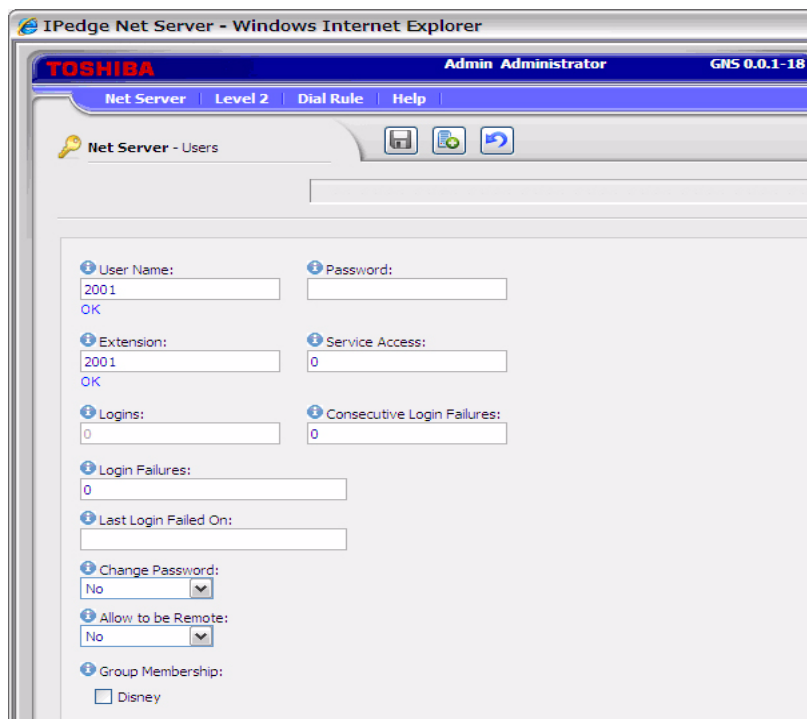


Setup Setup sub menu allows the administrator to manage client users, service components, applications, and groups.

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.



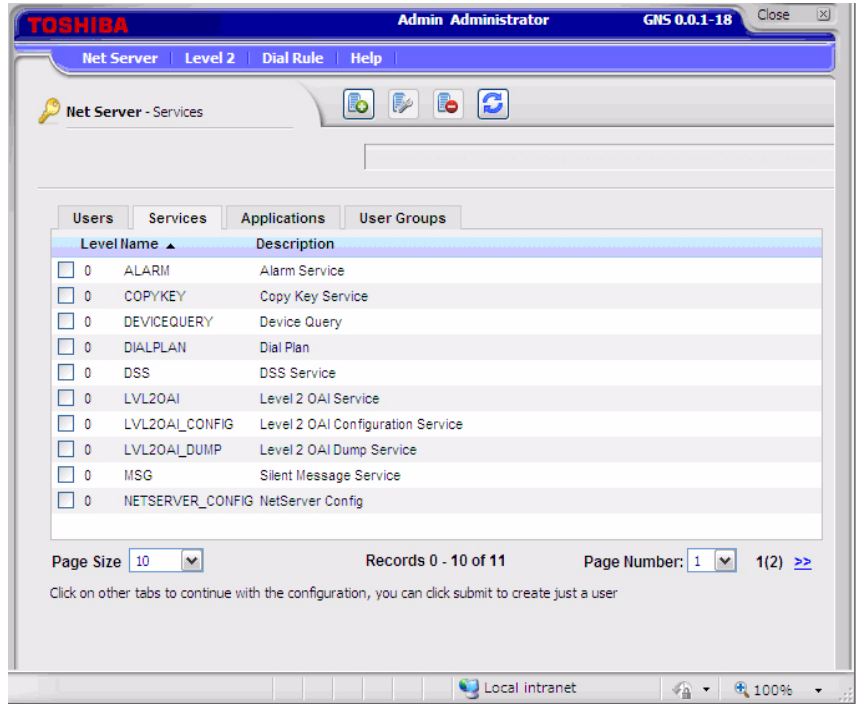
When you Add or Edit a checked entry, data can be entered from the following screen.



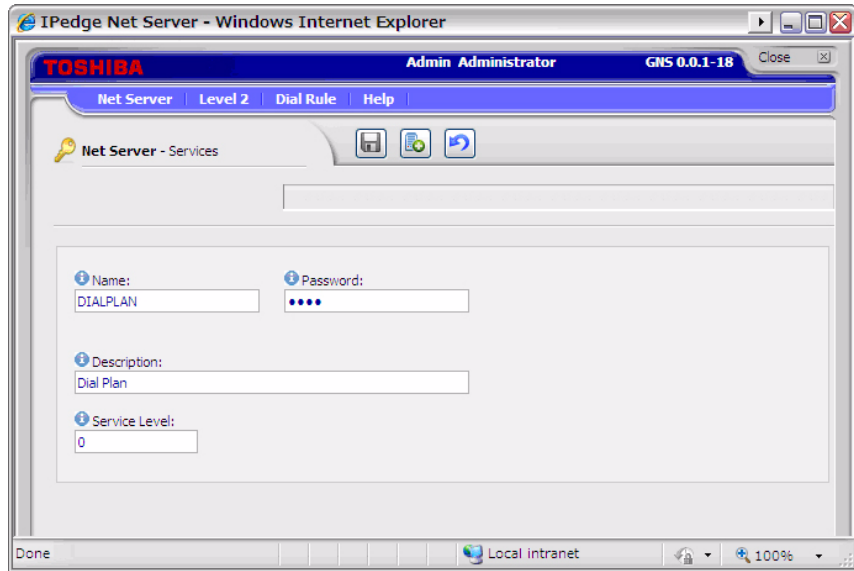
| Name | Description |
|----------------------------|---|
| User Name | Name of the user to use for Net Server login |
| Password | Password used for Net Server login |
| Extension | Directory Number (DN) of extension that the user controls |
| Service Access | This is a number that determines which 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.



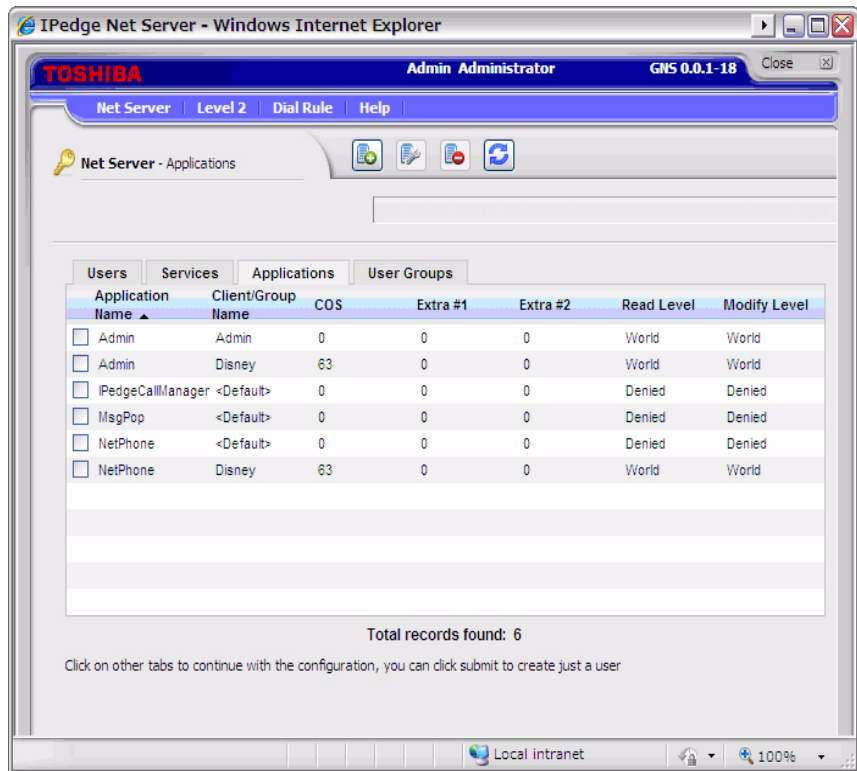
When you Add or Edit a checked entry, data can be entered from the following screen.



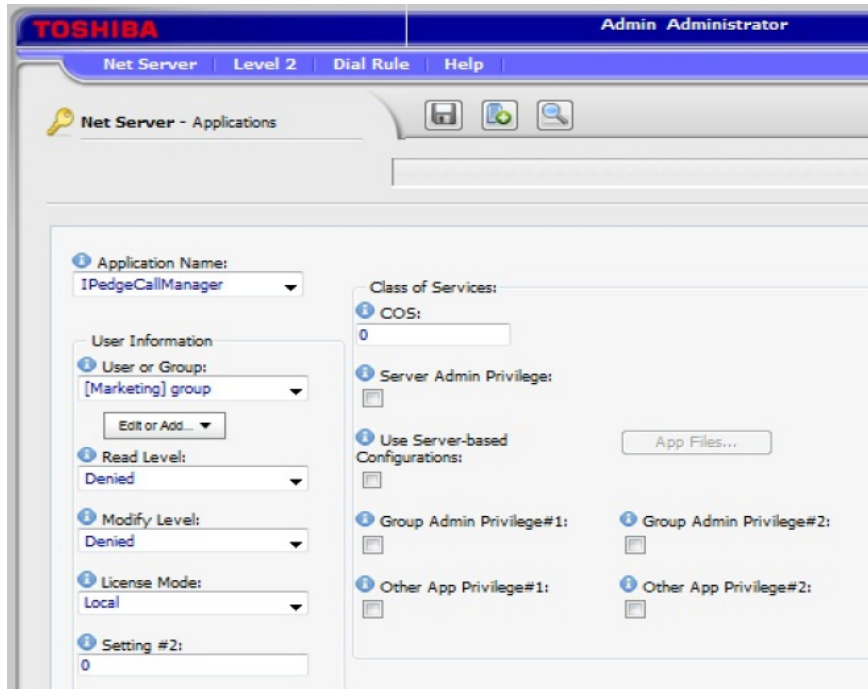
| Field | Description |
|---------------|---|
| Name | Service name which must be unique in the system |
| Password | Password for the service to login to Net Server. Typically, it should not be changed. |
| Description | Description of the service |
| Service Level | Service Level determines which clients 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 11-19](#) 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.



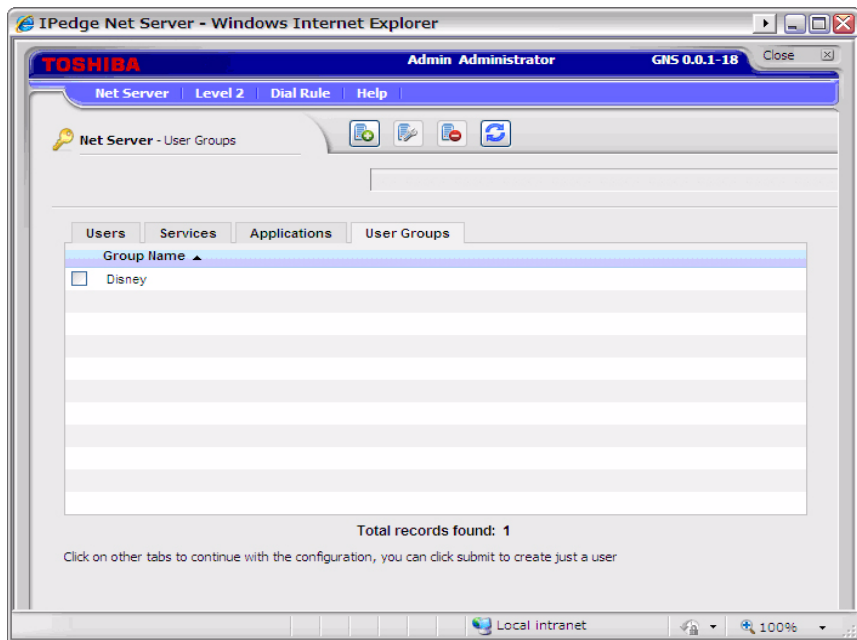
| Field | Description |
|------------------|---|
| Application Name | Name of the application |
| User or Group | Usually, the client name of the user is shown (see Clients). When it is set to <Default> (or leaving it blank) the settings for the Default User can be defined. It can be used to define the 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. |

(Sheet 1 of 2)

| Field | Description |
|--------------------------------|--|
| Server Admin Privilege | Enables the user to do administration of server configuration files. (value: 1) |
| 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) |

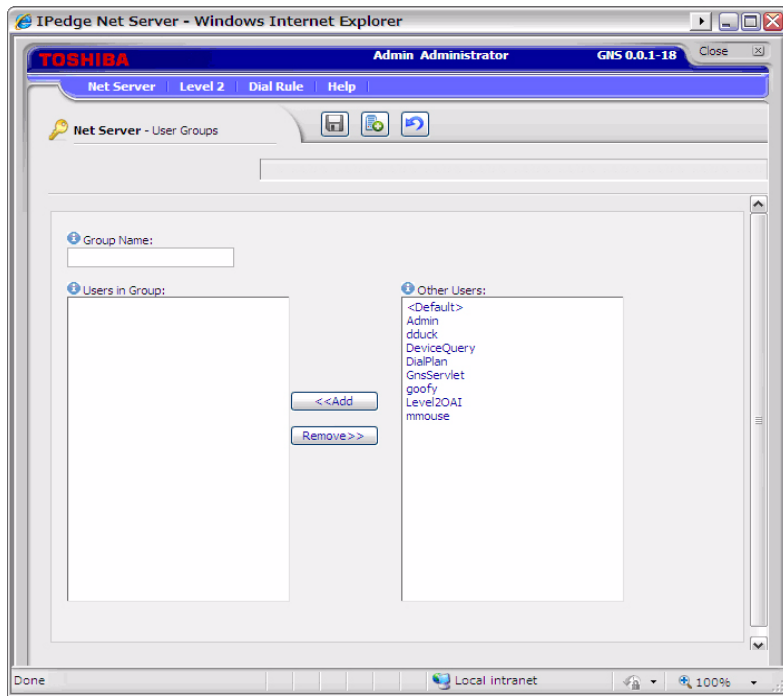
(Sheet 2 of 2)

User Groups Tab User Groups tab defines the group of users to apply the common settings to multiple users.



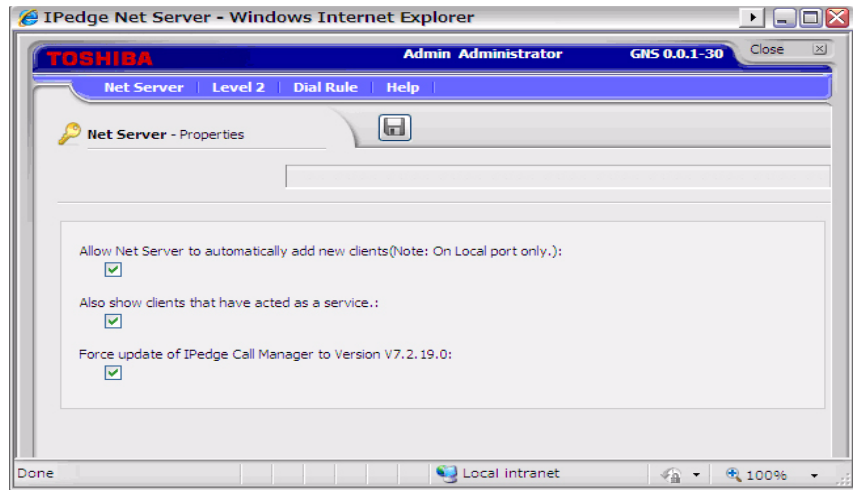
When you Add or Edit a checked entry, data can be entered from the following screen.

For an example refer to [“Create User Groups”](#) on page Chapter 11 –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) | <p>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.</p> <p>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".</p> |
| Also show clients that have acted as a service | <p>Control whether to show a component that is acting as a server in the client list.</p> <p>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.</p> |
| Force update of IPedge Application Server Call Manager to Version Vx.x.x.x | <p>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.</p> |

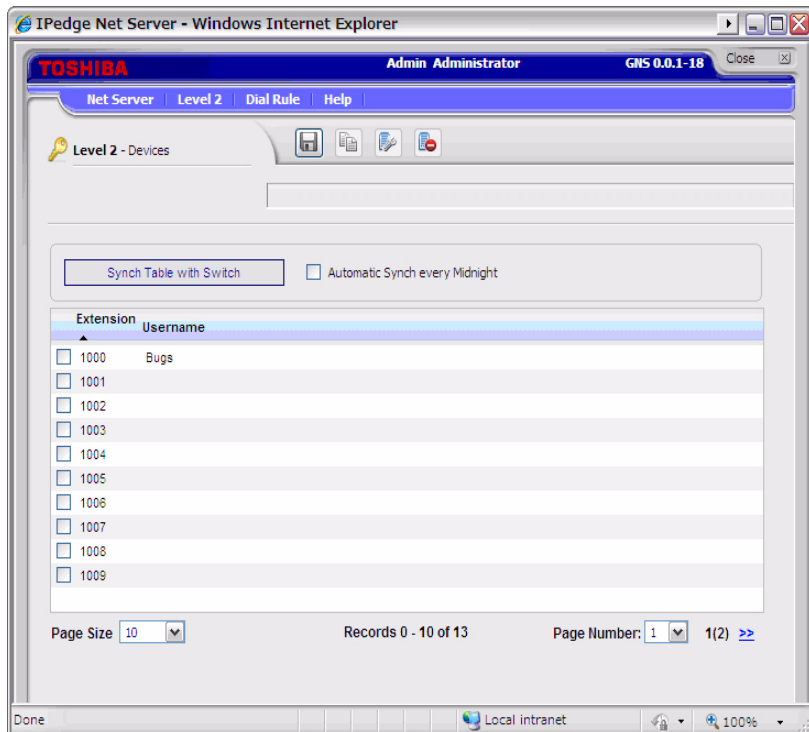
LEVEL 2 MENU

Level2 menu allows the administrator to configure various items managed by Level2 which processes the Computer Telephony Integration with the IPedge Application Server.



Devices Menu

Device menu manages the device table which provides an Extension Directory for Call Manager.



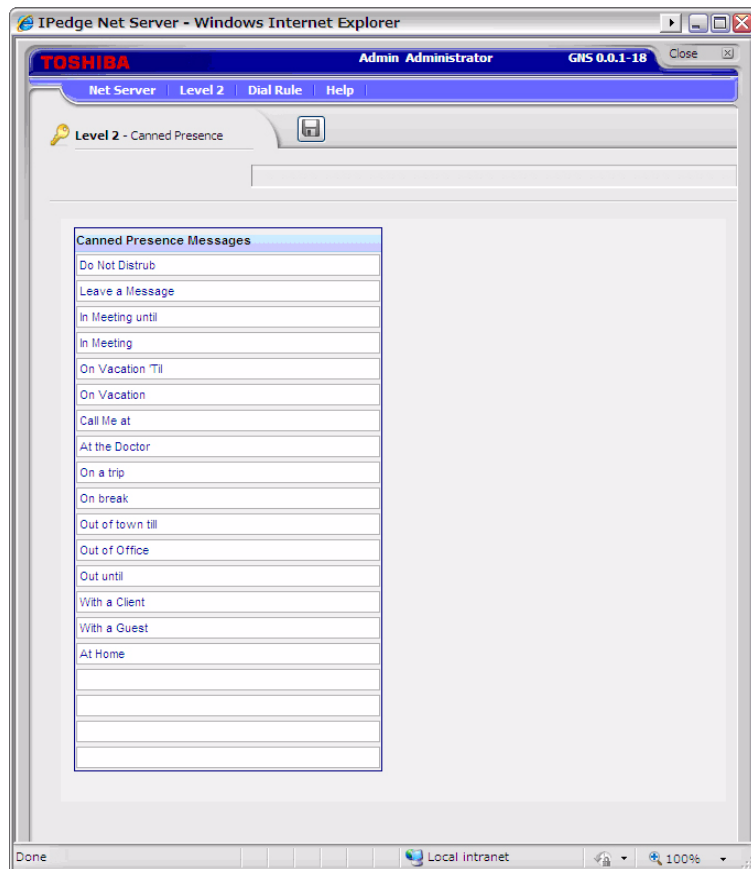
Device Table

Device table can be created manually by creating or copying an entry, or it can be automatically populated by using Synch Table with Switch.

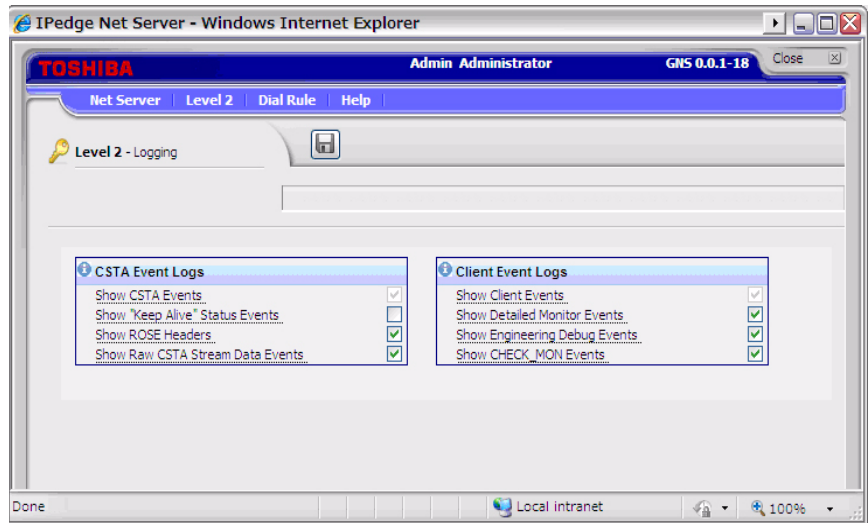
It is also possible to automatically update every midnight by checking Automatic Synch Every Midnight check box.

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.



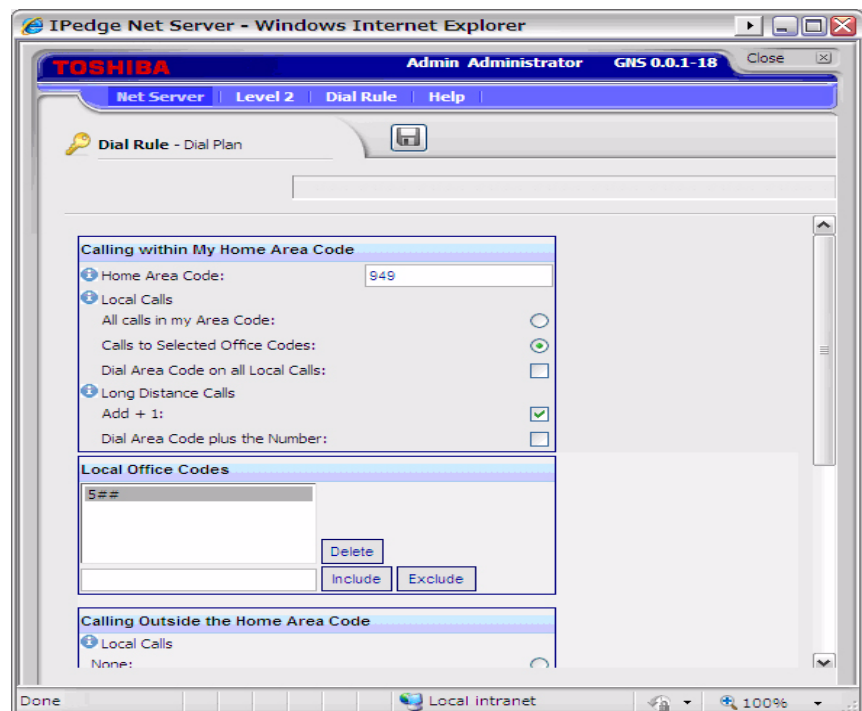
Each area of the US uses a different set of rules for determining which calls are local or long distance calls. The opening pages of your phone book are a good source for how to dial different numbers in your area. Your System Administrator will also need to define access codes for reaching outside lines. 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

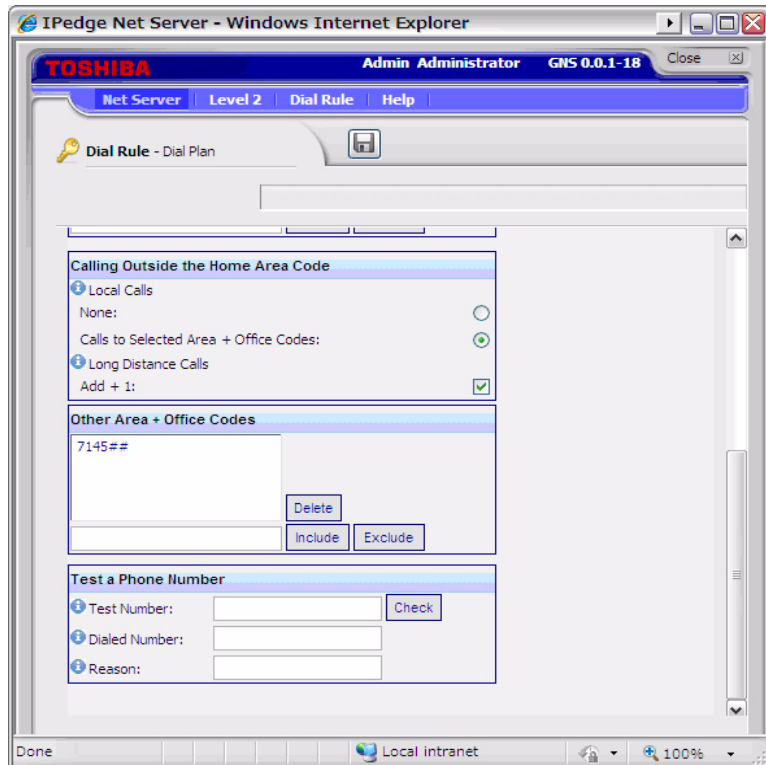
- Home Area Code – Set this to the Area code where the phone is located. This will be used by Call Manager to determine which dialed calls are within your home area code and when searching a contact manager (reverse screen-pop) the dialed number will need the area code included, i.e. Microsoft Outlook.
- 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.

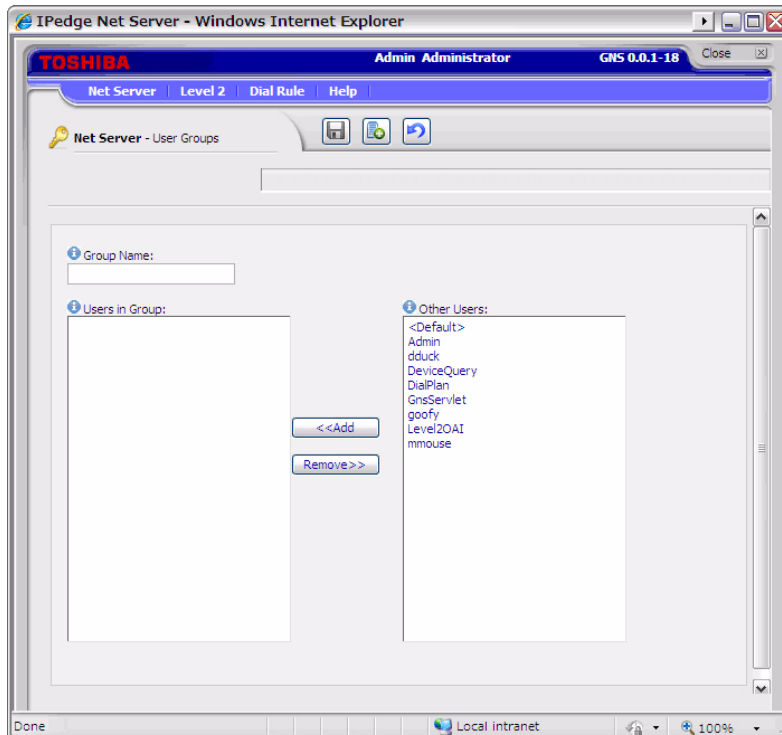
Server Based Call Manager Configuration

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.

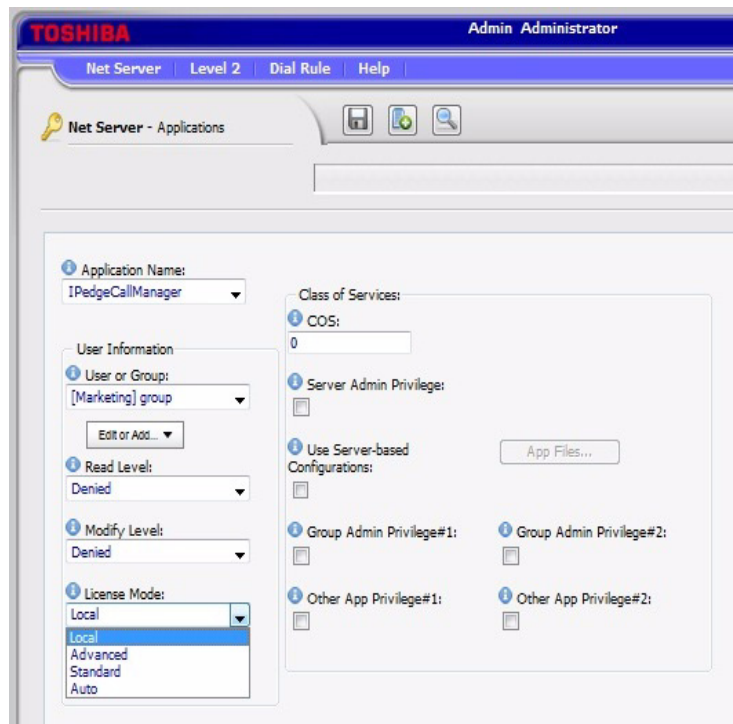


4. Click Add button again, and this time, type in a name to represent the Call Manager Users' group (Call Manager User in this example).
5. Repeat above steps for other groups if necessary.

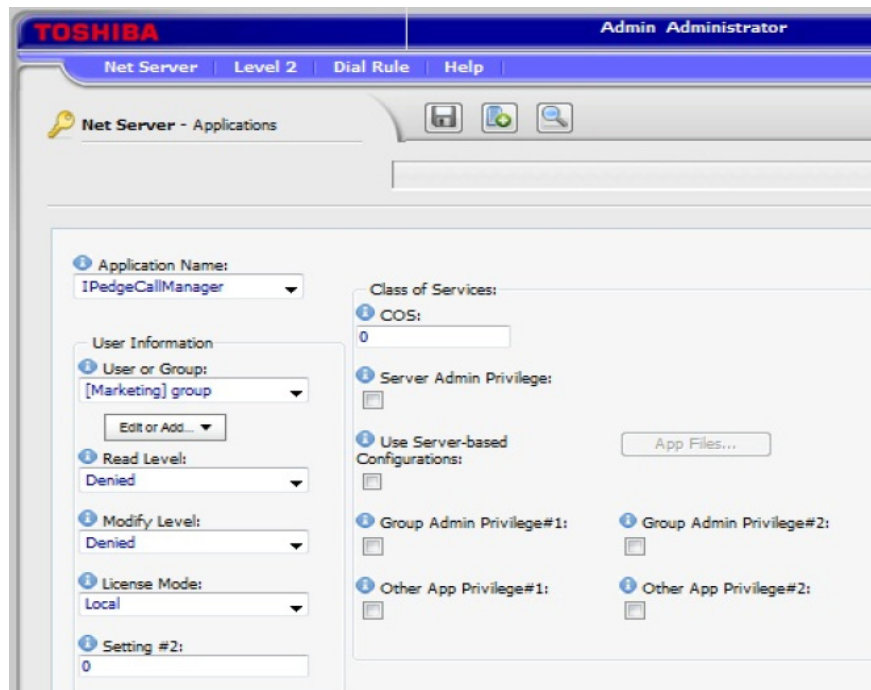
Assign Users to Call Manager Application

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.

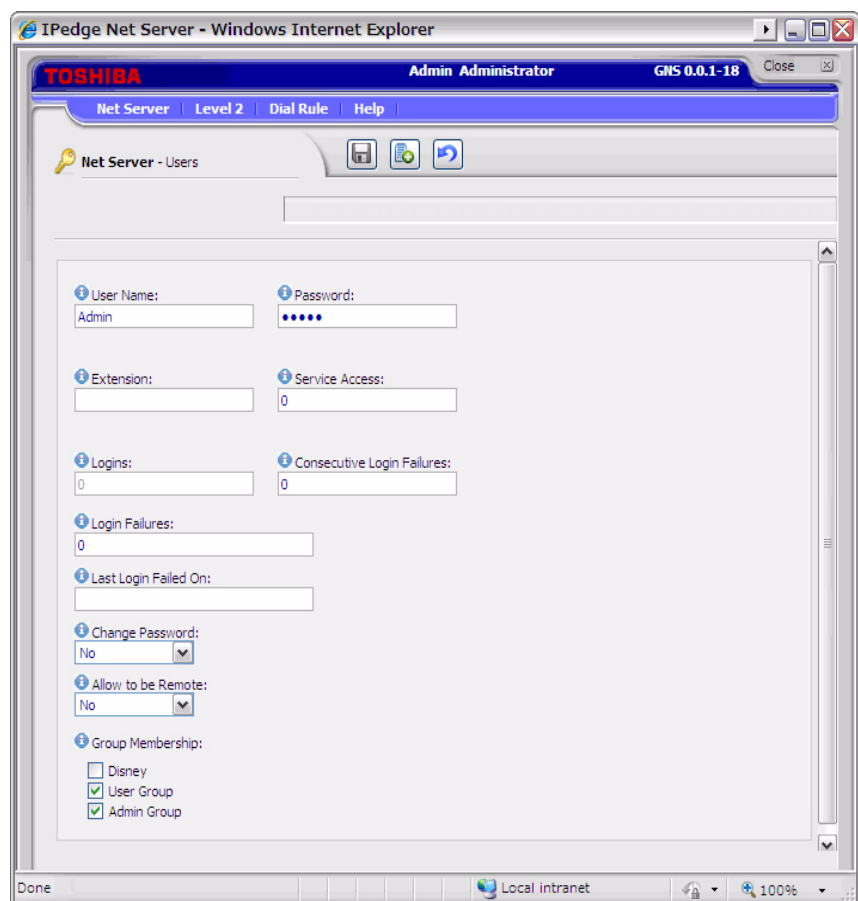


16. Repeat the preceding steps to add any remaining Call Manager user groups.
17. Default in User or Group can be used to setup the default settings for all users that are not included in any group or individual.
18. To exclude certain users from the Default, choose an individual user.

Assign Users to User Groups

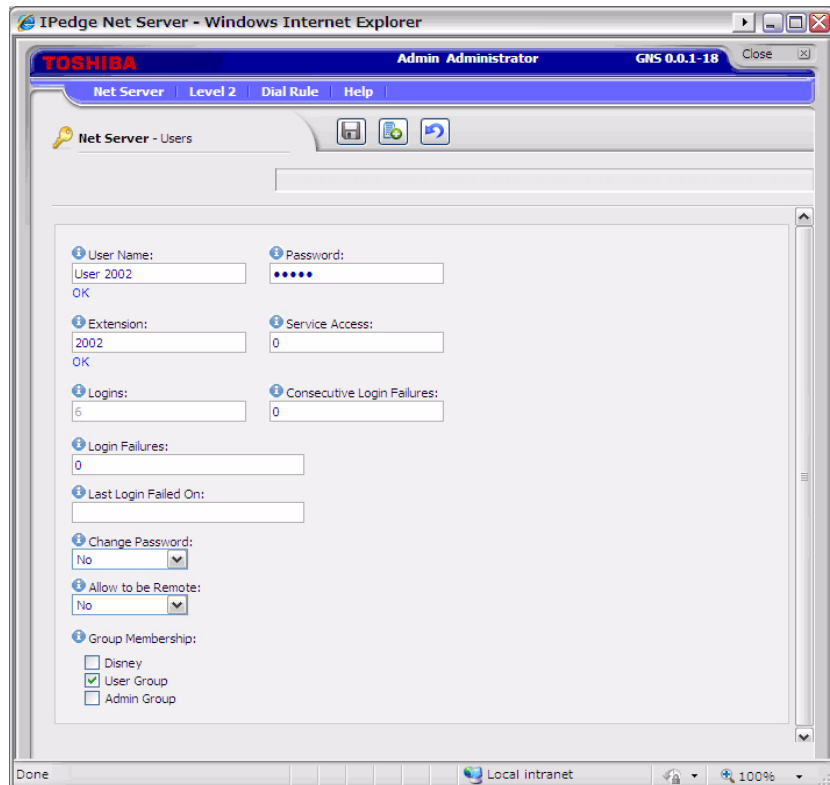
To Assign Users as Call Manager Administrators

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.

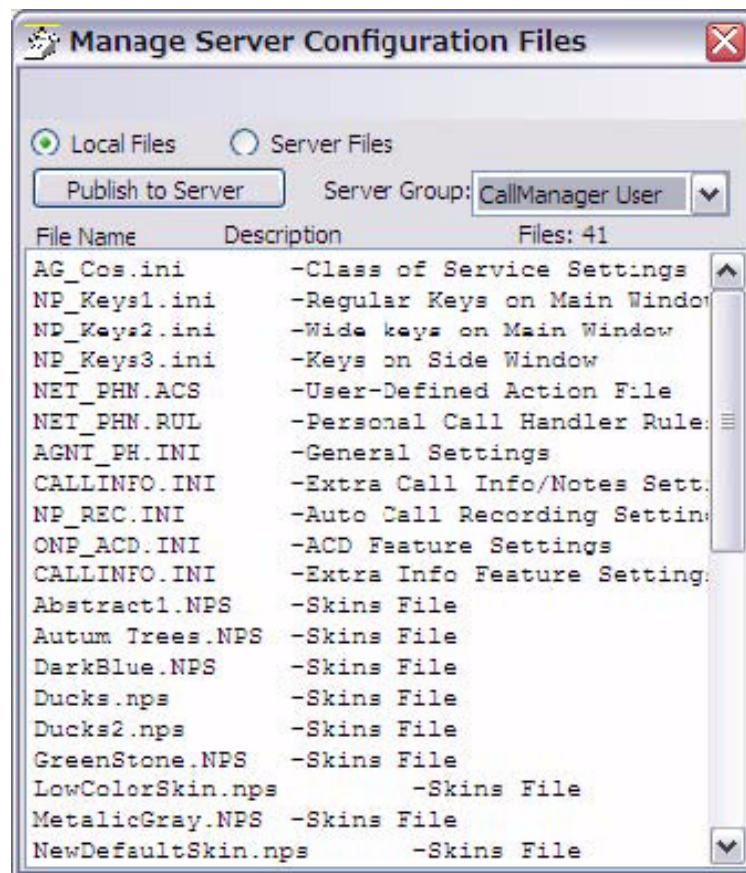


Create Configuration Files
using Admin Call Manager

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.



```
AG_COS.INI - Notepad
File Edit Format View Help
[[cos]
Chg_Actions=Y
Chg_Rules=Y
Chg_StdKeys=Y
Chg_PgmKeys=Y
Chg_BotKeys=Y
Chg_MainSet=Y
Chg_OutLookSet=Y
Chg_Tnf0Set=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

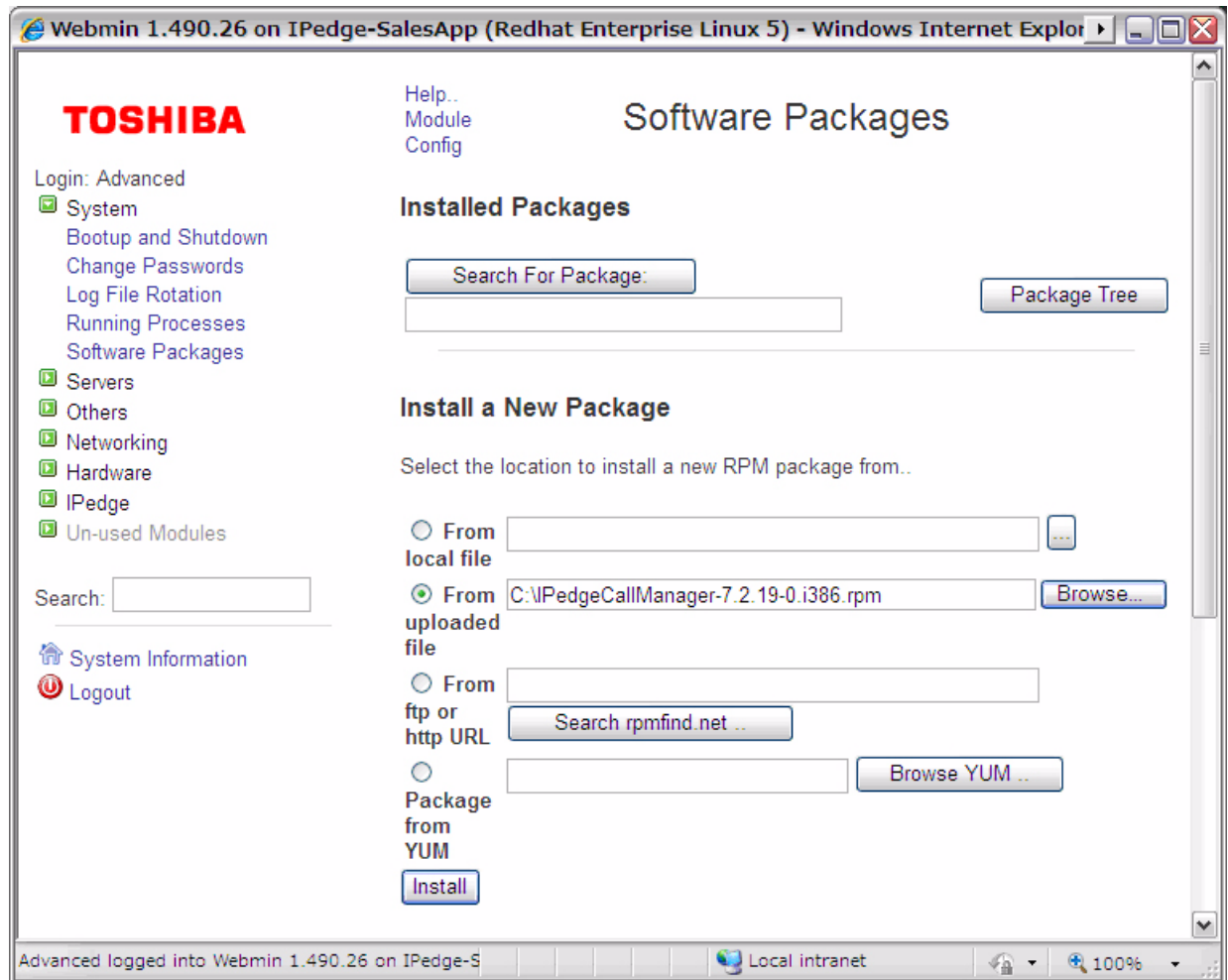
When the new Call Manager is released, it is possible to install the upgrade on the server so that it can be downloaded to the client. If the server based upgrade is configured, the Call Manager user will be prompted to upgrade the software when the Call Manager is launched.

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.

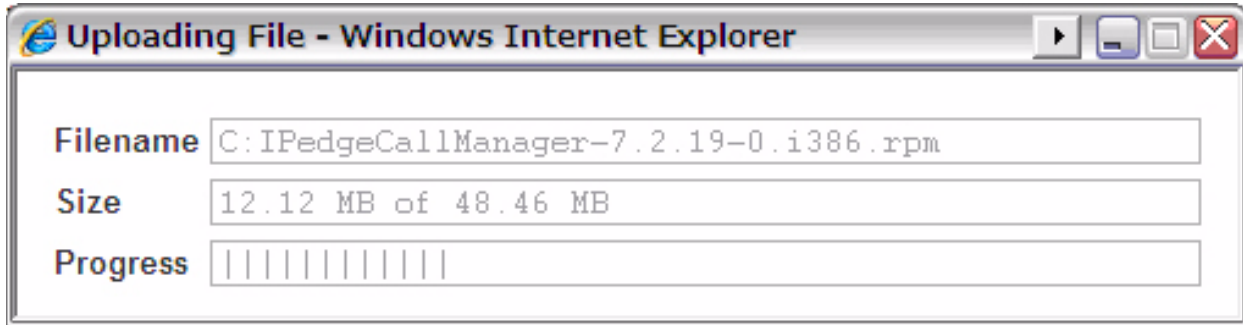
Installation

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 Application Server through Webmin from Enterprise Manager.

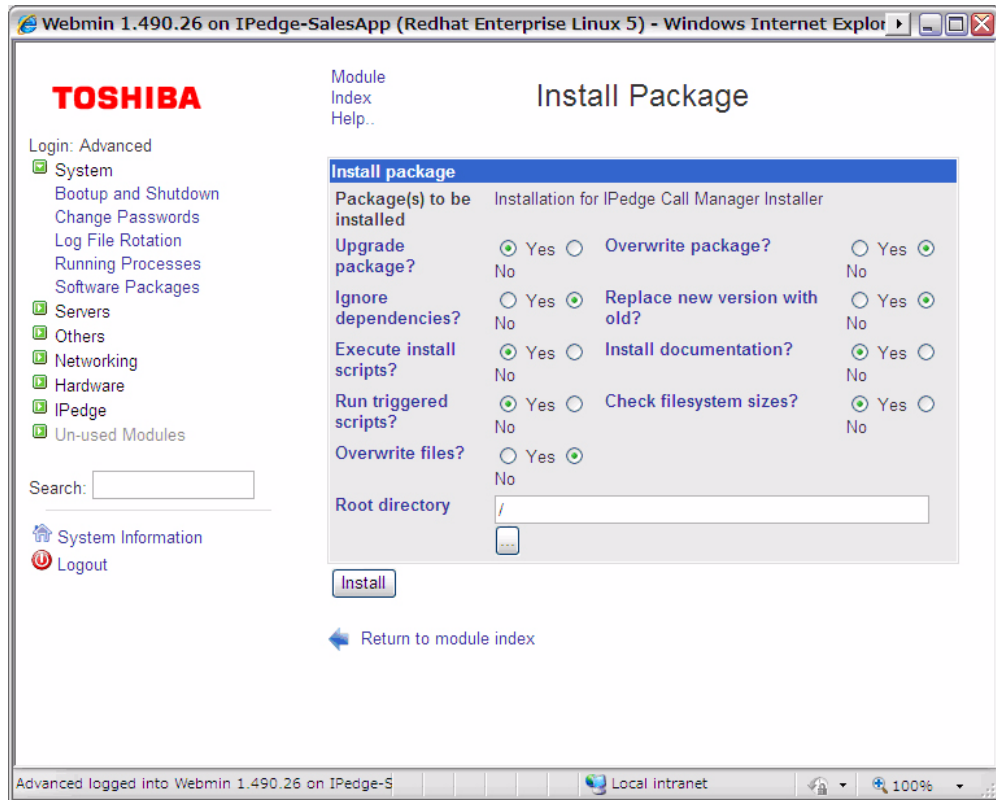
From the PC, launch Enterprise Manager and run Webmin. In the Webmin, select Software Packages menu under System menu. Then, select From uploaded file, and click Browse to specify the Call Manager upgrade software file. Then click Install.



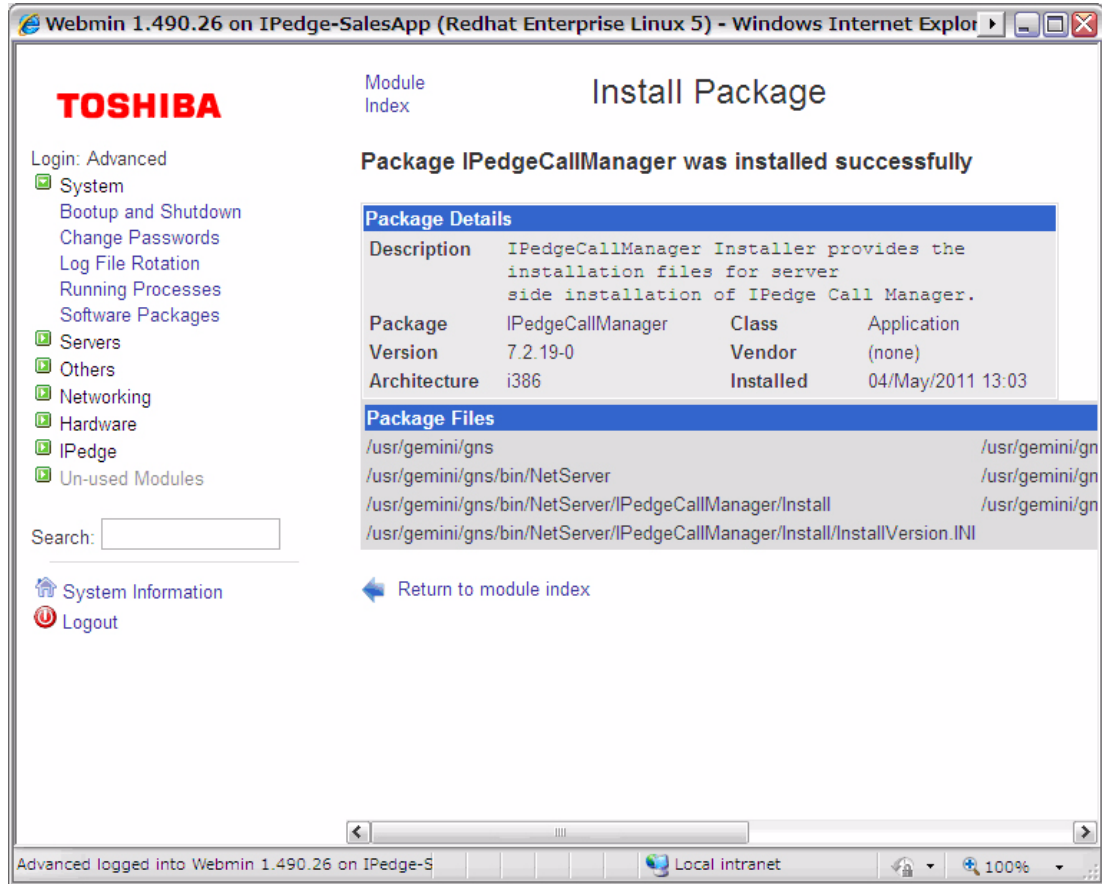
After clicking install, the following progress bar is shown to indicate the progress of the file upload to the server.



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.

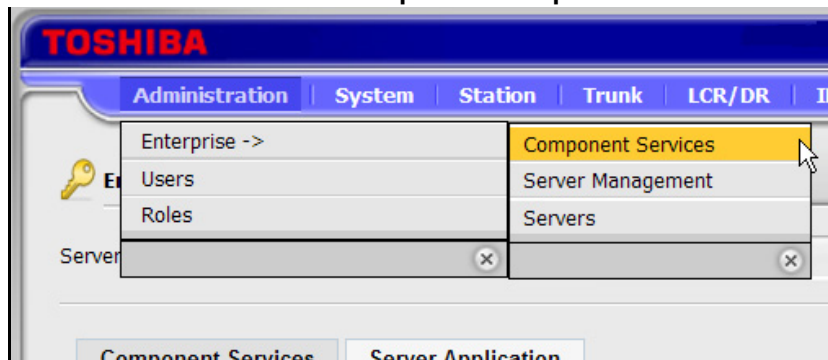
In the Net Server admin screen, select Properties menu from Net Server tab. Then, check “Force update of IPedge Call Manager to version V (displayed version)” and click Save to enable the Server Based Call Manager upgrade. To disable the Server Based Call Manager upgrade, deselect it and click Save. Note that the version number is the actual Call Manager version installed on the IPedge Application Server.

Chapter 12 – Messaging

Messaging is pre installed on the IPedge Application Server and can be activated using 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 the **New** icon.
6. Select Voice Mail from the list.



7. Add the IP Address of the IPedge server, do not enter 127.0.0.1 as the address.
8. Click on **OK**.

SETUP THE I/O PORTS

1. Launch Network e Manager and connect to the Strata CIX system.
2. From the System menu, select **I/O Device**.
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. Enter the IP address of the IPedge Application server into the Client IP address field.
7. Client Port No. is 1000.
8. Click the **Submit** icon.

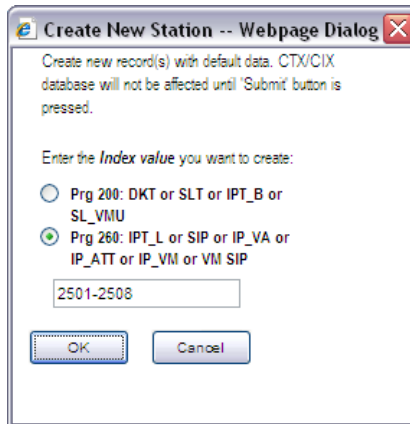
IO Logical DeviceLAN DeviceRS232 Serial Port

801 CIX/CTX NETWORK JACK LAN DEVICE ASSIGNMENTS

| | | | |
|----------------------------------|--|-------------------------------------|-------------------------------------|
| 00 LAN Port Index No. | <input type="text" value="2"/> | <input type="button" value="List"/> | |
| 01 Protocol | <input type="text" value="TCP"/> | 02 Application Type | <input type="text" value="Client"/> |
| 03 Data Flow | <input type="text" value="Asynchronization"/> | 04 Server Port No. | <input type="text" value="0"/> |
| 05 Client IP | <input type="text" value="IP Address of the IPedge Application Server"/> | | |
| 06 Client Port No. | <input type="text" value="1000"/> | | |
| 07 Read Retry No. | <input type="text" value="1"/> | 08 Write Retry No. | <input type="text" value="1"/> |
| 09 CallerName Set To CSTA | <input type="text" value="No"/> | | |

ASSIGN THE VOICEMAIL SIP STATIONS

1. Using Network eManager, select Station > Assignments
2. Click Create. Select Prg 260: IPT_L or SIP or IP_VA or IP_ATT or IP_VM and enter the range of the VM stations. Click on **OK**.



3. Setup the following:
 - A. Change program 260-01 **Type** to SIP VM
 - B. Enter the _IPU equipment number in to **02 PDN Equipment Number**
 - C. Select the Interface Number in **03 LAN Interface Number** to 1 (MIPU = 1)
 - D. Enter the Voice Mail Pilot DN in **15 Display DN**.

ADD STATIONS TO A STATION/HUNT GROUP

1. Using Network eManager, add the voicemail ports to the Hunt Groups by going to **Station > Station Groups**.

2. Click on the **New** icon. Make the following selections:
 - A. **Hunt Method** is Distributed.

-
- B. **Pilot Number** should be the one used in the Numbering scheme
Example: When the Message button is pressed, it dials 3090.
 - C. **Multiple DN Hunt** is set to Disable
 - D. Auto Campon is an option.
3. Click on the **Submit** 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 **Submit** icon.

System 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 (optional).

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 **Submit** icon.

Stations

1. Select **Station > Station Assignment**, then select one of the DNs.
 - A. Enter the VMID (voice mail box number) for this DN in **19 VMID** field
 - B. In the **20 MW to VM Port** field enter the VM Pilot DN..
2. Set up all of the stations.

PROGRAM MESSAGING

The Messaging setup should have been completed during the initial setup in Chapter 5. If this has not been completed refer to [“CONFIGURE IPedge MESSAGING”](#) on [page 5-10](#).

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 |
|-------------------------------------|--------------------------|-------------------------|
| Administration | | |
| <input checked="" type="checkbox"/> | Mail Server | 192.168.254.1 |
| <input checked="" type="checkbox"/> | SysAdmin1 | admin@xyzco.company.com |
| <input type="checkbox"/> | SysAdmin2 | |
| Channel Alerts | | |
| <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 | |
| Maximum Disk Usage Alert | | |
| <input checked="" type="checkbox"/> | HD Used | 80 |
| <input checked="" type="checkbox"/> | HD Used Repetitions | 5 |
| Database Errors | | |
| <input checked="" type="checkbox"/> | Database Error Message | %s |

2. Under Administration, enter the name 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

Messaging backup is to separate files using procedures separate from the IPedge Application Server 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 Application Server hard disk drive. These backup files can be automatically forwarded to a FTP server.

Backups can also be manually created on demand.

MANUAL BACKUP

Use this procedure to configure the backup utility for Messaging.

1. Login to Enterprise Manager then, select **Application > Messaging**. Select the server.
2. In the Messaging monitor select **Utilities > Recovery**.

The screenshot displays the 'Utilities - Recovery' configuration page. At the top, there are navigation tabs: Mailboxes, Department, COS, Site Parameters, System, and Utilities. The main content area is titled 'Utilities - Recovery' and contains two primary sections: 'Backup' and 'Restore'.
Backup Section:
- **Backup Directory:** A text input field contains '/usr/Sm/backup', followed by a 'Save' button.
- Two buttons are present: 'Backup to Directory' and 'Retrieve Backup to Local PC'.
Define FTP Backup Section:
- Fields for 'FTP Name or IP:', 'Username:', 'Password:', and 'Path:' are provided, each with an adjacent empty input box.
- Below these fields are buttons for 'Test FTP Location' and 'Save'.
Restore Section:
- **Last Backup available:** Displays the timestamp 'Fri Oct 14 03:01:51 PDT 2011'.
- Two buttons, 'Restore From Directory' and 'Restore From FTP', each have a 'Restore Key' checkbox next to them.
- A sub-section titled 'Restore From Directory' includes a 'Browse...' button and an 'Upload File and Restore' button with a 'Restore Key' checkbox.

-
3. 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 first backup the data to the local folder and then upload the backup to the FTP server. At the end of the process a message will be displayed. 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, t3.tgz and t4.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 **Site Parameters > Settings**.
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 sections of a settings page. The top section is titled "House Keeping" and 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" to its right, and "Script" with the text "house1_script". The bottom section is titled "Run Backup" and also has a blue information 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 input field.

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 3:00am.

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 "vmbbackup_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.

This page is intentionally left blank.

Chapter 13 – Fax

The Messaging fax module consists of the following three components:

- Fax mail system – Fax mail allows users to receive faxes in their voice mailbox and view them via unified text messaging (e.g., an email attachment) or use the telephone interface to re-route the incoming fax to a physical fax machine. The latter is particularly useful from a remote location like a hotel since the user can access their voicemail remotely.
- Fax-on-demand – This component allows incoming callers to access a library of documents and select a specific fax document to be faxed to them.
- Fax print server – This component provides the ability to send faxes from your desktop through a central system. This option is particularly beneficial to multiple users in a server environment instead of sending the fax via fax modem.

FAX MAIL SYSTEM

Messaging SIP supports fax using T.38 protocol. The gateway or SIP trunk provider to which the Strata CIX system is connected must support the T.38 protocol. To enable fax on the IPedge Application Server for CIX, an AudioCodes FXO gateway is required.

FAX FEATURE DESCRIPTION

Messaging's fax solution requires:

- One or more AudioCodes analog to IP gateways to interface between the IPedge Application Server IP connection and Strata CIX analog ports
- Unified Messaging license for each user that wishes to send or receive a fax on their desktop

Once configured, Messaging fax offers the following features and functions.

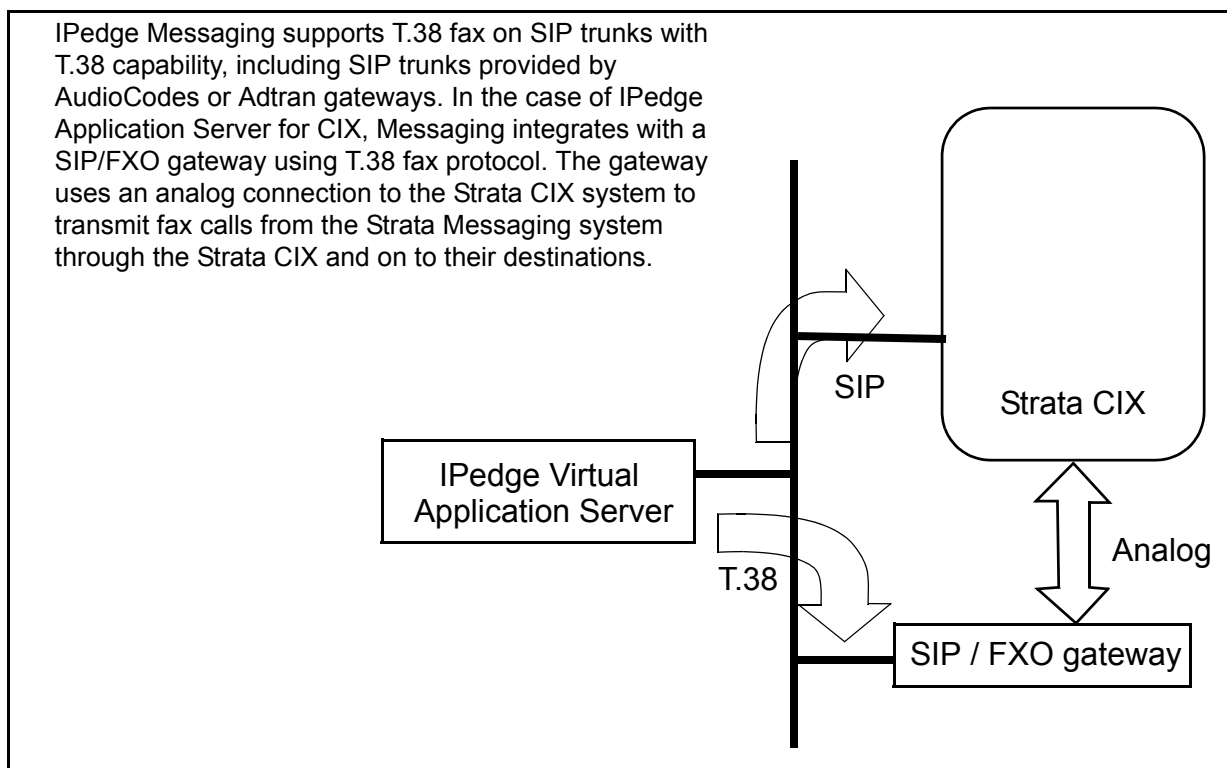
| | |
|------------------|---|
| Fax Mail | Fax mail allows a mailbox owner to receive faxes in his voice mailbox and view them via unified messaging (an email attachment) or use the telephone interface to re-route the incoming fax to a physical fax machine. Requires Unified Messaging license. |
| Fax from Desktop | Provides the ability to send faxes from the mailbox owner's desktop. Requires Unified Messaging license. |
| Incoming Fax DID | For inbound fax messages, a DID number may be associated with the mailbox. An incoming fax to this number will automatically trigger a fax tone and the fax will be stored in the mailbox. |

| | |
|--------------------------------------|--|
| Fax Auto Print | <p>The Auto Print client allows automatic printing of incoming faxes to network printers in a Microsoft® Windows® network environment. The client connects using ftp (file transfer protocol) to the Strata Messaging system at pre-set intervals, downloads incoming faxes and prints them to a printer pre-defined for each user. Up to 30 printers can be defined in the network, each one associated with a printer ID. In turn, users can select a printer where their faxes will be printed.</p> <p style="margin-left: 40px;">Important! The Auto Print client is a Windows based application so therefore cannot be installed on Linux server. It must be installed on a Windows system on the company network with access to desired network printers. There can be only one Auto Print client per Strata Messaging system. The printer configuration is shared by the system among all users. Attempting to install the Auto Print client on multiple network servers could cause erratic feature behavior.</p> |
| Fax Log | <p>A web-based report displays the mailbox owner's outbound faxes. The fax log includes date, time, status of an outbound fax, fax destination, account and billing codes.</p> |
| Fax-on-Demand | <p>This component allows incoming callers to access a library of documents and select a specific fax document to be faxed to them.</p> |
| Fax Queue | <p>A web-based report displays the mailbox owner's outbound faxes currently queued for transmission.</p> |
| Fax Settings | <p>The mailbox owner may set personal outbound fax settings, such as number of times to retry fax delivery based on busy or no answer and how long to wait between each try. Each fax user can transmit their own name and number (CSID) on outbound faxes.</p> |
| Incoming Fax DID | <p>For inbound fax messages, a DID number may be associated with the mailbox. An incoming fax to this number will automatically trigger a fax tone and the fax will be stored in the mailbox.</p> |
| Incoming Fax Target | <p>Faxes may be re-routed from an incoming mailbox to a secondary mailbox.</p> |
| SOFTWARE REQUIREMENTS for FAX | <p>All IPedge Messaging versions support fax. If configuring a IPedge Application Server for CIX, the host Strata CIX must be running version MT028 or later with either MIPU or GIPU firmware at version 0128 or later. These software versions are available on FYI for all models of Strata CIX systems.</p> |
| HARDWARE REQUIREMENTS for FAX | <p>As previously mentioned, Messaging's fax functionality requires the use of a SIP-FXO analog gateway to pass the fax transmissions to and from the system when running on a IPedge Application Server for CIX.</p> <p>Toshiba has tested and approved the AudioCodes gateway model MP114 (Toshiba part number MP114/4O/SIP).</p> <p>Analog circuits must also be installed and programmed in the Strata CIX.</p> |

FAX PART NUMBERS

| Part Numbers | Descriptions |
|--------------|--|
| I-MSG-ADV | IPedge IP Messaging Advanced mailbox - per user. One required for each voice mailbox includes unified messaging and fax. |
| MP114/4O/SIP | AudioCodes SIP to FXO analog gateway – four circuits. One gateway is required for each four fax channels on the IPedge Application Server for CIX. |

NETWORK CONFIGURATION for FAX



FAX INSTALLATION

The installation process for fax through Messaging on the IPedge Application Server;

- Program the Strata CIX for SLT ports and DID call routing.
- Program Messaging for outbound faxing.
- Install and configure AudioCodes gateway.

CIX PROGRAMMING

When connected to the Strata CIX system, Messaging will use the AudioCodes (AC) MP 114 gateway as its T.38 gateway. The AC FXO ports are connected to SLT ports on the CIX. Incoming fax calls are

directed to these SLT ports. The CIX will send in-band DTMF to indicate the destination mailbox for the call. Messaging will detect the DTMF and open the required mailbox. AC will detect CNG, send REINVITE with T.38 SDP and a T.38 session will commence between Messaging and the AC gateway.

1. Assign an SLT station in the Strata CIX database for each AC FXO port.
2. Set the Circuit Type for each SLT to be Voice Mail:

200 STATION DATA

| | | | |
|----------------------|-------------------------------------|-----------------|---|
| 01 PDN Equipment No. | <input type="text" value="010202"/> | | |
| 02 Station Type | <input type="text" value="SLT"/> | 03 Circuit Type | <input type="text" value="Voice Mail"/> |

3. Set the Control Method to be Inband/DTMF for each of the SLT ports:

580 VM PORT DATA

| | | |
|---------------------------|--|-------------------------------------|
| 00 VM Port DN | <input type="text" value="209"/> | <input type="button" value="List"/> |
| 01 Control Method | <input type="text" value="Inband/DTMF"/> | |
| 02 Send A/D Tone | <input checked="" type="radio"/> Enable <input type="radio"/> Disable | |
| 03 Send B Tone | <input type="text" value="No Tone"/> | |
| 04 End-to-End | <input checked="" type="radio"/> Enable <input type="radio"/> Disable | |
| 07 VM to VM Call Blocking | <input type="radio"/> Blocking <input checked="" type="radio"/> Non Blocking | |

4. Assign all of these SLT ports to a hunt group.
5. Set the Call Forward – All Call Record, Busy Record, and No Answer Record fields to * (asterisk):

579 SYSTEM VOICE MAIL DATA

| | |
|-------------------------------------|---|
| 01 DID/DNIS or DN VMID Option | DN VMID |
| 02 Cancellation Method for VM MW | Access Code Cancel |
| 03 Message Desk Number | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| 04 Output of CLASS / ANI and DNIS | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| 05 Calling Number Digits Sent to VM | 10 |
| 06 Blank Digits Sent to VM | 2 |
| 07 Auto Cancel of VM and MW | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| 08 DTMF Duration | 80msec |
| 09 Voice Mail Soft Keys | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| 10 Central VM Callback | 555 |
| 11 CF - All Call Record | * |
| 12 CF - Busy Record | * |
| 13 CF - No Answer Record | * |

6. Program the VM ID field in the CIX database for DID trunks. This example defines DID digits 3001 to be directed to the AC gateways for fax processing:
- The DID Number is defined as 3001.
 - The hunt group of the SLT ports connected to the gateway FXO (pre-defined as 3200) is entered in the Audio Day1 Dst Digits field.
 - The DID/DNIS No. VMID field contains 5678, which is the value of the Fax DID field of the destination mailbox for which the incoming Fax will be received.

ILG Group Number

309 DIRECT INWARD DIALING

| | | | |
|--------------------------|---|-------------------------------------|-----------------------------------|
| 01 DID Number | <input type="text" value="3001"/> | <input type="button" value="List"/> | |
| 02 MOH Source | <input type="text" value="1 Processor MOH Jack"/> | | |
| 03 GCO Key Group | <input type="text" value="0"/> | 04 Pooled Key Group | <input type="text" value="0"/> |
| 05 Audio Day1 Dst Type | <input type="text" value="Dialing Digits"/> | Audio Day1 Dst Digits | <input type="text" value="3200"/> |
| 06 Audio Day2 Dst Type | <input type="text" value="No Data"/> | Audio Day2 Dst Digits | <input type="text"/> |
| 07 Audio Night Dst Type | <input type="text" value="No Data"/> | Audio Night Dst Digits | <input type="text"/> |
| 08 Data Day1 Dst Type | <input type="text" value="No Data"/> | Data Day1 Dst Digits | <input type="text"/> |
| 09 Data Day2 Dst Type | <input type="text" value="No Data"/> | Data Day2 Dst Digits | <input type="text"/> |
| 10 Data Night Dst Type | <input type="text" value="No Data"/> | Data Night Dst Digits | <input type="text"/> |
| 11 DID/DNIS No. VMID | <input type="text" value="5678"/> | 12 DID/DNIS Name | <input type="text"/> |
| 15 VM Application Digits | <input type="text"/> | 16 Tenant Number | <input type="text" value="1"/> |

MESSAGING PROGRAMMING

The follow configuration applies specifically to the IPedge Application Server for CIX. Login to the Messaging Web Controller Administration mailbox and perform the following tasks;

For fax CNG tone detection, confirm the following parameter is set correctly.

- Go to **Registry > VoIP** and set "Enable Tone Detection" to 1.

For outbound faxing, each FXO port on the AC needs to be associated with a port on Messaging.

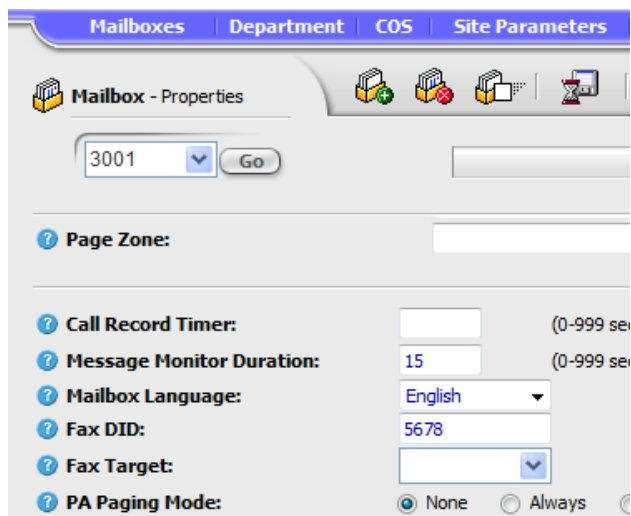
1. In PBX > Port Definition, define the SIP URI in the Fax Extension field using the following format: sip:ext@gw_ip_address – for example: sip:3205@172.16.2.45

In this example the Strata CIX system analog voice mail ports connected to the FXO jacks on the AC gateway are extensions 3205, 3206, 3207, 3208. The IP address of the AC gateway is 172.16.2.45.

| Chnl | DN | Dep. | Rec. Calls | Init. Calls | Mode | Type | PSTN Gateway | Fax Extension |
|------|------|------|------------|-------------|------------|---------|--------------|----------------------|
| 1 | 3101 | 1 | Yes | Yes | AutoAttend | Primary | 0 | |
| 2 | 3102 | 1 | Yes | Yes | AutoAttend | Primary | 0 | |
| 3 | 3103 | 1 | Yes | Yes | AutoAttend | Primary | 0 | |
| 4 | 3104 | 1 | Yes | Yes | AutoAttend | Primary | 0 | |
| 5 | 3105 | 1 | Yes | Yes | AutoAttend | Primary | 0 | sip:3205@172.17.2.17 |
| 6 | 3106 | 1 | Yes | Yes | AutoAttend | Primary | 0 | sip:3206@172.17.2.17 |
| 7 | 3107 | 1 | No | Yes | AutoAttend | Primary | 0 | sip:3207@172.17.2.17 |
| 8 | 3108 | 1 | No | Yes | AutoAttend | Primary | 0 | sip:3208@172.17.2.17 |

2. Configure the mailbox to receive the FAX DID. It is important that these digits are unique and are not a mailbox in the system database.

Enter the DID digits configured in the CIX Programming section, Step 6, into the FAX DID: field. In the example shown below, the DID digits are 5678. The Strata messaging system searches the mailbox database for these digits. In this example mailbox 3001 will receive faxes when the DID digits 5678 are received.



The screenshot shows the 'Mailbox - Properties' configuration window. At the top, there are tabs for 'Mailboxes', 'Department', 'COS', and 'Site Parameters'. Below the tabs, there is a search bar with '3001' selected and a 'Go' button. The main configuration area includes several fields: 'Page Zone' (empty), 'Call Record Timer' (empty), 'Message Monitor Duration' (15), 'Mailbox Language' (English), 'FAX DID' (5678), 'Fax Target' (empty dropdown), and 'PA Paging Mode' (radio buttons for 'None' and 'Always', with 'None' selected).

3. After completing the above steps, configure the rest of the parameters in **Site Parameters > Fax Settings** where the following fields are displayed:

Company name – Enter the name of the company to be displayed on the fax header.

Outbound Calls prefix – Enter the prefix to be used in sending faxes.

Default area code – Enter the local area code of the system. If the fax number dialed begins with the default area code, it will be omitted from the dialing.

Area code prefix – This field is used in conjunction with the above field (Default area code). If you need to omit both country code and city code from the dialing string, enter the country code in the Default area code field and the city code in the Area code prefix field. If the number dialed begins with the Default area code but has a city code different from the Area code prefix, only the Default area code will be omitted. If the Area code prefix is also identical, both numbers will be omitted.

General Delivery mailbox – This is the mailbox to which faxes are directed, unless otherwise specified.

Length of local extension (DN) – If the number to be dialed is longer than this length, the system will add the Outbound Call Prefix to the number when dialing.

Dialing method – Select the pulse or tone option button. Not applicable in SIP.

Number of tries – Number of attempts to transmit a fax before removing from the send queue.

Delay after NA – Number of minutes to wait before retrying to dial out after a No Answer Condition.

Delay after BY – Number of minutes to wait before retrying to dial out after a Busy Condition.

Delay after Error – Number of minutes to wait before retrying to dial out after a transmission error Condition.

Retrieving Faxes

To retrieve faxes via unified messaging, refer to the Mailboxes chapter of the Messaging manual.

To retrieve faxes via telephone interface, refer to the Messaging User Guide section on Redirect Fax Messages.

FAX ON DEMAND

The Fax-On-Demand application is implemented using a script mailbox. The script op-codes are used to select and verify a document, enter and verify a callback fax machine number, and submit the fax.

Steps to create a fax-on-Demand application:

1. Create a new script mailbox.
2. Program the script options using the Fax related op-codes (explained below).
3. Upload the fax documents in to the mailbox directory (explained below).
4. Designate access to the script mailbox by routing a DID to it or providing access.

To create and upload documents into the Fax on Demand Server:

1. The Fax documents are stored in the directory of the script mailbox (/usr/Sm/mailbox/xxxxxxx where xxxxxx represents the mailbox number). For example, mailbox 3001 will have a directory location 0003001. The format of the files can be either TIFF (Tagged Image File Format) or text. To be accessible by phone, the names of the fax files should be numeric.

Example: A fax file can be named 1234.fax (the extension .fax must be lower case). When the user is prompted to select a document number, s/he will enter 1234 to retrieve fax file 1234.fax.

2. The Fax File List frame at the bottom of the script page will show all fax files in a specific mailbox.

-
3. You will need to copy all required documents to the mailbox directory. You can use FTP to place the files in the directory.
 4. If the original document is a hard copy, you can simply fax it into the server (to any Fax Mail enabled mailbox), download the message to your local PC, rename it to the correct format and FTP it to the directory on the server.
 5. If the original document is in electronic format, use a TIFF conversion program, rename it to the correct format and FTP it to the directory on the server.
 6. Recommended TIFF conversion program is "Document Converter" from Neevia Technology (www.neevia.com). When converting to TIFF, make sure to convert to Black & White G3 fax format with No End Of Line (No EOL).

FAX-ON-DEMAND SCRIPT FUNCTIONS

The following are the Fax-on-demand script functions.

Script Functions

To create a fax-on-demand script the following functions are available.

Choose Doc – Use this function to receive the document number required by the caller. In the Parameter field enter the number of digits to be received.

OK – Document number is valid.

ERR – No such document exists or no digits were received.

Get Phone No

Use this function to receive the telephone number of the fax machine to send the document to. In the parameter field enter two parameters: minimum number of digits to receive and maximum number of digits. Use a comma to separate between the two parameters. The # key can be used by the caller to terminate number entry if it is less than the maximum number of digits.

OK – Sufficient number of digits was entered.

ERR – Not enough digits were entered.

Trans. Fax

Use this function to send the fax to the required destination. Parameters available for this function are:

No Parameter – Send the selected fax (Choose Doc.) to the selected number.

PlayBack selected Doc [/D] – Play the selected document number (to confirm entry).

PlayBack selected phone num [/P] – Play the selected telephone number (to confirm entry).

Submit fax [/S] – Submit fax to queue in a dedicated line call.

Divert to fax device [/N] – Divert a call to a fax port and save the fax in the current script box

Divert to fax device and save in [/Nxxx] – Divert a call to a fax port and save it in mailbox xxx

To send a specific document number (as required by the Menu 1 Digit command), add the document number to the /S (e.g. if the document number is 110 then the command is TransFax/S110).

OK – Fax sent.

ERR – Not able to send fax.

Document Selection

The document can be selected in two ways:

1. **ChooseDoc** – and a parameter indicating the number of digits to receive. You should record a message “Please enter document number.”
2. **Menu 1 Digit** – record a message containing a list of available documents. For each document, assign a corresponding menu entry, which will go to a separate line in the script. This line should contain a TransFax with a specific document number.

To select multiple documents, you can repeat the ChooseDoc opcode. The PlayBack Selected Document function will always repeat the number of the last fax selected. When selecting multiple documents, you can issue the PlayBack opcode after each ChooseDoc entry.

Example of Fax on Demand

The script prompts the caller to enter a phone number (the system expects between 7 to 11 digits), then to enter document number (3 digits). It then reads out the information and puts the fax in the sending queue. You must make sure that after the fax is sent the OK statement is used to continue the flow.

To test this script, upload some 3 digit files into the mailbox and record the following messages:

- 01 – Please enter your fax number
- 02 – Please choose document number
- 03 – The document number you selected is...
- 04 – Your fax number is...
- 08 – Fax sent successfully
- 15 – Error sending fax

FAX CONTACTS

Fax Contacts is the personal address book for each user that is used with the fax client application. When a user sends a fax they can choose addresses from either the MAPI (standard Windows mail API) address book or this personal (Strata Messaging internal) address book.

To set up personal contacts navigate to Fax>Fax Contacts in the WebController and select the New Fax Contact icon. Enter in the contact information and click Create. To delete a contact click Delete to the right of the contact.

FAX LOG

The fax log screen, found under **Fax > Fax Log** in the WebController displays all outbound faxes from this user, including the following information. Click on a specific line to view the sending history of the specific fax.

Recipient – The name of the person the fax was sent to (as entered in the outbound fax request).

Fax Number – The fax number that was dialed (as entered in the outbound fax request).

Date and Time – The date and time of the fax transmission.

Pages – The number of pages transmitted.

Size – The size of the fax file (in Kilo Bytes).

Quality – The quality of the transmission – Normal or Fine (as entered in the outbound fax request).

Account Code – The account code dialed before the number (if available).

Billing Code – The billing code number entered by the user.

CSID – The CSID of the receiving fax device.

Requested CSID – The CSID requested by the user as the authorized recipient (optional)

Result – The result of the transmission.

Error Msg – Error message generated in case of failure.

View Fax – The actual fax file can be viewed.

FAX QUEUE

The fax queue screen, found under **Fax > Fax Queue** in the WebController displays all outbound faxes currently queued for transmission, including the following information.

Recipient – The name of the person the fax was sent to (as entered in the outbound fax request).

Fax Number – The fax number that was dialed (as entered in the outbound fax request).

Date and Time – The date and time of the fax transmission.

Status – The status of the transmission.

Tries – The number of tries already attempted.

Priority – For future use.

Quality – The quality of the transmission – Normal or Fine (as entered in the outbound fax request).

CSID – The CSID of the receiving fax device.

Error Msg – Error message generated in case of failure.

Resubmit – Resubmit the current fax immediately.

Delete – Delete the current fax from the queue immediately.

AUDIOCODES INSTALLATION

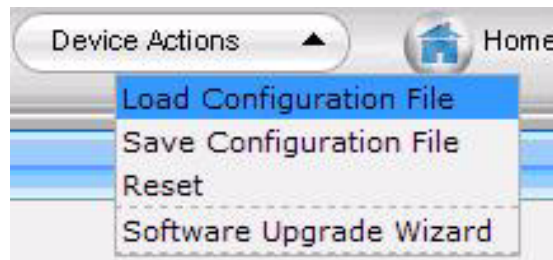
Use the Autocoders model MP-114 FXO gateway with AudioCodes firmware version 5.60A.029.004. or later

LOAD AUDIOCODES TEMPLATE

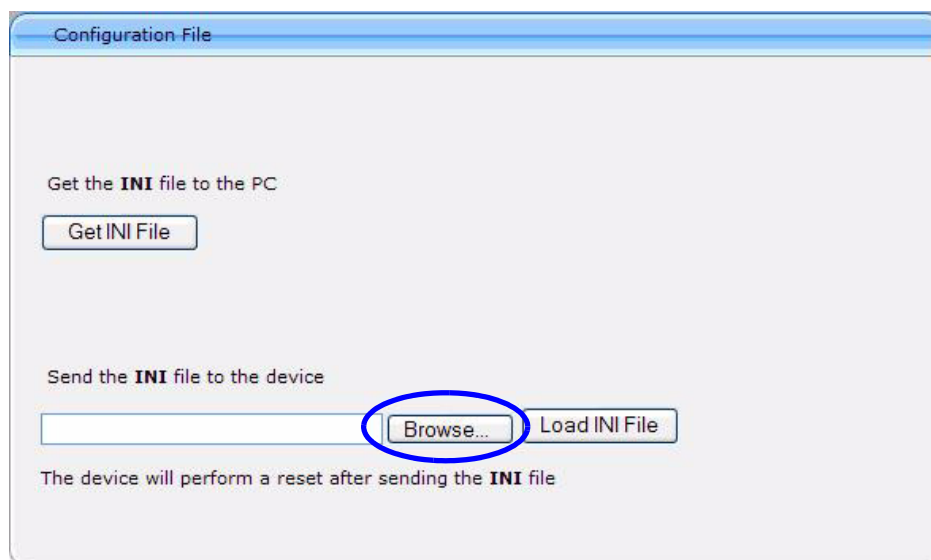
1. Open a browser and enter the factory default IP address:
http://10.1.10.11
2. Login with the user name: **Admin** and password: **Admin**
The main AudioCodes menu will display:



3. Download the Strata Messaging Fax gateway configuration file from FYI.
SM_Audio_Codes_Fax.ini
4. Upload the Default Strata Messaging Fax gateway configuration to the gateway.
5. Select **Device Actions/Load Configuration File**.



6. Click on the Browse button to find the location of the SM_Audio_Codes_Fax.ini configuration file.



7. Click the **Load INI File** button.
8. A confirmation message is displayed, click on **Ok**.
9. The AudioCodes gateway will reset automatically. A status message saying; The device is now restarting and will not be available for 60 seconds will display. The site will be refreshed automatically.
10. When the User name and Password dialog box appears, login with the user name: **Admin** and password: **Admin**
The main AudioCodes menu will display.

CONFIGURE THE AUDIOCODES FAX GATEWAY

Important! Always click on the **Submit check** button to save changes.

1. Configure the AudioCodes IP address settings.
Select **Configuration/Network Settings/IP Settings**.

Enter the IP Address/Subnet Mask/Default Gateway address that match the network configuration the gateway is connected to.

Shown below is an example configuration.

| Single IP Settings | |
|-------------------------|---------------|
| IP Address | 172.16.2.45 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway Address | 172.16.2.254 |

2. Enter the NTP server IP address (optional) and the DNS Primary Server (optional). Select **Configuration Network/Settings/ Application Settings**.
3. Select **Configuration > VoIP > SIP Definitions > General Parameters**. Change the SIP Destination Port to 5070.
4. Select **Configuration/Protocol Configuration/Protocol Definition/ Proxy & Registration**. Verify that **Use Default Proxy** is set to **Yes**.
5. Ensure that the **Proxy Name** field is left blank (no data). Entering any value in this field will prevent the AudioCodes Gateway from functioning.

6. Define the IP address of Strata Messaging proxy (Strata Messaging system IP address). Select **Configuration/Protocol Configuration/ Protocol Definition/Proxy Sets Table**. Enter the IP address of the Strata Messaging system as the **Proxy Address**. Set the Transport Type to **UDP**.

| | Proxy Address | Transport Type |
|---|---------------|----------------|
| 1 | 172.16.2.4 | UDP |

7. Verify that the codec is set to **G711U-law** (and other settings as shown below). Select **Configuration/Protocol Configuration/ Protocol Definition/Coders**.

| Coder Name | Packetization Time | Rate | Payload Type | Silence Suppression |
|------------|--------------------|------|--------------|---------------------|
| G.711U-law | 20 | 64 | 0 | Enable |

8. Select **Configuration/Protocol Configuration/Endpoint Settings/Automatic Dialing**. Define the station numbers of the CIX Voice Mail (DTMF) analog ports connected to the Fax gateway (FXO).

Automatic Dialing

| Gateway Port | Destination Phone Number | Auto Dial Status |
|--------------|--------------------------|------------------|
| Port 1 FXO | 3205 | Enable |
| Port 2 FXO | 3206 | Enable |
| Port 3 FXO | 3207 | Enable |
| Port 4 FXO | 3208 | Enable |

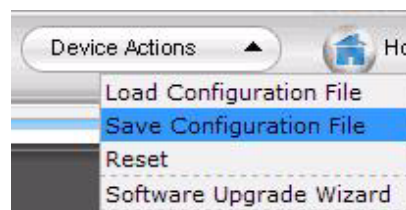
Important! The parameters entered in Step 7 and Step 8 must match for the Fax gateway to function properly.

9. Select **Configuration/Protocol Configuration/Endpoint Number/Endpoint Phone Number**. Enter the station numbers of the CIX Voice Mail (DTMF) analog ports connected to the Fax gateway (FXO).

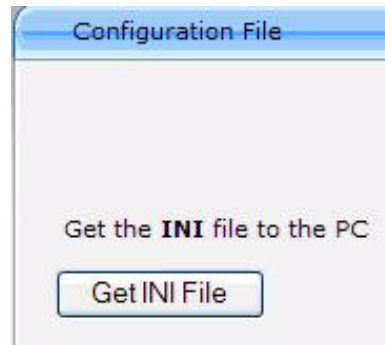
Endpoint Phone Number Table

| | Channel(s) | Phone Number | Hunt Group ID | Profile ID |
|---|------------|--------------|---------------|------------|
| 1 | 1 | 3205 | | 1 |
| 2 | 2 | 3206 | | 1 |
| 3 | 3 | 3207 | | 1 |
| 4 | 4 | 3208 | | 1 |

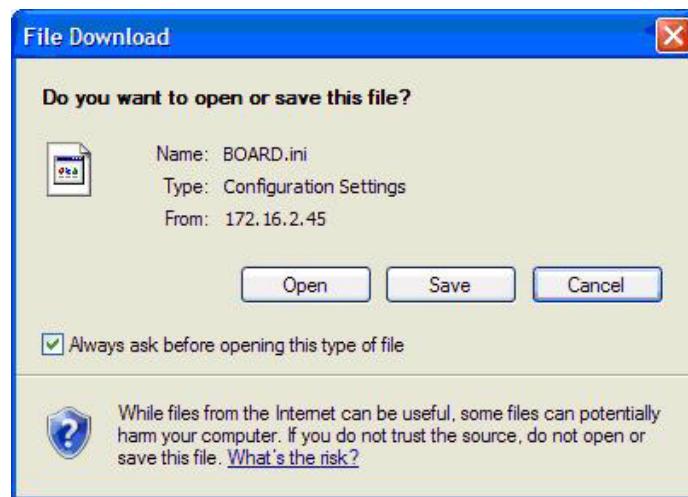
10. Press **Submit** then, press **Register**.
11. Save the Fax gateway configuration. Select **Device Actions/Save Configuration File**.



12. Click on **Get INI File**.



13. Click on **Save** to download and save the configuration file.



14. A dialog box will open allowing you to select the location and or name of the file. Click on **Save**.

15. Burn the new configuration to the Fax gateway internal flash memory, so that the configuration can be restored in the event that the gateway is reset or power is lost.

16. Select **Management/Maintenance Actions**.



17. Click on the **BURN** button.

18. Verify incoming and outgoing Fax transmission with the Strata Messaging system.

CLIENT INSTALLATION

The Fax Printer Driver software is installed on the client computers to support the Messaging fax features. You will need to install the Messaging fax driver on each client machine. You can download the fax driver installation program from Toshiba's FYI web site.

FAX PRINTER DRIVER

The following procedure is used to install and configure the Messaging Fax printer software on the client machines.

1. From a client system download the Messaging Fax printer driver version 4.01 (or later) from Toshiba's FYI web site.
2. Click **Start > Run**. In the Run dialog box click on the **Browse** button. Browse the file downloaded from FYI. The path and file name will be an executable file in the Messaging_Fax_Printer_Driver folder. For example:
C:\Messaging_Fax_Printer\MessagingFaxDriverSetup4.01.exe
3. Click **OK**.
4. The Messaging Fax Driver setup wizard will appear. Click on **Next**.
5. The End User License Agreement will display. Read the EULA then click on the **I accept the terms of the license agreement** radio button.
6. Click on **Next**.
7. In the Messaging Web Fax Driver dialog box enter the IP address or the computer name of the Strata Messaging system.

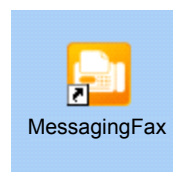
Note: To use the host name instead of the IP address, the host name must be entered in the DNS server on your network. Check with your network administrator.

8. Click **Next**.
9. In the Customer Information dialog box enter the **User Name** and **Company Name** of the client machine then, click **Next**.
10. Accept the default installation directory and click **Next**.
11. In the Ready to Install the Program dialog box click on **Install**.
12. When the installation is complete the confirmation dialog box is displayed. Click on **Finish**.

FAX PRINTER DRIVER CONFIGURATION

When the Fax Printer Driver software has been installed it must be configured before it can be used.

1. Double click on the desktop fax icon or access from **Start > All Programs > TAIS/Messaging Fax Driver > MessagingFax**.



-
2. This will load the configuration controls into the lower right of the Windows task bar.
 3. This fax icon will also appear when a fax is printed. It will remain until the Exit option or the PC is shutdown and restarted.
 4. To view the options move the mouse cursor over the center of the icon and Right click.

Click on **Fax** to see the Options menu:

- Fax queue
- User Information (link to the Web Controller to configure Mailbox Fax options).
- Fax Log (history of sent Faxes)

Account Administration — Provides a link to log on to the Web Controller to configure mailbox Fax options.

System Options — Change the IP address/Name of the Messaging system from which you are printing faxes.

Exit — Exit the Messaging Fax Printer driver configuration utility.

WEB CONTROLLER MAILBOX FAX OPTIONS

Select **Mailboxes > Fax** then:

Fax Settings

- **Busy/Err Delay** – Number of minutes to wait between attempts when faxing out, if the previous attempt failed because of a busy signal or a transmission error.
- **No Answer Delay** – Number of minutes to wait between attempts when faxing out, if the previous attempt failed because of no answer.
- **Retries** – Total number of attempts to transmit a fax.
- **No. of rings before No Answer** – Number of rings before a fax call times out.
- **Incoming Format** – The format of the fax document that will be sent as an attachment to an email. Can select between TIF or PDF. This field also applies to the format of the faxes sent as an attachment to the fax verification email when sending outbound faxes.
- **Personal CSID (Identification Phrase)** – The CSID, both for outgoing faxes and incoming faxes, transmitted for this mailbox.

Incoming Faxes

- **Accept Incoming Faxes Y/N** – This option allows you to select whether to receive or deny faxes. If you select not to receive faxes, this mailbox will not receive any faxes unless there is a Fax DID defined in the mailbox properties. In this case the fax will only be accepted if the call was received on the Fax DID number of the mailbox. This is to minimize spam faxes to non fax users.

Fax Confirmation

Outgoing faxes – This field defines the type of confirmation the user will receive for outbound faxes. The confirmation will be sent as an email to

the email address defined in Mailbox-Email Settings under the send mail frame.

- Deactivate: No email confirmation.
- Successful Only: Notification will be sent only if the fax transmission was successful.
- Failed Only: Notification will be sent only if the fax transmission failed.
- All: Notification will be sent for every fax attempt, both successful and failed.

Auto Print **Active** – Select this box if you wish to have all faxes automatically sent to a printer. Auto Print requires that auto print service is running on a Windows machine on the local office network. Refer to [“AUTO PRINT” on page Chapter 13 – 21.](#)

Fax Contacts This list is used by the Printer driver (clicking on the Phone Book Icon).

Fax Log Record of past Faxes sent using the printer driver.

Fax Queue Displays any faxes currently being processed

Cover Information Cover page Information (entered when printing a fax)

Fax Confirmation **Printer Name** – Select the printer name you wish the faxes to print to from the drop down list.

AUTO PRINT

Messaging Fax allows you to have all of your faxes automatically sent to a networked printer in a Microsoft® Windows® network environment. Auto Print must be installed on one computer on the Messaging network.

The Messaging Fax Auto Print installation procedure is shown below.

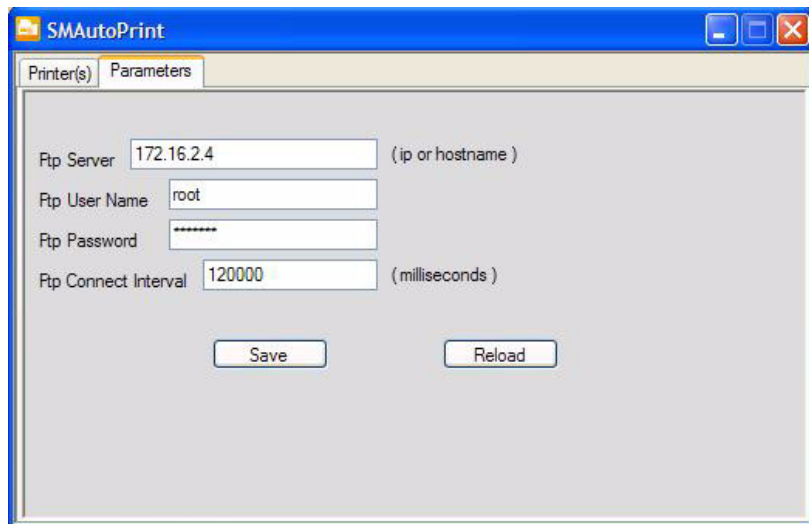
1. Download the Messaging Fax Auto Print client version 3.2 (or later) from the Toshiba FYI web site. Save the downloaded file on the Auto Print computer.
2. At the Auto Print machine click on **Start > Run** then click on the **Browse** button.
3. Browse to the location of the installation file obtained from FYI and click **OK**.
4. The **Massaging Auto Print** install shield wizard will open. Click on **Next**.
5. The End User License Agreement dialog box will open.
6. Read the agreement. Click the **I accept the terms of the license agreement** button.
7. Click on **Next**.
8. In the Customer Information dialog box enter the User Name and Company Name, click the **Anyone who uses this computer (all users)** button then, click on **Next**.

9. In the Setup Type box click to select **Standard** installation and click on **Next**.
10. In the Choose Destination Location dialog accept the default installation directory, click on **Next**.
11. When the Ready to Install dialog box opens click on **Install**.
12. When the Install Shield Wizard Complete box opens, click on the **Finish** button to complete the installation.

AUTOPRINT SERVICE

Use the following procedure to configure the Messaging AutoPrint service.

1. To configure it double click the icon or on the desktop task bar select; **Start > All Programs > TAIS > Messaging AutoPrint > Launch Messaging AutoPrint**.
2. Select the Parameters tab
3. Enter the following information:
 - FTP server – the IP address or host name of the Messaging system
 - FTP user name – enter root as the user name
 - FTP Password – enter toshiba as the password
 - FTP Connect Interval – the interval (in milliseconds) between FTP connections to the Messaging main server. Default value is 120,000 milliseconds (120 seconds)
4. Click on the **Save** button.
5. When making any changes to the Parameters tab, make sure to stop and start the SM Print service for changes to take effect.
6. To cancel changes and revert back to previous settings, click on the **Reload** button.



The screenshot shows the SMAutoPrint application window with the Parameters tab selected. The window contains the following fields and buttons:

- Printer(s)** tab (inactive)
- Parameters** tab (active)
- Rtp Server**: 172.16.2.4 (ip or hostname)
- Rtp User Name**: root
- Rtp Password**: *****
- Rtp Connect Interval**: 120000 (milliseconds)
- Save** button
- Reload** button

AutoPrint on Windows Vista and Windows 7

The following procedure is for Auto Print running on Windows Vista® and Windows 7 operating systems. If your print service is running on the Windows XP operating system go to [“Printer Configuration” on page 13-24](#).

1. The Messaging print service on Windows Vista and Windows 7 must run under a user account with Administrative privileges.
2. In the task bar select **Start > Control Panel > Administrative Tools > Computer Management > Local Users and Groups**.
3. Click on **Local Users and Groups/Users**.
4. Right click **Users** then, select **New User**.
5. Enter a user name and password.
6. Select **Password never expires**.
7. Click **OK**.
8. Double click on **Users**.
9. Double click on the User account that was just created.
10. Click the **Member Of** tab.
11. Click the **Add** button then click **Advanced**.
12. Click **Find Now**. Click **Administrators** then click **OK**.
13. Click **OK** then click **OK** on the next screen to complete.
14. Configure the MessagingPrint service to run under the user account. **Start > Control Panel > Administrative Tools > Services** then, double click on MessagingPrint.
15. Click on the **Log On** tab. Click on **This account**.
16. Click on **Browse > Advanced > Find Now** then, select the user account that was created in step 4. Click **OK** until you return the list of services.
17. Right click on MessagingPrint and select **Start** to start the service.
18. Select **Startup** type. Change to **Automatic**.
19. Go to [“Printer Configuration” on page 13-24](#).

Printer Configuration

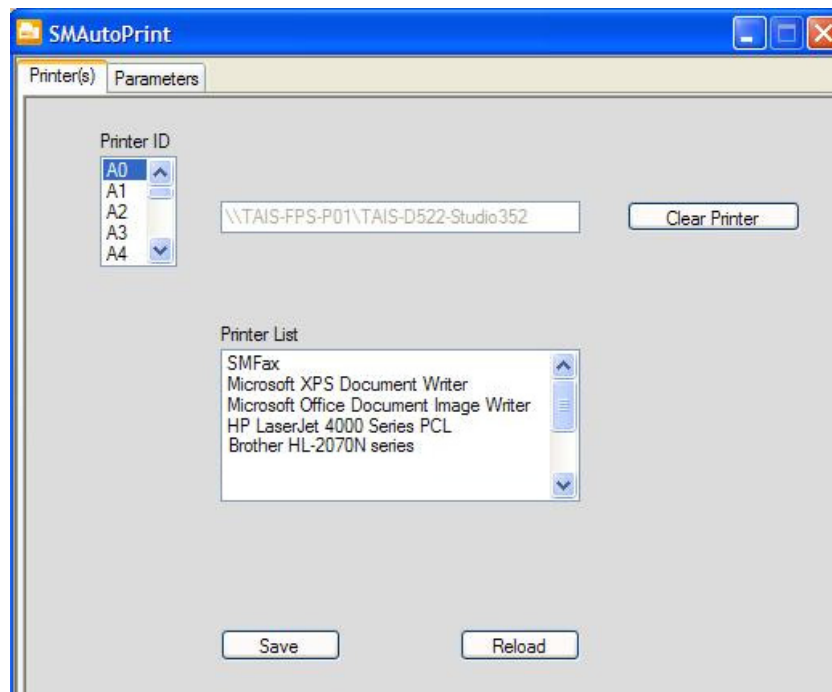
Printer configuration procedure for the Messaging system:

Note: This is the list that appears in the Webcontroller Fax Settings configuration page for each mailbox. This list is shared by the Strata Messaging system.

1. Click the Printer ID you wish to update.
2. From the printer list, select the printer you want to associate with the Printer ID.
3. Repeat for all printers you want to define.
4. To remove a value from a printer ID, click on the **Clear Printer** button.
5. Click on the **Save** button.
6. When making any changes to the Printers tab, make sure to Stop then, Start the SMPrint service for changes to take effect.

To start or stop the print service; on the system desktop select **Start > Control Panel > Administrative Tools > Services > SMPrint**.

7. Select **Startup** type. Change to **Automatic**.
8. To cancel changes and revert to previous settings, click on the **Reload** button.



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 for iDRAC7 documentation.

IPedge VIRTUAL APPLICATION SERVER RECOVERY

If the hard disk drive(s) (HDD) in the IPedge server is damaged or corrupted contact Technical Support.

SERVER FAN REPLACEMENT

SERVER FAN REPLACEMENT

Each server contains several cooling fans. Refer to the Dell owner guide for you server for replacement instructions.

SERVER POWER SUPPLY REPLACEMENT

You must shut down the system to replace a power supply module on the R220 and R420 servers. The Dell 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 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.

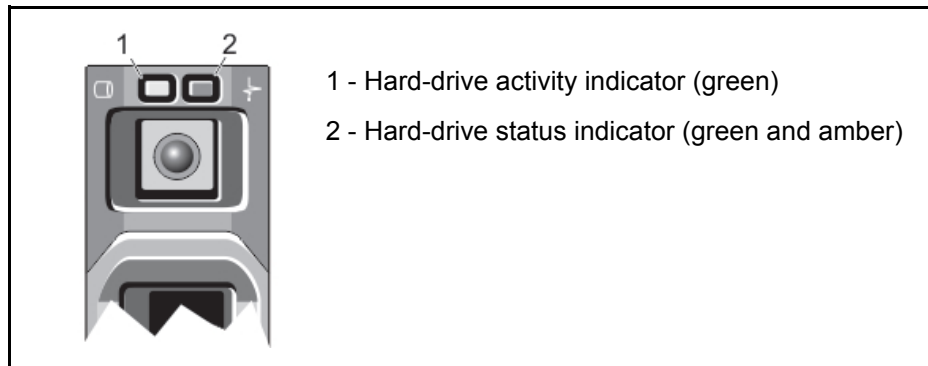


Table 14-1 RAID HDD Indicators

| 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 NOTE: 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 |

(Sheet 1 of 2)

Table 14-1 RAID HDD Indicators (continued)

| Drive-Status Indicator Pattern (RAID Only) | Condition |
|---|------------------|
| Blinks amber four times per second | Drive failed |
| Blinks green slowly | Drive rebuilding |
| Steady green | Drive online |

(Sheet 2 of 2)

THIS IS THE END OF THE DOCUMENT.