

MITEL

Live Business Gateway



Installation and Maintenance Guide
Release 3.4 SP2

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

Mitel and Live Business Gateway are trademarks of Mitel Networks Corporation.

Windows and are trademarks of Corporation.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Other product names mentioned in this document may be trademarks of their respective companies and are hereby acknowledged.

Installation and Maintenance Guide

Release 3.4 SP2

August 2013

®,™ Trademark of Mitel Networks Corporation
© Copyright 2013, Mitel Networks Corporation
All rights reserved

Chapter 1: Overview

Overview	3
Audience	3
How Live Business Gateway Works	3
What's New in this Release	4
Release 3.4 SP2	4
Release 3.4	4
System Requirements	5
Industry Standards	7
Communication	7
Supported MCD Versions	7
Supported Phones	8
Personal Ring Group Support	9
Monitoring prime extensions of PRG	9
Monitoring non-prime extensions of PRG	9

Chapter 2: Installation

Installation and Configuration Overview	13
Specifying MCD Settings	14
MiTAI/TAPI Computer Integration	14
Class of Service Options	14
Before You Begin	14
Resource Allocation on the Live Business Gateway Virtual Machine	16
Downloading Live Business Gateway	16
Installing Live Business Gateway Release 3.4	16
ODM/IDM Rule Import and Export	22
Configuring Live Business Gateway in Lync 2010/2013 for Remote Call Control	22
Configuring Lync Server 2010/2013 for Remote Call Control in TLS Mode	23
Configuring Lync Server 2010/2013 for Remote Call Control in TCP Mode	24
Configuring Users for Remote Call Control	25
Configuring Lync Server 2010/2013 and Port 5060	26
Configuring Network Interface Cards	26
Deploying Live Business Gateway Release 3.4 in a VMware vSphere Environment	26
VMware vSphere Management Tools	27
Deploying Live Business Gateway Release 3.4 in a Microsoft Hyper-V Environment	28
Microsoft Hyper-V Management Tools	29
Offline License Activation	29
Disabling Service Failure Recovery	29

Upgrading Live Business Gateway Software and Licenses 30
 Before You Begin 30
 Upgrading Live Business Gateway Software 30
 Upgrading Live Business Gateway Licenses 31

Chapter 3: Security Certificates for TLS

Creating a Security Certificate for Live Business Gateway 35
 Prerequisites 35
 Requesting the Live Business Gateway Certificate (Windows Server 2008 R2 Workstations) . 35
 Downloading the LBG Certificate (on Windows Server 2008 R2 Workstations) 36
 Requesting the LBG Certificate (on Windows Server 2003/2003 R2 (SP2) Workstations) . . . 38
 Downloading the LBG Certificate (on Windows Server 2003/2003 R2 (SP2) Workstations) . . 39
 Converting Certificates to PEM 40
 Converting gwkey.pvk to PEM 41
 Accessing the gwkey.pvk File 41
 Installing the Certificates and the Key 41
 Migrating MSL Configuration Files to Windows 42
 Migrating MSL Configuration Files 42
 Migrating Data Using Text Console 42
 Migrating Data Using WINS SCP 43

Chapter 4: Troubleshooting

Diagnosing Problems 47
 Using the Log Viewer Tool (MSPLogs.exe) 53
 Error Reporting Utility 53
 Troubleshooting Procedures 54
 Configuring a Prime Line Phone in Live Business Gateway 54
 Verifying the MCD Address 55
 Verifying Live Business Gateway Is Running 55
 Verifying the User Account in Active Directory 56
 CSTA References 56



Chapter 1
Overview

Overview

Mitel® Live Business Gateway enables communication between Microsoft Lync Server 2010/2013 and Mitel Communications Director (MCD) enabling Lync users to take advantage of the basic and supplementary phone services of MCD. Using Microsoft Lync Server 2010/2013, the Lync client controls the phones connected to MCD.

Live Business Gateway is supported in a VMware® vSphere and Microsoft Hyper-V® environment. Mitel supports vSphere and Hyper-V to enable voice and business applications to run together in a virtual environment.



Note: Throughout this guide we refer to Lync Server 2010/2013, rather than Office Communications Server 2007/2007 R2. Live Business Gateway will continue to support Office Communications Server 2007/2007 R2.

Audience

This guide instructs solution providers on how to order, license, and install the Live Business Gateway software.

How Live Business Gateway Works

Live Business Gateway

- Enables users with Mitel desk phones to place and receive calls from the Lync client and Microsoft Office Suite.
- Provides enterprise presence information about users to the Lync client and Office Suite (for example, Jane Doe is "on a call")
- Uses the industry standard SIP/CSTA protocol, which is simpler to understand than the MCD call control API. (To learn about CSTA, refer to "CSTA References" on page 56)
- Allows desktop applications to use the following call control features:
 - Make Call
 - Answer Call
 - Clear Call
 - Deflect Call
 - Hold
 - Retrieve Call
 - Consultation Call
 - Transfer
 - Alternate Call
 - Set Forwarding

The following scenario illustrates this type of communication.

John, using the Lync client, receives a text message from David, who has requested an online review of a specific document. John uses the Lync client to start a document-sharing session which allows both John and David to

- See the same document at their PCs
- View any typing or cursor movements
- Make updates to the document

At some point during the session John decides to call David, and simply clicks David's name in the contact list to place the call. David is alerted and answers the call.

What's New in this Release

Release 3.4 SP2

- **Support for Lync Server DNS Load Balancing:** Live Business Gateway Release 3.4 SP2 supports the use of Lync Server DNS Load Balancing. Refer to Microsoft Lync Server Documentation for details.

Release 3.4

- **Support of Live Business Gateway in Hyper-V Virtualized Environments:** Live Business Gateway Release 3.4 is supported in a Microsoft Windows Server 2008 R2 Hyper-V environment. See "Deploying Live Business Gateway Release 3.4 in a Microsoft Hyper-V Environment" on page 28 for more information.
- **ODM/IDM Rule Import and Export:** Live Business Gateway 3.4 provides a facility to import/export the MCD ODM/IDM rule templates to a CSV file. See "ODM/IDM Rule Import and Export" on page 22 for more information.
- **Error Reporting Utility:** Live Business Gateway Release 3.4 has an error reporting utility that can send e-mail alerts to the System Administrator when certain critical errors are logged on the server. See "Error Reporting Utility" on page 53 for more information.
- **Support for Servers with Multiple NICs:** Live Business Gateway Release 3.4 supports multiple NIC cards when voice and data are on separate networks. The Live Business Gateway configuration applet now provides the ability to input two Live Business Gateway configuration IP addresses. See "Configuring Network Interface Cards" on page 26 for more information.
- **Support for Mitel Communications Director 5.0 SP1 and SP2:** See "Supported MCD Versions" on page 7 for a list of all the MCD versions that Live Business Gateway Release 3.4 supports.
- **Support for DSS/BLF Key:** Live Business Gateway Release 3.4 supports the use of the DSS/BLF key. Users can perform all the telephony operations with the DSS/BLF key from the IP phone. Live Business Gateway also supports the "Secretarial" line type along with the "DSS/BLF" line type.

- **Support for vSphere 5.0:** Live Business Gateway Release 3.4 is supported in a VMware vSphere ESX or ESXi 5.0 environment. See “Deploying Live Business Gateway Release 3.4 in a VMware vSphere Environment” on page 26 for more information.
- **Use of Visual Studio 2010:** Live Business Gateway Release 3.4 software is compiled using Visual Studio 2010.
- **Personal Ring Group Support:** Live Business Gateway partially supports the Personal Ring Group (PRG) feature of the MCD. See “Personal Ring Group Support” on page 9 for more information.

System Requirements

Communication between the Lync client and MCD requires

- MCD 4.0 SP4 and greater
- Microsoft Lync Server 2010/2013
- Microsoft Lync client
- Microsoft Active Directory Server
- Mitel supported phone (IP or DNIC)
- Layer 2 Ethernet Switch

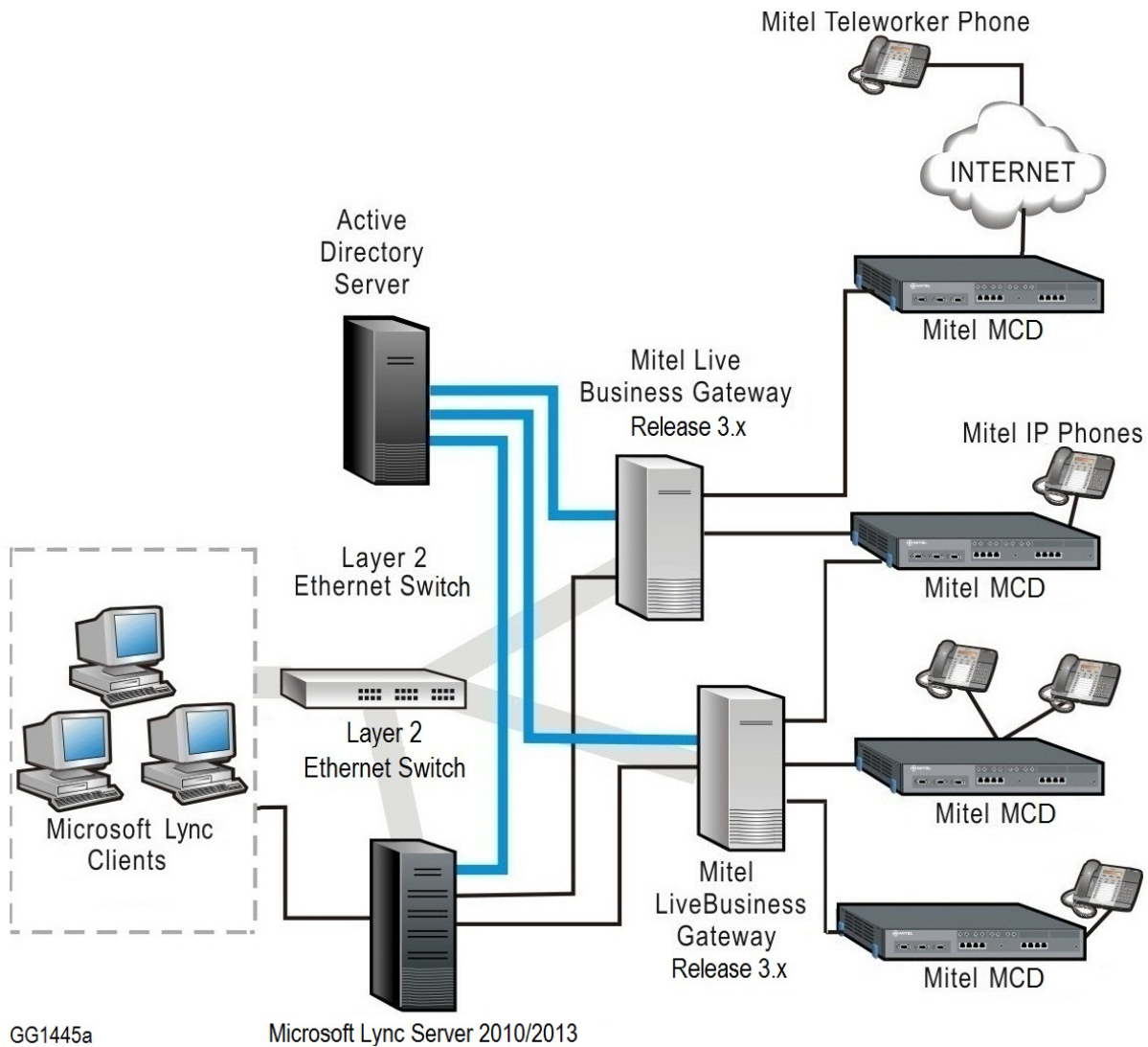


Figure 1: Live Business Gateway Information Flow

The flow of information is as follows:

1. The Lync client sends messages to and registers with Lync Server 2010/2013.
2. Lync Server 2010/2013 sends requests to and receives events from Live Business Gateway on behalf of the Lync client. Live Business Gateway communicates with Lync Server 2010/2013 using SIP/XML/CSTA messages.
3. Live Business Gateway sends requests to MCD using Mitel proprietary messages.



Note: Mitel phones communicate only with MCD.

Industry Standards

Live Business Gateway uses the following industry standards:

- Standard ECMA-269 6th edition (June 2004) - Services for Computer Supported Telecommunications Applications (CSTA) Phase III: This standard allows integration between a desktop application and a PBX.
- Standard ECMA-323 3rd edition (June 2004) - XML Protocol for Computer Supported Telecommunications Applications (CSTA) Phase III: This standard defines the XML schema for the services part of the integration including Call Control, Capability Exchange, Call Routing, Message Waiting and Forwarding.
- CSTA for SIP Phone User Agents (uaCSTA) as described in EMCA Technical Report TR/87, *Using CSTA for SIP Phone User Agents (uaCSTA)*, 1st Edition (June 2004): This report describes how messages are transported over a SIP session.

Communication

Session Initiation Protocol (SIP) is used to transmit XML messages between the Lync client, Lync Server 2010/2013, and Live Business Gateway. Authentication and authorization is shared by Lync Server 2010/2013 and Live Business Gateway as follows:

- Lync Server 2010/2013 authenticates Lync client users.
- Live Business Gateway authorizes the monitoring and control of the MCD phone.
- The SIP interface between Lync Server 2010/2013 and Live Business Gateway is secured by Mutual Transport Layer Security (TLS).

SIP proxies can be placed between Lync Server 2010/2013 and Live Business Gateway to provide any required policies for authentication and message routing.

Supported MCD Versions

Live Business Gateway supports the following MCD versions:

- MCD 6.0 SP2
- MCD 6.0 SP1
- MCD 6.0
- MCD 5.0 SP2
- MCD 5.0 SP1
- MCD 4.2 SP2
- MCD 4.1 SP2
- MCD 4.0 SP4

Supported Phones

Live Business Gateway supports the following phones (in MiNet mode only):

- 420 DNI Phone
- 4015 DNI Phone
- 4025 DNI Phone
- 4125 DNI Phone
- 4150 DNI Phone
- 5212 IP Phone
- 5215 IP Phone
- 5220 IP Phone
- 5224 IP Phone
- 5235 IP Phone
- 5240 IP Phone
- 5304 IP Phone
- 5312 IP Phone
- 5320 IP Phone
- 5320e IP Phone
- 5324 IP Phone
- 5330 IP Phone
- 5330e IP Phone
- 5340 IP Phone
- 5340e IP Phone
- 5360 IP Phone
- Navigator



Note: You use the Lync client only to monitor and control the prime line of Mitel phones.



Note: Live Business Gateway does not support the monitoring of ACD agents.



Note: Live Business Gateway Release 3.4 and greater supports the use of the DSS/BLF key. Users can perform all the telephony operations with the DSS/BLF key from the IP phone.

Personal Ring Group Support

Live Business Gateway partially supports the Personal Ring Group (PRG) feature of the MCD.

Monitoring prime extensions of PRG

Live Business Gateway is able to monitor the prime extensions of the PRG. Users are able to perform all telephony operations from the MOC/phone of an LBG monitored prime extension of a PRG.

Monitoring non-prime extensions of PRG

Live Business Gateway is able to monitor the non-prime extensions of the PRG. Users are able to perform all telephony operations from the MOC/phone of an LBG monitored non-prime extension of a PRG.



Note: Live Business Gateway does NOT support the "One busy all busy" feature.



Chapter 2
Installation

Installation and Configuration Overview

Table 1 provides an overview of the installation and configuration tasks. You *must complete* tasks 1 to 4 before you install Live Business Gateway. You must perform the tasks in the order listed.

Table 1: Installation and Configuration Tasks

	Task	Description
1.	Deploy Lync Server 2010/2013	This includes installing an Active Directory server on Windows Server 2003/2003 R2 (SP2) or Windows Server 2008 R2. For more information, refer to the Microsoft documentation at http://technet.microsoft.com/en-us/office/bb267356.aspx .
2.	Deploy the Lync client on desktop PCs	Refer to the Microsoft documentation at http://office.microsoft.com/en-us/communicator/
3.	Deploy MCD 4.0 (SP4) or greater	When deploying MCD <ol style="list-style-type: none"> 1. Configure an application user account. An ESM user account and password are required for tasks 2 and 6. 2. Verify the MCD MiTAI/TAPI Computer Integration License and Option Selection option is enabled. See "Resource Allocation on the Live Business Gateway Virtual Machine" on page 16 for instructions on how to change this setting. 3. Set Class of Service options for each phone that is controlled by Lync Server 2010/2013. See "Class of Service Options" on page 14 for details.
4.	Deploy Mitel phones	Refer to the list of supported Mitel Phones, See "Supported Phones" on page 8.
5.	Install the Live Business Gateway software	Refer to "Before You Begin" on page 14 and "Downloading Live Business Gateway" on page 16.
6.	Verify routing	Verify Lync Server 2010/2013 static routing is configured to route calls to Mitel Live Business Gateway. See page 31.
7.	Configure Lync	Manually configure Lync to use Live Business Gateway.
8.	Sign in users	Sign in Lync users. For more information, refer to the <i>Live Business Gateway Quick Reference Guide</i> available at Mitel OnLine.

Specifying MCD Settings

You specify the following settings to enable Live Business Gateway to communicate with MCD.

MiTAI/TAPI Computer Integration

If you did not enable the **MiTAI/TAPI Computer Integration** option while installing MCD, you must enable it now and restart the MCD server. All service will be interrupted for approximately 20 minutes. We recommend you schedule the system to restart during a period of low use.

To enable the MiTAI/TAPI Computer Integration option

1. Launch the ESM and log in.
2. Select **System Configuration>System Capacity>License and Option Selection**.
3. Click **Change**.
4. Under the **MiTAI/TAPI Computer Integration**, click **Yes**.
5. Type the password and then click **Save**.
6. Restart the MCD server for changes to take effect.

Class of Service Options

You must specify Class of Service (COS) options for each phone controlled and monitored using the Lync client.

1. On the Class of Service Options Assignment form, set the following options to **Yes** for all IP phones that use RCC:

HCI/CTI/TAPI Call Control Allowed YES
HCI/CTI/TAPI Monitor Allowed YES



Note: The default value of the preceding options is *No*.

Before You Begin

You must complete the tasks listed in Table 2 before you can use Live Business Gateway.

Table 2: Pre-installation Checklist

	Task	Notes
1.	If you have not already done so, complete the Lync Server 2010/2013 and MCD installation and configuration tasks.	See "Installation and Configuration Overview" on page 13. and complete the tasks listed.

Page 1 of 2

Table 2: Pre-installation Checklist (continued)

	Task	Notes
2.	Verify the hardware requirements of the workstation on which you will install Live Business Gateway	Verify the workstation has the following hardware: For 2,500 or fewer users: <ul style="list-style-type: none"> • 1 GHz processor (minimum) • 1 GB RAM (minimum) • 40 GB hard drive (minimum) For 2,500 to 10,000 users in a Lync Server 2010/2013 environment: <ul style="list-style-type: none"> • 2 GHz processor (minimum) • 2 GB RAM (minimum) • 40 GB hard drive (minimum)
3.	Verify resource allocation on the Live Business Gateway virtual machine	Refer to “Resource Allocation on the Live Business Gateway Virtual Machine” on page 16 and verify resource allocation on the virtual machine.
4.	Deploy MCD 4.0 (SP4) or greater	To Configure the MCD servers that will connect to Live Business Gateway <ol style="list-style-type: none"> 1. Configure the MCD server addresses as <i>static</i> IP addresses. 2. Verify the MCD MiTAI/TAPI Computer Integration option is enabled. See “MiTAI/TAPI Computer Integration” on page 14 for instructions to change this setting.
5.	Verify the operating system	Verify one of the following operating systems has been installed: <ul style="list-style-type: none"> • Windows Server 2003 • Windows Server 2003 R2 (SP2) • Windows Server 2008 R2
6.	Verify runtime components	<ul style="list-style-type: none"> • Windows .NET 2.0 or later • Visual C++ 2010 Redistributable Package: Obtain the Visual C++ 2010 Redistributable Package available on the LBG download page on MOL
7.	Verify network requirements	Verify that the specific network configuration requirements for Live Business Gateway have been set up. For more information, contact your Mitel representative.
8.	Order Live Business Gateway license(s)	Place your order with Mitel Customer Services for the required number of Live Business Gateway licenses. The CCC adds the ordered products to your AMC license account.
9.	Create an Application Record for Live Business Gateway	In your AMC account, create an Application Record for Live Business Gateway installation and assign the licenses you ordered in step 6. Make a note of the Application Record ID number: you will need to enter it before you can activate Live Business Gateway.
10.	Install the Live Business Gateway software	Complete the steps in the following sections to download and install the software.

Resource Allocation on the Live Business Gateway Virtual Machine

The vSphere and Hyper-V requirements for the Live Business Gateway virtual machine are provided in Table 3.

Table 3: vSphere and Hyper-V Requirements

Users	RAM		vCPU		Hard Disk Storage
	Total	Reserved	Total	Reserved	
2,500	1 GB	1 GB	1 vCPU	1 GHz	40 GB
10,000	2 GB	2 GB	2 vCPU	2 GHz	40 GB

Downloading Live Business Gateway

To download Mitel Live Business Gateway software from Mitel OnLine

1. Log on to Mitel OnLine.
2. Move your cursor over **Technical** and click **Software Downloads**.
3. Select **Live Business Gateway**.
4. Click the links to download the software and any associated release notes.

Installing Live Business Gateway Release 3.4

The following section details how to install Live Business Gateway and configure the MCD and Lync Server 2010/2013 servers to work with Live Business Gateway.



Note: Microsoft Lync 2010/2013 Enterprise DNS load balancing is not supported. Load balancing can still be achieved by using a separate hardware load balancer.

Disclaimer: Although Mitel has attempted to set up the interop testing facility as closely as possible to a customer premise environment, the implementation setup could be different on site. YOU MUST EXERCISE YOUR OWN DUE DILIGENCE IN REVIEWING, PLANNING, IMPLEMENTING, AND TESTING A CUSTOMER CONFIGURATION.



Note: Do not install any other third party software on the workstation where Live Business Gateway is installed.



Note: If you are upgrading to a newer version of Live Business Gateway, refer to “Upgrading Live Business Gateway Software and Licenses” on page 30.



Note: Lync Server 2010/2013 does not support dual forking. Twinning of a users desk phone with the users Lync softphone is possible via the Mitel Communications Director Personal Ring Group feature.



Note: The Live Business Gateway configuration instructions apply only to the basic Remote Call Control configuration that uses TCP communication with Lync.

To install Live Business Gateway

1. Complete the tasks detailed in the pre-installation checklist. See “Before You Begin” on page 14.
2. Download the software from the Mitel MOL web site.
3. Double click **LBG.exe** to start the installation.
4. Click **Next** to start the installation wizard.
5. Read the license agreement and click **Yes**.
6. Click **Next** to install the files in the default directory or click **Browse** to select another directory on the workstation.
7. In the **Start Copying Files** window, verify the directory path for installation and click **Next** to begin installing files. To optionally change any values, click **Back**. The Live Business Gateway Settings window opens.
8. On the **Live Business Gateway** tab:
 - Select the **Use Multiple NIC?** checkbox if the voice and data traffic are on different networks.
 - In the **Data IP** field, enter either:
 - a.) the primary IP address of the LBG server if it is not configured on multiple NICs, or
 - b.) the data traffic NIC address.
 - In the **Voice IP** field, enter the voice IP address of the LBG server if it is configured on multiple NICs. Otherwise, the IP address will be the same as the data traffic NIC address and this field will be disabled. Refer to “Configuring Network Interface Cards” on page 26 for more information.
 - In the **SIP Port** field, enter the SIP port number.
 - Select the **TLS** check box if you are deploying LBG in TLS mode.



Note: You use the Transport Layer Security protocol for communication between Live Business Gateway and Lync Server 2010/2013. TLS requires you create security certificates. The certificates used for all services must come from the same Certificate Authority. For more information, refer to “Security Certificates for TLS” on page 33. If TLS is not being used, leave this box unselected; see “Configuring Lync Server 2010/2013 for Remote Call Control in TCP Mode” on page 24 for details.



Note: If Live Business Gateway is used with Lync Server 2010/2013, and being deployed in TLS mode, ensure the Windows Firewall is either disabled or has rules in place to allow traffic on port 5060 or 5061. The default setting for the firewall in Windows 2008 R2 is *Enabled*.

The Live Business Gateway ICP tab includes the information required to identify, log in, and route call control messages to a specific MCD.



Note: The Live Business Gateway service will not start unless at least one ICP is configured.

9. On the **ICP** tab, specify the following information for each MCD Live Business Gateway will use:

- After **IP Address**, type the IP Address of MCD.
- After **Remote Call Control SIP URI**, type a value. The value must exactly match the "Line Server URI" specified for each user in the Lync configuration and use this format:

sip:<username>@<PBX name>.<LBG name>.<FQDN>

For example, sip:LBG@PBX1.LBG1.mitel.com where 'LBG' is a generic service name that is common to all users, 'PBX1' is the unique name of MCD, 'LBG1' is the unique name of Live Business Gateway associated with the ICP, and the FQDN 'mitel.com' is specific to Live Business Gateway.



Note: You can use the Lync Server 2010/2013 format listed above to identify a new Live Business Gateway or new ICP added to an Lync Server 2010/2013 system. However, you cannot use the Lync Server 2010/2013 format to create a new SIP URI for an existing ICP/Live Business Gateway pair that already has a SIP URI in the Lync Server 2010/2013 format.

- After **ESM User Name**, type the user name for the Live Business Gateway account programmed on MCD.
- After **ESM Password**, type a password for the Live Business Gateway account programmed on MCD.
- After **ARS Leading Digits**, type a prefix number you dial to access PSTN calls. This numeric entry is the trunk prefix inserted by Live Business Gateway when you dial using a TEL URI in the format tel:+123635 (that is, a TEL URI without phone context). If the dial string is NOT in the format tel:+nnnnnn (where nnnnnn represents the number), the trunk prefix is not used. If you select this option, Live Business Gateway will treat the number as an internal number and will not add ARS digits to the number before it sends the number to MCD. This prevents potential problems when storing internal numbers in E.164 format.
- Select the **Clustered Network** check box if Live Business Gateway communicates with one MCDs or a clustered MCD system (in this scenario, each phone number is unique). A clustered network consists of multiple MCDs where each directory number is unique throughout the entire network. Do not select the check box if Live Business Gateway communicates with a networked environment of MCDs where phone numbers are not unique (for example, when the same extension exists on two different nodes).

10. Click **Add**. ICP information appears.
11. Continue adding ICPs. When you are finished, click **Apply**. To remove an ICP you have added, select it in the window and click **Remove** and then click **Apply**.
12. On the **Licensing** tab, after **Service Link ID**, type the Application Record ID used for licensing the Live Business Gateway server against the AMC.
13. Click **Update License**.
14. On the **Active Directory** tab, specify the following information:



Note: If Live Business Gateway is in the same domain as the Active Directory server and there is only one Active Directory, you do not need to specify additional information in this window. Proceed to step 15 (if applicable) or step 16.

- After **AD FQDN**, type the Fully Qualified Domain Name of the Active directory domain controller that resides on the domain with Lync Server 2010/2013. This is the Active Directory with which Live Business Gateway communicates.
- After **User Name**, type the account name and password (in the format domain\user-name) that have LDAP query privileges/allow Live Business Gateway to access Active Directory.
 - a. Click **Add To List**. The user name information is displayed in the window.
 - b. Continue to add servers. When you are finished, click **Apply**. Only Active Servers named in the list will be contacted.



Note: To remove a user name, select the name in the window and click **Remove** and then click **Apply**.

15. On the **ODM** (Outgoing Digit Modification) tab, modify leading numbers in the dial string used to make calls from the Lync client. By default, digit modification is disabled. To enable it, specify leading numbers and replacement numbers. If entries are made on this tab, all dial strings used to make calls will be checked.

- If you have added more than one ICP, after **Please select an ICP**, select the appropriate entry from the list.
- After **Device ID Length**, specify the number of digits for the TEL URI digit string (for example, if the Calling Device ID TEL URI is tel:2001;phone-context=lbq@abc.local, the Device ID Length is 4), *OR* enter "*" to add a "wild card" which indicates the string can be any length (for both old and new ODM rules).



Note: You must enter a value greater than 0 (or type * to specify any length) and does not exceed 2 digits. Otherwise your entry will be rejected.

- After **Leading Digits**, type the leading digit pattern to replace.



Note: You must enter a unique numeric value between 1 and 26. If the pattern already exists in the Digit Modification list, your entry will be rejected.

- After **Replacement Digits**, type the digit string that will replace the leading digits, or leave this field blank to prevent removal of the leading digits. The value does not have to be unique as multiple digit patterns can be replaced by the same replacement string.



Note: You must enter a numeric value between 1 and 26 digits in length or leave this field blank. Otherwise, your entry will be rejected. The device ID length and the leading digits together define the unique key of the outgoing digit modification rule. You cannot enter two rules that have the same device ID length *and* leading digits.

- Select the **Ignore ARS** check box to treat the number as an internal number and not apply ARS digits to it. See Note.
- To remove individual digit modification pairs from the list, click **Remove**. To clear the entire list, click **Clear**.
- If you have added two or more rules, to change the order in which they are searched select a rule in the table and click **Move Up** or **Move Down** to change its position. The first rule that satisfies the condition with the Outgoing call device ID will be used.



Note: Live Business Gateway performs digit modification before it checks ARS leading digits. For example, if you enter a digit modification pair of {77,1} on the Digit Mod tab and an ARS leading digit of 9 on the ICP tab, when the Lync client sends tel:+7712345 to Live Business Gateway, the + character is removed and the dial string is marked as a global number. Digit modification changes the number from 7712345 to 112345, and then ARS is applied and the dial string sent to the MCD server is 9112345.



Note: ARS is applied only to global numbers. When using the Lync client, you must enter a leading "+" character to indicate a global dial string. Digit Modification is applied to both local and global numbers. PSTN calls from the Lync client should start with a "+" or an ARS leading digit.



Note: Digit modification data, when entered, is stored in the ICP_config.txt file, enclosed in "digits-mod-start" and "digits-mod-end" tags.

16. Live Business Gateway now provides a facility to import/export the MCD ODM rule templates to a file. Live Business Gateway Release 3.4 and greater provides the following rule template import/export buttons on the ODM tab:

- **Import:** Allows you to import the ODM rule templates for a selected ICP only.
- **Import All:** Allows you to import the ODM rule templates for all the ICPs present in the drop-down list.
- **Export:** Allows you to export the ODM rule templates for a selected ICP only.
- **Export All:** Allows you to export the ODM rule templates for all ICPs present in the drop-down list.



Note: For more information on the ODM rule templates, refer to "ODM/IDM Rule Import and Export" on page 22.

17. On the **IDM** (Incoming Digit Modification) tab, change the leading numbers in the dial string for incoming calls to modify the format of the Inbound Calling Device ID sent to the Lync Server 2010/2013. Order the rules in the list to specify the search order. Any rule with blank leading digits should be last on the list.

Example: **Device ID Length:** 4; **Leading Digits:** 2; **Replacement Digits:** 16135921; **Add "+":** Enabled. Calling Device ID TEL URI: tel:2001;phone-context=lbg@abc.local.
Returned TEL URI: tel:+16135921001.

Caution: The converted number is added to the user's Recent Contact list in Lync, allowing the user to click Call Back to return the call. Ensure that Digit Modification has been set up correctly to prevent the outbound call from failing.

- After **Please select an ICP**, if you have added more than one ICP, select the appropriate entry from the list.
- After **Device ID Length**, specify the number of digits for the TEL URI digit string (TEL URI (for example, if the Calling Device ID TEL URI is tel:2001;phone-context=lbg@abc.local, the device ID length is 4).



Note: You must enter a numeric value that is greater than 0 and does not exceed 2 digits. Otherwise, your entry will be rejected.

- After **Leading Digits**, type the leading digit pattern to replace. The number of digits must be less than that of the device ID length. If this field is left blank, replacement digits will be added as a prefix to the ID.



Note: You cannot enter two rules that have the same Device ID Length *and* Leading Digits, including blank. Leading and Replacement digits cannot both be blank at the same time. Otherwise, your entry will be rejected.

- After **Replacement Digits**, type the digit string that will replace the leading digits, or leave this field blank to prevent removal of the digits.



Note: The Leading and Replacement digits fields cannot both be blank at the same time. Otherwise, your entry will be rejected.

- Select the **Add "+"** check box to return the number in E.164 format. All data after the semicolon in the TEL URI is truncated. This will not affect a number that is already in E.164 format.
- If you have added two or more rules, to change the order in which they are searched select a rule in the table and click **Move Up** or **Move Down** to change its position. The first rule that satisfies the condition with the Outgoing call device ID will be used.

18. Live Business Gateway now provides a facility to import/export the MCD IDM rule templates to a file. Live Business Gateway Release 3.4 and greater provides the following rule template import/export buttons on the IDM tab:

- **Import:** Allows you to import the IDM rule templates for a selected ICP only.
- **Import All:** Allows you to import the IDM rule templates for all the ICPs present in the drop-down list.
- **Export:** Allows you to export the IDM rule templates for a selected ICP only.
- **Export All:** Allows you to export the IDM rule templates for all ICPs present in the drop-down list.



Note: For more information on the IDM rule templates, refer to “ODM/IDM Rule Import and Export” on page 22.

19. The Application Record ID is used for licensing the Live Business Gateway server against the AMC. On the **Licensing** tab, after **ServiceLink ID**, type the Application Record ID number that you created in Step 5 of the “Installation and Configuration Overview” on page 13.

20. Click **Update License**. One of the following results will occur:

- The Live Business Gateway server contacts the AMC server, downloads your licensing files, and displays the resulting details in the License Details box on the Licensing tab. Click **OK** and then click **Finish**. On the Live Business Gateway tab, click **Start** to start Live Business Gateway.

OR

- The Live Business Gateway server fails to contact the AMC licensing server (for example, there is no Internet connection) and displays an error message asking if you want to continue with a removable media. Proceed to “Offline License Activation” on page 29 to perform a manual license activation, or click **No** to cancel the license update.

ODM/IDM Rule Import and Export

Live Business Gateway provides a facility to import/export the MCD ODM/IDM rule templates to a file. There can be numerous rules for ODM/IDM associated with a particular MCD and to enter these rules one by one in the Live Business Gateway configuration applet is time consuming. Therefore, to simplify this task, Live Business Gateway provides a facility for importing and exporting templates of the rules from a file.

The ODM/IDM rule templates are imported from a CSV (Comma Separated Value) file. This file can be viewed and edited by both Microsoft Excel and any other text editor such as Notepad.

The rules in the CSV file must be entered in the following format before import:

```
<IP address>, <Add Plus (0/1)/ Ignore ARS (0/1)>, <Device ID Length>,  
<Leading digits>, <Replacement digits>
```

The following are samples for ODM/IDM rule template import:

```
192.168.0.61,0,6,9999,#6866  
192.168.0.61,1,66,9999,6668  
192.168.0.61,0,9,9999,*6668
```

Live Business Gateway Release 3.4 and greater provides the following template import/export buttons on the ODM and IDM tabs of the Live Business Gateway configuration applet:

- **Import:** Allows you to import the ODM/IDM rule templates for a selected ICP only.
- **Import All:** Allows you to import the ODM/IDM rule templates for all the ICPs present in the drop-down list.
- **Export:** Allows you to export the ODM/IDM rule templates for a selected ICP only.
- **Export All:** Allows you to export the ODM/IDM rule templates for all ICPs present in the drop-down list.

Configuring Live Business Gateway in Lync 2010/2013 for Remote Call Control

Configuring Remote Call Control (RCC) in a Mitel Live Business Gateway (LBG)/Lync Server 2010/2013 environment consists of the following:

- Set up the Mitel LBG in TLS (default) or TCP mode.
- Set up the Lync Server for RCC.
- Configure users.
- Configure the Lync Server to listen on Port 5060.

When you configure Lync in TLS or TCP mode, use the address format examples provided in Table 4.

Table 4: Installation Addresses

Server	Address
Lync 2010/2013 Server FQDN	Lync 2010/2013 Server FQDN (for example, Lync.mitel.com)
LBG Server FQDN	LBG1.mitel.com
LBG Server IP	10.10.10.11
LBG Server Port	TLS/5061
Line Server URI (for AD Lync users) / Remote Call Control SIP URI (LBG)	3300@mitel.lbg.com

Lync Server 2010/2013 uses PowerShell cmdlets for a large proportion of the configuration.

Configuring Lync Server 2010/2013 for Remote Call Control in TLS Mode

To configure Lync Server 2010/2013 for Remote Call Control in TLS mode, ensure that the LBG is configured for TLS mode.

1. In the Control Panel, click **Live Business Gateway**.
2. On the **Live Business Gateway** tab, make sure that the **TLS** check box is selected.
3. Click **OK**.
4. Click **Start > All Programs > Microsoft Lync Server 2010/2013 > Lync Server Management Shell** to open Lync PowerShell.
5. Configure Lync Server 2010/2013 for RCC in TLS mode as follows:

a. Create Trusted Application Pool:

```
New-CsTrustedApplicationPool -Identity lbg1.mitel.com -Registrar Lync.mitel.com -Site 1 -TreatAsAuthenticated $True -ThrottleAsServer $True -RequiresReplication $False
```

b. Create Trusted Application:

```
New-CsTrustedApplication -ApplicationID RCC -TrustedApplicationPoolFqdn lbg1.mitel.com -Port 5061 Enable-CsTopology
```

c. Create Static TLS route variable to LBG server:

```
$tlsRoute = New-CsStaticRoute -TLSRoute -Destination lbg1.mitel.com -UseDefaultCertificate $true -Port 5061 -MatchUri mitel.lbg1.mitel.com
```

```
Set-CsStaticRoutingConfiguration -Route @{Add=$tlsRoute}
```

```
Enable-CsTopology
```

d. Export Lync Topology to XML File:

```
Get-CsTopology -AsXml | Out-File C:\rcc.xml
```

- e. Apply workaround within the XML File:
Edit the LBG Application section within the XML file, replacing the "0.0.0.0" (seen below) with the actual IP address of the LBG server and click **Save**:

```
<Cluster Fqdn="lbg1.mitel.com" RequiresReplication="false" RequiresSetup="true">
  <ClusterId SiteId="1" Number="3" />
  <Machine OrdinalInCluster="1" Fqdn="lbg1.mitel.com">
    <NetInterface InterfaceSide="Primary" InterfaceNumber="1" IPAddress="0.0.0.0" />
  </Machine>
</Cluster>
```
- f. Publish Topology from Edited XML File:
`Publish-CsTopology -FileName C:\rcc.xml`

Configuring Lync Server 2010/2013 for Remote Call Control in TCP Mode

To configure Lync Server 2010/2013 for Remote Call Control in TCP mode, ensure that the LBG is configured for TCP mode.

1. In the Control Panel, click **Live Business Gateway**.
2. On the **Live Business Gateway** tab, make sure that **TLS** check box is *not* selected.
3. Click **OK**.
4. Click **Start > All Programs > Microsoft Lync Server 2010/2013 > Lync Server Management Shell** to open Lync PowerShell.
5. Configure Lync Server 2010/2013 for RCC in TCP mode as follows:
 - a. Create Trusted Application Pool:
`New-CsTrustedApplicationPool -Identity lbg1.mitel.com -Registrar Lync.mitel.com -Site 1 -TreatAsAuthenticated $True -ThrottleAsServer $True -RequiresReplication $False`
 - b. Create Trusted Application:
`New-CsTrustedApplication -ApplicationID RCC -TrustedApplicationPoolFqdn lbg1.mitel.com -Port 5060 -EnableTcp`
 - c. Create Static TCP route variable to the LBG server:
`$tcpRoute = New-CsStaticRoute -TCPRoute -Destination 10.1.1.53 -Port 5060 -MatchUri lbg1.mitel.com`

`Set-CsStaticRoutingConfiguration -Route @{Add=$tcpRoute}`

`Enable-CsTopology`

The topology will then need to be exported to XML and a manual workaround applied to get Remote Call Control working with Mitel Live Business Gateway in a Lync environment.

Caution: Before implementing the next steps, test it in an isolated environment before making changes to any production environment.

- d. Export Lync Topology to XML File:

```
Get-CsTopology -AsXml | Out-File C:\rcc.xml
```
- e. Apply workaround within the XML File:
 After "Primary" InterfaceNumber="1" IPAddress=" edit the LBG Application section within the XML file, replacing "0.0.0.0" with the actual IP address of the LBG server (for example, 10.1.1.53) and click Save.

```
<Cluster Fqdn="lbg1.mitel.com" RequiresReplication="false" RequiresSetup="true">
  <ClusterId SiteId="1" Number="3" />
  <Machine OrdinalInCluster="1" Fqdn="lbg1.mitel.com">
    <NetInterface InterfaceSide="Primary" InterfaceNumber="1"
    IPAddress="0.0.0.0" />
  </Machine>
</Cluster>
```
- f. Publish Topology from Edited XML File:

```
Publish-CsTopology -FileName C:\rcc.xml
```
- g. Add SIP Server TCP Port:

```
Set-CsRegistrar "registrar.lync.mitel.com" -SipServerTcpPort
5060"
```

Configuring Users for Remote Call Control

For each user that needs to be setup for RCC, go into their account details in the Lync Server Control Panel.

1. In the **Telephony** drop-down list, select **Remote Call Control**.
2. In the **Line URI** field, enter the Line Uniform Resource Identifier for the user, using the following format:

```
tel+#####;ext=XXXX
```

 e.g.: tel:+441632456765;ext=6765
3. In the **Line Server URI** field, enter the Line Server Uniform Resource Identifier for the user. Ensure this value matches the Remote Call Control SIP URI specified on the ICP tab in the Live Business Gateway control panel.
4. Click **Commit**.



Note: Each user needs to have their corresponding extension field value (e.g. 6765) configured in their Active Directory account so the Mitel LBG can know that the user is setup for that phone number.

Configuring Lync Server 2010/2013 and Port 5060

The Lync Front End Server needs to be configured to listen on port 5060 for SIP TCP so it can receive traffic from the Mitel LBG. Do this by running a PowerShell cmdlet from Lync Server.

1. Click **Start > All Programs > Microsoft Lync Server 2010/2013 > Lync Server Management Shell** to open Lync PowerShell.
2. Enter the following cmdlet:

```
Set-CsRegistrar "Registrar:lync.<Your Server FQDN>" -SipServerTcp-Port 5060.
```

Configuring Network Interface Cards

Live Business Gateway Release 3.3 and greater supports multiple NIC cards. When multiple NICs are connected to the server, Live Business Gateway uses the NIC whose IP address is configured in the Live Business Gateway control panel applet for all communications.

Live Business Gateway uses a single NIC for both incoming (from Lync) and outgoing (to Lync and to MCD) sockets. Live Business Gateway uses the NIC whose IP address is configured on the Live Business Gateway tab.

We recommend you configure Live Business Gateway on the primary IP address of the computer with multiple NICs to avoid licensing issues.

Live Business Gateway also supports multiple NIC cards when voice and data are on separate networks. Some sites with multiple NICs configure their server so that one NIC card is used for data and the other is used for voice. The Live Business Gateway configuration applet provides the ability to input two Live Business Gateway configuration IP addresses. In this case, one IP address is used to communicate with the Lync/OCS server and the other is used to communicate with MCDs. If only one NIC card is being used, then you must enter the same IP address in both input boxes (Data IP and Voice IP fields).

Deploying Live Business Gateway Release 3.4 in a VMware vSphere Environment

Live Business Gateway is supported in a VMware vSphere environment, which enables voice and business applications to run together in a virtual environment. Live Business Gateway is able to take advantage of the improved performance, ease of use, and comprehensive management capabilities of data center virtualization.

The key benefits for customers who deploy Live Business Gateway in a vSphere environment include

- **Reduced capital expenditure:** Consolidation of Live Business Gateway as part of a virtual infrastructure enables businesses to further optimize server use. Dedicated physical servers (or appliances) are no longer required for Live Business Gateway deployments.
- **Reduced operation and maintenance costs:** Integration of Live Business Gateway within the fabric of vSphere virtual infrastructure management enables the solution to be managed cohesively alongside other virtualized business applications, further integrating IT processes and reducing maintenance costs.

- **Reduced power consumption:** Businesses can take advantage of the inherent power savings of virtual environments enabled by vSphere server virtualization—reduced servers and vSphere Distributed Power Management.
- **Integrated business continuity:** Consolidating Live Business Gateway within the management framework of a virtual data center environment enables the solution to take advantage of integrated disaster recovery management available through vSphere virtualization. Management methodologies and best practices are consistently applied across all applications in the data center saving the IT department time and money.
- **Consistent feature set and licensing:** Live Business Gateway deployed in a vSphere environment offers the same feature set and maintains the same product licensing options as Live Business Gateway deployed on a physical server. Familiarity of the solution is maintained for Mitel authorized PARTNERS and end customers.

Live Business Gateway is a standalone application that runs on Windows OS versions. Live Business Gateway is not supplied as a Virtual appliance (vApp), however, Live Business Gateway has been qualified in a VMware vSphere environment using VMware vSphere ESX or ESXi 4.0, 4.1, and 5.0.

Details of how to deploy Live Business Gateway in a VMware vSphere environment are outside the scope of the Live Business Gateway product documentation. Please refer to the relevant VMware vSphere product documentation for information on deploying applications in vSphere environments.

VMware vSphere Management Tools

The following vSphere Management Tools from vCenter have been qualified with Live Business Gateway:

Power On, Shutdown Guest, Reset/Restart, and Snapshot

Live Business Gateway continues to function correctly when the virtual machine is rebooted or restarted by using the Power On, Shutdown Guest, Reset/Restart and Snapshot (Powered Off) management tools from vCenter.

Cloning

A clone is a copy of an existing virtual machine. The virtual machine on which Live Business Gateway is installed can be cloned using the vCenter management tool.



Note: The AMC license is linked with the hardware ID of the virtual machine. The vSphere application assigns a new hardware ID to the cloned machine that fails to synchronize the license from the AMC server. Live Business Gateway needs to re-register the AMC license on the cloned virtual machine.

Cold Migration

vSphere Cold Migration focuses on reducing the total-migration time. When cold migration occurs, the virtual machine stops executing any programs currently working and copies the current page table to the machine where the virtual machine migrates.



Note: The testing of cold migration has been limited to the same Host and Data store.

Health Monitoring and Performance Reports

Live Business Gateway is a standalone windows application and is not directly affected by health monitoring and performance reporting. Live Business Gateway qualification testing confirmed that no extra memory resources are used by Live Business Gateway when these tests are run.

Deploying Live Business Gateway Release 3.4 in a Microsoft Hyper-V Environment

Live Business Gateway is supported in a Microsoft Hyper-V environment, which enables voice and business applications to run together in a virtual environment. Live Business Gateway is able to take advantage of the improved performance, ease of use, and comprehensive management capabilities of data center virtualization.

The key benefits for customers who deploy Live Business Gateway in a Hyper-V environment include

- **Reduced capital expenditure:** Consolidation of Live Business Gateway as part of a virtual infrastructure enables businesses to further optimize server use. Dedicated physical servers (or appliances) are no longer required for Live Business Gateway deployments.
- **Reduced operation and maintenance costs:** Integration of Live Business Gateway within the fabric of Hyper-V virtual infrastructure management enables the solution to be managed cohesively alongside other virtualized business applications, further integrating IT processes and reducing maintenance costs.
- **Reduced power consumption:** Businesses can take advantage of the inherent power savings of virtual environments enabled by Hyper-V server virtualization—reduced servers and Distributed Power Management.
- **Integrated business continuity:** Consolidating Live Business Gateway within the management framework of a virtual data center environment enables the solution to take advantage of integrated disaster recovery management available through Hyper-V virtualization. Management methodologies and best practices are consistently applied across all applications in the data center saving the IT department time and money.
- **Consistent feature set and licensing:** Live Business Gateway deployed in a Hyper-V environment offers the same feature set and maintains the same product licensing options as Live Business Gateway deployed on a physical server. Familiarity of the solution is maintained for Mitel authorized PARTNERS and end customers.

Live Business Gateway is a standalone application that runs on Windows OS versions. Live Business Gateway is not supplied as a Virtual appliance (vApp), however, Live Business Gateway has been qualified in a Microsoft Windows Server 2008 R2 Hyper-V environment.

Details of how to deploy Live Business Gateway in a Hyper-V environment are outside the scope of the Live Business Gateway product documentation. Please refer to the relevant Microsoft Hyper-V product documentation for information on deploying applications in Hyper-V environments.

Microsoft Hyper-V Management Tools

The following Hyper-V Management Tools have been qualified with Live Business Gateway:

- Shutdown Guest
- Save
- Pause
- Reset
- Snapshot
- Live Migration

Offline License Activation

Complete these steps *only* if your online license activation has failed:



Note: You will need an Internet-connected workstation and a compatible portable storage medium (diskette, memory key, etc.) to download the license file.

1. When prompted to continue with removable media, click **Yes**. The Create Disk window opens.
2. Insert the storage medium, enter the destination drive, and then click **OK**. Live Business Gateway creates a Manual Sync disk.
3. When disk has been created, remove the storage medium and take it to an Internet-connected workstation.
4. Click **Start>Run** to open the command prompt window and type **cmd**. At the command prompt, type **ManualSync.bat**. Executing this file opens communication with the AMC and downloads your licensing files to the storage medium.
5. Remove the storage medium and return to the workstation where you installed Live Business Gateway.
6. At the prompt, insert the storage medium and click **OK**. The license files are copied to your system.
7. Click the **Live Business Gateway** tab and click **Start**. Live Business Gateway is started.



Note: Live Business Gateway does not communicate with MCD until the Lync client logs in.

Disabling Service Failure Recovery

Live Business Gateway service will restart automatically upon error.

To disable system recovery

1. In Control Panel, select **Administrative Tools**.
2. Double click **Services**.

3. In the Detail pane, Right-click the **Mitel Live Business Gateway** service and click **Properties**.
4. On the **Recovery** tab, select **Take No Action** for the First failure, Second failure and Subsequent failures options.

Upgrading Live Business Gateway Software and Licenses

To register new licenses

1. In Control Panel, click **Live Business Gateway**.
2. On the **Licensing** tab, in the **ServiceLink ID** field, enter the Application Record ID that applies to the Live Business Gateway installation.
3. Click **Update License**. Live Business Gateway synchronizes with the AMC and your new licenses are registered.



Note: Live Business Gateway does not communicate with MCD until Lync client logs in.



Note: Live Business Gateway Release 3.4 does not support Mitel Standard Linux (MSL). If you are upgrading from an earlier version of Live Business Gateway, use the MSL to Windows conversion utility to migrate your data to the Live Business Gateway Windows version. See "Migrating MSL Configuration Files to Windows".

Before You Begin

Before you begin to upgrade LBG you must verify the

- Live Business Gateway service is stopped (AppGW.exe is not running in Task Manager)
- Live Business Gateway Control Panel applet is NOT displayed (that is, the Mitel Networks Live Business Gateway icon does not appear in the Task Bar)
- Log Viewer Tool is **not** running (LogView.exe is not listed as running in Task Manager)



Note: Upgrades do not overwrite existing Live Business Gateway configurations.

Upgrading Live Business Gateway Software

To upgrade the software

1. Download the software from Mitel OnLine. (See page 16 for download instructions.)
2. If a previous version of Live Business Gateway exists, you are prompted to upgrade the current installation.



Note: An upgrade does not overwrite existing Live Business Gateway configurations.



Note: If you are upgrading within a release, you are prompted to modify, upgrade, or remove. You will need to remove the old version and install the new software. You can backup your Live Business Gateway switch configuration by copying "ICP_config.txt and gwcert.pem, cacert.pem and gwkey.pem from C:\Program Files\Mitel Networks\Live Business Gateway\Service; once installation is completed copy these files back to the directory. You will need to reconfigure your Licensing, Active Directory and Digit Mod tabs.



Note: If you are upgrading from Live Business Gateway Release 3.3 to 3.4, the Number of Log Files and Size of Each File (KB) settings on the Live Business Gateway settings Log tab will be set to 5 and 10240 respectively. You can modify these values.

3. Click **Yes** to upgrade or **No** to cancel.
4. When the upgrade is complete, the Live Business Gateway Settings window appears.
5. On the Live Business Gateway tab, click **Start** to start Live Business Gateway.
6. When the Installation Completion window appears, click **Finish**.



Note: If Live Business Gateway is upgraded on a virtual machine, then you need to re-sync the application since the upgrade does not recognize the licensing data from the previous version. Click the **Update License** button on the Licensing tab to re-sync the licenses.

Upgrading Live Business Gateway Licenses

To add user licenses

1. Contact Mitel Customer Services or your Distributor and place your order using the part numbers provided in Table 5. The ordered products are added to your AMC License account.
2. In your AMC account, access the Application Record that applies to this Live Business Gateway server. Assign the upgrade licenses from your License account to the Application Record. The AMC updates your licenses on its hourly synchronization. You can force an immediate synchronization using the Live Business Gateway Control Panel applet.

To manually synchronize the license update

1. In Control Panel, click **Live Business Gateway**.
2. On the **Licensing** tab, in the **ServiceLink ID** field, enter the Application Record ID that applies to this Live Business Gateway installation.
3. Click **Update License**. Live Business Gateway synchronizes with the AMC and the new license is registered.



Note: If there is no Internet connection, Live Business Gateway prompts you to follow the manual synchronization process.

Table 5: Live Business Gateway Part Numbers

Part Number	Description	Notes
54002580	Live Business Gateway Windows version	Every Live Business Gateway deployment must have this base level of service. Includes 40 user licenses.
54002584	Live Business Gateway Demo kit Windows version	Includes 10 user licenses
54002210	Live Business Gateway 10 user licences	Enables additional user licenses (in packs of 10) to be added to part number 54002580 or 54002584



Chapter 3

Security Certificates for TLS

Creating a Security Certificate for Live Business Gateway

Live Business Gateway does not communicate with MCD until the Lync client logs in. The SIP interface between Lync Server 2010 and Live Business Gateway is secured by Mutual TLS which requires that security certificates be created. You need a certificate for Live Business Gateway. We recommend you use the same Certificate Authority (CA).



Note: When you select *Mutual TLS*, ensure you also select *TLS* in the Lync client.

Prerequisites

- Download the certificate configuration document available at www.microsoft.com for certificate creation instructions. This configuration procedure involves adding a certification authority snap-in using Management Console (MMC).
- Download the *Windows Server 2003 PKI Operations Guide* at <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03pkog.mspx> for instructions on how to install and manage a Certificate Authority.
- Ensure Certificate Services is installed on a workstation running Windows Server 2003, Windows Server 2003 R2 (SP2), or Windows Server 2008 R2. Certificate Services is an optional service. You can use the Add/Remove program in Control Panel to add this service.
- Ensure that Certificate Services is installed on a Windows Server 2003, Windows Server 2003 R2 (SP2), or Windows Server 2008 R2 server that can be contacted by the workstation running Live Business Gateway.

Requesting the Live Business Gateway Certificate (Windows Server 2008 R2 Workstations)

1. On the Live Business Gateway Windows 2008 R2 workstation, launch Internet Explorer.
2. Enter the Certificate Service location in the address field using the format **http://<name of the PC where the Certificate Services server is>/certsrv**. (For example, <http://10.30.40.50/certsrv>.)
3. Click **Request a certificate**.
4. Click **Advanced certificate request**.
5. Click **Create and submit a request to this CA**.
6. Choose **one** of the following options:
 - If the CA does *not* use templates, follow the instructions in Step 7.
 - If the CA uses templates, follow the instructions in Step 8.
7. Complete the required information on the form. Note the following information fields:
 - After **Name**, type the FQDN of Live Business Gateway. For example `workstation_name.mitel.com`. This must be the same FQDN of Live Business Gateway that was entered during the installation procedure. You must be able to ping the FQDN from the Certificate Services server.



Note: When you select *Mutual TLS*, ensure you also select *TLS* in the Lync client.



Note: If you selected *TCP* on the Live Business Gateway tab, the following steps are not required.

- After **Type of Certificate Needed**, select **Other**.
 - After **OID**, type **1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.3**. In this step, you are specifying both the Client Authentication Certificate and the Server Authentication Certificate.
 - After **Key Options**, select **Create new key set**.
 - After **Key Usage**, select **Both**.
 - Select the following
 - Automatic key container name
 - Mark keys as exportable
8. Complete the required information on the form. Note the following information fields:
- Select the **Subordinate Certification Authority** template.
 - After **Name**, type the FQDN of Live Business Gateway. For example `workstation_name.mitel.com`. This must be the same FQDN of Live Business Gateway that was entered during the installation procedure. You must be able to ping the FQDN from the Certificate Services server.
 - After **Key Options**, type **Create new key set**.
 - After **Key Usage**, select **Both**.
 - Select the following
 - Automatic key container name
 - Mark keys as exportable
9. Click **Submit**.
10. On the workstation with the Certificate Service, use MMC to open the certificate console.
11. Click **Certification Authority**.
12. Browse to the **Pending Requests** folder and select it.
13. Right-click the **Certificate Request**, and select **All Tasks>Issue**.

The certificate is then issued. You can verify it was issued by opening the **Issued Certificates** folder and locating the certificate.

Downloading the LBG Certificate (on Windows Server 2008 R2 Workstations)

1. On the Live Business Gateway Windows Server 2008 R2 workstation, launch Internet Explorer.
2. Enter the Certificate Service location in the address field using the format **http://<name of the PC where the Certificate Services server is>/certsrv** (for example, `http://10.30.40.50/certsrv`).

3. Click **View the status of a pending certificate request**.
4. Click **Install this certificate**. You will be prompted to download the root certificate from the CA. The certificate will be stored in the **Trusted Root Certification Authority** folder with **Issued To** as the CA name.
5. In **MCC**, open **Certificates Snap-in** on the Live Business Gateway Server.
6. Click **Personal>Certificates** to open the **Certificates** folder. The folder contains certificates recently requested.
7. Right-click **Certificate** and select **All Tasks>Export**.
8. In the **Certificate Export Wizard**, click **Yes, export the private key**.
9. Under **Export File Format**, click **Next** to accept the default settings.
10. Enter **"test"** for the password to encrypt the private key you are exporting.
11. Confirm the password, and click **Next**.
12. After **File Name**, type a file name (gwkey.pfx), specify the path for the PKCS #12 file used to store the exported certificate and private key, and click **Next** and **Finish**.
13. Locate the certificate again, right-click it and select **All Tasks>Export**. To verify the certification was successful, locate it in the **Issued Certificates** folder.
14. In the **Certificate Export Wizard**, click **No, do not export the private key**, and click **Next**.
15. Select the **Base 64 Encoded X.509(Cer.)** file and save it as **gwcert.cer**.
16. In **MMC**, locate the **Trusted Root Certification Authority>Certificates** folder.
17. Right-click the **CA root certificate**.
18. Click **All Tasks>Export**.
19. Select the **Base 64 Encoded X.509(Cer.)** file format.
20. Save the file as **cacert.cer**.
21. Rename the **cacert.cer** and **gwcert.cer** files as **cacert.pem** and **gwcert.pem** respectively.
22. Download and install OpenSSL1.0.
23. Enter the following command in **OpenSSI** to extract the private key from the **gekey.pfx** file.


```
openssl pkcs12 -in <PFX_FILE> -nocerts -nodes -out <PEM_KEY_FILE>
```
24. Enter **"test"** as the password while executing this command.
25. Copy **gwcert.pem**, **cacert.pem** and **gwkey.pem** to the Service directory of the Live Business Gateway Server (**C:\Program Files\Mitel Networks\Live Business Gateway\Service**).

Requesting the LBG Certificate (on Windows Server 2003/2003 R2 (SP2) Workstations)

1. On the Live Business Gateway Windows Server 2003/2003 R2 (SP2) workstation, launch Internet Explorer.
2. Enter the Certificate Service location in the address field using the format **http://<name of the PC where the Certificate Services server is>/certsrv** (for example, http://10.30.40.50/certsrv).
3. Click **Request a certificate**.
4. Click **Advanced certificate request**.
5. Click **Create and submit a request to this CA**.
6. Choose **one** of the following options:
 - If the CA does *not* use templates, follow the instructions in Step 7.
 - If the CA uses templates, follow the instructions in Step 8.
7. In the form, enter the required information. Note the following information fields:
 - After **Name**, type the FQDN of Live Business Gateway. For example workstation_name.mitel.com. This must be the same FQDN of Live Business Gateway that was entered during the installation procedure. The FQDN must also be ping-able from the Certificate Services server.
 - After **Type of Certificate Needed**, select **Other**.
 - After **OID**, type **1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.3**. In this step, you are specifying both the Client Authentication Certificate and the Server Authentication Certificate.
 - After **Key options**, select **Create new key set**.
 - After **Key Usage**, select **Both**.
 - Select the following
 - Automatic key container name
 - Mark keys as exportable
 - Export keys to file
 - After **Full path name**, type **gwkey.pvk**
 - Select **Store certificate in local computer certificate store**.
 - Proceed to Step 9.
8. In the form, enter the required information. Note the following information fields:
 - Select a template with the correct properties (as listed in Step 7).
 - After **Name**, type the FQDN of Live Business Gateway. For example workstation_name.mitel.com. This must be the same FQDN of Live Business Gateway that was entered during the installation procedure. The FQDN must also be ping-able from the Certificate Services server.
 - After **Key options**, type **Create new key set**.
 - After **Key Usage**, select **Both**.

- Select the following
 - Automatic key container name
 - Mark keys as exportable
 - Export keys to file
 - After **Full path name**, type **gwkey.pvk**.
 - Select **Store certificate in local computer certificate store**.
9. Click **Submit**.
 10. In the window that asks you to confirm that you want to request a certificate now, click **Yes**.
 11. In the window that asks you to confirm that you want to create a private key gwkey.pvk, click **Yes**.
 12. If you are requesting an additional certificate or if gwkey.pvk already exists in the local directory a window displays that asks you if you wish to overwrite the private key gwkey.pvk. Click **Yes**.
 13. In the **Create Private Key Password** window, enter "**test**" as the password, confirm it, and click **OK**.

This places the private key (gwkey.pvk) in your selected directory on the workstation. Now that you have created the certificate, you must issue it.
 14. Browse to the Windows Server 2003, Windows Server 2003 R2 (SP2), or Windows Server 2008 R2 server with the Certificate Service and use MMC to open the certificate console.
 15. Click on **Certification Authority**.
 16. Browse to the **Pending Requests** folder and select it.
 17. Right-click the Certificate Request, and select **All Tasks>Issue**.

The certificate is now issued. You can verify that the issue was successful by opening the **Issued Certificates** folder and ensuring the requested certificate is listed.

Downloading the LBG Certificate (on Windows Server 2003/2003 R2 (SP2) Workstations)

1. Browse to the URL of the Certificate Service (for example, <http://<name of the PC where the Certificate Services server is>/certsrv>).
2. Click **View the status of a pending certificate request**.
3. Click the certificate request link to be viewed.
4. Select **DER encoded**.
5. Click **Download certificate chain**.
6. Save the certificate chain in a local directory.

Converting Certificates to PEM

The CA Certificate and the Live Business Gateway Certificate are created in different formats. In order for the certificates to communicate with each other, you must convert the format of the CA Certificate to the Live Business Gateway Certificate format, Privacy Enhanced Mail (PEM). PEM is an Internet Engineering Task Force (IETF) standard for secure e-mail that is defined in RFC 1421 through 1424. The PEM format is used for encoding certificates and keys in ASCII text.

1. Locate the certificate chain file you saved in the "Download the Certificates" procedure and double-click it.
2. Browse to the **Certificates** folder.
There are two certificates: the Live Business Gateway certificate and the Certificate Authority certificate. The certificates are identified in the **Intended Purposes** column.
3. Right-click the Live Business Gateway certificate and select **All Tasks>Export**.
The Live Business Gateway Certificate name must be the same as the FQDN of the Live Business Gateway workstation.
4. In the Welcome window, click **Next**.
5. Select **Base-64 encoded X.509 (CER)** and click **Next**.
6. Browse to a local directory and save the file as **gwcert**. The file is saved as gwcert.cer.
7. Click **Next**.
8. Click **Finish**. The window displays "The export was successful".
9. Click **OK**.
10. Browse to where you saved the gwcert.cer file.
11. Rename the file to **gwcert.pem**.
12. Confirm that you want to change the extension by clicking **Yes**.
13. Return to the **Certificates** folder that you accessed in Step 2.
14. Right-click the Certificate Authority certificate and select **All Tasks>Export**. The CA certificate name is the name chosen by the CA.
15. Select **Base-64 encoded X.509 (CER)** and click **Next**.
16. Browse to a local directory and save the file as **cacert**. The file is saved as cacert.cer.
17. Click **Next**.
18. Click **Finish**. The window displays "The export was successful".
19. Click **OK**.
20. Browse to where you saved the **cacert.cer** file and rename the file to **cacert.pem**
21. Confirm that you want to change the extension by clicking **Yes**.



Note: If you un-install the Live Business Gateway software the certificate files will be lost. We strongly recommend you back them up now.

Converting gwkey.pvk to PEM

The Certificate key gwkey.pvk file is stored in an encoded format. This format needs to be converted to an encoded format, such as Privacy Enhanced Mail (PEM), that Live Business Gateway can understand.

Accessing the gwkey.pvk File

To access the file

1. Copy the gwkey.pvk file to **C:\Program Files\Mitel Networks\Live Business Gateway Edition\Tools**.
2. Click **Start>Run** to open a command prompt window.
3. Type **cmd** and click **OK**.
4. In the command prompt window, type **cd** to change to the directory where you stored the file (for example, **cd C:\<path to the file>**).
5. At the prompt, type **pvk -in gwkey.pvk -out gwkey.pem**.
6. Enter "**test**" for the password.
7. When you are prompted for the PEM passphrase, type **test** again. The gwkey.pem is stored in the Tools directory.
8. When asked to verify the passphrase, type **test** again.

Installing the Certificates and the Key

To install the certificates and the key

1. Copy **gwcert.pem**, **cacert.pem** and **gwkey.pem** to the Service directory of the Live Business Gateway Server (**C:\Program Files\Mitel Networks\Live Business Gateway\Service**).
2. In **Control Panel**, double-click the Live Business Gateway icon to open the applet.
3. Select the **Live Business Gateway** tab and click **Stop**.
4. Select the **TLS** check box.
5. In the **SIP Port** field, enter the same TLS port as the Lync Server 2010 port. (Default is 5061)
6. Click **Start** to restart Live Business Gateway for the changes to take effect.



Note: Ensure that you have installed the certificates in Lync Server 2010 *and* in the Lync clients. (Refer to the documents listed in "Creating a Security Certificate for Live Business Gateway" on page 35.)

Migrating MSL Configuration Files to Windows



Note: Live Business Gateway Release 3.2 or greater does not support MSL. If you are upgrading from an earlier version of Live Business Gateway, use the MSL to Windows (MslToWin) conversion utility to migrate your data to the Live Business Gateway Windows version.

MslToWin is a Win32 DOS-based exe file that uses the appgw.ini conversion file to generate three files compatible with Windows:

- ICP_config.txt
- line_store.txt
- micc_config.txt

Migrating MSL Configuration Files



Note: Use WinSCP or another open source utility to copy files securely from the MSL server to the Live Business Gateway server.

Migrating Data Using Text Console

To migrate data

1. Install Live Business Gateway Release 3.2 or greater.
2. Access Text console.
3. Log on to the MSL server as "**root**" and type the administrator password.
4. At the **command prompt**, type **/etc**.
5. In the **etc** directory, locate the **appgw.ini** file and copy it to **C:\Program Files\Mitel Networks\Live Business Gateway\Tools**.
6. Click **Start>Run** to open a command prompt window.
7. Type **cmd** and click **OK**.
8. In the **command prompt** window, type **cd** to change to the directory where you stored the file (for example, **cd C:\<path to the file>**).
9. At the prompt, type **msltowin appgw.ini** and press **Enter**.
10. Locate the **ICP_config.txt**, **line_store.txt** file and the **micc_config.txt** file and copy and paste them to **C:\Program Files\Mitel Networks\Live Business Gateway\Service** to overwrite the existing files.
11. On the **Live Business Gateway Windows Server**, locate the **Live Business Gateway** tab in the Control Panel applet and change the IP address of the MSL server.

Migrating Data Using WINSXP

To migrate data

1. Browse to **<http://winscp.net/eng/download.php#download2>** to obtain WINSXP and install it on a computer running Windows.
2. Open WINSXP.
 - Type the host name/IP address and select **Port 22**.
 - Log on to the MSL server as "**root**", type the administrator password, and click **Login**.
3. In the right pane, double-click the "up one level" icon to access the root directory.
4. In the left pane, open the "**ect**" folder and locate the **appgw.ini** file.
5. Copy and paste the **appgw.ini** file to **C:\Program Files\Mitel Networks\Live Business Gateway\Tools** on the Live Business Gateway Windows server.
6. On the Live Business Gateway Windows server, click **Start>Run** to open a command prompt window, change the directory to **C:\Program Files\Mitel Networks\Live Business Gateway\Tools** and enter the following command:

msitowin "C:\Program Files\Mitel Networks\Live Business Gateway\Tools\Appgw.ini"

7. Copy the **ICP_config.txt**, **line_store.txt**, and **micc_config.txt** file from **C:\Program Files\Mitel Networks\Live Business Gateway\Tools** to **C:\Program Files\Mitel Networks\Live Business Gateway\Service**.
8. If you are prompted to overwrite existing files, select **Yes**.



Chapter 4
Troubleshooting

Diagnosing Problems

Use the following table to identify possible usability issues and their solutions. Mitel Technical Support may ask you to enable logs using the Live Business Gateway Log Viewer Tool when they diagnose problems.



Note: To view all of the logs, you must start the log viewer tool *before* you start Live Business Gateway.

Table 6: Possible Usability Issues and Solutions

Error Description	Problem	Action
<p>The log file size and number of log files are insufficient to gather a complete set of data.</p>	<p>Need to capture all data to troubleshoot issues Need to increase the number of log files generated and their capacity to capture all data</p>	<p>Note: If you are installing Live Business Gateway for the first time, or if you are upgrading from Live Business Gateway Release 3.3 to 3.4, the default settings for Number of Log Files and Size of Each File (KB) are set to 5 and 10240 respectively.</p> <ol style="list-style-type: none"> 1. In Control Panel, click Live Business Gateway. 2. On the Log tab, after Number of Log Files, type a numerical value between 2 and 10. Do not leave the field blank or your entry will be rejected. 3. After Size of Each File (KB), type a numerical value between 10240 and 102400 and click OK. Do not leave the field blank or your entry will be rejected.

Table 6: Possible Usability Issues and Solutions (continued)

Error Description	Problem	Action
<p>The Lync client interface displays a phone icon with a red exclamation mark (!) within a yellow warning sign:</p> <ul style="list-style-type: none"> • in the upper right- hand corner for Office Communicator 2007 • In the bottom left-hand corner for Lync <p>Placing the cursor over this icon displays the following: <i>Lync is not properly configured to make phone calls.</i></p>	<p>The Phone integration icon is displayed on the Lync client after logon.</p>	<p>Lync Server 2010 static routing to Live Business Gateway</p> <ol style="list-style-type: none"> 1. Confirm Lync Server 2010 static routing to Live Business Gateway. 2. Confirm that Active Directory User Account is programmed. For more information, refer to “Verifying the User Account in Active Directory” on page 56. 3. Confirm that PC is a "trusted" PC with the appropriate certificates installed. 4. Confirm that the client extension has the correct COS options enabled. 5. Confirm that client registry edits are entered correctly. 6. Confirm the client is enabled for phone integration and either the automatic option is selected or the correct manual configuration is entered. 7. Confirm that the date and time of MCD is in synch with the Live Business Gateway workstation and that they are displaying the correct time. 8. Confirm that rules are added to any firewall to allow communication between the Office Business Gateway and Lync Server 2010 or MCD.
<p>The Lync client interface displays a phone icon with a red exclamation (!) at the bottom right hand corner.</p>	<p>The user cannot make calls to MCD phones using the Lync client.</p>	<p>This indicates that there is no communication with Live Business Gateway. Perform the following actions:</p> <ol style="list-style-type: none"> 1. “Verifying the MCD Address” on page 55 2. “Verifying Live Business Gateway Is Running” on page 55 3. “Verifying the User Account in Active Directory” on page 56 4. Log out of the Lync client. Enable the logs in the Log Viewer Tool. Attempt to make a call from the Lync client and capture the log. (For more information, refer to “Using the Log Viewer Tool (MSPLogs.exe)” on page 53.)

Table 6: Possible Usability Issues and Solutions (continued)

Error Description	Problem	Action
<p>The following error message is displayed: <i>Cannot perform the selected action. Your phone service may be experiencing temporary difficulties, or the action may not be supported by your phone system. Please try again.</i></p>	<p>The user is not notified that an extension is Out of Service when making call.</p> <p>The user gets error message when calling a phone in Do Not Disturb (DND) mode.</p> <p>The user has dialed incorrectly.</p>	<p>This is Lync client designed behavior and does not indicate a fault in the phone system operation.</p>
<p>The following error message is displayed: <i>An error occurred while trying to take the call off Hold. Please try again. If the problem persists, contact your system administrator.</i></p>	<p>The user cannot cancel Call Transfer by hanging up.</p>	<p>This is Lync client designed behavior and does not indicate faulty operation. The transfer has occurred. Disregard this message.</p>
<p>The following error message is displayed: <i>An error occurred while trying to place the call on Hold. Please try again. If the problem persists, contact your system administrator.</i></p>	<p>During a call, two callers place each other on hold and are unable to resume their conversation.</p>	<p>This is Lync client designed behavior and does not indicate faulty operation.</p> <p>Two callers cannot put each other on hold and then resume their conversation using the Lync client conversation window.</p>
<p>When a twinned phone answers a Lync client call, the twinned phone call features are disabled.</p>	<p>When the Lync client is integrated with Mitel Unified Communicator Mobile service the Unified Communicator Mobile twinned phone call features are disabled.</p>	<p>This is Lync client designed behavior and does not indicate faulty operation.</p>
<p>When a user attempts to display audio controls, the following error message is displayed "Closing Audio controls will stop all voice conversations in this window. Are you Sure you want to close Audio Controls?"</p>	<p>The user cannot display audio controls during a call.</p>	<p>This is Lync client designed behavior and does not indicate faulty operation.</p>
<p>Page 3 of 6</p>		

Table 6: Possible Usability Issues and Solutions (continued)

Error Description	Problem	Action
<p>The following error message is displayed: <i>An error occurred while trying to answer the call. Your phone may be off the hook or your phone service may be experiencing difficulties. Please answer the call manually. If the problem persists, contact your system administrator.</i> <i>Call ended.</i></p>	<p>If a user Camps On two callers, no icons are displayed for control of the second call. The user cannot put the caller on hold or hang up because the icons are disabled. The user cannot Camp On more than one call.</p> <p>The user establishes a conference call between a number of callers. When user tries to leave the conference (presses Hangup), a message indicates that the call has been ended.</p>	<p>This is Lync client designed behavior and does not indicate faulty operation.</p> <p>If you Camp On more than one call at a time, this message is displayed. To disconnect this type of call use Cancel or place the receiver onhook and close the conversation window.</p> <p>Although user receives message that the call is ended after cancelling conference call, the conference call is still in progress.</p>
<p>The following error message is displayed: <i>Cannot end the call. Please click Hang Up again or disconnect the call manually at the phone. If the problem continues, please contact your system administrator.</i></p>	<p>The user has attempted to hang up with a call on hold in a Lync client conversation window.</p> <p>The user has used the Lync client to hang up when dialed into Voice Mail.</p>	<p>This is Lync client designed behavior and does not indicate faulty operation.</p> <p>Do not use the Lync client to hang up this type of call; use Cancel or place the receiver onhook.</p>
<p>The Lync client displays "Online" when the user has placed the phone in Do Not Disturb (DND) via a feature access code (FAC)</p>	<p>The user logged into the Lync client activates DND on phone via FAC but status window indicates user is in online mode.</p>	<p>This is Lync client designed behavior and does not indicate faulty operation.</p> <p>The Lync client displays both phone status and online status. Users must remember to place themselves back into online mode when appropriate.</p>
<p>Calls which recall from Call Hold are automatically answered</p>	<p>Callers are placed on Hold and time-out and recall to a Lync client. These calls are automatically answered by the user who placed them on hold.</p>	<p>This is Lync client designed behavior and does not indicate faulty operation.</p> <p>Increase the Call Hold recall timer in the COS for Lync clients.</p>
<p>When calls from more than one MCD are conferenced, the users on one MCD cannot see users dialed in to the conference from other MCDs.</p>	<p>Conference calls involving more than one MCD do not display all the users correctly</p>	<p>This is Lync client designed behavior and does not indicate faulty operation.</p>
<p>Problems with the use of Split or Trades soft keys when on conference call</p>	<p>When Split or Trades soft keys are used, user cannot make or receive calls.</p>	<p>If this behavior happens, return control of the phone to the desktop client by logging in and out of the Lync client.</p>
<p>Page 4 of 6</p>		

Table 6: Possible Usability Issues and Solutions (continued)

Error Description	Problem	Action
The names of users are not updated when a call is transferred to another network	When a user is transferred to another party on a remote MCD, The Lync client display is not updated to display the new user.	This is Lync client designed behavior and does not indicate faulty operation.
The Lync client displays the calling party number instead of name	The calling party Lync client shows the name of the called party but the called party Lync client displays the number of the calling party.	The calling party name is only displayed if the calling party is included in the called party's contact list.
The settings on phone and the Lync client are not in sync	Interaction of features enabled or disabled by the Lync client and then enabled or disabled on the desktop phone device may cause these features to be out of sync.	This is Lync client designed behavior and does not indicate faulty operation. To avoid this problem, do not use multiple devices to set and disable features.
Private numbers displayed in Call Announcement display	When the MCD Privacy release option is enabled, the caller number is displayed in the Call Announcement display.	This is Lync client designed behavior and does not indicate faulty operation.
The Lync client does not provide a popup for call answer when in DND	The user has placed their device in DND using the Lync client. A caller presses Ring Anyway. The device in DND rings but the Call Announcement display is not displayed to answer the call.	This is Lync client designed behavior and does not indicate faulty operation. Use discretion when assigning users the Executive Busy Override option in their COS (which enables them to override DND).
The Lync client does not pop up an incoming call alert window	Client has phone integration but does not have a pop-up when there is an incoming call	<p>If you have Live Business Gateway Release 3.2 or earlier</p> <ol style="list-style-type: none"> 1. Confirm the Live Business Gateway servers do not have multiple NICs. Live Business Gateway Release 3.2 or earlier supports only servers with a single NIC enabled. If multiple NICs exist then you should disable them in the Bios or in the Windows O/S. 2. Confirm Lync Server 2010 is ping-able from the Live Business Gateway PC. 3. Confirm that firewall rules are added (if applicable) between the Lync client and Lync Server 2010.

Table 6: Possible Usability Issues and Solutions (continued)

Error Description	Problem	Action
A user cannot retrieve a call after transferring to second party who does not answer	The user transfers a call to a second party by Right-clicking on the second party's user name and selecting "Call". This puts the call on hold but if the second party does not answer, the user is unable to retrieve the held call using the Lync client window. If the user hangs up, a blind transfer is made.	This is Lync client designed behavior and does not indicate faulty operation.
The Lync client window does not list entire phone number	If a call is made on a Lync Server 2010-monitored phone and the digits before outpulsing are set to the default of 4, then only the first four digits are shown in the Lync client window.	If you specifically state the number of digits to follow or set it to blank in ARS, then the entire number is displayed.
Office Communicator indicates "Online" while in a call after a Callback matures	A user has initiated a call to a busy phone using the Lync client and then activated a Callback message via their Mitel phone. The Callback has matured, provided triple ring-back and the call has been established.	This is Lync client designed behavior and does not indicate faulty operation.
Lync presence awareness not updated for Group Pickup phones using FAC to answer calls	When a Lync client ('A') calls a member of a Pickup Group ('B'), and 'B' picks up the call using FAC on another member phone (C), the Lync display for 'C' does not indicate that it is in a call. Other clients with 'C' as a contact do not show that it is in a call.	This is Lync client designed behavior and does not indicate faulty operation.
The Lync client displays an error message when attempting to hang up on voice mail	If a Lync client is used to hang up on voice mail while the hang-up option is not available, it receives the following error message: "Cannot end the call. Please click Hang Up again, or disconnect the call manually at the phone. If the problem persists, contact your system administrator."	Do not use Lync to hang up.

Using the Log Viewer Tool (MSPLogs.exe)

The log viewer tool is a Windows-compatible utility that records information in two log files that contain error and warning information:

- appgw.log (Live Business Gateway server logs)
- appgwcpl.log (Control Panel logs)

When you install your Live Business Gateway two directories are created by default in C:\Program Files\Mitel Networks\Live Business Gateway:

- **Logs:** contains a log file created by MSPLogs.exe
- **Service:** contains the software files required to execute Live Business Gateway



Note: You must manually install the MSPLogs.msi file.

The log file contains the following information:

- A record of the messages sent to and received from Lync Server 2010
- Error and warning information
- Live Business Gateway status information

To access the Log Viewer tool from Windows installations

1. Navigate to **C:\Program Files\Mitel\MSPLogs**.
2. Double-click **MSPLogs.exe**. From this point in time forward, all logs are displayed in this view. To view previous logs, select **File>Connect to MSPLogfile**.
3. Browse to the **Logs** folder in the Live Business Gateway directory.
4. Do one of the following:
 - To view Live Business Gateway server logs, select **appgw.log**.
 - To view Control Panel logs, select **appgwcpl.log**.

The maximum log file size is 10 Megabytes. When the size limit is exceeded, the log is backed up and renamed (for example, appgw.log.1). A maximum of five renamed/backed up files can be stored. You can change the default logging level of "Errors/Warnings" on the **Log** tab of the Live Business Gateway interface.

Error Reporting Utility

Live Business Gateway Release 3.4 and greater has an error reporting utility that can send e-mail alerts to the System Administrator when certain critical errors are logged on the server.

The System Administrator first needs to configure the error reporting utility for the e-mail alerts.



Note: The e-mail alerts can be enabled or disabled in the error reporting utility.

The following fields need to be configured in the Error Reporting tab:

- **Email ID:** The e-mail address of the Live Business Gateway System Administrator.
- **Password:** The password of the Live Business Gateway System Administrator e-mail account.
- **SMTP:** The SMTP server name where the Live Business Gateway System Administrator e-mail account is registered.
- **Port:** The port number on which the SMTP server will communicate with the Live Business Gateway.
- **Encryption Type:** The encryption details that are used to connect with the SMTP server.
- **Subject:** The title that will be used for the e-mail alert.
- **Recipients:** The e-mail address(es) of the e-mail alert recipient(s). Multiple recipients must be separated by a semi-colon.
- **Errors:** The type of error to include in the e-mail alert. Various error types can be added to the watch list from the drop-down list.

Troubleshooting Procedures

Configure a test user account to use when you monitor or control a phone for troubleshooting purposes. For more information, refer to the following procedure.



Note: Live Business Gateway does not support the monitoring of ACD agents.

Configuring a Prime Line Phone in Live Business Gateway

Live Business Gateway uses Active Directory user accounts to authorize users on MCD but, for test purposes, it can also use a local configuration file, **line_store.txt**, to authorize users and to obtain configuration information.



Note: Update the line_store.txt file only if a user's information has *not* been added to Active Directory.

If it is necessary to update the line_store.txt file, use the following procedures:

Windows Installations

1. Disable Live Business Gateway.
2. Navigate to **C:\Program Files\Mitel Networks\Live Business Gateway\Service**
3. Open line_store.txt with any text editor. The following fields are displayed:
 - **ESM-Password:** provided during Live Business Gateway installation. Change this value through the Live Business Gateway applet in Control Panel only.
 - **ESM-User Name:** provided during Live Business Gateway installation. Change this value through the Live Business Gateway applet in Control Panel only.
 - **ICP-IP Address:** provided during Live Business Gateway installation. Change this value through the Live Business Gateway applet in Control Panel only.

- **lines-start/lines-end:** The lines between "lines-start" and "lines-end" define prime line phone information and the associated user.

The following example illustrates the line_store.txt file.

```
ARX-leading-digits    9
ESM-Password mitel
ESM-UserName          AppAdmin
ICP-IP-address 10.37.129.20

lines-start
tel:***:phone-context=pbx1.mitel.com test@ottawa.mitel.com
lines-end
```

4. Insert the phone and user information between "lines-start" and "lines-end" using one of the following example formats:
 - **tel:3005;phone-context=pbx1.mitel.com simon@ottawa.mitel.com:** this format indicates that MCD with FQDN pbx1.mitel.com and local phone with prime line number 3005 can be monitored and controlled by simon.
 - **tel:+12356344;ext=3006john@ottawa.mitel.com:** this format indicates that MCD with local phone (with prime number 3006) can be monitored and controlled by John. +12356344 represents a E.164 standard global number.
5. If another phone is to be monitored and controlled by another user, repeat step 3 and add the new information between "lines-start" and "lines-end".

Verifying the MCD Address

To verify the MCD IP address

1. In the Live Business Gateway configuration interface, select the **ICP** tab.
2. Verify that the IP Address, ESM User Name and ESM Password are correct for the MCD being used.

Verifying Live Business Gateway Is Running

To verify Live Business Gateway is running

1. In the Live Business Gateway configuration interface, select the **Live Business Gateway** tab.
2. For Windows installations, verify that the **Stop** bar is displayed. If the Stop bar is displayed, Live Business Gateway is running. If the Start bar is displayed, press **Start**.

For additional details, consult the MCD online help in ESM (Maintenance and Diagnostics). Select Logs>Login/Logout Audit logs. Confirm that the application user name is logged in. To view the logs associated with Live Business Gateway, select the user login ID that matches the ICP Gateway Setting ESM user name.



Note: In Windows applications, you can also use Task Manager to confirm that the Live Business Gateway process (AppGW.exe) is running.

Verifying the User Account in Active Directory

To verify the User Account in Active Directory

1. Verify that each Lync client user has an account programmed in the Active Directory server. For more information on programming accounts, refer to the documentation at <http://www.microsoft.com/technet/prodtechnol/office/livecomm2005/default.aspx>
2. Verify that the fields defined in the Active Directory User Objects for each user are correct.

CSTA References

- Services for Computer Supported Telecommunications Applications (CSTA) Phase III, ECMA-269, 6th edition.
- XML Protocol for Computer Supported Telecommunications Applications (CSTA) Phase III, ECMA-323, 3rd edition.
- Web Services Description Language (WSDL) for CSTA Phase III, ECMA-348, 2nd edition.
- Extensible Markup Language (XML) 1.0, 3rd Edition, W3C Recommendation
- Simple Object Access Protocol (SOAP) 1.1, W3C
- Hypertext Transfer Protocol – HTTP/1.1, RFC2616, W3C Recommendation
- Session Initiation Protocol, RFC3261, IETF

Tel: +1(613) 592-2122 Tel: +1(480) 961-9000 Tel: +44(0)1291-430000 Tel: +1(613) 592-2122 Tel: +61(0) 2 9023 9500
Fax: +1(613) 592-4784 Fax: +1(480) 961-1370 Fax: +44(0)1291-430400 Fax: +1(613) 592-7825 Fax: +61(0) 2 9023 9501

FOR MORE INFORMATION ON OUR WORLDWIDE OFFICE LOCATIONS, VISIT OUR WEBSITE AT MITEL.COM/OFFICES

THIS DOCUMENT IS PROVIDED TO YOU FOR INFORMATIONAL PURPOSES ONLY. The information furnished in this document, believed by Mitel to be accurate as of the date of its publication, is subject to change without notice. Mitel assumes no responsibility for any errors or omissions in this document and shall have no obligation to you as a result of having made this document available to you or based upon the information it contains.

M MITEL (design) is a registered trademark of Mitel Networks Corporation. All other products and services are the registered trademarks of their respective holders.

© Copyright 2012, Mitel Networks Corporation. All Rights Reserved.

mitel.com

