

MITEL

Live Content Suite

Installation and Administrator Guide
Release 1.1



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 the Mitel Logo are trademarks of Mitel Networks Corporation.

Mitel Live Content Suite and UC Express are trademarks of Mitel Networks Corporation or its Licensors.

Windows and Microsoft are trademarks of Microsoft Corporation.

Adobe Acrobat Reader is a registered trademark of Adobe Systems Incorporated.

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

Mitel Live Content Suite Installation and Administration Guide
Release 1.1
June 2010

® Trademark of Mitel Networks Corporation
© Copyright 2010, Mitel Networks Corporation or its Licensors
All rights reserved

LIVE CONTENT SUITE INSTALLATION	3
Prerequisites.....	3
Hardware Requirements.....	4
Live Content Suite Application Overview.....	5
Initial Setup BEFORE You Install Live Content Suite.....	5
Live Content Suite Installation	6
Live Content Suite Configuration	13
Testing the Installation.....	30
Upgrading from Live Content Suite 1.0.....	30
Database Version	30
Key Programmers.....	30
Updating Configuration	31
Adding a new MCD Host	31
LIVE DESKTOP PORTAL ADMINISTRATION	34
Accessing Live Desktop Portal	34
System Settings.....	35
Permissions	35
Additional Links.....	56
Adding a Link	57
Editing a Link	58
Deleting a Link	58
Help Go-Link.....	59
Log Page	59
Changing Log Source	60
Downloading Log Files	61
Navigating Log Contents	62
Log Levels.....	62
Multi-User	63
Rollout.....	63
Select User	67
Selecting a User by Username	68
Selecting a User by DN	69
Permissions When Programming another User's Phone	70
Supporting Additional Languages.....	70

Backup and Restore	72
Backup	72
Restoring Live Content Suite	74
System Updates	76
NETWORK REQUIREMENTS OF LIVE CONTENT SUITE	77
Phone Connectivity	77
LDAP Connectivity	77
Global Catalog Connectivity	78
Mitel MCD Host Connectivity	78
Network Requirements for adding an MCD Host with the Configuration Wizard	78
Network Requirements for the 5300 HTML Application Uploader	79
Network Requirements for Programming Phones	79
Network Requirements for Retrieving HTML Applications	79
Appendix – Open Source Software	81
APPENDIX – FOR YOUR INFORMATION	85
Live Content Suite and Microsoft Framework 2.0	85

Live Content Suite Installation

The InGenius Live Content Suite application provides an easy way to program keys on your Mitel 5300 series IP Phone.

The InGenius Live Content Suite application automatically pulls information from two different sources:

- **Microsoft Active Directory** for user information
- **Mitel Communications Director (MCD) Host(s)** for phone programming

Prerequisites

Live Content Suite has a number of required components needed to run:

- **Microsoft Windows Server 2003.**
- **Microsoft Internet Information Services (IIS).** This component is an optional part of the operating system. A default installation of IIS is all that is required.
- **Microsoft .NET framework 2.0.** This component can be [downloaded](#) from Microsoft.



Note: If not installed, the Live Content Suite installer indicates where to download and install it.

- **Microsoft Active Directory (AD).** Live Content Suite uses the LDAP protocol to connect to AD to look up users. Their phone extensions need to be present in some Active Directory field for each user of this product and need to correspond to their DN in the MCD Host(s) to be used. The domain and forest functional level must be at least Windows 2000 Native mode. Live Content Suite supports deployment in an Active Directory forest which enables users in another domain within the same AD forest to access the web application. It also supports secure LDAP as provided by Active Directory.
- **Microsoft SQL Server 2005** (Express Edition or higher). This component can be [downloaded](#) from Microsoft.
- **Installed on a computer on a network that can access the MCD Host(s).** Live Content Suite needs to connect to the Mitel 3330 ICP to read and write phone key programming for users.
- **Mitel MCD 4.1 SP2** or higher. You can support a standalone MCD host or multiple MCD hosts in a single cluster. Phone DNs must be unique throughout the cluster.
- **Mitel Phones** – The following phones are supported for programming:
 - **Mitel 5212/5224** (does not support live content)
 - **Mitel 5304** (does not support live content)
 - **Mitel 5312/5324** (does not support live content)

- **Mitel 5320/5330/5340**
- **Mitel 5360**
- The following phones are supported for Live Content with the listed firmware:
 - **Mitel 5360 firmware** 03.00.03.03 or higher.
 - **Mitel 5320/5330/5340 firmware** 01.06.03.04 or higher.

There are also the following considerations:

- The person doing the installation should be at least somewhat familiar with Active Directory, Internet Information Services, and SQL Server.
- The person doing the installation and configuration should be a local administrator on the server, and also have permission to create a database on the SQL server.
- You should ensure that the machine where you intend to install Live Content Suite is connected to the Internet during installation. This is necessary to verify your registration key. (There is a manual registration method using email if necessary.)
- The computer where the Live Content Creator web application is installed needs permanent access to the internet in order to download content for the applications (e.g. current weather from the weather service).

Hardware Requirements

If you wish to install Live Content Suite and the SQL database on a single server, the server should meet the following requirements.

Hardware Component	Minimum Requirement	Recommended Requirement
CPU	1.5 GHz	Dual-core 2GHz or higher
RAM	2GB	3GB or higher

Live Content Suite Application Overview

Simply put, the Live Content Suite application makes it easy to program your phone keys from any web browser. Its intuitive interface has a very small learning curve for the end-user.

Also included is the Live Content Creator, which lets you put apps on your phone that contain live content from various services, like weather, Twitter feeds, Blogger feeds, etc.

Initial Setup BEFORE You Install Live Content Suite

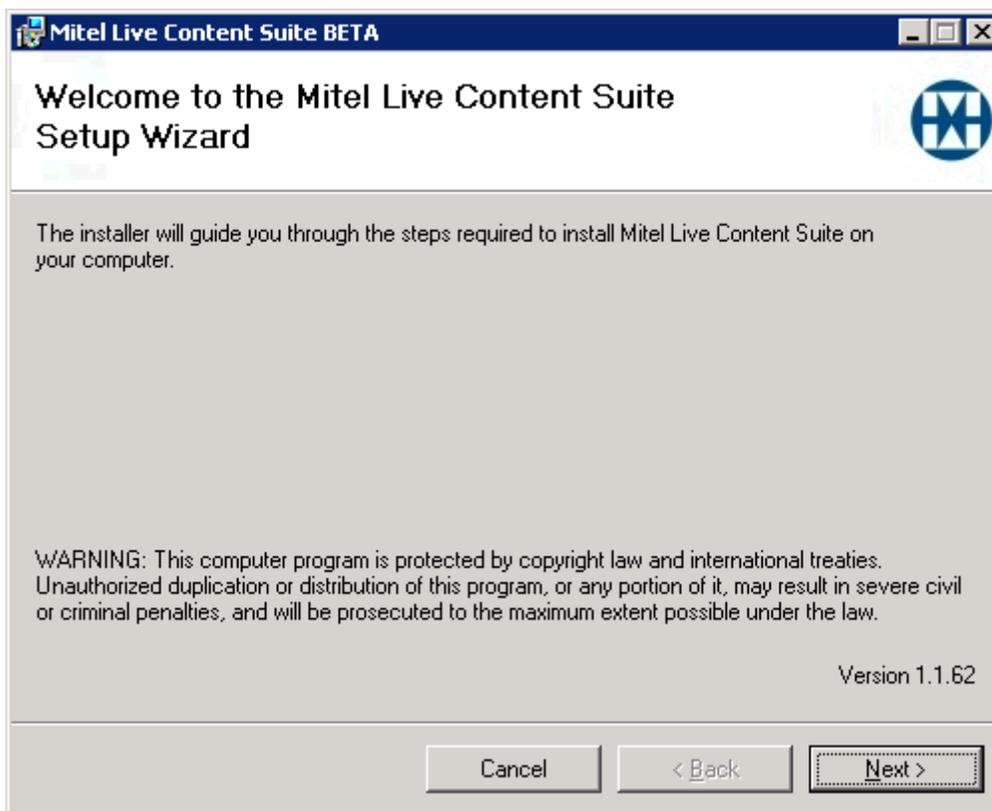
1. **Ensure access to Microsoft SQL Server 2005 or later.**
If you don't have an installation of **Microsoft SQL Server** to point to, you can [download](#) and install Microsoft SQL Server 2005 Express Edition available for free from Microsoft. The Live Content Suite uses a SQL Server database to store application data. However, SQL Server and the Live Content Suite application may be hosted on different machines. However, for best performance, we recommend that they be installed on the same server.
2. **Ensure that user information in Active Directory is up to date.**
Extensions are read from a field in the user's entry in Active Directory. The phone extension field in Active Directory must contain the given user's extension in order to be found so that they can program their phone.
3. **Create a user on each MCD Host to be used with Live Content Suite.**
Live **Content** Suite needs to log on to each MCD Host as a user in order to read and write phone key and screensaver programming. Follow the steps below to create a user with the appropriate permissions:
 - a. Use ESM to create a new admin policy on the "Admin Policies" page. Set the default access type to 'No Access'.
 - b. Using ESM navigate to the "User Authorization Profiles" page and create a new user authorization profile. Select the "System Admin" checkbox and select the admin policy you created above from the "System Admin Policy Name" dropdown menu. Save your changes. This will allow the Live Content Suite application to login to the switch. Once it has logged in its internal certificate will grant the required permissions.

Live Content Suite Installation

Log in to the computer where you want to install Live Content Suite as a domain user that is an administrator of this computer.

Run Live Content SuiteSetup.exe on the machine where you want to install the Live Content Suite service.

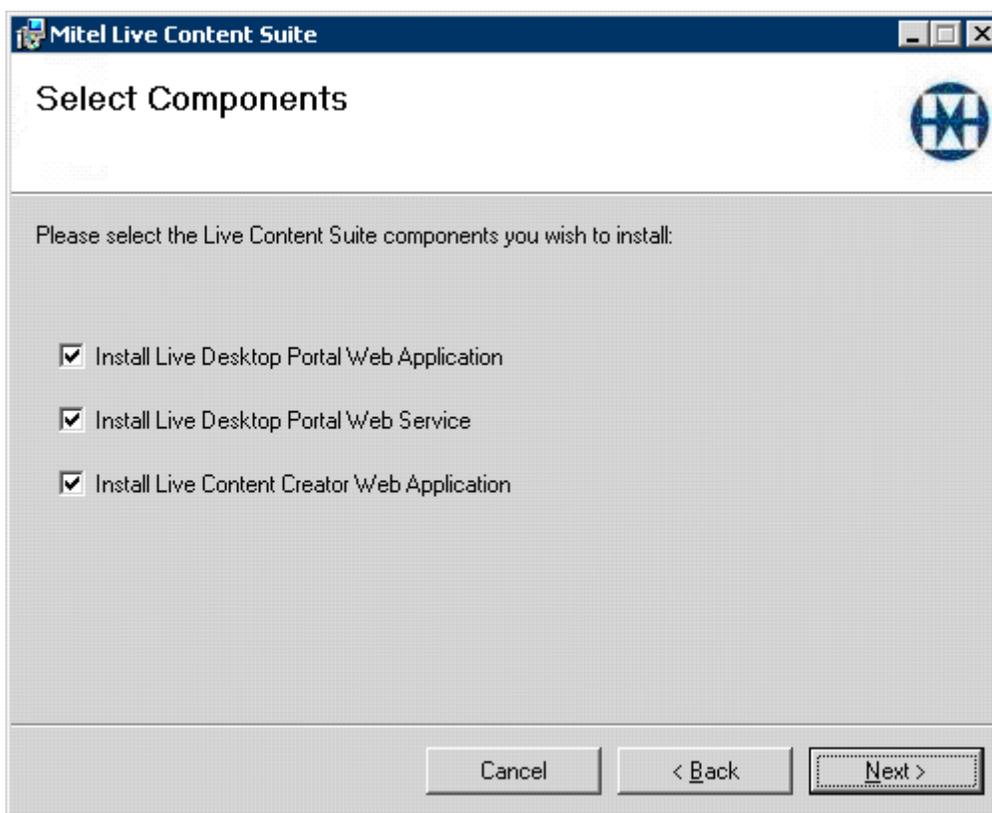
1. Welcome page. Click **Next**:



2. License Agreement page. Agree to License Agreement and click **Next**:

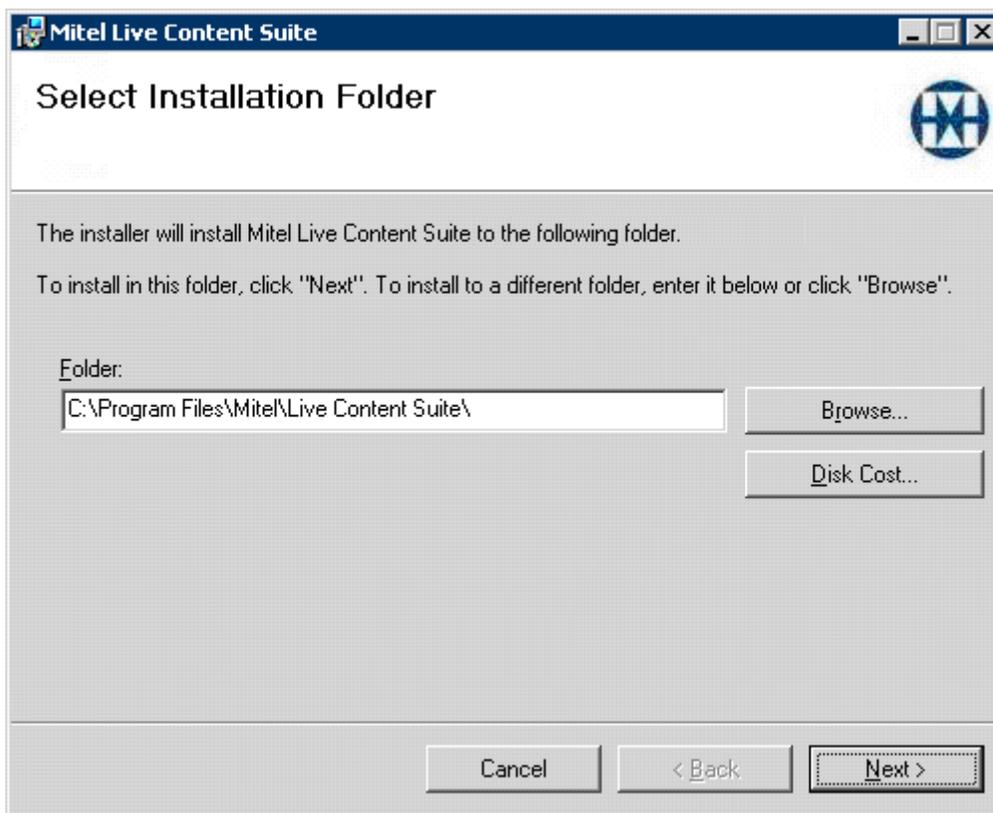


3. Select Components page. Specify what you want to install and click **Next**:



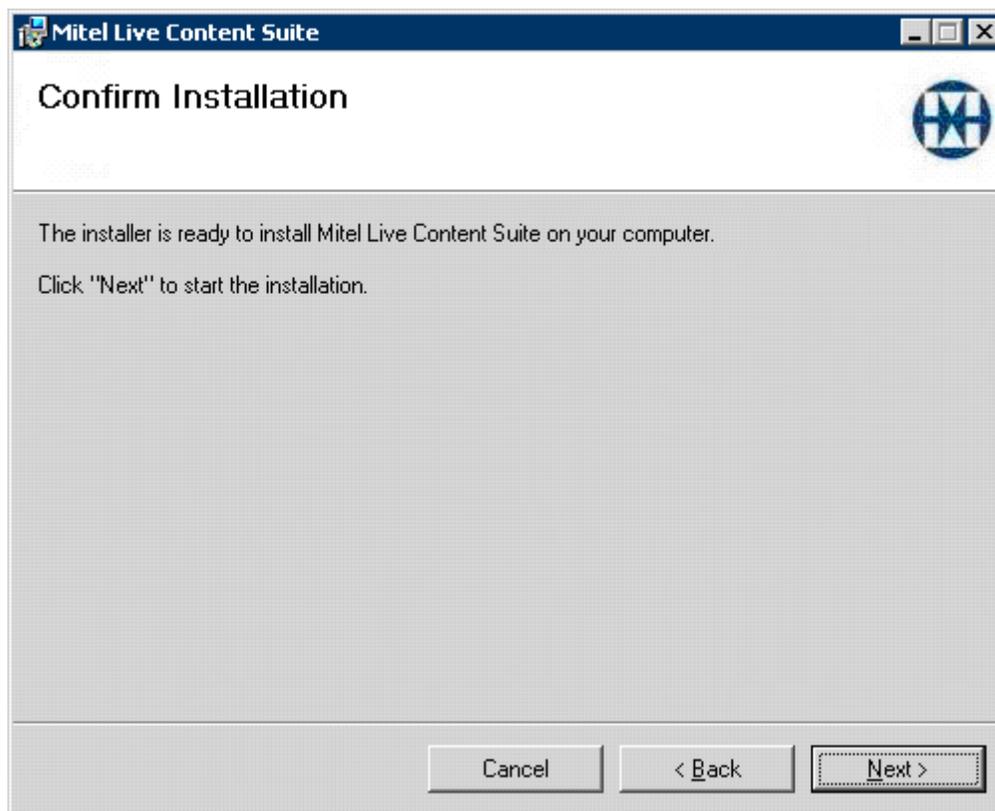
The components can all be installed on the same computer for simplicity, or on separate computers in a larger environment. If they are installed on separate computers, then during configuration you will be prompted for the URLs to components installed elsewhere.

4. Select Installation Folder page. Specify where you want to install and click **Next**:

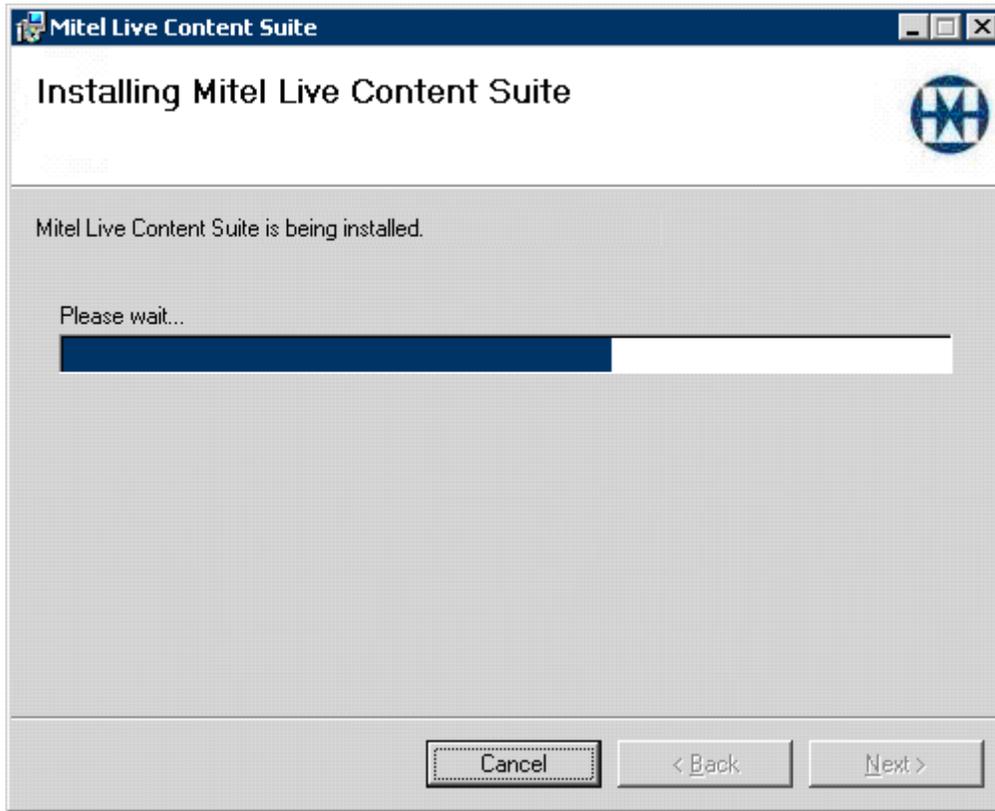


The optional “Disk Cost” button will display a list of the local disk drives and their associated total and free space based on the current drive selected for installation.

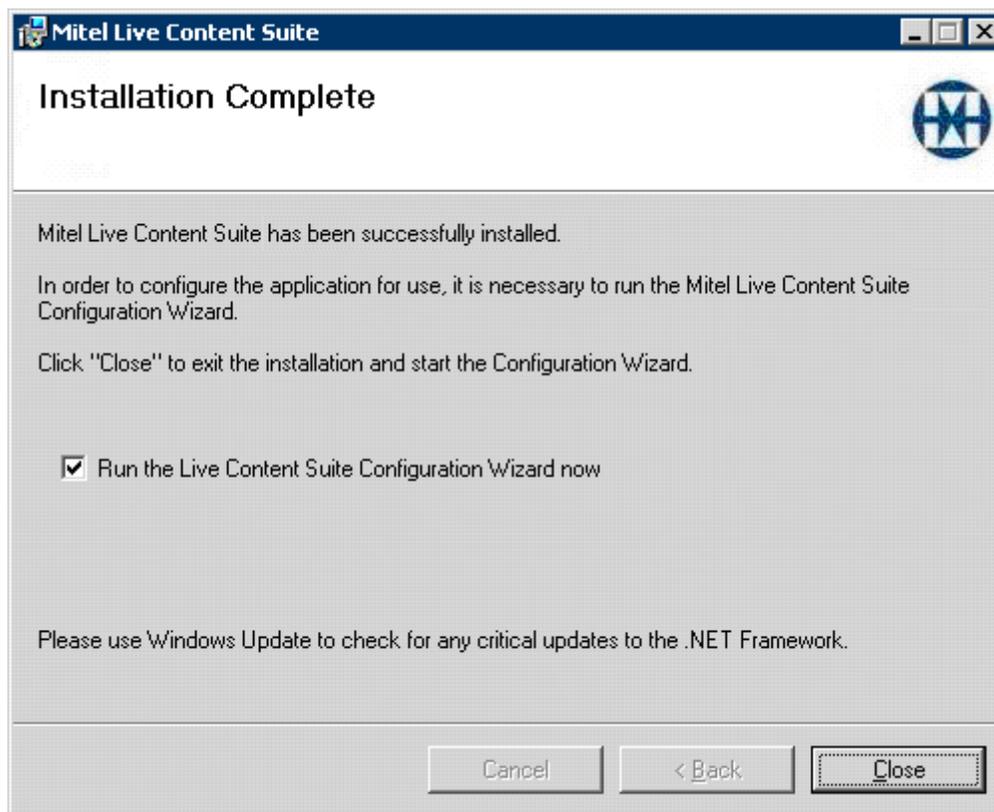
5. Confirm Installation page. Click **Next**:



6. Installing page:



7. Installation Complete page. Leave checkbox selected to run Configuration Wizard and click **Close**:



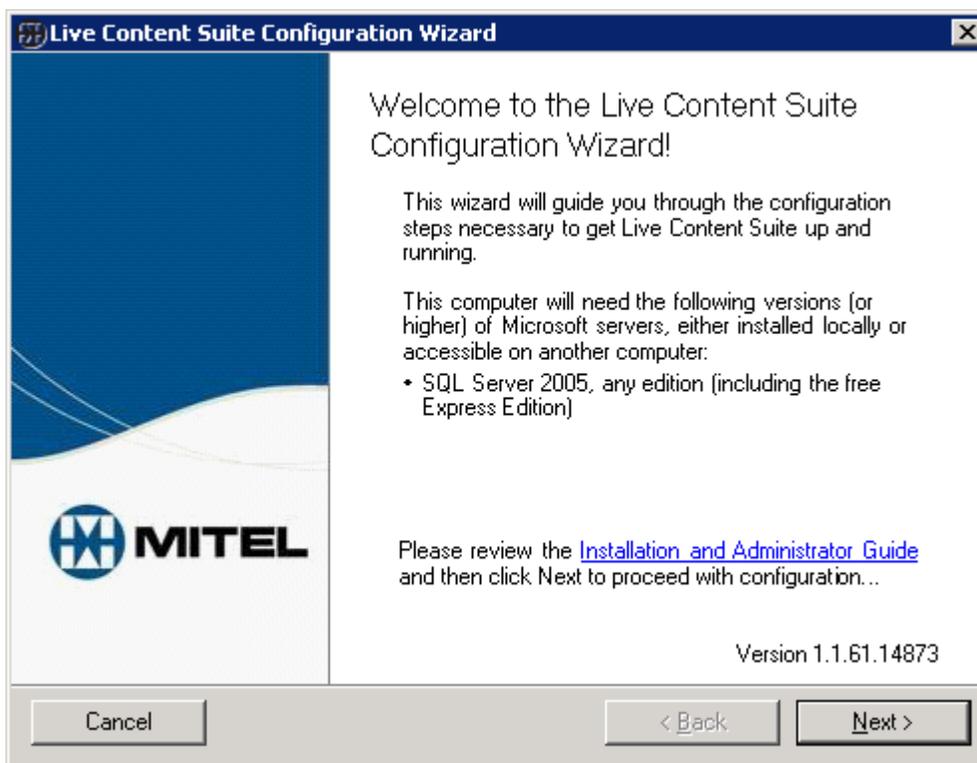
Live Content Suite Configuration

You should run the Configuration Wizard as a user who meets the following requirements:

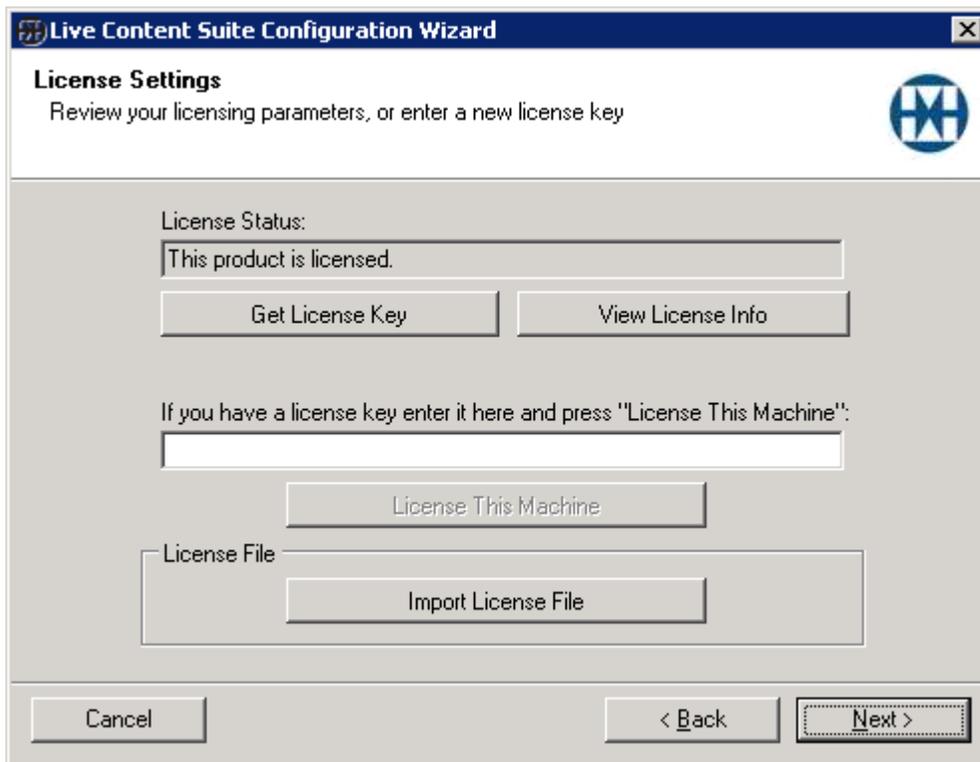
- The user must be a domain user.
- The user must be a local administrator on the server on which Live Content Suite is installed.
- The user must have permission to create databases on the database server. If the database is local then being a local administrator should provide the necessary permissions.

 **Note:** If you choose not to run the Configuration Wizard after the installation, you can open it at a later time from the Start menu. Select Start, All Programs, InGenius Software, Live Content Suite, Live Content Suite Configuration Wizard. Also, you can re-run the Configuration Wizard at any time later to change any settings necessary.

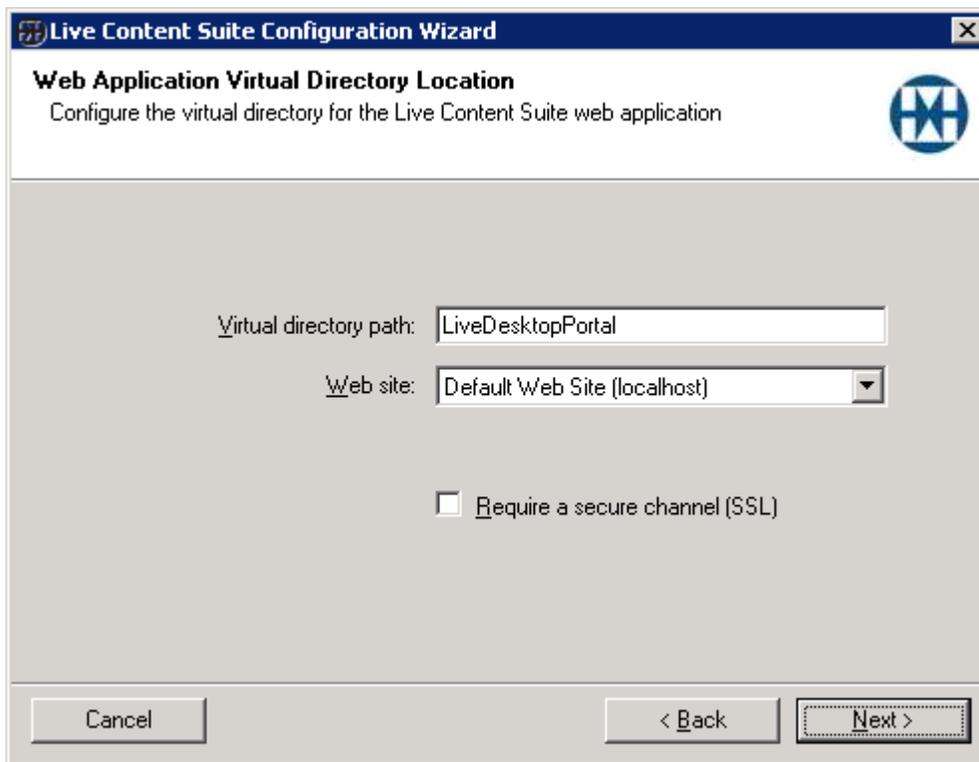
1. Welcome page. Click **Next**:



2. Licensing parameters page. Enter your license key in the box provided, and click "License This Machine". Once licensed, click **Next**:



3. Web Application Virtual Directory page. Choose the virtual directory name and site you want to use for the Live Desktop Portal web application. This name and site form the URL to which users will navigate in their browser to run the application. For example: `http://servername/LiveDesktopPortal`. Click **Next**:



The screenshot shows a window titled "Live Content Suite Configuration Wizard" with a sub-header "Web Application Virtual Directory Location". Below the sub-header is the instruction "Configure the virtual directory for the Live Content Suite web application". The main area contains three input fields: "Virtual directory path:" with the text "LiveDesktopPortal", "Web site:" with a dropdown menu showing "Default Web Site (localhost)", and a checkbox labeled "Require a secure channel (SSL)" which is currently unchecked. At the bottom of the window are three buttons: "Cancel", "< Back", and "Next >".

If the Web Site is configured with an SSL certificate, you will have the option of requiring SSL to access the Web Application virtual directory. This will provide a secure channel for communication between the client web browser and the Live Desktop Portal server.

 **Note:** Mitel does not provide certificates for encrypting the Web Application.

In order to enable SSL support the web site must meet the following conditions:

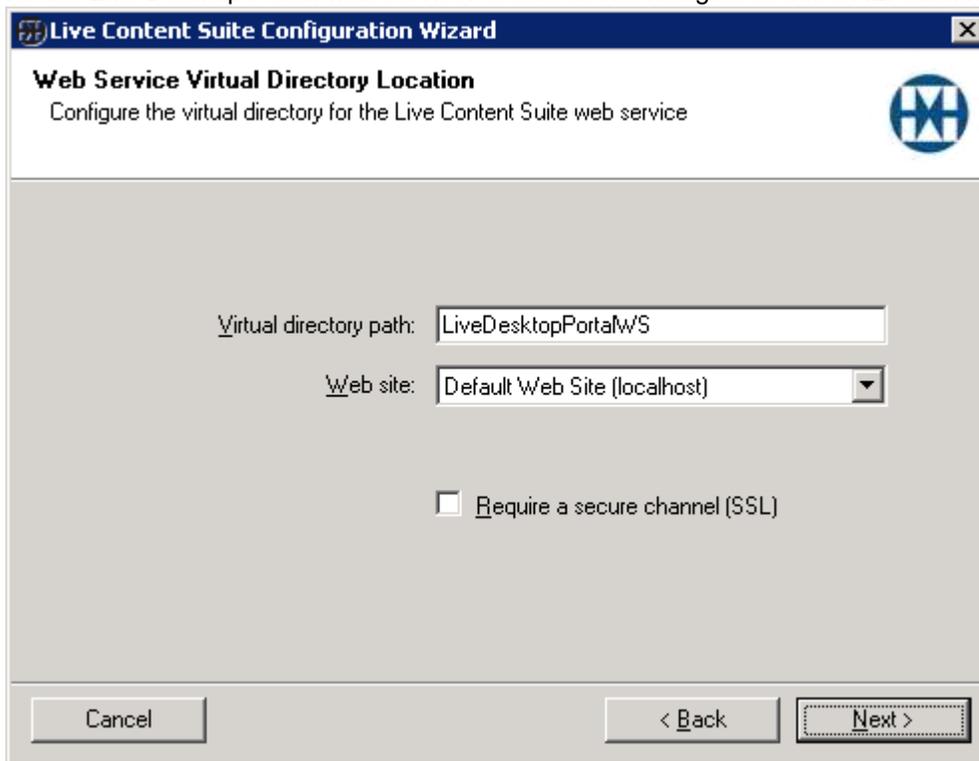
- Must be configured with an SSL certificate. Refer to IIS documentation for details about configuring a web site with an SSL certificate.
- Must be assigned an SSL port. By default this is port 443.
- Must be assigned a non-SSL port. By default this is port 80.

If your web site meets these conditions, the "Require a secure channel (SSL)" checkbox will be enabled on the Web Application Virtual Directory Location page. If you select it during configuration then users must access the Live Desktop Portal using SSL, as shown below:

`https://servername/LiveDesktopPortal`

If the website is not configured with an SSL certificate then the "Require a secure channel (SSL)" checkbox will be grayed-out.

4. Web Service Virtual Directory page. Choose virtual directory name and site you want to use for the Live Desktop Portal web service. Users do not navigate to this URL. Click **Next**:



If the Web Site is configured with an SSL certificate, you will have the option of requiring SSL to access the Web Application virtual directory. This will provide a secure channel for communication between the Web Application and the Web Service.

 **Note:** Mitel does not provide certificates for encrypting the Web Service.

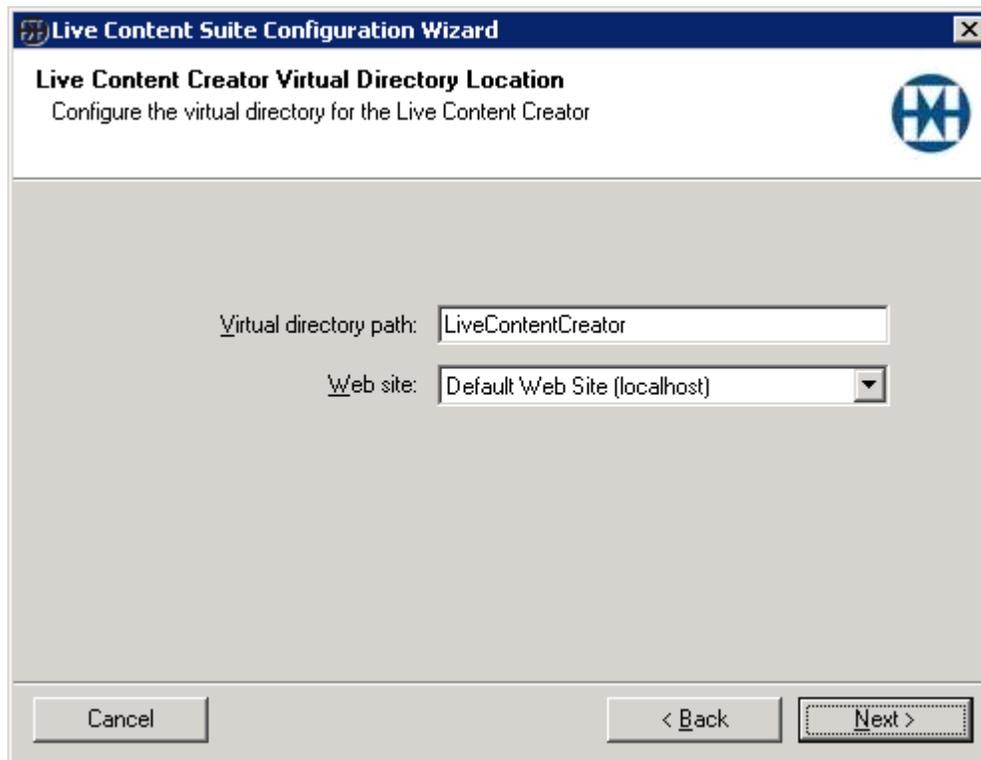
In order to enable SSL support the web site must meet the following conditions:

- Must be configured with an SSL certificate. Refer to IIS documentation for details about configuring a web site with an SSL certificate.
- Must be assigned an SSL port. By default this is port 443.
- Must be assigned a non-SSL port. By default this is port 80.

If your web site meets these conditions, the “Require a secure channel (SSL)” checkbox will be enabled on the Web Application Virtual Directory Location page.

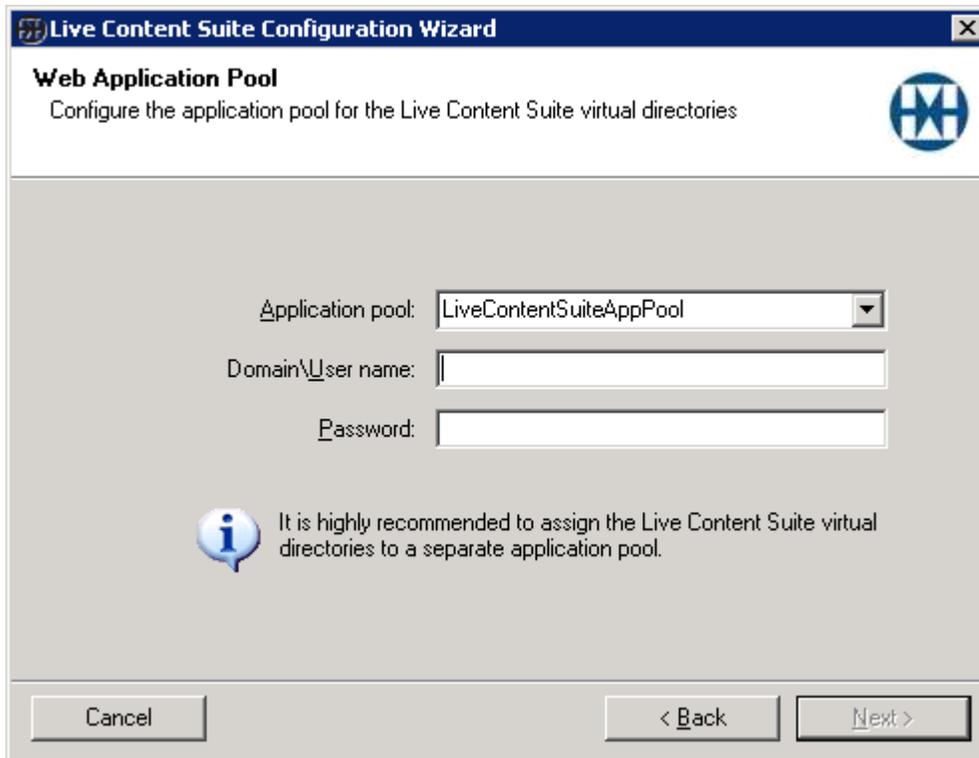
If the website is not configured with an SSL certificate then the “Require a secure channel (SSL)” checkbox will be grayed-out.

5. Live Content Creator Virtual Directory page. Choose virtual directory name and site you want to use for the Live Content Creator web application. Phones navigate to this URL to run Live Content applications. Click **Next**:



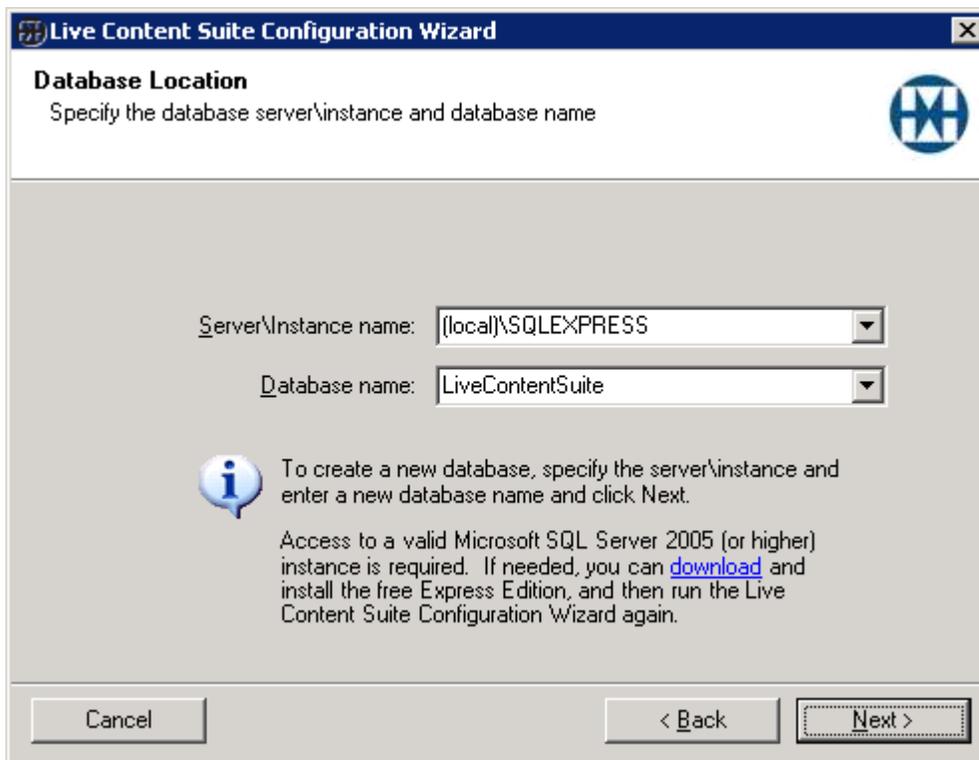
The screenshot shows a dialog box titled "Live Content Suite Configuration Wizard" with a close button in the top right corner. The main heading is "Live Content Creator Virtual Directory Location" and the subtitle is "Configure the virtual directory for the Live Content Creator". A logo is visible in the top right of the main area. The dialog contains two input fields: "Virtual directory path:" with a text box containing "LiveContentCreator", and "Web site:" with a dropdown menu showing "Default Web Site (localhost)". At the bottom, there are three buttons: "Cancel", "< Back", and "Next >".

6. Application Pool page (IIS 6.0+ only). Select the IIS Application pool name of your choice, and Domain\Username and Password for the domain user that will run the application pool process. Typically this would be a service account created for this purpose, and needs no special rights. The account does not require special privileges but it must be a domain user. Click **Next**:



For more information on application pools, please consult the Microsoft Internet Information Services documentation.

7. Database Configuration page. Choose SQL database server (whether local or another server) and SQL database name and click Next. If an existing database is chosen, it must be one already used for Live Content Suite or empty of all tables and stored procedures. If the database doesn't exist you will be prompted to create it:



When the Configuration Wizard runs it grants the Application Pool user account read/write permissions to the database.

For more information on SQL Server, please consult the Microsoft SQL Server documentation.

8. User Lookup Settings page. Select or type the LDAP field name to search for phone extensions. Provide credentials to use while doing lookups. Click **Next**:

The screenshot shows the 'User Lookup Settings' dialog box within the 'Live Content Suite Configuration Wizard'. The title bar reads 'Live Content Suite Configuration Wizard'. The main title is 'User Lookup Settings' with a subtitle: 'Configure settings for accessing user information via LDAP queries and to enable lookup of users by extension'. There is a blue circular icon with a white 'i' on the right side. The dialog contains the following fields and options:

- 'LDAP query root:' followed by an empty text input field.
- An information icon (blue circle with 'i') and a tooltip: 'Enter an LDAP path to a particular LDAP server if desired. If in doubt, just leave this blank.'
- 'Field to search for users by phone extension:' followed by a dropdown menu showing 'telephoneNumber'.
- Two radio button options:
 - Use the application pool user for LDAP queries
 - Specify the user to use for LDAP queries:
- Below the second radio button, there are two text input fields: 'Domain\User name:' and 'Password:'.
- At the bottom, there are three buttons: 'Cancel', '< Back', and 'Next >'.

You can also provide the LDAP query root, which is the location to bind to LDAP to search for users and groups. You can specify an LDAP query root in these ways:

- LDAP://DomainControllerName (Can use host name, FQDN, or IP Address)
- LDAP://ActiveDirectoryDomainName.suffix

If an Enterprise Certificate Authority is installed in your environment you may be able to use secure LDAP. To use secure LDAP you add port 636 to the end of the query root, as shown below:

- LDAP://DomainControllerName:636
- LDAP://ActiveDirectoryDomainName.suffix:636

If you are in an Active Directory forest you can locate users and groups forest-wide by binding to a Global Catalog server. You can specify a Global Catalog server for the LDAP query root in these ways:

- GC://GlobalCatalogServerName (Can use host name, FQDN, or IP Address)
- GC://RootForestDomain.suffix

If an Enterprise Certificate Authority is installed in your environment you may be able to use a secure Global Catalog connection. To use a secure Global Catalog connection you add port 3269 to the end of the query root, as shown below:

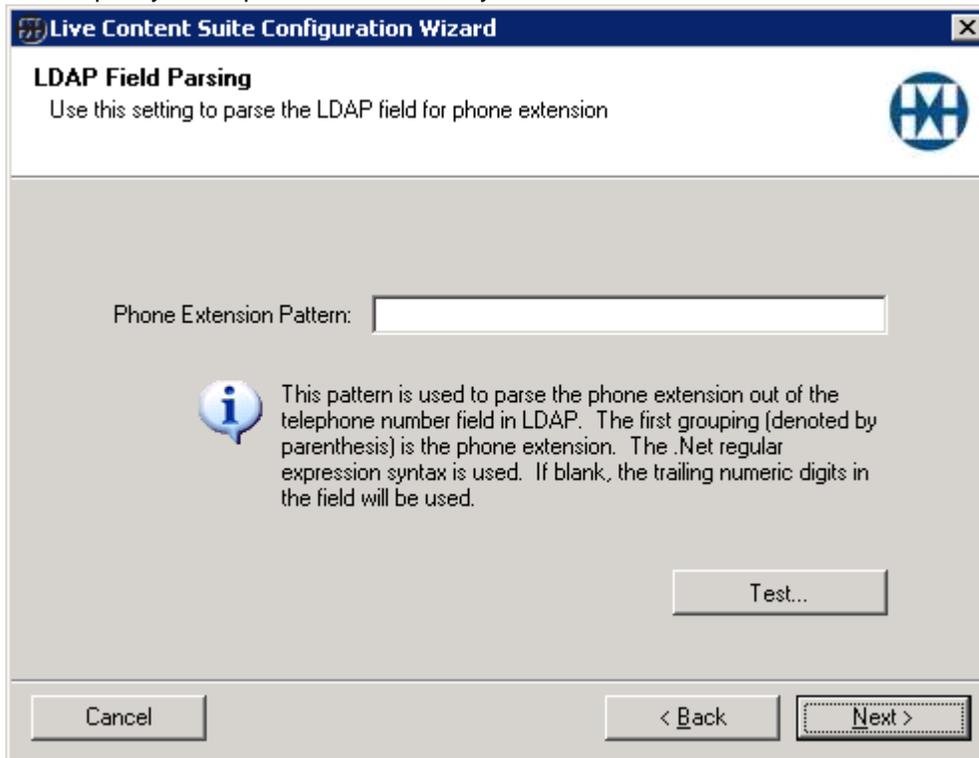
- GC://GlobalCatalogServerName:3269

- GC://RootForestDomain.suffix:3269

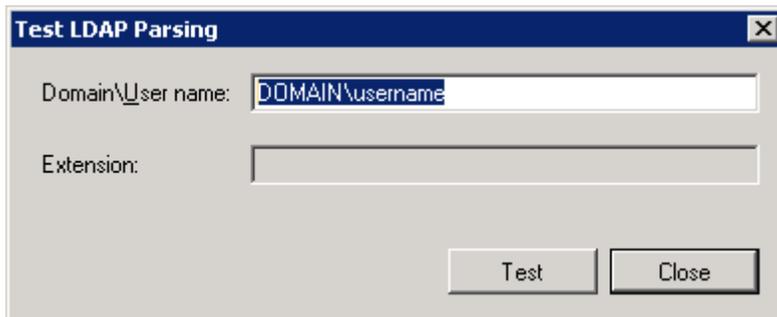
If you leave the LDAP query root blank, Live Content Suite will locate a Global Catalog server from the local Active Directory site.

The field to search must be the field in Active Directory that contains the extension for each user. If the extension is not at the end of the number in the field, a custom regular expression can be specified in the next step to retrieve it.

- LDAP Field Parsing page. If the extension is the entire or trailing numeric digits of the specified LDAP field, then you need to enter a regular expression to extract them from the field. Specify the expression if necessary and click **Next**:



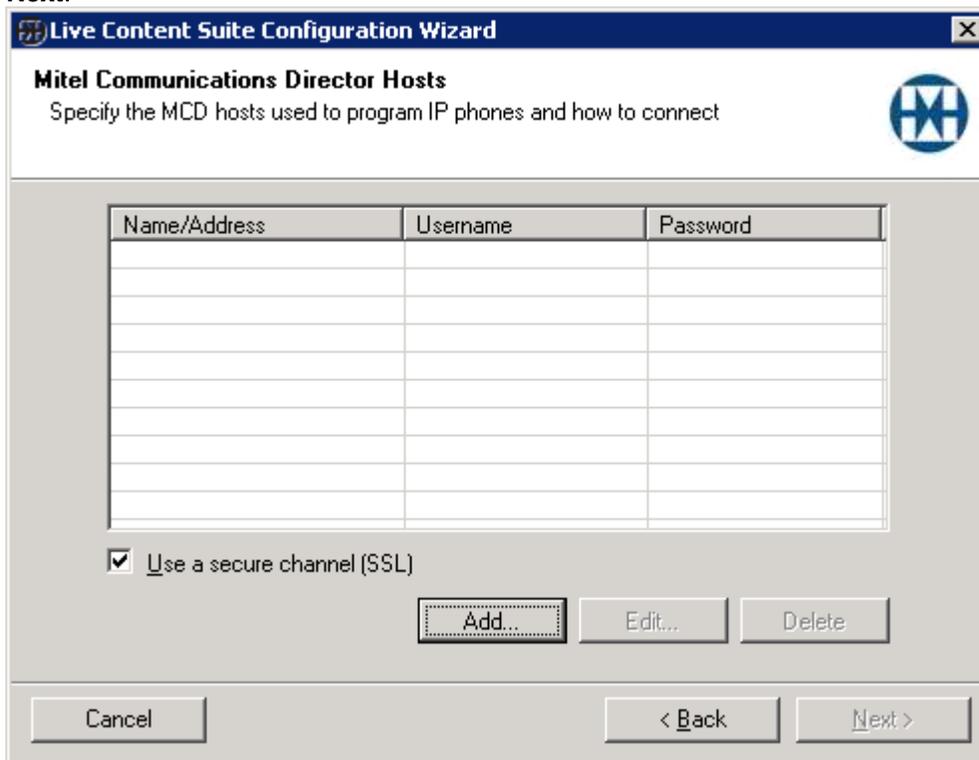
If you want to test your regular expression to see if it will retrieve extensions properly, press the **Test...** button and try various known usernames in the test dialog:



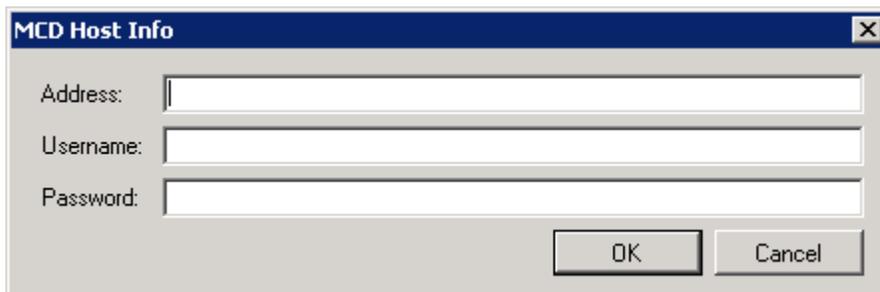
For example, if the extension was the set of trailing digits (or the characters * or #) in the field (the default), the regular expression syntax to extract it is **([0-9*#]+)\$**.

The regular expressions supported use Microsoft .NET Framework syntax. If you need help on the syntax, consult the .NET regular expression documentation in MSDN.

- Mitel Communications Director Hosts page. Specify the addresses to the MCD hosts and the credentials to use for each host (for the user[s] set up in the Prerequisites step) and click **Next**:

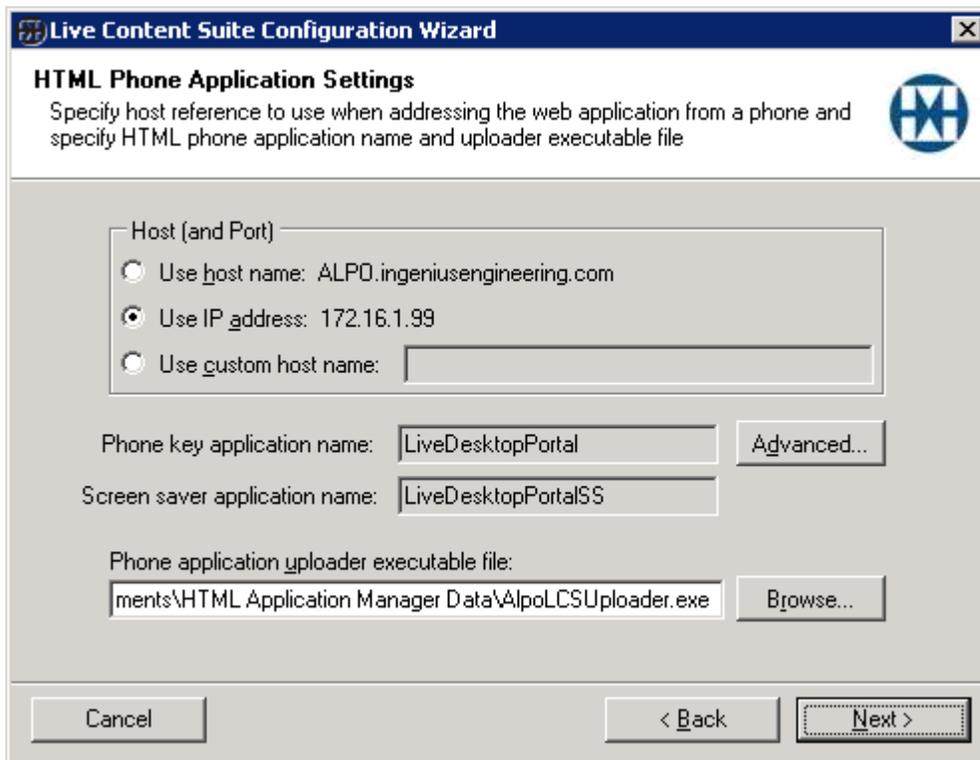


To add an MCD host, press the **Add...** button and enter the host address (name or IP), and valid credentials for each host:

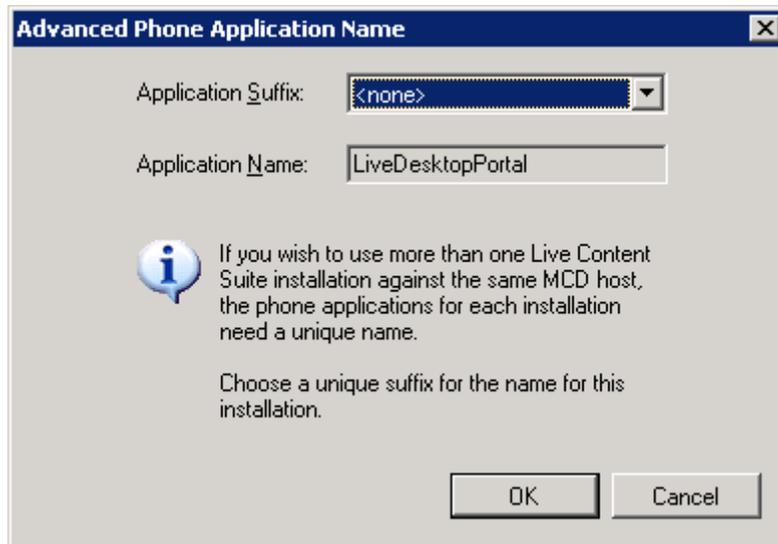


Note: Normally you should enable the “Use a secure channel (SSL)” checkbox to ensure that all network communication between the Web Service and the MCD host(s) is secure. Enabling or disabling SSL takes effect for all MCD hosts you have added. It is not necessary to configure a certificate on the MCD hosts since they come with one by default.

11. Phone Applications page. Specify how you want the phone to address the web application host specified in Step 3. If the MCD Host is configured to support DNS, then it's best to use the host name, otherwise use the IP address (provided that it is a fixed address). There is also the capability to provide a custom host name if you've configured a special host name or IP address for this machine that wasn't detected. The Application names are the names of the applications that will appear as available applications under Programmable Keys (that should never be programmed directly on the phone) once the compressed phone .spx is uploaded to the MCD Host. Click **Next**:



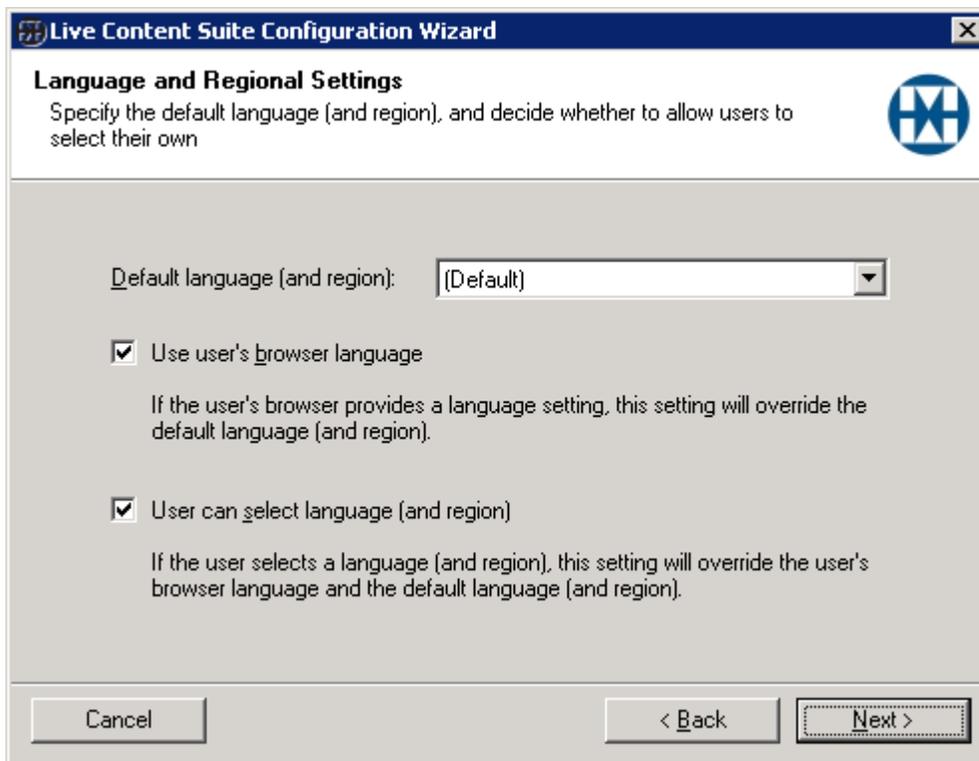
If you are using more than one Live Content Suite installation against the same MCD host, a unique set of phone application names are required for each Live Content Suite installation. For one of the installations, you need to change the name of the application from the default. Do so by clicking the **Advanced...** button, which will bring up this dialog:



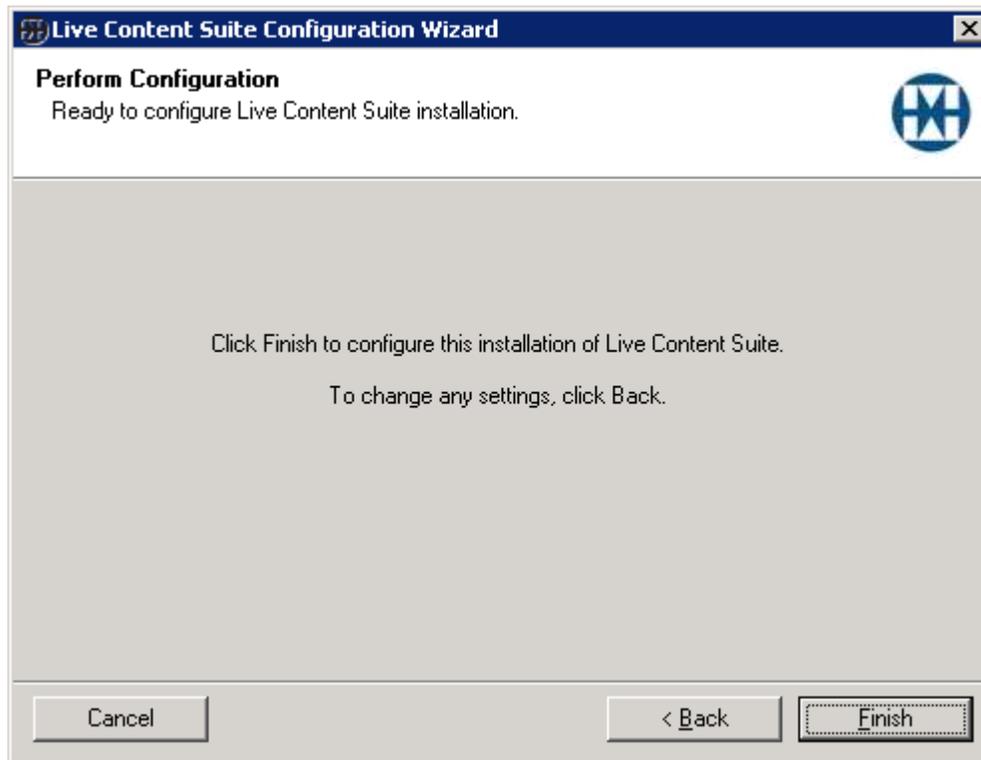
If you wish to change the name or location of the self-extracting upload program, either type the new path in the **Phone application uploader executable file:** box or click the **Browse...** button which will bring up a standard Save As dialog.



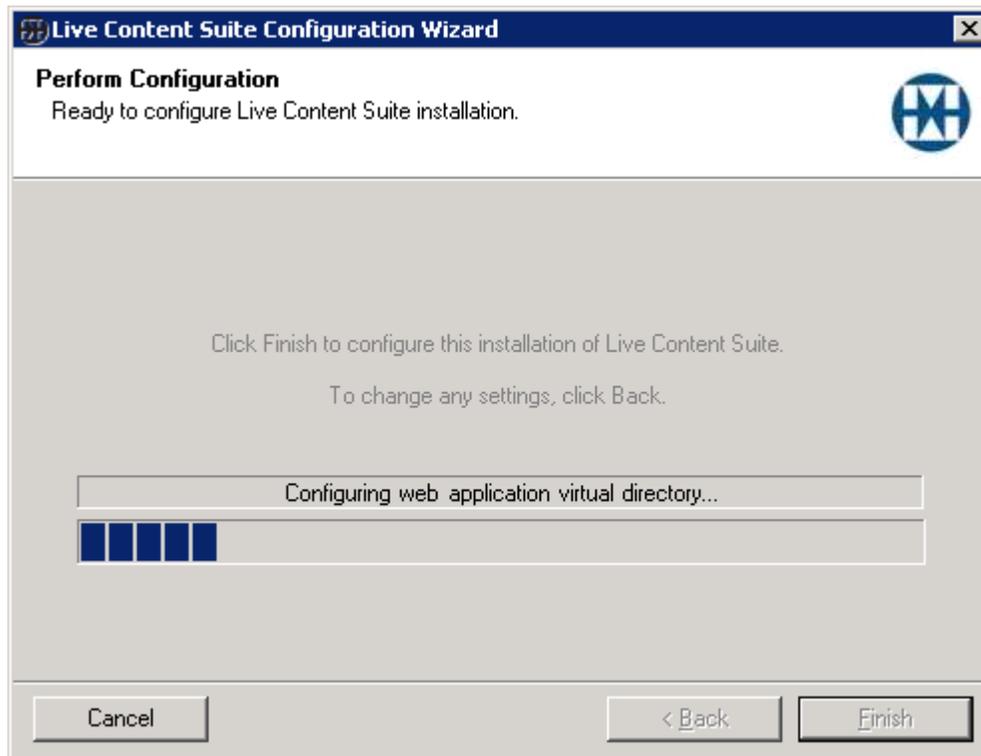
12. Language and Regional Settings page. Select the default language (and region) for the user interface (default is the installed language of Windows on this server), and whether the user's browser language should be used or whether users should be allowed to change the language for themselves. Click **Next**:



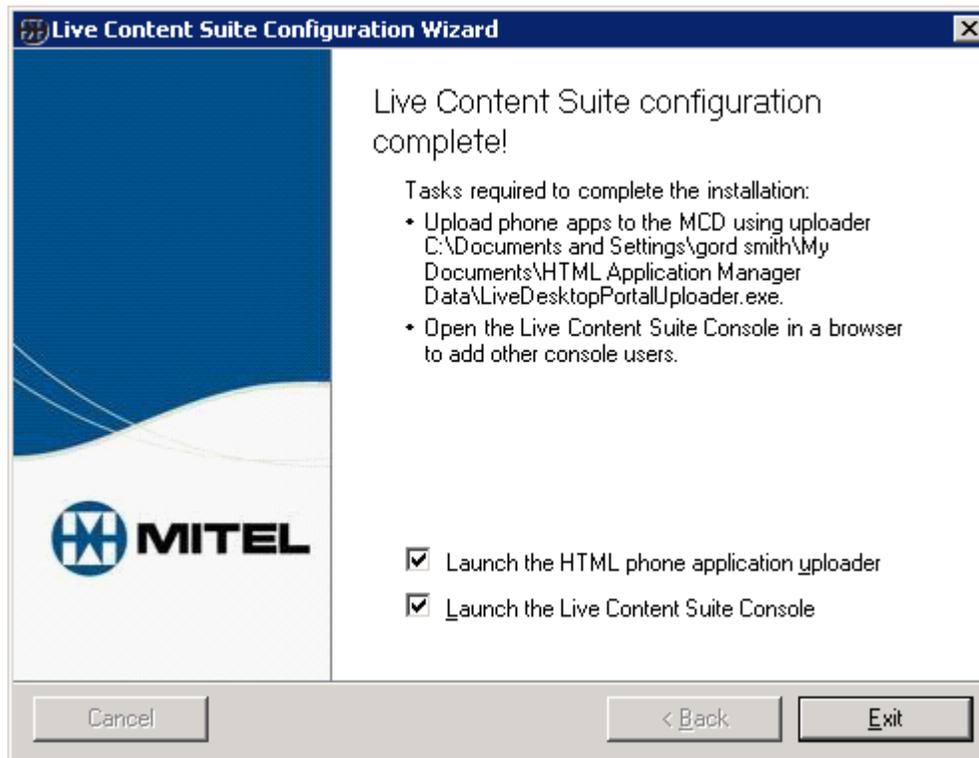
13. Perform Configuration page, click **Finish** to start the configuration process:



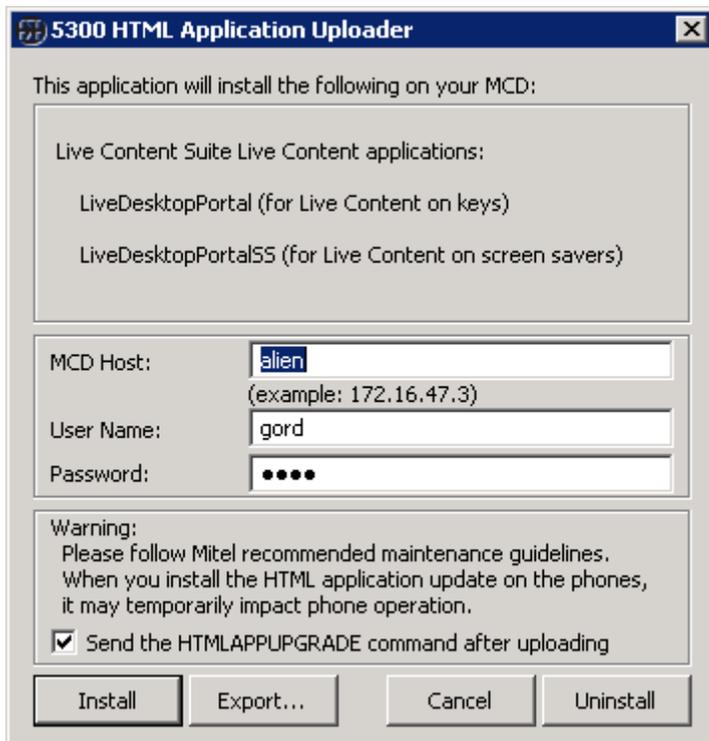
14. Perform Configuration progress:



15. Configuration Complete page, click **Exit**:



16. With the **Launch the HTML phone application uploader** checkbox checked, you will then be prompted to upload the phone application specified in Step 11 to each MCD host specified in Step 10. Ensure the credentials are correct, and leave the Send the HTMLAPPUPGRADE command after uploading checkbox is checked if so desired (otherwise this will have to be done manually later) and press **Install**:



 **Note:** Refer to the Network Requirements section if you are unable to upload the phone application.

Testing the Installation

Launch the Live Content Suite Console, and log on. Verify that it found your phone extension and that you can program keys on your phone. Also try to program a Live Content application (“My Apps”) and verify that the application works on the phone.

Upgrading from Live Content Suite 1.0

If you have an installation of Live Content Suite 1.0 you can perform an in-place upgrade to Live Content Suite 1.1. When you upgrade you perform the same steps as a regular installation:

- Install the Live Content Suite software
- Run the Configuration Wizard and provide configuration details
- Upload the phone application to the MCD hosts(s)

Below are some considerations to be aware of when upgrading.

Database Version

Live Content Suite 1.1 contains changes in the database structure which require the 1.0 database to be upgraded during configuration. The Configuration Wizard will notify you if it detects the 1.0 database and give you the choice of proceeding with the database upgrade or not. You must upgrade the database to complete the configuration of Live Content Suite 1.1.

You may want to consider backing up the Live Content Suite 1.0 database before upgrading the database.

Key Programmers

The Key Programmer role in Live Content Suite 1.0 has been deprecated in this release. If you have any Key Programmers in your Live Content Suite 1.0 environment, they will be handled using the following rules during the upgrade procedure:

- All Key Programmers are assigned the ‘User’ role
- Users who were Key Programmers are given permission to program the special workgroup named ‘All Users’. Workgroup settings are discussed later in this document.

The resultant effect after upgrade is that the users will have the same ability to program any other user’s phone.

Updating Configuration

You may need to change the configuration from time to time. To change the configuration you must run the Configuration Wizard again. You might re-run the Configuration Wizard in the following circumstances:

- Adding a new switch
- Deleting a switch
- Changing switch
- Adding a license

 **Note:** You are able to change any configuration option; however, it is not recommended that you change the 'Phone key application name' on the "HTML Phone Application Settings" page. Doing so will result in previously programmed Live Content applications not working.

It is important to plan any configuration changes to take place during non-peak times. The last step of the Configuration Wizard restarts the web application which results in a brief interruption in service.

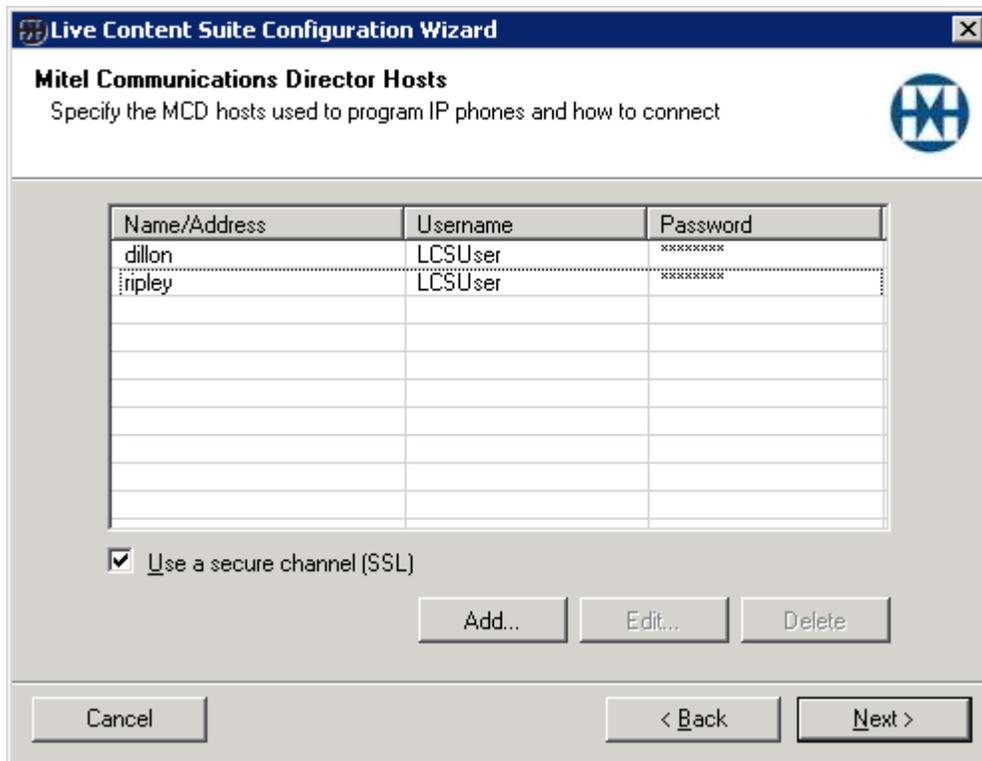
Adding a new MCD Host

You may add a new MCD host to your existing cluster. If you want to be able to use Live Desktop Portal to program the phones on the new MCD host then you must add the MCD host to the configuration using the Configuration Wizard.

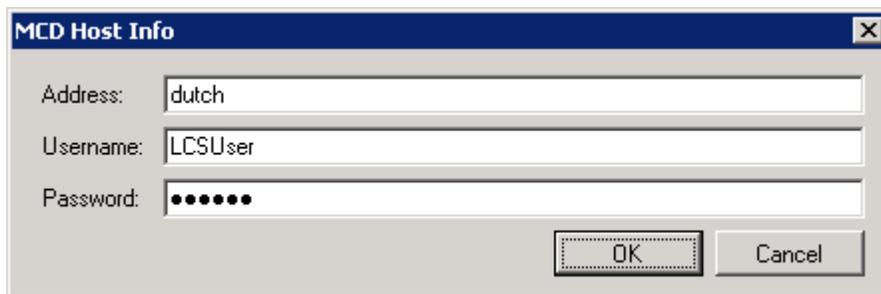
 **Note:** You should only add an MCD host if the DNs are different from existing hosts.

To add an MCD host to the configuration follows these steps:

1. Run the Configuration Wizard.
2. Each page will be prefilled with the current configuration settings. Click **Next** until you reach the Mitel Communications Director Hosts page.
3. On the Mitel Communications Director Hosts page you will see the existing hosts listed. Click **Add**.



- Specify the address of the new MCD host and the credentials to use and click **OK**.



- Click **Next** and complete the Configuration Wizard. Do not make any further changes unless required.
- On the Configuration Complete page, click **Exit**. Make sure the **Launch the HTML phone application uploader** checkbox is enabled.
- You must run the **5300 HTML Application Uploader** to upload the phone application to the new MCD host. You do not need to upload the phone application to the existing MCD hosts.

It is only necessary to re-upload the phone application to an MCD host in the following situations:

- You changed the phone application name on the HTML Phone Application Settings page.
- You changed the Host setting on the HTML Phone Application Settings page.
- You changed the virtual directory path on the Web Application Virtual Directory Location page.

- You are upgrading Live Content Suite to a newer version. In-place upgrades are supported.

Live Desktop Portal Administration

After you have installed and configured Live Content Suite, you need to perform some administrative functions to give users the proper access to the application so they can begin programming keys on their phones. Live Desktop Portal is the web-based tool you use to manage your Live Content Suite configuration. Using Live Desktop Portal an administrator can perform the following functions:

- Add Users and Groups
- Set User and Group Access
- Assign Key Programming Permissions to Users and Groups
- Create Custom Links
- View System Logs
- Program Keys for any User
- Rollout Key Programming to multiple phones at once

Details are provided in the following sections.

Accessing Live Desktop Portal

If you are logged on the local Live Content Suite server, you can access Live Desktop Portal from the Program menu by clicking Start → All Programs → Mitel → Live Content Suite → Live Content Suite Portal.

You can also access it from a remote computer by entering the path provided in the Configuration Wizard. By default it is `http://servername/livedesktopportal`.

Live Desktop Portal will open in your default browser. If integrated authentication is enabled in the browser you will be automatically logged in. If integrated authentication is not enabled, you must provide authentication details by entering your username and password. You must prefix your username with your domain name: `DOMAIN\username`.

 **Note:** The domain user who runs the Configuration Wizard is added to Live Content Suite as the default Administrator. The default Administrator adds other administrators as required.

System Settings

Most of the Administrator's tasks will be performed in the "System Settings" area.

The image below shows how Live Desktop Portal will appear when the default Administrator logs in for the first time.

The screenshot shows the Live Desktop Portal interface. On the left is a navigation menu with buttons for My Phone, Select User, System Settings (highlighted), Help, Administrator Help, About, and Logout. The main content area has four tabs: Permissions (selected), Additional Links, Log, and Multi-User. Under the Permissions tab, there is a 'User Information' section with a 'Refresh' button and a form to 'Add an Active Directory user or group' with an 'Add' button. Below this is a table of users:

Type	Display Name ^	Username	Role	Action	Delete
	All Users		User	Edit	
	Administrator	MEGACORP\Administrator	Administrator		

Below the table is a 'Phone Information' section showing 'Logon User: MEGACORP\Administrator'.

The "System Settings" area contains four tabs:

- Permissions
- Additional Links
- Log
- Multi-User

Each section is covered below.

Permissions

The "Permissions" section enables the administrator to perform the following actions:

- Add and Remove Users and Groups
- Assign Roles to Users and Groups

- Assign Workgroup Permissions to Users and Groups
- Assign Key Programming Permissions to Users and Groups

Live Desktop Portal Roles

Live Desktop Portal defines two roles which can be assigned to a user. The role defines the level of access which the user will have when they login to Live Desktop Portal. The roles are described in the table below.

User Role	Description
User	Enables the user to login to Live Desktop Portal and program keys on their own phone.
Administrator	Can program any phone that Live Desktop Portal can locate. Also enables the user to add and delete users and groups, assign access levels, assign key programming permissions, and view system logs.

 **Note:** The Key Programmer role has been deprecated in this release of Live Content Suite.

All Users

When you login to Live Desktop Portal for the first time you will notice the following two entries in the Permissions tab on the System Settings page:

- Administrator – The user who ran the Configuration Wizard is added as the default administrator.
- All Users – Any user in the domain who is able to authenticate.

By default the “All Users” group is granted the ‘User’ role. This means that all users in the domain can login and will be granted permissions assigned to the “All Users” group. If you do not want to give access to everyone you should change the access for the role for the “All Users” group to ‘No Access’.

 **Note:** Every user or group you add to Live Desktop Portal inherits the settings assigned to the “All Users” role.

Adding Live Desktop Portal Users

As an Administrator you can give Active Directory users access to Live Desktop Portal on an individual basis by adding the user to Live Desktop Portal and then assigning them a role.

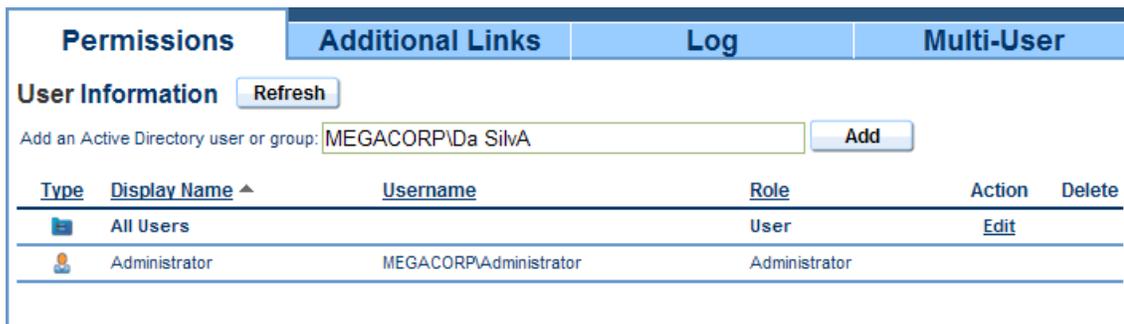
Use the following procedure to add a user and assign them a role:

1. On the “Permissions” page, type the user name in the “Add an Active Directory user or group” text box. Notice that the system returns search results after typing a few characters.



Note: Users are matched by their Active Directory login name (SAMAccountname). You should be aware of your organization’s naming convention for user account names.

2. Select the user or group from the available matches and click “Add”.



3. The user appears in the list below.



Note: Notice that the user is assigned the 'User' role. By default any user or group you add will be assigned the 'User' role. You can change it as needed as shown in the "Changing Roles for Live Desktop Portal Users" section below.

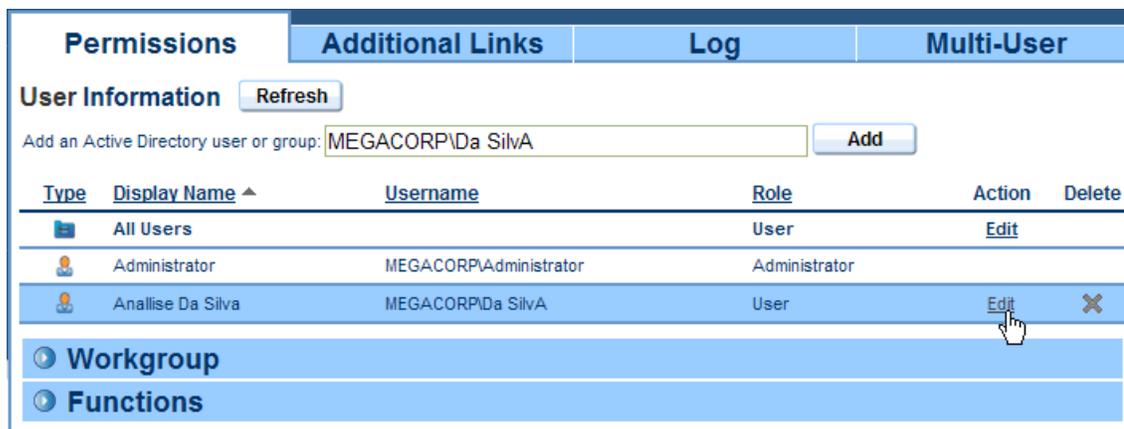
You use the same procedure to add a User or Administrator, except that you set the role to the appropriate level.

Changing Roles for Live Desktop Portal Users

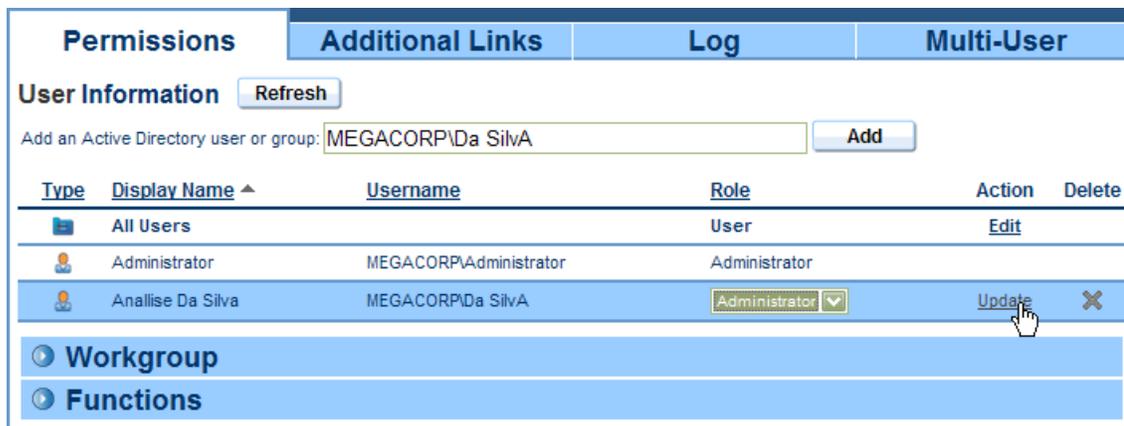
You can assign a user or group a role when you add them to Live Desktop Portal. You can also change their role at any time.

The following example illustrates how to change the role for a user from 'User' to 'Administrator':

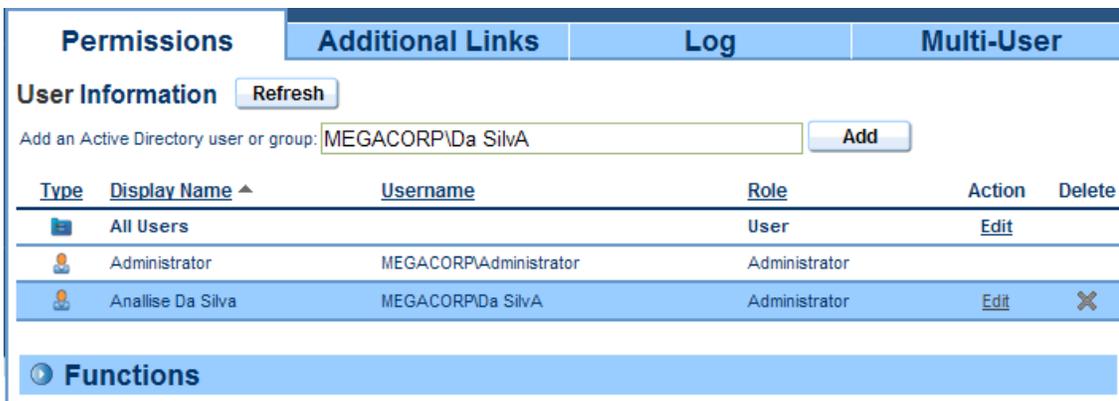
1. On the "Permissions" page select the user in the list of users and groups and click "Edit".



2. Select the 'Administrator' role under the "Role" column and click "Update".



3. The user will now have their role set to 'Administrator' in the "Role" column.



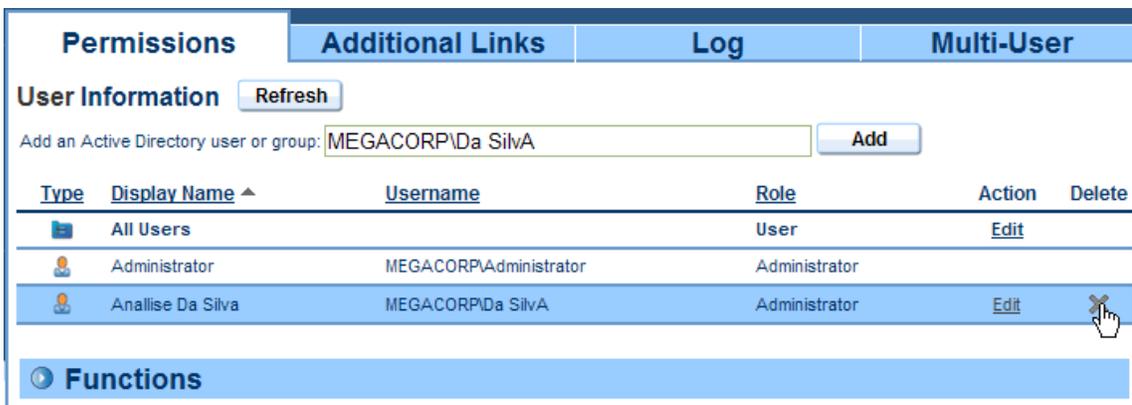
You use the same procedure to change the user’s role to: User, Administrator, and No Access.

Deleting Live Desktop Portal Users

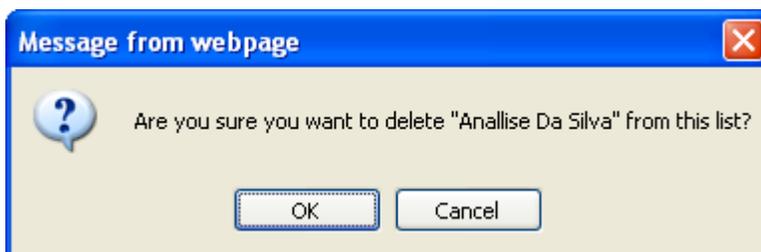
As an Administrator you can delete existing users as needed.

Use the following procedure to delete an existing user:

1. On the “Permissions” page, select the user in the list.
2. Click on the delete icon in the row for the user.



3. Click **OK** to confirm the deletion.



When you delete a user it deletes the user from the database along with any Key Programming and Workgroup permissions assigned to them explicitly, but it does not delete the Live Content

programming for their phone from the database. If this user is a member of any defined groups (other than the All Users group), then they will retain the access and permissions inherited from those groups. If you want to prevent one particular user from having access to the Live Desktop Portal, assign them the No Access role directly.

 **Note:** If you also want to clear all of their key programming you should select their phone and clear all keys. You should clear all key programming if their DN is being assigned to another user. Otherwise it is possible for private information to be viewable by the new user. You must clear all keys before deleting the DN from the MCD host.

On the other hand, you may want to preserve their programming and allow them to continue accessing Live Desktop Portal via group membership. In this case (as explained above) their role and key programming permissions will be derived by their group membership.

Providing Access to Live Desktop Portal through Groups

Using Live Desktop Portal you can add Active Directory groups as well as users. This enables you to give users access to Live Desktop Portal through their existing Active Directory group membership.

The process for adding a group and assigning it a role is the exact same as for users, except that you provide the name of the Active Directory group. Once you've added a group and assigned it a role, any user in the group can login to Live Desktop Portal under the role assigned to the group.

The process for deleting a group is also the same as it is for users. When you delete a group the group is removed from the database along with all key programming permissions. Any users who are a member of the group may see a change in their role and effective key programming permissions.

Combined Permissions

If a user is added explicitly to Live Desktop Portal as an individual and they are also in a group which has access, they will have the access level assigned to their user account. For example, if their user account is assigned the "User" role and they are a member of a group that has "Administrator" role, then they will have the access rights of a user.

If a user is a member of multiple groups but they are not added to Live Desktop Portal as an individual, then their access level will be the highest level assigned to any of the groups. For example, if they are in a group named "Sales" that is assigned the "User" role, and they are a member of a group named "Managers" that has the "Administrator" role, then they will have the access rights of an Administrator. The same is true if the user is a member of nested groups – the user will be granted the greatest role inherited from any group they are a member of.

If any of the groups is assigned the "No Access" role, the user will receive the highest level of access granted to the other groups of which they are a member.

Single Domain Group Requirements

When you deploy Live Content Suite in an environment with one domain, you can add any of the following types of Active Directory groups to Live Desktop Portal:

- Global Security groups
- Domain Local Security groups
- Universal Security groups

Groups may be nested and can contain other groups of any kind.

 **Note:** You should not use Distribution Groups for providing access to Live Desktop Portal

Multiple Domain Group Requirements (Active Directory Forest)

When you deploy Live Content Suite in an environment with more than one domain, such as an Active Directory forest, you cannot use Global groups or Domain local groups. You can add the following types of Active Directory groups to Live Desktop Portal:

- Universal Security groups

Groups may be nested but can only contain other Universal groups.

Refresh

The “Permissions” page has a ‘Refresh’ button. You use this button to refresh the users and groups displayed in the list to reflect any changes in Active Directory. You should use the ‘Refresh’ button when the following Active Directory changes occur:

- An Active Directory user or group has been deleted by a domain administrator.
- An Active Directory user or group has been renamed by a domain administrator

Until you click the ‘Refresh’ button, the name change or deletion will not be reflected in Live Desktop Portal.

Group Members

You can view the members of any group that has been added to Live Desktop Portal. To view the members of a group perform the following steps:

1. Select the group in the Permissions area.

Permissions | Additional Links | Log | Multi-User

User Information

Add an Active Directory user or group:

Type	Display Name ^	Username	Role	Action	Delete
	All Users		User	Edit	
	Administrator	MEGACORP\Administrator	Administrator		
	Anallise Da Silva	MEGACORP\Da Silva	Administrator	Edit	<input type="button" value="X"/>
	LCS-Key-Programmers	MEGACORP\LCS-Key-Programmers	User	Edit	<input type="button" value="X"/>

Group Members
 Workgroup
 Functions

Note: The example above shows the view when the 'Group Members' list is collapsed. i.e. the triangle is pointing up.

- Click the triangle beside 'Group Members' to expand the view and display the members of the group. i.e. the triangle should point down. The 'Group Members' list is only available when you select a group.

Permissions | Additional Links | Log | Multi-User

User Information

Add an Active Directory user or group:

Type	Display Name ^	Username	Role	Action	Delete
	All Users		User	Edit	
	Administrator	MEGACORP\Administrator	Administrator		
	Anallise Da Silva	MEGACORP\Da Silva	Administrator	Edit	<input type="button" value="X"/>
	LCS-Key-Programmers	MEGACORP\LCS-Key-Programmers	User	Edit	<input type="button" value="X"/>

Group Members
 Workgroup
 Functions

			1 2 3 4 5 6 7 8 9 10 ... >>									
Type	Display Name	Username										
	Chip Niedens	MEGACORP\NiedensC										
	Bosiljka Coxall	MEGACORP\CoxallB										
	Carola Hoehling	MEGACORP\HoehlinC										
	Candida Hruska	MEGACORP\HruskaC										
	Brand Pantalone	MEGACORP\PantaloB										
	Anna-diana Taki	MEGACORP\TakiA										
	Aleta Security	MEGACORP\SecurityA										
	Begum Thisdel	MEGACORP\ThisdelB										
	Betty-Ann IrcInternal-Docs	MEGACORP\IrcInteB										
	Caridad Cribbs	MEGACORP\CribbsC										

Workgroup
 Functions

The group members appear in a paginated list, with each page assigned a number. You can click on any number to view the group members displayed on that page. Click on the ... to jump to the

next or previous group of ten pages. Click on the << or >> to jump to the front of the list or the end of the list.

You can collapse the 'Group Members' list by clicking on the triangle again.



Workgroup

Live Content Suite 1.1 introduces the concept of Workgroups. Every user or group has a Workgroup, which is comprised of a list of users or groups. A user can program the phone of any user or group member who has been added to their Workgroup, in addition to their own phone.

The Workgroup area only displays if you select a user or group that holds the 'User' role. The Workgroup area can be expanded or collapsed by clicking on the triangle icon.

Adding to a Workgroup

To add a user or group to a Workgroup, perform the following steps:

1. Select the user or group whose Workgroup you want to change.
2. Expand the Workgroup area.

Permissions	Additional Links	Log	Multi-User		
User Information <input type="button" value="Refresh"/>					
Add an Active Directory user or group:			<input type="text" value="MEGACORP\LCS-Key-Programmers"/>		
			<input type="button" value="Add"/>		
Type	Display Name ▲	Username	Role	Action	Delete
	All Users		User	Edit	
	Administrator	MEGACORP\Administrator	Administrator		
	Anallise Da Silva	MEGACORP\Da Silva	User	Edit	<input type="button" value="X"/>
	LCS-Key-Programmers	MEGACORP\LCS-Key-Programmers	User	Edit	<input type="button" value="X"/>
Workgroup					
Specify the Active Directory Groups and Users whose phones this user can program.					
Add an Active Directory user or group:			<input type="text"/>		
			<input type="button" value="Add"/>		
Inherited Permissions					
None					
Functions					

3. In the 'Add an Active Directory user or group' text field type the name of a user or group in Active Directory that you want to add to the Workgroup permissions.
4. Select the target user or group from the list of matches and click 'Add'.

Permissions | **Additional Links** | **Log** | **Multi-User**

User Information

Add an Active Directory user or group:

Type	Display Name ^	Username	Role	Action	Delete
	All Users		User	Edit	
	Administrator	MEGACORP\Administrator	Administrator		
	Anallise Da Silva	MEGACORP\Da Silva	User	Edit	

Workgroup

Specify the Active Directory Groups and Users whose phones this user can program.

Add an Active Directory user or group:

Inherited Permissions

None

Functions

5. The user or group is added to the Workgroup.

Permissions | **Additional Links** | **Log** | **Multi-User**

User Information

Add an Active Directory user or group:

Type	Display Name ^	Username	Role	Action	Delete
	All Users		User	Edit	
	Administrator	MEGACORP\Administrator	Administrator		
	Anallise Da Silva	MEGACORP\Da Silva	User	Edit	

Workgroup

Specify the Active Directory Groups and Users whose phones this user can program.

Add an Active Directory user or group:

Type	Display Name	Username	Delete
	Jamie Jones	MEGACORP\Jamie	

Inherited Permissions

None

Functions

Now Analise can program Jamie Jone's phone.

You can also add a group to the user's Workgroup using the same steps – just type the name of a group to select. In the example below the group "Marketing Dept" has been added to Analise's Workgroup.

Permissions
Additional Links
Log
Multi-User

User Information Refresh

Add an Active Directory user or group: Add

Type	Display Name [▲]	Username	Role	Action	Delete
All Users			User	Edit	
Administrator		MEGACORP\Administrator	Administrator		
Analise Da Silva		MEGACORP\Da Silva	User	Edit	✕

Workgroup

Specify the Active Directory Groups and Users whose phones this user can program.

Add an Active Directory user or group: Add

Type	Display Name	Username	Delete
Jamie Jones		MEGACORP\Jamie	✕
Marketing Dept		MEGACORP\Marketing Dept	✕

Inherited Permissions

None

Functions

Now Analise can program Jamie's phone and the phone of anyone who is a member of the "Marketing Dept" group.

Note: To program another user's phone in this situation, they must have their DN entered in the correct Active Directory field.

Removing from a Workgroup

To remove a user or group from a Workgroup, perform the following steps:

1. Select the user or group whose Workgroup you want to change.
2. Expand the Workgroup area.
3. Locate the user or group you wish to remove from the Workgroup permissions and click the delete icon for that entry.

Permissions | **Additional Links** | **Log** | **Multi-User**

User Information

Add an Active Directory user or group:

Type	Display Name ^	Username	Role	Action	Delete
	All Users		User	Edit	
	Administrator	MEGACORP\Administrator	Administrator		
	Anallise Da Silva	MEGACORP\Da Silva	User	Edit	

Workgroup

Specify the Active Directory Groups and Users whose phones this user can program.

Add an Active Directory user or group:

Type	Display Name	Username	Delete
	Jamie Jones	MEGACORP\Jamie	
	Marketing Dept	MEGACORP\Marketing Dept	

Inherited Permissions

None

Functions

4. Click 'OK' to confirm the deletion. The user is removed from the Workgroup.

Permissions | **Additional Links** | **Log** | **Multi-User**

User Information

Add an Active Directory user or group:

Type	Display Name ^	Username	Role	Action	Delete
	All Users		User	Edit	
	Administrator	MEGACORP\Administrator	Administrator		
	Anallise Da Silva	MEGACORP\Da Silva	User	Edit	

Workgroup

Specify the Active Directory Groups and Users whose phones this user can program.

Add an Active Directory user or group:

Type	Display Name	Username	Delete
	Marketing Dept	MEGACORP\Marketing Dept	

Inherited Permissions

None

Functions

In the example shown, Analise can no longer program Jamie's phone.

Program All Phones

To allow a person or group to program any phone on any switch you can add the 'All Users' group to their Workgroup permissions. In this situation the DN does not need to be added to Active Directory.

You add the 'All Users' group using the same procedure for any other group – just type the name and add it.

In the example shown below, the "All Users" group has been added to Analise's Workgroup. Analise can now program any phone that Live Desktop Portal can locate.

Permissions
Additional Links
Log
Multi-User

User Information Refresh

Add an Active Directory user or group: Add

Type	Display Name ^	Username	Role	Action	Delete
	All Users		User	Edit	
	Administrator	MEGACORP\Administrator	Administrator		
	Anallise Da Silva	MEGACORP\Da Silva	User	Edit	X

Workgroup

Specify the Active Directory Groups and Users whose phones this user can program.

Add an Active Directory user or group: Add

Type	Display Name	Username	Delete
	All Users		X

Inherited Permissions

None

Functions

Inherited and Combined Workgroup Permissions

A user inherits Workgroup memberships from all groups of which they are a member. Workgroup membership which a user inherits are displayed under 'Inherited Permissions' when you select the user.

You cannot delete a user's inherited Workgroup memberships.

A user's effective Workgroup is a combination of the Workgroup membership assigned to them as an individual and the Workgroup membership of each group of which they are a member.

In the example shown below, Analise has inherited permission to program phones for any member of "Manager Group".

Permissions
Additional Links
Log
Multi-User

User Information Refresh

Add an Active Directory user or group: Add

Type	Display Name ^	Username	Role	Action	Delete
	All Users		User	Edit	
	Administrator	MEGACORP\Administrator	Administrator		
	Anallise Da Silva	MEGACORP\Da Silva	User	Edit	X
	Phone Programmers	MEGACORP\Phone Programmers	User	Edit	X

Workgroup

Specify the Active Directory Groups and Users whose phones this user can program.

Add an Active Directory user or group: Add

Type	Display Name	Username	Delete
	Marketing Dept	MEGACORP\Marketing Dept	X

Inherited Permissions

Type	Display Name	Username
	Manager Group	MEGACORP\Manager Group

Functions

Workgroup Permissions and User Roles

The Workgroup permissions are only available for the 'User' role. If you select an Administrator you will not see the Workgroup area.

When you change a user or group's role from 'User' to 'Administrator' they Workgroup permissions are discarded. This means that if you have any Workgroup permissions defined for a user and you change their role to Administrator, and then back to User – the Workgroup permissions will be lost. In this case you must re-assign the Workgroup permissions.

Functions

Live Desktop Portal provides the ability to assign key programming permissions to users and groups. This enables you to give a user or group the permission to program specific functions while not allowing them to program others.

To assign key programming you should expand the "Functions" view by clicking the triangle beside the functions label. The key programming permissions for the currently selected user or group will be displayed. You can collapse the view by clicking the triangle icon again.

The example below shows the default permissions for the "All Users" group:

Permissions
Additional Links
Log
Multi-User

User Information Refresh

Add an Active Directory user or group: Add

Type	Display Name ^	Username	Role	Action	Delete
	All Users		User	Edit	
	Administrator	MEGACORP\Administrator	Administrator		
	Anallise Da Silva	MEGACORP\Da Silva	User	Edit	X
	Phone Programmers	MEGACORP\Phone Programmers	User	Edit	X

Workgroup

Functions

Available Functions

- ACD
- Analog Line
- Call Announce
- Call History View
- Call Park
- Call Park - Retrieve
- Call Pickup
- Callback
- Campon
- Cancel
- CDE Speedcall
- Customize: Branding
- Customize: Call Forwarding
- Customize: Clear All Phone Keys

Allowed Functions

- Account Code Non-Verified
- Account Code Verified
- Auto Answer
- Customize: Screen Saver
- Do Not Disturb
- Emergency Call
- Forwarding
- Group Presence
- Handoff
- Headset
- Music
- Personal Presence
- Phone Application
- Phone Lock

Denied Functions

Drag and drop functions between columns.

Legend

- Inherited Function
- Inherited Function (Denied By Parent)

Save
Cancel

You will see the three columns shown above, described in the table below.

Column	Description
Available Functions	Shows a list of functions which you can assign to a user or group. Functions which appear in this list for a user or group will not be available to that user or group during key programming.
Allowed Functions	Shows a list of functions which have been assigned to the user or group. The list will include functions assigned explicitly as well as functions which are inherited from group membership. Keep in mind that the COS settings on the MCD switch may prevent a user from programming a function which is in the "Allowed Functions" list.
Denied Functions	Shows functions which are explicitly denied for a user or group, regardless of other permissions. Denied functions override allowed functions. For example, if a user is a member of a group that has the "Do Not Disturb" function in their "Allowed Functions" list, and they are a member of another group which has "Do Not Disturb" in the "Denied Functions" list, then the user will not be able to program a key with "Do Not Disturb".



Customize Functions

Live Content Suite 1.1 introduces several functions which were not available in the previous release. They are described in the table below.

Function Name	Function Description
Customize: Branding	<p>Enables a user to program their phone with a branding application which the Administrator has uploaded to the MCD host.</p> <p>Branding applications allow you to customize the appearance of the phone GUI and are created using Mitel HTML Toolkit.</p> <p>“Branding...” becomes available under ‘Customize’ if a user is assigned the ‘Customize: Branding’ function.</p>
Customize: Call Forward	<p>Enables a user to program their phone’s Call Forwarding settings. The Call Forwarding setting applies to Call Forward Always.</p> <p>“Call Forwarding...” becomes available under ‘Customize’ if a user is assigned the ‘Customize: Call Forward’ function.</p>
Customize: Clear All Phone Keys	<p>Enables a user to clear all key programming on their phone.</p> <p>“Clear All Phone Keys” becomes available under ‘Customize’ if a user is assigned the ‘Customize: Clear All Phone Keys’ function.</p> <p>Only use the “Clear All Phones” feature when you are sure you want to clear all programming – it can not be undone.</p>
Customize: Screensaver	<p>Enables a user to program their phone with any screensaver that is deployed to their MCD host, including Live Content screensavers such as Blogger, Twitter, etc.</p> <p>If a user’s phone is configured with a branding screensaver the screensaver they program using Live Desktop Portal will override it. If they clear their screensaver programming using Live Desktop Portal their phone will revert to the default screensaver, in which case any branding screensaver will override the default screensaver.</p> <p>“Screen Saver...” becomes available under ‘Customize’ if a user is assigned the ‘Customize: Screensaver’ function.</p>
Customize: Voicemail	<p>Enables a user to program their Voicemail to E-Mail forwarding setting. The Administrator must enable Forward to E-Mail in ESM.</p> <p>“Voicemail...” becomes available under ‘Customize’ if a user is assigned the ‘Customize: Voicemail’ function.</p>

Assigning Functions

To assign a user or group a new function, thus enabling them to program that function, perform the following steps:

1. Select the user or group and expand the “Functions” view.

Permissions | **Additional Links** | **Log** | **Multi-User**

User Information

Add an Active Directory user or group:

Type	Display Name ^	Username	Role	Action	Delete
	All Users		User	Edit	
	Administrator	MEGACORP\Administrator	Administrator		
	Anallise Da Silva	MEGACORP\Da Silva	User	Edit	
	Phone Programmers	MEGACORP\Phone Programmers	User	Edit	

Workgroup

Functions

Available Functions	Allowed Functions	Denied Functions
ACD	Account Code Non-Verified	
Analog Line	Account Code Verified	
Call Announce	Auto Answer	
Call History View	Customize: Screen Saver	
Call Park	Do Not Disturb	
Call Park - Retrieve	Emergency Call	
Call Pickup	Forwarding	
Callback	Group Presence	
Campon	Handoff	
Cancel	Headset	
CDE Speedcall	Music	
Customize: Branding	Personal Presence	
Customize: Call Forwarding	Phone Application	
Customize: Clear All Phone Keys	Phone Lock	

Drag and drop functions between columns.

Legend

- Inherited Function
- Inherited Function (Denied By Parent)

2. Select a function in the “Available Functions” and drag it over to the “Allowed Functions” list. In this example we move the “ACD” function over.
3. Click “Save”.

Permissions
Additional Links
Log
Multi-User

User Information Refresh

Add an Active Directory user or group: Add

Type	Display Name ^	Username	Role	Action	Delete
	All Users		User	Edit	
	Administrator	MEGACORPAdministrator	Administrator		
	Anallise Da Silva	MEGACORPDa Silva	User	Edit	X
	Phone Programmers	MEGACORPPhone Programmers	User	Edit	X

Workgroup

Functions

Available Functions

- Analog Line
- Call Announce
- Call History View
- Call Park
- Call Park - Retrieve
- Call Pickup
- Callback
- Campon
- Cancel
- CDE Speedcall
- Customize: Branding
- Customize: Call Forwarding
- Customize: Clear All Phone Keys
- Customize: Voicemail

Allowed Functions

- ACD
- Account Code Non-Verified
- Account Code Verified
- Auto Answer
- Customize: Screen Saver
- Do Not Disturb
- Emergency Call
- Forwarding
- Group Presence
- Handoff
- Headset
- Music
- Personal Presence
- Phone Application

Denied Functions

Drag and drop functions between columns.

Legend

- Inherited Function
- Inherited Function (Denied By Parent)

Save Cancel

Note: Notice that the “ACD” function is listed in the “Allowed Functions” in a different color from the other functions. This is because the other functions are inherited from the “All Users” group while the “ACD” function is assigned directly to the user.

The user should now be able to program a key with the “ACD” function, unless COS settings prevent them from doing so.

Denying Functions

If you want to prevent a user from programming a specific function you can deny them the function. Denied functions override the allowed functions. This means if the user inherits the ability to program a key from one group, and inherits the key as a denied function from another group, then the user will not be able to program the function at all.

Note: If you deny previously programmed functions for a user they will still be able to use the key on the phone, but they will not be able to change the label for the key or program a fresh one.

To deny a user or group a function, thus preventing them from programming that function, perform the following steps:

1. Select the user or group and expand the “Functions” view.

The screenshot shows the 'Permissions' management interface. At the top, there are tabs for 'Permissions', 'Additional Links', 'Log', and 'Multi-User'. Below the tabs is the 'User Information' section, which includes a 'Refresh' button and a text input field for adding an Active Directory user or group, with an 'Add' button. Below this is a table listing users and their roles.

Type	Display Name	Username	Role	Action	Delete
Folder icon	All Users		User	Edit	
Person icon	Administrator	MEGACORP\Administrator	Administrator		
Person icon	Anallise Da Silva	MEGACORP\Da Silva	User	Edit	X
Folder icon	Phone Programmers	MEGACORP\Phone Programmers	User	Edit	X

Below the table, there are two expandable sections: 'Workgroup' and 'Functions'. The 'Functions' section is expanded, showing three columns: 'Available Functions', 'Allowed Functions', and 'Denied Functions'.

Available Functions:

- Analog Line
- Call Announce
- Call History View
- Call Park
- Call Park - Retrieve
- Call Pickup
- Callback
- Campon
- Cancel
- CDE Speedcall
- Customize: Branding
- Customize: Call Forwarding
- Customize: Clear All Phone Keys
- Customize: Voicemail

Allowed Functions:

- ACD
- Account Code Non-Verified
- Account Code Verified
- Auto Answer
- Customize: Screen Saver
- Do Not Disturb
- Emergency Call
- Forwarding
- Group Presence
- Handoff
- Headset
- Music
- Personal Presence
- Phone Application

Denied Functions: (Empty list)

At the bottom, there is a legend with two items:

- Inherited Function
- Inherited Function (Denied By Parent)

There are 'Save' and 'Cancel' buttons at the bottom right.

2. Select a function from the “Available Functions” list and drag it over to the “Denied Functions” list. In this example we will use the ‘Call History View’ function.
3. Click “Save”.
4. You will encounter a warning. Make sure you understand the warning and then click OK to save the changes.

Permissions
Additional Links
Log
Multi-User

User Information Refresh

Add an Active Directory user or group: Add

Type	Display Name ^	Username	Role	Action	Delete
	All Users		User	Edit	
	Administrator	MEGACORP\Administrator	Administrator		
	Anallise Da Silva	MEGACORP\Da Silva	User	Edit	X
	Phone Programmers	MEGACORP\Phone Programmers	User	Edit	X

Workgroup

Functions

Available Functions

- Analog Line
- Call Announce
- Call Park
- Call Park - Retrieve
- Call Pickup
- Callback
- Campon
- Cancel
- CDE Speedcall
- Customize: Branding
- Customize: Call Forwarding
- Customize: Clear All Phone Keys
- Customize: Voicemail
- Direct Page

Allowed Functions

- ACD
- Account Code Non-Verified
- Account Code Verified
- Auto Answer
- Customize: Screen Saver
- Do Not Disturb
- Emergency Call
- Forwarding
- Group Presence
- Handoff
- Headset
- Music
- Personal Presence
- Phone Application

Denied Functions

- Call History View

Drag and drop functions between columns.

Legend

- Inherited Function
- Inherited Function (Denied By Parent)

Save Cancel

Now the user will not be able to program a key with “Call History View” even if they inherit the ability to from their group membership.

Inherited Functions

A user inherits both allowed and denied functions from all groups of which they are a member. Allowed and denied functions which are assigned directly to a user or group are shown in blue, while inherited functions are shown in two different colors – one for allowed and one for denied. The example below illustrates the distinction.

Permissions		Additional Links	Log	Multi-User
User Information <input type="button" value="Refresh"/>				
Add an Active Directory user or group: <input type="text"/>				<input type="button" value="Add"/>
Type	Display Name ^	Username	Role	Action Delete
	All Users		User	Edit
	Administrator	MEGACORPAdministrator	Administrator	
	Anallise Da Silva	MEGACORPDa Silva	User	Edit <input type="button" value="X"/>
	Phone Programmers	MEGACORPPhone Programmers	User	Edit <input type="button" value="X"/>
Workgroup				
Functions				
Available Functions		Allowed Functions	Denied Functions	
<ul style="list-style-type: none"> Analog Line Call Announce Call Park - Retrieve Call Pickup Callback Campon Cancel CDE Speedcall Customize: Branding Customize: Call Forwarding Customize: Clear All Phone Keys Customize: Voicemail Direct Page Double Flash 		<ul style="list-style-type: none"> ACD Account Code Non-Verified Account Code Verified Auto Answer Customize: Screen Saver Do Not Disturb Emergency Call Forwarding Group Presence Handoff Headset Music Personal Presence Phone Application 	<ul style="list-style-type: none"> Call History View Call Park 	
Drag and drop functions between columns.		Legend <input type="checkbox"/> Inherited Function <input type="checkbox"/> Inherited Function (Denied By Parent)	<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

In this example the user's effective permissions are a combination of assigned permissions and inherited permissions, identified as follows:

- Assigned "Allowed Functions" – The "ACD" function is assigned directly to the user.
- Inherited "Allowed Functions" – All other functions listed in "Allowed Functions" are inherited from the user's group membership. This includes functions inherited from the "All Users" group.
- Assigned "Denied Functions" – The "Call History View" function is directly denied for the user.
- Inherited "Denied Functions" – The "Call Park" function is denied for a group which the user is a member of.

It is possible to move inherited functions from the "Allowed Functions" column to the "Denied Functions" column but not to the "Available Functions" column. When you move an inherited function from "Allowed Functions" to "Denied Functions" it shows up in yellow.

Building on the previous example, the "Music" function has been moved from "Allowed Functions" to "Denied Functions", as shown below. Since "Music" was previously inherited as "Allowed", it will show as yellow.

Permissions | **Additional Links** | **Log** | **Multi-User**

User Information

Add an Active Directory user or group:

Type	Display Name ^	Username	Role	Action	Delete
	All Users		User	Edit	
	Administrator	MEGACORPAdministrator	Administrator		
	Anallise Da Silva	MEGACORP Da Silva	User	Edit	<input type="button" value="X"/>
	Phone Programmers	MEGACORPPhone Programmers	User	Edit	<input type="button" value="X"/>

Workgroup

Functions

Available Functions	Allowed Functions	Denied Functions
Analog Line	ACD	Call History View
Call Announce	Account Code Non-Verified	Music
Call Park - Retrieve	Account Code Verified	Call Park
Call Pickup	Auto Answer	
Callback	Customize: Screen Saver	
Campon	Do Not Disturb	
Cancel	Emergency Call	
CDE Speedcall	Forwarding	
Customize: Branding	Group Presence	
Customize: Call Forwarding	Handoff	
Customize: Clear All Phone Keys	Headset	
Customize: Voicemail	Personal Presence	
Direct Page	Phone Application	
Double Flash	Phone Lock	

Drag and drop functions between columns.

Legend
 Inherited Function
 Inherited Function (Denied By Parent)

You cannot move “Inherited Functions (Denied by Parent)” from the “Denied Functions” column to any other column. For example, in the example above you cannot move “Call Park” into “Available Functions” or “Allowed Functions”.

Note: If you set "All Users" to 'No Access', users and groups still inherit the key permissions from the "All Users" group.

Selecting Multiple Functions

When you assign allowed or denied functions you can select more than one function by holding the control key while selecting each individual functions, or the shift key to select a range of functions. You can then drag the selected keys into the required column.

Additional Links

You use the “Additional Links” page to add custom links to the Live Desktop Portal page. The default appearance is shown below.



Adding a Link

Perform the following steps to add a custom link to Live Desktop Portal:

1. Navigate to System Settings → Additional Links.
2. Click on the “Add” button.
3. Enter a Link Name and Target URL.

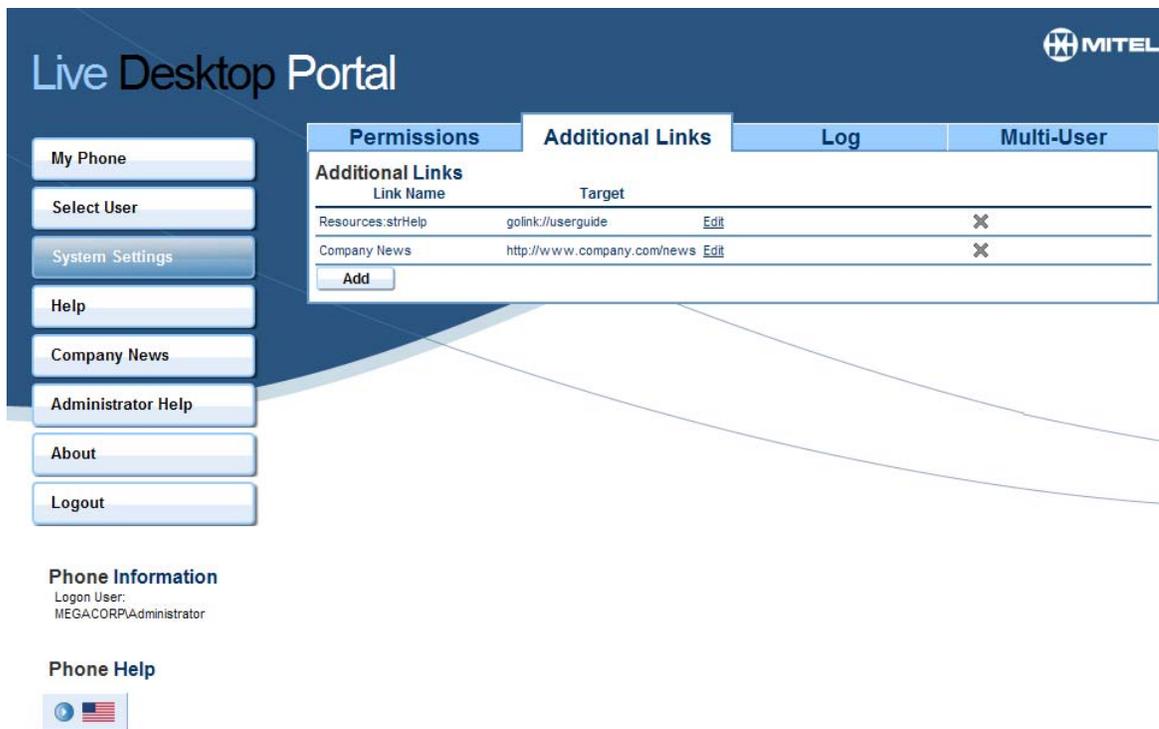
Link Name:

Target:

4. Click “Add” again to save changes.



Press F5 to refresh the browser page. The Custom Link will appear in the left hand column as shown below.



Editing a Link

You can change the Target URL for an existing link.

Perform the following steps to edit the URL:

1. Navigate to System Settings → Additional Links.
2. Select an existing link and click “Edit”
3. Modify the target URL to meet the new requirements and click on “Update”

Deleting a Link

You can delete any existing link.

Perform the following steps to delete a link:

1. Navigate to System Settings → Additional Links.
2. Select an existing link and click “X” on the right,



The link is removed from the list.

Help Go-Link

There is a default link listed when you first login to Live Desktop Portal. The link is defined with the following values:

Link Name: Resources:strHelp

Target: golink://userguide

This is the link for the “Help” option displayed in Live Desktop Portal. This is an internally defined link and has special syntax unlike normal names and URLs.

The default target is a go-link that points to the online document provided by Mitel. If you wish to provide an alternate target you can edit the link and change the target to suit your needs.

 **Note:** The target URL can be any valid URL e.g. www.company.com/help

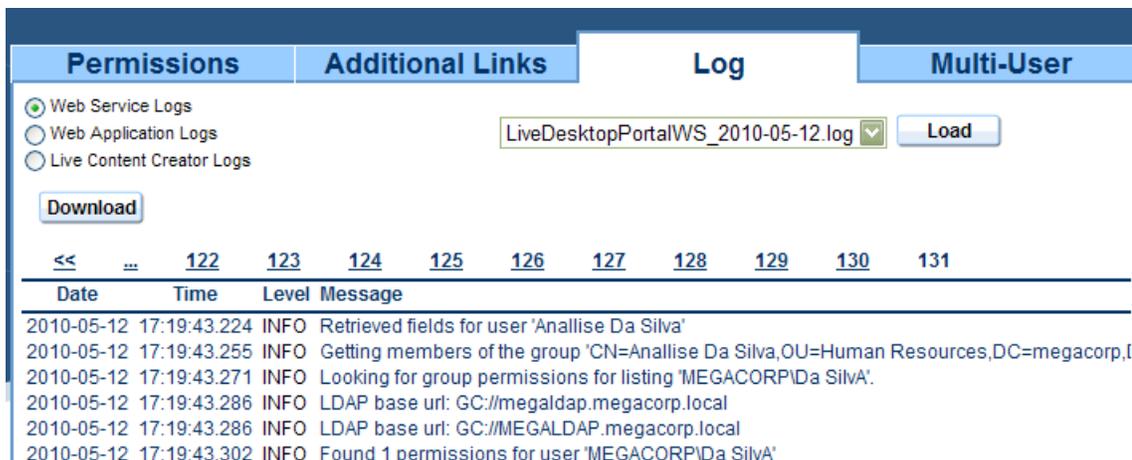
One potential use for this is to enable a company to provide their own online help for users for programming custom HTML applications. Help is not provided with live Desktop Portal for custom HTML applications.

Log Page

You use the “Log” page to view log entries for each of the following web components:

- Live Desktop Portal Web Service
- Live Desktop Portal Web Application
- Live Content Creator Web Service

When you view the “Log” page the Web Service Logs for today are displayed by default.



The log displays with the most recent entries selected.

Changing Log Source

You can change the source used to retrieve log entries. There are three source options: Web Service Logs, and Web Application Logs, and Live Content Creator Logs. They are summarized in the table below.

Log Source	Description
Web Service Logs	<ul style="list-style-type: none"> • Logs actions related to the Live Desktop Portal Web Service. • Logs MCD switch access operations. • Logs Active Directory and user lookup operations. • Logs database operations.
Web Application Logs	<ul style="list-style-type: none"> • Logs actions related to the Live Desktop Portal web application. • Logs user login success and failure. • Logs web application activities.
Live Content Creator Logs	<ul style="list-style-type: none"> • Logs requests for Live Content

View the Service Logs by selecting the “Web Service Logs” radio button.



The Web Service logs will immediately load.

View the Web Application Logs by selecting the “Web Application Logs” radio button as shown below.

- Web Service Logs
 Web Application Logs
 Live Content Creator Logs

The Web Application logs will immediately load.

View the Live Content Creator Logs by selecting the “Live Content Creator Logs” radio button as shown below.

- Web Service Logs
 Web Application Logs
 Live Content Creator Logs

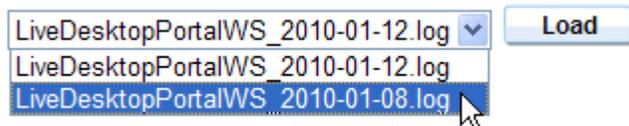
The Live Content Creator logs will immediately load.

Loading a Different Log File

By default the current day's logs are displayed. You can view a previous day's log file by selecting it in the dropdown menu.

The example below illustrates how to load an earlier log file for the Web Service log.

1. Ensure the “Web Service Logs” is selected.
2. Select the previous log file in the dropdown menu.



3. Click the “Load” button.



The contents for the log file will display below.

Downloading Log Files

You can download the current log file to your local computer as a CSV file by clicking the “Download Link”. When you click the link you are given the option of saving it locally or opening it directly.

You can view the downloaded file using Microsoft Excel or any other program which supports the CSV file format. You can then use the program to process the log file contents.

Navigating Log Contents

When you select a log to view the contents are displayed in a paginated view. By default the last page showing the most recent entries is selected.

<<	...	9	10	11	12	13	14	15	16	17	18
Date	Time	Level	Message								

You can view any page by clicking the number at the top. In the example below we've selected Page 10, which is indicated by the number not having a line beneath it.

1	2	3	4	5	6	7	8	9	10	...	>>
Date	Time	Level	Message								

You can jump to the very first page by clicking the << link, or jump to the very last page by clicking the >> link.

If you wish to jump to the next grouping of ten click on the ... link on either side.

Log Levels

The Web Application and Web Service logs both create log entries with the following levels:

Log Level	Description
INFO	Represents a normal operation that can be used to track the health of the application.
WARNING	Represents unexpected behavior that is recoverable by the application.
ERROR	Represents an unrecoverable operation resulting in end-user service issues.

The entries are color coded as shown.



Multi-User

Live Content Suite 1.1 introduces the “Multi-User” page which enables an Administrator to copy the programming from one source phone to a set of target phones. Using this feature you can program a phone in a specific way, and then clone that phone’s programming to one or more target phones.

Rollout

Cloning a source phone to one or more target phones is called a ‘rollout’. You use the Rollout page area to perform all rollout actions.

Overview of Rollout Procedure

The basic approach for rolling out phone programming is described in the following steps:

1. Program a source phone to have the programming you want.
2. Enter the source phone DN in the “Select the DN rollout” field. If you click on the “View” button it will open that phone in a new window so you can review or finalize the programming.
3. Select the items to rollout. Choose one or more of the following programming items: Key Programming, Screen Saver, and Branding. The programming items you select will be rolled out to the target phones.
4. Specify the phones to target either by group or DN range.
5. Select targeted models under “Advanced” – optional. Any targeted phones will be skipped if their model is not selected in the “Advanced” section. By default all supported models are selected.

The example shown below will read the programming for DN 32500 and copy Key Programming, Screen Saver, and Branding to the phone for each user in the ‘Sales Dept’ Active Directory Group.

Permissions | **Additional Links** | **Log** | **Multi-User**

Rollout

Select the DN to rollout:

Select the items to rollout:

- Key Programming
- Screen Saver
- Branding

Rollout To:

Group:

DN Range:

Example: 2267,5360,7000-8000

Advanced

Select the target models:

<input checked="" type="checkbox"/> 5304	<input checked="" type="checkbox"/> 5212	<input checked="" type="checkbox"/> 5224	<input checked="" type="checkbox"/> 5312	<input checked="" type="checkbox"/> 5324
<input checked="" type="checkbox"/> 5320	<input checked="" type="checkbox"/> 5330	<input checked="" type="checkbox"/> 5340	<input checked="" type="checkbox"/> 5360	<input checked="" type="checkbox"/> HotDesk

[Select All](#) | [Unselect All](#)

Rollout Activity History

None

The example below will read the programming for DN 32500 and copy the Screen Saver and Branding programming to all 5360 phones in the DN range from 32501 to 32510.

Permissions | **Additional Links** | **Log** | **Multi-User**

Rollout

Select the DN to rollout:

Select the items to rollout:

- Key Programming
- Screen Saver
- Branding

Rollout To:

Group:

DN Range:

Example: 2267,5360,7000-8000

Advanced

Select the target models:

<input type="checkbox"/> 5304	<input type="checkbox"/> 5212	<input type="checkbox"/> 5224	<input type="checkbox"/> 5312	<input type="checkbox"/> 5324
<input type="checkbox"/> 5320	<input type="checkbox"/> 5330	<input type="checkbox"/> 5340	<input checked="" type="checkbox"/> 5360	<input type="checkbox"/> HotDesk

[Select All](#) | [Unselect All](#)

Rollout Activity History

None

6. Once you have made your selections, click “Go”. You will encounter a warning that programming on all targeted phones will be overwritten. Click “OK” to initiate the rollout process.

During the rollout process Live Desktop Portal will read the programming for the source phone and replicate the programming on the target phones one at a time until the process has completed for all targeted phones. If any errors are encountered during programming, Live Desktop Portal will log the error and continue with the remaining programming. A summary of the rollout is displayed in the “Rollout Activity History” section.

More detail is provided below.

Programming Items

Using the rollout features you can clone the following programming items from the source phone to the target phones:

- **Key Programming** – Key programming from the source phone is replicated on the target phones. This includes traditional key programming, HTML applications, and Live Content applications such as Twitter, Flickr, etc.
- **Screen Saver** – The screensaver programming from the source phone will be replicated on the target phones. This only applies to phones that support screensavers.
- **Branding** – The branding application programming from the source phone will be replicated on the target phones. This only applies to phones that support branding applications.

You can choose which of the programming items to include in your rollout but you must select at least one.

Selecting Phones to Target

You can select the phones to target using the two mechanisms described below:

- **Group** – Provide the Active Directory group you wish to target by typing the name and selecting it from the list of matches. Any users who are a member of that group will have their phone added to the list of targeted phones – provided their DN is entered in Active Directory.
- **DN Range** – List the DNs to target using a comma separated list, DN range, or a combination of both. Example: 2267,5360,7000-8000.

Advanced – Filter by Phone Model

You can filter the targeted DNs by phone model. To filter by phone model you must expand the “Advanced” section and then select the phone models you wish to include in the rollout and de-select any phone models you wish to exclude from the rollout. If you exclude a model from the rollout it will prevent any phone of that model from being targeted even if the phone falls within the DN range.

Keep the following considerations in mind when targeting phones:

- HTML applications will only work on a targeted phone if the model supports it. They will be programmed on the phone but will not do anything.
- Licensed HTML applications will only work on a targeted phone if the phone has an HTML license.

- Targeted phones with different Class of Service settings may not be able to use all of the keys programmed.
- Any 5360 phones that you target must have an HTML Infrastructure license. If they do not, they will be skipped during rollout.
- If you target a phone which has never been programmed with Live Desktop Portal, the phone will be automatically licensed during the rollout. For instance, if you have 50 available licenses and you target 10 phones which are not licensed, after the rollout you will have 40 available licenses. The exception is for 5360 phones which do not require a license to be programmed by Live Desktop Portal. Administrators can view available licenses by clicking on the “About” dialog.
- Programmable key layouts vary for different Mitel phones. If there are more keys on the source phone than on the target phone, the keys will be programmed in order until there are no available keys on the target phone. The remaining keys will not be programmed.

You will get the best results if you target phones that are the same model as the source phone since the programmable key layout and feature-set is the same. If you target phones of a different model, Live Desktop Portal will attempt to program each key. If it encounters an error it will move on to the next key until it runs out of keys to program.

Rollout Activity History

The Rollout Activity History area displays a summary of the rollouts that have been run. You must expand the Rollout Activity History to view the existing history. You can collapse it to hide the view.

The following columns are included in the summary:

- **Date** – The date and time of the rollout.
- **Source DN** – The DN of the phone that was used as the source.
- **Target** – This either lists the DN range that was targeted in the rollout, or the Active Directory group that was targeted.
- **# Completed** – The number of target phones that were programmed during the rollout.
- **Status** – The result of the rollout. If the rollout encountered errors it will indicate so in the status. If there were no errors it will say ‘OK’. If errors are noted in the status message you can inspect the Web Service logs to look for entries that may describe the problem.

The example below shows the results for a successful rollout.

Permissions	Additional Links	Log	Multi-User										
<p>Rollout</p> <p>Select the DN to rollout: <input type="text" value="32500"/> <input type="button" value="View"/></p> <p>Select the items to rollout:</p> <p><input type="checkbox"/> Key Programming</p> <p><input checked="" type="checkbox"/> Screen Saver</p> <p><input checked="" type="checkbox"/> Branding</p> <p>Rollout To:</p> <p><input type="radio"/> Group: <input type="text"/></p> <p><input checked="" type="radio"/> DN Range: <input type="text" value="32501-32510"/> <input type="button" value="Go"/></p> <p><small>Example: 2267,5360,7000-8000</small></p>													
<p>Advanced</p>													
<p>Rollout Activity History</p> <table border="1"> <thead> <tr> <th>Date</th> <th>Source DN</th> <th>Target</th> <th># Completed</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>6/10/2010 11:32:34 AM</td> <td>32500</td> <td>32501-32510</td> <td>10</td> <td>OK</td> </tr> </tbody> </table>				Date	Source DN	Target	# Completed	Status	6/10/2010 11:32:34 AM	32500	32501-32510	10	OK
Date	Source DN	Target	# Completed	Status									
6/10/2010 11:32:34 AM	32500	32501-32510	10	OK									

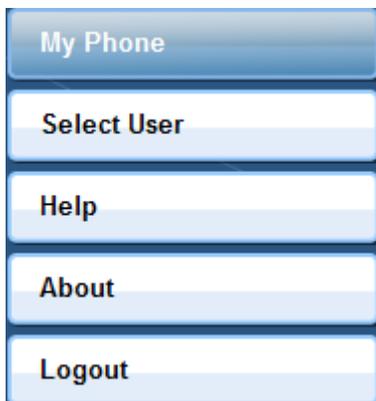
Select User

The “Select User” link is available for Administrators and for users who have been given permission to program other phones via their Workgroup configuration. You use the “Select User” feature to locate and program the phone for a user in the organization.

The menu available to Administrators is shown below.

- [My Phone](#)
- [Select User](#)
- [System Settings](#)
- [Help](#)
- [Administrator Help](#)
- [About](#)
- [Logout](#)

If a user has permission to program at least one other user’s phone via their Workgroup configuration, they will see the menu shown below.



Notice that both users have access to the “Select User” link but us does not have access to the System Settings page or the Administrator Help.

Users who do not have a user or group added to their Workgroup configuration will see the menu shown below.



Notice that they do not see the “Select User” link and therefore can only program their own phone.

Selecting a User by Username

Both Administrators and users with sufficient permissions can locate a user’s phone by providing the target user’s username.

When you provide the username Live Desktop Portal will look in the phone field for the user’s DN. If it finds a DN it will locate that DN on the switch or within the cluster. If the phone field is empty Live Desktop Portal will not be able to locate a phone for the user.

 **Note:** The phone field is specified when you run the Configuration Wizard.

Perform the following steps to select a user by their username:

1. Click on “Select User”.

2. Begin typing the user's username. (Login name). All matching results will be displayed.

 **Note:** If the user has a DN entered in their phone field it will be displayed in their listing.

3. Select the user from the list and click 'OK'.

Live Desktop Portal will attempt to locate the user's phone. Once the phone comes up the Administrator or user can begin programming the other user's phone. Refer to the User's Guide for detail on programming keys.

 **Note:** If multiple users or Administrators are programming the same phone, but separate keys, then both keys will be saved. If they attempt to program the same key the last one to save the change will take effect.

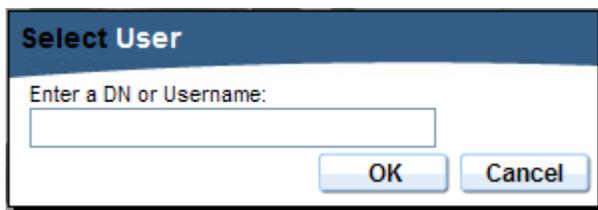
Selecting a User by DN

An Administrator can locate a user's phone by providing their DN. The Administrator can locate any supported phone on the switch by providing a valid DN.

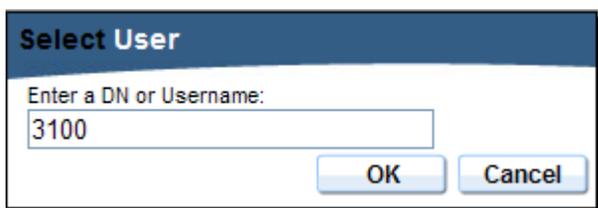
A user cannot locate another user's phone by DN unless they have the 'All Users' group added to their Workgroup permissions.

Perform the following steps to select a phone by DN:

1. Click on "Select User".



2. Enter the full DN and click 'OK'.



Live Desktop Portal will attempt to locate the phone. Once the phone comes up the Administrator or user can begin programming the phone. Refer to the User's Guide for detail on programming keys.

 **Note:** If multiple users are programming the same phone, but separate keys, then both keys will be saved. If they attempt to program the same key the last one to save the change will take effect.

Permissions When Programming another User's Phone

When an Administrator or user selects another user's phone they do not receive the key programming permissions assigned to that user - they maintain their personal key programming permissions. So if a user who is able to program screensavers selects the phone for a user who is not permitted to program a screensaver, then they will be able to program the user's phone with a screensaver.

Supporting Additional Languages

The Live Content Creator component generates the live content that displays on the phones by using the local instance of Internet Explorer. This means that the content will render on the phone as it will when you use Internet Explorer on the server.

You may find that some fonts are not rendered properly on the phone. This is normally because the font is not installed on the server. Mitel recommends that you enable 'Supplemental language support' on the server to support additional language fonts.

Until you enable supplemental language support Asian characters may appear on the phone as shown in the example below.

DAILY SPECIALS



Ling Ling Lunch

\$4.95

\$8.50

\$9.25

\$25

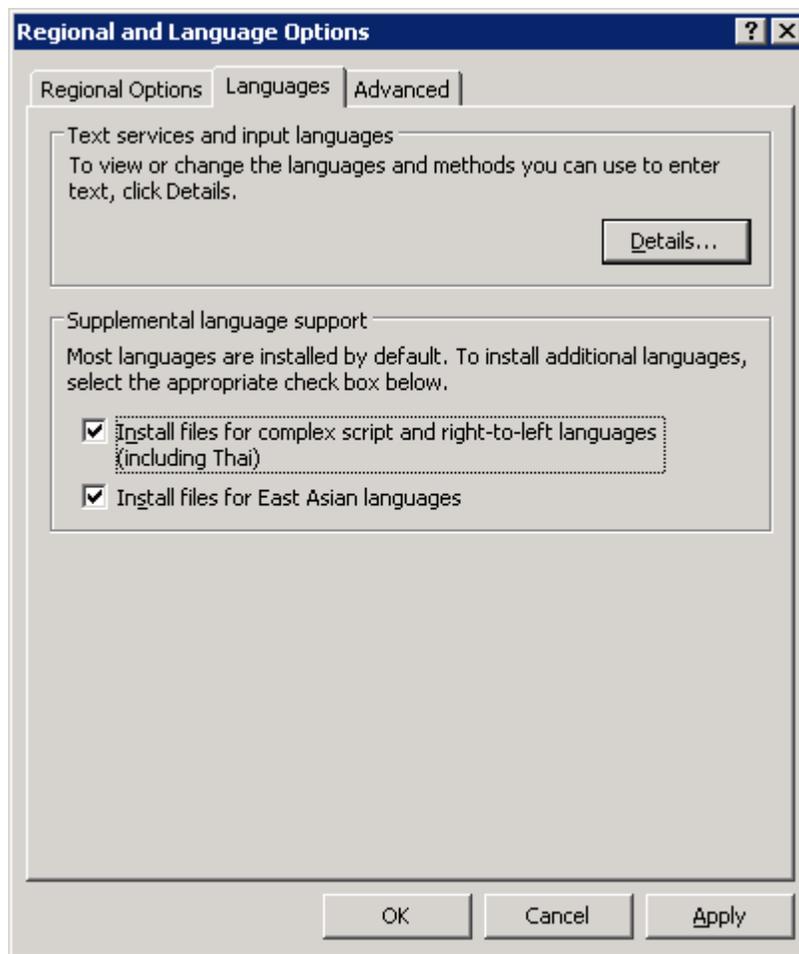
\$2

\$3.50

Note: Asian languages will not render properly on the phone if you do not have the fonts on the server.

Perform the following steps on the server to increase the language fonts you can support:

1. Open Control Panel.
2. Double-click "Regional and Language Options".
3. Click on the 'Languages' tab.
4. In the 'Supplemental language support' section select the two checkboxes as shown. Click OK to clear each warning.



5. Click OK. You may need to provide the Windows installation CD.
6. Reboot the server to activate complete the process.

After you reboot you should be able to render more fonts with Live Content applications. You can verify by first viewing the affected web page using Internet Explorer on the server, and then programming a phone to view the same content.

Backup and Restore

This section discusses what is required to backup and restore Live Content Suite.

Backup

To guarantee a proper backup of your Live Content Suite server, you should backup the following components:

- Database

- License
- Configuration Settings

Backing up the Database

The database is the most important component of a Live Content Suite installation to backup. The license can be replaced and the configuration settings can be determined, but the database must be backed up using a proper backup method.

The Live Content Suite database includes the following information:

- Users
- Groups
- Key Programming Permissions
- Key Programming for Live Content Applications (Twitter account information for example)
- Switch Information (includes switch names, addresses, and login information)

You should backup the database using a regular schedule that meets your needs.

Microsoft has a Knowledge Base article on how to schedule backups for a SQL 2005 Standard database. The article is available [here](#).

The article does not apply to SQL Express which does not natively support scheduled backups. If you are using SQL Express you can rely on the Windows Scheduled Tasks to run SQL backup scripts according to the required schedule. Refer to Knowledge Base article available [here](#) for details required to script a SQL 2005 Express database backup.

Backing up the License

You should backup the license key you used to license Live Content Suite. You can re-use the same license if you are re-installing Live Content Suite on the same physical server – even if you reinstall Windows. If you are installing on a different physical server you will need to get a new license.

When you uninstall Live Content Suite the license file is left behind in the following location:

`\Documents and Settings\All Users\Application Data\InGenius\LCS\Licenses.xml`

If you re-install Live Content Suite it will automatically be licensed using the existing license file.

 **Note:** Do not edit the license file manually or the product will become unlicensed.

Documenting Configuration Settings

When you run the Configuration Wizard you should document the settings you provide. It will make rebuilding or restoring Live Content Suite easier if you document the following configuration settings:

- Application Pool username and password (Web Application Pool page)
- LDAP Query root (User Lookup Settings page)
- Field to search for users by phone extension (User Lookup Settings page)
- LDAP username and password (User Lookup Settings page)
- Phone Extension Pattern (LDAP Field Parsing page)
- Phone key application name (HTML Phone Application Settings)

It's very important to use the same 'Phone key application name' or existing Live Content Application programming will not work.

 **Note:** If are rebuilding the Live Content Suite server but you did not document the application name, you can login to one of the MCD hosts, locate a phone that is programmed with a Live Content key on the "Multiline Set Key Assignment" form, and view the application name for the key.

If you did not document the configuration information you provided when you first configured Live Content Suite, you can re-run the Configuration Wizard and document the settings that are displayed. Instead of completing the Configuration Wizard however, you can abort it by clicking Cancel.

Restoring Live Content Suite

To fully restore Live Content Suite you must restore the following components:

- Database
- License
- Configuration Settings

The method you use to restore Live Content Suite depends on your situation. Consider the following cases:

- Case 1 - Live Content Suite is working but the database needs to be restored to the same location.
- Case 2 – Live Content suit is working but the database needs to be restored to a new location.
- Case 3 - The database is intact and up to date but Live Content Suite needs to be re-installed
- Case 4 - The database needs to be restored and Live Content Suite needs to be re-installed.

 **Note:** You can restore your Live Content Suite configuration to a new server; however, it must be a member of the same domain.

Case 1

If the Live Content Suite server is working but the database is corrupt or has been lost, you should take the following steps to if you are going to restore the database to the same database server:

1. Use IIS Manager to stop the Live Content Suite application pool.
2. Restore the SQL database using a proper restoration method. Microsoft provides instructions in the MSDN article available [here](#).
3. Use IIS Manager to start the Live Content Suite application pool.

You will then have Live Content Suite restored to the most recent backup.

Case 2

If the Live Content Suite server is working but the database is corrupt or has been lost, you should take the following steps if you are going to restore the database to a different database server:

1. Use IIS Manager to stop the Live Content Suite application pool.
2. Restore the SQL database using a proper restoration method. Microsoft provides instructions in the MSDN article available [here](#).
3. Run the Configuration Wizard and change the 'Server\Instance name' on the Database Location page to the new location for the database.
4. Use IIS Manager to start the Live Content Suite application pool.

Case 3

If the Live Content Suite software needs to be re-installed but the database is intact you should take the following steps:

1. Install the Live Content Suite software.
2. Run the Configuration Wizard.
3. Provide the license if necessary. If installing on the same server you can use the same license. If installing on a new server you should obtain a new license.
4. Complete the Configuration Wizard providing the configuration information you documented from the original installation.
5. On the Database Location page point to the 'Server\Instance name' and database name for the existing Live Content Suite database.
6. Be sure to upload the phone application to all of the switches, especially if you are installing Live Content Suite on a different server.

 **Note:** If you restore Live Content Suite to a new server it must meet all of the pre-requisites.

Case 4

If the Live Content Suite software needs to be re-installed and the database needs to be restored then you should take the following steps:

1. Restore the SQL database using a proper restoration method. Microsoft provides instructions in the MSDN article available [here](#).
2. Install the Live Content Suite software.
3. Run the Configuration Wizard.
4. Provide the license if necessary. If installing on the same server you can use the same license. If installing on a new server you should obtain a new license.
5. Complete the Configuration Wizard providing the configuration information you documented from the original installation.
6. On the Database Location page point to the 'Server\Instance name' and database name for the existing Live Content Suite database.
7. Be sure to upload the phone application to all of the switches, especially if you are installing Live Content Suite on a different server, since the phones will need to connect to a different server address.

 **Note:** If you restore Live Content Suite to a new server it must meet all of the pre-requisites.

System Updates

Before updating any of the pre-requisite components, such as installing service packs for Windows or SQL, you should visit <http://www.livecontentsuite.com/> for information pertaining to supported update scenarios. You should also check there for information about fixes and upgrades to Live Content Suite. In-place upgrades will be supported with all fixes and upgrades.

Network Requirements of Live Content Suite

Live Content Suite requires specific network connectivity to the following systems:

- Mitel IP phones
- LDAP server (Active Directory domain controller)
- Global Catalog Server (Active Directory domain controller)
- Mitel MCD host

Phone Connectivity

The Mitel IP phones connect to the Live Content Suite server using the HTTP protocol over TCP port 80 to download live content images for applications such as Twitter, Weather, etc. With this in mind, you can support live content applications on any phone that meets the following network requirement:

- There is a network route between the PC and the phone.
- All intervening firewalls, VPN clients, or routers allow traffic from the TCP port 80 on the Live Content Suite server to pass to the phone at a random port number. If your environment segregates phones from PCs using a VLAN you must enable routing between the two VLANs.

In addition, if during configuration you use the host name for the Live Content Suite server on the “HTML Phone Application Settings” page of the Configuration Wizard, then the phones must be configured with a DNS server that can resolve the host name. The same is true if you use a custom host name.

LDAP Connectivity

The Live Content Suite server connects to the domain controller using the LDAP protocol over TCP port 389. In a Windows Active Directory environment this should already be configured to allow normal domain operation. If you have an Enterprise Certificate Authority in your environment you may be able to use secure LDAP, which uses TCP port 636.

To enable searching the LDAP directory you must ensure the following conditions are met:

- There is a network route between the Live Content Suite server and the domain controller.
- If you are using regular LDAP, all intervening firewalls, VPN clients, or routers allow traffic from the Live Content Suite server to TCP port 389 on the LDAP server to pass.
- If you are using secure LDAP, all intervening firewalls, VPN clients, or routers allow traffic from the Live Content Suite server to TCP port 636 on the LDAP server to pass.

Global Catalog Connectivity

The Live Content Suite server connects to the Global Catalog server over TCP port 3268. In a Windows Active Directory environment this should already be configured to allow normal domain operation. If you have an Enterprise Certificate Authority in your environment you may be able to use a secure Global Catalog connection, which uses TCP port 3269.

To enable searching the Global Catalog server you must ensure the following conditions are met:

- There is a network route between the PC and the LDAP server
- If you are using a regular Global Catalog connection, all intervening firewalls, VPN clients, or routers allow traffic from the Live Content Suite server to TCP port 3268 on the Global Catalog server to pass.
- If you are using a secure Global Catalog connection, all intervening firewalls, VPN clients, or routers allow traffic from the Live Content Suite server to TCP port 3269 on the Global Catalog server to pass.

Mitel MCD Host Connectivity

Live Content Suite connects to a Mitel MCD host in the following ways:

- When you add a switch in the Configuration Wizard
- When you run the 5300 HTML Application Uploader at the end of the Configuration Wizard
- During normal programming operations using the Live Desktop Portal web application.
- When retrieving model-specific HTML applications from the MCD host

The network requirements for each case are summarized below.

Network Requirements for adding an MCD Host with the Configuration Wizard

When adding an MCD host using the Configuration Wizard it connects to the MCD host using the HTTP protocol over TCP port 80. If you choose to use a secure channel it connects using SSL over HTTP (HTTPS) on TCP port 443.

To add an MCD host using the Configuration Wizard, you must ensure the following conditions are met:

- There is a network route between the Live Content Suite server and the MCD host.
- If you are using regular HTTP, all intervening firewalls, VPN clients, or routers allow traffic from the Live Content Suite server to TCP port 80 on the MCD host to pass.
- If you are using SSL over HTTP (HTTPS), all intervening firewalls, VPN clients, or routers allow traffic from the Live Content Suite server to TCP port 443 on the MCD host to pass.

Network Requirements for the 5300 HTML Application Uploader

When running the 5300 HTML Application Uploader after the Configuration Wizard completes, it connects to the MCD host using the FTP protocol to upload the phone applications. It also connects to the RTC command shell over TCP port 2002 to issue the HTMLAPPUPGRADE command.

To upload the phone applications using the 5300 HTML Application Uploader, you must ensure the following conditions are met:

- There is a network route between the Live Content Suite server and the MCD host.
- All intervening firewalls, VPN clients, or routers allow traffic from the Live Content Suite server to TCP port 21 on the MCD host to pass. This is for the FTP control channel.
- All intervening firewalls, VPN clients, or routers allow traffic from the Live Content Suite server to TCP port 20 on the MCD host to pass. This is for the FTP data channel.
- All intervening firewalls, VPN clients, or routers allow traffic from the Live Content Suite server to TCP port 2002 on the MCD host to pass. If this access is not possible then you can issue the HTMLAPPUPGRADE command using ESM.

Network Requirements for Programming Phones

During most situations the Live Content Suite communicates with the MCD host using the HTTP protocol over TCP port 80. If you chose to use a secure channel during configuration it connects using SSL over HTTP (HTTPS) on TCP port 443.

To allow normal phone programming you must ensure the following conditions are met:

- There is a network route between the Live Content Suite server and the MCD host.
- If you are using regular HTTP, all intervening firewalls, VPN clients, or routers allow traffic from the Live Content Suite server to TCP port 80 on the MCD host to pass.
- If you are using SSL over HTTP (HTTPS), all intervening firewalls, VPN clients, or routers allow traffic from the Live Content Suite server to TCP port 443 on the MCD host to pass.

Network Requirements for Retrieving HTML Applications

To retrieve a model-specific list of HTML applications supported on a given phone, Live Content Suite connects to the MCD host using the FTP protocol. This means a user with a Mitel 5360 phone will not see applications for a Mitel 5340 phone, for example.

To support model-specific HTML applications lists, you must ensure the following conditions are met:

- There is a network route between the Live Content Suite server and the MCD host.
- All intervening firewalls, VPN clients, or routers allow traffic from the Live Content Suite server to TCP port 21 on the MCD host to pass. This is for the FTP control channel.

- All intervening firewalls, VPN clients, or routers allow traffic from the Live Content Suite server to TCP port 20 on the MCD host to pass. This is for the FTP data channel.
-  **Note:** If FTP access is not possible, Live Content Suite retrieves the list of phone applications using HTTP or HTTPS; however, the list will not be model-specific and will include all HTML applications available on the MCD host.

Appendix – Open Source Software

The following open source software, or portions thereof, has been used in creating the Live Content Suite software product.

1. Yahoo UI Library, Copyright (c) 2009, Yahoo! Inc. All rights reserved.
<http://developer.yahoo.com/yui/license.html>
2. HTML Agility Pack, Copyright (C) 2003-2005 Simon Mourier. All rights reserved.
<http://htmlagilitypack.codeplex.com/license>
3. log4net:

Copyright (C) The Apache Software Foundation. All rights reserved.
Modifications Copyright (C) 2001-2002 Neoworks Limited. All rights reserved.
For more information on Neoworks, please see <http://www.neoworks.com/>.
The source and binaries for log4net can be downloaded from
<http://logging.apache.org/log4net/>.

License can be found here:

<http://logging.apache.org/log4net/license.html>. Text of license is reproduced here:

Apache License
Version 2.0, January 2004
<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

- 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.*
- 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses*

granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

- (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and*
- (b) You must cause any modified files to carry prominent notices stating that You changed the files; and*
- (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and*
- (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.*

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions.

Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. *Disclaimer of Warranty.* Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. *Limitation of Liability.* In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. *Accepting Warranty or Additional Liability.* While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software

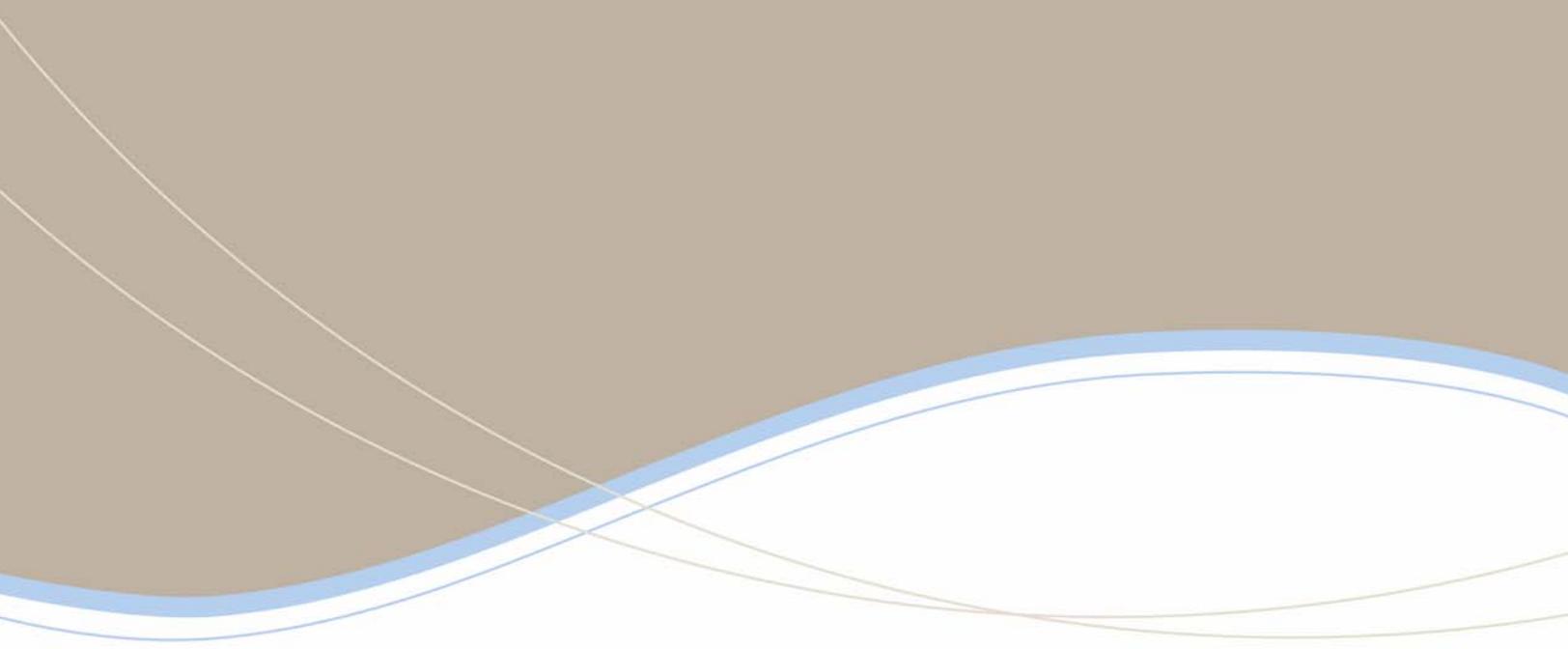
distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Appendix – For Your Information

Live Content Suite and Microsoft Framework 2.0

In order to install the Live Content Suite application, your PC will also need to have the Microsoft .NET Framework 2.0 installed.

- If the Microsoft .NET Framework 2.0 is not installed when you install the Live Content Suite application, the install will direct you to a webpage where you can download and install the Framework at that time.
- The Microsoft .NET Framework 2.0 must also be present if you uninstall the Live Content Suite application.



Global Headquarters	U.S.	EMEA	CALA	Asia Pacific
Tel: +1(613) 592-2122	Tel: +1(480) 961-9000	Tel: +44(0)1291-430000	Tel: +1(613) 592-2122	Tel: +852 2508 9780
Fax: +1(613) 592-4784	Fax: +1(480) 961-1370	Fax: +44(0)1291-430400	Fax: +1(613) 592-7825	Fax: +852 2508 9232

www.mitel.com

For more information on our worldwide office locations, visit our website at www.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 2010, Mitel Networks Corporation. All Rights Reserved.