VoIPIntegration

EM Single Sign On 1.2 (1018)

Installation and Administration Guide

VoIPIntegration
201K Sand Creek Road
Brentwood, California, USA.

Phone : +1-925-513-4400
Fax : +1-925-513-4401
www.VoIPintegration.com

Table of Contents

Product Overview

VoIP Integration EM Single Sign On (EM-SSO) is a Windows based client software solution which automatically logs users into their Cisco phone as they log in to windows.

EM-SSO is designed to increase productivity by saving user time. Let EM-SSO sign in to the phone quickly and seamlessly, allowing users to be productive more rapidly.

Extension Mobility login can be cumbersome at best especially when your Cisco Unified Communications Manager infrastructure is integrated with Microsoft Active Directory. AD integrated users must key in their username on the phone using the phone keypad one letter at a time. (For example john.smith would require 24 key strokes on the phone keypad)

EM-SSO is compatible with all Cisco IP Phones that can be used in conjunction with Extension Mobility.

Requirements

Application Requirements

- Windows PC with Microsoft Dot Net 3.5 or greater.
  Note: Windows on VM Ware is not supported.
- WinPcap (http://www.winpcap.org/) if using automatic device detection.

Call Manager

- Call Manager 5+ (Tested on Call Manager 5 through 10)
- Call Manager User with AXL and EM Proxy Authentication rights.
- AXL Service activated and running on Call Manager Server.
- Extension Mobility service activated and running on Call Manager Server.

Network Connectivity

- The PC running EM Single Sign On must be able to connect to the Call Manager server on TCP port 8443.
- EM Single Sign On will work through NAT and over VPN.

EM Profile Requirements

- Profiles may not have shared lines.

Device Requirements

- If using the Manual Device Assignment option the logged out phone must not contain any shared lines.
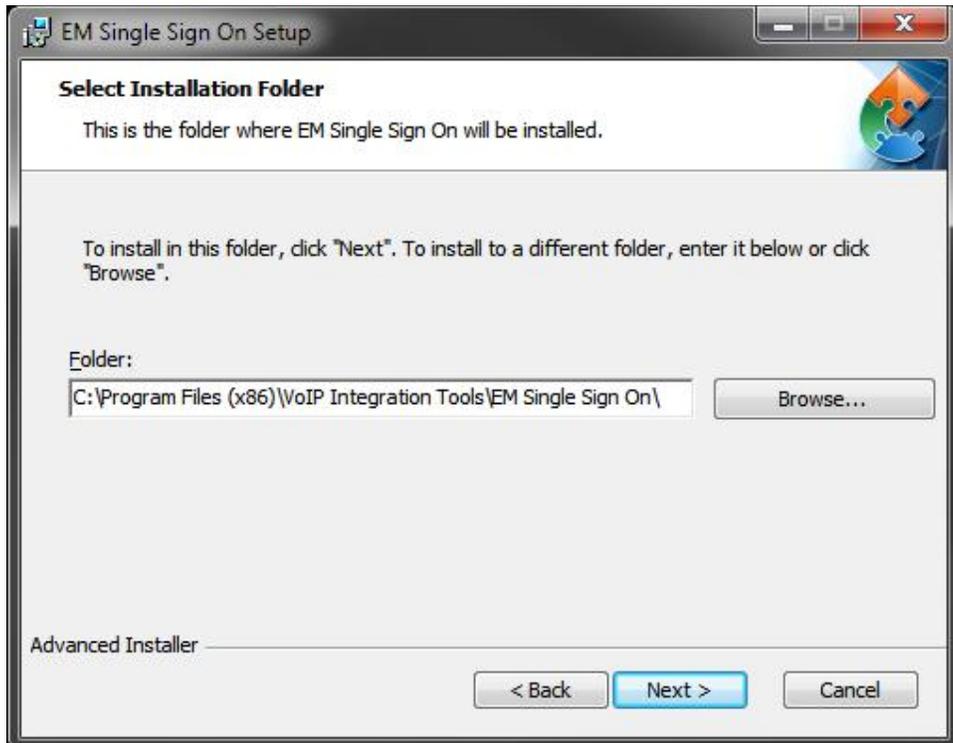
Installation Process

Loading EM Single Sign On

To begin the installation, download the installer from our website at http://www.voipintegration.com, and double-click the saved file.
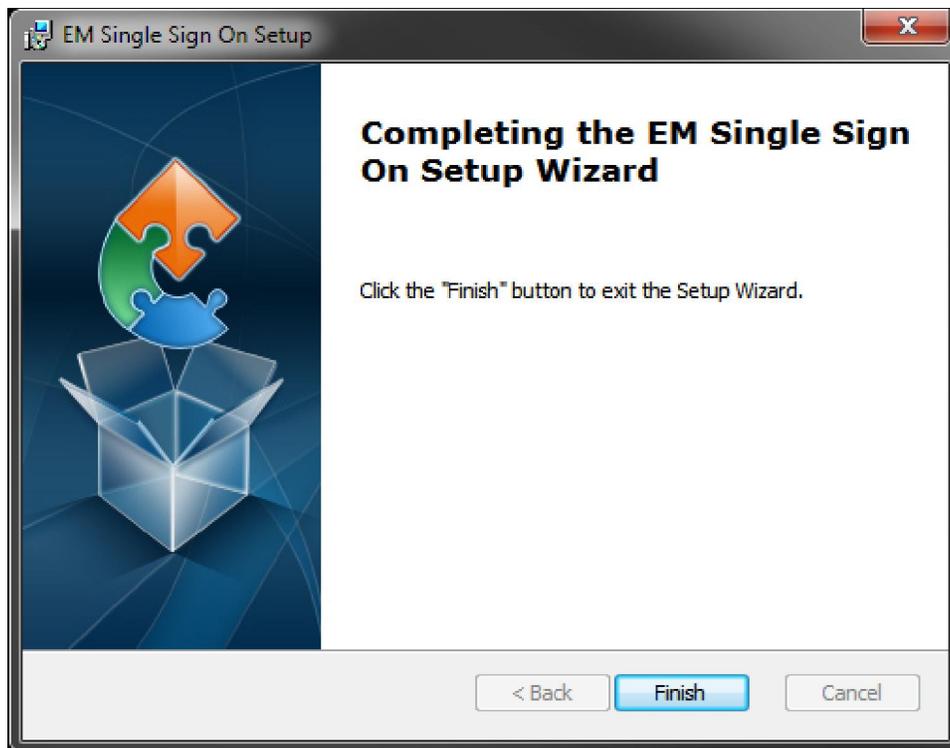
Click *"Next>"*

Enter the installation path you would like EM Single Sign On installed in and click *Next>*.
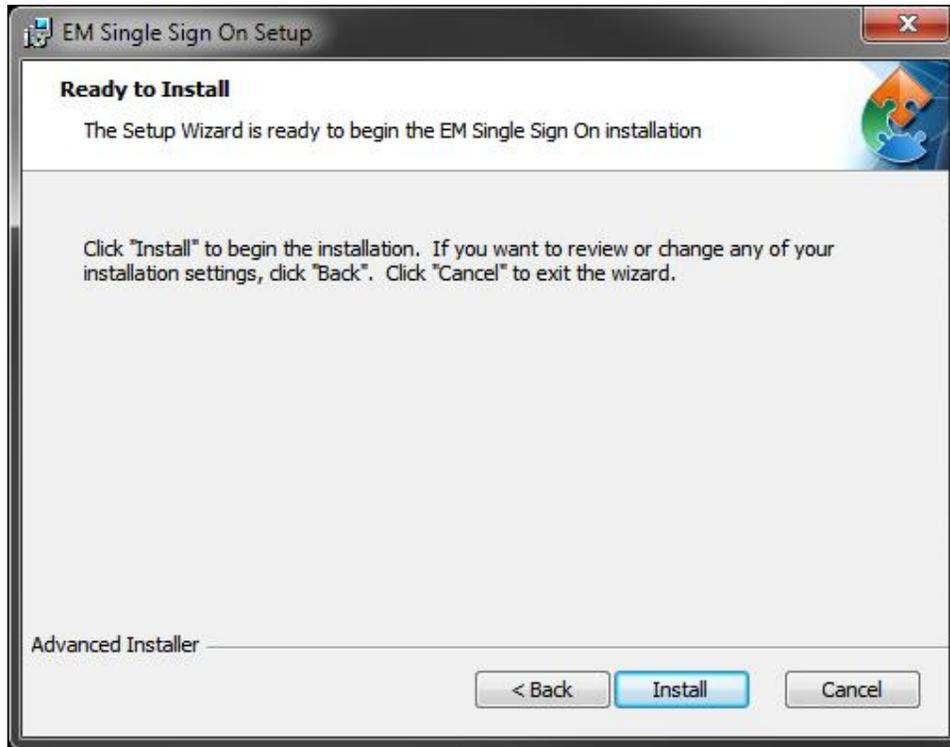
To complete the installation click *Install.*

When the install has completed, click *Finish* to close the installer.

Master Configuration File (MCF)

EM Single Sign On has several settings that can be configured that will change the behavior of the application. In order to change those settings as well as add the license and Call Manager AXL User credentials, a Master Configuration File (MCF) needs to be created.

The Master Configuration File editor can be accessed by starting EM-SSO using the -admin command line argument. "EM-SSO.exe -admin"

With the MCF editor you can create a new MCF or edit an existing MCF. The MCF can then be installed either during the installation of EM Single Sign On using the command line option or the file can be imported when EM-SSO is run for the first time.

Once the MCF file has been created it can be hosted on a web server or placed on a file share so that it can be accessed by the client during installation.

A new or existing MCF can be deployed to the client installs if the behavior or settings of EM-SSO needs to be changed after installing the software. Options can be added or removed or the default values can be changed by editing the MCF and then deploying the file by running EM-SSO using the command line option.

See the *Silent Installs* or *Command Line Options* sections of this document for the specific commands to import the MCF during or after installation.

The Master Configuration File is not required to install EM-SSO. All of the required settings can be manually configured when EM-SSO is run for the first time however if you are installing the application on several PCs the MCF is recommended to simplify the installation process.

EM-SSO		
Config File Location :		Browse
License Key :	1234-ABCD-5678-EFGH	
Call Manager IP Address(es) :	192.168.1.1,192.168.2.1	
AXL Username :	AXLUser	
AXL Password :	•••••••	

Allow User to Change Setting		Default Setting
Automatic Device Discovery :	☑	Enabled
Manual Device Assignment :	☑	Enabled
Auto Device Login Delay :	☑	30
Logout on PC Lock :	☑	Enabled
Logout During Screen Saver :	☑	Enabled
Cancel Auto Login Option :	☑	Enabled
Login Menu Option :	☑	Enabled
Logout Menu Option :	☑	Enabled
Show Device History :	☑	Enabled
Open Display on Startup :		Show Form
Show Tray Icon Only :		Allow Access to Display
Manual ID Assignment :	☑	

☑ Lock Master Config File   Export Master Config

Settings

Config File Location: This is the URL or File location of the MCF to be imported.

License Key: License to use the software

Call Manager IP Address(es) : This is a list of comma separated Call Manager servers running the AXL and Extension Mobility services. It is recommended to have as many call managers as possible in this list for redundancy.

AXL Username: User account with AXL permissions

AXL Password: AXL User account password

Automatic Device Discovery: Enables CDP/LLDP device discovery to determine the device directly connected to the PC.

Manual Device Assignment: Enables manual device assignment in the event that the device that will be logged into is not directly connected. If you are in a Citrix or Terminal Server environment you will need to use this setting.

Auto Device Login Delay: When manual device assignment is enabled, this is the delay between the program starting and the configured account being logged in.

Logout on PC Lock: When the PC is locked the EM profile is logged out. The EM profile will be logged back in when the PC is unlocked

Logout on Screen Saver: When the PC screen saver is activated the EM profile is logged out. The EM profile will be logged back in when the screen saver is de-activated

Cancel Auto Login Option: When the manual device assignment option is enabled and the login delay is enabled this setting will give the user the option to cancel the login.

Login Menu Option: This will add a login option the context menu.

Logout Menu Option: This will add a logout option the context menu.

Show Device History: This setting will display the last few devices and accounts that were logged in by this user.

Open Display on Startup: Opens the display screen when the program starts to show the program state.

Show Tray Icon Only: This option completely disables the display screen and only displays the application status via the system tray icon. Users will only have access to the login and logout context menu options if they are enabled. The Exit Application option in the context menu will always be available to the user.

Manual ID Assignment: This option allows the user to set the User Account that EM-SSO will obtain the EM profile for. By default EM-SSO will use the account name that is currently logged into the PC.

Lock Master Config File: This option is only available when EM-SSO is run with the -admin command line option.   By enabling this option users will not be able to edit the MCF when it is imported during the initial use of EM-SSO.

Application Use

Detection Methods

EM-SSO has 2 methods of determining the device in which to log the EM profile into; Automatic Device Detection which uses CDP or LLDP to determine which phone is directly connected to the PC and Manual Device Assignment which allows the user to specify the device that should be logged into.

Launching EM Single Sign On

When EM-SSO is first launched it will check for a valid configuration file to determine the local settings. If a configuration file is not present then the user will be prompted to either download the MCF or enter the configuration details the cluster and user interface. If EM-SSO finds the configuration file then the application will step through the standard process outlined below.

- Detect Connected Device (If auto detect is enabled)
- Start countdown for connection to manually configured device (If manually configured device and delay is configured)
- Obtain EM profile name from Call Manager for user (Configured User ID or UserID of current PC User)
- Attempt Login

Application Status

EM Single Sign On will display the status of the application in the system tray. There are 4 status icons that will be displayed.

 - Logged In   - Attempting Log in

 - Logged Out   - Error or Failed Login

Application Exit

When EM-SSO is closed any EM Profile that was logged in will be logged out. If the PC that EM-SSO is running on is gracefully shut down the Profiles will also be logged out.

Application Logging

An application log is kept in the Users Data directory found in one of the following locations:

Windows 7 – "C:\Users\(User ID)\AppData\Local\VoIP Integration\EM Single Sign On\Logfile.txt"

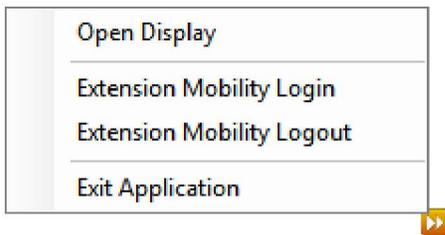**Windows XP or 2000** – "C:\Documents and Settings\All Users\Application Data\EM Single Sign On\Logfile.txt"

Screen Shots

Display Screen with both Detection Methods

Display Screen with Settings tab Open

Context Menu with all options available

Silent Installs

EM-SSO can be installed silently using msiexec. The following syntax can be used to install the master configuration file during the installation.

MCF Hosting Type	Syntax
File Location	msiexec /i "<EM-SSOInstaller.msi file location>" FILE="<The file location of the MCF>" /quiet
URL	msiexec /i "<EM-SSOInstaller.msi file location>" HTTP="<The URL of the MCF>" /quiet

Note: EM-SSO can be silently installed without the MCF portion by omitting the FILE or HTTP arguments.

Command Line Options

EM Single Sign On can be invoked with several command line options to assist in the management of the application settings. Only one command line option can be used at a time

Command Line Option	Required Value
-admin	None
-file	File location of the Master Configuration File
-http	URL location of the Master Configuration File

Note: Options must have a space between selected option and value.

Using the command line options will allow an administrator to create or update the default settings for EM Single Sign On.

Examples:

Command Line	Result
EM-SSO.exe -admin	Grants access to the master configuration file tool.
EM-SSO.exe -file \\share\MaterFile.xml EM-SSO.exe -file C:\MaterFile.xml	Imports the master configuration file from the specified file location.
EM-SSO.exe -http http://webserver/MasterFile.xml	Downloads the master configuration file from the specified URL.

Appendix A: Call Manager Pre Requisite Configuration

AXL Service

For EM Single Sign On to function with Call Manager you will need to ensure you have the AXL service active and running on your server and will need.

To Validate you have the AXL service running:

- Use a web browser to access the Call Manager Serviceability web page.
- https://<Call Manager>/ccmservice
- Select the **Tools > Service Activation** menu
- Under the Database and Admin Section
- Ensure that the Cisco AXL Web Service is activated. If not, click the checkbox and then click the save button at the top of the page.
- Select **Tools > Control Center - Feature Services** menu
- Ensure that the Cisco AXL Web Service is running. If not, click the radio button and then click the start service button at the top of the page.

Service Activation

Database and Admin Services		
	Service Name	**Activation Status**
☑	Cisco AXL Web Service	Activated
☐	Cisco UXL Web Service	Activated
☐	Cisco Bulk Provisioning Service	Activated
☐	Cisco TAPS Service	Deactivated

Control Center – Feature Services

Database and Admin Services				
Service Name	**Status**	**Activation Status**	**Start Time**	**Up Time**
○ Cisco AXL Web Service	Started	Activated	Mon Feb 15 13:38:55 2010	20 days 20:56:57
○ Cisco UXL Web Service	Started	Activated	Mon Feb 15 13:38:55 2010	20 days 20:56:57
○ Cisco Bulk Provisioning Service	Started	Activated	Mon Feb 15 13:37:17 2010	20 days 20:58:35
○ Cisco TAPS Service	Not Running	Deactivated		

AXL User

You may choose to use a Call Manager administrator username and password with EM Single Sign On or assign the required permissions to a new or existing Application User.

Any user who has the group membership of **Standard CCM Super Users** Group will be able to use EM Single Sign On to log user into extension mobility without adding the following process.

If you choose to add a user new group for permissions and want to restrict permissions to the minimum required, you will need to work through the following process. This new group can then be added to a new or existing application user in Call Manager.

From within Call Manager Administration

- Select User Management
- Select User Groups
- Click Add New

- Enter a Group Name such as (EM-SSO Admin)
- Click Save
- Select the Assign Role to User Group from the related links
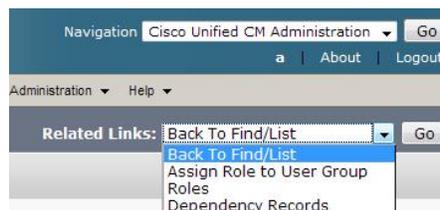
- Click Assign Role to Group button

- Add the following Roles:

  Standard AXL API Access, Standard EM Authentication Proxy Rights.

- Click Save

Now find your application user in Call Manager Administration > User Management > Application Users and add the group created above. This will allow the user to access the AXL service and log users into Extension Mobility but not allow access to any of the Call Manager Admin web pages.

- Click Save.