

Install - Setup Engage Server

Engage Voice Recorder

Release 5.2

Issue 1.0

1 Introduction	9
1.1 Installation Overview	9
1.2 Installation Pre-Planning Meeting	10
1.3 Signed Statement of Work (SOW)	11
1.4 Installation Forms	11
2 Pre-Installation Tasks and Readiness Meeting	12
2.1 Pre-Installation Documents Completed	14
2.2 Dedicated Local or Domain Account Created	14
2.3 Document the SMTP Server Information	14
2.4 Basic Server Preparation and Verification	15
2.5 Recording Server Network Interface Cards (NICs)	17
2.6 PBX License and Configuration Requirements	18
2.7 Recording Method Hardware (deployment dependent)	19
2.8 Testing Telephone and Workstation	20
2.9 Pre-Installation Planning for Web Client Roles - Recommendations	20
3 SQL Server Software Installation	25
3.1 Server 2003, XP and Windows 6 Additional Requirements	25
3.2 Add the Application Server Role to SQL Server	27
3.3 Install SQL 2012 Server Software	31
3.4 Install SQL 2005 Backwards Compatibility Software	35

3.5 Configure the SQL Instance for TCP/IP	37
3.6 Create SQL Login Accounts	39
3.7 Verify SQL Management Studio Connection	41
4 Web Server Software Installation	44
4.1 Add Engage Service Account to Local Administrators Group	44
4 Digital Certificates	45
4.2 Add and Configure Web Server (IIS) and Application Server Roles - Required	51
4.2.1 For Windows Server 2012	52
4.2.2 For Windows Server 2008	59
4.2.3 For Windows 7	63
4.3 Install Engage Services, HTTPS (if used) and the Web Client	64
4.4 Configure Folder Permissions	73
4.5 Rewrite HTTP to Redirect to HTTPS	75
4.6 Verify Web Client HTTP and HTTPS Screen	83
5 Engage Record Server Installation	85
5.1 Engage Server Prerequisite Setup	85
5.1.1 Partition Configuration and Adding the Domain Account	85
5.1.2 Enable the Desktop Experience feature	86
5.2 Add the Application Server Role to SQL Server	87
5.2.1 Windows Server 2003 and XP Additional Requirements	91

5.2.2 Microsoft Visual C++ 2008 and 2010 - Auto-installed	92
5.2.3 Install Sun Java Runtime Environment (JRE)	94
5.2.4 WinPcap: Required for All VoIP Deployments - auto-installed	96
5.3 Installing Engage Server Software	98
5.4 Install Engage SOA Services	107
5.5 Restart the Recording Server	110
6 Post-Installation Configurations	112
6.1 Server Configuration (CommSrv) Setup	112
6.2 Change the FromEmailAddress Registry Value	123
6.3 Apply New Soft License V2C File	126
6.4 Configure the SQL Server	129
6.4.1 Limit SQL Memory	129
6.4.2 Configure SQL for Engage Databases	132
6.5 Create SQL Account for Engage	136
6.5.1 Create SQL Account for Windows Authentication	136
6.6 Create SQL Account for SQL Authentication	139
6.6.1 A More Secure Option	142
6.7 Configure Service Accounts via JAVA Client	143
6.8 Configure Anti-Virus Real-Time Exclusions	148
6.8.1 Logging On for the First Time	149

6 Recorder Setup	151
6.8.1 Configuring Recorders on the Web Client	151
6.9 Verify VoIP Module Configuration Meets Requirements	153
6.9.1 Web Client VoIP Tab	154
6.9.2 Mass Archive	154
6.9.3 Recording Schedule	155
6.9.4 Ports	157
6.9.5 SMTP Server Settings	158
6.9.6 Configuring Live Monitoring	159
6.10 Administration	162
6.10.1 Bulk Data Import (Users Data)	166
6.10.2 Setup Tab and E-Mail	169
6.10.3 Playback Groups Configuration	174
6.10.4 Dialed Numbers	176
6.10.5 User Roles	176
6.10.6 User Configuration	178
7 Installation Completeness Checklist	183
7 Engage Installation Completeness Checklist	184
7.1 Security Scans on Engage Recorders	187
7.2 Verify Anti-Virus Real Time Scanning Exclusions	188

7.3 Verify Customer's Input Data vs. Customer's Worksheet Data	189
7.4 Verify VoIP Module Configuration Meets Requirements	189
7.5 Verify Licenses	191
7.6 Verify Engage Is Connected	191
7.7 Verify Engage is Recording	192
7.8 Verify Email Alerts are Received	192
7.9 Verify Engage Services are Started	192
7.10 Verify SQL Dedication	194
7.11 Validate Screen Capture Recording	194
7.12 Verify Live Monitoring - if deployed	194
7.13 Validate Manual SQL Backups	194
7.14 Validate Encryption Functionality	194
7.15 Voice Recording Configuration Check	194
8.1 Web Client Administration Setup	195
8.2 Playback Log	195
8.3 Active Calls	196
8.4 Recorder Administration	197
8.5 Administration	199
8.6 SQL Backups	203
8.7 Support	203

9 Monitoring	204
10 Troubleshooting	206
10.1 Web Server (IIS)	206
10.2 Setting Verbose Web Logs	206
10.3 Web Server Upgrade Failure - Rolling Back Action	209
10 HTTP Error 500 Web Client Timeout	212
10.4 HTTP Error 503 The service is unavailable	213
10.5 Troubleshoot (405) Method Not Allowed Issue	215
10.6 Web Server upgrade fails if Application Server Role not Enabled	215
10.7 Troubleshoot "Not connected to Database" Errors	216
10.8 Recorder Version is Blank in the Manage Recorders window	220
10 HTTP Error 500 Web Client Timeout	223
10.9 Troubleshoot "Engage Record Server Not Found" errors	224
10.9.1 TmpInfo.log shows InitLicenses() Failed	226
10.9.2 TmpInfo.log shows SQL Connection Error 80043c9d	228
10.9.3 TmpInfo.log shows SQL Connection Error 80040000	229
10.9.4 TmpInfo.log shows Database 'Config' could NOT be created	230
10.10 Engage Server Not Found - Dongle Release Mismatch	230
10.11 Troubleshoot "Download Service Not Found" Error	231
10.12 Troubleshoot License Management	233

10.13 Troubleshoot Playback Calls	234
10.13.1 Audio Playback Fails in IE11, IE10 and IE9	234
10.14 Timeline Graphic Fails in IE11, IE10 and IE9	235
10 Playback Fails for Administrator	236
10.15 Windows Audio Service Crashes Server Config	236
10.16 Event Monitor not Functioning	238
10.17 TALC Card Traces and Commands	239

1 Introduction

This document contains specific information and procedures to follow to successfully install the Engage Voice Recorder software onto one or more servers, including:

- Pre-installation documentation, readiness checks for deployment and setting installation schedules.
- Installation documentation, planning and required tasks.
- Initial system installation, configuration and setup tasks.
- Post-installation configuration, system monitoring and initial customer training.

1.1 Installation Overview

This document contains information and procedures for installing the Engage voice recorder system on one or more servers in a deployment.

Typical installations proceed in the following phases:

Installation Planning

- Pre-installation planning meetings.
- Statement of Work (SOW) created after pre-installation meetings and sent out for review.
- Customer approves SOW and SOW discussion meetings, as needed.
- Installation scheduled.

Pre-Installation readiness meeting *(5 business days before installation start)*

- Review recording and user forms, check server readiness.
- Check PBX and SQL readiness.
- Transfer software onto server.

- Discuss SOW and any changes, as needed.
- Confirm installation dates.

Installation

- Load and install the product and support software.
- Setup basic recording configuration and start monitoring.

Post Installation Configuration & Monitoring

- Configure system and any add-on capabilities.
- Conduct first level Administrator Training and review of setup.
- Begin monitoring events.
- Conduct second level training (Administrator & Supervisor).

1.2 Installation Pre-Planning Meeting

Once the order is received, the installation scheduling team reaches out to the reseller / customer for key installation contacts and the pre-installation planning meeting is scheduled.

During the pre-installation planning meetings, all aspects of the installation are discussed.

Dependencies are discussed and expectations are set.

Key information is collected, and this allows the Statement of Work to be generated.

Forms are also sent out and should be returned with the SOW if possible. If the data is not yet available, it must be returned by the pre-installation readiness. Should the key recording information not be made available by the Pre-installation readiness call, the installation may need to be rescheduled which can add significant delay.

- Server forms containing all defined system and network administrator user accounts, IP addresses, NIC card assignments and SQL instance names completed and returned.
- Project information forms with project personnel names, email addresses, phone numbers, schedules, locations and responsibilities are completed and returned.
- Completed pre-installation forms for recording information such as phones, agent names and IDs, the recording rules for the recording schedule, playback forms for playback access such as user names, user IDs, user roles, and organizational permissions.

User forms provided before start of installation will be data filled into the product by the installer. Should user forms not be supplied, the customer will be responsible for configuring user accounts and agents.

1.3 Signed Statement of Work (SOW)

The Statement of Work (SOW) includes an overview of products purchased, infrastructure required, storage requirements, dependencies, and a provisioning overview.

The SOW is sent out for review, and the customer approves or requests changes to the SOW.

Once the SOW is returned, the installation is scheduled, and a pre-installation readiness meeting is planned five (5) business days before start of installation. Additional meetings can be scheduled as needed.

1.4 Installation Forms

The following documents must be filled out and returned to the project manager prior to the Pre-installation readiness call.

- **Server forms:** These contain all defined system and network administrator user accounts, IP addresses, NIC card assignments and SQL instance names completed and returned.
- **Pre-installation forms:** These are used for recording information such as agent names and IDs, the recording rules for the recording schedule, playback forms for playback access such as user names, user IDs, user roles, and organizational permissions.

2 Pre-Installation Tasks and Readiness Meeting

At the beginning of each installation project, TelStrat will provide the customer/reseller with details and information regarding their pre-installation tasks via meetings, emails and documentation. All tasks must be completed prior to the start of installation or the schedule could be jeopardized.

The following topics will be discussed during the pre-installation planning meeting. Any topics with an (*) are to have a corresponding **Parature** checkbox or field to document.

Pre-Installation Tasks and Checklist
SCOPE OF WORK
<input type="checkbox"/> Has the Distributor / End User tech read the scope of work?
<input type="checkbox"/> Do they have questions on the Scope of Work?
<input type="checkbox"/> * Is the Scope still valid as to the current customer requirements? Any changes since the SOW was written? Will This require the project to be re evaluated?
<input type="checkbox"/> Have they filled out and returned Documents?
SERVER & NETWORK
<input type="checkbox"/> Is the server on the network and joined to the domain?
<input type="checkbox"/> Is the correct operating system installed per SOW?
<input type="checkbox"/> Is the system hardware configured as per the SOW (Partitions, Ram, and CPU)?
<input type="checkbox"/> Identify the TLAN and CLAN IP Addresses?
<input type="checkbox"/> Firewalls and TCP/UDP ports requirements?
<input type="checkbox"/> Have you logged in as the account you will be installing under?
<input type="checkbox"/> Download Latest software of Engage, SOA Services and Web?
<input type="checkbox"/> Download Prerequisites?

Pre-Installation Tasks and Checklist

- Download SQL Express (if Needed)?
- Download extra software features? i.e. Screen Capture, ODRC?

Download any extra Hot fixes?

If Customer is to download:

- Have [HTTP://ESUPPORT.TELSTRAT.COM](http://esupport.telstrat.com) downing instructions provided?

PBX CONFIGURATION

- Verify they have programmed the PBX according to installation type?

CTI Application Login (Application User Account, AES Account, Etc)

Correct licenses? (DMCC Full, LAN CTE. etc.)

Phone provisioning – (AST, BIB, Etc)

Verify they have downloaded their TSP client, i.e. Avaya, Cisco, ShoreTel

TAP Cards, Splitter and Cabling in place? (If applicable)

TALC Cards and wiring in place? (If applicable)

LICENSING

- PROXY Licenses requested? (If applicable)
- Soft Dongle License is required after hours

LOGISTICS

- Verify Connection method for Remote installation(Webex, VPN, Team Viewer, Etc)
- PC and Phone Available for Testing
- Verify the Installation Start Times and any After hour start times (verify their time zone)

Pre-Installation Tasks and Checklist

- Ensure you have the contact's phone number to call at the start times
- Ensure that the tech will be available by phone when needed

2.1 Pre-Installation Documents Completed

Prior to the deployment, all company related and TelStrat installation forms must be completed and returned to TelStrat for review. This is an important step to keep the deployment moving smoothly.

2.2 Dedicated Local or Domain Account Created

Engage requires a local user or domain account be created **with a password that never expires**.

This domain account must be configured as a **local administrator** on each Engage server.

The domain account is created for the following requirements:

- If recordings are to be archived on a remote shared storage location such as a Storage Area Network (SAN), Network Attached Storage (NAS), or remote file server.
- If screen capture is to be used.
- If speech analytics is to be used.
- If encryption is to be used.

If the Engage deployment meets any of the above criteria, a domain account with a password that never expires must be created, and this domain account and password must be available during the Engage software installation. This can be one account.

2.3 Document the SMTP Server Information

The voice recording server is a mission critical business service. It may depend on access to other parts of the customer network or remote SQL servers. Engage attempts to issue alerts for detected system issues via SNMP or Email alerts. Email alert notification is the preferred choice for most deployments and will only function if the correct SMTP server information is entered into Engage.

It is important for the customer to provide the SMTP Server information to the Engage installation technician for configuration in Engage. Otherwise, emailed system alerts will not be available, which will result in extended installation and system down time.

The Engage server must be added as a trusted host on the Email relay server. Deployments with a dedicated web server require that both the Engage Record server and web server be added as a trusted host.

The FROM address found in Critical Event Services emails can be changed to a specific address, if desired.

2.4 Basic Server Preparation and Verification

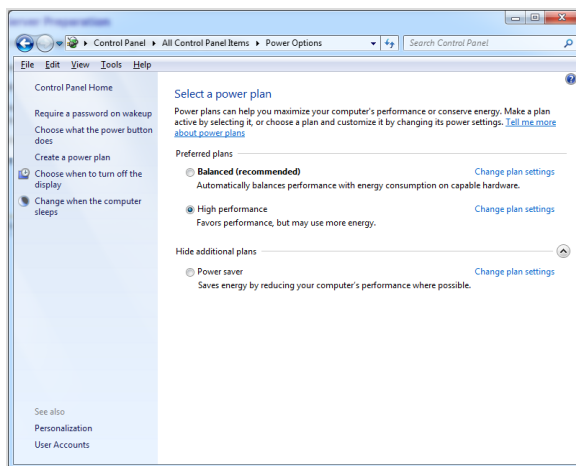
All Engage servers require the following basic server preparations and verifications:

- **Windows Updates Must Be Applied.** Prior to the start of installation, the customer must apply Windows Updates. This can save up to one hour of installation time per server depending on the installed OS type and release date.

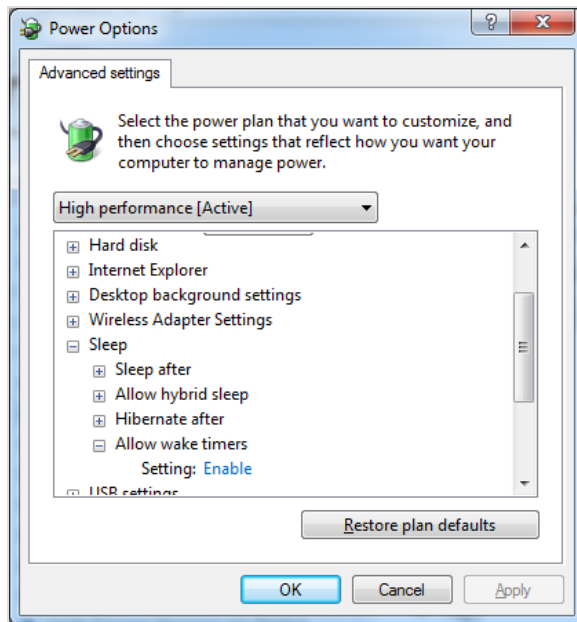
NOTE: TelStrat recommends that customer server software updates be monitored and supervised and not set to be performed automatically. Should customers need to perform unattended software updates, TelStrat recommends testing all server functionality after updating to verify that the updates did not negatively impact the system's ability to record and playback calls, screen captures, encryption key use, etc. Customers can request that TelStrat be available during their server updating procedures and arrangements for technical support can be made by contacting TelStrat Technical Services Support.

- **Add the Engage Domain Account to the Local Administrator's Group.** Prior to the start of installation, the customer must add the Engage Domain Service Account to the local Administrator group on each Engage server.
- **Storage Partitions and Mass Archive Must Be Setup.** All storage partitions defined in the Scope of Work must be defined. Any Mass Archive locations(s) must be defined and the Engage Domain account must be granted full permission to this shared location. Refer to the *pre-installation scope of work* document for the recommended partitions and sizes required. Windows Server 2008 and newer includes Partition tools in the *Disk Management* tool located at *Administrative Tools » Computer Management*.

- **Static IP Addresses Must Be Assigned.** The static IP addresses must be assigned to all Engage Record servers.
- **Anti-Virus Software must be DISABLED During Installation.** Any anti-virus software must be disabled on the Engage servers during installation.
- **Power settings Must Be Confirmed:** Power settings must be set to enable *Wake Timers* and must be set to default to OS High Performance under **Control Panel » Power Options** for all Engage servers and the SQL server. If power settings are not set to High performance, Engage may fail to record calls due to Allow Wake Timers being disabled. These important settings are found here:
 - *Power Options* - Select a Power Plan



- *Power Options - Advanced*



2.5 Recording Server Network Interface Cards (NICs)

Refer to the provided statement of work documents which should define the number of Ethernet NIC(s) required for the recording server. Most deployments require 2 Ethernet NIC(s):

- **C-LAN:** The Customer LAN (C-LAN), is typically used for Server Administration and Engage Client access.
- **T-LAN:** The Telephony LAN (T-LAN) interface handles CTI and any RTP packets.

The following deployments require a 3rd Ethernet NIC:

- **Port Spanning:** Deployments utilizing port spanning require a dedicated NIC for processing spanned RTP traffic. If port spanning is used, the customer or reseller is responsible for deploying a port spanning capable Ethernet switch and configuring it for port spanning.
- **CS 1000 VoIP:** Meridian Link Services requires a dedicated Ethernet NIC per PBX requirements.

Additional Engage products and most VoIP deployments will require additional ports to be opened on the firewall. Refer to the [FIREWALL_PORT_REFERENCE_GUIDE](#) and the specific vendor deployment for Engage Voice Recorder and Engage Feature (Screen Capture, Encryption, Mass Archive, etc) port requirements for additional firewall configurations.

2.6 PBX License and Configuration Requirements

All PBX implementations will be different in size, connectivity to Engage and tasks required to complete the the deployment. The following PBX configurations must be completed prior to the Engage installation commencing:

- *PBX licenses* (if required) need to be purchased, imported and configured according to the customer’s specific voice system requirements.
- *PBX configurations* need to be completed for the proposed recording solution defined in the project’s documentation (ex. Cisco, Avaya, ShoreTel, BroadSoft, etc...).

PBX Licenses: There are a number of software licenses that come with PBXs. Engage will be looking for specific ones. The customer must purchase any PBX licenses required for call recording prior to starting the Engage software installation.

Voice platform licensing requirements, by platform, include:

Voice Platform	CTI Software Download onto Engage	Required Voice Platform Licenses
Avaya ACM	Avaya Telephony Server API (TSAPI)	Avaya TSAPI and DMCC licenses must be purchased from an Avaya reseller.
Avaya IP Office	TAPI2 Service Provider located from the User DVD	Avaya CTI Link Pro license must be purchased from an Avaya reseller.
Avaya CS 1000	None	Avaya Meridian Link Services MLS is required for VoIP phone recording and/or MLS Trunk recording.

Broadsoft Broadworks	None	Call Recording license, which is user-based, in order to make use of SIPREC
Cisco UCM	Cisco TAPI Service Provider (TSP)	None
Mitel	MiTAI CTI protocol	Mitel Recording Licenses
ShoreTel	ShoreTel DVS	ShoreTel TAPI Application Server license

PBX configurations: Refer to the PBX configuration documentation supplied by the TelStrat project manager for any steps that must be completed prior to starting the installation.

Some tasks that may be required are:

- A PBX or voice platform system login and password for Engage (Defined in specific voice system documentation).
- Security access for Engage.
- CTI software downloaded on the Engage Recording Server.
- Configuration of the PBX and designated phones to enable phone device recording.
- Enabling of additional unique PBX features such as Extension Mobility, OnDemand recording, etc...

2.7 Recording Method Hardware (deployment dependent)

Depending on the customer's recording method, additional hardware may be required. Typically analog, digital and port spanning deployments will require additional hardware in order for Engage to capture or tap the RTP voice stream.

- **Spanning Switches:** If using the Port Spanning method in the deployment, a Layer 2 switch with switch port analyzer (SPAN) capabilities is required. Port Spanning is available in most SIP or digital environments.

- **TAP Card:** If using analog lines, analog radios, analog DISA Trunks, microphones, T1, E1 or PRI recording methods, a hardware TAP card will need to be installed.
- **TALC Card:** If recording Avaya CS 1000 digital phones, the customer must replace the Engage server's digital line card with the TelStrat-provided TALC card.

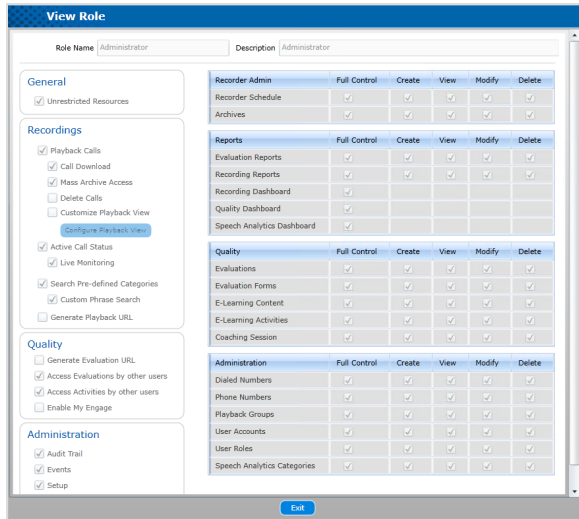
2.8 Testing Telephone and Workstation

For proper testing of a newly installed Engage Voice Recorder system (and its optional features, if installed), some test telephones and a workstation must be set up and made available. The minimum needed are:

- At least one working telephone to make test calls to be recorded.
- At least one computer workstation must be available to use with the Web Client.
- If contact center software is installed, then at least one operational agent ID must be configured. An agent call must be recorded as part of the customer acceptance testing.
- Microsoft Silverlight version 5.1.30514.0 or newer must be deployed on all workstations using the Web Client unless only basic call playback is required.

2.9 Pre-Installation Planning for Web Client Roles - Recommendations

Each user role defined in the web client **Administration » User Roles** tab has selections available that enable or disable features, reports, quality and administration tasks and access for the specific role assigned to the user. The following are TelStrat's recommendations for the roles definitions which are made at the Web Client User Role tab:



The recommendations for each role definition is taken from this core set of selections:

Role Name	Role Permissions Descriptions	Description	Full Control	Create	View	Modify	Delete
General	<input checked="" type="checkbox"/> Unrestricted Resources						
Recordings	<input checked="" type="checkbox"/> Playback Calls						
	<input checked="" type="checkbox"/> Call Download						
	<input checked="" type="checkbox"/> Mass Archive Access						
	<input type="checkbox"/> Delete Calls						
	<input type="checkbox"/> Customize Playback View						
	<input type="checkbox"/> Configure Playback View						
	<input checked="" type="checkbox"/> Active Call Status						
	<input type="checkbox"/> Live Monitoring						
	<input checked="" type="checkbox"/> Search Pre-Defined Categories						
	<input type="checkbox"/> Custom Phrase Search						
	<input type="checkbox"/> Generate Playback URL						
Quality	<input type="checkbox"/> Generate Evaluation URL						
	<input checked="" type="checkbox"/> Access Evaluations by other users						
	<input checked="" type="checkbox"/> Access Activities by other users						
	<input type="checkbox"/> Enable My Engage						
Administration	<input checked="" type="checkbox"/> Audit Trail						
	<input checked="" type="checkbox"/> Events						
	<input checked="" type="checkbox"/> Setup						
	<input type="checkbox"/> Service Accounts						
Recorder Admin			Full Control	Create	View	Modify	Delete
	Recorder Schedule		X	X	X	X	X
	Archives		X	X	X	X	X
Reports			Full Control	Create	View	Modify	Delete
	Evaluation Reports		X	X	X	X	X
	Recording Reports		X	X	X	X	X
	Recording Dashboard		X				
	Quality Dashboard		X				
	Speech Analytics Dashboard		X				
Quality			Full Control	Create	View	Modify	Delete
	Evaluations		X	X	X	X	X
	Evaluation Forms		X	X	X	X	X
	E-Learning Content		X	X	X	X	X
	E-Learning Activities		X	X	X	X	X
	Coaching Session		X	X	X	X	X
Administration			Full Control	Create	View	Modify	Delete
	Dialed Numbers		X	X	X	X	X
	Phone Numbers		X	X	X	X	X
	Playback Groups		X	X	X	X	X
	User Accounts		X	X	X	X	X
	User Roles		X	X	X	X	X
	Speech Analytics Categories		X	X	X	X	X

Administrator Role

The following are **Administrator** Role recommendations.

Administrator Role Recommendations		Release 5.1					
Role Name	Administrator	Description	Administrator Role				
General	<input checked="" type="checkbox"/> Unrestricted Resources	Recorder Admin	Full Control	Create	View	Modify	Delete
Recordings	<input checked="" type="checkbox"/> Playback Calls	Recorder Ports	X	X	X	X	X
	<input checked="" type="checkbox"/> Call Download	Recorder Schedule	X	X	X	X	X
	<input checked="" type="checkbox"/> Mass Archive Access	VoIP	X	X	X	X	X
	<input type="checkbox"/> Delete Calls	Archives	X	X	X	X	X
	<input type="checkbox"/> Customize Playback View	Reports	Full Control	Create	View	Modify	Delete
	<input type="checkbox"/> Configure Playback View	Evaluation Reports	X	X	X	X	X
<input checked="" type="checkbox"/> Active Call Status	<input checked="" type="checkbox"/> Live Monitoring	Recording Reports	X	X	X	X	X
<input checked="" type="checkbox"/> Search Pre-Defined Categories	<input checked="" type="checkbox"/> Custom Phrase Search	Recording Dashboard	X				
<input type="checkbox"/> Generate Playback URL		Quality Dashboard	X				
Quality	<input type="checkbox"/> Generate Evaluation URL	Speech Analytics Dashboard	X				
	<input checked="" type="checkbox"/> Access Evaluations by other users	Quality	Full Control	Create	View	Modify	Delete
	<input checked="" type="checkbox"/> Access Activities by other users	Evaluations	X	X	X	X	X
	<input type="checkbox"/> Enable My Engage	Evaluation Forms	X	X	X	X	X
Administrator	<input checked="" type="checkbox"/> Audit Trail	E-Learning Content	X	X	X	X	X
	<input checked="" type="checkbox"/> Events	E-Learning Activities	X	X	X	X	X
	<input checked="" type="checkbox"/> Setup	Coaching Session	X	X	X	X	X
	<input checked="" type="checkbox"/> Service Accounts	Administration	Full Control	Create	View	Modify	Delete
		Dialed Numbers	X	X	X	X	X
		Phone Numbers	X	X	X	X	X
		Playback Groups	X	X	X	X	X
		User Accounts	X	X	X	X	X
		User Roles	X	X	X	X	X
		Speech Analytics Categories	X	X	X	X	X

Local Administrator Role

The following are **Local Administrator** Role recommendations.

Local Administrator Role Recommendations		Release 5.1					
Role Name	Local Administrator	Description	Local Admin Role Recommendations				
General	<input checked="" type="checkbox"/> Unrestricted Resources	Recorder Admin	Full Control	Create	View	Modify	Delete
Recordings	<input checked="" type="checkbox"/> Playback Calls	Recorder Ports			X	X	X
	<input type="checkbox"/> Call Download	Recorder Schedule			X	X	X
	<input checked="" type="checkbox"/> Mass Archive Access	VoIP			X	X	X
	<input type="checkbox"/> Delete Calls	Archives			X	X	X
	<input type="checkbox"/> Customize Playback View	Reports	Full Control	Create	View	Modify	Delete
	<input type="checkbox"/> Configure Playback View	Evaluation Reports	X	X	X	X	X
<input checked="" type="checkbox"/> Active Call Status	<input checked="" type="checkbox"/> Live Monitoring	Recording Reports	X	X	X	X	X
<input type="checkbox"/> Search Pre-Defined Categories	<input type="checkbox"/> Custom Phrase Search	Recording Dashboard	X				
<input type="checkbox"/> Generate Playback URL		Quality Dashboard	X				
Quality	<input type="checkbox"/> Generate Evaluation URL	Speech Analytics Dashboard	X				
	<input checked="" type="checkbox"/> Access Evaluations by other users	Quality	Full Control	Create	View	Modify	Delete
	<input checked="" type="checkbox"/> Access Activities by other users	Evaluations					
	<input type="checkbox"/> Enable My Engage	Evaluation Forms					
Administrator	<input checked="" type="checkbox"/> Audit Trail	E-Learning Content					
	<input checked="" type="checkbox"/> Events	E-Learning Activities					
	<input checked="" type="checkbox"/> Setup	Coaching Session					
	<input checked="" type="checkbox"/> Service Accounts	Administration	Full Control	Create	View	Modify	Delete
		Dialed Numbers	X	X	X	X	X
		Phone Numbers	X	X	X	X	X
		Playback Groups	X	X	X	X	X
		User Accounts	X	X	X	X	X
		User Roles	X	X	X	X	X
		Speech Analytics Categories	X	X	X	X	X

Supervisor Role

The following are **Supervisor** Role recommendations.

Supervisor Role Recommendations		Release 5.1	
Role Name	Supervisor	Description	Supervisor Role Recommendations
General	<input type="checkbox"/> Unrestricted Resources	Recorder Admin	Full Control Create View Modify Delete
Recordings	<input checked="" type="checkbox"/> Playback Calls	Recorder Ports	
	<input type="checkbox"/> Call Download	Recorder Schedule	
	<input checked="" type="checkbox"/> Mass Archive Access	VoIP	
	<input type="checkbox"/> Delete Calls	Archives	
	<input type="checkbox"/> Customize Playback View	Reports	Full Control Create View Modify Delete
	<input type="checkbox"/> Configure Playback View	Evaluation Reports	X X X X X X
<input checked="" type="checkbox"/> Active Call Status		Recording Reports	X X X X X X
<input checked="" type="checkbox"/> Live Monitoring		Recording Dashboard	X
<input type="checkbox"/> Search Pre-Defined Categories		Quality Dashboard	X
<input type="checkbox"/> Custom Phrase Search		Speech Analytics Dashboard	
<input type="checkbox"/> Generate Playback URL		Quality	Full Control Create View Modify Delete
Quality	<input type="checkbox"/> Generate Evaluation URL	Evaluations	
	<input type="checkbox"/> Access Evaluations by other users	Evaluation Forms	
	<input type="checkbox"/> Access Activities by other users	E-Learning Content	
	<input type="checkbox"/> Enable My Engage	E-Learning Activities	
Administrator		Coaching Session	
<input type="checkbox"/> Audit Trail		Administration	Full Control Create View Modify Delete
<input type="checkbox"/> Events		Dialed Numbers	
<input type="checkbox"/> Setup		Phone Numbers	
<input type="checkbox"/> Service Accounts		Playback Groups	
		User Accounts	
		User Roles	
		Speech Analytics Categories	

Unrestricted Supervisor Role

The following are **Unrestricted Supervisor Role** recommendations.

Unrestricted Supervisor Role Recommendations		Release 5.1	
Role Name	Unrestricted Supervisor	Description	Unrestricted Svr Recommendations
General	<input checked="" type="checkbox"/> Unrestricted Resources	Recorder Admin	Full Control Create View Modify Delete
Recordings	<input checked="" type="checkbox"/> Playback Calls	Recorder Ports	
	<input type="checkbox"/> Call Download	Recorder Schedule	
	<input checked="" type="checkbox"/> Mass Archive Access	VoIP	
	<input type="checkbox"/> Delete Calls	Archives	
	<input type="checkbox"/> Customize Playback View	Reports	Full Control Create View Modify Delete
	<input type="checkbox"/> Configure Playback View	Evaluation Reports	X X X X X X
<input checked="" type="checkbox"/> Active Call Status		Recording Reports	X X X X X X
<input checked="" type="checkbox"/> Live Monitoring		Recording Dashboard	X
<input type="checkbox"/> Generate Playback URL		Quality Dashboard	X
<input type="checkbox"/> Search Pre-Defined Categories		Speech Analytics Dashboard	
<input type="checkbox"/> Custom Phrase Search		Quality	Full Control Create View Modify Delete
<input type="checkbox"/> Generate Playback URL		Evaluations	
Quality	<input type="checkbox"/> Generate Evaluation URL	Evaluation Forms	
	<input checked="" type="checkbox"/> Access Evaluations by other users	E-Learning Content	
	<input type="checkbox"/> Access Activities by other users	E-Learning Activities	
	<input type="checkbox"/> Enable My Engage	Coaching Session	
Administrator		Administration	Full Control Create View Modify Delete
<input type="checkbox"/> Audit Trail		Dialed Numbers	
<input type="checkbox"/> Events		Phone Numbers	
<input type="checkbox"/> Setup		Playback Groups	
<input type="checkbox"/> Service Accounts		User Accounts	
		User Roles	
		Speech Analytics Categories	

Agents Role

The following are **Agents Role** recommendations.

Agent Role Recommendations		Release 5.1	
Role Name	Agent	Description	Agent Role Recommendations
General		Recorder Admin Full Control Create View Modify Delete	
<input type="checkbox"/>	Unrestricted Resources	Recorder Parts	
Recordings		Recorder Schedule	
<input type="checkbox"/>	Playback Calls	VoIP	
<input type="checkbox"/>	Call Download	Archives	
<input type="checkbox"/>	Mass Archive Access	Reports Full Control Create View Modify Delete	
<input type="checkbox"/>	Delete Calls	Evaluation Reports	
<input type="checkbox"/>	Customize Playback View	Recording Reports	
<input type="checkbox"/>	Configure Playback View	Recording Dashboard	
<input type="checkbox"/>	Active Call Status	Quality Dashboard	
<input type="checkbox"/>	Live Monitoring	Speech Analytics Dashboard	
<input type="checkbox"/>	Search Pre-Defined Categories	Quality Full Control Create View Modify Delete	
<input type="checkbox"/>	Custom Phrase Search	Evaluations	
<input type="checkbox"/>	Generate Playback URL	Evaluation Forms	
Quality		E-Learning Content	
<input type="checkbox"/>	Generate Evaluation URL	E-Learning Activities	
<input type="checkbox"/>	Access Evaluations by other users	Coaching Session	
<input type="checkbox"/>	Access Activities by other users	Administration Full Control Create View Modify Delete	
<input checked="" type="checkbox"/>	Enable My Engage	Dialed Numbers	
Administrator		Phone Numbers	
<input type="checkbox"/>	Audit Trail	Playback Groups	
<input type="checkbox"/>	Events	User Accounts	
<input type="checkbox"/>	Setup	User Roles	
<input type="checkbox"/>	Service Accounts	Speech Analytics Categories	

3 SQL Server Software Installation

Engage requires the installation and configuration of one or more SQL instances. SQL Server software may be deployed in one of the following supported configurations:

- A dedicated SQL server added for Engage (large deployments).
- Co-Located SQL server on the Engage Record server (smaller deployments).
- Co-located SQL server on an existing SQL server (smaller deployments).

Customers who want to use existing SQL servers will need to add at least one dedicated SQL instance for Engage Record and configure the SQL login account to be used by Engage.

Engage requires at least one dedicated SQL instance for the call recording database (cache). A second SQL instance is recommended to contain all mass archive databases and the web application database.

Depending on the machine configurations (ex. existing SQL2003 or XP), some *additional software may need to be installed first* before installing SQL2008, SQL2012 or SQL2014.

NOTE: Customers should be reminded to set up and use periodic SQL database backups for data loss protection for all Engage product databases.

3.1 Server 2003, XP and Windows 6 Additional Requirements

NOTE: Windows Server 2012 and Server 2008 R2 do not require this step as long as the Application Server role is already added in the Server Manager.

Installing these software packages can occur in different steps in the installation process depending on machine and software configurations.

Note: Microsoft .NET software is installed in this release of Engage software and does not need to be manually installed.

If the current system is equipped with Windows Server 2003 or XP and is being upgraded to SQL 2008, then these software packages need to be installed at this time:

Install Windows Installer 4.5 and then reboot the server. If unsure, proceed with the installation of SQL 2008 R2 Express and a link will be provided by the setup software. Locate, In the downloaded software folders located on the Engage Voice Recorder:

Navigate to [EngageSoftware » Engage x.x Pre-Reqs & Tools NO SQL » Windows Pre-Reqs » Windows Installer 4.5](#) and click on either:

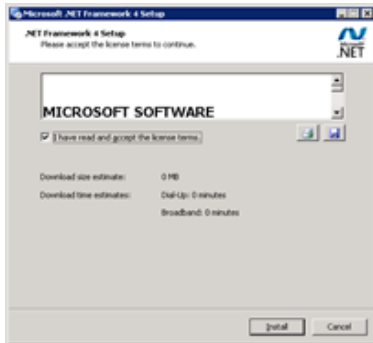
- [WindowsServer2003-KB942288-v4-x64.exe](#) for the 64-bit version.
- [WindowsServer2003-KB942288-v4-x86](#) for the 32-bit version.
- [WindowsXP-KB942288-v3-x86](#) for the Windows XP version.
- [Windows6.0-KB942288-v2-x64](#) for the Windows 6 64-bit version.
- [Windows6.0-KB942288-v2-x86](#) for the Windows 6 32-bit version.

Install Microsoft .Net framework on the server.

The Microsoft .NET Framework enables multiple Engage applications as well as the Web Client user interface to communicate successfully with the Engage recorder. The Web Client requires Microsoft .NET 4.0 or later.

To install the .NET Framework on a Windows 7 Professional, 2003 or XP server, install the complimentary copy of Microsoft .NET Framework from the Engage folder:

1. Navigate to [EngageSoftware » Engage x.x Pre-Reqs & Tools NO SQL » Windows Pre-Reqs .](#)
2. Click on the [dotNetFx40_Full_x86_x64](#) file to install .NET Framework.
3. When the setup wizard has opened, select *I have read and accept the license terms* checkbox.



4. Click *Install* and *Finish* when installation is complete.

3.2 Add the Application Server Role to SQL Server

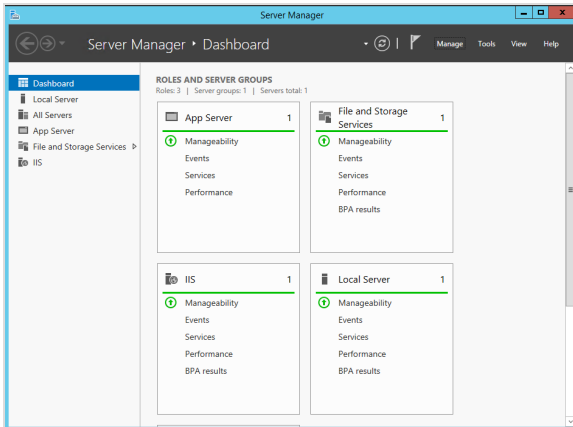
The Application Server role provides central management and hosting of high performance distributed business applications such as those built with Enterprise Services and .NET Framework 4.5 and is required for Engage.

If the server platform is going to support both the Application Server AND the Web Server (IIS), both sets of role settings can be implemented at this time. Use this subsection to administer the Application role and refer to the Web Server (IIS) Support settings in the web server installation section of this document to perform both roles settings and configurations in one session.

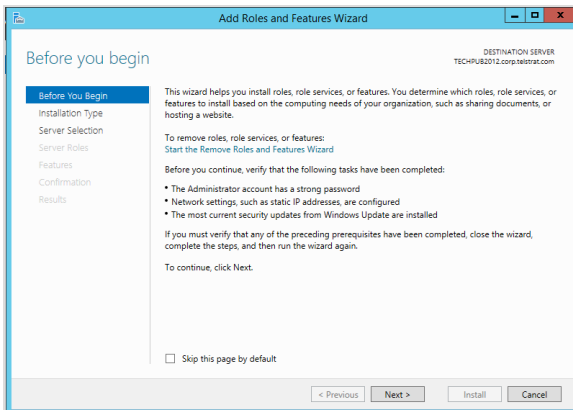
NOTE: This step typically requires a restart upon completion.

Select the Application Server Role:

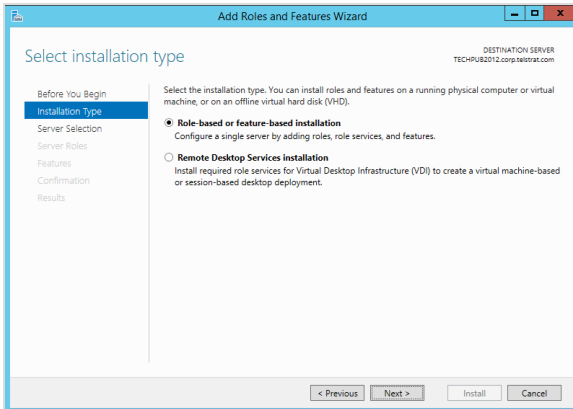
1. From the Desktop or Start menu, launch the *Server Manager* tool.



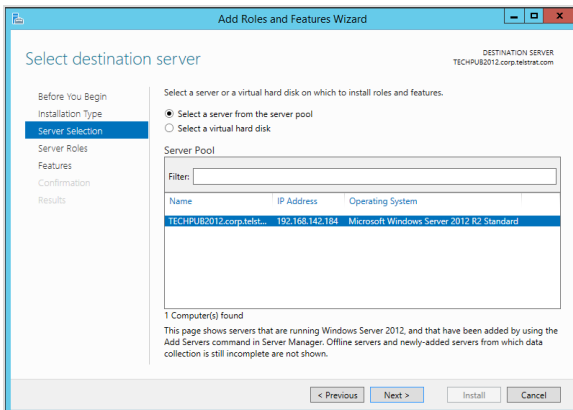
2. On the left-hand top side, click on *Manage* to get the menu and click on *Add Roles and Features* command. The *Before you Begin* window appears. Click *Next*.



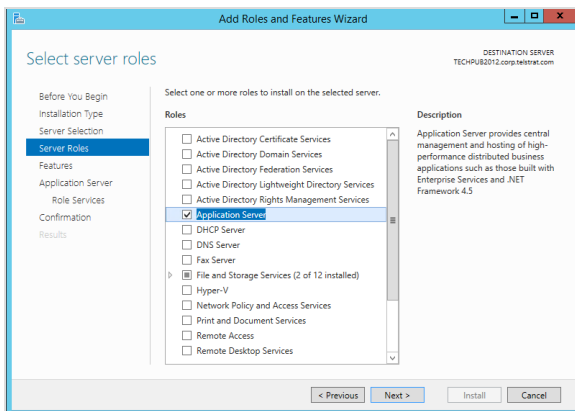
3. On the *Select Installation type* window, make sure the button for *Role-based or feature-based installation* is selected, then click *Next*.



4. On the *Server Selection* window, make sure the correct server name (ex. *techpubs2012*) is selected, then click *Next*.



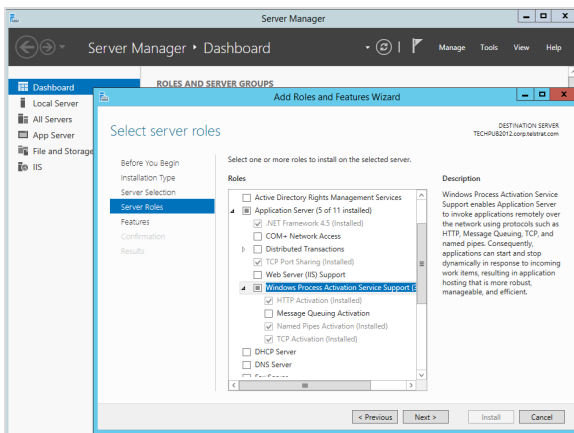
5. On the **Select Server Roles** window, scroll down the Roles list, locate and enable the checkbox for *Application Server*. Click *Next*.



NOTE: Another pop-up window may appear requiring both .NET Framework and Windows Process Activation Service to be installed. Click the **Add Required Features** button to install these additional role services for the Application Server, then click **Next**.

Select server features

1. At the *Select features* window, make sure to click on and select the following features:



- **.NET Framework 3.5.1**
- **TCP Port Sharing**
- **HTTP Activation**

NOTE: The Engage Voice Recorder uses WCF services for internal communications. HTTP Activation is required for WCF.

2. Click **Next** then click **Install** at the *Confirm Installation Selections* pane.
3. Click **Close** when the installation has succeeded and **Close** the *Server Manager*.

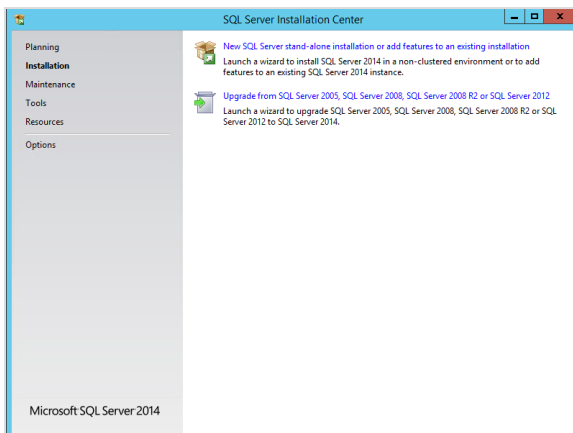
NOTE: If desired, make sure the **File and Storage Services** role is turned on. When File Services is turned on, Windows can manage storage and faster file searching.

3.3 Install SQL 2012 Server Software

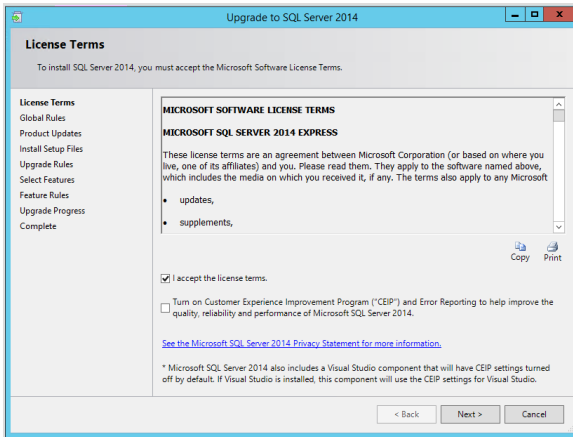
The Engage recorder uses SQL databases to collect and sort all of the various voice and call event data packets for call playback, mass archives, contact center agent information and other data storage.

To install SQL 2012 server using the provided SQL 2012 Express edition, use the downloaded software found on the Engage server in the folder *C://EngageSoftware/MicrosoftSQL*.

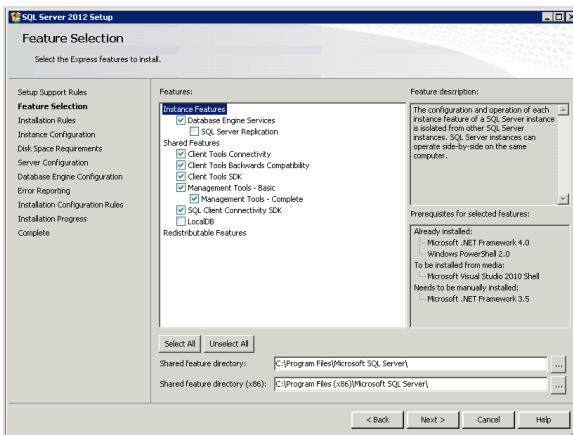
1. Start the SQL Installation application by clicking on the appropriate executable filename for the deployment found in this folder. Examples are:
 - *en_sql_server_2012_express_edition_with_tools_with_sp1_x64.exe* for the 64-bit version.
 - *en_sql_server_2012_express_edition_with_tools_with_sp1_x86.exe* for the 32-bit version.
2. A window will ask to let this program make changes to this server. Click *Yes*.



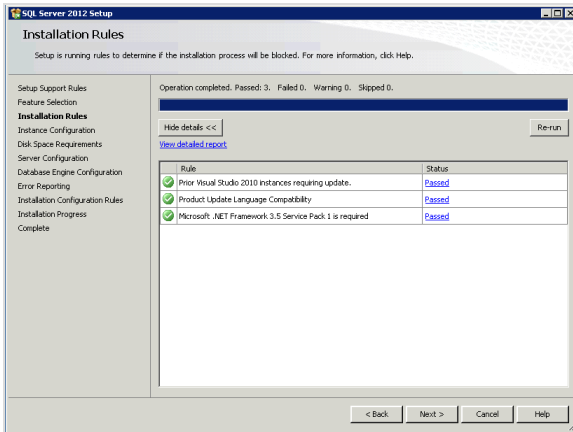
3. From the *SQL Server Installation Center*, click on either:
 - *New SQL Server stand-alone server or add features to an existing installation*: To get a fresh, new SQL 2012 installation (not for a cluster environment).
 - *Upgrade from SQL Server 2005, SQL Server 2008, SQL Server 2008 R2*: To update an existing SQL to SQL 2012.
4. When prompted for License Terms, check the *I accept the license terms* check box and click *Next*.



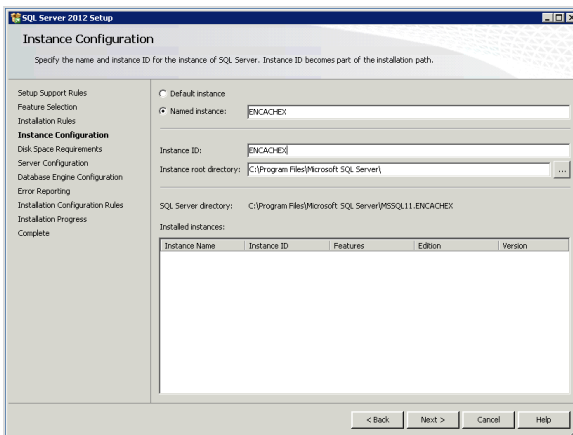
5. When prompted with *Product Updates*, verify that the *Include SQL Server product updates* check box is selected, click *Next*.



6. In the *Feature Selection* window, *LocalDB* can be left unchecked and will not affect performance. The shared feature directory will stay at the default folder of **C:\Program Files\Microsoft SQL Server** . Click *Next*.



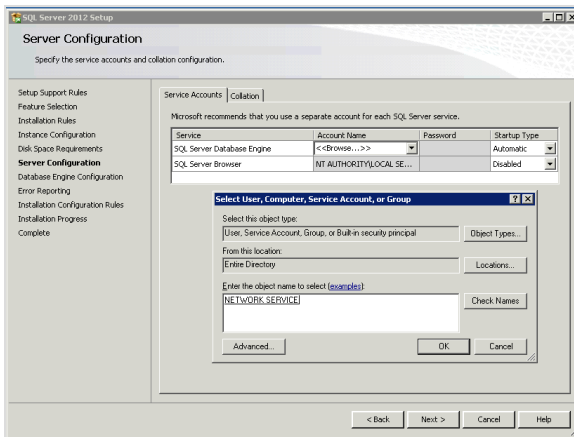
7. At the *Installation Rules* window, click **Next**.



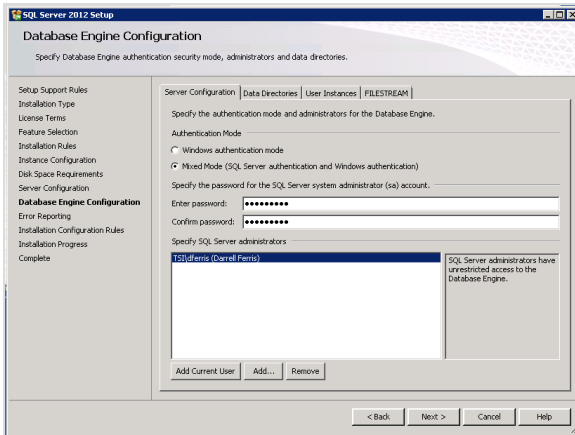
8. At the *Instance Configuration* window, name the database instance and location of the SQL Call Cache Database.

- Rename the *Named Instance* to the desired Instance name (ex. **ENCACHEX** or **ENCACHE**).
- Leave the default **Instance Root Directory** path for the Cache Database unless a different partition is desired for the SQL database instance. If using a separate SQL server, the Instance root directory will be the UNC path. The .WAV files location will be configured in the Engage Installer. Click **Next**.

NOTE: TelStrat installers will use ENCACHEX for SQL Express and ENCACHE for full SQL deployments.



9. At the *Server Configuration* window, *Service Accounts* tab, select **NETWORK SERVICE** as the SQL Database Engine.
 - a. From the *Service Accounts* tab, locate the table line with *SQL Server Database Engine*, click the **Account Name** cell and click **Browse**.
 - b. The *Select User, Computer, Service Account or Group* window will open. Locate the **Enter the object name to select** box.
 - c. Type the word **Network** in the *Enter the object name to select* box and click **Check Names**.
 - d. Click on **Network Service** to select it and click **OK** then click **OK** again to return to the *Server Configuration* window.
 - e. From the *Service Accounts* tab, locate the table line with *SQL Server Browser*, click on the **Startup Type** cell and click on **Automatic**.
 - f. Under the *Collation* tab, select **SQL_Latin1_General_CP1_CI_AS**. Typically this is the default setting.
 - g. Click **Next**.



10. At the *Database Engine Configuration* window, *Server Configuration* tab, click the **Mixed Mode** button.
 - a. Enter and confirm the password for the Engage service account (sa) login. The password must meet the domain security requirements. *Add any additional SQL administrators at this time.*
 - b. Click **Next**.

11. Click on the *Data Directories* tab. If using a different partition for the SQL Database Instance, browse for the directory location. If using a separate SQL server, the Instance root directory will be the UNC path.
 - a. At the *Error Reporting* window, click **Next**.
 - b. The **Send Error Reports** check box is optional for the deployment.

12. The Installation process begins. When complete, select **Close** and then click **Close** for the SQL Installer.

13. Re-run the install process to create all other instances required for the deployment.

NOTE: Second SQL Instances: It is recommended to install a second SQL instance for the web database / mass archive database for sites larger than 200 recording seats. Engage Record will use one SQL instance (config and SRecordingCache), and a second SQL instance is for all other applications (web application database, mass archive, WFM, etc.).

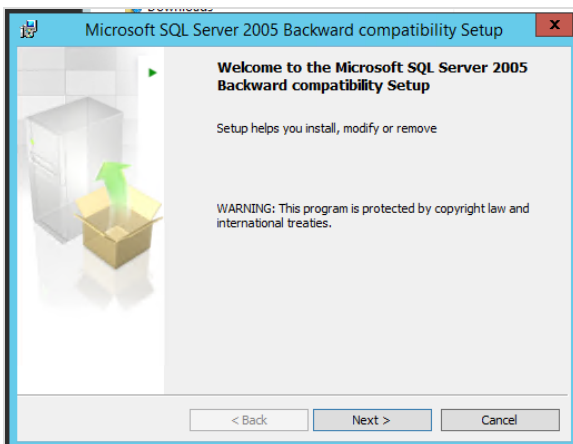
3.4 Install SQL 2005 Backwards Compatibility Software

This package of Microsoft software (SQL2005 Backwards Compatibility) is about making existing features come together with new ones by reducing problems.

1. To install the SQL 2005 Backwards Compatability software, use the downloaded software found on the Engage server in the folder [C://EngageSoftware/MicrosoftSQL](#) folder. Click on the appropriate link for the deployment:

- [SQLServer2005_BCx64.msi](#) for the 64-bit version.
- [SQLServer2005_BCx86.msi](#) for the 32-bit version.

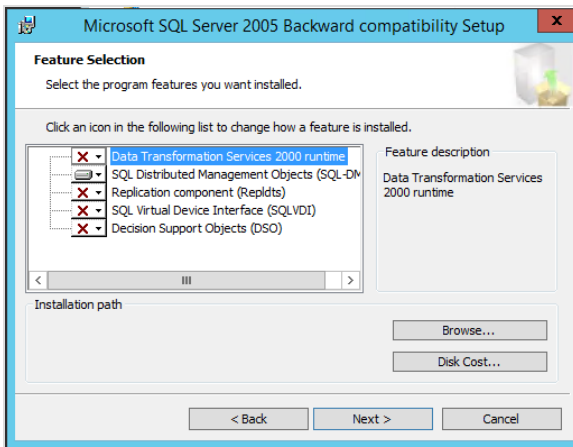
2. When the installer appears, click [Next](#).



3. Check the checkbox to **Accept the terms of the Licensing Agreement**. Click [Next](#)

4. If desired, enter a name and organization. Click [Next](#).

5. On the **Feature Selection** window, *deselect all choices except [SQL Distributed Management Objects \(SQL-DMO\)](#)*. Click [Next](#).



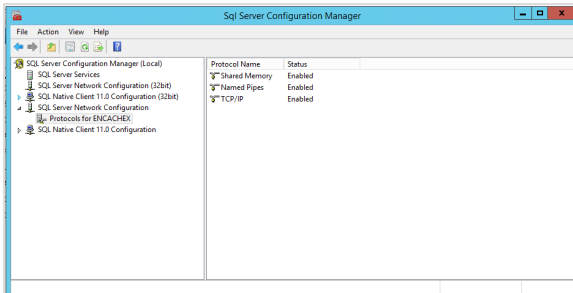
6. Click **Install**. When the install has finished. Click **Finish** and close the installer.

3.5 Configure the SQL Instance for TCP/IP

To configure TCP\IP and Named Pipes on the Engage SQL instance:

For Windows 7, Windows Server 2008 or 2012:

1. Launch to the **SQL Server Configuration Manager**.



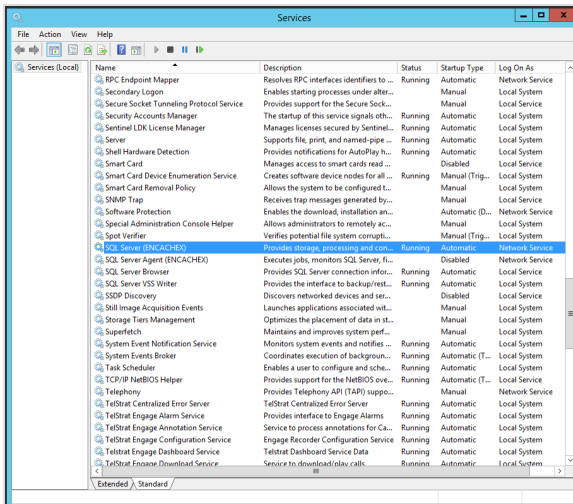
2. From the left pane, click on **SQL Server Network Configuration » Protocols for <INSTANCE>**, typically ENCACHEX or ENCACHE.

3. **Right click** on **TCP/IP** to select properties. Select **Enable**. A warning appears, click **OK**. Restart of the SQL server instance service is required to apply the new setting.

4. **Right click** on **Named Pipes** to select properties. Select **Enable**. A warning appears, click **OK**. Restart of the SQL server instance service is required to apply the new setting.

Restart the SQL Server <instance> Service

1. Navigate to **Start » Administrative Tools » Services**.
2. Expand **Services (Standard) or (Local)**.



3. Scroll down and locate **SQL Server <instance>** (ex. **ENCACHEX** or **ENCACHE**).
4. Restart the service by right clicking on the name to get the pop-up menu and selecting **Restart**.

For Windows XP or Windows Server 2003:

1. Open **Start » Control Panel » Administrative Tools » Services**.
2. Scroll down to **SQL Server <instance>**.
3. Restart the service by right clicking on the name to get the pop-up menu and clicking on **Restart**.

After a new SQL install, if the SQL database cannot connect from a different PC, check these items:

- From the **Services** window, verify **SQL Server Browser** is in **Automatic** mode and is **Started**.
- Verify that TCP/IP is enabled in the SQL Server Configuration Manager. This program is located at **Start » Programs » MS SQL Server » Configuration Tools » SQL Server Configuration Manager**. The TCP/IP parameter must be enabled under **SQL Server Network Configuration » Protocols for <instance name>** such as **ENCACHEX** or **ENCACHE**.

NOTE: The memory of the Engage SQL Instance **must** be limited if any other Engage components are on the same SQL server to ensure Engage has access to available memory. Refer to the [POST-INSTALLATION CONFIGURATIONS](#) section of this document which is done after any Engage databases are installed so all SQL configuration can be done at one time.

3.6 Create SQL Login Accounts

SQL requires a SysAdmin account for each SQL application within the deployment. The account will interact with:

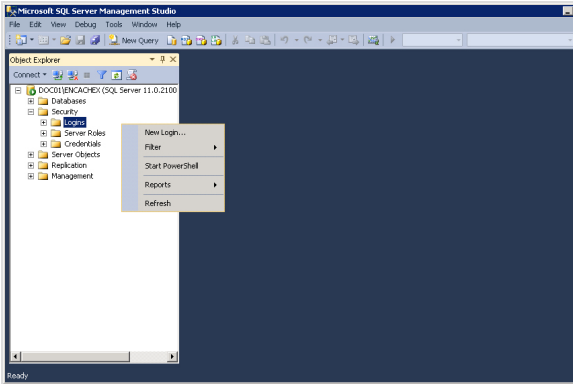
- **Engage Server:** Connects the Cache instance to Engage.
- **Web Client:** Connects the Web application database to Engage.
- **Remote SQL Server:** Connects a Remote SQL Server or cluster to Engage.
- **Mass Archive:** Connects Engage to the storage location.

If the customer is hosting all databases on one server or using a dedicated SQL server for all instances, then a single SysAdmin account for Engage is sufficient.

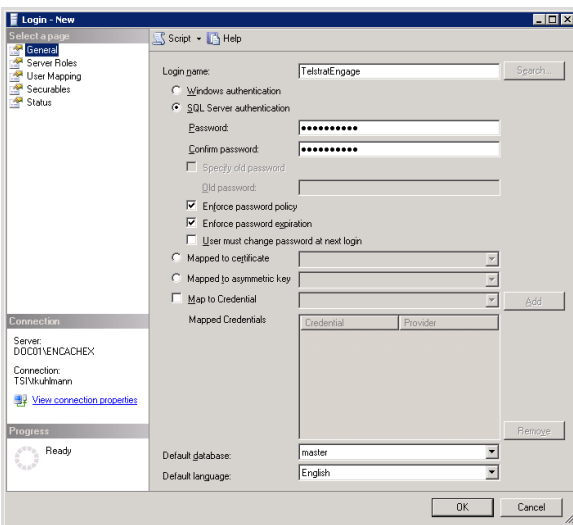
If the customer is hosting several different SQL applications on separate servers, then each application of SQL will need its own access through a SysAdmin SQL Account.

To create a SysAdmin account in SQL:

1. Open [Start » Programs » Microsoft SQL » SQL Server Management Studio](#).
2. Login either using SQL Authentication with the [sa](#) login and password setup previously in the SQL install or login using Windows Authentication with the account presently logged into the server. The login window is CASE SENSITIVE.
3. From the Object Explorer, expand [<Server\Instance Name> » Security](#)



4. Right Click on **Logins** and select **New Login...**
5. Create a new <sysadmin> login for Engage to communicate with the SQL database.
 - Enter a **Login Name**.
 - Select **SQL Server authentication**.
 - Uncheck **User must change password at next login**.
 - In the Select a page bar on the left, select **Server Roles**.
 - Check the box for **sysadmin**.
 - Click **OK**.

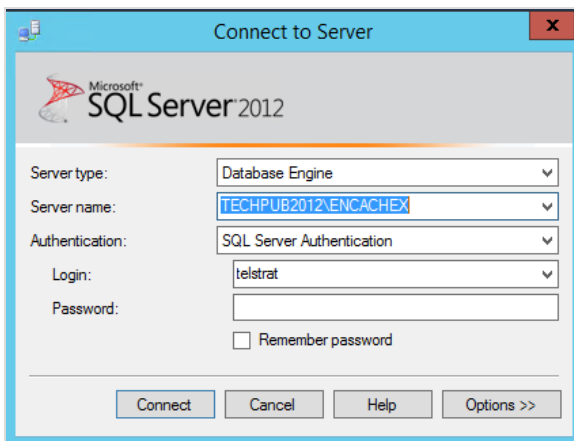


WARNING: If this SQL login or password for the Engage Server is ever changed, Engage will no longer record calls. TelStrat highly recommends that this login and password be provided to our Support group in order to provide faster service and a source for lost passwords.

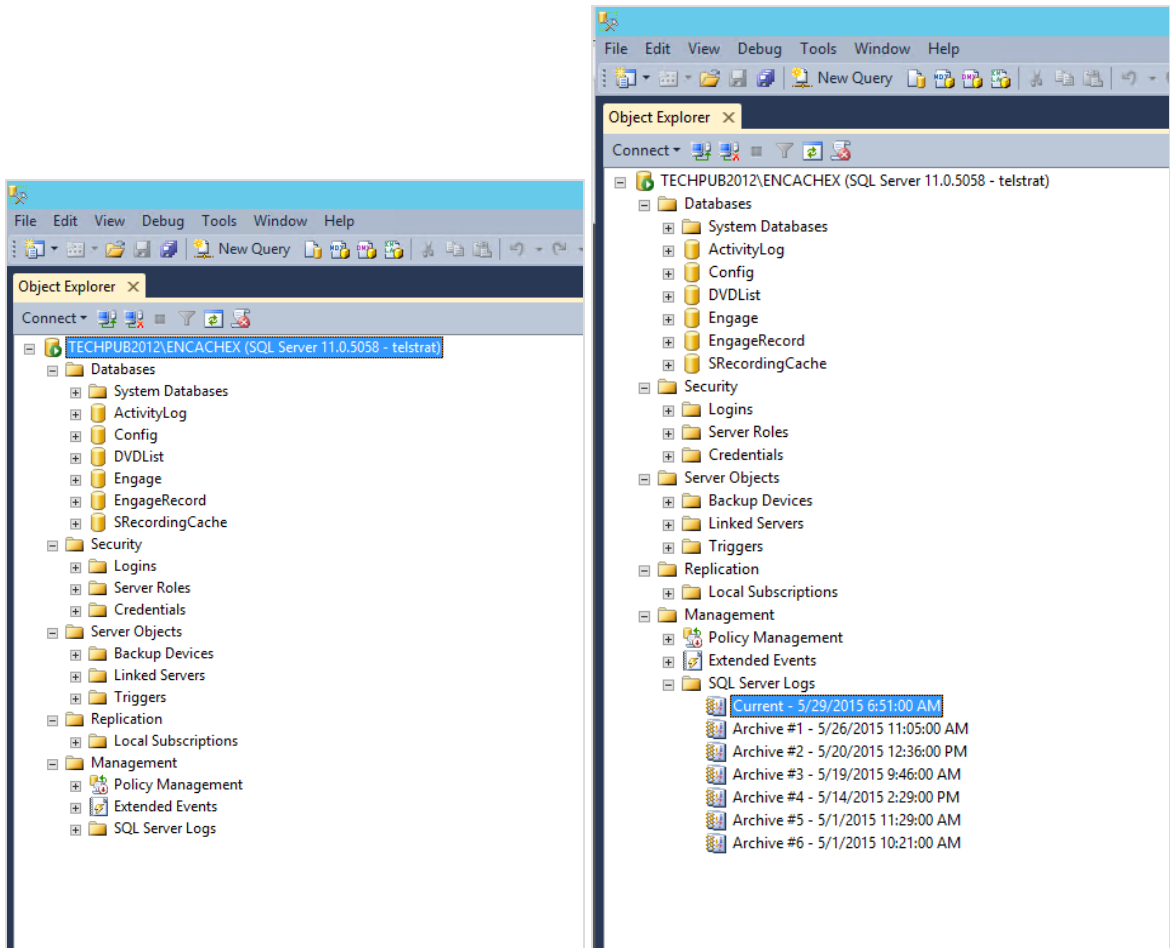
3.7 Verify SQL Management Studio Connection

After installing the SQL database software and instances, verify that the SQL Management Studio can connect with the Engage Recorder. This connection must exist to continue the installation.

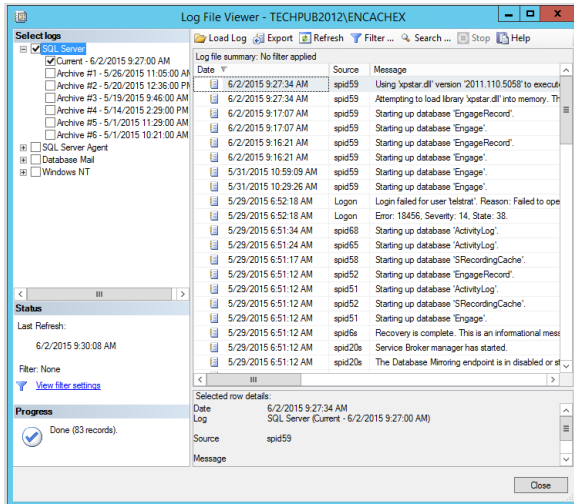
1. Launch the **SQL Server xxxx Management Studio**, select the database *instance* (ex. ENCACHEX or ENCACHE) of the Engage Recorder and log in.



2. Expand (+) the **Databases** tab of the *instance*. Look for various databases to be established in the list of Databases.



3. Expand (+) the **SQL Server Logs** tab and check for connectivity status.



4. Double-click on the *Current* log file to open it and examine the entries. They should show current date and time and status.
5. Exit the **SQL Server xxxx Management Studio** when done.

4 Web Server Software Installation

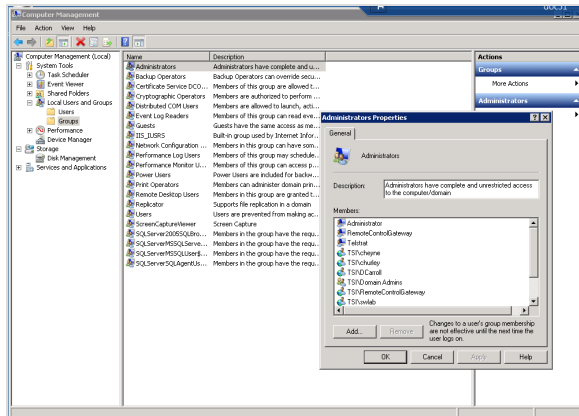
NOTE: SQL 2008 or SQL 2012 must be installed and online before installing the web server software.

Both the Web Server role AND the Application Server role are REQUIRED by the Engage Recorder. If the Web Server and the Application server will reside on the same server, then both roles can be installed at this time.

This section provides the procedures to install the Engage web server software and some Engage services that reside on the web server. These services include:

- TelStrat Engage Search Service.
- TelStrat Engage Dashboard Service.
- TelStrat Engage Quality Dashboard Service.

4.1 Add Engage Service Account to Local Administrators Group



Be sure that the Engage Service Account has been added to the local *Administrators Group* on each Engage server in the deployment.

This is to make sure there will be no operating deficiencies or issues with regards to the Engage services.

4 Digital Certificates

TelStrat customers and their companies are responsible for the procurement, management and deployment of their business related SSL certificates. Each company will have its own web browsing security plan to follow. Engage servers and web clients will operate using either an unsecured HTTP protocol or an HTTPS protocol using a self-signed or entity-signed certificate.

This capability is programmed during the Engage Services and Web Client installation process.

What is a Self-Signed Certificate

A self-signed certificate is created and configured on the host server and contains just a friendly name and provides a digital certificate for use in testing or for narrow business use, such as that connection between an Engage server and an Engage web client. It does not require a third party for signing.

What is a Signed Certificate

A signed certificate is created and configured using the host server and a third party signing source. A signed certificate contains much more information about the owner of the certificate such e-mail addresses, owner's name, registered business name, certificate usage, duration of validity and resource location which includes the Common Name and the certificate ID of the person or entity who certifies or signs this information. A third party will "validate or certify" the certificate and its content acting as a signing Certification Authority (CA). Some companies require this.

What are Signing Certification Authorities

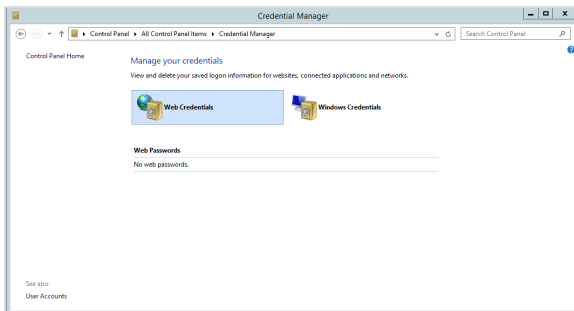
A Certification Authority (CA) is an business/entity that generates and issues signed digital certificates. Companies submit Certificate Signing Requests (CSRs) to these agencies which, after some processing, provide that customer with a signed digital certificate.

There are numerous certifying authorities available including Verisign, Thawt, Godaddy, RapidSSL or StartSSL. Usually the user's browser or application is already loaded with the root certificate of some of these well known Certification Authorities (CA) or root CA Certificates. The CA maintains a list of all signed certificates as well as a list of revoked certificates. CAs are usually preloaded on all web browsers and provide the assurance that the user's certificate is signed by a CA that is known by the browser. Only if this happens do you get the green lock icon in the browser.

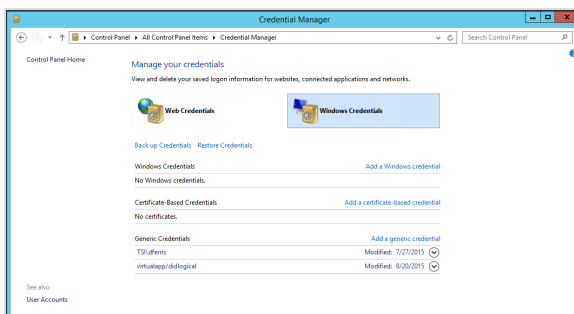
How to View Trusted CAs Already Loaded in the Engage Server

Users can view the list of CAs loaded into the OS with the server's Certificate Manager. To do this:

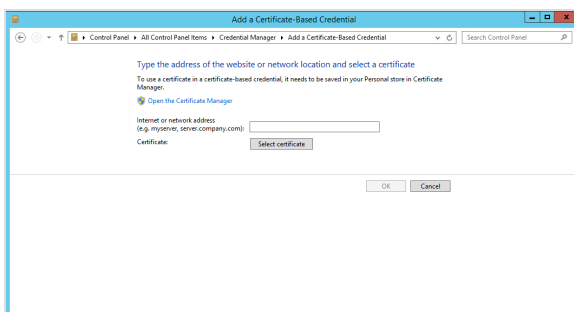
1. Logon to the Engage server and launch the **Start** menu and click on the **Control Panel**.
2. Click on **Control Panel » All Control Panel Items » Credential Manager**.



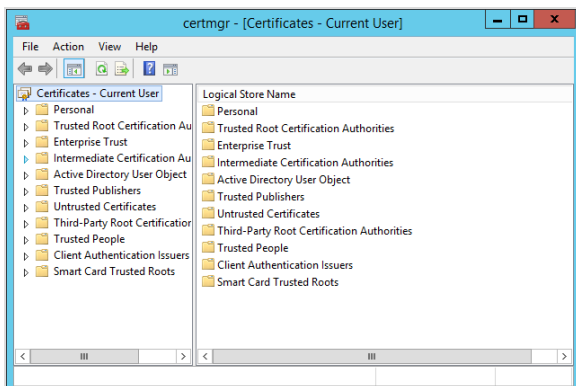
3. Click on **Windows Credentials** to expand the window.



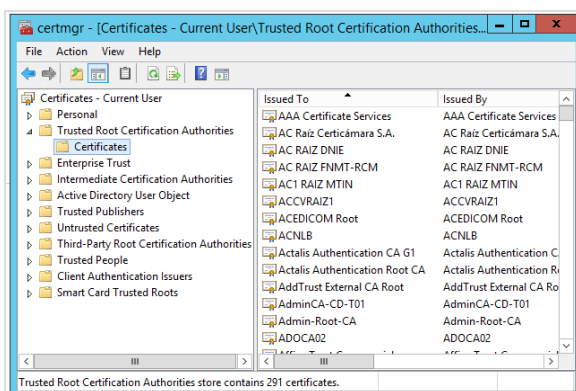
4. Click on **Add a certificate-based credential** to open the Add a Certificate-Based Credential window.



5. Click on **Open the Certificate Manager** to get the certmgr Certified Current User window.



- Click on **Trusted Root Certification Authorities** and expand **Certificates** to see the list of trusted certificates.

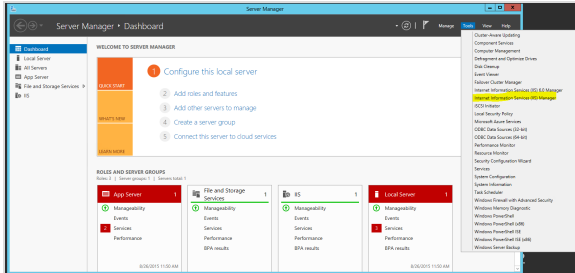


- When completed, this process will allow users to see a trusted certificate for an Engage URL if it were a good certificate signed back to a CA.

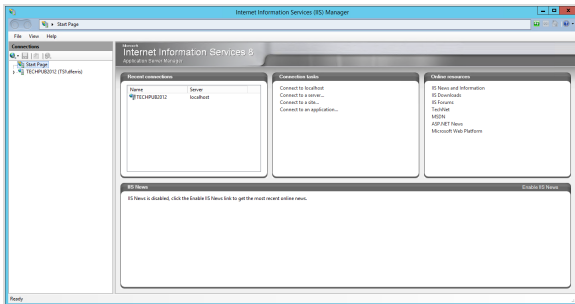
Create a Self-Signed Certificate for the Server

Engage can be configured to use a self-signed certificate to secure the connection between the server and web clients. The certificate can be generated and configured without having to go to a third party source for a digital certificate.

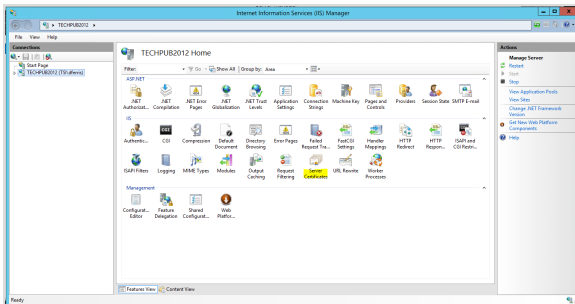
1. Launch the Engage server's **Server Manager**,



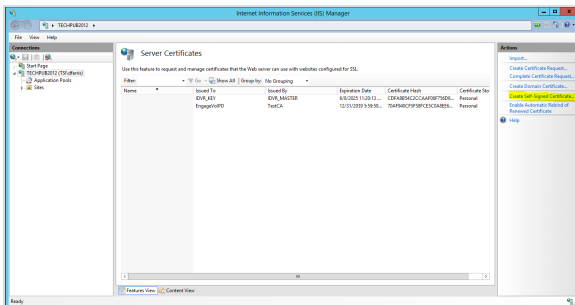
2. Click on the **Tools** menu and click on **Internet Information Services (IIS) Manager** to get the IIS Manager window.



3. Highlight the server's name (ex. **TECHPUB2012**) to get the server's **Home** page. Double-click on the **Server Certificates** icon to get the **Server Certificates** window.

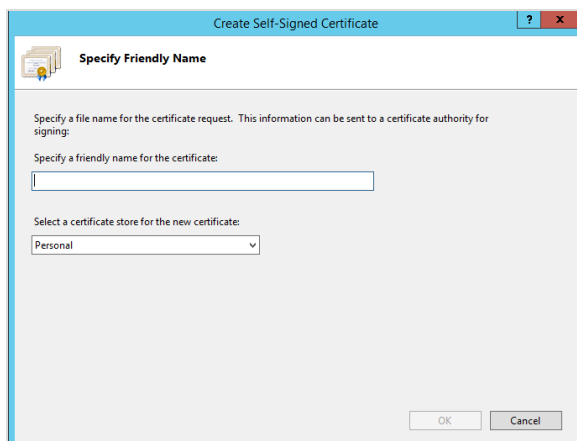


4. On the right-hand pane, click on **Create Self-Signed Certificate** and get the **Create Self-Signed Certificate** window.

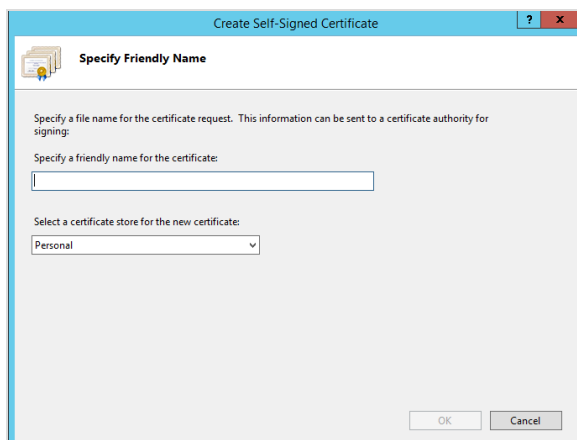


5. Complete the **Create Self-Signed Certificate** entries as follows:

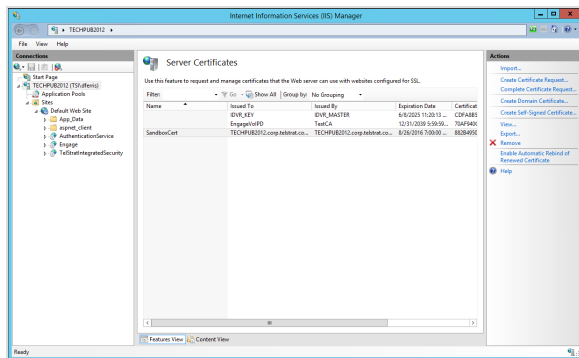
- a. **Specify a friendly name for the certificate:** Enter a name that the certificate will be issued as (ex. *SandboxCert*).



- b. **Select a certificate store for the new certificate:** Select *Personal*. Click *OK*.

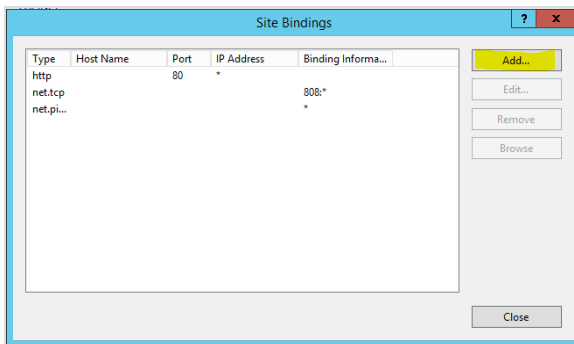


- The screen will close to the **Server Certificates** window. The new certificate with a name (ex. *SandboxCert*) will be displayed.



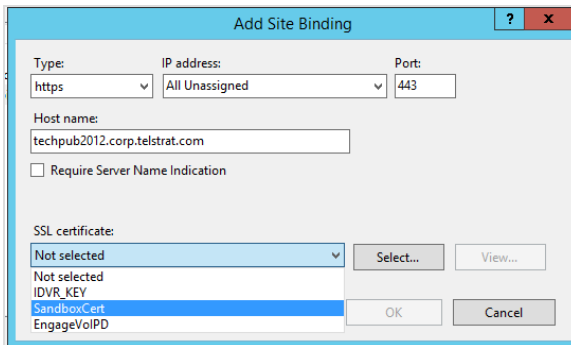
Set the HTTPS Site Binding

- On the left-hand pane, highlight *Default Web Site* to get the **Default Web Site Home** window. On the right-hand pane of the Home window, click on *Bindings...*. In the **Site Binding** window, click *Add*.



- Enter the following binding elements:
 - Type:** Use the drop-down menu to select *https*.
 - IP Address:** Leave at default of *All Unassigned*.
 - Port:** Leave at HTTPS default port of *443*.
 - Hostname:** Enter your host name (ex. *techpub2012.corp.telstrat.com*).
 - Require Server Name Indication** checkbox: Leave unchecked.

- **SSL Certificate:** Use the dropdown menu to select the self-signed certificate name (ex. *SandboxCert*).
- If needed, click **View** to see details of the certificate. Otherwise, click **OK**.
- Note the new binding has been added. Click **Close**.



Be sure to test the browser's access to the Engage Web Client AFTER the web client software is installed.

4.2 Add and Configure Web Server (IIS) and Application Server Roles - Required

Web Server (IIS)

The *Web Server (IIS) role is required* and must be added and configured on the web server. Select the appropriate operating system that the Web Server will be installed on and follow the steps.

With Web Server IIS, Microsoft includes a set of programs for building and administering Web sites, a search engine, and support for writing Web-based applications that access databases, such as the Engage Web Client.

Application Server

The *Application Server role is required* for Engage to operate and function properly.

The Application Server provides the central management and hosting of high performance distributed business applications such as .NET Framework 4.5, TCP Port sharing and the Windows Process Activation Service Support which provides HTTP activation, TCP activation and Named Pip Activation.

If the Web Server (IIS) and the Application Server are going to reside on the same server platform, then both of these roles can be added and installed during one installation session.

4.2.1 For Windows Server 2012

There are two ways to setup the Application Server and the Web Server (IIS):

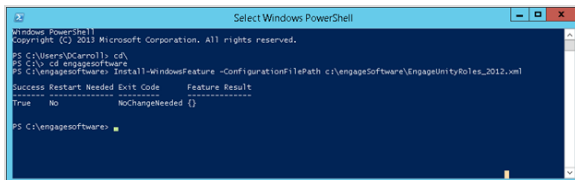
- Using a TelStrat, Inc. provided XML file that will import the changes to the settings.
- Manually configuring the changes to the settings.

Import Windows Server 2012 Application Server and Web Server (IIS) Roles and Features Changes

This XML file can be used to make the needed Roles and Features changes on Application Server and the Web Server (IIS). The procedure is:

1. Go [HTTP://SUPPORT.TELSTRAT.COM](http://SUPPORT.TELSTRAT.COM) , and login in to download the XML file software, if not already done.
2. Copy the *EngageUnityRoles_2012.xml* file from the **Engage 02-CUSTOMER PRE-REQS/Engage x.x Pre-Req & Tools/Windows Roles XML/** folder to the server's **C:\EngageSoftware** folder.
3. Open *Windows PowerShell* as an administrator and run the following command:
 - *Install-WindowsFeature -ConfigurationFilePath c:\engageSoftware\EngageUnityRoles_2012.xml*
 - *Windows PowerShell* should show “Start Installation.....” with progress to 100%
4. Close the *PowerShell* program and skip the remaining manual steps.

Note that this XML file can also be used to repair the server role and features, if the necessary. For roles that are already selected, the power shell will indicate no changes needed, as shown here:



```
Windows PowerShell
Copyright (c) 2012 Microsoft Corporation. All rights reserved.

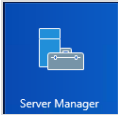
PS C:\Users\A\Carroll> cd\
PS C:\> cd engageSoftware
PS C:\engageSoftware> Install-WindowsFeature -ConfigurationFilePath c:\engageSoftware\EngageUnityRoles_2012.xml
Success Restart Needed Exit Code  Feature Result
-----
True          No          NoChangeNeeded {}

PS C:\engageSoftware>
```

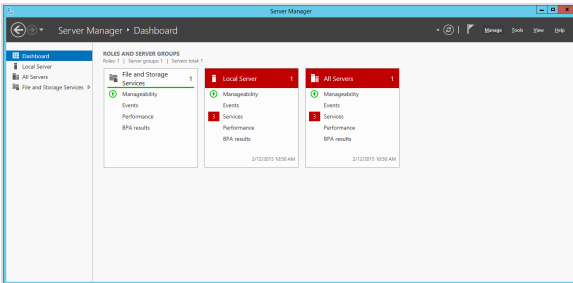
Manually Add Windows Server 2012 Application Server and Web Server (IIS) Roles and Features Changes

If needed, the Application Server and Web Server (IIS) Roles and Features can be manually configured. The procedure is:

1. Launch the Server Manager tool from the desktop icon or from the Start menu.

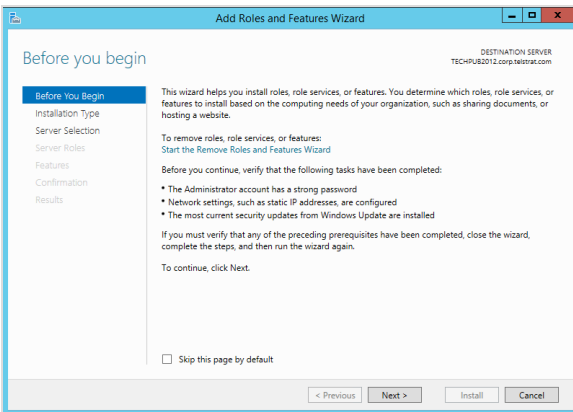


2. On the *Server Manager* window, click **Manage** to get the menu and then click **Add Roles and Features**.



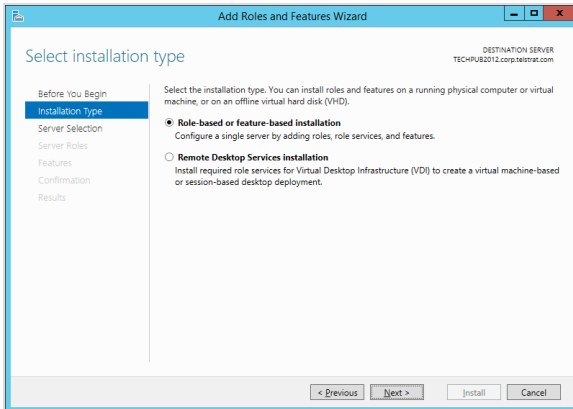
3. Before you Begin

Click **Next** to go past the *Before you Begin* window.



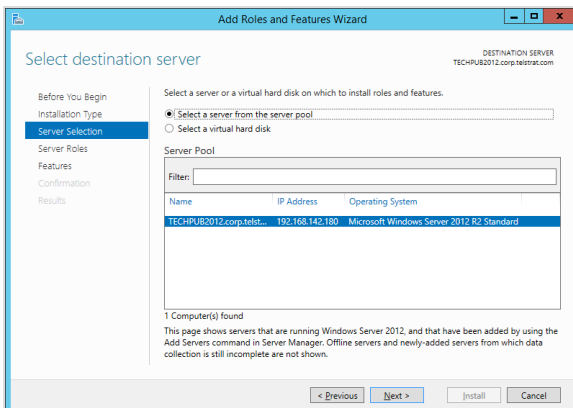
4. Installation Type

At the *Select installation type* window, click **Role based or feature based installation**.



5. Server Selection

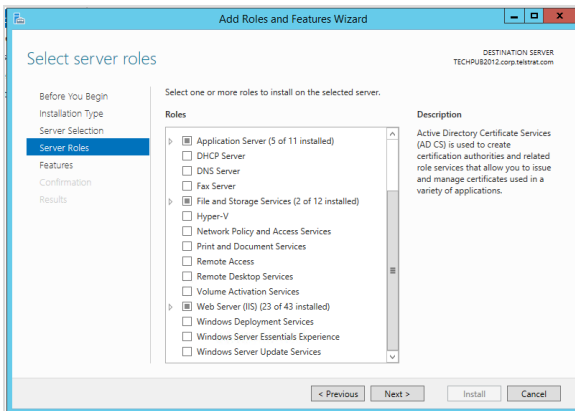
On the *Select destination server* window, click *Select a server from the server pool*, click on the Engage server and click *Next*.



6. Server Roles

On the *Select server roles* window:

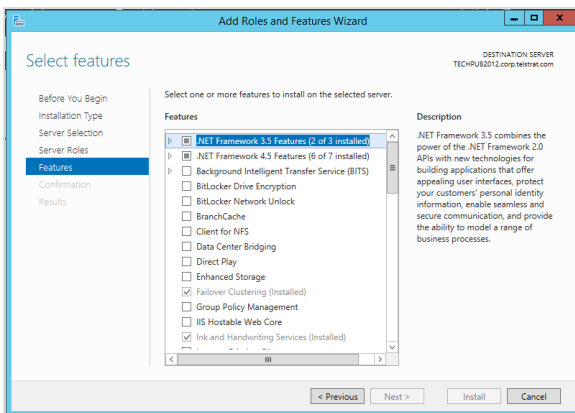
- a. Select the *Application Server* check box.
- b. Scroll down and select the *Web Server (IIS)* check box.
- c. Click *Next* to continue the install.

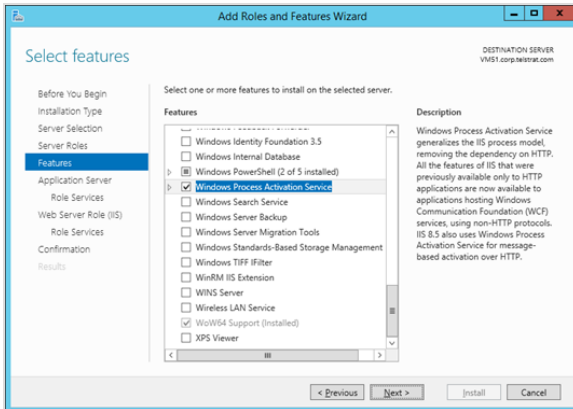


7. Features

On the *Select Features* window, select:

- a. *.NET Framework 3.5*
- b. *.NET Framework 4.5*
- c. Scroll down and select *Windows Process Activation Service*
- d. Click **Next**.

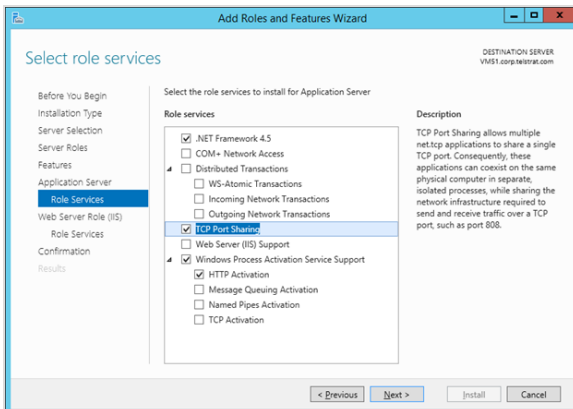




8. Application Server

On the *Select Role services for the Application Server* window, select:

- a. *.NET Framework 4.5*
- b. *TCP Port Sharing*
- c. *HTTP Activation*
- d. Click **Next**.



9. Web Server Role (IIS)

In the *Select role services* window:

- a. Under *Common HTTP Features*, select:
 1. *Default Document*
 2. *Directory Browsing*
 3. *HTTP Errors*
 4. *Static Content*
 5. *HTTP Redirection*

- b. Under *Health and Diagnostics*, select:
 1. *HTTP Logging*
 2. *Request Monitor*
 3. *Tracing*

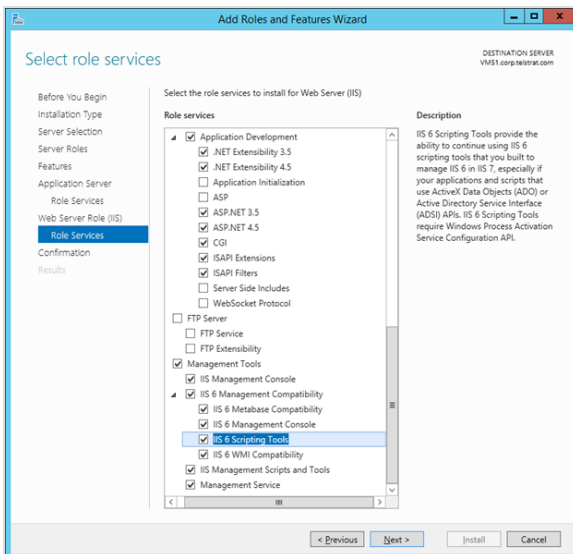
- c. Under *Security*, select:
 1. *Request Filtering*
 2. *Windows Authentication*

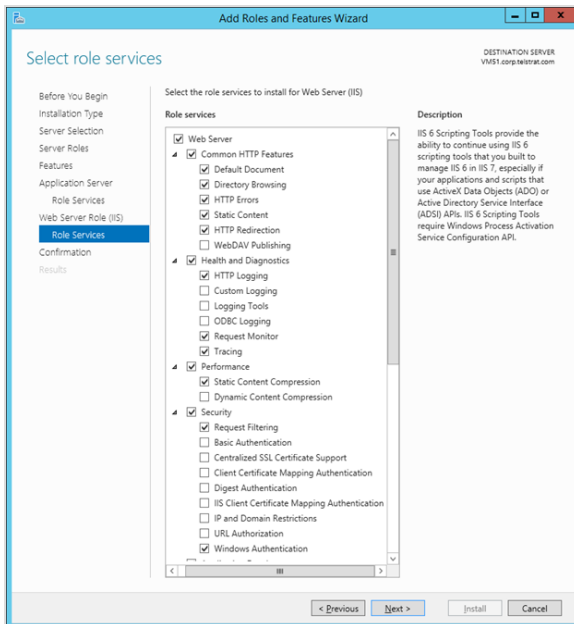
- d. Expand *Application Development* and select:
 1. *.NET Extensibility 3.5*
 2. *.NET Extensibility 4.5*
 3. *ASP.NET 3.5*
 4. *ASP.NET 4.5*
 5. *CGI*
 6. *ISAPI Extensions*
 7. *ISAPI Filters*

- e. Under *Management Tools*, select:
 1. *IIS Management Console*
 2. *IIS Management Capability*
 3. *IIS Management Scripts and Tools*
 4. *Management Service*

- f. Expand *IIS 6 Management Capability* and select:
 1. *IIS 6 Metabase Compatibility*
 2. *IIS 6 Management Console*
 3. *IIS 6 Scripting Tools*
 4. *IIS 6 WMI Compatibility*

10. Verify the following selections are made and then click **Next** to continue to the *Confirmation* window:





11. Confirmation

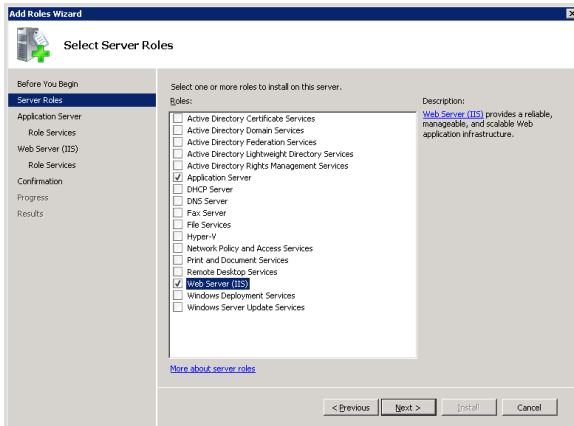
- At the *Confirmation* window, select **Install** to install the updated settings

12. Click **Close** when the installation has succeeded and close the *Server Manager*.

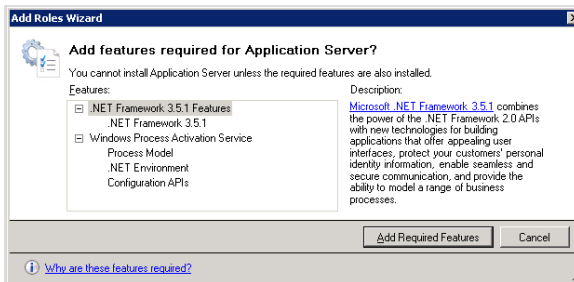
4.2.2 For Windows Server 2008

The procedure to add and configure the Web Server 2008 (IIS) role is:

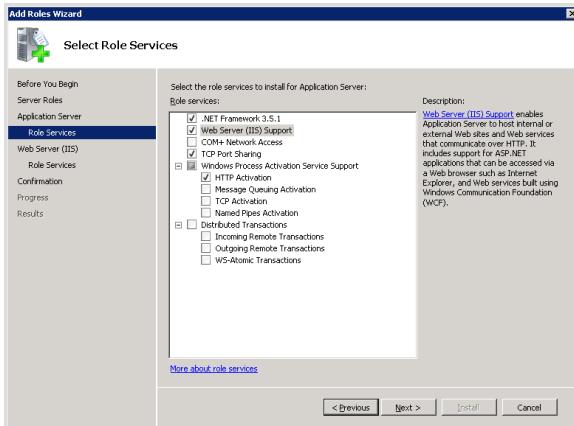
1. Open **Start » Administrative Tools » Server Manager** and launch the Wizard.
2. Check if the *Web IIS Server* has been installed by clicking on **Roles** in the left pane, expanding it or **Server Manager » Roles**.
 - a. For a new server, click **Add Roles** in the right pane to install Web Server (IIS).
 - b. If Web Server (IIS) is already installed, then right click on **Web Server (IIS)** in the left pane and click **Add Roles** to verify the entire role services listed in this document are already selected.
3. From the *Add Roles Wizard* window, select **Next**. Click **Next** on the *Before You Begin* window. The *Select Server Roles* window appears.



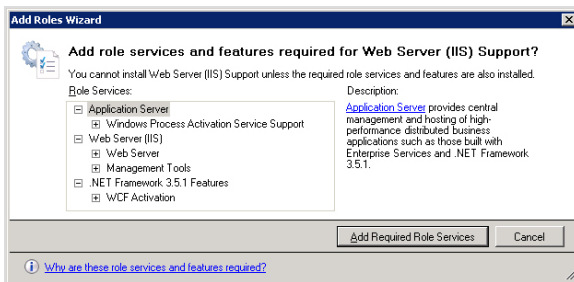
4. Select the checkbox for **Application Server**.
5. Another pop-up window will appear requiring both **.NET Framework** and **Windows Process Activation Service** be installed. Select **Add Required Features** to install these additional role services for the Application Server.



6. Select the checkbox for **Web Server IIS**. Click **Next**. At the *Introduction to Application Server* window, select **Next**.
7. At the *Application Server Select Role Services* window, enable the following services:

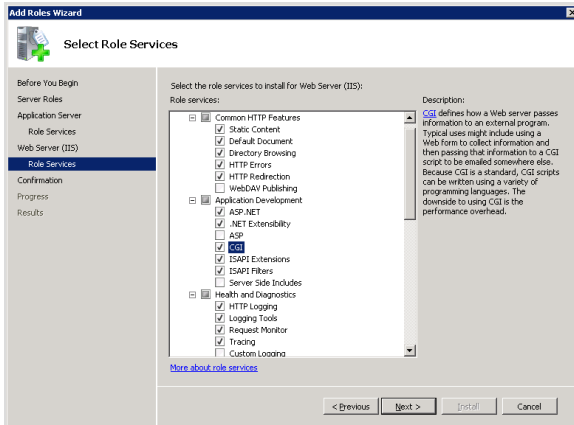


- a. Select **.NET Framework 3.5.1**
- b. Select **Web Server (IIS) Support**



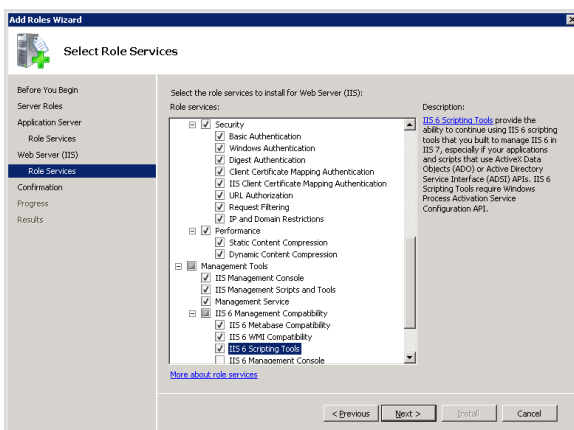
8. A pop-up window will appear noting additional Application Server, Web Server (IIS) and .NET Framework services. Select **Add Required Role Services**.
 - a. Select **TCP Port Sharing**
 - b. Select **HTTP Activation**
 - c. Select **Next**. At the *Introduction to Web Server (IIS)* window, select **Next**.
9. On the *Select role services* window, required services will be selected when Web Server (IIS) Support Required Role Services are installed. Select ALL additional services in **BOLD**:
 - Under *Common HTTP Features*, verify that *Static Content*, *Default Document*, *Directory Browsing*, *HTTP Errors* and *HTTP Redirection* are selected.

- Under *Application Development*, verify that *ASP.NET*, *.NET Extensibility*, *CGI*, *ISAPI Extensions*, and *ISAPI Filters* are selected. Under *Health and Diagnostics*, verify that *HTTP Logging*, *Request Monitor*, and *Tracing* are selected.



- Under *Security*, verify that *Windows Authentication* and *Request Filtering* are selected.
- Under *Management Tools*, verify that *IIS Management Console*, *IIS Management Scripts and Tools*, and *Management Service* are selected.

10. Select **IIS6 Management Compatibility**, then **IIS 6 Metabase Compatibility**, **IIS 6 WMI Compatibility**, and **IIS6 Scripting Tools** check boxes.



11. Select **Next**, then click **Install** at the *Confirm Installation Selections* pane.
12. Select **Close** when the installation is completed and click **Close** on the *Server Manager*.

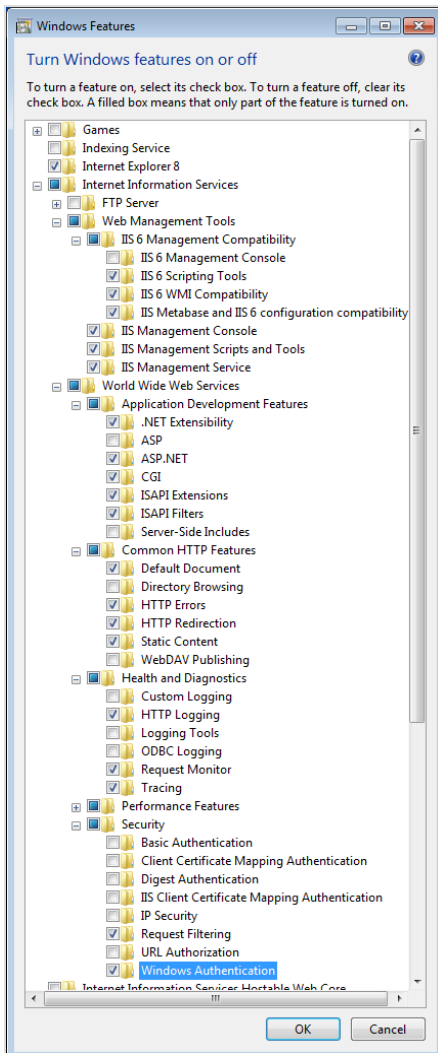
NOTE: File Services can also be turned on so that Windows can manage storage and faster file searching. If desired, make sure the *File Server* role is turned on.

4.2.3 For Windows 7

The procedure to add the Web Server (IIS) role on Windows 7 Professional Workstation is:

1. Click *Start » Control Panel » Programs » Programs & Features*. In the left menu, click *Turn Windows Features on and off*.
2. Under *Internet Information Services » Web Management Tools » IIS 6 Management Compatibility*, check the following roles: *IIS 6 Scripting Tools, IIS 6 WMI Compatibility, IIS Metabase and IIS 6 configuration compatibility, IIS Management Console, IIS Management Scripts and Tools* and *IIS Management Service* checkboxes.
3. Under *Internet Information Services » World Wide Web Services » Application Development Features*, check the following roles: *.NET Extensibility, ASP.NET, CGI, ISAPI Extensions and ISAPI Filters* checkboxes.
4. Under *World Wide Web Services » Common HTTP Features*, check the following roles *Default Document, HTTP Errors, HTTP Redirection and Static Content* checkboxes.
5. Under *World Wide Web Services » Health and Diagnostics*, check the following roles *HTTP Logging, Request Monitor, Tracing* checkboxes.
6. Under *Security*, check the following roles *Request Filtering* and *Windows Authentication* checkboxes.
7. Click *OK*. Windows 7 will take a few minutes to make the changes to the Features settings and show progress with a window.

8. When completed, reboot the Windows 7 machine.



4.3 Install Engage Services, HTTPS (if used) and the Web Client

With the server OS and SQL software installed and configured, the following can be installed:

- TelStrat Engage Services.
- Engage Web Client and its database.

- HTTPS, is used.
- Another web database for backup and upgrade purposes.

NOTE: If the customer requires a secure HTTPS URL for the server-web client connections, a digital SSL certificate name will need to be available for this installation. Refer to HTTPS Certificates for details.

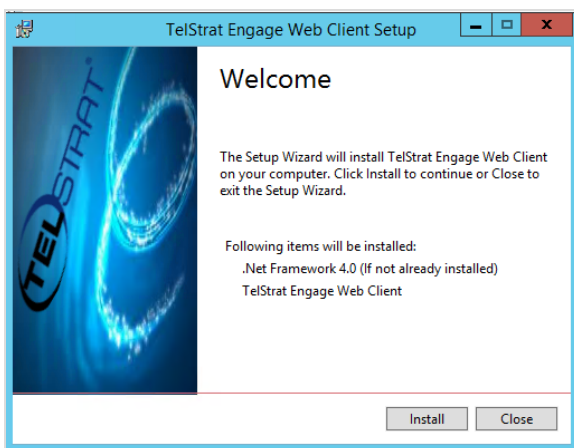
Engage software installation is normally accomplished by launching a setup.exe type file which will step through the installation of the various services, HTTPS and web client installations.

Begin the Engage Services and Web Client software installation (locally or remotely):

NOTE: If the setup program encounters a problem, click **OK** to end the installation process and refer to the Troubleshooting section of this guide, specifically, Web Server Troubleshooting topics for help.

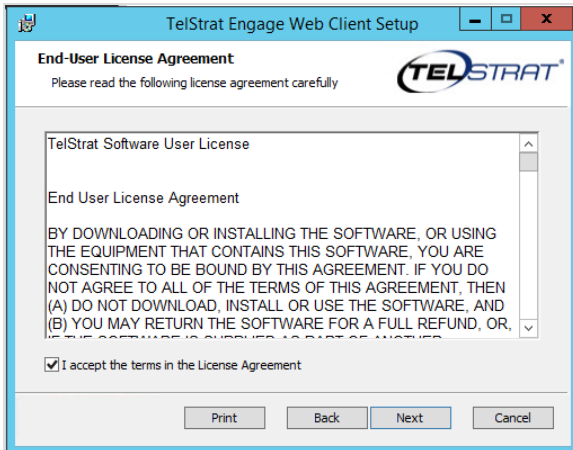
To install the Engage Services and Web Client software, use the downloaded software found on the Engage server in the folder **C://EngageSoftware/Engage5.x.x**.

1. Navigate to **Engage 5.x.x**. » **Engage 5.x.x.x Web.zip** folder, unzip it and execute the **TelStrat.exe** file to begin to installation procedure. The Welcome window appears. Click **Install**.



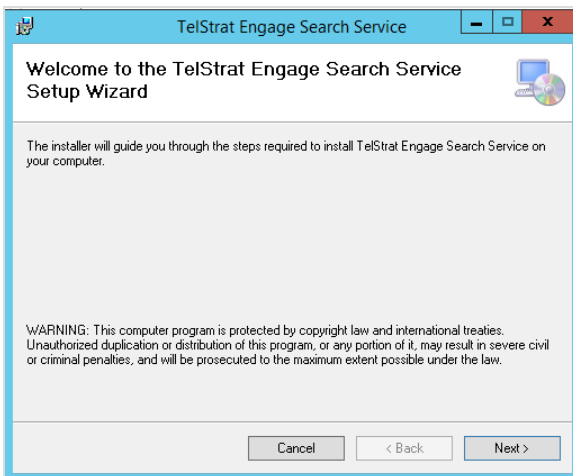
2. There will be a series of setup progress screens that will pop up as the wizard installs various software services and components.

3. At the **End-User License** window, click on *I accept the terms of the License Agreement* and click **Next**.



Install the TelStrat Engage Search Service

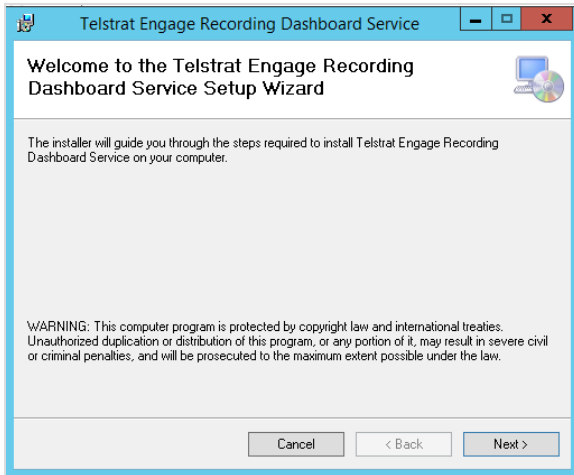
1. When the *TelStrat Engage Search Service* window appears, click **Next**.



2. Use the default installation folder for the *Search Service* (ex. **C:\Program Files (x86)\TelStrat\TelStrat Engage Search Service**).
3. Click **Next**.
4. Confirm the installation by clicking **Next**. When the installation is complete, click **Close**.

Install the TelStrat Engage Recording Dashboard Service

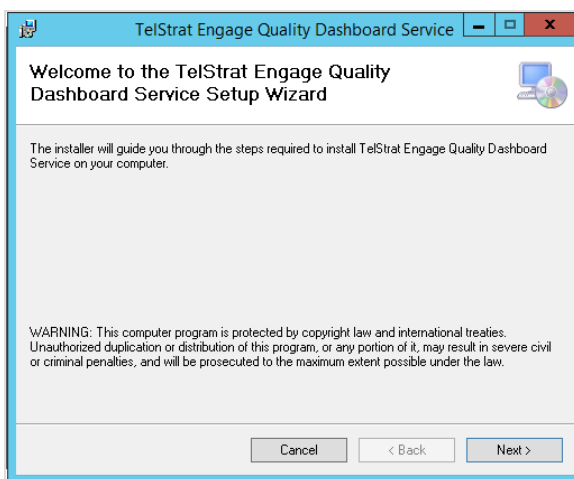
1. When the *TelStrat Engage Recording Dashboard Service* window appears, click **Next**.



2. Use the default installation folder for the *Dashboard Service* (ex. **C:\Program Files (x86)\TelStrat\TelStrat Engage Dashboard Service**).
3. Click **Next**.
4. Confirm the installation by clicking **Next**. When the installation is complete, click **Close**.

Install the TelStrat Engage Quality Dashboard Service

1. When the *TelStrat Engage Quality Dashboard Service* window appears, click **Next**.



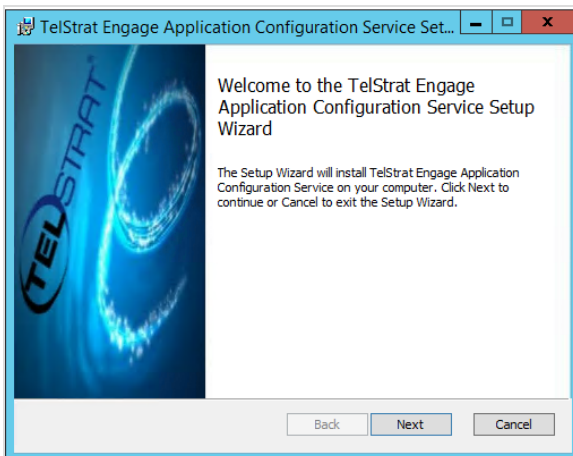
2. Click **Next**. Use the default installation folder for the *Quality Dashboard Service* (ex. **C:\Program Files (x86)\TelStrat\TelStrat Engage Quality Dashboard Service**).
3. Click **Next**.
4. Confirm the installation by clicking **Next**. When the installation is complete, click **Close**

Install the TelStrat Engage Application Configuration Service

Besides installing this service, this part of the software installation will create a new web database and name in SQL for the Web Client to use (ex. Engage).

NOTE: When installing a new Release 5.x or are upgrading from Release 4.x or earlier to Release 5.x for the first time, **ALWAYS** install another new web database to be used by the **Import Data** web client program to import data from an existing release 4.x or 5.x database. This procedure preserves the content of this release of web server's database structure to allow for import of the previous release's configurations and structure.

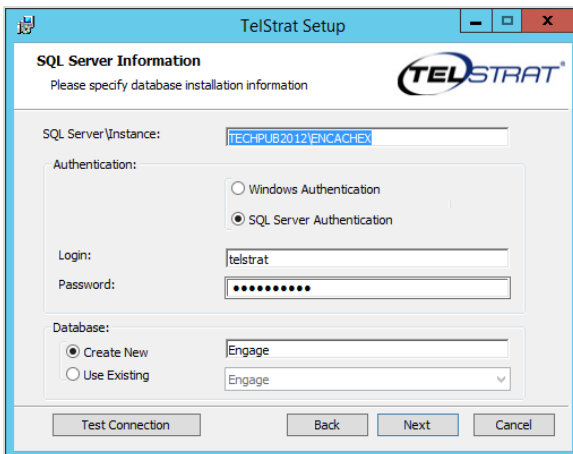
1. When the *TelStrat Engage Application Configuration Service* window appears, click **Next**.



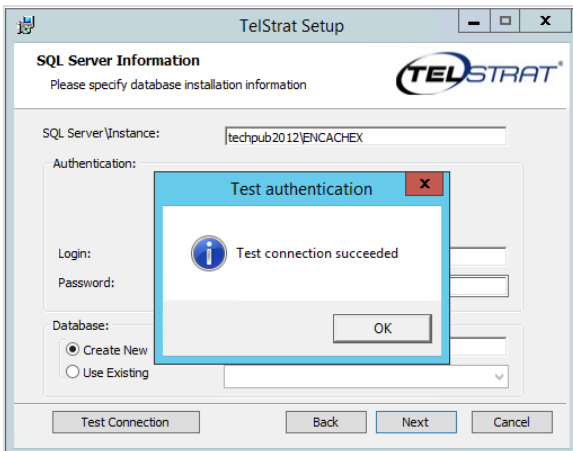
2. Check **I accept the terms of the licensing agreement**. Click **Next**.
3. In the *SQL Server Information* window, complete these fields with:
 - **SQL server\instance**: The server and instance names for the cache database (ex. *tech-pub2012\ENCACHEX*).

- **Authentication:** Click the SQL Server Authentication button and enter the Login (*sa*) and Password.
- **Database:** Click on *Create New* database that the Web Client will use. TelStrat installers use the default name *Engage* for this field.

NOTE: If upgrading from a previous major release, do not connect to an existing database. Create a new database and then complete the upgrade which includes steps for importing data from a previous major release. If upgrading from the same major release, an existing database may be used.



4. Click the *Test Connection* button to make sure the SQL Cache Database is accessible. Look for the *Test Connection Succeeded* box. Click *OK*. Click *Install*.



5. After the installation is complete, click **Finish**.

NOTE: At the end of this installation procedure, there is an additional step (**Create an Empty 5.0 Database**) to RERUN the Web installer to create the new empty database with a different name (ex. Engage51).

Install the TelStrat Recurring Report Service

1. When the TelStrat Engage Recurring Report window appears, click **Next**.
2. Click **Next**. Use the default installation folder for the *Quality Dashboard Service* (ex. **C:\Program Files (x86)\TelStrat\TelStrat Engage Recurring Report Service**).
3. Click **Next**.
4. Confirm the installation by clicking **Next**. When the installation is complete, click **Close**.

Install the TelStrat Engage Web Service

1. When the TelStrat Engage Web Service window appears, click **Next**.
2. Click **Next**. Use the default installation folder for the *Quality Dashboard Service* (ex. **C:\Program Files (x86)\TelStrat\TelStrat Engage Web Service**).
3. Click **Next**.
4. Confirm the installation by clicking **Next**. When the installation is complete, click **Close**.

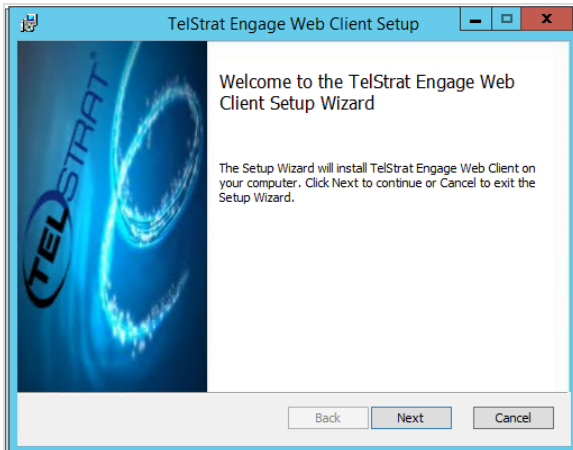
Install the TelStrat Engage Speech Analytics Dashboard Service

1. When the TelStrat Engage Speech Analytics Dashboard Service window appears, click **Next**.
2. Click **Next**. Use the default installation folder for the *Quality Dashboard Service* (ex. **C:\Program Files (x86)\TelStrat\TelStrat Engage Speech Analytics Dashboard Service**).
3. Click **Next**.
4. Confirm the installation by clicking **Next**. When the installation is complete, click **Close**.

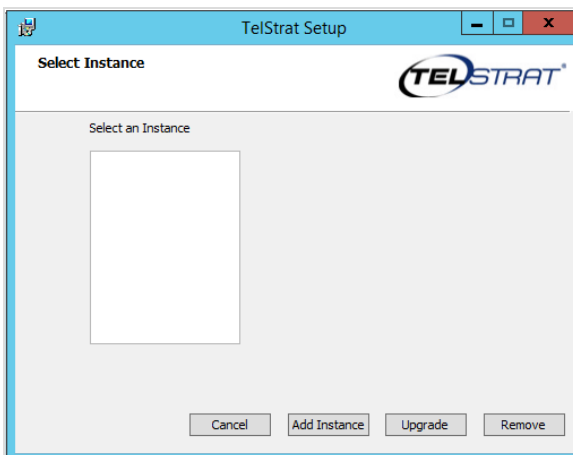
A number of pop-up windows will flash by as the setup and installation process continues.

Install the TelStrat Engage Web Client

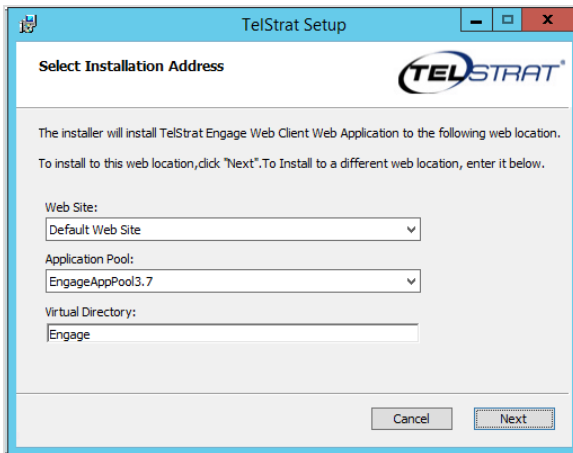
1. When the **TelStrat Engage Web Client Setup** window appears, click **Next**.



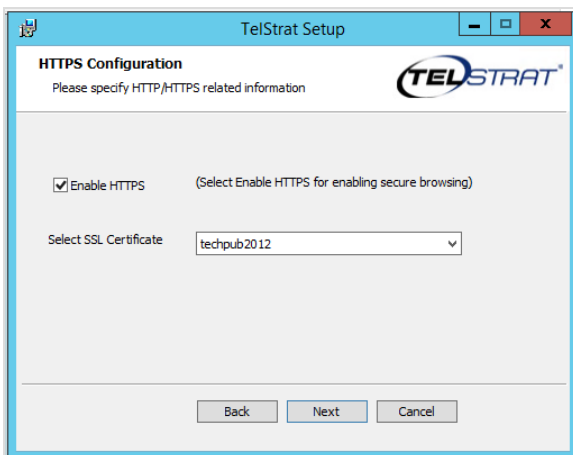
2. Click on **I accept the terms of the License Agreement** and click **Next**.
3. At the **Select Instance** window, click on **Add Instance**.



4. At the **Select Instance Address** window, enter **Engage** into the Virtual Directory field and click **Next**.

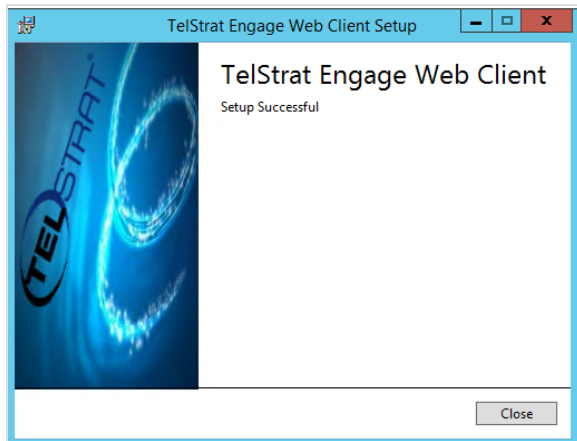


5. At the **HTTPS Configuration** window,
 - If the customer configuration **does not require** HTTPS URL security and no SSL certificate is available, click **Next** to bypass this window.
 - If the customer configuration **does require** a secure HTTPS web URL, check the **Enable HTTPS** checkbox and select the appropriate **SSL certificate** from the drop-down menu, then click **Next**.



6. Confirm the installation by clicking **Next**.
7. Start the installation by clicking **Install**. A number of installation screens and pop-ups occur.
8. When the installation is complete, click **Finish**.

There will be a few more update screens while the setup process continues. When installation is complete, **Setup Successful** will display. Click **Close**.



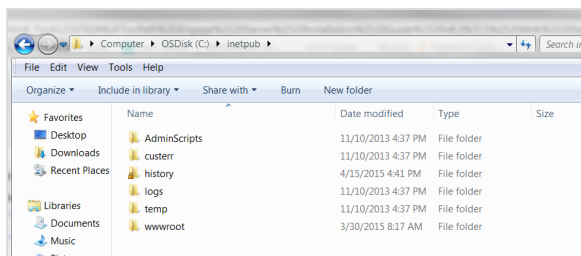
4.4 Configure Folder Permissions

After the Services and Web Client software is installed on the IIS web server, folder permissions must be configured or playing back of calls will result in *File not Found* error messages.

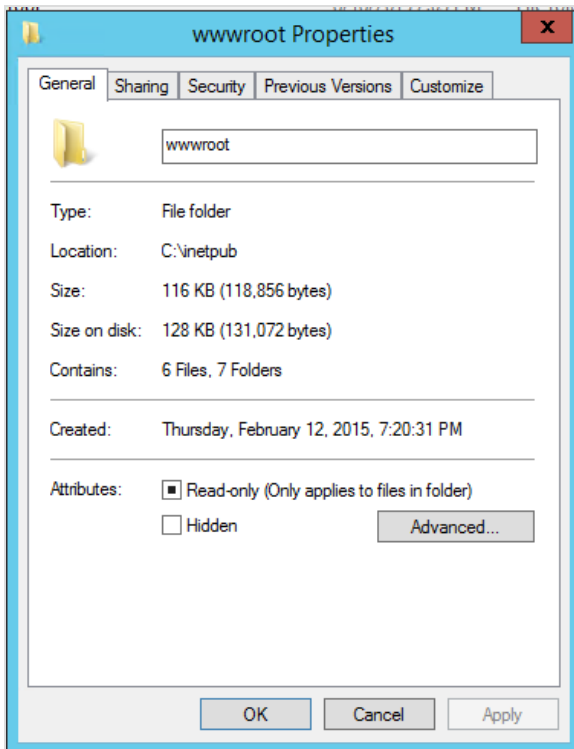
After making this change, a logoff and logon to the Web Client is required or an **Internal Server Error** message will appear.

NOTE: Required for ALL deployment types.

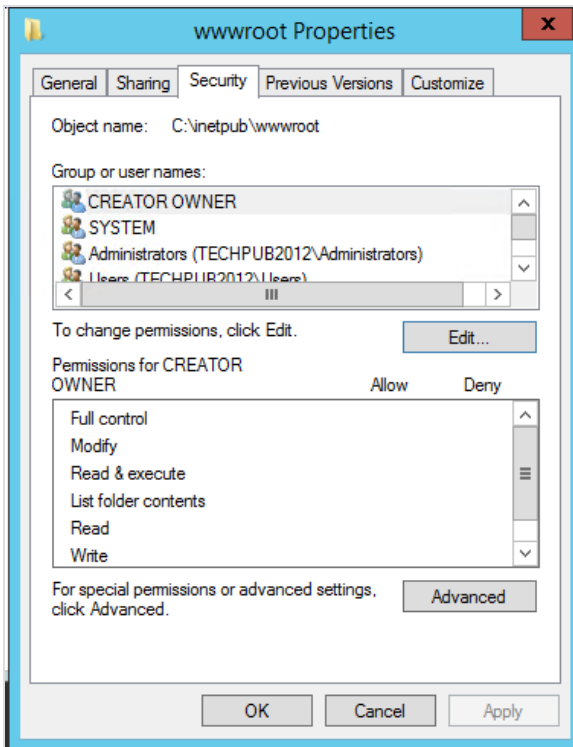
To provide IIS full permissions for attachments on the web server, make these changes:



1. On the Engage voice recorder server, navigate to **[c:\inetpub\wwwroot](#)**.
2. Highlight the folder **wwwroot**, right-click on it to get the pop-up menu and click on **Properties**.



3. *De-select* the *Read Only* check box.
4. Click *Apply*.
5. Select the **Apply changes to this folder, subfolders and files** button. There will be a few update windows. Click *OK*.
6. Click the *Security* tab.



7. Click **Edit** then click **Add**. The **Select Users, Computers, Service Accounts, or Groups** window appears.
8. Enter *Authenticated Users* or the appropriate group of users if the customer's IT person is available.
9. Click **Check Names** button. *Authenticated Users* should become underlined.
10. Click **OK**.
11. While highlighting *Authenticated Users*, click on all Permissions **checkboxes**, click **Apply** then **OK**.
12. If prompted by a new window, select **Apply Changes** to this folder, subfolders and files to complete the process.

4.5 Rewrite HTTP to Redirect to HTTPS

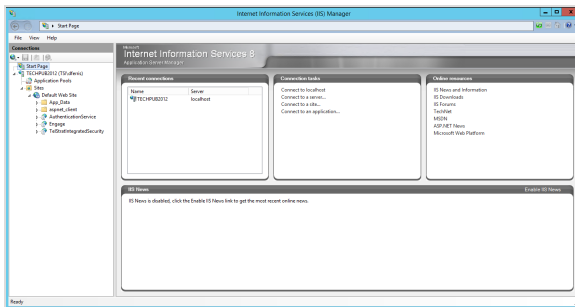
If the customer's configuration requires the use of HTTPS secure URLs, it will necessary to REDIRECT all *HTTP://<servername>/Engage* requests to the *HTTPS://<servername>/Engage* URL.

To have the server redirect an HTTP:// type URL request redirected to an HTTPS:// type URL, the server's IIS needs to be prepared.

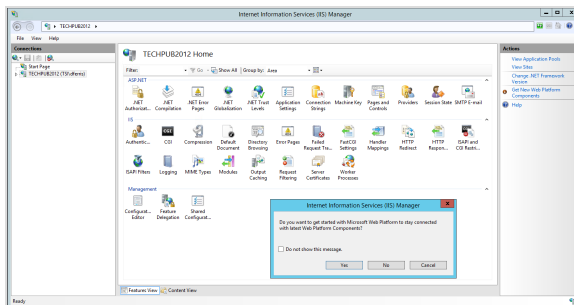
Note: If using IIS 8, the user will need to install the URL Rewrite module. If already installed, skip to Create Rewrite URL Rule subsection.

Install URL Rewrite Software Module

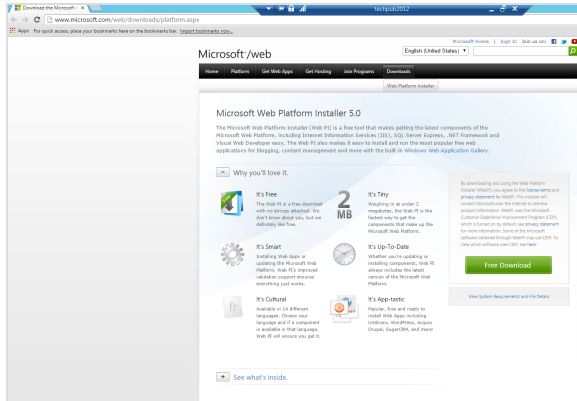
1. Logon to the Engage server as an administrator.
2. From the *Server Manager*, launch the **Internet Information Services (IIS) Manager**.



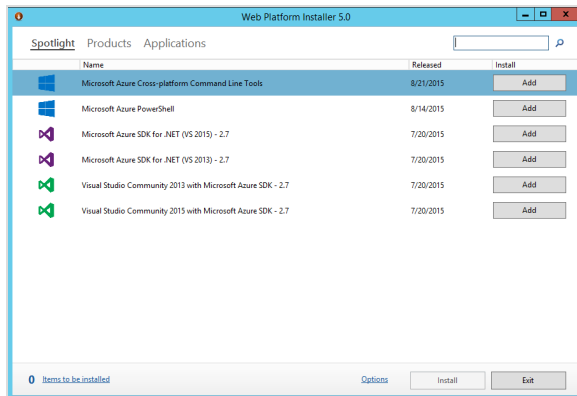
3.
 - a. If not already installed, a request will be made to install the **Web Platform Components** installer into the IIS Manager. Click [Yes](#).



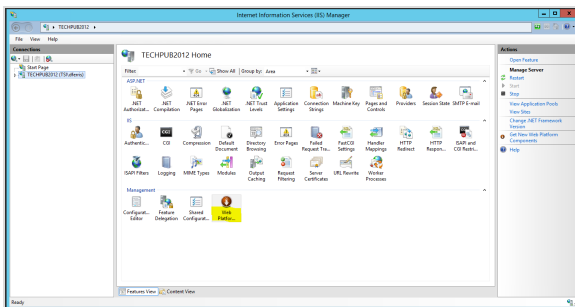
- b. If installation is needed, the user is directed to a Microsoft website. Click [Free Download](#) to start installation of the free **Microsoft Web Platform Install** tool.



c. Click **Add**.

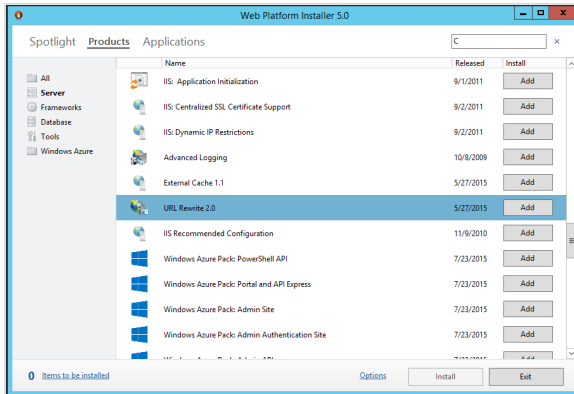


4. When completed, the **Web Platform Installer** icon will be available on the in the **IIS Manager** of the <servername> server (ex. techpub2012).

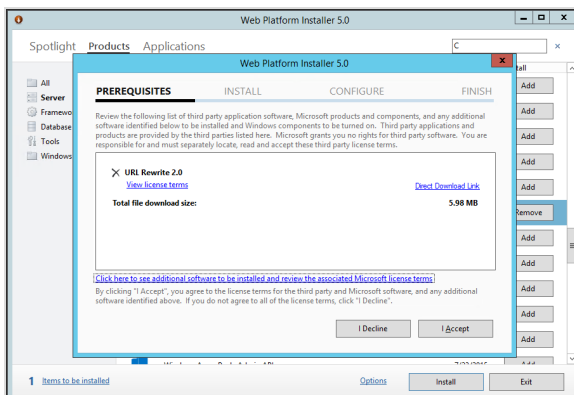


5. Click on the **Web Platform Installer** icon to generate the list of software that could be added to the server. Click on the **Products** heading then click on **Name** to get an alphabetical list.

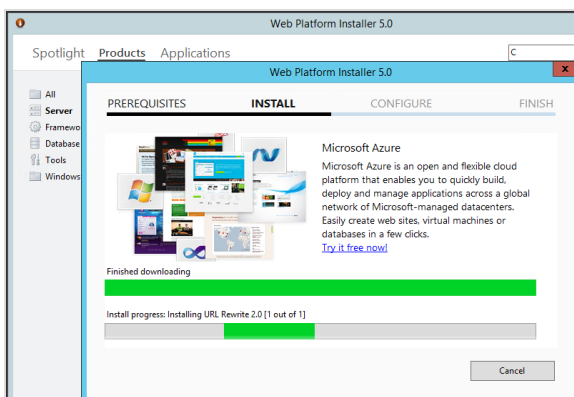
6. Scroll down the list and locate **URL Rewrite x.x** and click the **Add** button.



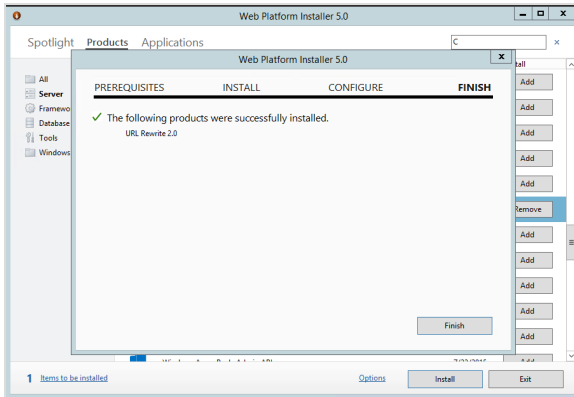
7. Click on **I Accept** for the license.



8. Click on **Install** to begin the installation of the **URL Rewrite x.x** software into the **IIS Manager**.

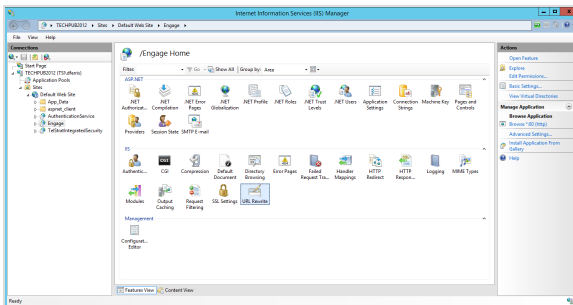


9. Click **Finish** to close the install when completed.

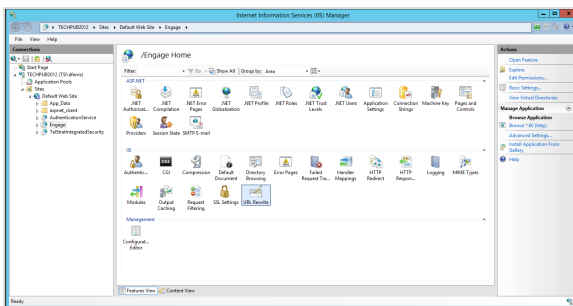


Create a Rewrite URL Rule

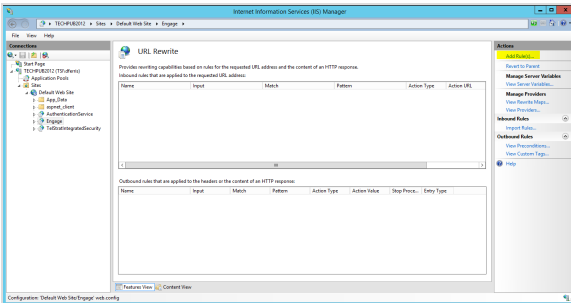
1. Return to the server's **IIS Manager** page and expand <servername> and click on the newly installed **URL Rewrite** icon. If the icon is not present after the install, exit and re-enter the **IIS Manager** to get the content of the tool refreshed.



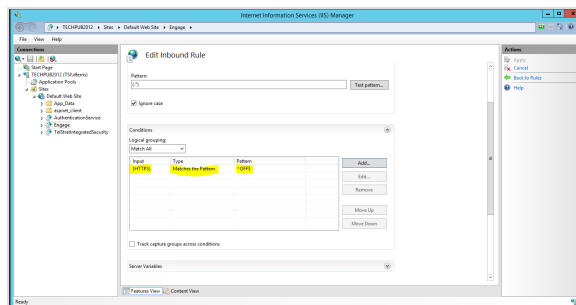
2. Expand the folders for <servername> » **Sites** » **Default Web Site** and highlight the **Engage** folder.
3. Double-click on the **URL Rewrite** icon to get the **URL Rewrite** page.



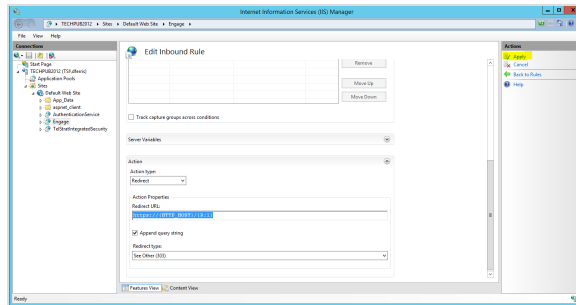
4. On the right-hand **Action** pane, click on **Add Rule** to get the **Add Rule** window.



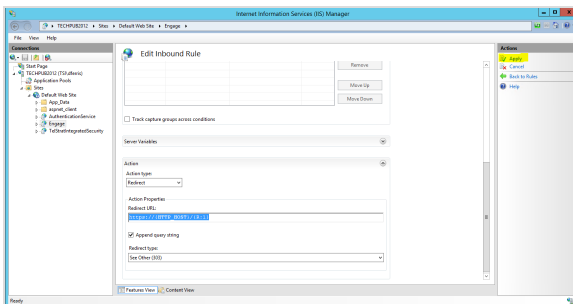
5. Click on **Blank Rule** and click **OK** to get the **Edit Inbound Rule** screen and enter the following:
 - a. **Name:** Enter a descriptive name, such as HTTP to HTTPS.
 - a. **Match URL box:**
 - **Requested URL:** Leave the default of *Matches the Pattern*.
 - **Using:** Leave the default of *Regular Expressions*.
 - **Pattern:** Enter **(.*)** (open round bracket, dot, star, close round bracket).
 - **Ignore case** checkbox: Remains checked.
 - a. **Conditions:** Click on the down arrow to get the **Conditions** box.
 - Click **Add**.
 - **Condition input:** Enter **{HTTPS}** (open curly bracket, H T T P S closed curly bracket).
 - **Check if input string:** Leave at default of *Matches the Pattern*.
 - **Pattern:** Enter **^OFF\$** (caret, O F F, \$).
 - Click **OK**.



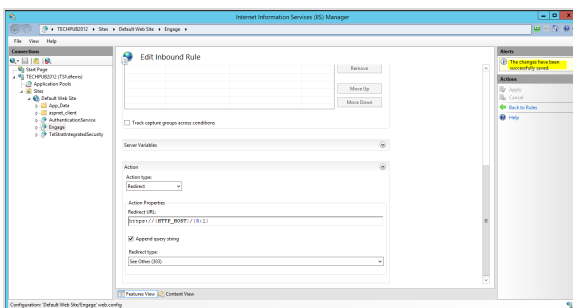
- a. **Action:** Click on the down arrow to be the **Action** box.
 - **Action Type:** Click on the drop-down menu and select **Redirect**.
 - **Redirect URL:** Enter **`https://{HTTPS_HOST}/{R:1}`** using open and closed curly brackets.
 - **Append query timing** checkbox: Remains checked.
 - **Redirect type:** Select **See Other (303)** from the drop-down menu.



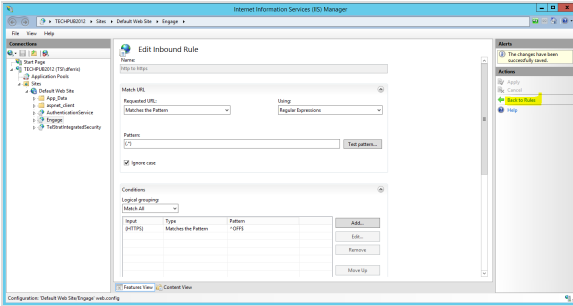
6. Click on **Apply** in the upper right hand **Actions** pane.



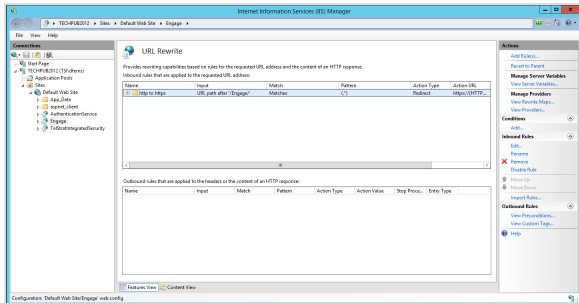
7. Check that the rules were applied successfully by finding the statement that the rules were applied successfully.



8. In the right-hand **Actions** pane, click on *Back to Rule* and check the entry.

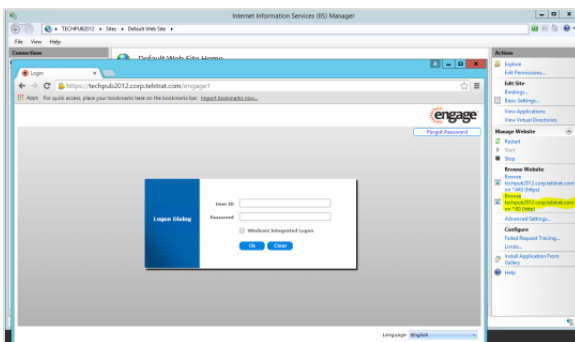


9. Click the + symbol to expand for a few more details.



Check that Redirect Occurs

- Check that the REDIRECT from and HTTP:// URL to an HTTPS:// URL works by using the Default Web Site window.
- On the right-hand pane, click on the *Browsecom on *:80 (http)* command.
- Observe the browser that launches and make sure the **https://** version of the URL appears in the browser indicating the redirect functioned correctly.



4.6 Verify Web Client HTTP and HTTPS Screen

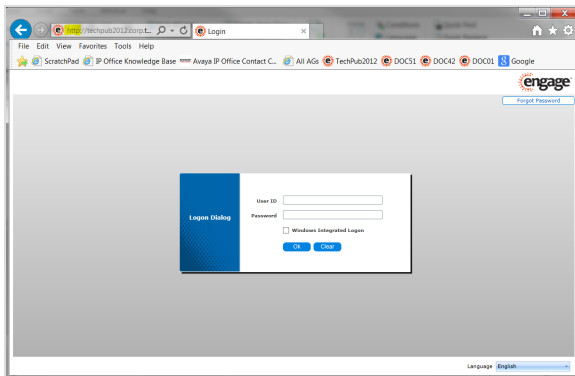
It is very important that the Web Client can be accessed by workstations in the deployment. Depending on the type of deployment relative to non-secure and secure URLs, access testing will be different.

HTTP Only

If the deployment is using HTTP non-secure URLs to access the Web Client, check workstations access to the Web Client using HTTP. From a workstation, launch a browser and access the Web Client using an HTTP URL with the syntax: **http://<servername>/engage**

(ex. <http://techpub2012.corp.telstrat.com/engage/>).

Verify the Logon Screen appears with HTTP in the address box.

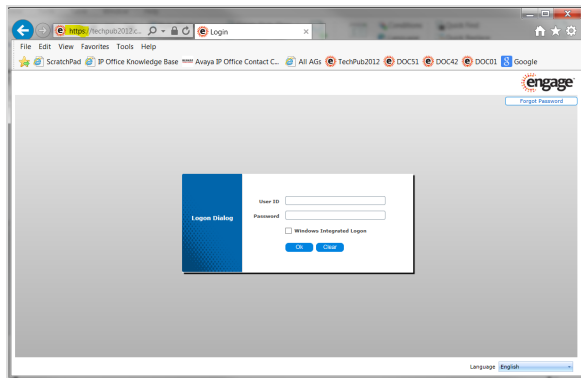


HTTPS Only

If the deployment is using HTTPS secure URLs to access the Web Client, check workstations access to the Web Client using HTTPS. From a workstation, launch a browser and access the Web Client using an HTTPS URL with the syntax: **https://<servername>/engage**.

(ex. <https://techpub2012.corp.telstrat.com/engage/>).

Verify the Logon Screen appears with HTTPS in the address box.



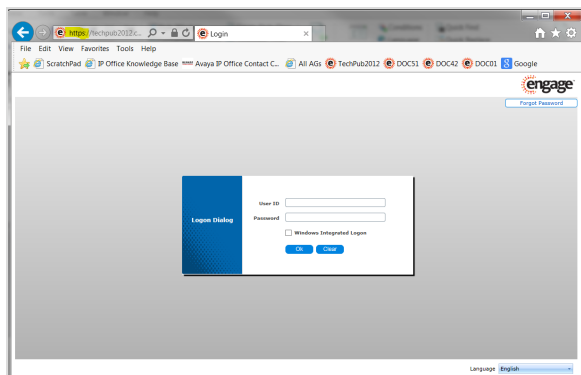
HTTP Redirected to HTTPS

Additionally, because a deployment is using HTTPS secure URLs, a test is needed to make sure that an HTTP non-secure URL is rewritten to point to the HTTPS secure URL.

Check this ability from a workstation by launching a browser and entering an HTTP URL with the syntax:

http://<servername>/engage.

(ex. <http://techpub2012.corp.telstrat.com/engage/>)



Verify the Logon Screen appears with **HTTPS** and not HTTP in the address box.

Refer to the WEB SERVER (IIS) section of this guide if this screen does not appear.

5 Engage Record Server Installation

Installation and configuring the Engage Voice Recorder software consists of:

- Making sure all appropriate prerequisite software is installed and settings are made.
- Downloading and installing the Engage product software.
- Downloading and installing support software and tools.
- Configuring the server and restarting services.

5.1 Engage Server Prerequisite Setup

Prior to beginning the Engage software installation processes, some preparation and prerequisite software must already be in place. Prerequisite requirements are:

- Partition configuration and Domain Account Setup.
- Enabling the Desktop Experience feature.
- Adding the Application Server Role.
- Installing JAVA JRE.

Some Engage software-dependent components will be installed as part of the recorder software installation process and do not need to be individually installed, as in previous releases of Engage. These components include:

- Installing .NET software.
- Installing Microsoft Visual C++ 2008 and 2010.
- Installing the WinPCap for VoIP.
- Installing WinPCap (for a Cisco deployment Only).

5.1.1 Partition Configuration and Adding the Domain Account

All **storage partitions** must be setup and in place before installing the Engage software on the voice recording server. Refer to the customer's SOW, project requirements and system specifications for the details for this

specific deployment.

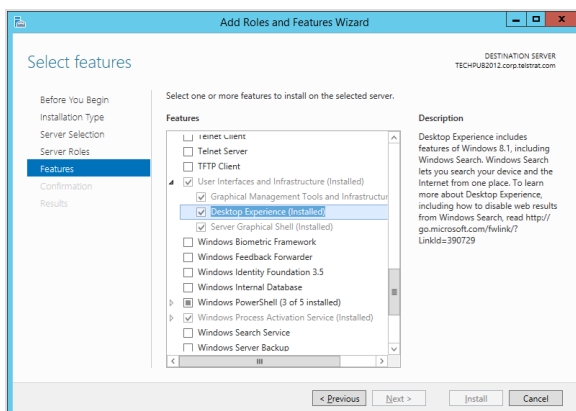
The **Engage Domain Service Account** must be added to the local Administrator group on each Engage server to ensure no operating deficiencies or issues with regards to the Engage services.

5.1.2 Enable the Desktop Experience feature

The **Desktop Experience** feature allows installation of a variety of applications and features that are provided in the Windows client operating system on a server that is running a Windows Server operating system.

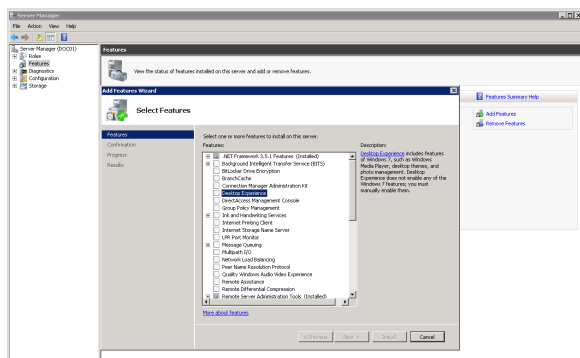
For *Windows Server 2012*, the **Desktop Experience** feature must be enabled to support playing call recordings on the recording server for testing purposes. Install **Desktop Experience** using the Server 2012 Server Manager wizard with these steps:

1. Launch the *Server Manager*.
2. On the toolbar, click *Manage* then *Add Roles and Features*.
3. Click *Next*, then *Next* again. Select the server by highlighting it, click *Next*.
4. Click *Features* and scroll down and find *User Interfaces and Infrastructure*.
5. Select the *Desktop Experience* check box, and click *Next*.
6. Complete the wizard by clicking *Install*.
7. A **Restart** will be required to add the feature to the server.



For *Windows Server 2008 R2*, the **Desktop Experience** feature must be enabled to support playing call recordings on the recording server for testing purposes as well. Install the Desktop Experience feature using the Windows Server 2008 R2 Server Manager wizard.

1. Launch the *Server Manager*.
2. On the left hand pane, click *Features*.
3. On the right-hand side, look for and click *Add Features*. The **Select Features** window appears.
4. Scroll down the list and find **Desktop Experience** and check the checkbox.
5. An *Add Features Wizard* box will appear demanding confirmation for adding the feature. Click *Add Requested Feature*.
6. Click *Next* and complete the wizard by clicking *Install*.
7. Click *Close* to terminate the Install Wizard.
8. A reminder will appear that a **Restart** will be required to add the feature.



5.2 Add the Application Server Role to SQL Server

The Application Server role provides central management and hosting of high performance distributed business applications such as those built with Enterprise Services and .NET Framework 4.5 and is required for Engage.

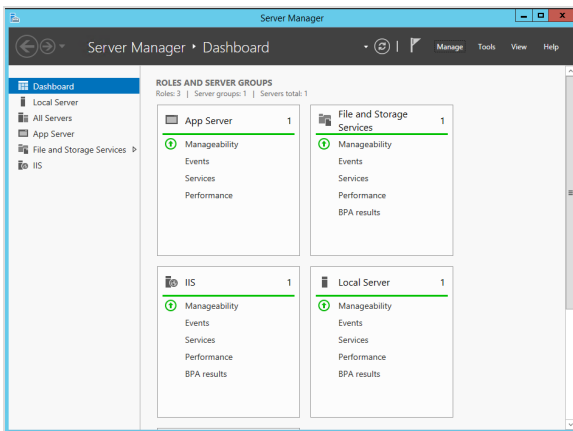
If the server platform is going to support both the Application Server AND the Web Server (IIS), both sets of role settings can be implemented at this time. Use this subsection to administer the Application role and

refer to the Web Server (IIS) Support settings in the web server installation section of this document to perform both roles settings and configurations in one session.

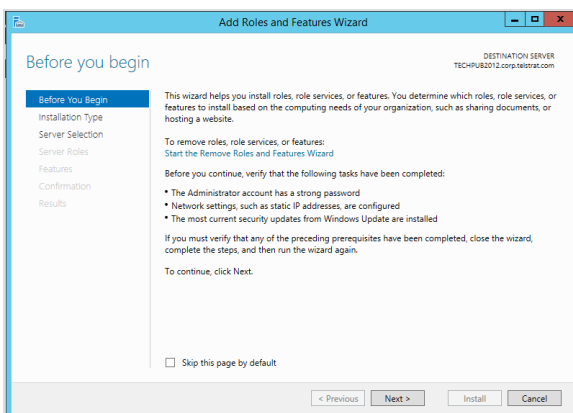
NOTE: This step typically requires a restart upon completion.

Select the Application Server Role:

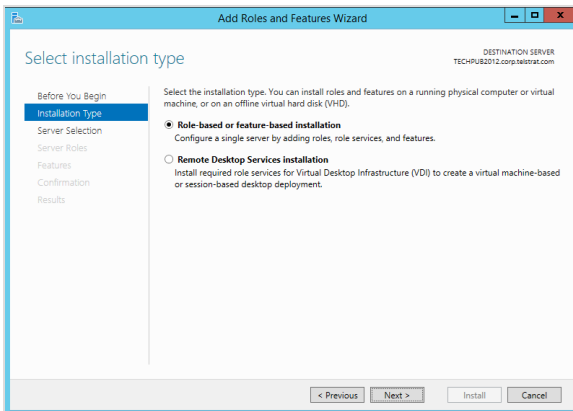
1. From the Desktop or Start menu, launch the *Server Manager* tool.



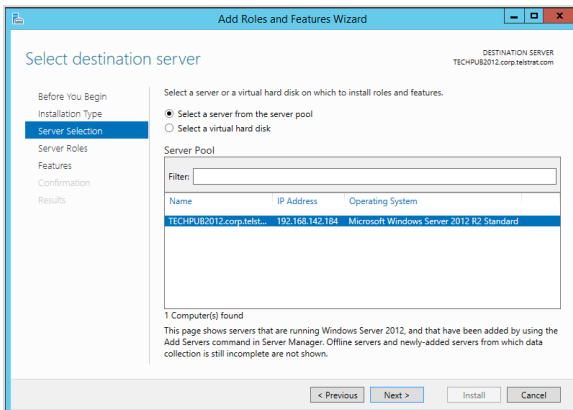
2. On the left-hand top side, click on *Manage* to get the menu and click on *Add Roles and Features* command. The *Before you Begin* window appears. Click *Next*.



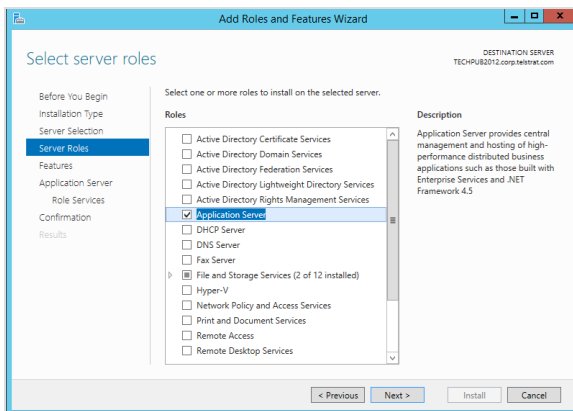
3. On the *Select Installation type* window, make sure the button for *Role-based or feature-based installation* is selected, then click *Next*.



4. On the *Server Selection* window, make sure the correct server name (ex. *techpubs2012*) is selected, then click *Next*.



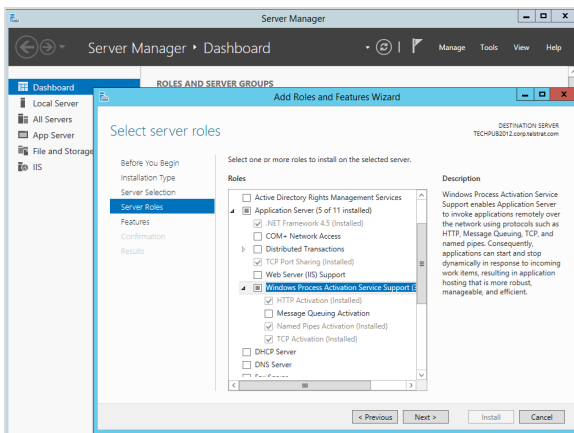
5. On the **Select Server Roles** window, scroll down the Roles list, locate and enable the checkbox for *Application Server*. Click *Next*.



NOTE: Another pop-up window may appear requiring both .NET Framework and Windows Process Activation Service to be installed. Click the **Add Required Features** button to install these additional role services for the Application Server, then click **Next**.

Select server features

1. At the *Select features* window, make sure to click on and select the following features:



- **.NET Framework 3.5.1**
- **TCP Port Sharing**
- **HTTP Activation**

NOTE: The Engage Voice Recorder uses WCF services for internal communications. HTTP Activation is required for WCF.

2. Click **Next** then click **Install** at the *Confirm Installation Selections* pane.
3. Click **Close** when the installation has succeeded and **Close** the *Server Manager*.

NOTE: If desired, make sure the **File and Storage Services** role is turned on. When File Services is turned on, Windows can manage storage and faster file searching.

5.2.1 Windows Server 2003 and XP Additional Requirements

Installing these software packages can occur at different steps in the installation depending on machine configurations. However, they must be installed for Engage to function properly.

NOTE: If the current system is equipped with Windows Server 2003 and XP and is being upgraded to SQL 2008, then these software packages need to be installed.

Install Windows Installer 4.5 and then reboot the server. If unsure, proceed with the installation of SQL 2008 R2 Express and a link will be provided by the setup software. Locate, In the downloaded software folders located on the Engage Voice Recorder:

Navigate to [EngageSoftware » Engage x.x Pre-Reqs & Tools NO SQL » Windows Installer 4.5](#) and click on either:

- [WindowsServer2003-KB942288-v4-x64.exe](#) for the 64-bit version.
- [WindowsServer2003-KB942288-v4-x86](#) for the 32-bit version.
- [WindowsXP-KB942288-v3-x86](#) for the Windows XP version.
- [Windows6.0-KB942288-v2-x64](#) for the Windows 6 64-bit version.
- [Windows6.0-KB942288-v2-x86](#) for the Windows 6 32-bit version.

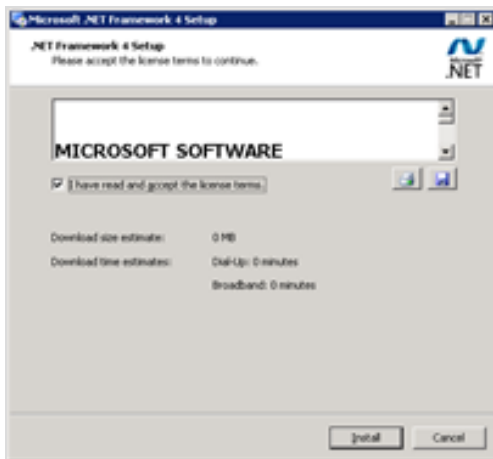
NOTE: Windows Server 2012 and 2008 R2 do not require the following step as long as the Application Server role is already added in the Server Manager.

Install Microsoft .Net framework

The Microsoft .NET Framework enables multiple Engage applications as well as the Web Client user interface to communicate successfully with the Engage recorder. The Web Client requires Microsoft .NET 4.0 or later.

To install the .NET Framework on a Windows 7 Professional, 2003 or XP server, install the complimentary copy of Microsoft .NET Framework from the Engage Pre-Reqs folder:

1. On the server, navigate to [EngageSoftware » Engage x.x Pre-Reqs & Tools NO SQL » Windows Pre-Reqs](#).
2. Click on the [dotNetFx40_Full_x86_x64](#) file to install .NET Framework.
3. When the setup wizard has opened, select *I have read and accept the license terms* checkbox.



4. Click **Install** and **Finish** when installation is complete.

5.2.2 Microsoft Visual C++ 2008 and 2010 - Auto-installed

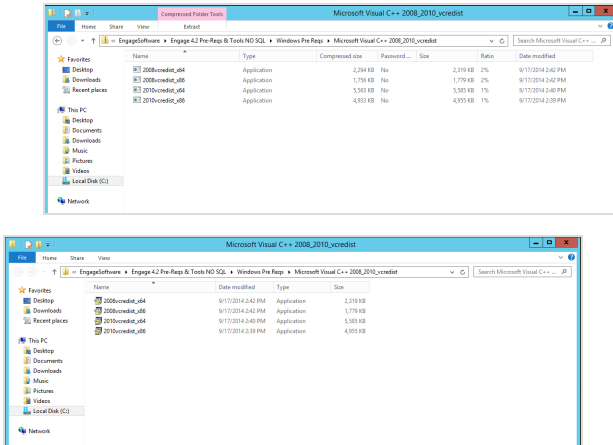
Microsoft Visual C++ 2008 is automatically installed by Engage Voice Recorder installation software and does not need to be manually installed.

Microsoft Visual C++ 2010 is required for all Engage installations to:

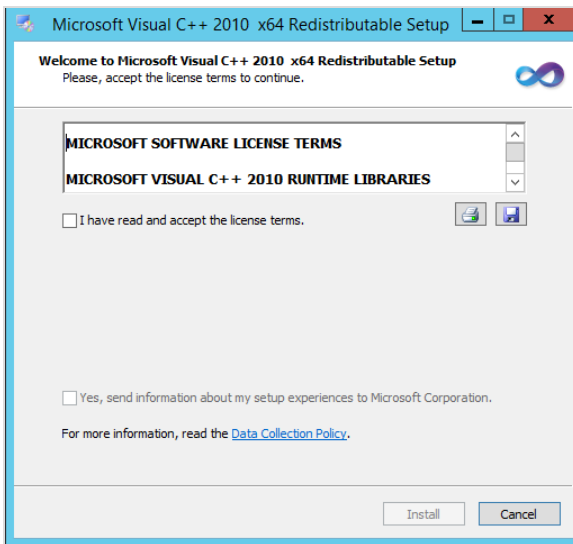
- Playback calls in the timeline player for IE11, IE10, and IE9.
- Required to download an .MP3 call recording.
- Required for the Event Monitor to function.

These are the steps to install Microsoft Visual C++ 2010, if needed:

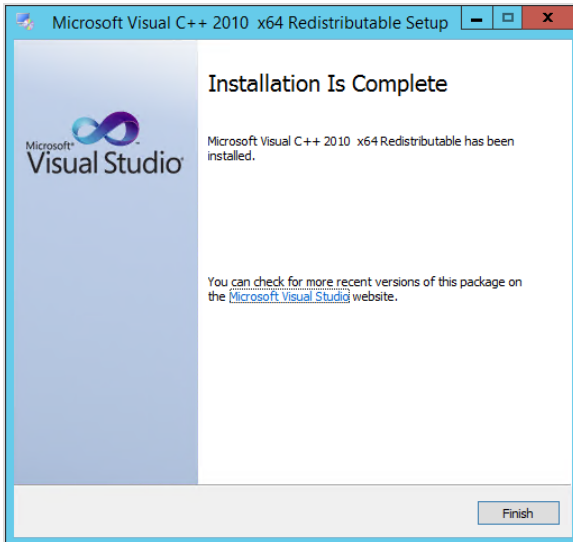
1. Navigate to [EngageSoftware » Engage x.x Pre-Reqs & Tools NO SQL » Windows Pre-Reqs » Microsoft Visual C++ 2008_2010_vcrist](#) . Contents are zipped.



2. Select one of the following according to the deployment's need by double-clicking the filename (ex **2010vccredit_x64**) file to unzip the file.
 - **2008vccredit_x64**
 - **2008vccredit_x86**
 - **2010vccredit_x64**
 - **2010vccredit_x86**
3. Execute the file to get the Visual C++ Setup window.



4. Click the checkbox for *I have read and accept the license terms*, then click *Install* and



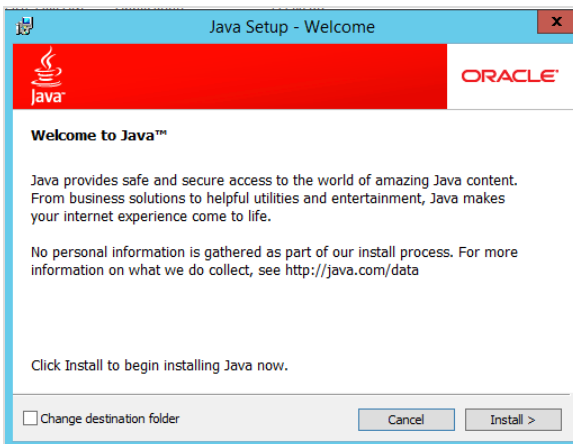
5. Click *Finish* to complete the installation.

5.2.3 Install Sun Java Runtime Environment (JRE)

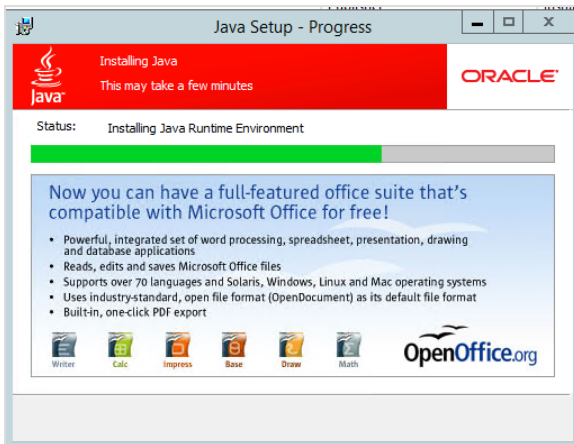
The Sun Java Runtime Environment (JRE) is required for the Windows Server 2012, 2008, 2003 and XP operating systems. The JRE is essential for the Engage JAVA client to run properly on the server.

To install the Java Runtime Environment on the Engage recording server:

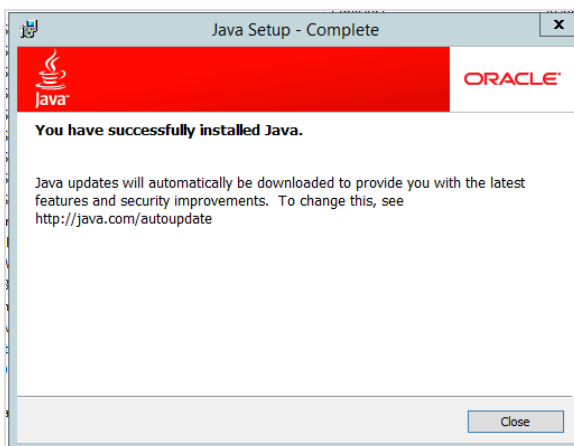
1. Navigate to *EngageSoftware » Engage x.x Pre-Reqs & Tools NO SQL » Windows Pre-Reqs* folder.
2. Double-click on the *jre-6u21-windows-i586-s.exe* file to get the Java Welcome window.



3. Click **Install** to begin installation.



4. When installation is finished, click **Close**.



NOTE: If no Internet access is available, use these steps.

Sometimes the Engage server does not have internet access and the JRE will fail to install. Engage has provided a similar program in the Engage *Pre-Reqs & Tools* folder which can be loaded without internet access; however, TelStrat recommends installing the JRE instead.

To install on an Engage Server that has *no internet access*:

1. Navigate to the [EngageSoftware » Engage x.x Pre-Reqs & Tools NO SQL » Windows Pre-Reqs](#) folder.
2. Double-click on the file [rootsupd for java no access to internet](#).
3. Install the JRE using the previous steps.

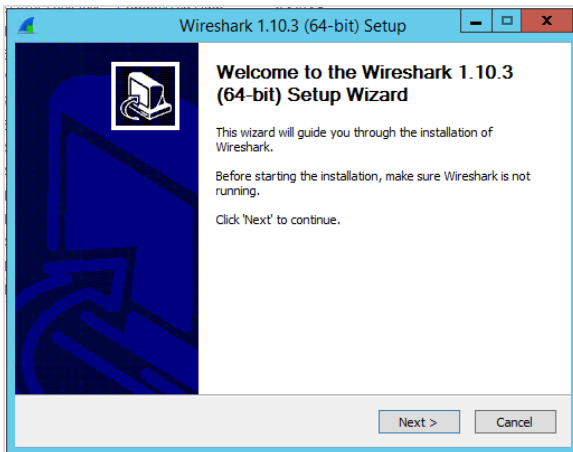
5.2.4 WinPcap: Required for All VoIP Deployments - auto-installed

WinPcap software is automatically installed by Engage Voice Recorder installation software and does not need to be manually installed.

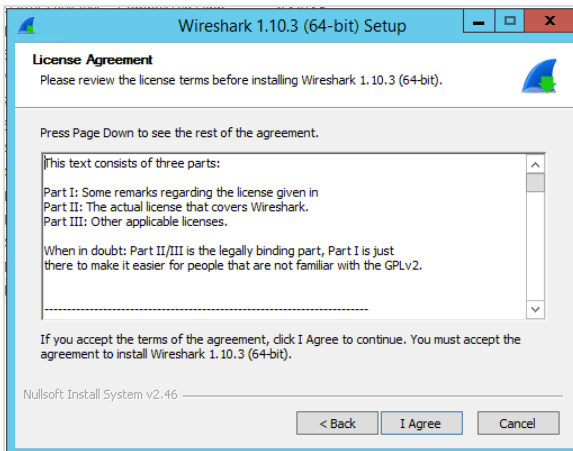
The Engage Recorder requires that the WinPcap tool be installed for any VoIP call recording. WinPcap is the packet capture and filtering engine of many open source and commercial network tools, including protocol analyzers, network monitors, network intrusion detection systems, sniffers, traffic generators and network testers. The tool is a component of the Wireshark tool.

If needed, WinPcap can be installed using these steps:

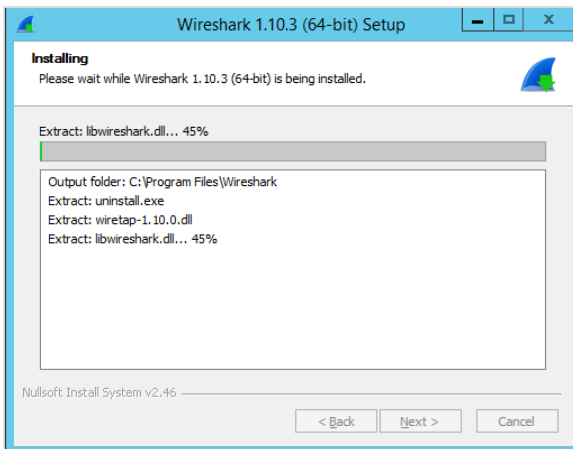
1. Navigate to the [EngageSoftware » Engage x.x Pre-Reqs & Tools NO SQL » Technician Tools Only](#) folder.
2. Double-click either [Wireshark-win32.exe](#) for 32-bit systems and [Wireshark-win64.exe](#) for 64-bit systems.
3. At the Wireshark Setup Wizard window, click [Next](#).



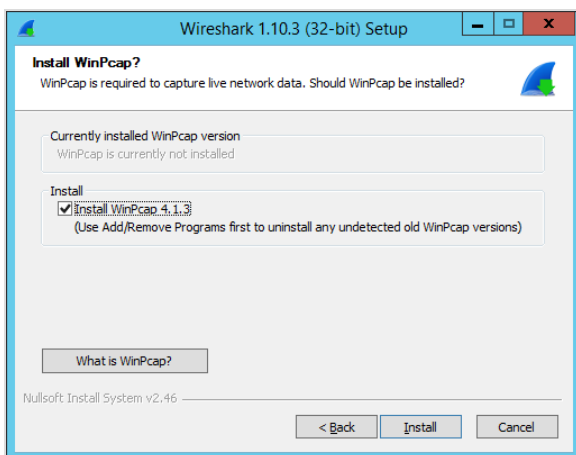
4. Click [I Agree](#) at the **License Agreement** window.



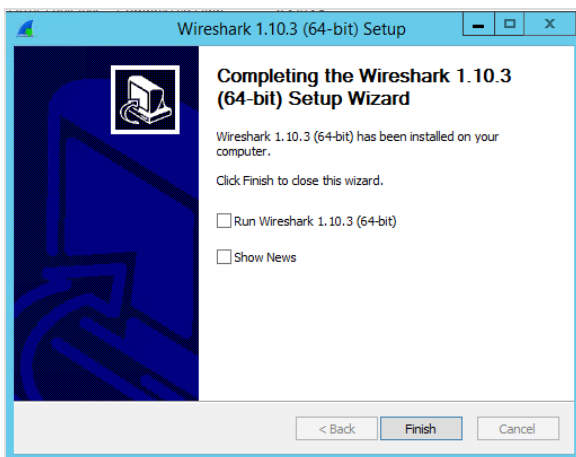
5. Click **Next** to get past *default components*, click **Next** to get past *default additional tasks* and click **Next** at the *default destination* window.
6. Select the **Install WinPcap 4.1.3** checkbox and click **Install** for Wireshark installation.



7. When complete, click **Next**.
8. At the *WinPcap 4.1.3 Setup Wizard*, click **I Agree** the *Licensing Window*. Click **Install**.



9. Click **Finish** when install is complete.



NOTE: Manually remove the Engage Packet Driver if upgrading Engage to release 4.2 or better.

5.3 Installing Engage Server Software

WARNING: If any versions of the Engage Record software have previously been installed on this server, those versions must be uninstalled BEFORE installing Engage Record 5.2.

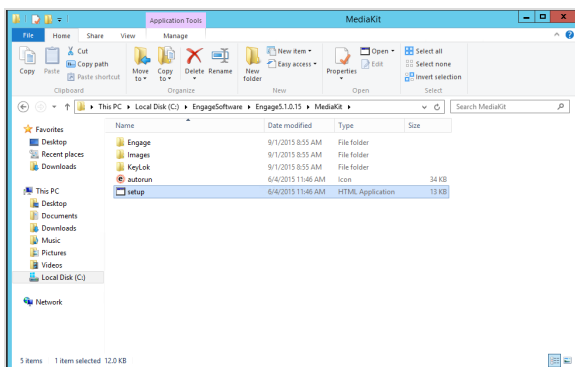
There are two versions of Engage Server software available for downloading. Be sure to select the proper version for the customer's specific deployment.

From the Engage product software that was downloaded to the server folder: [C:\EngageSoftware\EngageSuite 5.x.x](#) there will be one of two zipped versions of software to choose from depending on the deployment:

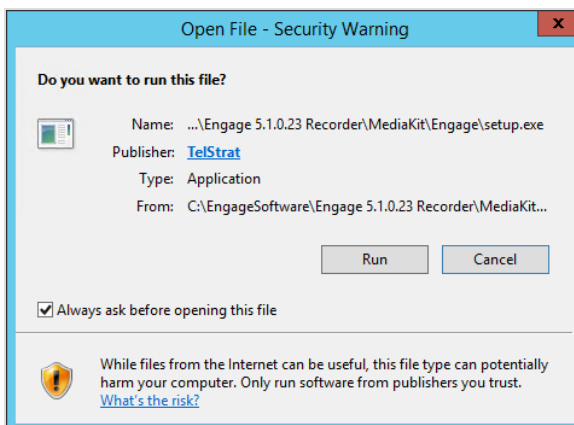
- 64-bit Cisco deployments, use: [\Engage5.x.x\Engage 5.x.x.xx Recorder-Cisco\(x64\).zip\MediaKit \(x64\)\Engage](#).
- All other deployments, use: [\Engage5.x.x\Engage 5.x.x.xx Recorder.zip\MediaKit\Engage](#).

Install the Engage Recorder Software

1. Unzip the folder of Engage software by double-clicking on the folder icon. Select *Open with Windows Explorer* and click **OK**. Click on the *MediaKit* folder to open it.



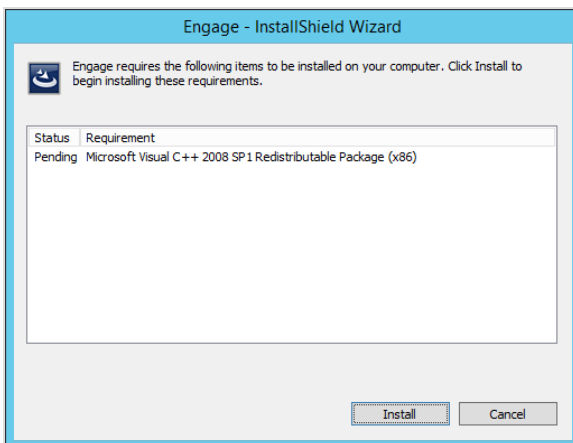
2. In the folder contents list, double-click the [Setup.exe](#) file to run the Engage installer.
3. A *Security Warning* window may appear. Click on **Run**.



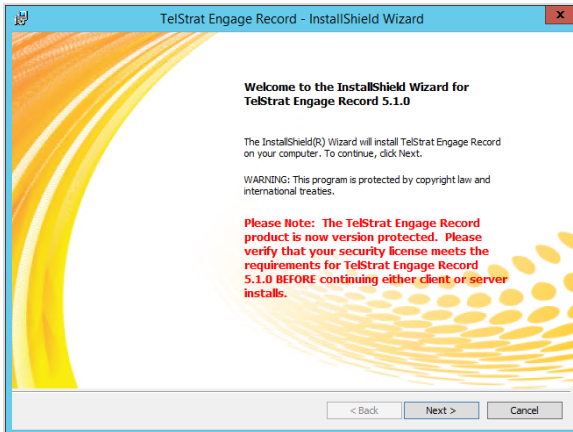
4. At the *Welcome to the InstallShield Wizard for Engage 5.2.0* window, under *Install*, click the **Engage Server, Client and tools** link.



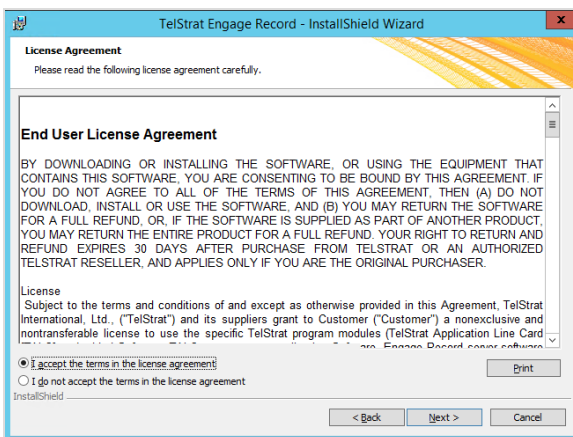
5. The InstallShield Wizard may install Microsoft Visual C++ 2008 SP1 Redistributable Package if it is not already installed. Click **Install**.



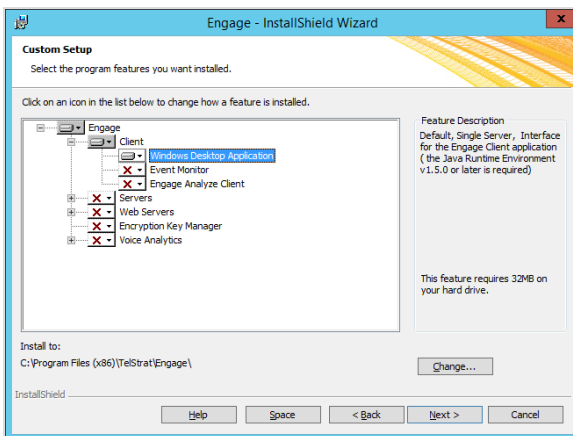
6. The TelStrat Engage Record - InstallShield Wizard opens. Click **Next**.



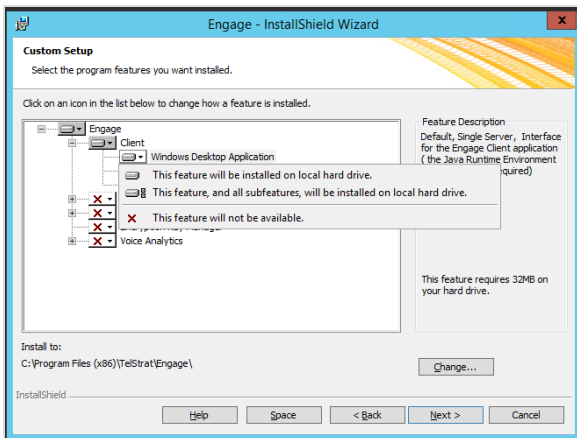
7. At the *License Agreement* window, select *I accept the terms of the Licensing Agreement* and click **Next**.



8. In the *Custom Setup* window, expand *Client* and click on the *Windows Desktop Application* (for Engage JAVA Client) dropdown menu box.

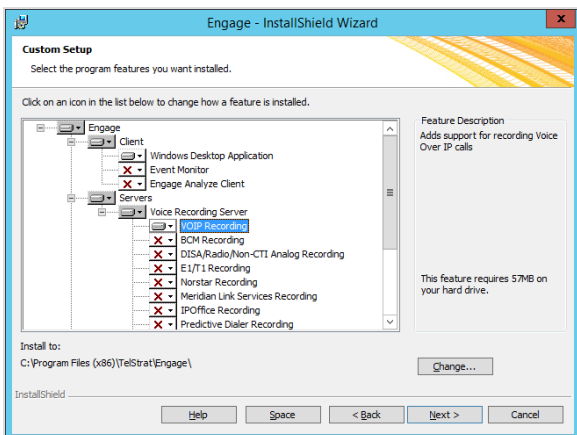


- Click on *This feature will be installed on local hard drive* to install the Engage JAVA client.

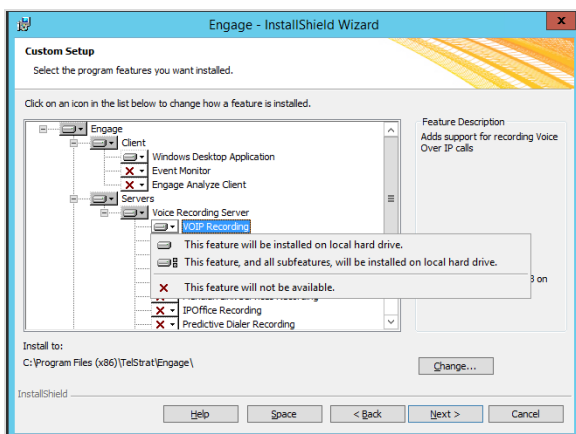


NOTE: The JAVA client is used for the first initial setup and server administration only. It is not supported as an end user client and should not be provided for users to logon to Engage with.

- Expand *Servers » Voice Recording Server* and click on the *VOIP Recording* dropdown menu box.

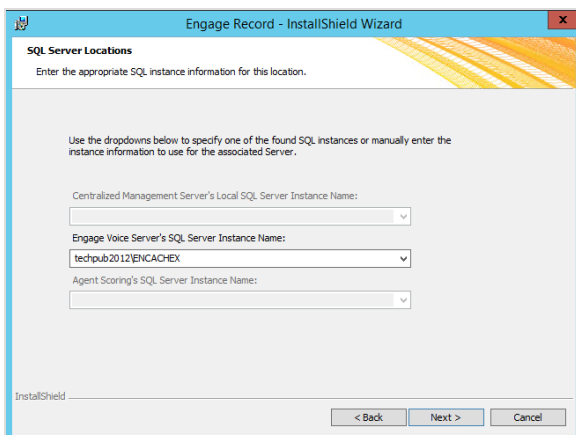


- Click on *This feature will be installed on local hard drive*. Click *Next* to install the Engage related applications. Click *Next*.

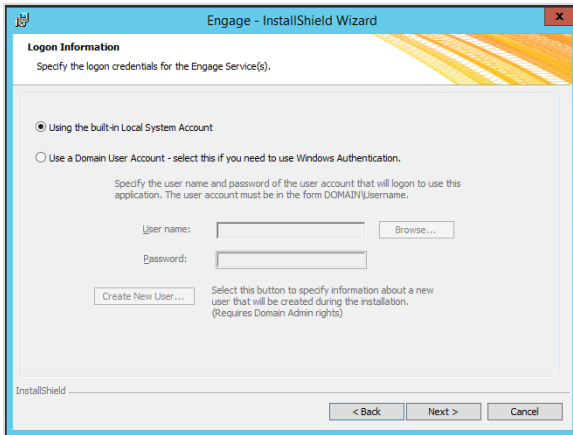


NOTE: Other recording methods are available and may be selected if the deployment is using a method other than VoIP recording.

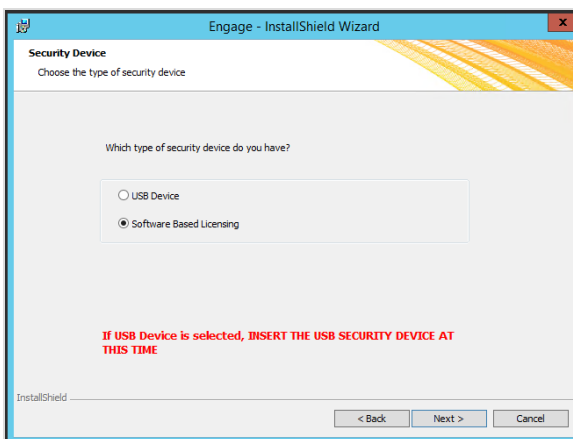
- At the **SQL Server Locations** window, enter the location of the SQL Cache Database (*Server-InstanceName*) (ex. *techpub2012\ENCACHEX*) in the *Engage Voice Server's SQL Server Instance Name* box. Click *Next*.



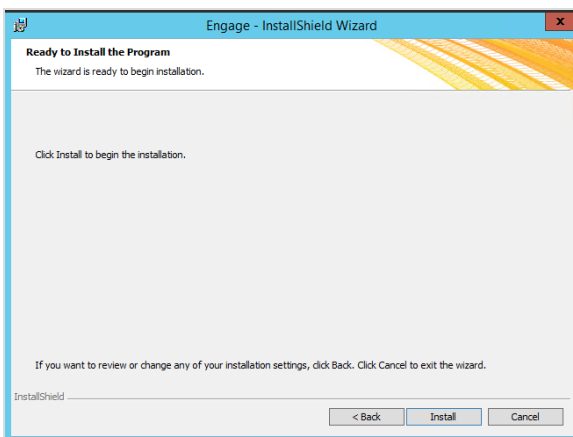
- At the **Login Information** window, select *Using the built-in Local System Account*. If screen recording or speech analytics are being deployed, then select *Use a Domain User Account* and enter the Engage domain account with the domain. Select *Next*.



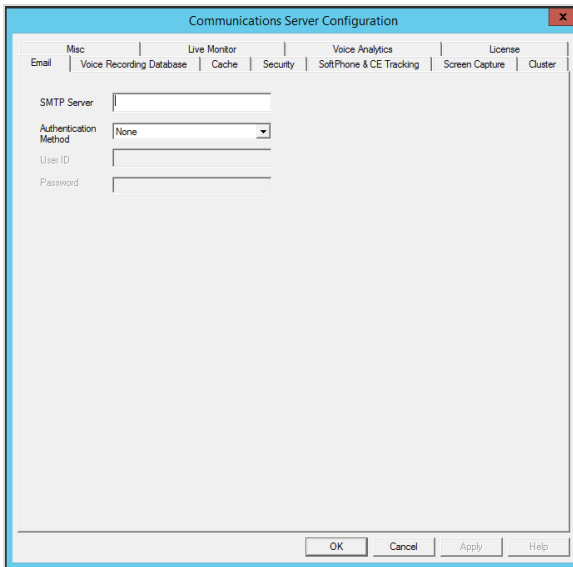
14. At the **Security Device** window, select *Software Based Licensing* then click *Next*.



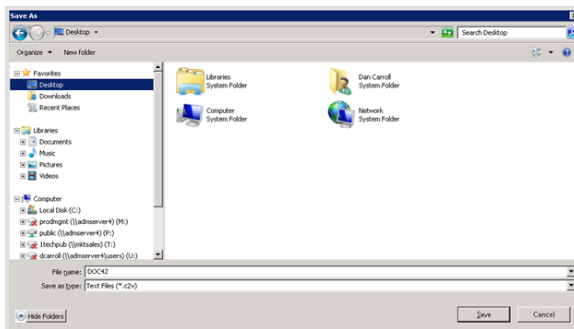
15. At the **Ready to Install the Program** window, click *Install* to begin installation.



16. During the installation, the **Communications Server Configuration** (CommSrv) screen will appear. **These settings can be applied now** as defined in the SERVER CONFIGURATION (COMMSRV) SETUP topic. Configuring them now removes one restart of the TelStrat Voice Recording Service later during the installation.



17. BEFORE CLOSING the COMMSRV tool, generate the security fingerprint file before closing the Communication Server Configuration tool, as follows:
- On the Communications Server System Configuration tool, select the **License** tab.
 - Click the **Use Soft License** button and then click on **Generate Fingerprint** button.
 - Save the *filename.c2v* file (customer to vendor) on the desktop or some other location such as the Documents folder.



- d. Email the saved *customer-original.c2v* file to this email address, REGKEYS@TELSTRAT.COM , and wait for a reply.

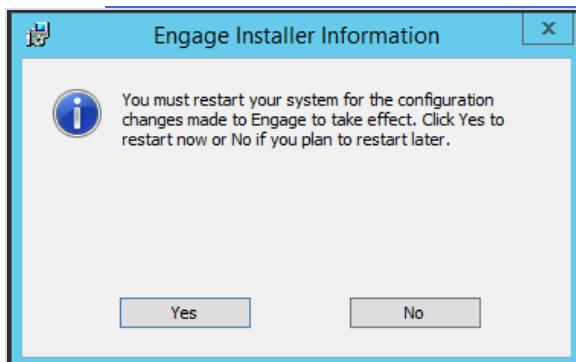
WARNING:DO NOT generate another fingerprint during this time. It will not match the fingerprint of the file sent to TelStrat and confuse the process.

- e. When received, the reply email from TelStrat will contain a licensing file with a *filename.v2c* extension. This file could be contained in a .zip folder and may need extraction. Save this file in an easily accessible location on the server, such as *Documents*. The v2c file can be applied now or at a later date. The Engage system will use a short three (3) day temporary license to operate on until the v2c file is applied. Refer to section RECEIVE AND APPLY THE NEW V2C FILE to apply the v2c license, once it is available.

18. Click **OK** on the screen to continue the installation.

19. Click **Finish** when the installation process is complete.

NOTE: Detailed step-by-step instructions for Server Configuration are defined in the Post-Installation configuration section of this document at SERVER CONFIGURATION (COMMSRV) SETUP.



Warning: Do not reboot the server. A reboot of the server is required, but will be done later.

5.4 Install Engage SOA Services

Engage SOA Services must be present on the Engage recording server to allow the Web Client application to access the Engage recording server.

The Engage Web Client uses the following services to communicate when it communicates with the Engage Server:

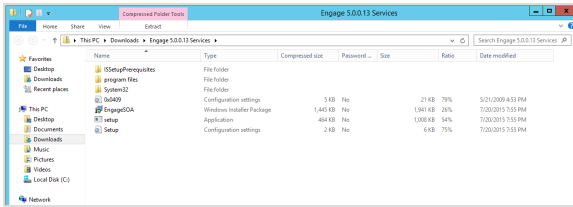
- TelStrat Engage Alarm Service.
- TelStrat Engage Annotation Service.
- TelStrat Engage Configuration Service.
- TelStrat Engage Download Service.
- TelStrat Engage Mass Archive Service.
- TelStrat Engage Notification Service.
- TelStrat Engage VoIP Configuration Service.

Install the Engage SOA Services

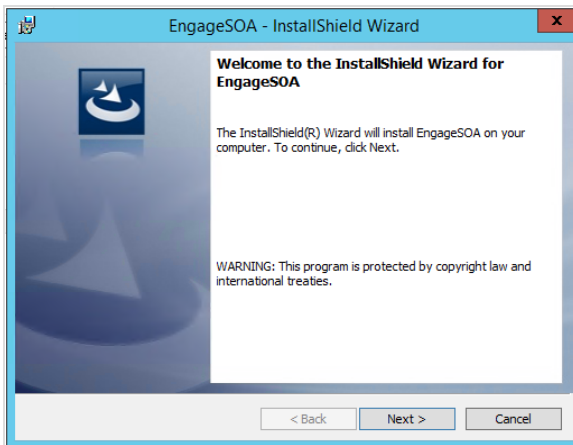
From the Engage product software that was downloaded to the server folder: **C:\EngageSoftware\EngageSuite 5.x.x** there will be a folder:

\Engage5.x.x\Engage 5.x.x.xx Services

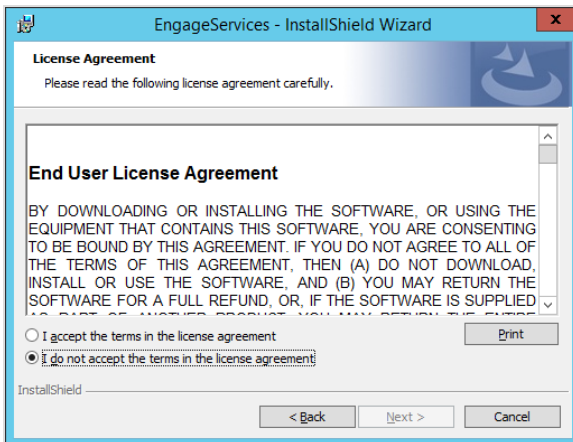
1. Unzip the folder of Engage software by double-clicking on the folder's icon. A confirmation window will appear. Select *Open with Windows Explorer* and click **OK**. A new folder window will open displaying a folder named Engage 5.x.x.xx Services with some contents.
1. From the unzipped folder, click and launch the **Setup.exe** file to run the Engage Services installer to execute the **Engage Services** setup file.



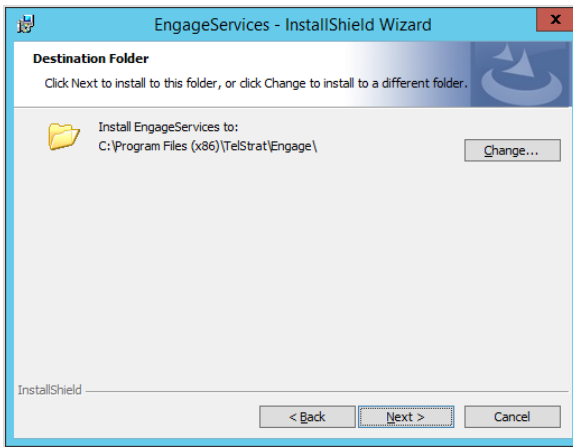
2. The installer will appear. Click **Next**.



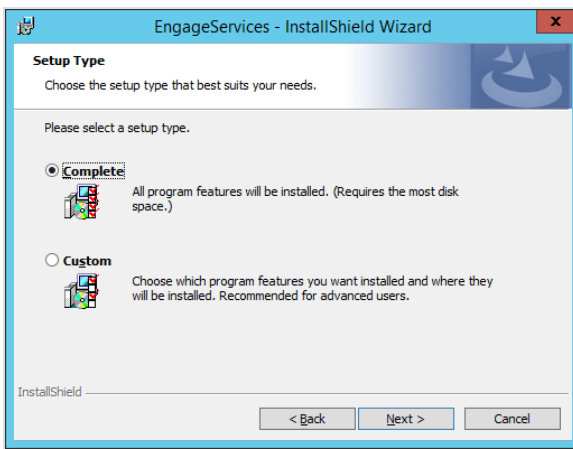
3. Select **I accept the terms in the License Agreement**. Click **Next**.



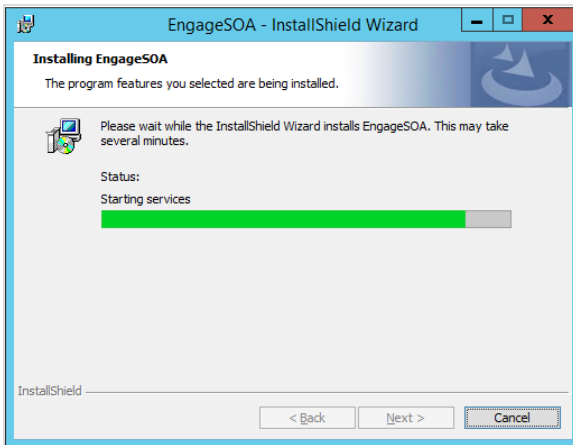
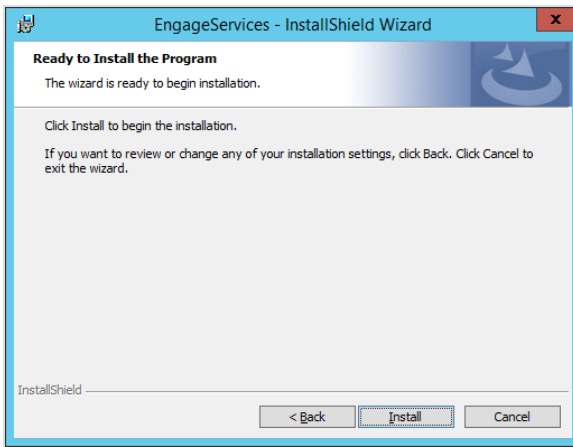
4. Install the *Engage Services* to the default folder. Click **Next**.



5. Select **Complete** for the *Setup Type*. Click **Next**.



6. Click **Install** and **Finish** when the installation is complete. It may take a few minutes to install and start the Engage Services.



5.5 Restart the Recording Server

Now that prerequisite software and tools, Engage Recording server software, Engage SOA Services, and web client software are installed, **restart the Engage Recording server now** to complete the installation of the Engage server software.

How to Restart

After initial installation is completed, rarely is a restart required. However, occasionally, the need arises to restart the machine to set software such as updating the Engage TAPI software version to match that of the CUCM version, changing any CTI Options and changing CTI Server names all require a restart for the change to take effect.

WARNING: Only use a restart when it is clearly understood what is being affected.

If a restart of the Engage Voice Recording Service is needed, do the following:

1. Open the [Services](#) tool on the Engage Server.
2. Scroll down to the [TelStrat Engage Voice Recording Server](#) service.
3. *Right-click* on the [TelStrat Engage Voice Recording Server](#) service and select [Stop](#).
4. Wait 10 seconds, and then right-click on [Start](#) to start the server.

When not to use Restart

There is no need to restart the system when adding, modifying, or deleting port mapping (user and agent data) via the Web Client or with individual port mapping.

6 Post-Installation Configurations

With all of the various software components successfully installed, post-installation configurations and tasks must be accomplished to finish the Engage voice recorder installation. Some of these tasks are:

- Configuring the SQL database memory limits and file systems.
- Applying licenses to systems.
- Setting up and configuring the Web Client.
- Configuring Engage accounts.

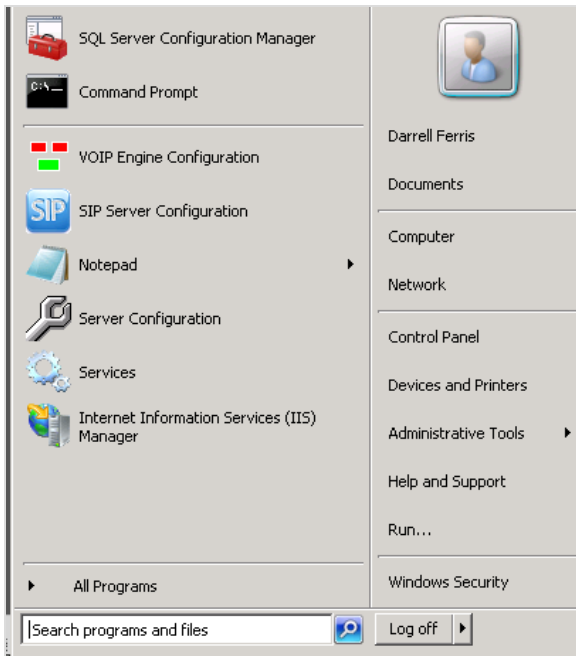
6.1 Server Configuration (CommSrv) Setup

The Communication Server (CommSrv) Configuration program on the Engage Record server must be setup as part of the Engage Record server installation. Configurations are set using tabs in the program. After making all of the changes identified here, restart the *TelStrat Engage Voice Recording Server service*.

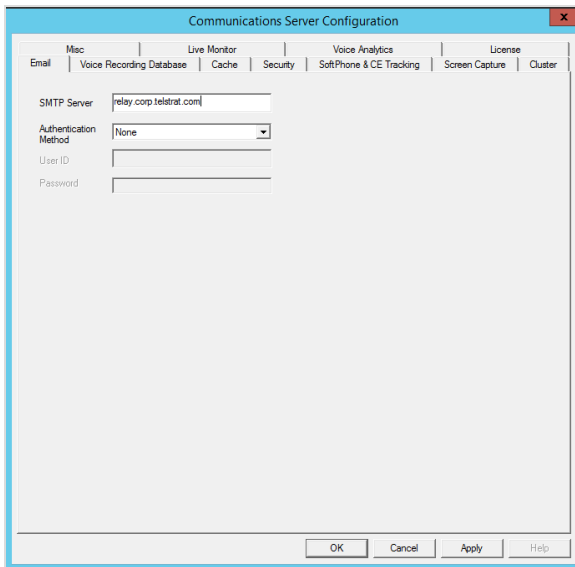
Most of these settings are considered **one time setup and as such, do not dynamically update the recording server**. Therefore, a restart of the TelStrat Voice Recording Service will be required after making all of these configurations on the Communications Server Configuration tool.

Perform these steps to complete the *one-time* server configurations needed on each of the following tabs:

1. Logon to the Engage Voice Recorder server using an administrator's user ID and password.
2. Launch the **Communication Server Configuration (CommSrv)** program by clicking on the **Server Configuration** icon or by clicking on the *Start » Server Configuration* menu command.

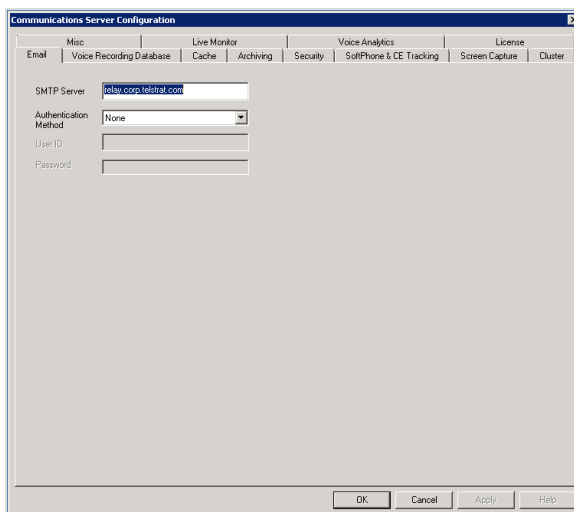


3. The *Communications Server Configuration* window (also known as *CommSrv*) and its tabs will appear.



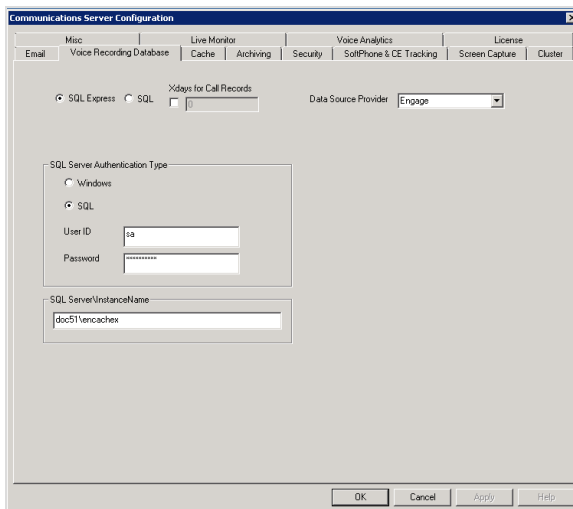
Make the following changes to the CommSrv program tabs:

1. **Email tab (Required):** System alerts are a **Critical Function**. This tab is used to program Engage to send alert messages to users using their email account. Enter the following, as required:
 - a. **SMTP Server** field: Enter the SMTP server's name that control's the customer's email. (ex. [corp.-telstrat.com](http://corp.telstrat.com)). The **SMTP Server** field shown **MUST** be filled out in order for email alerts to work. This can be set or modified at any time and no service restart is required.
 - b. **Authentication Method** field: Select the method of authentication from the following and enter the user ID and password:
 - **LOGIN PLAIN:** Used for local login.
 - **AUTH LOGIN:** Used for network authentication.
 - **CRAM MD5:** Used to encrypt login requests only. Largely replaced by other secure login methods that encrypt the entire email.
 - **None:** No authentication required.
 - c. Click **Apply** and go to the next tab.



2. **Voice Recording Database tab (Required):** Defines the location and authentication for the recording database.

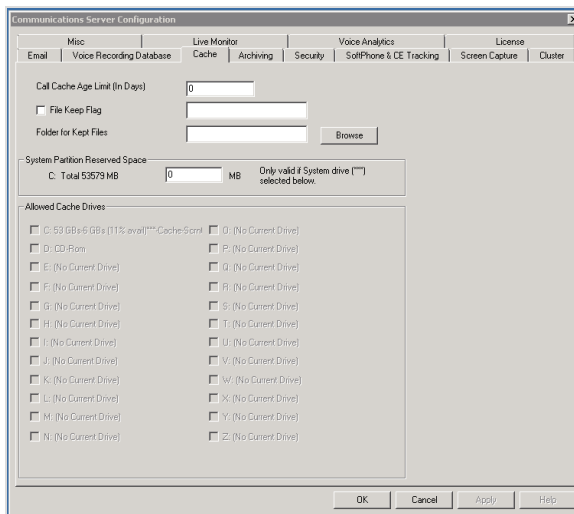
- a. Check the **SQL Server\InstanceName**. If this is not already correct, reconfigure it now (ex. *doc51\en-chachex*).
- b. Set **SQL Server Authentication Type** by selecting either the *Windows* or *SQL* button. Enter the SQL authentication User ID and password, if using **SQL** authentication.
- c. Set **SQL database type** by selecting the button for *SQL Express* or *SQL*. Engage uses this information to limit the call cache database to either 2M records (SQL Express) or 7M records (SQL). Note that mass archive supports an unlimited amount of call records as long as sufficient SQL storage is available.
- d. **Xdays for Call Records**: If the customer has a requirement to delete calls after so many months or days, you must configure that number of days in this location and the same number of days in the *Cache configuration tab*.
- e. **Data Source Provider**: Set to the default *Engage* value unless instructed otherwise. Click *Apply* and go to the next tab.



3. **Cache tab (Required)**: Sets the location and authentication for recorded .WAV file storage.
 - **Call Cache Age Limit (in Days)**: If the customer has a requirement to delete calls after so many months or days, you must configure that number of days in this location and the same number of

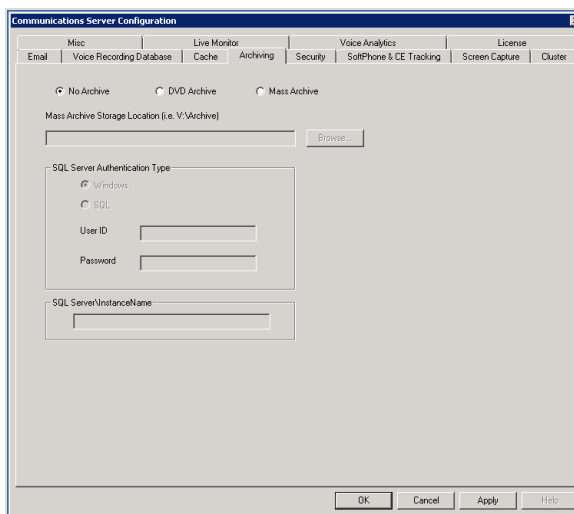
days in the *Voice Recording Database* tab.

- **File Keep Flag:** If the customer needs to keep specific audio recordings in the call cache and prevent them from being purged, select this check box and enter a word to use such as “keep” in the associated text box. You must also select a folder that will be used to store these recordings. Users can enter the keep phrase in Remark1 or Remark2 and Engage will keep the recording rather than purge it when space is exhausted.
- **System Partition Reserved Space:** This should not be used as it only applies if the C:\ drive is used to store calls which is not recommended.
- **Allowed Cache Drives:** For new installations, select one partition that is dedicated to audio call storage. When referencing this tab on an existing deployment, Engage automatically detects the presence of any drives that contain a \RecordingCache folder and will select these. Do not select C:\. Multiple drives should not be selected except for legacy deployments where server storage was limited due to available technology at the time.
- Click **Apply** and go to the next tab.



4. **Archiving** tab: Sets the type and location for archives of recorded calls.

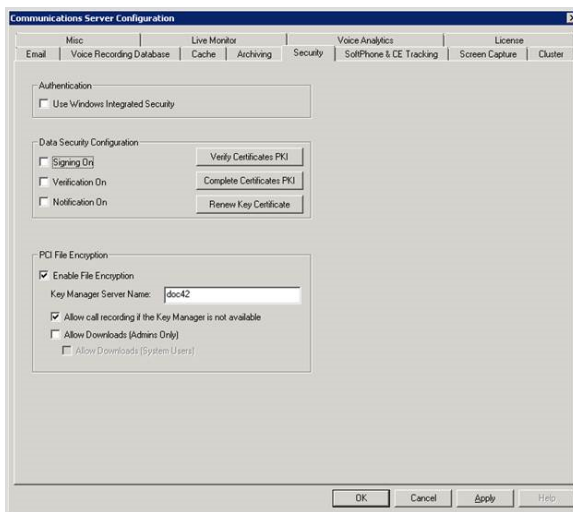
- Select the type of archiving.
 - **No Archive** button is *selected now for ALL new deployments*. Prevents use of Legacy mass archiving.
 - **DVD Archive** button: NOT USED for new deployments.
 - **Mass Archive** button: Refers to first generation Mass Archive, which has a limited feature set and is not used for new deployments.
- **Mass Archive Storage Location**: Only used with the legacy first generation mass archive
- **SQL Credentials**: Only used with the legacy first generation mass archive
- Click **Apply** and go to the next tab.



5. Security tab:

- **Authentication**: **Do not select Use Windows Integrated Security**. This only applies to the internal service account used by the web server, live monitor, and a couple of Administrator accounts used to access the JAVA client.
- **PCI File Encryption**: Refer to the Encryption Configuration Guide for setting up file encryption

- **Data Security Configuration:** This feature supports signing audio recordings, verifying the integrity of a signed audio recording, and notifying the user during playback of verification errors. To use the Data Security Configuration option:
 - Select **Signing On**, and then select **Verify Certificates PKI** and verify the pop up indicates verification is **OK**
 - Select **Verification On**, and then select **Complete Certificates PKI**. Verify the pop up indicates completion **OK**.
 - Select **Notification On**, and then **Renew Key Certificate**. Confirm that you wish to renew the key certificate and then verify the renewal completed successfully.
 - Click **Apply** and go to the next tab.

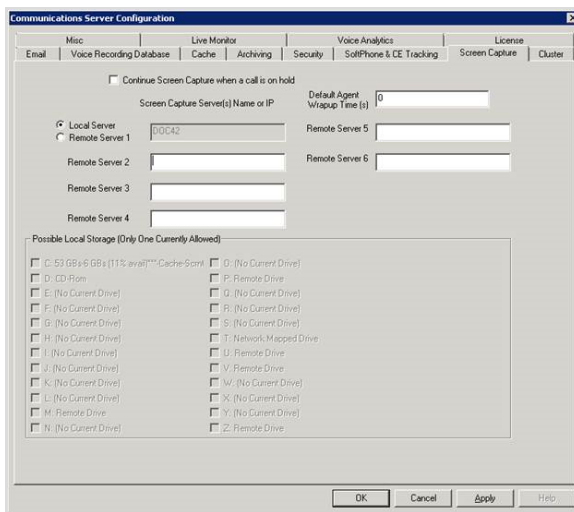


6. **Screen Capture tab:** This tab is only used when optional screen capture licenses are purchased.

- **Continue Screen Capture when a call is on hold:** Enable this if you would like to continue recording the workstation when a call is placed on hold.
- **Default Agent Wrap up Time(s):** Enter a time in seconds for typical wrap up time. Wrap up time is how long the recording server should continue screen recording after an audio call completes. Note that if a new call is presented to the agent, the existing screen capture session will end and the new

call will be recorded with screen capture. The wrap up time can also be set as part of the recording schedule. Wrap up time is no longer managed on an individual agent basis.

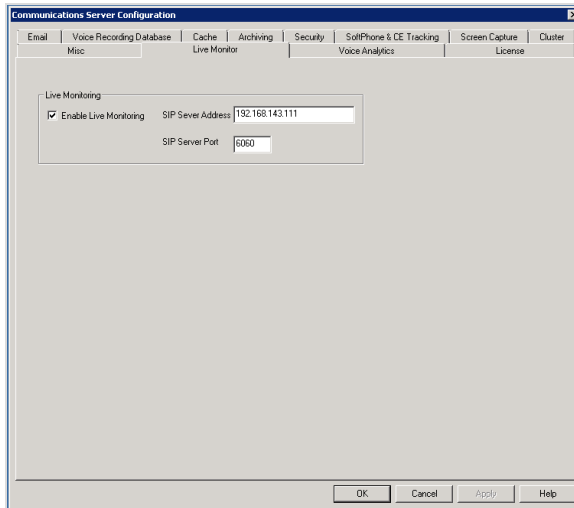
- **Local Server:** Select **Local Server** if Proxy Gateway software will be installed on the Voice Recording server. This is only an option for sites up to 200 recording channels.
- **Remote Server 1-6:** Enter the *DNS name* or *Static IP address* of up to 6 screen capture gateway servers.
- Click **Apply** and go to the next tab.



7. Live Monitor tab:

- **Enable Live Monitoring** checkbox: This should be enabled at initial installation as enabling it after the installation requires a maintenance window to restart the Voice Recording Service.
- **SIP Server Address:** Enter the *DNS name or static IP address* of the voice recording server.
- **SIP Server Port:** Use the default value of **6060**.

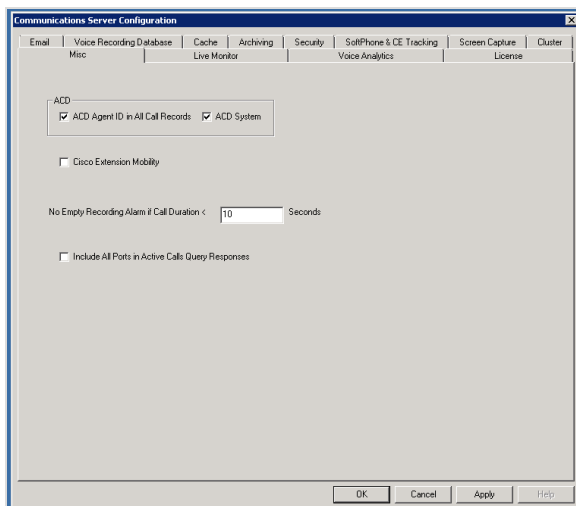
- Click **Apply** and go to the next tab.



8. Misc tab:

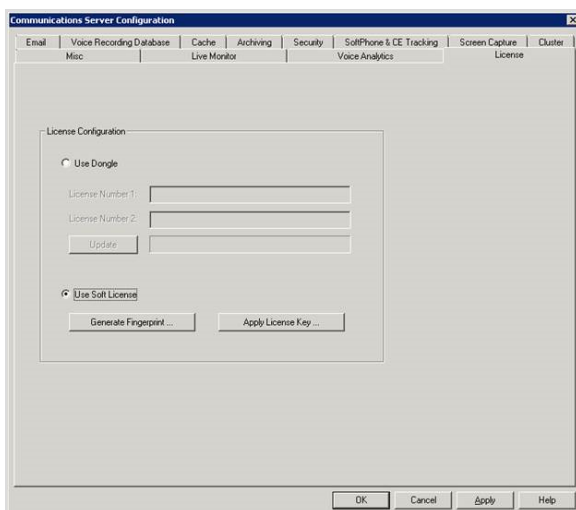
- **ACD Agent ID in All Call Records:** Enable this setting for any contact center (ACD) deployments. This setting will help add the Agent ID to any calls placed by the agent while they are logged into the Contact Center. When Engage is deployed with some systems, the agent ID will not be placed into the call record for outbound calls for example unless this is enabled.
- **ACD System:** Enable this setting for any contact center (ACD) deployments.
- **Cisco Extension Mobility:** Enable this setting only for a Cisco UCM TAPI deployment that uses the Cisco Extension Mobility Feature. This is required for Engage to interact with the mobility server to obtain mobility user ID for new calls.
- **No Empty Recording Alarm if Call Duration < 3 seconds:** Change this value to **10 seconds**. This will prevent Engage from sending unnecessary alerts for calls that were so short recording could not be established before the call disconnected.
- **Include All Ports in Active Calls Query Response:** Leave disabled by default. Enable this to see all ports in the Active Calls Screen. This is introduced with the screen-only recording feature, and it must be set for screen-only recording. This can be set for any deployment, however the active calls screen loading will be slowed.

- Click **Apply** and go to the next tab.



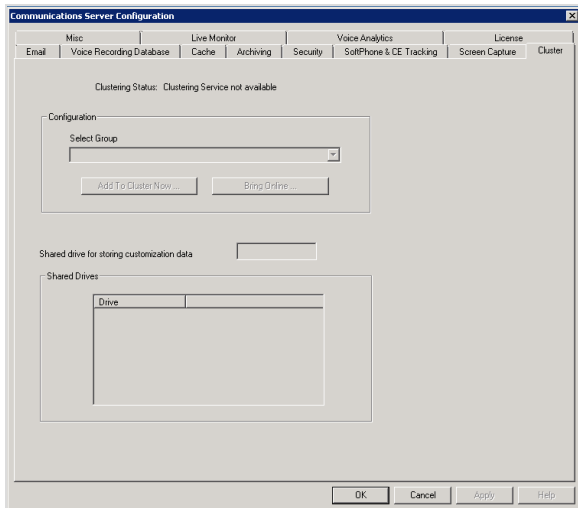
9. **License tab (Required):** Enable hard dongle or soft dongle licensing management:

- **Use Soft License:** This is the default setting for all new installations. Refer to the documentation on applying the software license for additional details.
- **Use Dongle:** This is for legacy customer sites or highly secure sites that do not allow any network access to the Engage Record server.
- Click **Apply** and go to the next tab.



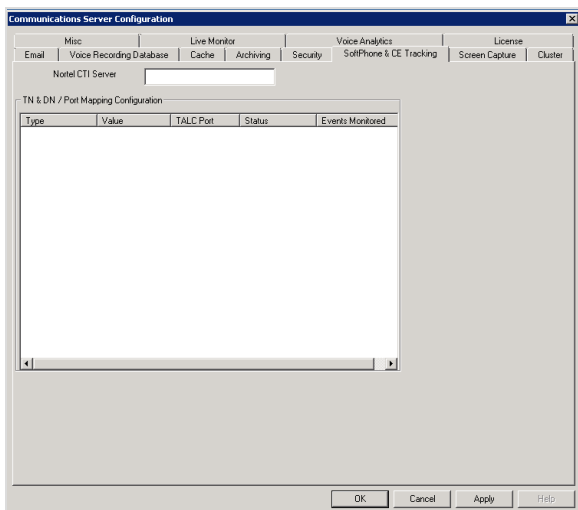
10. **Cluster tab:**

- This tab will only be setup as part of an Engage Record clustered server installation.



11. **SoftPhone & CE Tracking tab:**

- This tab is only used with some CS 1000 VoIP deployments. The CS 1000 configuration will configure this tab if required.



12. Click **OK** to close the **Communications Server Configuration** tool.

13. **Restart** the *TelStrat Engage Voice Recorder Service*:
 - a. Open the *Services* tool on the Engage Voice Recording Server.
 - b. Scroll down to the *TelStrat Engage Voice Recorder Service*.
 - c. Right-click on TelStrat Voice Recording Service and select *Stop*.
 - d. Wait 10 seconds, and right-click on *Start* to start the server.

6.2 Change the FromEmailAddress Registry Value

Each voice recorder server's Registry contains a value entry (*EmailFromAddress*) where a customer can provide a FROM email address in the header of emails sent TO assigned email addresses designated to receive email regarding events from the Engage Voice Recorder. This FROM address must be a valid email address that can flow through the company's SMTP email receiving and delivery processes.

Change the Entry in the Engage Voice Recorder

This Registry entry must be changed to reflect the customer's specific company address in the FROM part of the email header. If not changed, then the *engage@telstrat.com* default address will be inserted as the FROM address in server produced emails.

Change the Entry in Multiple Engage Voice Recorders

If the customer has multiple recorders in the deployment, EACH recorder's Registry entry needs to be changed and provided the same address. A unique email address, per server, is not needed since the text in the body of the event email message will note the server name creating the event.

An example of a critical server produced message is:

From: engageABB@corpname.com [mailto:engageABB@corpname.com (address retrieved from Registry entry)

Sent: Monday, August 10, 2015 10:37 PM

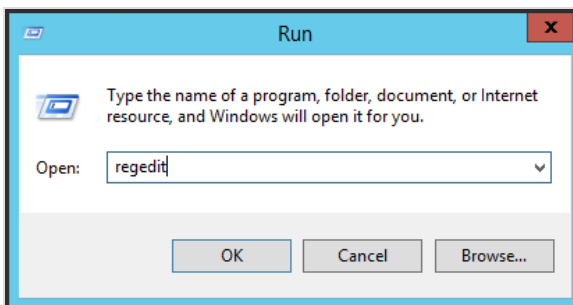
To: Tom Clark (address provided by Web Client)

Subject: TelStrat Critical Email Notification

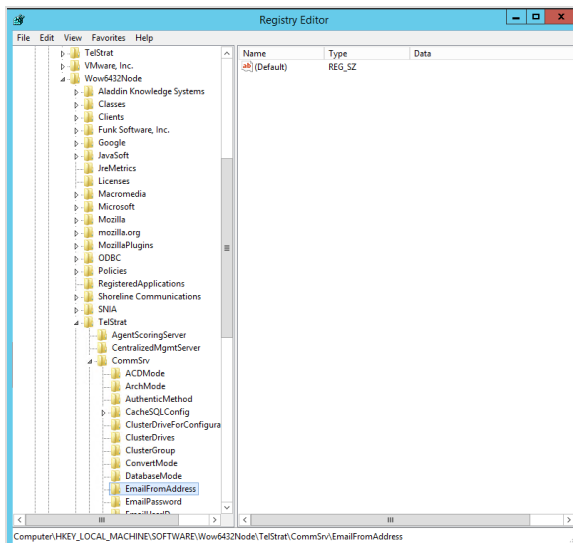
TelStrat Critical Email Notification received from Machine: TSEN-JST-01 EventID: COMM0049 at 8/10/2015 23:37:8. Description: Unable to connect to Gateway Server - TSEN-JST-01 - (affected server name is TSEN-JST-01-)

To make this registry change:

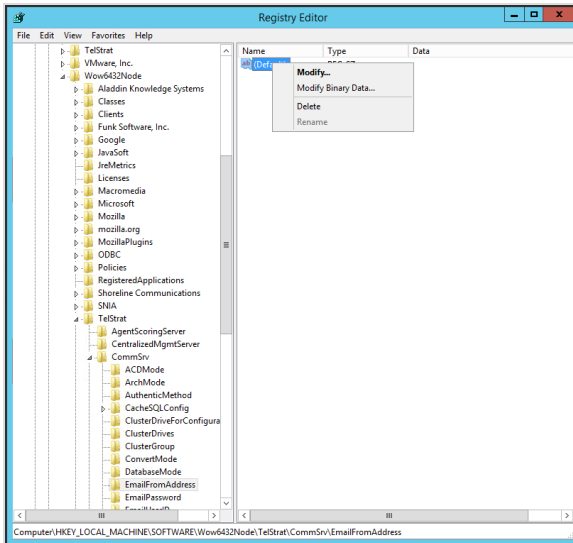
1. From the Start menu, Open a Command **Run** box and enter **Regedit** and click **OK** to launch the **Registry Editor**. Be very careful in this area of the server. Make no changes other than this one value change.



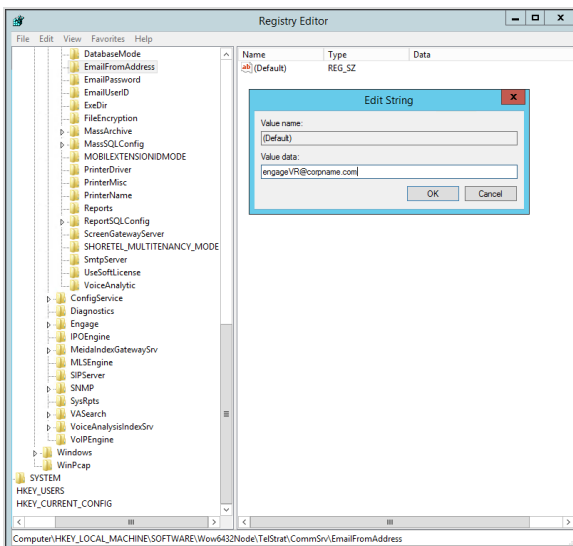
2. When the **Registry Editor** window appears, open the various folders to get to the following location:
 - **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TelStrat\CommSrv\EmailFromAddress**

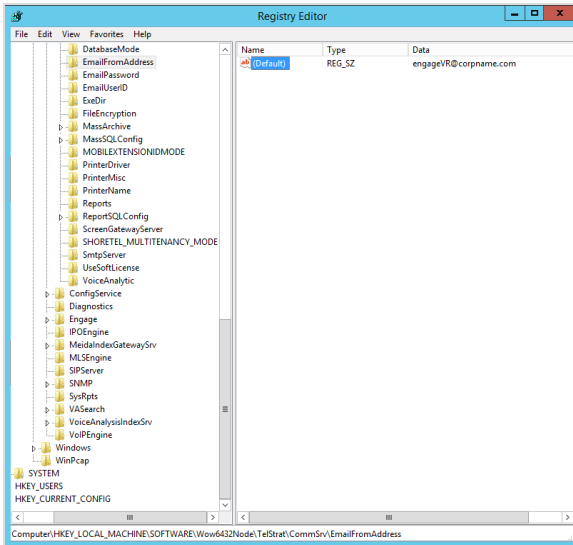


3. Click on the **(Default)** entry and right-click to get the pop-up menu and click on **Modify...**



- In the **Value Data:** field, enter a VALUE in form of the company provided email address (ex. engageVR@corpname.com) and click **OK** to make the change.





5. Close the **Registry Editor**.

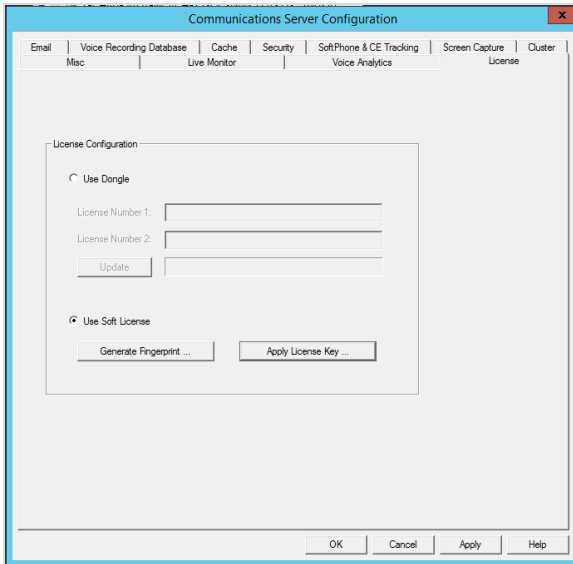
6.3 Apply New Soft License V2C File

For a new deployment and product order, the steps to obtain and apply soft licenses are:

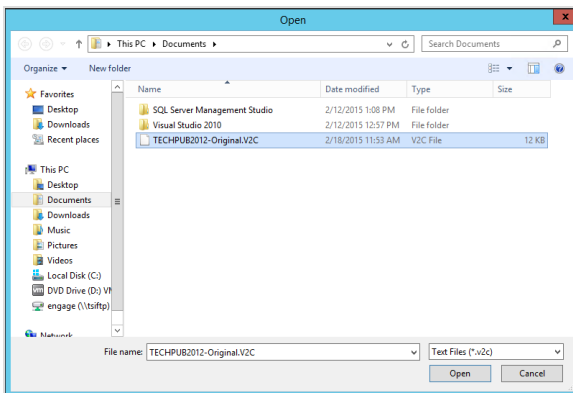
- Create an *Original* customer to vendor file (*filename-original.c2v*) (a fingerprint) and send it to TelStrat.
- TelStrat will return a vendor to customer file (*filename.v2c*) to the customer.
- The customer must create a *final customer to vendor* (*filename.final.c2v*) file and send it back to TelStrat.

WARNING: DO NOT generate another fingerprint during this time. It will not match the fingerprint of the file sent to TelStrat and confuse the process.

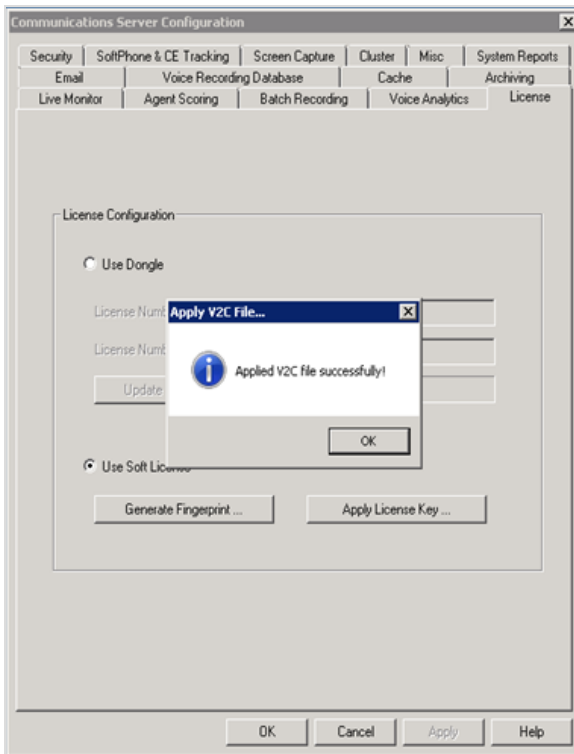
1. When received, the reply email from TelStrat will contain a licensing file with a *filename.v2c* extension. This file could be contained in a .zip folder and may need extraction. Save this file in an easily accessible location on the server, such as *Documents*.



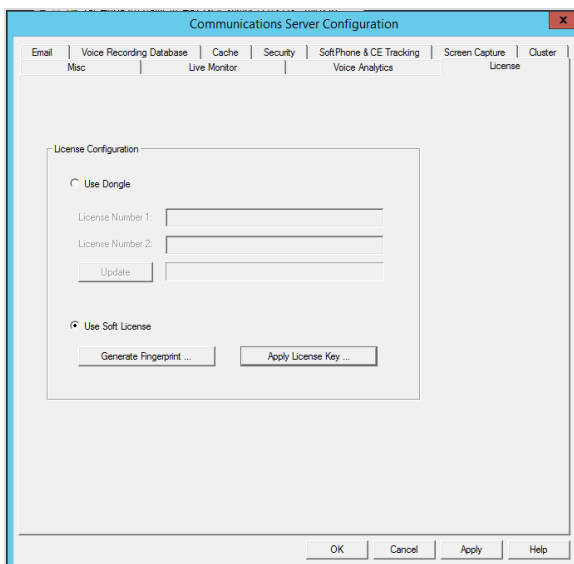
2. Return to the *Server Configuration* window and the *License* tab and click the *Apply License Key* button.



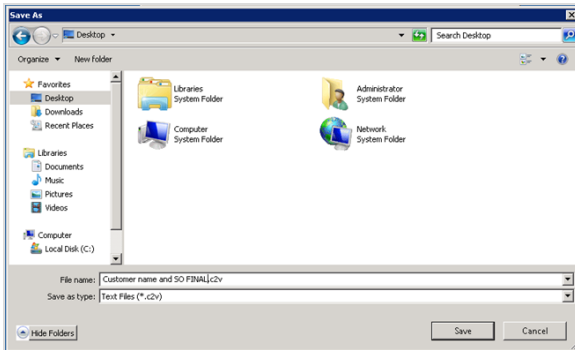
3. The *Open* window will display. Navigate to the location of the saved .v2c file just received from TelStrat, select the file and press the *Open* button. The *Apply V2C File* window should appear.



4. *Applied V2C file successfully!* confirmation window will display. Click **OK**.



5. Click the **Generate Fingerprint** button to generate a *filename-final.c2v* file to email back to TelStrat



6. The **Save As** window will display. Name the file using the customer's name followed by "- Final.c2v" (Example: *Jane's Bakery-Final.c2v*). Navigate to a location that is easily accessible and that will allow for emailing to TelStrat. Click **Save**.
7. Email this *filename-Final.c2v* file to this email address: REGKEYS@TELSTRAT.COM.

NOTE: TelStrat will keep this filename-Final.c2v on file. It will be used to generate any future license key updates such as seat counts and / or maintenance renewal expiration dates.

6.4 Configure the SQL Server

Now that all required software has been installed on the server platform, it is time to set the configurations of the various software components to that Engage can begin recording calls and call data.

Two SQL configurations require attention and are needed.

The first is for memory limits. The memory of the Engage SQL Instance **must** be limited if any other Engage components are on the same SQL server. This will ensure Engage has access to available memory.

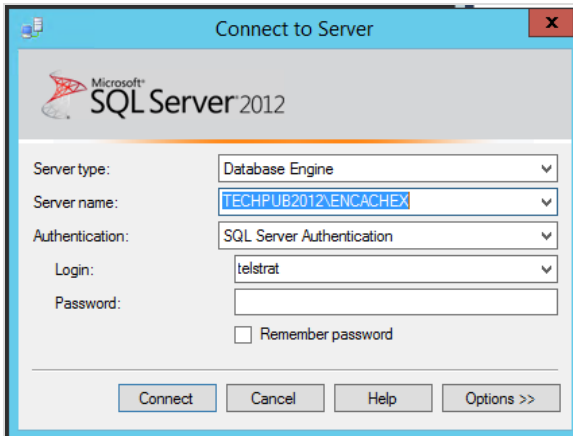
The second is configuring the four databases that Engage will use to record calls and call data.

6.4.1 Limit SQL Memory

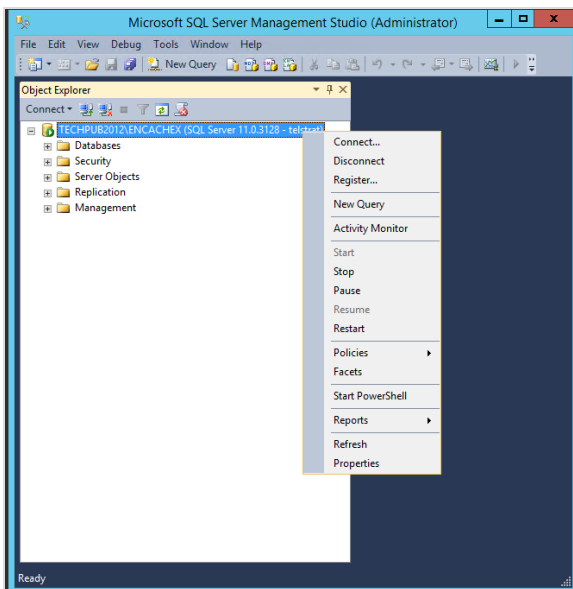
If any other Engage component software is running on the SQL server, the memory needs to be limited to make sure Engage has access to enough memory to operate correctly.

To set the SQL memory limits:

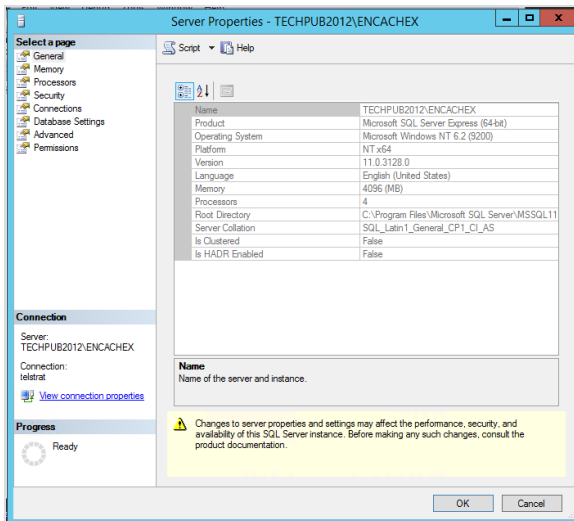
1. Start the *SQL Server Management Studio*.



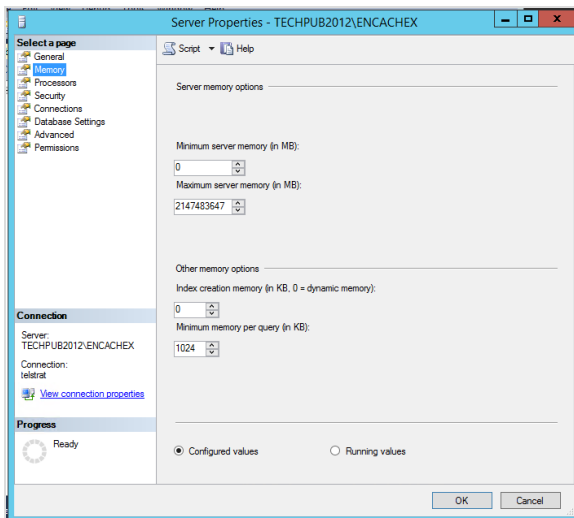
2. *Login* using either *SQL Authentication* with the login and password setup previously in the SQL install or login using *Windows Authentication* with the account presently logged into the server. Click *Connect*. The SQL Server Management Studio pops up.



3. From the Object Explorer, right click the *<Server\InstanceName>* and open *Properties*.



4. The *Properties* window <Server\InstanceName> appears.



5. On the *Server Properties* left window pane, click on *Memory*.

Change the *Maximum Server Memory* to one of the following:

If using SQL Express edition, the setting is:

- **1024 – 1GB.** SQL Express edition limits memory usage to 1,024 MB (1GB).

If the SQL Server used is **not dedicated** and running on the same server as other Engage software, then set the SQL memory limit to 25% of available memory as follows:

- 1000 – (1GB) if the server has 4GB of total memory.
- 2000 – (2GB) if the server has 8GB of total memory.
- 4000 – (4GB) if the server has 16GB of total memory.

If the SQL Server is dedicated then Maximum Server Memory is not required, but could be set to 75% of available memory.

6.4.2 Configure SQL for Engage Databases

NOTE: The following steps cannot be completed until the Engage Recording server has successfully started and the Engage databases have been automatically created.

Within the SQL server, Engage requires the following databases:

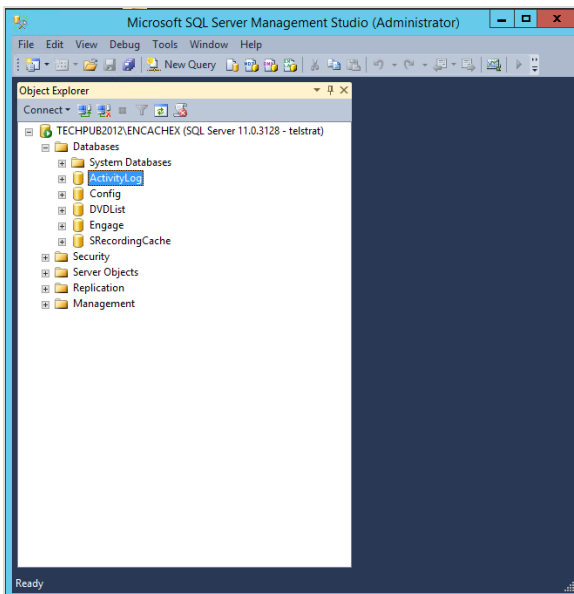
- **Config** – Recorder configuration
- **SrecordingCache** – Call records for call cache (non-archive)
- **ActivityLog** – Must be present
- **DVDList** – Must be present, but only filled if DVD archiving is used
- **Engage** - In addition, the web server requires a configurable SQL database which is typically named with the same name as the virtual directory such as Engage
- **Mass Archive Databases** – In addition, each time an archive is added Engage automatically creates a database, but the following settings must be applied to this new database.

This procedure will make the following changes to the SQL databases:

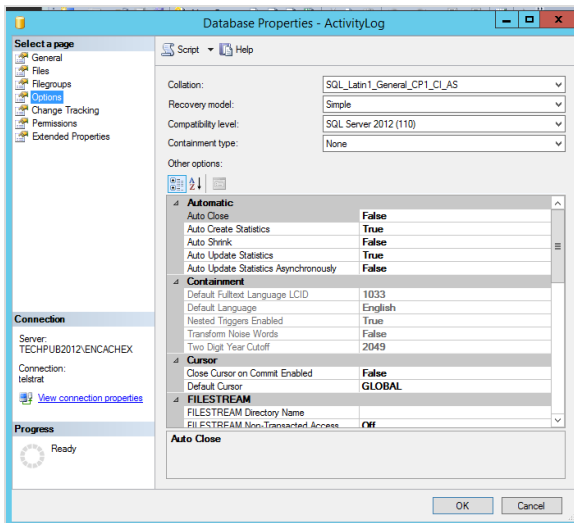
- Recovery model is set to **Simple** (to permit high-performance bulk copy operations while keeping log space requirements small - should be set to simple by default).

- Customers may choose to set recovery model to Full, but the transaction log must be managed following SQL best practices.
- If the transaction log becomes full, new calls will not be archived, and data loss could occur if the call cache fills up and starts purging.
- Auto Close is set to **False** (so each database will stay open and not close due to inactivity).

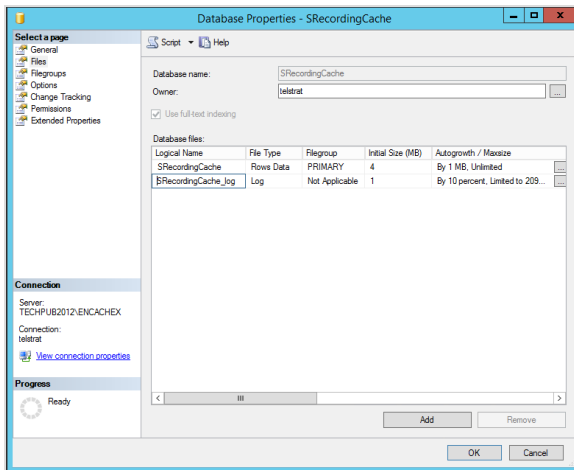
Follow these steps for each of the four new Engage Recorder databases:



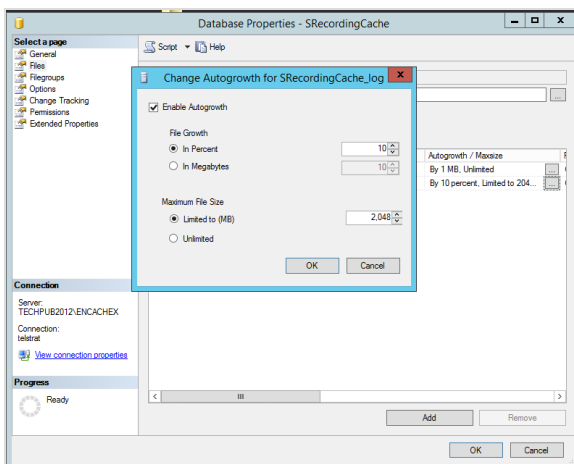
1. Logon to the *SQL Server Management Studio*. Double click on *Databases*. The list of databases expands. Note the databases named: **ActivityLog**, **Config**, **DVDList**, and **SRecordingCache**.



2. From the Object Explorer, click **Databases » Activity Log** and right click on **Properties**. On the *Database Properties - ActivityLog* window, click **Options**. Make sure *Recovery model* is set to **Simple** and change *Auto Close* to **False**. Select **OK** to save changes.
3. From the Object Explorer, click **Databases » Config** and right click to open **Properties**. On the *Database Properties - Config* window, click **Options**. Make sure the *Recovery model* is set to **Simple** and change *Auto Close* to **False**. Select **OK** to save changes.
4. From the Object Explorer, click **Databases » DVDList** and right click on **Properties**. On the *Database Properties* window, click on **Options**. Check and make sure the *Recovery model* is set to **Simple** and change *Auto Close* to **False**. Select **OK** to save changes.
5. From the Object Explorer, click **Databases » SRecordingCache** and right on **Properties**. On the *Database Properties - SRecordingCache* window, click **Options**. Make sure the *Recovery model* is set to **Simple** and change *Auto Close* to **False**. **Continue with the next step before saving changes for SRecordingCache properties.**
6. On the *Database Properties - SRecordingCache* window, click on **Files** to configure the **Autogrowth** for the SRecordingCache_Log.



7. In the *Database Properties - SRecordingCache* window, click on *Files*.
8. Locate the *SRecordingCache_Log Logical Name* in the table and click on the (...) button in the *Autogrowth / Maximize* column.



9. In the **Change Autogrowth for SRecordingCache** box, under *Maximum File Size*, click *Limited to (MB)* and enter **2048** for a maximum of 2GB files.
10. Click **OK** to save the size and click **OK** again to save the SRecordingCache Options changes.
11. Close the SQL Server Management Studio.

6.5 Create SQL Account for Engage

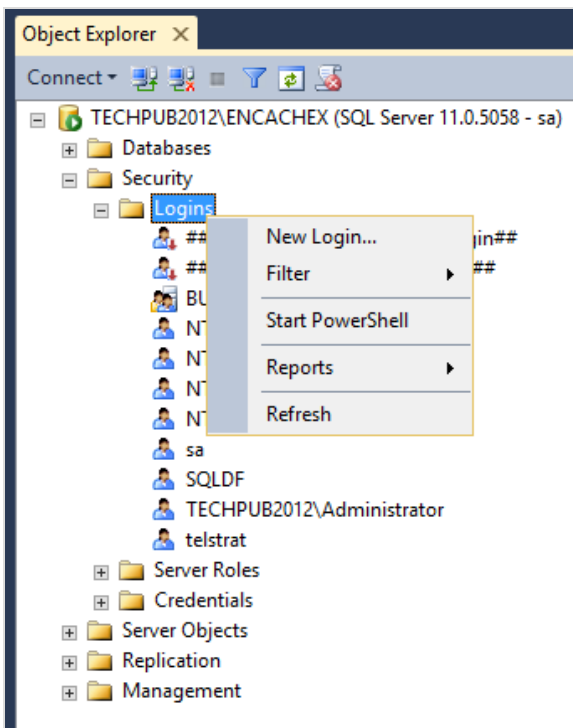
This step will create a SQL account on the SQL server for Engage. The account must be created differently depending if Engage will use SQL Authentication or Windows Authentication to connect to SQL.

6.5.1 Create SQL Account for Windows Authentication

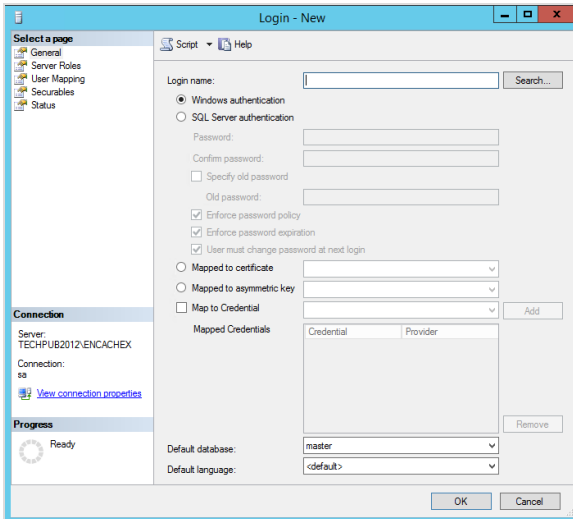
This procedure creates an account on the SQL instance for Engage to connect to SQL using **Windows Authentication**.

Perform the following steps on any SQL Database instance(s) that Engage must access.

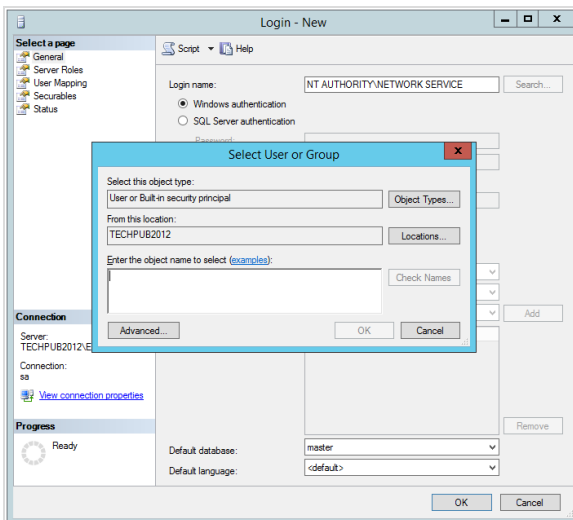
1. Launch and logon to the SQL Server Management Studio. Go to and expand *instance » Security » Logins* and right-click on *Logins*.



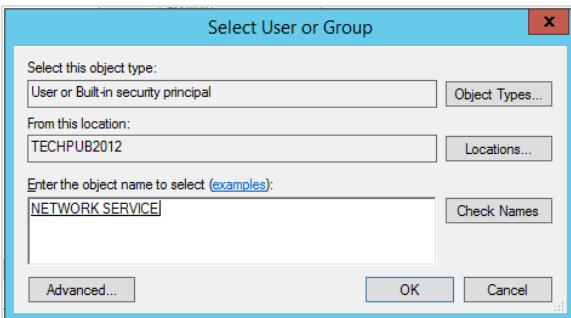
2. Click *New Login* and the following pop-up window will appear:



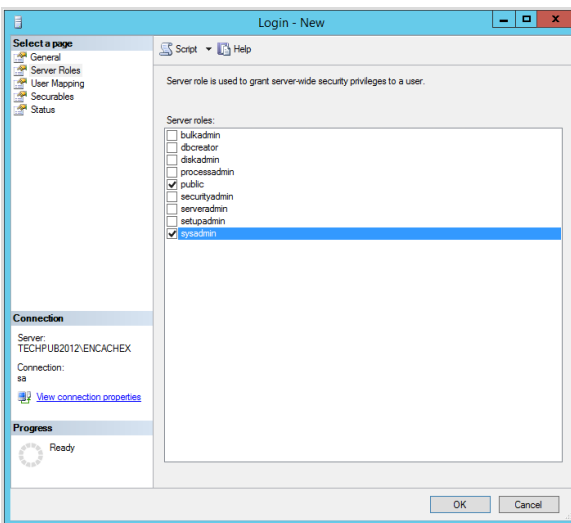
- If SQL is on the local Engage server, then in the *Login Name* field, type **NT AUTHORITY\NETWORK SERVICE** or select *Search* and the following pop-up will appear:



- Type in *Network Service* in the **Enter the object name to select field** and select *Check Names* and select **OK**.



5. Access **Server Roles** on the left hand side of the window.

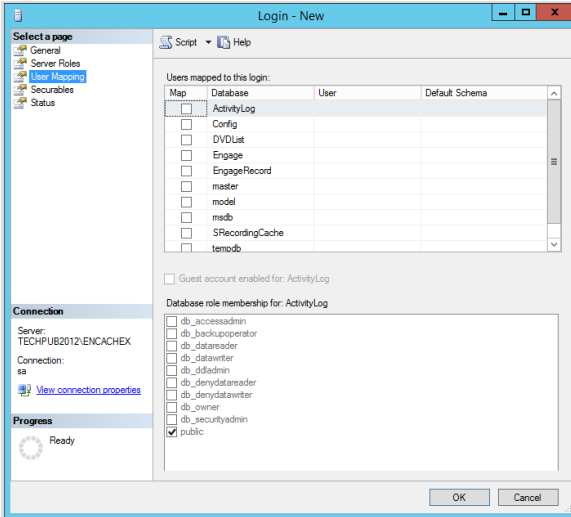


6. For simple administration, you can check the **SysAdmin** role checkbox. Click **OK** to finish.

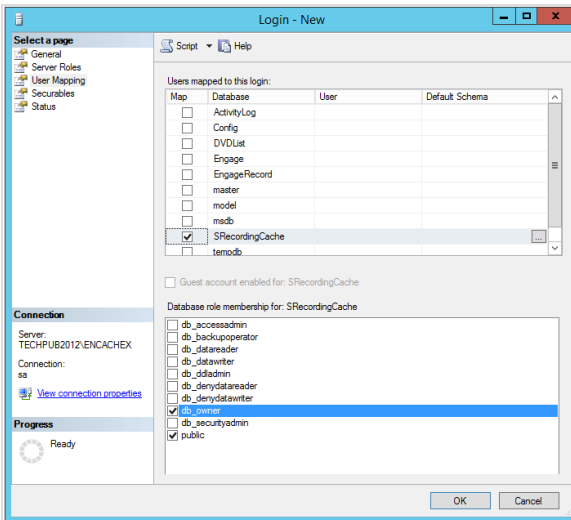
A More Secure Option

A more secure option is to choose a subset of databases that the Web Client can access under the User Mapping option.

1. On the left hand pane, select **User Mapping** and the following screen will appear:



2. Select any databases that the Web Client must access such as the Web Client database or the Recorder Databases, SrecordingCache and any Mass Storage databases.



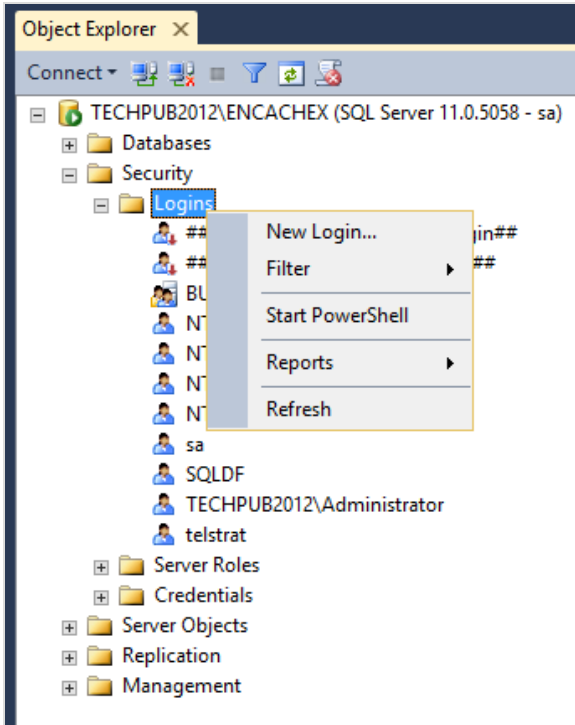
3. Click the **db_owner** checkbox.
4. Select **OK** to save the user.

6.6 Create SQL Account for SQL Authentication

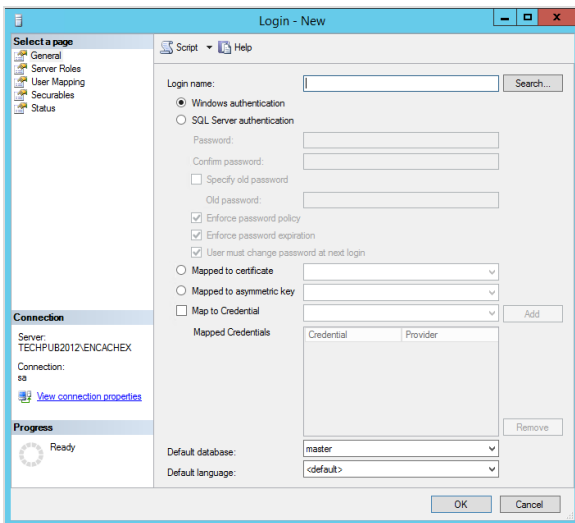
This procedure creates an account on the SQL instance for Engage to connect to SQL using **SQL Authentication** (logon and password).

Perform the following steps on any SQL Database instance(s) that Engage must access.

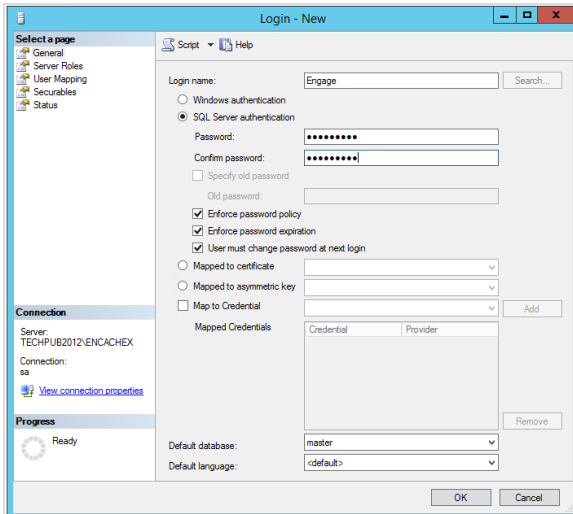
1. Launch and logon to the SQL Server Management Studio. Go to and expand *instance » Security » Logins* and right-click on *Logins*.



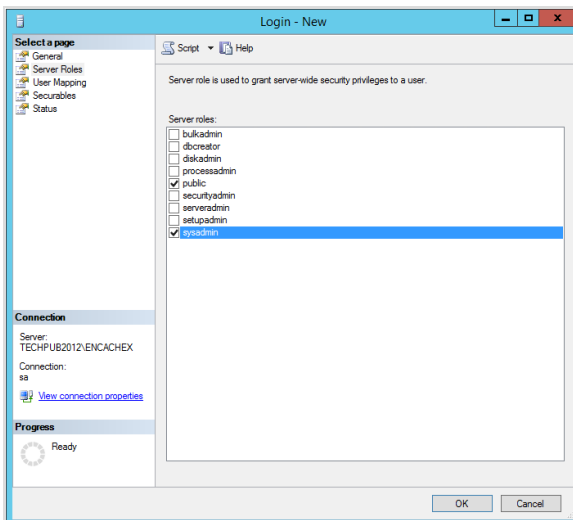
2. Click *New Login* and the following pop-up window will appear:



3. Click on the **SQL Server Authentication** button.



4. Enter the Login name that Engage will use to logon to SQL for this instance (ex. Engage).
5. Enter the password that Engage will use to logon to SQL for this instance. Confirm the password.
6. Access **Server Roles** on the left hand side of the window.

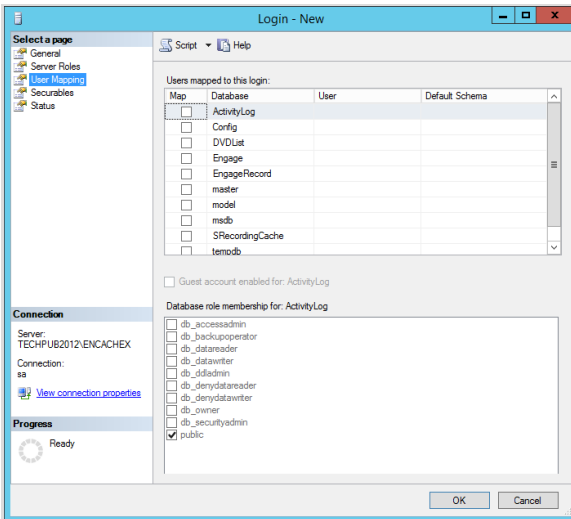


7. For simple administration, you can check the **SysAdmin** role checkbox. Click **OK** to finish.

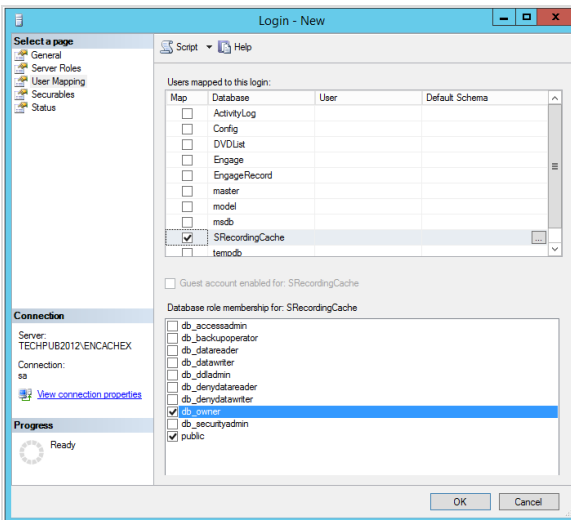
6.6.1 A More Secure Option

A more secure option is to choose a subset of databases that the Web Client can access under the User Mapping option. To do this:

1. On the left hand pane, select **User Mapping** and the following screen will appear:



2. Select any databases that the Web Client must access such as the Web Client database or the Recorder Databases, SRecordingCache and any Mass Storage databases



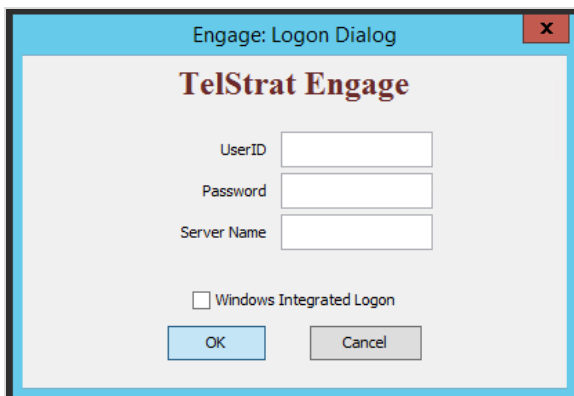
3. Click the **db_owner** checkbox

4. Select **OK** to save the user

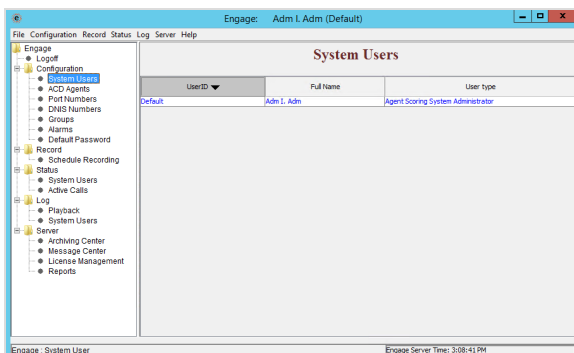
6.7 Configure Service Accounts via JAVA Client

These steps verify the Engage voice recorder is running and configures two necessary Engage service accounts, **WebClient** and **LiveMonitor**.

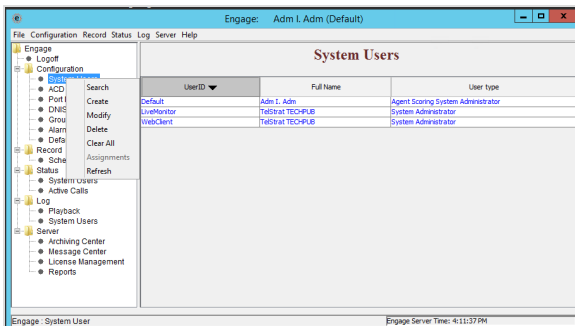
- **WebClient** is used by the web server to connect to the recorder.
 - **LiveMonitor** is used by the SIP service to connect to the recorder for live monitoring.
1. Logon to the recording server and navigate to **Start » TeStrat » Engage » Engage Client** JAVA application.



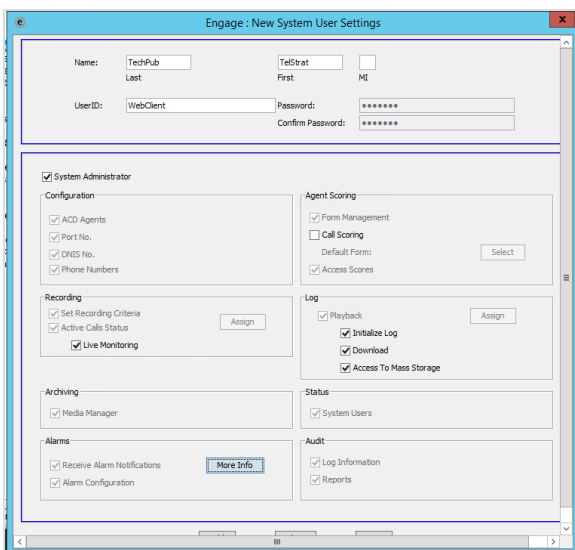
2. Login with the user name **DEFAULT** and **no password**.



3. The System Users window appears with only the Default User ID listed.



4. Click on **Configuration** and right click on **System Users** and click **Create**.



5. At the *Engage: New System Users Settings* window, enter the following:

- The name of the system, such as **TelStrat Web** in the **First Name** and **Last Name** fields.
- Type **WebClient** into the **User ID** field. Note that this User ID will be used with the Manage Record-ers screen.
- Check the **System Administrator** box.
- Click on the **More Info** button associated with **Alarms**.
- In the **Alarm Notification Recipient** window, enter an email distribution list address used by the IT department to receive email alerts.

- f. Click **OK** then click **Add**.
- g. The new user appears on the System Users list.

Engage: Alarm Notification Recipient Communication Information

Name: TechPub (Last) TelStrat (First) MI

e-mail: alertdist@techpub.com

e-mail2:

e-mail3:

Module	Critical	Serious	Warning	Information
Voice Recording Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Agent Scoring Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
System Report Replication Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
BCM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
AudioCodes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Norstar	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
MLS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
TALC	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VoIP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

OK Cancel

NOTE: TelStrat suggests the use of an email distribution list already in use by the IT department rather than individual email accounts that can become obsolete as personnel changes occur in the organization.

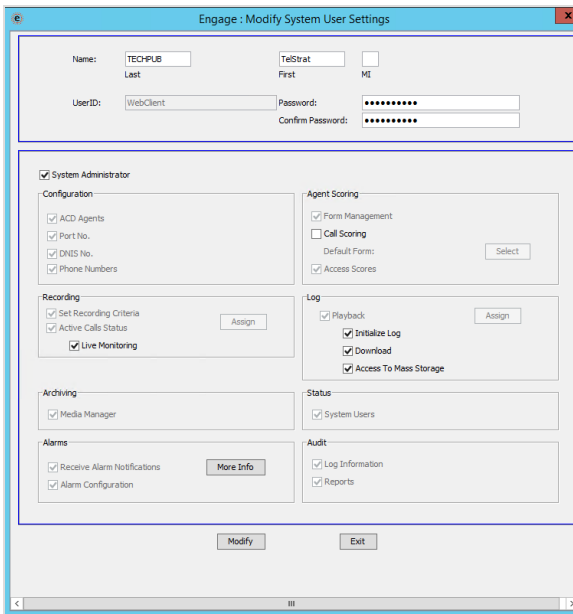
Engage: Adm I. Adm (Default)

System Users

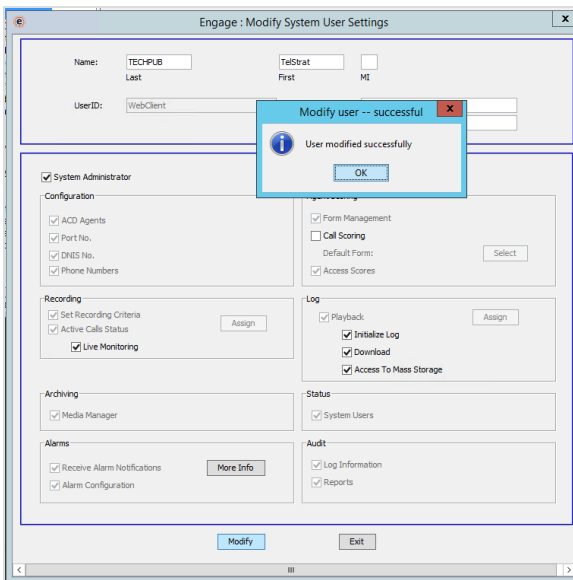
UserID	Full Name	User type
Default	Adm I. Adm	Agent Scoring System Administrator
WebClient	TelStrat TELSTRAT	System Administrator
WebClient	TelStrat TELSTRAT	System Administrator

Engage - System User

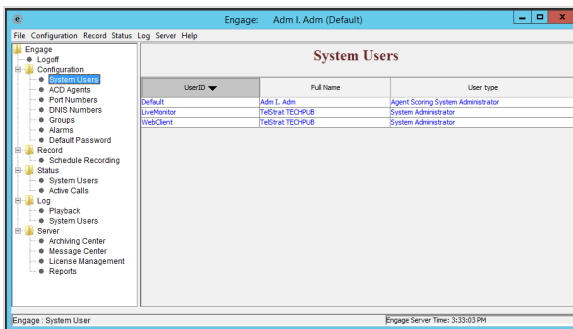
6. Change the password on the new Web Client user account. In the *System Users* window:



- Under the *User ID* column, right click on *WebClient* and Click *Modify*.
- In the *Modify System User Settings* window, enter a new password in the *Password* box.
- Repeat the new password in the *Confirm Password* box.
- Click *Modify* then *OK*, then *Exit*. Use this new password on the next Web Client login session.

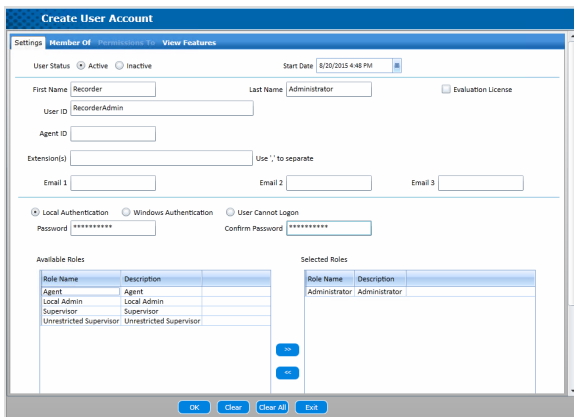


7. Create the *LiveMonitor* service account using the same system name in the First and Last Name fields.
 - a. In the User ID field, type *LiveMonitor*.
 - b. In the Password field enter *LiveMonitor* and check the **System Administrator** box.
 - c. Click *Add*. Be sure to change the password on this account.



8. When the service accounts are added, review the accounts in the *System Users* window.
9. *Close* the Engage Client.
10. Open a browser and access, for the first time, the **Web Client Logon Dialog** screen and enter the following information to access and configure the built-in user account. On the screen:
 - a. **User ID:** Enter *default*.
 - b. **Password:** Enter *default*.
 - c. There will be a prompt to change the built-in password to something other than *default*.
 - d. After changing the password, **logon** again with the new password.
 - e. The presented **Playback Log** will be empty since no call recorder has been configured yet.
 - f. Click *Add*
11. On the Web Client, click on *Administration » Users » New User* to create users.
12. Create a system user for the *Recorder Administrator* who will be managing the recorder. This will need to be a *System Administrator* account as well.

- a. **First name:** Enter *Recorder*.
- b. **Last name:** Enter *Admin*.
- c. **User ID:** Enter *RecorderAdmin*.
- d. Local Authentication should be selected.
- e. **Available Roles:** Highlight *Administrator* and click the » symbol to assign Administrator to this user.
- f. Click *OK* then *Exit* when finished.



Role Name	Description
Agent	Agent
Local Admin	Local Admin
Supervisor	Supervisor
Unrestricted Supervisor	Unrestricted Supervisor

Role Name	Description
Administrator	Administrator

13. If live monitoring of calls is desired, create another system user account for Live Monitoring (ex. *LiveMonitor*). Click *Add*. Click *Exit* when finished.

6.8 Configure Anti-Virus Real-Time Exclusions

This step can only be completed now that the TelStrat Voice Recording Service has started for the first time and created the recording folder.

Engage creates a large amount of voice recording files. The folder that stores the files is typically *D:\RecordingCache* and this folder should be excluded from anti-virus real-time file checking to avoid server performance issues.

Real-time protection, on-access scanning, background guard, resident shield, autoprotect, and other synonyms refer to the automatic protection provided by most antivirus, anti-spyware, and other anti-malware programs.

This monitors computer systems for suspicious activity such as computer viruses, spyware, adware, and other malicious objects in 'real-time', in other words while data is loaded into the computer's active memory such as when inserting a CD, opening an email, or browsing the web, or when a file already on the computer is opened or executed.

The *scanning* to set the exclusion from is the *real time or on-access scanning*, such as scanning a file when it is created or new to the server.

On demand (scheduled) scanning of files when the system is idle or nearly idle would be fine.

It is recommended to exclude the following items and components from real time scanning:

- The *C:\Program files (x86)\TelStrat* directory.
- The *SQL DB and its log file* directories.
- The *TelStrat WAV cache* directories.
- *Proxynetworks screen capture cache* directories, if using screen capture.

6.8.1 Logging On for the First Time

If the Web Client was successfully installed, it will be able to be launched from a browser. The URL to access the Web Client is usually in this format: <http://engage-server-name/Engage> where *engage-server-name* is the server name for the recorder (ex. techpub2012 or VoiceRecorder).

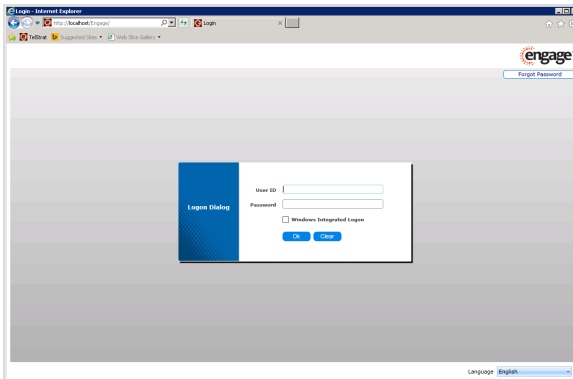
If logging on for the first time from the Engage server itself, in a browser on the server, enter <http://localhost/Engage> to access the Web Client.

If logging on for the first time from a different workstation, in a browser on the workstation, enter <http://engage-server-name/Engage> to access the Web Client.

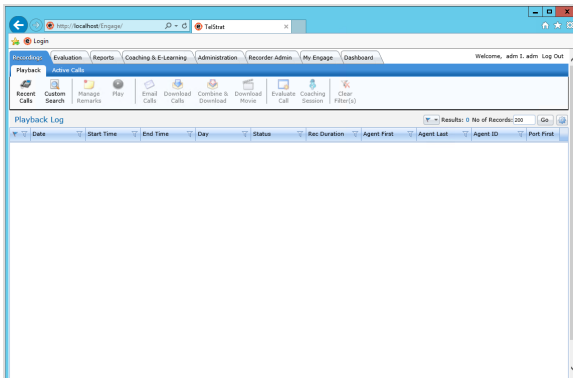
The first time login will require the user to change the default password before beginning *Administration* page configurations.

To do this after accessing the Web Client via the URL:

1. Enter the User ID as *default* .
2. Enter the password as *default*.
3. Click *OK*.



4. Prompting will occur to change the built-in password to something other than *default*. After changing the default password, logon again with the new password.



5. The *Playback Log* page will display and be empty since no call recorder has been configured for the Web Client yet. Continue to the Administration configuration section.

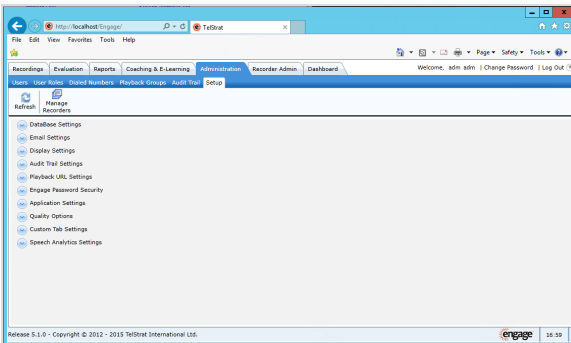
6 Recorder Setup

This section contains instructions required to setup the Engage Voice Recorder to record and playback audio calls using tabs in the Web Client and the CommSrv program.

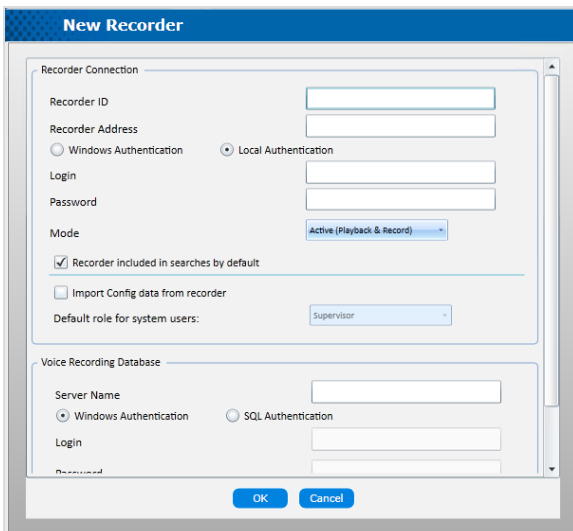
6.8.1 Configuring Recorders on the Web Client

On the Web Client, the *Manage Records* icon is used to connect the web server to each Engage Record server.

1. On the web client, navigate to *Administration » Setup* tab and click on the *Manage Recorders* button.



2. Click *New*.



New Recorder

Recorder Connection

Recorder ID:

Recorder Address:

Windows Authentication Local Authentication

Login:

Password:

Mode:

Recorder included in searches by default

Import Config data from recorder

Default role for system users:

Voice Recording Database

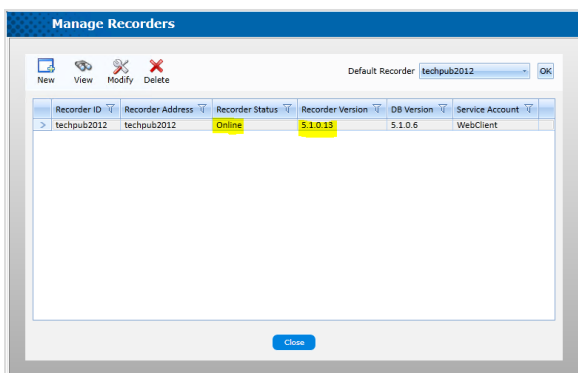
Server Name:

Windows Authentication SQL Authentication

Login:

Password:

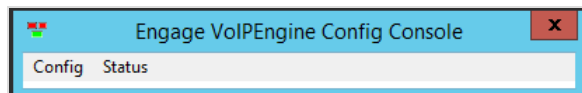
3. Enter the following into the **New Recorder – Recorder Connection** fields:
 - **Recorder ID:** A name used to refer to the recorder.
 - **Recorder Address:** The DNS name or static IP address for the recorder. Note that failure to resolve by DNS name can be worked around by entering the static IP address of the recorder.
 - **Windows Authentication or Local Authentication:** Set to **Local Authentication** for almost all new deployments. Some legacy deployments may have 3rd party software that authenticates to the Engage Record server with Windows Authentication. In this case refer to the User Guide / Manage Recorders section for detailed instructions.
 - **Login:** Enter **WebClient** which is the login ID of the Service Account created on the recorder dedicated for the web server.
 - **Mode:** Mode is **Active** unless connecting to the file store and database of a recorder that is no longer intended to record new calls.
 - **Recorder included in searches by default:** Leave this selected by default unless this is a redundant 2N recording server that is only included by searches when users specifically request it.
 - **Import Config from recorder:** *Do not select this checkbox for a new installation.* This option is for upgrading from 3.6 or previous releases only. Refer to the upgrade documentation before attempting an upgrade.
 - **Default role for system users:** Grayed out but filled with supervisor.
 - **Voice Recording Database:** This information will populate automatically as long as the Configuration Service is installed and running on the Engage Recording server. If it does not populate after leaving the recorder address field, then escalate for help.
4. Click **OK**.
5. If the information used is correct and the installation has proceeded successfully, the **Recorder Status** and **Recorder Version** column fields will be filled with status (ex. **Online**) and a version number (ex. **5.2.0.16**).
6. Click **Close** to exit.



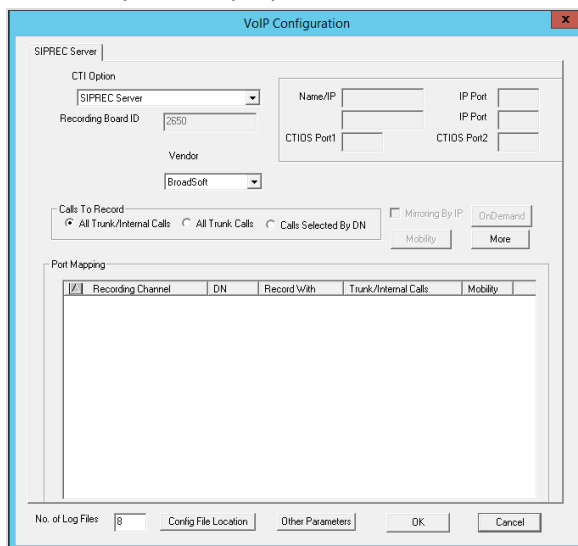
6.9 Verify VoIP Module Configuration Meets Requirements

Verify that the VoIP module configuration meets the customer's specifications and needs.

Use the **Engage VoIP Engine Config Console** to configure the platform that the Engage Recording Service will integrate with.



Each vendor's platform has unique elements, settings and configurations to work with Engage properly. Use the **Config** menu command to call up the **VoIP Configuration » CTI Option** drop-down menu to select the vendor's platform for the Engage end of the recording connection. This is an example of a BroadSoft VoIP system deployment.



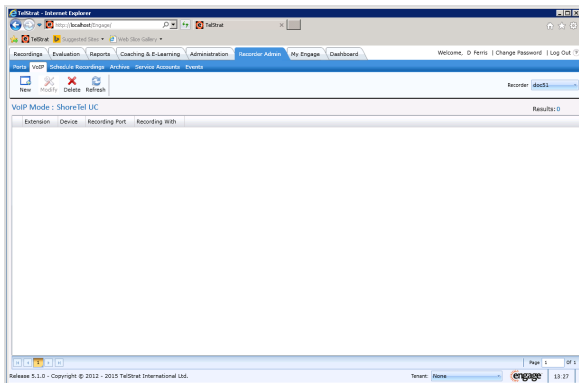
After configuration, check for any obvious issues that may be preventing recording. Usually, these issues can be traced back to the initial setups and configurations.

Some examples of out-of-specification issues to look for are:

- Too many softphones for an Avaya red installation have been configured.
- Each customer has procured a virtual phone in the Avaya CM for each soft phone configured.
- Check [VoIPInfo.log](#) making sure there are not unnecessary registrations (ex. soft phone registration failure events).
- Ensure auto learning is enabled, whenever possible.

6.9.1 Web Client VoIP Tab

Once the one time VoIP configuration has been completed using the **VoIP Configuration Console** for the platform being deployed, the VoIP devices (telephones) to record can be managed from the web client at the [Recorder Admin » VoIP](#) tab.



This is documented in the specific Configuration Guide for the voice platform (ex. Avaya CM, Cisco UCM, Nortel CS 1000, etc...) being integrated. There are differences for each voice platform.

6.9.2 Mass Archive

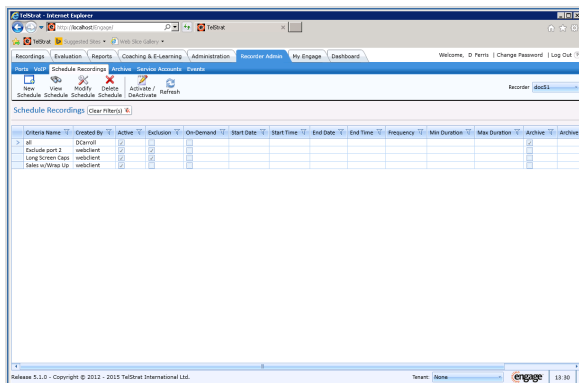
All Mass Archive storage locations should be defined first *before the recording schedule* so that the recording schedule can be used to map sets of calls into specific archives, if desired.

The mass archive defines the storage location and options such as how long to retain calls and limiting the system to archive only at off-peak hours for maximum system performance.

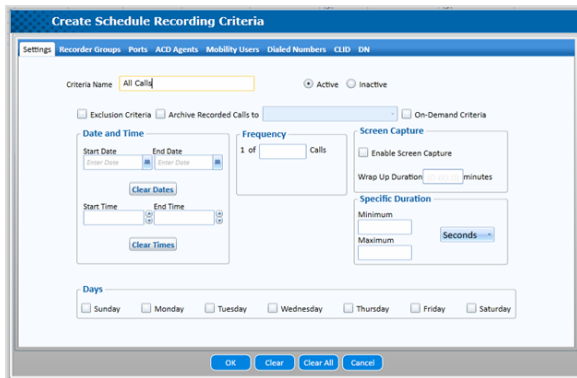
Refer to the **Setup - Mass Archive** document and the customer's prerequisite documentation for full details on setting up and activating Mass Archives.

6.9.3 Recording Schedule

Engage requires a recording schedule to record any calls. To record all calls, build an **All Calls** recording schedule using the following:



1. Logon to the web client and access the **Recorder Admin » Schedule Recordings** tab.
2. Select **New Schedule** to create recording schedules.
3. Type in a name for the recording schedule (ex. **All Calls**).
4. Verify the **Active** button is selected.
5. If *mass archive* is required, select the Archive Recorded Calls to checkbox. You must select the archive from the drop down box which contains a list of pre-defined archives. Archiving can be setup later, but as part of setting up the archive you must modify the recording schedule to select the archive. Any calls recorded without an archive selected will not be archived.
6. Select **OK**.



Engage is typically deployed to record all calls on monitored phones. However, Engage includes a configurable recording schedule rules which includes:

- Exclude specific extensions (for privacy)
- Time of Day
- Date ranges
- Extension
- Calling number (ANI)
- Dialed Number (DNIS)
- 1 of n
- Duration based
- Day of the week
- Agent Group
- Agent ID

Refer to the *Schedule Recording* section of the **Administration Activities** document for setting up more complex recording schedules.

When archiving of calls to the online mass storage, be sure to, first, create the archives so the recording schedule can reference the archive. When calls are recorded, the calls will be sent to the archive which is defined for the matching recording schedule.

If a call meets multiple recording schedules that define different archive IDs, then the longest duration archive will be selected by the software.

The customer's prerequisite documentation will provide the information needed to set up recording schedules.

6.9.4 Ports

Engage ports will reference specific VoIP devices (telephones typically). For example, a unique extension may be configured as a VoIP port mapping on Engage port number 2400:001. The port number is 2400:001 which consists of a board ID (2400) and recording channel (001).

Engage port numbers are required for configuring the following add-on features that require a workstation mapping:

- Screen recording
- On Demand Recording Client (ODRC)
- Desktop Analytics (DA)

For non-ACD calls, Engage port numbers can be mapped to user accounts to define which calls a restricted user may playback. Deployments with contact center agents typically assign groups of agents or individual agent IDs to user accounts, but if agents are not present, ports can be assigned to user accounts to control which calls a restricted user can playback. In this case it is advantageous to assign a name to a port to make administration easier.

When setting up ports for non-contact center deployments, it is recommended to enter a name for each port that is used when assigning ports to user accounts. For example, name a port *Nurse Station1*, and then when creating a user account for the nursing manager, you can assign the port with this name to the manager.

Engage port numbers can be used to allocate Evaluation Licenses if there are more agents than evaluation license purchased.

Note that users can be granted unrestricted resources to all calls, and these user accounts do not require port assignment.

If any of these conditions are met, configure the Engage ports for the recorded devices.

6.9.5 SMTP Server Settings

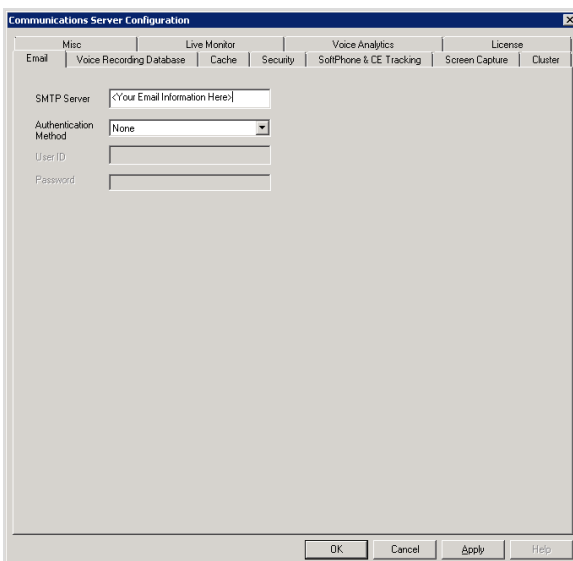
The Engage Voice Recorder sends notifications of issues it encounters in the form of emails. Two configurations are needed for the feature to operate correctly.

Communications Server Configuration (CommSrv) setup

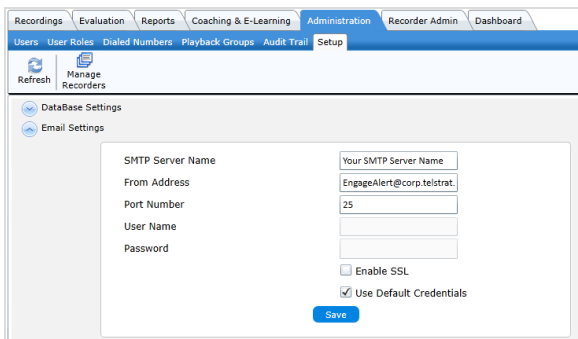
The Engage server's Communications Server Configuration (CommSrv) must be configured with the customer's SMTP server information to be able to send email alerts (error events).

NOTE: If this is setup prior to adding the Manage Recorders connection, the SMTP server information will autofill into the web client's Setup Email Settings. However the From Address should still be configured

1. In the CommSrv tool, verify the Setup Email Settings and the Server Configuration SMTP are entered.



2. On the Web Client, configure the **SMTP Server Name** and **From Address** on the Web Client's Email Settings.



The screenshot shows the 'Email Settings' configuration page in the TelStrat web client. The page has a navigation bar at the top with tabs for 'Recordings', 'Evaluation', 'Reports', 'Coaching & E-Learning', 'Administration', 'Recorder Admin', and 'Dashboard'. Below the navigation bar, there are tabs for 'Users', 'User Roles', 'Dialed Numbers', 'Playback Groups', 'Audit Trail', and 'Setup'. The 'Setup' tab is active. On the left side, there are icons for 'Refresh' and 'Manage Recorders'. The main content area is titled 'DataBase Settings' and 'Email Settings'. It contains the following fields and options:

- SMTP Server Name: Your SMTP Server Name
- From Address: EngageAlert@corp.telstrat
- Port Number: 25
- User Name: (empty)
- Password: (empty)
- Enable SSL
- Use Default Credentials
- Save button

NOTE: This information can be configured without restarting the Voice Recording Service.

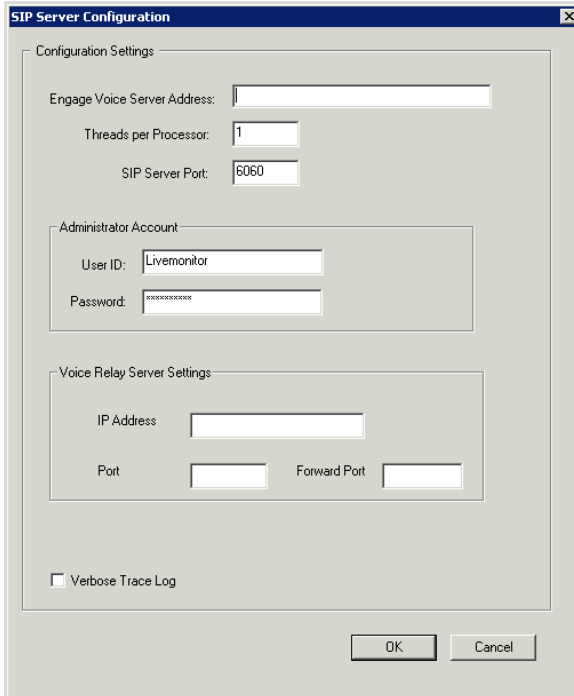
6.9.6 Configuring Live Monitoring

Refer to the [SETUP - LIVE MONITORING](#) document for more detailed step-by-step instructions and troubleshooting for setting up live monitoring.

If Live Monitoring of active calls is required, the *Server Configuration* and the *SIP Server* must be configured with a dedicated IP address and firewall ports.

To configure live monitoring:

1. Open **Start » TelStrat Engage » SIP Server Configuration**. Click on **Config** in the menu bar.



2. Enter the **IP address** of the recording server.
3. Leave **Threads Per Processor** at **1** and **Port** as **6060**.
4. Enter the **LiveMonitor** service account ID and password.

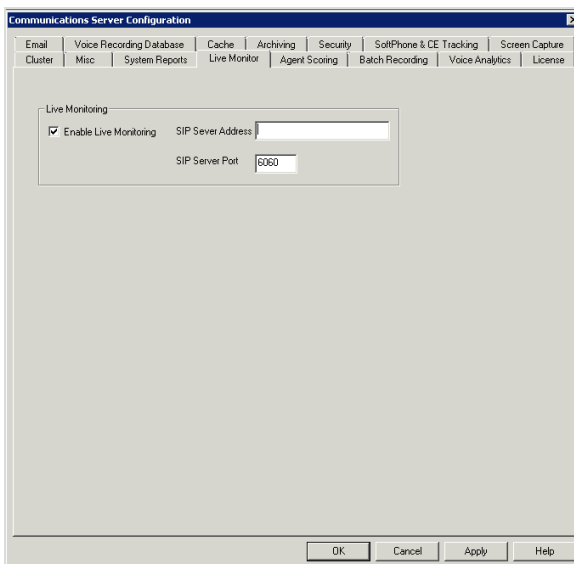
To configure Voice Relay Server setting:

The Voice Relay Server Settings are required if the SIP server needs to be enabled for Live Monitoring over the Internet, meaning the SIP server is installed and configured on a public facing server, generally the IIS server hosting the Engage web UI.

The following steps detail how to complete the Voice Relay Server settings.

1. **IP address** is the server's public facing IP address where the SIP server is installed.
2. **Port** is the server's public facing port for Live Monitoring transport. Firewall rules need to allow both TCP/UDP rules for this user definable port.

3. **Forward Port** is the port that must match the LMRelayPort registry setting explained in the above related prerequisite.
4. Click **OK and Exit**.
5. Open **Start » TelStrat Engage » Server Configuration**. On the **Live Monitor** Tab of the **Communication Server** window:
 - a. Check the **Enable Live Monitoring** checkbox.
 - b. Enter the **IP address** in the **SIP Server Address** text box.
 - c. If enabling Voice Relay Server, the IP address will match the configured IP address of the Voice Relay Server Settings IP address in the SIP server configuration.
 - d. Enter the **port number** in the **SIP Server Port** text box.
 - e. Click **OK**.



Any changes to the Communication Server window require a restart; however it is acceptable to make all changes prior to restarting the server.

6.10 Administration

User ID	First Name	Last Name	Extension(s)	Agent ID	Mobility User ID	Evaluation License	User Role(s)	Email Account(s)	Status	Last Login	IP
2026											
1111											
1128											
1130											
1137											
1138											
1143											
3004											
3005											
3033											
admin	admin	Admin					Administrator		Office	8/18/2015 3:44:53 PM	
admin	admin	Administrator					Administrator	admin@customer.com	Office		
agent	Matthew	Agent	8000				Recorder Admin		Office		
agent	Matthew	Agent									
agent	Matthew	Agent	1134								
agent	Matthew	Agent	3031								
agent	Matthew	Agent	3008								
agent	Matthew	Agent	3017								
agent	Matthew	Agent	3029								
agent	Matthew	Agent	3030								
agent	Matthew	Agent	3032								
agent	Matthew	Agent	3033								
agent	Matthew	Agent	3034								
agent	Matthew	Agent	3035								
agent	Matthew	Agent	3036								
agent	Matthew	Agent	3037								
agent	Matthew	Agent	3038								
agent	Matthew	Agent	3039								
agent	Matthew	Agent	3040								
agent	Matthew	Agent	3041								
agent	Matthew	Agent	3042								
agent	Matthew	Agent	3043								
agent	Matthew	Agent	3044								
agent	Matthew	Agent	3045								
agent	Matthew	Agent	3046								
agent	Matthew	Agent	3047								
agent	Matthew	Agent	3048								
agent	Matthew	Agent	3049								
agent	Matthew	Agent	3050								
agent	Matthew	Agent	3051								
agent	Matthew	Agent	3052								
agent	Matthew	Agent	3053								
agent	Matthew	Agent	3054								
agent	Matthew	Agent	3055								
agent	Matthew	Agent	3056								
agent	Matthew	Agent	3057								
agent	Matthew	Agent	3058								
agent	Matthew	Agent	3059								
agent	Matthew	Agent	3060								
agent	Matthew	Agent	3061								
agent	Matthew	Agent	3062								
agent	Matthew	Agent	3063								
agent	Matthew	Agent	3064								
agent	Matthew	Agent	3065								
agent	Matthew	Agent	3066								
agent	Matthew	Agent	3067								
agent	Matthew	Agent	3068								
agent	Matthew	Agent	3069								
agent	Matthew	Agent	3070								
agent	Matthew	Agent	3071								
agent	Matthew	Agent	3072								
agent	Matthew	Agent	3073								
agent	Matthew	Agent	3074								
agent	Matthew	Agent	3075								
agent	Matthew	Agent	3076								
agent	Matthew	Agent	3077								
agent	Matthew	Agent	3078								
agent	Matthew	Agent	3079								
agent	Matthew	Agent	3080								
agent	Matthew	Agent	3081								
agent	Matthew	Agent	3082								
agent	Matthew	Agent	3083								
agent	Matthew	Agent	3084								
agent	Matthew	Agent	3085								
agent	Matthew	Agent	3086								
agent	Matthew	Agent	3087								
agent	Matthew	Agent	3088								
agent	Matthew	Agent	3089								
agent	Matthew	Agent	3090								
agent	Matthew	Agent	3091								
agent	Matthew	Agent	3092								
agent	Matthew	Agent	3093								
agent	Matthew	Agent	3094								
agent	Matthew	Agent	3095								
agent	Matthew	Agent	3096								
agent	Matthew	Agent	3097								
agent	Matthew	Agent	3098								
agent	Matthew	Agent	3099								
agent	Matthew	Agent	3100								
agent	Matthew	Agent	3101								
agent	Matthew	Agent	3102								
agent	Matthew	Agent	3103								
agent	Matthew	Agent	3104								
agent	Matthew	Agent	3105								
agent	Matthew	Agent	3106								
agent	Matthew	Agent	3107								
agent	Matthew	Agent	3108								
agent	Matthew	Agent	3109								
agent	Matthew	Agent	3110								
agent	Matthew	Agent	3111								
agent	Matthew	Agent	3112								
agent	Matthew	Agent	3113								
agent	Matthew	Agent	3114								
agent	Matthew	Agent	3115								
agent	Matthew	Agent	3116								
agent	Matthew	Agent	3117								
agent	Matthew	Agent	3118								
agent	Matthew	Agent	3119								
agent	Matthew	Agent	3120								
agent	Matthew	Agent	3121								
agent	Matthew	Agent	3122								
agent	Matthew	Agent	3123								
agent	Matthew	Agent	3124								
agent	Matthew	Agent	3125								
agent	Matthew	Agent	3126								
agent	Matthew	Agent	3127								
agent	Matthew	Agent	3128								
agent	Matthew	Agent	3129								
agent	Matthew	Agent	3130								
agent	Matthew	Agent	3131								
agent	Matthew	Agent	3132								
agent	Matthew	Agent	3133								
agent	Matthew	Agent	3134								
agent	Matthew	Agent	3135								
agent	Matthew	Agent	3136								
agent	Matthew	Agent	3137								
agent	Matthew	Agent	3138								
agent	Matthew	Agent	3139								
agent	Matthew	Agent	3140								
agent	Matthew	Agent	3141								
agent	Matthew	Agent	3142								
agent	Matthew	Agent	3143								
agent	Matthew	Agent	3144								
agent	Matthew	Agent	3145								
agent	Matthew	Agent	3146								
agent	Matthew	Agent	3147								
agent	Matthew	Agent	3148								
agent	Matthew	Agent	3149								
agent	Matthew	Agent	3150								
agent	Matthew	Agent	3151								
agent	Matthew	Agent	3152								
agent	Matthew	Agent	3153								
agent	Matthew	Agent	3154								
agent	Matthew	Agent	3155								
agent	Matthew	Agent	3156								
agent	Matthew	Agent	3157								
agent	Matthew	Agent	3158								
agent	Matthew	Agent	3159								
agent	Matthew	Agent	3160								
agent	Matthew	Agent	3161								
agent	Matthew	Agent	3162								
agent	Matthew	Agent	3163								
agent	Matthew	Agent	3164								
agent	Matthew	Agent	3165								
agent	Matthew	Agent	3166								
agent	Matthew	Agent	3167								
agent	Matthew	Agent	3168								
agent	Matthew	Agent	3169								
agent	Matthew	Agent	3170								
agent	Matthew	Agent	3171								
agent	Matthew	Agent	3172								
agent	Matthew	Agent	3173								
agent	Matthew	Agent	3174								
agent	Matthew	Agent	3175								
agent	Matthew	Agent	3176								
agent	Matthew	Agent	3177								
agent	Matthew	Agent	3178								
agent	Matthew	Agent	3179								
agent	Matthew	Agent	3180								
agent	Matthew	Agent	3181								
agent	Matthew	Agent	3182								
agent	Matthew	Agent	3183								
agent	Matthew	Agent	3184								
agent	Matthew	Agent	3185								
agent	Matthew	Agent	3186								
agent	Matthew	Agent	3187								
agent	Matthew	Agent	3188								
agent	Matthew	Agent	3189								
agent	Matthew	Agent	3190								
agent	Matthew	Agent	3191								
agent	Matthew	Agent	3192								
agent	Matthew	Agent	3193								
agent	Matthew	Agent	3194								
agent	Matthew	Agent	3195								
agent	Matthew	Agent	3196								
agent	Matthew	Agent	3197								
agent	Matthew	Agent	3198								
agent	Matthew	Agent	3199								
agent	Matthew	Agent	3200								

The training will include a review of the following

- Explain that agent names populate based on call records that have an Agent ID.
- Agent names can be added after the call is recorded and they will then appear for next user login in the Playback Log
- Agent ID recycling is not supported in this release. The currently provisioned agent name will appear in the Playback Log
- Set Agent ID to appear in all call records in server config under Misc. tab.
- Evaluation licenses should be applied to agents unless there are too many agents due to multiple shifts (use Port licenses instead).

Admin » Dialed Numbers

This is typically only required for outsourced contact centers that share agents across multiple projects or customers. This can be used so a supervisor might only have rights to playback calls for a pre-defined list of dialed numbers (incoming numbers) for a particular project or customer.

Admin » Playback Groups

- Playback Groups can contain agents, dialed numbers, mobility users from multiple call recorders. Recording Groups are stored on the recorder and cannot contain resources from multiple recorders. Recording Groups can be referenced by a recording schedule or for assignment to a user account, but Playback Groups can only be used for assignments to a user account.
- Agents should be placed into Playback Groups and then assigned to any supervisors that are not granted the Unrestricted Resources permission.
- Agent groups are needed for the dashboard to display data by group and to compare agents within a group.
- Consider creating an “All Agents” group especially if no business users were granted Unrestricted Resources permission.

Audit Trail

- Show how the audit trail tracks who is playing back, live monitoring, or deleting calls. The call is tracked as well.

Setup Tab consists of these areas:

Manage Recorders

- View the recorder connection. Show how the web client connects to the recorder using a service account, and the recorder database location is listed to help find it for SQL backups

Database

- This tab shows the location of the application (web) database

Email Settings

- Review the SMTP server information located here and verify the same information is configured in Server Config under Email on the recording server.
- Configuring this via the web client will also push the same configuration to Server Config Email tab.
- The web setup SMTP settings are used for emailing calls, evaluations, or reports.
- Server Config email setting is used for emailing system events.

Display Settings

- Hide ACD Agents: Unchecked by default. Select if this is a non-agent deployment.
- Hide Mobility Users: Un-check only for Cisco UCM deployments if the customer uses extension mobility. Logoff and logon to the web client to add the Admin > Mobility Users tab
- Hide Find Related Calls : Un-check for Cisco UCM, Avaya ACM, CS 1000, and ShoreTel. Leave set for all others. If un-checking, then logoff and logon again so Tracking ID is available as an available column.
- Configure Default Playback View and explain that each role can be set as well.
- Un-select port names or move to the right past agent name

- Typical recommended setup is for a contact center:
 - Date
 - Start Time
 - End Time
 - Recording Duration
 - Direction
 - CLID
 - Dialed Number
 - Direction
 - Agent First
 - Agent Last
 - Agent ID
 - Remark1
 - Remark2
 - Recording Status

- Remove any unused columns such as encryption, screen capture, or archive status.

- Users will not be updated unless they select Restore Default View from Playback Log settings.

Playback URL Settings

- Verify Enable URL Playback is enabled

Local Password Security

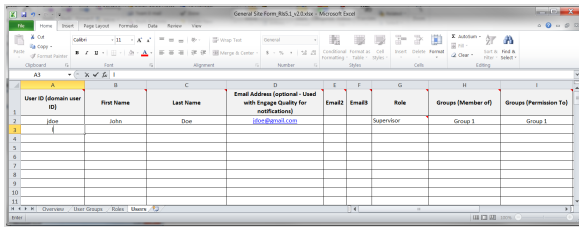
- Configure with the customer if users will be using local authentication

Application Settings

- Review the inactivity timer & web content storage folder

6.10.1 Bulk Data Import (Users Data)

This release of Engage supports importing users and their data from an XML file. Completed by the customer and TelStrat during the pre-installation planning effort, the **General_Site_Form_Rls5.1 Users** page is used to collect and sort all of the customer's users for this deployment. It must be completed prior to installation as it is a data source regarding users. It is also used to copy and paste that user data INTO the XML file for quick insertion into the system via a bulk data import action.



User ID (domain user ID)	First Name	Last Name	Email Address (optional - Used with Engage Quality for notifications)	Email1	Email2	Role	Groups (Member of)	Groups (Permission To)
	John	Doe	john@engage.com			Supervisor	Group 1	Group 1

For new Engage system installations or for bulk adding of additional users, use the following procedures:

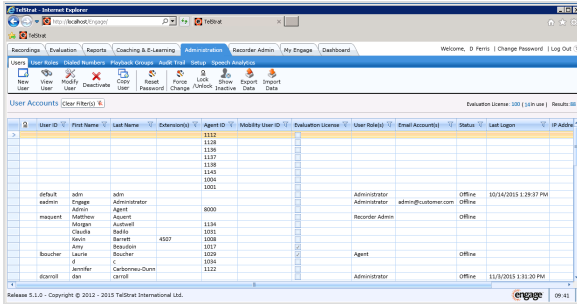
Create Roles and Groups

Use the Engage [WEB_CLIENT ADMINISTRATOR'S GUIDE](#) to get more details on how to create new user roles and groups. Prior to the Engage system going online, customers will need to:

1. Create all user roles on the Web Client first. This is important. Any users that use a specific role will not import into the new or updated Web Client unless that role exists already.
2. Create all user groups with names only (membership lists can be empty). This is important. Any users that are members of these groups or have permission to these groups will not be imported properly unless the group already exists.

Export Users Data into an XML File

1. Logon to the Web Client and go to the **Administration » Users** tab.



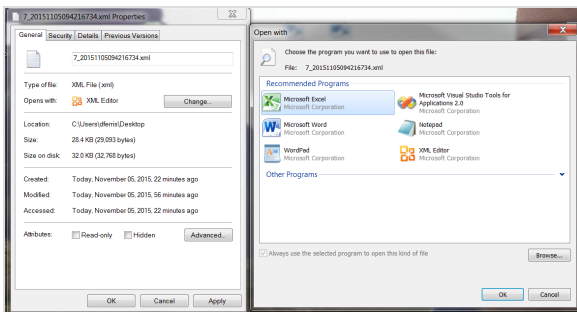
2. Select **Export Data** to export the user list and **Save** this .XML file. It is important to always do the export data from the system once the basic system Setup is complete and has shown or hidden ACD Agent ID and Mobility User IDs. The file will be found in the server's **Downloads** folder unless pointed someplace else.

Note: The exported file for a new installation will only include the default user account (used at startup) plus any other users that have already been added during the installation.

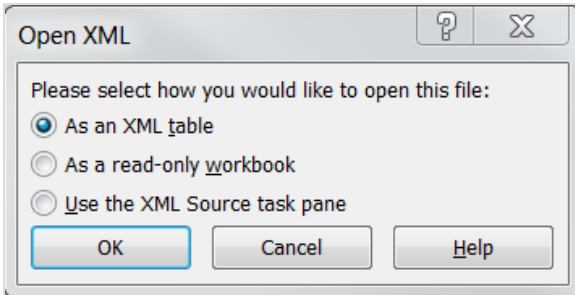
Place New User Data in the File

Depending on server software, the XML file may need to be moved to a computer system with Excel available. When the file is ready to be worked:

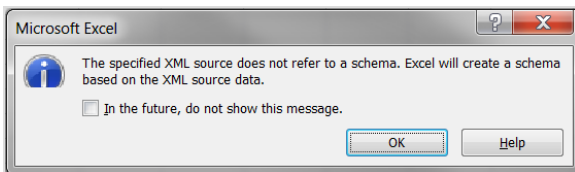
1. Open the exported .XML file using Microsoft Excel 2010 or newer. The **Properties** tab of the file will offer choices of programs to open it with. Set it for **Excel**.



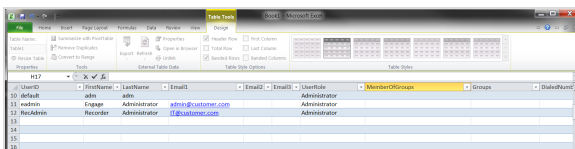
2. When prompted by **Excel**, open the file as an XML table by clicking the **As an XML table** button.



3. Select **Yes** to create a schema.

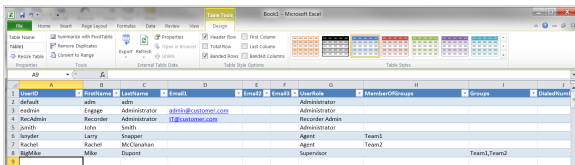


4. The file contents will appear as columns and line entries. Remember that a NEW system will only have the default user entries and any other users that were programmed (ex. *default*, *eadmin* and *recadmin*).

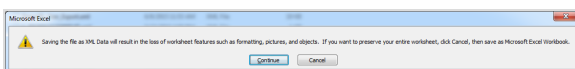


5. **Select** then **Copy** the user information from the **General_Site_Form_Rls5.1 Users** page of the worksheet and **Paste** it into to XML file.

- Make sure to have the customer fill out the Excel workbook prior to this task. The page has places for User Roles and Teams.

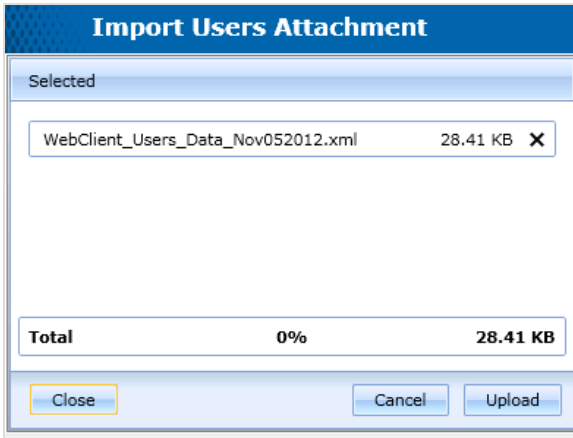


6. After pasting in the customer supplied user information, **Save** the file as an .XML file from Excel. Select **Continue** to save as .XML.

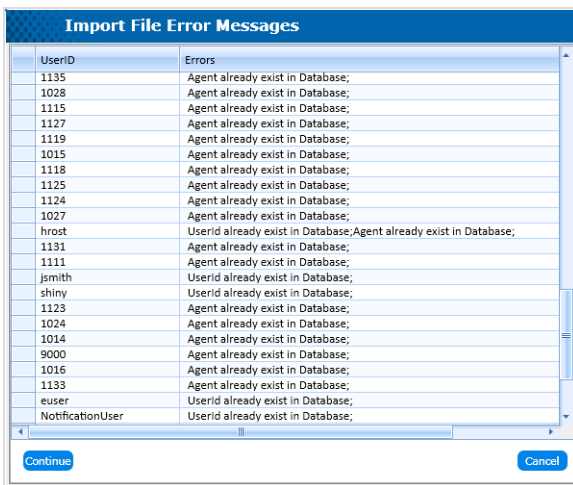


Importing the XML File of Bulk User Data

1. Back on the Web Client, go to the **Administration » Users** tab, select the **Import Data** icon to get the **Import Users Attachment** window and browse to find the .XML file that contains the saved additions and changes for bulk user data import to Engage . The file may need to be transferred back to the Engage server, if it data entries wer performed on another machine.



2. Any existing data being written over by the process will appear as a an error in a warning window. Select **Continue**.



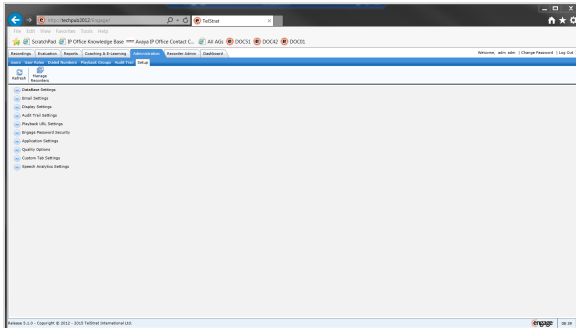
3. After import, the screen will refresh to show the NEW users and their data that have been added.

Note: Any user roles and user teams referenced by the .XML file must exist before importing the data.

6.10.2 Setup Tab and E-Mail

All sections within the **Setup** tab should be configured for the installation as follows:

NOTE: Setup options are described in the **Administration Activities** guide that is part of the *User Guide online help* under **Setup & Administration**.



- Database Settings
 - View the location of the application (web) database which gives the SQL server and sQL instance. This is useful to help find the location of the database before backing it up.
- Email Settings
 - Email settings are required for emailing calls by URL, call recordings .WAV files, evaluations, and reports. There is a similar setting on the recording server that is used to email system events. Both should be configured with the same SMTP Server Name.
 - From Address only applies to emails sent by the application software. A similar setting is available for the recording server for system alerts, but it can only be configured in the registry.
- Display Settings
 - Hide Evaluations tab
 - Hide Recorder Admin » VOIP tab
 - Hide Recorder Admin » Ports tab
 - Hide ACD Agents – This should be selected only for non-contact center deployments

- Hide Mobility Users – This is hidden by default, but should be de-selected for Cisco UCM deployments that use the Cisco Extension Mobility feature.
- Hide Find Related Calls – Engage supports Find Related Calls for the following integrations:
 - Avaya ACM - release 4.2.1 and later
 - Cisco UCM - release 4.2.1 and later
 - ShoreTel - release 4.2.1 and later
 - CS 1000 VoIP – release 4.2.2 and later
 - Siemens Openscape - release 4.2.2 and later
- De-select the *Hide Find Related Calls* if the above conditions are met. This allows the Call Tracking ID column to be selected in Customize Playback View. This also allows the timeline player to automatically find related calls (transfer and conference) and display related calls as tabs in the timeline player.
- Configure Default Playback View: This button opens a setup window used to select the Playback View columns to be displayed in the default Playback View, for most deployments:
 - System Flags (icon)
 - Date
 - Start Time
 - End Time
 - Status (recording)
 - Recording Duration
 - Hold Duration
 - User first (first name)
 - User last (last name)

- Agent ID
 - Extension
 - CLID
 - Dialed Number
 - Direction
 - Remark1
 - Remark2
 - Generic1: Only enable if Generic1 field data is configured for Cisco VoIP or Avaya ACM VoIP
 - Clicking the **Save** button will save this configuration and close the window.
- Audit Trail Settings
 - Leave the default settings
 - Playback URL Settings
 - Enable URL Playback – Select this by default.
 - Enable URL Encryption – Selecting this hides the UID in the playback URL. This prevents users from trying to guess other UIDs to playback other calls.
 - Engage Password Security
 - These settings only apply for user accounts that use Engage authentication. This is not required for if Windows Authentication is used to authorize user accounts.
 - The default password for new user accounts can be entered.
 - Passwords can be configured to expire after so many days.
 - Passwords can be set to have a maximum length.

- Passwords can be set with strong password requirements to require Upper case, Lower case, digits, or special characters.

- Application Settings
 - Inactivity Timeout – This should be left at the default value of 240 minutes to help close out user client sessions that are no longer active such as when a user leaves for the day.
 - Web Content Storage Folder Location – File attachments can be uploaded with Evaluations, Coaching sessions, and E-Learning assignments. These are stored at the location specified. Engage Quality deployments recommend a dedicated partition for these attachments to help prevent the C:\ drive from filling up and causing service to fail.

- Quality Options
 - Email completed evaluation notification to agent – If the agents are configured as users and have email accounts, then a notification can be sent to the user alerting them that they have an evaluation to review.
 - Email coaching notification to agent – This option allows agents to receive notifications when coaching sessions are created for calls taken by the user.
 - Email E-learning notification to agent – This option allows agents to receive notifications when e-learning sessions are assigned to the user.

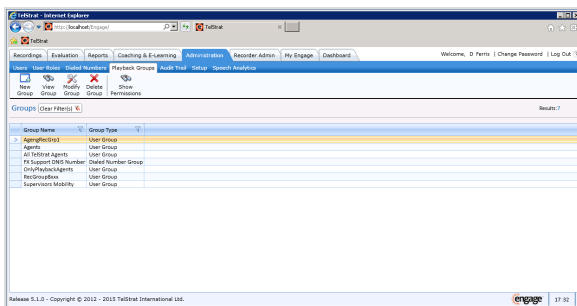
- Custom Tab Settings
 - This is not typically setup for new installations.

- Speech Analytics Settings
 - This feature is enabled via the checkbox for Enable Speech Analytics being selected and Saved.

6.10.3 Playback Groups Configuration

Refer to the Engage **Web Client Administrator's Guide** for detailed information regarding setup tasks.

The **Administration » Playback Groups** tab groups several users or dialed numbers together for assignment to user accounts. Modify the group membership as resources are added or removed from the group to simplify user account assignments instead of modifying each individual user account. Playback Groups can contain resources from multiple recorders, but cannot be used in a recording schedule.



Access the **Administration » Playback Groups** tab and create **Playback Groups** of agents after configuring the agents. Check that dashboard data populates once calls are taken by agent members of playback groups.

The grid includes the following columns:

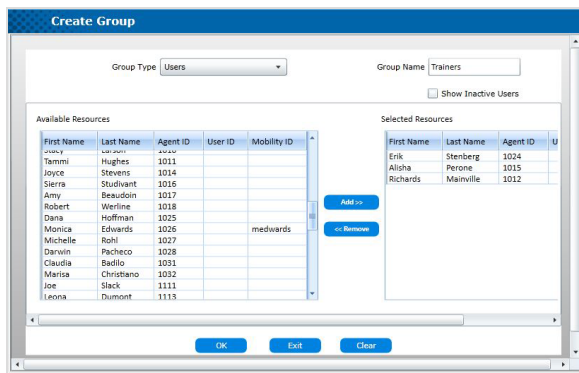
- **Group Name:** A description to help others know the nature of the group.
- **Group Type:** The type of resources inside the group. The options are by agent, port, mobility user or dialed numbers.

Groups have the following properties:

- Update user account permissions globally by assigning each user access by Playback Group. (Administration » Users)
- The Group can also be used to easily search for calls in the Playback Log (Recording » Custom Search).
- Running reports on a specific group can provide both overall and detailed information about how well the group compares with other groups. (Reports » New Report)

- Sorting is available by selecting the header at the top of each column. The first click will sort ascending, the second click will sort descending, and the third click will return to the default sort.
- Quick filters are available to refine a search. Click on the Filter Icon in the header of each column to select filter parameters for that column.

Create a Playback Group



To create a new Playback Group, use the following steps:

1. Access the **Administration » Playback Groups** tab.
2. Select the **New Group** icon from the ribbon bar and the Create Group window will appear.
 - a. Select a **Group Type** from the drop down box.
 - **Users:** Group of Users. If Inactive Users should be included in the Group, select the Show Inactive Users checkbox. Any users that have been deactivated will show in the list.
 - **Dialed Numbers:** Group of incoming Dialed Numbers
 - b. Enter the name of the group in the **Group Name** box.

WARNING: A Playback Group Name should not include special characters such as a comma (,) or a semicolon (;) as a custom searching and reports will fail.

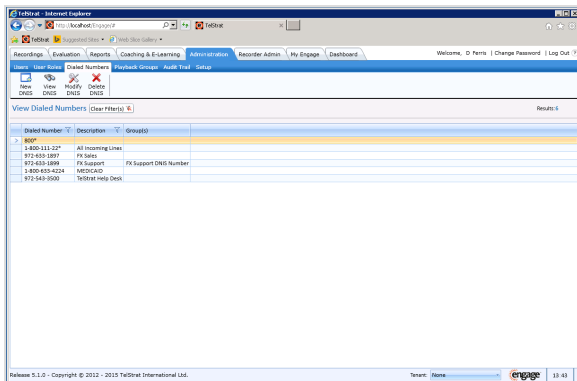
3. Select the appropriate resources from the **Available Resources** table.

4. Click the **Add** or **Remove** button, or drag/drop them to move selections to the *Selected Resources* table.
5. Select **OK** when complete and then select **OK** again from the **Create Group Confirmation** window.
6. The Create Group window will remain open to create another group. If complete, **Exit** this window.

NOTE: An Administrator may create or make changes to a role using any available feature permissions; however a non-administrator user is restricted in creating new roles with only permissions they are assigned to by their user account. For example, if a Local Admin user does not have permission for Recorder Ports, they will not be able to create a role that has the Recorder Ports permission.

6.10.4 Dialed Numbers

Dialed Numbers are not typically configured for new deployments.



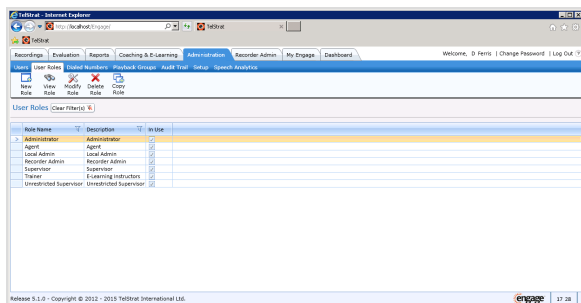
They are typically only required for outsourcer customers who have the same agents take inbound calls for multiple clients if users need to be able to listen to calls for only some clients.

For example, an outsourcer has five (5) clients and some agents take calls for multiple clients. If the end client requires that they be able to listen to calls, then they must be given a user account that only has access to their inbound dialed numbers.

6.10.5 User Roles

Refer to the Engage **Web Client Administrator's Guide** for more detailed information on User Role setup.

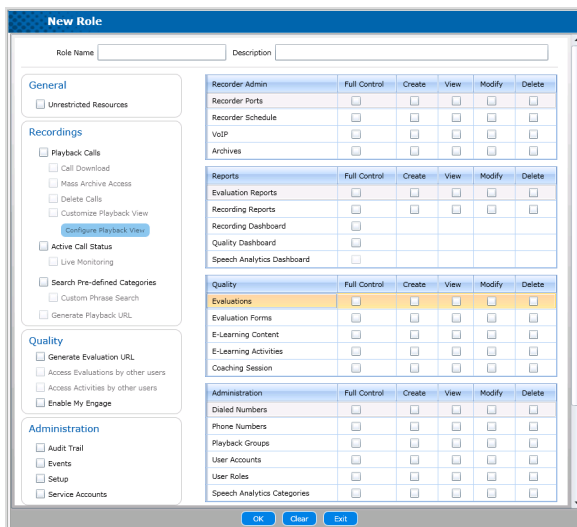
Configure the User Roles using the **Administration » User Roles** tab of the Web Client. This should be done with the customer IT department if possible, but can be adjusted during or after training. It's very important to know which users should be given which roles to minimize any reconfiguration. Start with the built-in roles, and these roles can be copied if needed.



Key questions to ask include:

- How many types of user access are there? There are typically some administrators, supervisors, agents, and possibly QA. A role is required for each class of user.
- Unrestricted Resources: Which users should be able to playback any call recording? These users should be given a role with Unrestricted Resources.
- Call Download: Which users should be able to download calls? Most deployments are very sensitive to allowing users to download .WAV files. Engage supports URL playback which supports emailing a URL of a call recording, and this recording can only be played back by users that have authenticated access to the customer network. URL Playback is suggested for most users, and only a few should be granted the Download Calls permission.
- Delete Calls: Which few users should be given permission to delete calls? Note that the audit trail keeps track of which users are deleting which calls.
- Were Quality licenses purchased?
 - Which users should be able to manage forms?
 - Which users should be able to manage Evaluations?

- Enable the Access Evaluations by other Users by default. This lets an evaluator see evaluations created by other evaluators. If the agent can logon this MUST be enabled or they will not see any evaluations created for them.
 - Which users (agents) should only be able to View evaluations? Be sure to enable Access Evaluations by Other Users for the agent role.
- Administration and Recorder Admin are typically granted to administrators only.
 - Which users require access to run reports?
 - Which users require access to the dashboards?



Role Name	Description	Full Control	Create	View	Modify	Delete
Recorder Admin						
Recorder Admin		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Recorder Parts		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Recorder Schedule		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VoIP		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Archives		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Reports						
Evaluation Reports		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Recording Reports		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Recording Dashboard		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Quality Dashboard		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Speech Analysis Dashboard		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Quality						
Evaluations		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Evaluation Forms		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E-Learning Content		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E-Learning Activities		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Coaching Session		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Administration						
Dialed Numbers		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Phone Numbers		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Playback Groups		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User Accounts		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User Roles		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Speech Analytics Categories		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Use [Administration » User Roles » New Role](#) tab to create and configure User Roles.

6.10.6 User Configuration

Refer to the Engage **Web Client Administrator's Guide** for more detailed information on User Configurations and setup.

User accounts are required for users to logon and use the Web Client. Users must have user names, IDs, passwords and are assigned to roles and groups with specific features. If agents take calls and can also logon to Engage, this release requires creating the user in the [Administration » Users](#) tab and in the [Administration » Agents](#) tab.

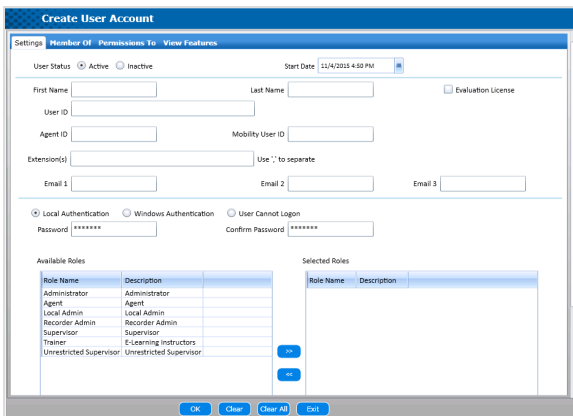
Create a new user:

To create a new user, go to the Web Client's [Administration » Users » New User](#) and get the [Create User Account » Settings](#) tab:

User accounts should be setup after first configuring the resources that can be assigned to user accounts (Agents, Mobility Users, Dialed Numbers, Playback Groups and/or Recorder Groups). The fields and their data are described as:

- **User Status:** Select Active or Inactive.
- **Start Date:** Selectable drop down field for entering a user's start date and time.
- **Last name:** Person's LAST name.
- **First name:** Person's FIRST name.
- **Evaluation License:** If Engage Quality is included in the deployment, an evaluation license can be assigned to a user. Evaluation Licenses are required to be assigned to agents only if other non-call related activities may need to be evaluated.
- **User ID:** Enter the account the user uses to logon to their workstation.
- **Agent ID:** This is intended for agents that are able to logon to Engage. Enter the contact center ID for the agent so the agent can listen to their calls, view their evaluations (if allowed).
- **Mobility User ID:** The mobility user ID to be used by the user to logon to the Cisco, Microsoft Lync or Mitel system.
- **Extensions:** The telephone stations being recorded for this user
- **Email1 / Email2 / Email3:** Optional and can be used so Engage can send evaluation alerts to evaluated users, coaching alerts to coached users, and e-Learning alerts when e-Learning assignments are made to a user.
- **Authentication type:** *Local Authentication*(Engage) or *Windows Authentication*. Windows Authentication is preferred for domain networks to remove the need to manage a password within Engage.

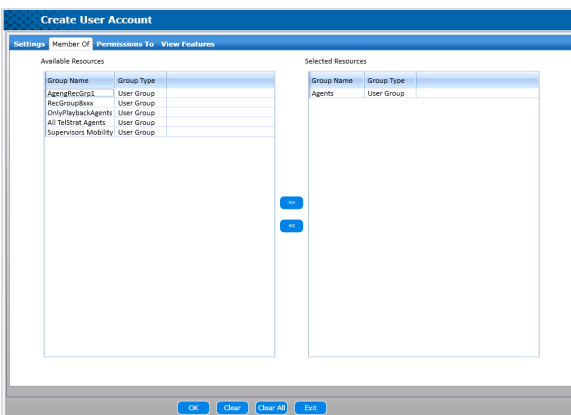
- **User Cannot Logon:** When selected, this button prevents the user from logging onto the Engage system until the button is released.
- **Password:** This is either not required (Windows Authentication) or can be set to the default password which is setup in [Administration » Setup » Engage Password Security](#).
- **Confirm Password:** Passwords entered here must be confirmed.
- **Available Roles:** Select one role for each user. Engage supports multiple roles, but one role is preferred. Highlight the role and click on the » symbol to move the role to the Selected Roles column.
- **Selected Roles:** When a role is selected for a user, it is listed in this column.
- **Assign resources :** Unless the role includes Unrestricted Resources, or the agent is using My Agent ID, you must assign resources to the user account. Refer to the User Guide documentation if needed.
- **View Permissions:** This can be used to check which permissions are granted to the user role(s) assigned to this user based on the selected role(s).



Assign User to a User Group:

Users may be a member of a team or group. Instead of entering each person in the Users tab and also adding them to a Playback Group, the tab in the [Creating User Account » Member of](#) window allows the administrator to add the user to a Playback Group as they create a user. The fields and tables of the Member of tab are:

- Available Resources: Contains a list of groups or teams to assign users to.
 - Group Name: A unique group name.
 - Group Type: Signifies the purpose of the group.
- Selected Resources: Groups names that the user has been assigned to.
 - Group Name: A unique group name the user has been assigned to.
 - Group Type: Signifies the purpose of that group.

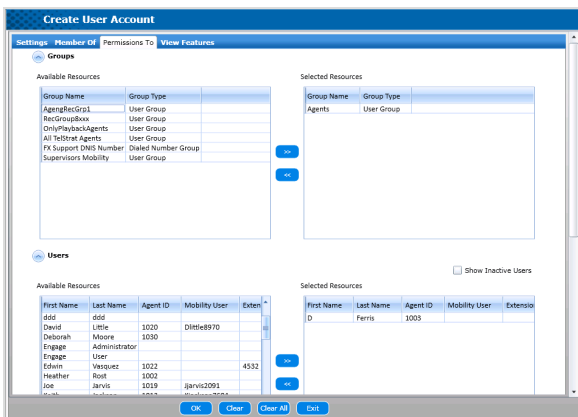


Assign Permissions to a User

Use the **Permissions to** tab to assign individual user accounts access to specific playback groups, or incoming dialed numbers will selectively designate each user access only certain calls or evaluations. Any call not taken by one of these resources will not be available for them to search, playback or evaluate. If the user has Unrestricted Resources, the Groups, Users and Dialed Number resources tabs will be greyed out.

- Group assignments organize agents or ports into logical groups. Group assignments are used to assign a specific Playback Group in order for the user to view. Users that have been assigned a group can still search for individual members of that group.
- User assignments can be used so a user can view calls for a specific set of other users. Typically used when a group of users is not available or only a partial set of users is needed such as all users that started in the last 30 days.

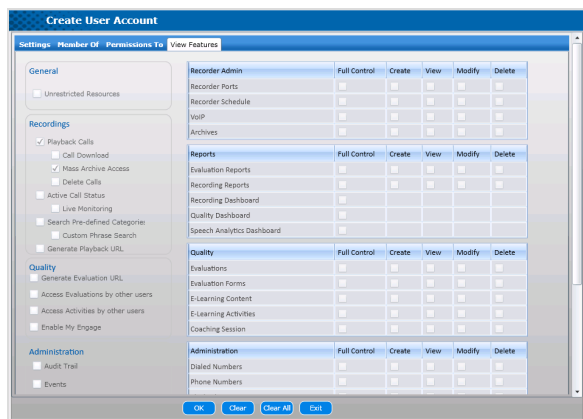
- Dialed Number assignments can be used so a user can view calls to a specific list of dialed numbers.



View a User's Features

View the sum total of permissions assigned to the user by going to the **View Features** tab. Permissions on this tab cannot be modified. To change the permissions for a user, change their assigned roles, or modify the permissions for an assigned User Role.

For more detailed information on setting up Users, Groups, Permissions and to view a users features, please refer to the **Web Client Administration Guide**.



7 Installation Completeness Checklist

With the completion of all installation tasks regarding the Engage server, it is time to check the systems various components to make sure it is operating correctly.

7 Engage Installation Completeness Checklist

Customer Name:

Customer Project #:

1	Security Scans on Engage Recorders	
	Verify restart of TelStrat Voice Recording Service after scans	
2	Apply Anti-Virus Real-time Scanning Exclusions to:	
	<i>C:\Program files (x86)\TelStrat</i> directory	
	SQL DB and log file directories	
	TelStrat .WAV cache directories	
	Proxynetworks screen capture cache directories	
3	Customer Worksheets	
	Verify Agent IDs and Names are correct	
	VoIP Module Mapping, show customer how to do this	
	If Screen Capture present, verify /port/workstation mappings	
	If On-Demand present, verify workstation mappings	
4	Verify VoIP Module Configuration	
	Check <i>VoIPInfo.log</i> for unnecessary registrations	
	Ensure Auto-Learning is enabled, when possible.	
	Check procured virtual phone for every softphone configured	
	Avaya Red: Check that softphones not over-provisioned	

5	Verify Licenses	
	Double check the number of licenses for features against order	
	Make sure .c2v files are submitted, captured and stored	
6	Verify Engage is connected	
	Logon to Web Client and verify Recorder status is Online	
7	Verify Engage is Recording	
	Configure a Recording Schedule	
	Make test calls on phones within recording schedule	
	Open Web Client and verify test call was recorded	
8	Verify Email Alerts are Received	
	Use the Web Client Test Email button, check delivery of email	
	Verify accounts and emails are configured properly	
	Suggest the use of SMTP to the customer	
9	Verify these TelStrat Engage Services are started	
	TelStrat Voice Recording Service	
	.Net TCP Port Sharing	
	SQL Server (InstanceName)	
	TelStrat Centralized Error Service	
	TelStrat Engage Alarm Service	
	TelStrat Engage Annotation Service	
	TelStrat Engage Configuration Service	

	TelStrat Engage Dashboard Service	
	TelStrat Engage Download Service	
	TelStrat Engage Mass Archive Service	
	TelStrat Engage Notification Service	
	TelStrat Engage Search Service	
	TelStrat Engage VoIP Configuration Service	
	TelStrat SIP Server	
	TelStrat VoIP Engine	
	Check the version of the <i>DownloadService.exe</i>	
10	Verify SQL Dedication (one of the following)	
	SQL memory enforces a max limit if Local SQL	
	SQL is running on a dedicated SQL server (no other Engage apps)	
11	Verify Screen Capture, if present	
	Check available licenses to enable Screen Capture are present	
	Telephones are associated with named workstations	
	Workstations have Proxy Pro Host installed	
	Engage Capture Server running Proxy Pro Gateway Administrator	
	Engage is programmed with mapping of workstations to phones	
12	Verify Live Monitoring, if present	
	Use Web Client to check that Live Monitoring is operational	
13	Validate Manual SQL Backups	

	Watch customer launch and capture manual SQL backups	
14	Validate Encryption Functionality	
	Test key import/export process and functionality	
15	Voice Recording Configuration Check (CommSrv)	
	On Voice Recording Database tab, check SQL settings are correct	
	On Cache tab, check cache partitioning	

7.1 Security Scans on Engage Recorders

Security scanning of Engage recorders can cause issues with performance and recordings. The process and its effects must be understood before running security scans on the Engage Recorder.

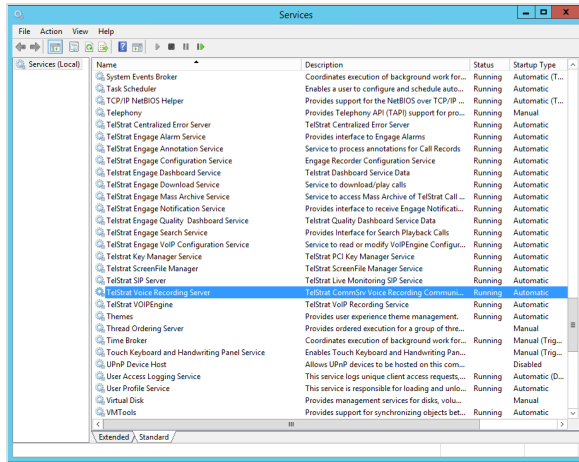
Security scanning is used to seek out flaws and security risk opportunities (bugs, misconfigurations, lack of updates, etc) to exploit on a network or host system. Two common types of Security Scanners are:

- Host Security Scanners: Tests for security risks on a single system starting with an authorized account.
- Network Security Scanners: Looks for security risks from one system from another, connected to the same network.

In normal operation, the Engage Recording Server is actively recording all stations and/or all trunks, all the time. This steady stream of voice and call event data is collected, sorted and stored within the server's systems. When the server is being scanned, there is an increase in processing required and overhead-type data unrelated to recordings that is flowing in and out of the server which can cause service issues and adversely affect recordings.

All companies will have different business requirements regarding security scanning, ranging from those that must scan everyday to those that are not performing scans at all. Regardless of the requirements, follow this procedure to stop the recording service during scans to minimize recording issues with Engage.

After running security scans on Engage servers:



Stop the TelStrat Voice Recording Service:

1. Logon to the Engage server.
2. Navigate to the *Services* portion of the **Server Manager**.
3. Scroll down the list and find **TelStrat Voice Recording Service** and right-click on it.
4. Select **Stop** and note that the Status should change from **Running** to an empty field.
5. **Run the security scans at this time.**

Restart the TelStrat Voice Recording Service:

1. After security scanning is completed, get back on the **Services** window of the Server Manager.
2. Locate the **TelStrat Voice Recording Service** entry in the list and right-click on it.
3. Click on **Start** and note the Status change from an empty field to **Running**.
4. Logon on to the Web Client and *verify call recording has resumed*.

7.2 Verify Anti-Virus Real Time Scanning Exclusions

Real-time protection, on-access scanning, background guard, resident shield, autoprotect, and other synonyms refer to the automatic protection provided by most antivirus, anti-spyware, and other anti-malware programs.

This monitors computer systems for suspicious activity such as computer viruses, spyware, adware, and other malicious objects in 'real-time', in other words while data is loaded into the computer's active memory such as when inserting a CD, opening an email, or browsing the web, or when a file already on the computer is opened or executed.

The scanning to set the exclusion from is the real time or on-access scanning, such as scanning a file when it is created or new to the server.

On demand (scheduled) scanning of files when the system is idle or nearly idle would be fine.

It is recommended to exclude the following from real time scanning:

- **C:\Program files (x86)\TelStrat** directory
- SQL DB and log file directories
- TelStrat .WAV cache directories
- Proxynetworks screen capture cache directories when using screen capture

7.3 Verify Customer's Input Data vs. Customer's Worksheet Data

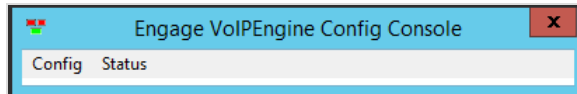
Check that the customer's deployment data is correctly inserted into the databases, including:

- Agent IDs and names of agents.
- VoIP module mappings (show customer how to import/export mappings for backup.
- If using screen capture, verify work station mappings.
- If using on demand feature, verify work station mappings.

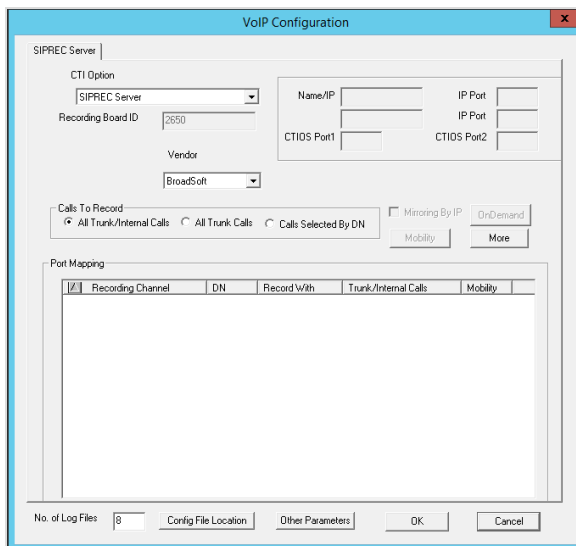
7.4 Verify VoIP Module Configuration Meets Requirements

Verify that the VoIP module configuration meets the customer's specifications and needs.

Use the **Engage VoIP Engine Config Console** to configure the platform that the Engage Recording Service will integrate with.



Each vendor's platform has unique elements, settings and configurations to work with Engage properly. Use the **Config** menu command to call up the **VoIP Configuration » CTI Option** drop-down menu to select the vendor's platform for the Engage end of the recording connection. This is an example of a BroadSoft VoIP system deployment.



After configuration, check for any obvious issues that may be preventing recording. Usually, these issues can be traced back to the initial setups and configurations.

Some examples of out-of-specification issues to look for are:

- Too many softphones for an Avaya red installation have been configured.
- Each customer has procured a virtual phone in the Avaya CM for each soft phone configured.
- Check VoIPInfo.log making sure there are not unnecessary registrations (ex. soft phone registration failure events).
- Ensure auto learning is enabled, whenever possible.

7.5 Verify Licenses



Follow these quick steps to verify licenses:

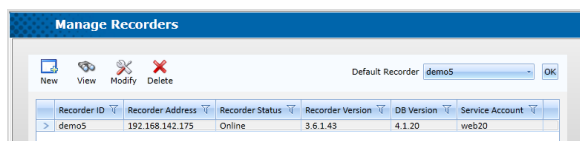
1. Once logged into the Engage JAVA Client, go to **Server » License Management**
2. The Engage Serial Number will be at the top of the window and a chart will list all the potential licenses that are available in the Engage system.
3. Double check the number of licenses for each feature against the Engage features that were purchased.
4. Make sure final c2v files are submitted, captured and stored.

7.6 Verify Engage Is Connected

Login to the Engage Web Client to verify that the databases and the recording software are connecting to the Engage Server.

Go to **Web Client » Administration » Setup » Manage Recorders** and make sure all Recorder Statuses are showing Online.

Need to troubleshoot the issue if a Recorder shows **offline**.



Recorder ID	Recorder Address	Recorder Status	Recorder Version	DB Version	Service Account
> demo5	192.168.142.175	Online	3.6.1.43	4.1.20	web20

7.7 Verify Engage is Recording

1. Configure a Recording Schedule that includes the phone to test the recording on.
2. TelStrat installers can also use a third-party call simulation software application.
3. Make a test call to the phone within the recording schedule.
4. Open the Web Client and the JAVA Client to see if the call was logged successfully.

If one or both of the clients did not receive the call successfully, contact the TelStrat Support Team.

7.8 Verify Email Alerts are Received

1. Navigate to *Recorder Admin » Email* tab and then select the *Test Email* icon to verify a test email can be sent.
2. Verify proper service account and emails are configured to customer satisfaction.
3. Suggest the use of the ability for SMTP monitoring to the customer.

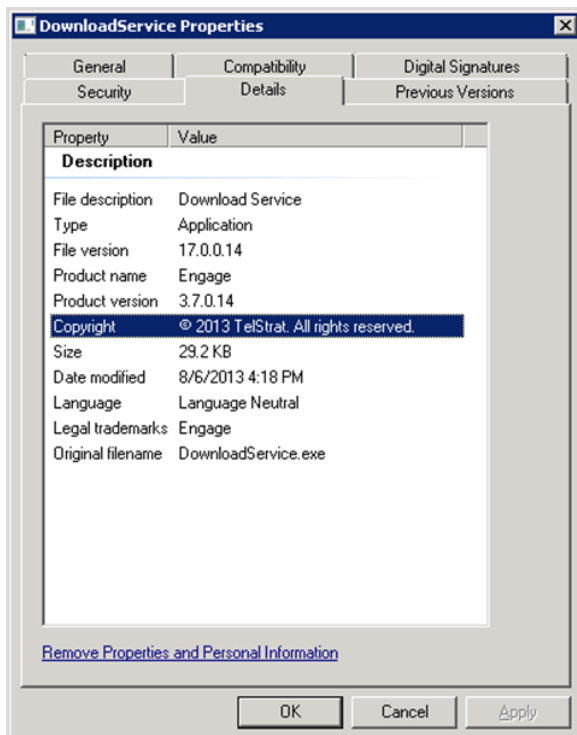
7.9 Verify Engage Services are Started

1. From the Windows desktop of the Engage Server, click *Start » Settings » Control Panel » Administrative Tools » Services*.
2. Scroll down to *TelStrat Voice Recording Server*, if the service is not started select *Start*.
3. Also verify that all these services are *Started*.
 - .Net TCP Port Sharing
 - SQL Server (InstanceName)
 - TelStrat Centralized Error Service
 - TelStrat Engage Alarm Service
 - TelStrat Engage Annotation Service
 - TelStrat Engage Configuration Service
 - TelStrat Engage Dashboard Service
 - TelStrat Engage Download Service

- TelStrat Engage Mass Archive Service
- TelStrat Engage Notification Service
- TelStrat Engage Search Service
- TelStrat Engage VoIP Configuration Service
- TelStrat SIP ServerTelStrat VoIP Engine

Check the version of the Download service:

1. Go to the following sub-directory *c:\program files (x86)\telstrat\engage\SOA Services\Download*.
2. *Right-click* properties on the *DownloadService.exe* application file.
3. Be sure to not accidentally check the properties of the *DownloadService.exe.xml* configuration file.
4. Trace Logs must be Enabled.



7.10 Verify SQL Dedication

Verify one of the following:

- SQL Memory enforces a maximum limit if Local SQL.
- SQL is running on a dedicated SQL server with NO other Engage applications.

7.11 Validate Screen Capture Recording

Refer to the [SETUP - SCREEN CAPTURE](#) document for details.

7.12 Verify Live Monitoring - if deployed

Live monitoring is the ability to listen to a conversation while it is in session and being recorded.

Use the Web Client Online Help system to determine if Live Monitoring is operating correctly.

Live Monitoring is fully documented in the online [WEB CLIENT USER GUIDES](#).

7.13 Validate Manual SQL Backups

The customer should launch and monitor the completion of a manual backup of the Engage SQL databases to show that this function operates correctly. Refer to the [MAINTENANCE - SQL](#) document for details.

7.14 Validate Encryption Functionality

Test and validate that the Encryption key import/export process and functionality works correctly, if installed.

Refer to the [SETUP - ENCRYPTION GUIDE](#) for more details.

7.15 Voice Recording Configuration Check

On the Voice Recording Server Communications Server tool, check the following:

- On the **Voice Recording Database** tab, check that the *SQL Express* or *SQL* settings are correct.
- On the **Cache** tab, check the *Cache partition* (one for new installations).

8.1 Web Client Administration Setup

This section of the installation configures user access for playing back calls and accessing the other WFO features of Engage.

8.2 Playback Log

Date	Start Time	End Time	Status	Rec Duration	Hold Duration	User First	User Last	Agent ID	Extension
8/17/2015	11:15:15 AM	11:15:45 AM		00:30		Barbara	Foley	1007	4584
8/17/2015	11:15:15 AM	11:15:45 AM		01:20		Charles	Lebrun	1006	4583
8/17/2015	11:15:15 AM	11:15:45 AM		00:50		Yulanda	Parley	1004	4582
8/17/2015	11:14:50 AM	11:15:15 AM		00:45		ID	Peris	1002	4580
8/17/2015	11:14:50 AM	11:15:15 AM		00:45		Heather	Root	1002	4579
8/17/2015	11:14:45 AM	11:15:15 AM		00:30		Joe	Black	1111	4578
8/17/2015	9:26:38 AM	11:15:03 AM	11:27	00:00		Joe	Black	1111	4578
8/17/2015	9:23:39 AM	9:23:39 AM	6:14	00:00		Joe	Black	1111	4578
8/17/2015	9:00:35 AM	9:07:09 AM		00:34		Joe	Black	1111	4578
8/17/2015	8:44:48 AM	8:50:26 AM		00:34		Joe	Black	1111	4578
8/4/2015	8:00:27 PM	8:00:23 PM		00:51		Carl	Peris	1114	4582
8/4/2015	8:00:22 PM	8:00:20 PM		01:01		Alfred	Ornela	1114	4581
8/4/2015	8:00:17 PM	8:04:17 PM		00:25		Leanne	Quinn	1113	4580
8/4/2015	8:00:07 PM	8:06:30 PM		01:20		Joe	Black	1111	4578
8/4/2015	8:00:02 PM	8:06:29 PM		00:52		Joe	Black	1111	4578
8/4/2015	8:00:28 PM	8:06:34 PM		01:01		Yulanda	Parley	1004	4581
8/4/2015	8:00:13 PM	8:07:25 PM		01:51		ID	Henry	1002	4580
8/4/2015	8:00:18 PM	8:07:25 PM		01:57		Heather	Root	1002	4579
8/4/2015	8:00:13 PM	8:00:44 AM		01:21		Charles	Lebrun	1006	4581
8/4/2015	8:00:13 PM	8:03:09 PM		00:52		Marisa	Edwards	1006	4582
8/4/2015	8:00:08 PM	8:03:14 AM		01:01		Chris	Steffan	1002	4579
8/4/2015	8:00:05 PM	8:04:24 PM		01:50		Eric	Stanberg	1004	4580
8/4/2015	8:00:00 PM	8:03:14 AM		00:26		Joe	Black	1002	4579
8/4/2015	8:00:01 PM	8:01:26 PM		00:24		Edwin	Leibman	1002	4579
8/10/2015	4:00:15 PM	4:00:54 PM		00:37		Barbara	Foley	1007	4584
8/10/2015	4:00:15 PM	4:00:11 PM		00:52		Yulanda	Parley	1004	4582
8/10/2015	4:00:15 PM	4:04:22 PM		01:01		Jane	Sythetic	1004	4581
8/10/2015	4:00:15 PM	4:04:40 PM		01:25		Jane	Smith	1002	4578
8/10/2015	4:00:15 PM	4:04:40 PM		01:25		Charles	Lebrun	1006	4583

- Recent Calls

- Recent calls fills the page upon user logon. New call recordings will only appear if you select *Recent Calls* again.
- Playback a call from IE to verify MP3.
- Delete calls (if user account is enabled). An audit trail record tracks who is deleting which calls.
- Quick filters and clear filter. Quick filters apply only to the subset of calls that are loaded.
- No. (number) of Records defaults to 200. Can be set up to 10,000 but will increase loading time

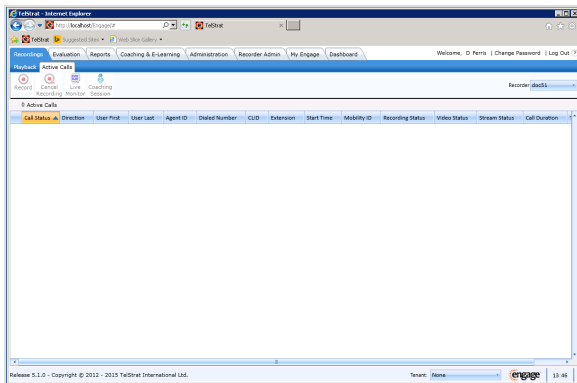
- Playback Log Grid

- Go over the columns.
- Status: Search for calls with a duration of 5 to 99999 seconds with a recording duration of 0 to 0 seconds. If any calls are found, show the Status icon and how it shows the calculated call duration. Red icons are present for 0 second records of calls > 5 seconds.

- **Custom Search**

- Show a basic time and date search.
- Search by Agent ID.
- Search by extension.

8.3 Active Calls



The Active Calls window can be used to:

- Verify new calls are recording
- Call Status
- Recording Status
- Stream Status
- Video Status
- Live Monitor Audio
- Live Monitor Screen Capture (if purchased)

8.4 Recorder Administration

Port Number	Port Name	Last Name	Analyze License	Evaluation License	Workstation Mapping	Capture License	On Demand Client Enabled	Delete Key	Pause Key	Grid
0001.000	Screen	Office	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00042	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
0001.001	00010001	00010001	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
0001.002	00010002	00010002	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
0001.003	00010003	00010003	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
0001.004	00010004	00010004	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
0001.005	00010005	00010005	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
0001.006	00010006	00010006	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
0001.007	00010007	00010007	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
0001.008	00010008	00010008	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
0001.009	00010009	00010009	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2100.000	TelStrat	Recruitment	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2100.001	Help Desk	Station A01	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	TS=ELAN2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2100.002	Help Desk	Station A02	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	TS=ELAN3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2100.003	Help Desk	Station A03	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	TS=ELAN3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2100.004	Help Desk	Station A04	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2100.005	Help Desk	Station A05	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2100.006	Help Desk	Supervisor	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2100.007	New Sales	Office S41	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2100.008	New Sales	Office S42	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2100.009	New Sales	Office S43	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2100.010	New Sales	Office S44	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2100.011	New Sales	Office S45	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2100.012	New Sales	Group Supervisor	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2100.013	Installs	Station B01	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2100.014	Installs	Station B02	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2100.015	Installs	Station B03	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2100.016	Installs	Station B04	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2100.017	Installs	Station B05	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2100.018	Installs	Group Supervisor	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2100.019	Customer Ser.	Minister	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

The training will include a review of the following tabs of the Web Client:

- **Recorder Admin » VoIP**
 - Add / Manage VoIP devices.
 - Select all VoIP devices from the web client and paste into Excel to keep a record of how the system was initially configured.
- **Recorder Admin » Ports**
 - Port names are recommended for non-agent call recording.
 - Verify any screen capture configuration (workstation mapping).
 - Verify ODRC settings if ODRC is in use (workstation mapping, delete option, pause option).
 - Select all Ports from the web client and paste into Excel to keep a record of how the system was initially configured.
 - Quality licenses should be applied to ports if all phones taking calls can be evaluated.
- **Recorder Admin » Recording Groups**
 - Recording groups are typically only created for deployments that have complex recording schedules that need to reference a group of ports, agents, dialed numbers, or mobility users within the recording schedule.

- **Recorder Admin » Recording Schedule**
 - Verify the recording schedule is set to record all calls or rules are setup as the customer requires.
 - Recording Schedule must reference any Gen2 archives.

- **Recorder Admin » Archive**
 - If the customer requires archiving, setup the archives based on customer requirements. Customers that require different retention policies require an archive per retention duration.
 - Does the customer require that calls are deleted from cache after so many days? Verify Server Config is setup to delete call records and call recordings after so many days.

- **Recorder Admin » Service Accounts**
 - There should be a Live Monitor, and Web Client service account plus default and one or two system administrators.
 - Add a distribution list or individual email destinations for the customer to monitor system events.
 - Add the Engage distribution list SystemAlerts@telstrat.com to receive alerts for new installations or upgrades unless a specific account email address has been created.

- **Recorder Admin » Events**
 - Test Email and verify the customer admin receives the alert. Verify TelStrat receives the email alert.
 - Show the events to the customer including the following:
 - *Server Ready to Receive Calls*: This should only happen when expected.
 - *VoIP Disconnected / Connected*: This should only happen at system start-up. If this occurs for unknown reasons it indicates a recording fault.
 - *VoIP Recording Empty*: This alert should be setup in Server Config under Misc. tab to only generate for calls > 10 seconds. Explain that this alert generates if Engage receives a call that exceeds 10 seconds but did not create a recording. Search for calls that may have generated this alert and show the Red icon in the Status column in the Playback Log. Very short calls of

a few seconds may not have time to setup the call recording and generate false error alerts. These are filtered out with the Server Config setting.

8.5 Administration

User ID	First Name	Last Name	Extension(s)	Agent ID	Mobility User ID	Evaluation License	User Role(s)	Email Account(s)	Status	Last Logon
1111										
1112										
1113										
1114										
1115										
1116										
1117										
1118										
1119										
1120										
1121										
1122										
1123										
1124										
1125										
1126										
1127										
1128										
1129										
1130										
1131										
1132										
1133										
1134										
1135										
1136										
1137										
1138										
1139										
1140										
1141										
1142										
1143										
1144										
1145										
1146										
1147										
1148										
1149										
1150										
1151										
1152										
1153										
1154										
1155										
1156										
1157										
1158										
1159										
1160										
1161										
1162										
1163										
1164										
1165										
1166										
1167										
1168										
1169										
1170										
1171										
1172										
1173										
1174										
1175										
1176										
1177										
1178										
1179										
1180										
1181										
1182										
1183										
1184										
1185										
1186										
1187										
1188										
1189										
1190										
1191										
1192										
1193										
1194										
1195										
1196										
1197										
1198										
1199										
1200										
1201										
1202										
1203										
1204										
1205										
1206										
1207										
1208										
1209										
1210										
1211										
1212										
1213										
1214										
1215										
1216										
1217										
1218										
1219										
1220										
1221										
1222										
1223										
1224										
1225										
1226										
1227										
1228										
1229										
1230										
1231										
1232										
1233										
1234										
1235										
1236										
1237										
1238										
1239										
1240										
1241										
1242										
1243										
1244										
1245										
1246										
1247										
1248										
1249										
1250										
1251										
1252										
1253										
1254										
1255										
1256										
1257										
1258										
1259										
1260										
1261										
1262										
1263										
1264										
1265										
1266										
1267										
1268										
1269										
1270										
1271										
1272										
1273										
1274										
1275										
1276										
1277										
1278										
1279										
1280										
1281										
1282										
1283										
1284										
1285										
1286										
1287										
1288										
1289										
1290										
1291										
1292										
1293										
1294										
1295										
1296										
1297										
1298										
1299										
1300										

The training will include a review of the following administration tabs of the Web Client:

Admin » Users

- Show the administrator how to Add / Manage User Accounts.
- If agents will logon to retrieve their calls, set **My Agent ID** for any agents.

Admin » User Roles

Go over the User Role Permissions for roles that are in use.

Discuss with the customer which roles should have the following permissions:

- Unrestricted Resources – Which users should be able to playback any call recording? If there are multiple QA or top level supervisors, then be sure to grant Unrestricted Resources permission to roles assigned to those users.
- Download Calls – Disable except for a few users

- Playback URL – Suggest enabling this for most users so they can email URL links to calls which are secure. These URLs can only be played back by recipients that have access to the customers network.
- Delete Calls – What users if any should have this permission.

Admin » Agents

- Explain that agent names populate based on call records that have an Agent ID.
- Agent names can be added after the call is recorded and they will then appear for next user logon in the Playback Log
- Agent ID recycling is not supported in this release. The currently provisioned agent name will appear in the Playback Log
- Set Agent ID to appear in all call records in server config under Misc. tab.
- Evaluation licenses should be applied to agents unless there are too many agents due to multiple shifts (use Port licenses instead).

Admin » Dialed Numbers

This is typically only required for outsourced contact centers that share agents across multiple projects or customers. This can be used so a supervisor might only have rights to playback calls for a pre-defined list of dialed numbers (incoming numbers) for a particular project or customer.

Admin » Playback Groups

- Playback Groups can contain agents, dialed numbers, mobility users from multiple call recorders. Recording Groups are stored on the recorder and cannot contain resources from multiple recorders. Recording Groups can be referenced by a recording schedule or for assignment to a user account, but Playback Groups can only be used for assignments to a user account.
- Agents should be placed into Playback Groups and then assigned to any supervisors that are not granted the Unrestricted Resources permission.

- Agent groups are needed for the dashboard to display data by group and to compare agents within a group.
- Consider creating an “All Agents” group especially if no business users were granted Unrestricted Resources permission.

Audit Trail

- Show how the audit trail tracks who is playing back, live monitoring, or deleting calls. The call is tracked as well.

Setup Tab consists of these areas:

Manage Recorders

- View the recorder connection. Show how the web client connects to the recorder using a service account, and the recorder database location is listed to help find it for SQL backups

Database

- This tab shows the location of the application (web) database

Email Settings

- Review the SMTP server information located here and verify the same information is configured in Server Config under Email on the recording server.
- Configuring this via the web client will also push the same configuration to Server Config Email tab.
- The web setup SMTP settings are used for emailing calls, evaluations, or reports.
- Server Config email setting is used for emailing system events.

Display Settings

- Hide ACD Agents: Unchecked by default. Select if this is a non-agent deployment.
- Hide Mobility Users: Un-check only for Cisco UCM deployments if the customer uses extension mobility. Logoff and logon to the web client to add the Admin > Mobility Users tab
- Hide Find Related Calls : Un-check for Cisco UCM, Avaya ACM, CS 1000, and ShoreTel. Leave set for all others. If un-checking, then logoff and logon again so Tracking ID is available as an available column.
- Configure Default Playback View and explain that each role can be set as well.
- Un-select port names or move to the right past agent name
- Typical recommended setup is for a contact center:
 - Date
 - Start Time
 - End Time
 - Recording Duration
 - Direction
 - CLID
 - Dialed Number
 - Direction
 - Agent First
 - Agent Last
 - Agent ID
 - Remark1
 - Remark2
 - Recording Status
- Remove any unused columns such as encryption, screen capture, or archive status.

- Users will not be updated unless they select Restore Default View from Playback Log settings.

Playback URL Settings

- Verify Enable URL Playback is enabled

Local Password Security

- Configure with the customer if users will be using local authentication

Application Settings

- Review the inactivity timer & web content storage folder

8.6 SQL Backups

Discuss SQL backups with the administrator.

- Will the customer be setting up a periodic SQL backup?
- Key databases to backup include Config, SRecordingCache, and Engage.

8.7 Support

- **Software Updates**
 - Service affecting issues are typically resolved in a patch upon request.
 - Periodic maintenance releases are released every 2-3 months as needed to roll-up patches into a single release.
- **Parature Ticket Process**
 - Administrator training by the trainer will cover the Parature ticket process.
 - Until the administrator training is provided, any issues found are managed through the installation ticket or new tickets are created by the software provider.

9 Monitoring

Once the installation is complete, the monitoring phase begins. The installation team will proactively monitor the system for five (5) business days. During this time, the system events will be monitored based on email alerts as well as periodic event retrieval.

If unattended access is provided, the system will be checked for call recording failures by running a search for calls longer than 5 seconds that have a 0 second recording duration.

Tasks performed during the monitoring phase include:

Proactive Monitoring and Cleanup with exit criteria:

- Five (5) days clean of unexpected [Recorder Admin » Events](#).
- No unexplained zero (0) second recordings for *call >10 seconds* in duration.

Event Monitoring:

- Create a user account with the installer or auditor's name.
- Installer will add SYSTEMALERTS@TELSTRAT.COM to receive events alerts.
- Run test email and verify we receive the alert.
- Monitor *Recorder Admin > Events* daily and make sure we are receiving email alerts for all events.
- Acknowledge alarms and put notes in the alarm about root cause.
- Verify that Mass Archive delivery path is setup via [Recorder Admin » Archive](#).

Proactive Call Recording Warning Search for five (5) days.

- Run customer search for call duration five (5) to 99999 seconds with recording duration zero (0) to zero (0) seconds for today and yesterday or since new installation or the last time checked.
- Resolve all RED status icons.

Mass Archive: On successive days after initial Engage startup:

- Double check the calls are being archived via MAG 2.
- Access the web client and go to [Recorder Admin » Archive » View](#)
- Check that the storage location status is OK.
- Verify there are no issues with a red ! .

dferris

Upon completion of the monitoring phase of the installation, the install team should remove their email addresses from the customer's system. The **systemalerts@TelStrat.com** email address will need to be removed from the customer's system, as well.

10 Troubleshooting

During the effort to install and configure an Engage Voice Recorder to a vendor's platform, there will be issues that arise. This section contains common troubleshooting issues and recommended fix actions to keep the installation moving.

10.1 Web Server (IIS)

If a user attempts to access the web server and the logon screen does not appear, additional details may be available by logging onto the web server and accessing the web URL directly from the web server itself.

More details are generally provided when accessing the web client from the web server.

This section details common Web Server - Application Server problems and how to troubleshoot them.

10.2 Setting Verbose Web Logs

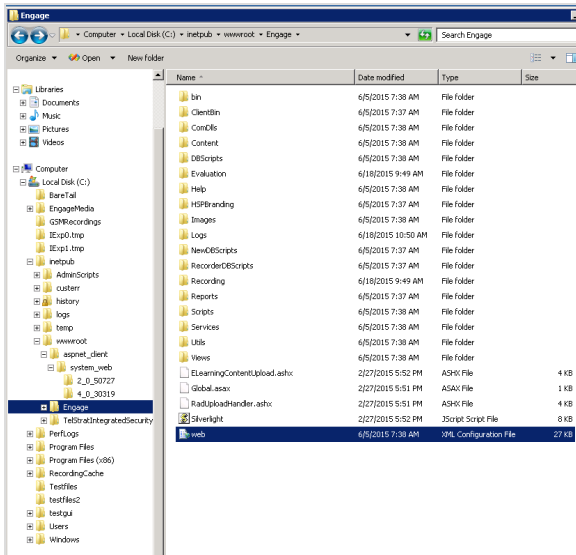
To get more detail in the log commentary (also known as verbose web logs), change this field value in the `web.config` file of the web site.

Enable *verbose web logs* by modifying the `web.config` file level value setting from `ERROR` to `ALL`. This file is located in the web site virtual directory.

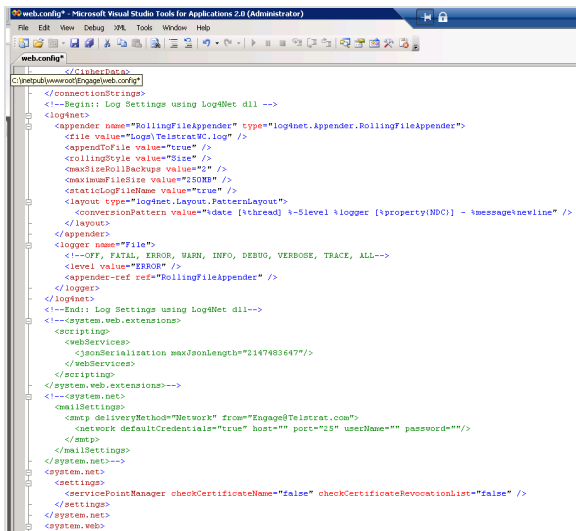
`Web.config` is the main settings and configuration file for an ASP.NET web application. The file is a XML document that defines configuration information regarding the web application. This file stores the information about how the web application will act. The `web.config` file contains information that controls module loading, security configuration, session state configuration, and application language and compilation settings. `Web.-config` files can also contain application specific items such as logging traits.

Warning: Be very careful to note what is changed in this file. Make a copy of this file for reference, if needed, by using the `Save web.config as...` file menu command.

1. On the web server, navigate to this location: `C:\inetpub\wwwroot\Engage`, scroll down to the bottom of the list and look for the `web` (also known as web.config) XML Configuration file.



2. Double-click on it to open the configuration file.



3. Scroll down the file and locate the XML file comment line: `<!--Begin:: Log Settings using Log4Net dll -->`

```

</configuration>
<!--Begin: Log Settings using Log4Net dll -->
<log4net>
  <appender name="RollingFileAppender" type="log4net.Appender.RollingFileAppender">
    <file value="Logs\TelstratWC.log" />
    <appendToFile value="true" />
    <rollingStyle value="Size" />
    <maxSizeRollBackups value="1" />
    <maximumFileSize value="250KB" />
    <staticLogFileName value="true" />
    <layout type="log4net.Layout.PatternLayout">
      <conversionPattern value="%date [%thread] %-5level %logger [%property{NDC}] - %message%nnewline" />
    </layout>
  </appender>
  <logger name="File">
    <!--OFF, FATAL, ERROR, WARN, INFO, DEBUG, VERBOSE, TRACE, ALL-->
    <level value="ERROR" />
    <appender-ref ref="RollingFileAppender" />
  </logger>
</log4net>
<!--End: Log Settings using Log4Net dll-->

```

4. Locate the line `<logger name="File" />`

```

<logger name="File">
  <!--OFF, FATAL, ERROR, WARN, INFO, DEBUG, VERBOSE, TRACE, ALL-->
  <level value="ERROR" />

```

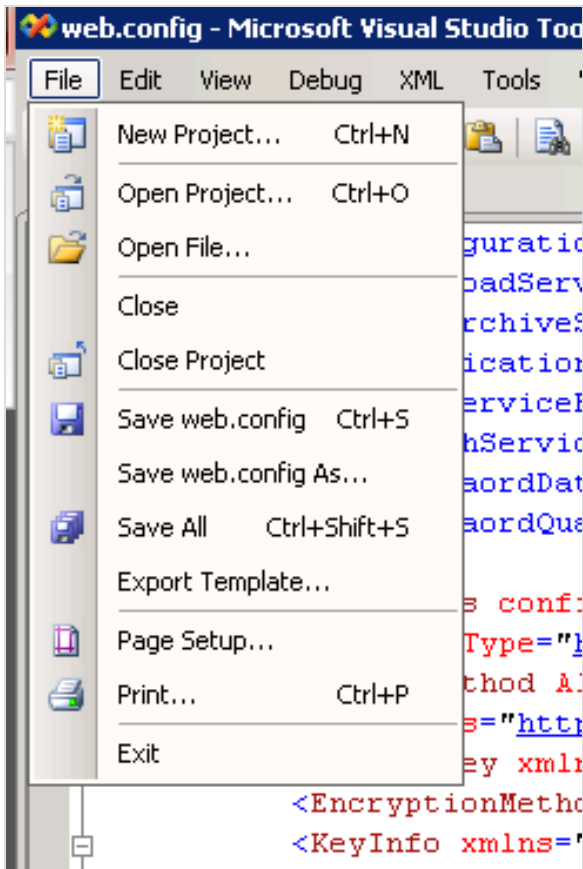
5. Locate the line `<level value ="ERROR" />`, highlight **"ERROR"** and change the value to **"ALL"**.

```

<!--Begin: Log Settings using Log4Net dll -->
<log4net>
  <appender name="RollingFileAppender" type="log4net.Appender.RollingFileAppender">
    <file value="Logs\TelstratWC.log" />
    <appendToFile value="true" />
    <rollingStyle value="Size" />
    <maxSizeRollBackups value="1" />
    <maximumFileSize value="250KB" />
    <staticLogFileName value="true" />
    <layout type="log4net.Layout.PatternLayout">
      <conversionPattern value="%date [%thread] %-5level %logger [%property{NDC}] - %message%nnewline" />
    </layout>
  </appender>
  <logger name="File">
    <!--OFF, FATAL, ERROR, WARN, INFO, DEBUG, VERBOSE, TRACE, ALL-->
    <level value="ALL" />
    <appender-ref ref="RollingFileAppender" />
  </logger>
</log4net>
<!--End: Log Settings using Log4Net dll-->

```

6. Under the File menu, click the **Save web.config** command to save the change.



7. Exit the program.

10.3 Web Server Upgrade Failure - Rolling Back Action

Symptom: Web client instance fails to install – Rolling Back Action

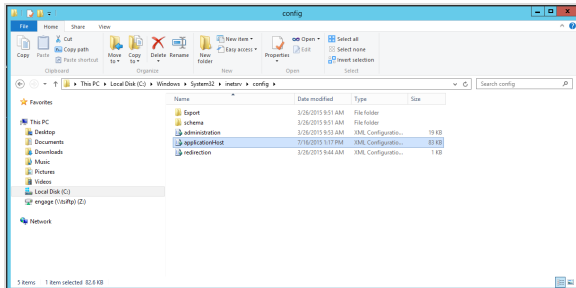
Cause: An issue has been observed during some web server upgrades. During the installation of the web client instance, the software indicates “Rolling Back Action” and then the installation fails. The following work around can be applied:

NOTE: This was discovered on a Server 2012 R2 machine so it is possible that the file could be in a different location for other OS.

Solution: Or the WORKAROUND:

The solution is to manipulate some file content as follows:

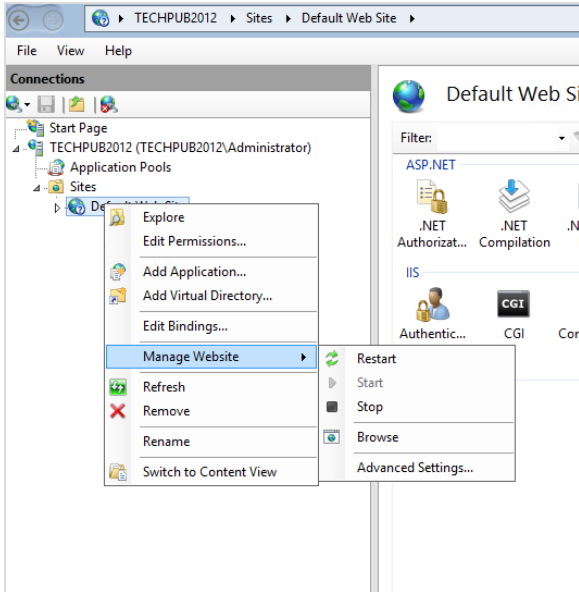
1. Locate the **applicationhost.config** file. This should be found in the folder **C:\windows\system32\inetsrv\config** folder.



2. Edit the **applicationhost.config** file. Find the section for **Engage** (the virtual directory that you are not able to install) and carefully remove it from the file. It should look like this:

```
<location path="Default Web Site/Engage">
<system.webServer>
<handlers accessPolicy="Read, Script" />
<security>
<authentication>
<windowsAuthentication enabled="false" />
<anonymousAuthentication enabled="true" />
.
.
.
<mimeTypeMap fileExtension=".xbap" mimeType="application/x-ms-xbap" />
</staticContent>
</system.webServer>
</location>
```

3. Use the **File** menu to *Save* the changed file.
4. Restart the IIS by navigating to the *IIS Manager » servername » Manage Website* and clicking on *Restart*.



5. Install the Web Client software again using "Engage" as the virtual directory.

10 HTTP Error 500 Web Client Timeout

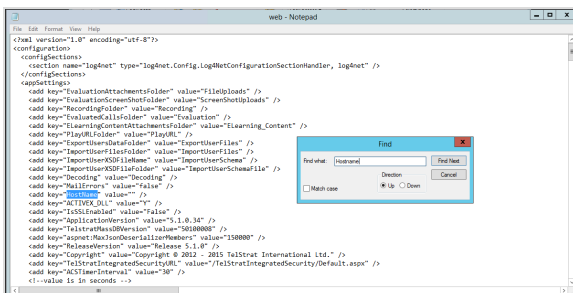
Symptom: When the Engage web server encounters an unexpected condition that prevents it from fulfilling the request by the web client for access to the requested URL, the web client can time-out and/or produce HTTP Error 500s.

Possible Cause: HTTP Error 500s are 'catch-all' errors generated by the web server indicating something has gone wrong, but the server can not be more specific about the error condition in its response to the client.

Solution: The Engage Web Client web.config file will need a change to be implemented on the "HostName" default value.

To make the change, do the following steps:

1. On the server, open the **Notepad** program as an *administrator*.
2. On the drop-down menu in the lower right-hand corner, change Text Documents (.txt) to **All Files**.
3. Open the **web.config** file located on the web server by going to **c:\inetpub\wwwroot\<database>\web**, which is the XML configuration file for the web client.
4. Click on the **Edit** menu command to get the pop-up menu, click **Find** to get the **Find** window and enter **HostName** to locate the specific line of code to change in the **add key=** list.



5. In the **web.config** XML file, the code string to work with is **<add key="HostName" value="" />**.
6. Highlight the two quote marks ("") in the string (ex. **<add key="HostName" value="" />**).

```

File Edit Format View Help
web - Notepad
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="logNet" type="logNet.Config.LogNetConfigurationSectionHandler, logNet" />
  </configSections>
  <appSettings>
    <add key="EvaluationAttachmentsFolder" value="fileUpload" />
    <add key="EvaluationScreenshotsFolder" value="ScreenShotsUpload" />
    <add key="RecordingFolder" value="Recording" />
    <add key="EvaluationAllFolder" value="Evaluation" />
    <add key="LearningContentAttachmentsFolder" value="Learning_Content" />
    <add key="PlayRtlFolder" value="PlayRtl" />
    <add key="ExportUserDataFolder" value="ExportUserFiles" />
    <add key="ImportUserFilesFolder" value="ImportUserFiles" />
    <add key="ImportUserXSDFiles" value="ImportUserSchema" />
    <add key="ImportUserXSDFilesFolder" value="ImportUserSchemaFile" />
    <add key="Decoding" value="Decoding" />
    <add key="NullItems" value="False" />
    <add key="HostName" value="localhost" />
    <add key="CTRL_EXIT" value="Y" />
    <add key="I555Enabled" value="False" />
    <add key="ApplicationVersion" value="5.1.0.34" />
    <add key="TelstratMaxDeserializersMembers" value="500000" />
    <add key="AspectMaxDeserializersMembers" value="150000" />
    <add key="ReleaseVersion" value="Release 5.1.0" />
    <add key="Copyright" value="Copyright © 2012 - 2015 Telstrat International Ltd." />
    <add key="TelstratIntegratedSecurityURL" value="//TelstratIntegratedSecurity/Default.aspx" />
    <add key="ACSInterval" value="30" />
  </appSettings>
  <!--value is in seconds-->

```

7. Enter **localhost** in between the quote marks (ex. <add key="HostName" value="**localhost**" />)

```

File Edit Format View Help
web - Notepad
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="logNet" type="logNet.Config.LogNetConfigurationSectionHandler, logNet" />
  </configSections>
  <appSettings>
    <add key="EvaluationAttachmentsFolder" value="fileUpload" />
    <add key="EvaluationScreenshotsFolder" value="ScreenShotsUpload" />
    <add key="RecordingFolder" value="Recording" />
    <add key="EvaluationAllFolder" value="Evaluation" />
    <add key="LearningContentAttachmentsFolder" value="Learning_Content" />
    <add key="PlayRtlFolder" value="PlayRtl" />
    <add key="ExportUserDataFolder" value="ExportUserFiles" />
    <add key="ImportUserFilesFolder" value="ImportUserFiles" />
    <add key="ImportUserXSDFiles" value="ImportUserSchema" />
    <add key="ImportUserXSDFilesFolder" value="ImportUserSchemaFile" />
    <add key="Decoding" value="Decoding" />
    <add key="NullItems" value="False" />
    <add key="HostName" value="localhost" />
    <add key="CTRL_EXIT" value="Y" />
    <add key="I555Enabled" value="False" />
    <add key="ApplicationVersion" value="5.1.0.34" />
    <add key="TelstratMaxDeserializersMembers" value="500000" />
    <add key="AspectMaxDeserializersMembers" value="150000" />
    <add key="ReleaseVersion" value="Release 5.1.0" />
    <add key="Copyright" value="Copyright © 2012 - 2015 Telstrat International Ltd." />
    <add key="TelstratIntegratedSecurityURL" value="//TelstratIntegratedSecurity/Default.aspx" />
    <add key="ACSInterval" value="30" />
  </appSettings>
  <!--value is in seconds-->

```

8. On the Notepad's **File** menu, click **Save** to save this change in the file.

9. Close the file.

10. From the Start menu, open a Command Prompt window and enter the command **IIRRESET**. This will restart the IIS server so that the new value will be used.

This specific change will be a default condition in future releases of Engage.

10.4 HTTP Error 503 The service is unavailable

The 503 Service Unavailable error is an HTTP status code that means the web site's server is simply not available right now.

Symptom: This error code has been seen when the Engage Application Pool under IIS is not started.

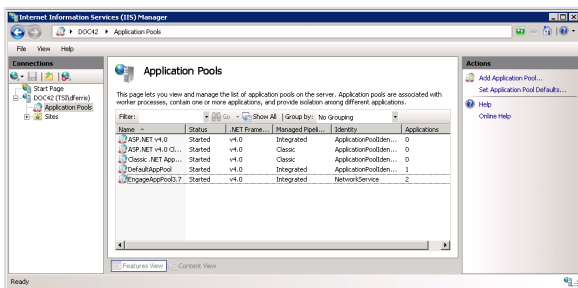


Solution:

1. Logon to the web server and open the IIS Manager tool.



2. Expand (+) the server connections, click on Application Pools and look for EngageAppPool3.7 and its status.



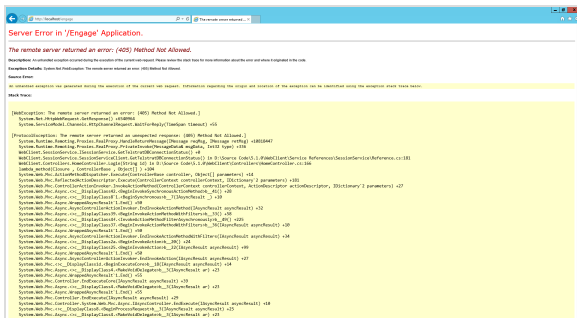
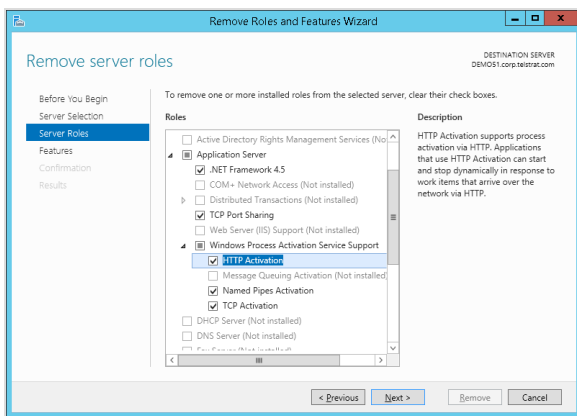
3. If it is **Stopped**, right-click on the pool line entry to get the pop-up menu and click **Start**.
4. Close the IIS Services Manager.

10.5 Troubleshoot (405) Method Not Allowed Issue

(405) Method Not Allowed may be resolved by adding HTTP Activation to the Application Server role on Windows Server 2012 under Windows Process Activation Service Support.

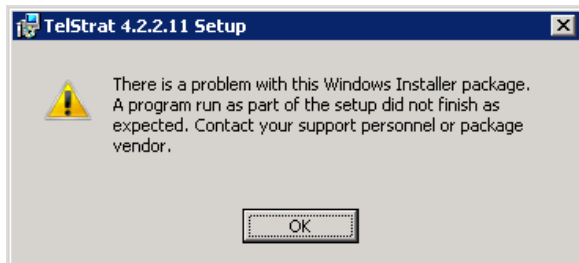
Refer to adding the Application Server role for Server 2012 procedure.

Verify all required application role selections are made as shown.



10.6 Web Server upgrade fails if Application Server Role not Enabled

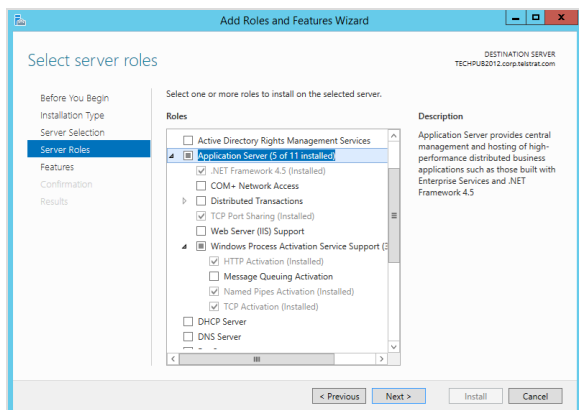
Symptom: During the installation process, the setup program execution encounters a problem and the following message may be displayed:



Possible Cause: Receiving this problem message could indicate that the Application Server role was not enabled during the Web Server installation process.

Solution:

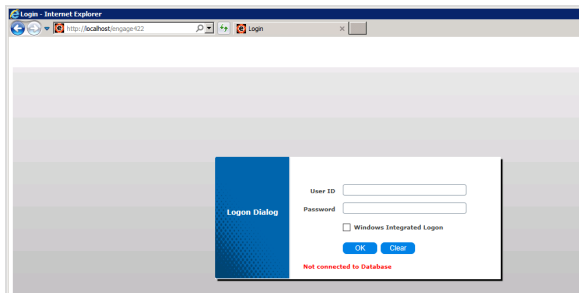
1. Click **OK** which will stop the installation process.
2. Go to the *Server Manager tool* of the Web Server.
3. Check that the status of the **Application Server role** is **Enabled** on the web server.
4. If not, Enable the Application Server role by using the steps in the Web Server section of this guide.



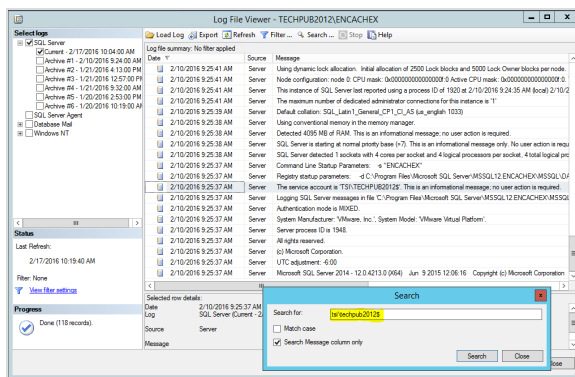
This has been known to resolve this issue. Once enabled, continue with the installation

10.7 Troubleshoot "Not connected to Database" Errors

If the statement "Not connected to Database" appears in the Web Client's Logon Dialog box, this indicates the account being used may not be properly configured. Perform these steps to troubleshoot the issue:



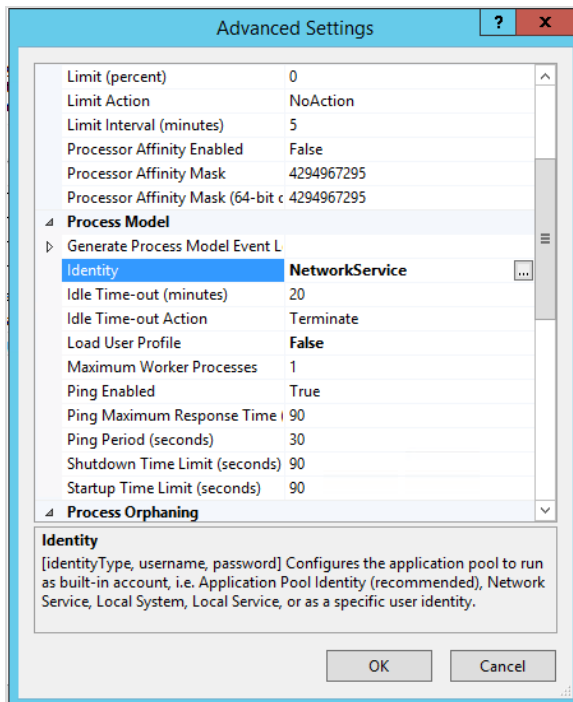
1. Confirm that the <domain\servername\$> is currently attempting to access the SQL Instance. On the recorder server:
 - a. Go to **Start » SQL xxxx Server Management Studio** and login.
 - b. On the **Object Explorer** window, scroll down the list to **Management » SQL Server Logs » Current - mm/dd/yyyy**.
 - c. Use the **Search** button to get the **Search** window and search the **Current** log for **domain\server-name\$** for logs with the \$ symbol (ex. ts\techpub2012\$).



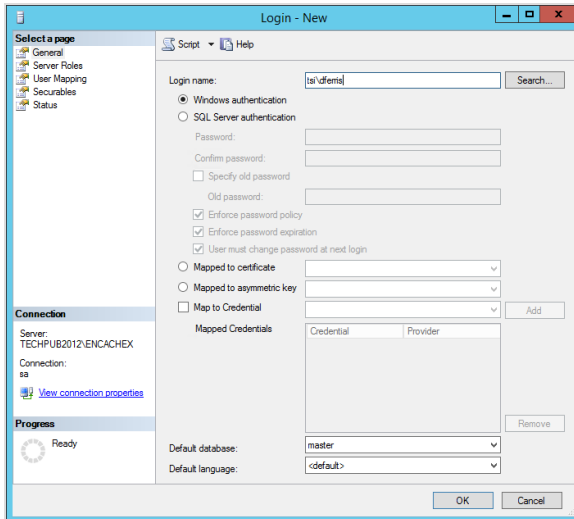
- d. When finished, close the log file and Exit out of the SQL Server xxxx Management Studio.

2. When the <domain\servername\$> attempts are confirmed by the SQL log search, update the web server's Local Administration Group with the Windows Account attempting to authenticate with SQL.
 - a. Open the **Server Manager » Computer Management » Local Users and Groups » Groups**.
 - b. ADD the Windows account that is to be used by the web client to the **Administrators Group**.

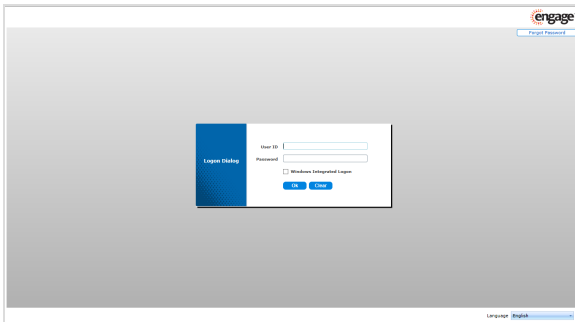
- c. Scroll down the list to **Process Model** and note the *Identity* field. The field may be updated to reflect the Windows Account just added into the Local Admin Group or it may indicate Network Service. Read the definition at the bottom of the window for more details about Identity.



4. Add the Windows Account into the SQL Instance and assign the necessary Server Roles and User Mappings. Use the [CREATE SQL ACCOUNT FOR ENGAGE FOR WINDOWS AUTHENTICATION.HTM](#) topic in this guide for details.



5. Reload the Web Client and confirm that the "Not connected to Database" warning is gone.



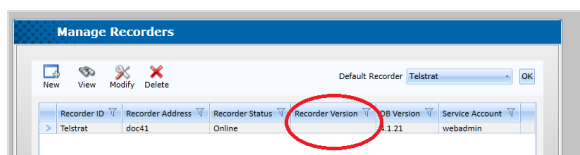
10.8 Recorder Version is Blank in the Manage Recorders window

Symptom:

When adding the connection to the recorder, the displayed recorder version is **blank**.

Cause:

This indicates an issue with the Engage SDK, which is used by the web server to connect to the recorder.

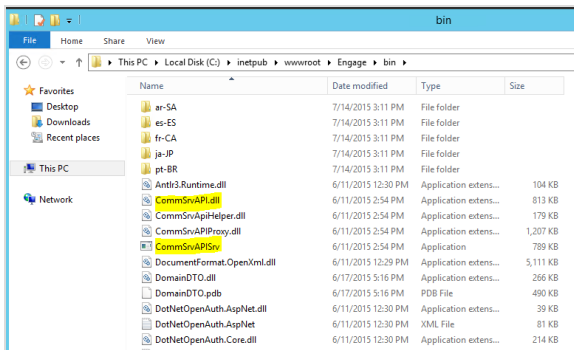


Solution:

This condition can be resolved by *registering these two interface files on the web server*:

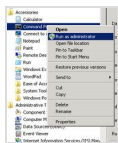
- CommSrvApiSrv.exe
- CommSrvApi.dll

1. Logon to the server. From the **Start** menu, go to **This PC** and navigate to **c:\inetpub\wwwroot\Engage\bin**. The files are located in the virtual directory **\bin** folder.



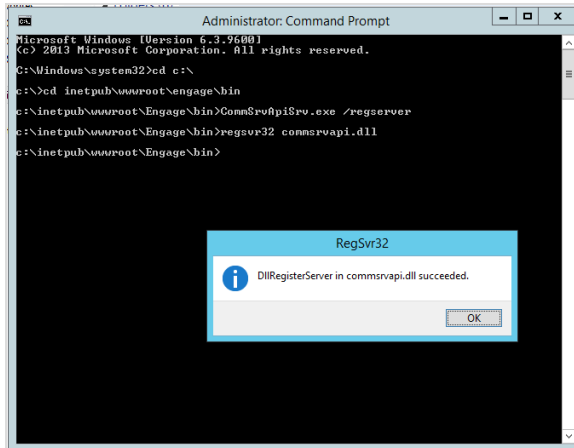
2. Manually search for and delete all copies of these files *except the ones located at the web server folder*. You can then register the files as follows:

- a. Open a Command Prompt and select *Run as an administrator*.

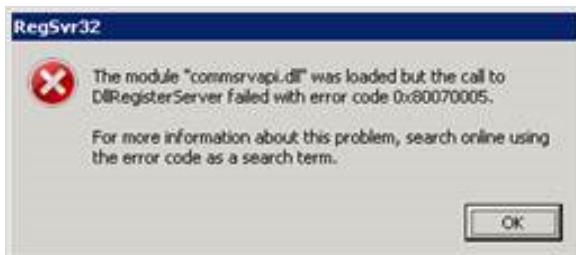


- b. At the Administrator Command prompt:
 - Enter **cd c:** to change the directory to the c: drive.
 - Enter **cd inetpub\wwwroot\engage\bin**
 - Enter **CommSrvApiSrv.exe /regserver**
 - Enter **regsvr32 commsrvapi.dll**

d. The response should be:



If you receive the following error message, it may be due to not running the command prompt as an administrator. Close the command prompt then repeat the above steps.



10 HTTP Error 500 Web Client Timeout

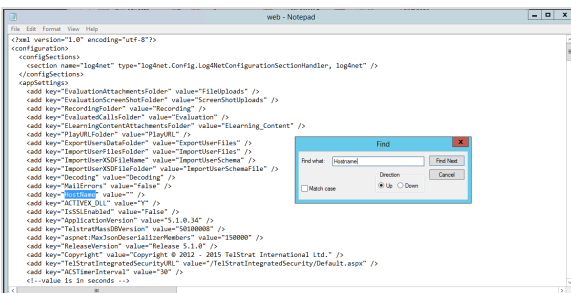
Symptom: When the Engage web server encounters an unexpected condition that prevents it from fulfilling the request by the web client for access to the requested URL, the web client can time-out and/or produce HTTP Error 500s.

Possible Cause: HTTP Error 500s are 'catch-all' errors generated by the web server indicating something has gone wrong, but the server can not be more specific about the error condition in its response to the client.

Solution: The Engage Web Client web.config file will need a change to be implemented on the "HostName" default value.

To make the change, do the following steps:

1. On the server, open the **Notepad** program as an *administrator*.
2. On the drop-down menu in the lower right-hand corner, change Text Documents (.txt) to **All Files**.
3. Open the **web.config** file located on the web server by going to **c:\inetpub\wwwroot\<database>\web**, which is the XML configuration file for the web client.
4. Click on the **Edit** menu command to get the pop-up menu, click **Find** to get the **Find** window and enter **HostName** to locate the specific line of code to change in the **add key=** list.



5. In the **web.config** XML file, the code string to work with is **<add key="HostName" value="" />**.
6. Highlight the two quote marks ("") in the string (ex. **<add key="HostName" value="" />**).

```

File Edit Format View Help
web - Notepad
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="logNet" type="logNet.Config.LogNetConfigurationSectionHandler, logNet" />
  </configSections>
  <appSettings>
    <add key="EvaluationAttachmentsFolder" value="fileUpload" />
    <add key="EvaluationScreenshotsFolder" value="ScreenShotsUpload" />
    <add key="RecordingFolder" value="Recording" />
    <add key="EvaluationAllFolder" value="Evaluation" />
    <add key="LearningContentAttachmentsFolder" value="Learning_Content" />
    <add key="PlayRtFolder" value="PlayRt" />
    <add key="ExportUserDataFolder" value="ExportUserFiles" />
    <add key="ImportUserFilesFolder" value="ImportUserFiles" />
    <add key="ImportUserXSDFile" value="ImportUserSchema" />
    <add key="ImportUserXSDFileFolder" value="ImportUserSchemaFile" />
    <add key="Decoding" value="Decoding" />
    <add key="MailServer" value="False" />
    <add key="HostName" value="localhost" />
    <add key="MCTRER.dll" value="*" />
    <add key="I555Enabled" value="False" />
    <add key="ApplicationVersion" value="5.1.0.34" />
    <add key="TelstratBusIDVersion" value="9B10000" />
    <add key="Aspet.MachineSerializersMembers" value="150000" />
    <add key="ReleaseVersion" value="Release 5.1.0" />
    <add key="Copyright" value="Copyright © 2012 - 2015 Telstrat International Ltd." />
    <add key="TelstratIntegratedSecurityURL" value="//TelstratIntegratedSecurity/Default.aspx" />
    <add key="MCTimerInterval" value="30" />
  </appSettings>
</configuration>
</value is in seconds -->

```

7. Enter **localhost** in between the quote marks (ex. <add key="HostName" value="**localhost**" />)

```

File Edit Format View Help
web - Notepad
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="logNet" type="logNet.Config.LogNetConfigurationSectionHandler, logNet" />
  </configSections>
  <appSettings>
    <add key="EvaluationAttachmentsFolder" value="fileUpload" />
    <add key="EvaluationScreenshotsFolder" value="ScreenShotsUpload" />
    <add key="RecordingFolder" value="Recording" />
    <add key="EvaluationAllFolder" value="Evaluation" />
    <add key="LearningContentAttachmentsFolder" value="Learning_Content" />
    <add key="PlayRtFolder" value="PlayRt" />
    <add key="ExportUserDataFolder" value="ExportUserFiles" />
    <add key="ImportUserFilesFolder" value="ImportUserFiles" />
    <add key="ImportUserXSDFile" value="ImportUserSchema" />
    <add key="ImportUserXSDFileFolder" value="ImportUserSchemaFile" />
    <add key="Decoding" value="Decoding" />
    <add key="MailServer" value="False" />
    <add key="HostName" value="localhost" />
    <add key="MCTRER.dll" value="*" />
    <add key="I555Enabled" value="False" />
    <add key="ApplicationVersion" value="5.1.0.34" />
    <add key="TelstratBusIDVersion" value="9B10000" />
    <add key="Aspet.MachineSerializersMembers" value="150000" />
    <add key="ReleaseVersion" value="Release 5.1.0" />
    <add key="Copyright" value="Copyright © 2012 - 2015 Telstrat International Ltd." />
    <add key="TelstratIntegratedSecurityURL" value="//TelstratIntegratedSecurity/Default.aspx" />
    <add key="MCTimerInterval" value="30" />
  </appSettings>
</configuration>
</value is in seconds -->

```

8. On the Notepad's **File** menu, click **Save** to save this change in the file.

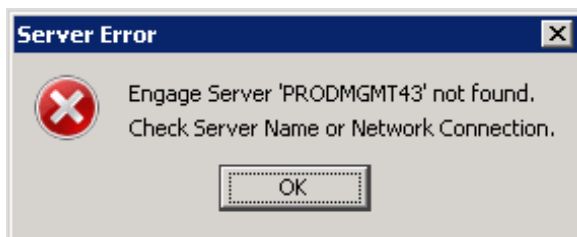
9. Close the file.

10. From the Start menu, open a Command Prompt window and enter the command **IIRRESET**. This will restart the IIS server so that the new value will be used.

This specific change will be a default condition in future releases of Engage.

10.9 Troubleshoot "Engage Record Server Not Found" errors

The Engage JAVA client is an essential tool for configuring the Engage Voice Recorder. There may be times when an error occurs that requires troubleshooting to isolate an issue that affects the JAVA client. The troubleshooting occurs on the Engage server where an error message may appear:



10.9.1 TmpInfo.log shows InitLicenses() Failed

Symptom: The *TmpInfo.log* shows the following error can occur if the installer did not configure Engage to use the software licenses or if the license key is invalid.

ILicenseManager::InitLicenses() Failed with error code 1! 12/06/14 14:08:18

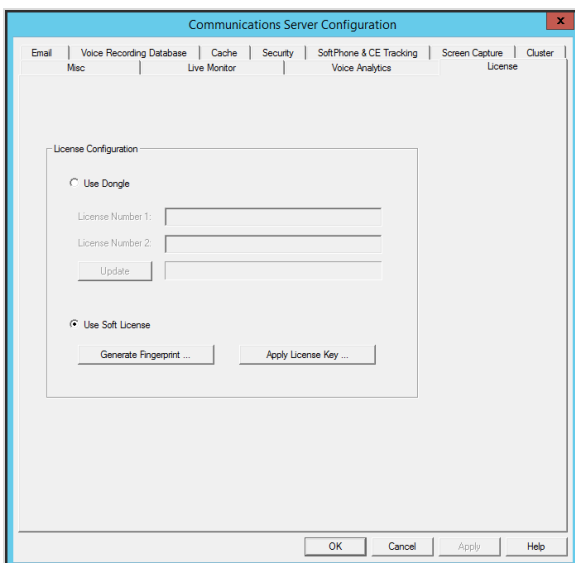
InitLicenseManager Failed - Will Retry in 30 second. 12/06/14 14:08:18

Cause: Engage may not be configured to use software licenses, the software license key may be invalid, or the Sentinel service is not running properly and CommSrv is unable to reach it.

Possible Solutions:

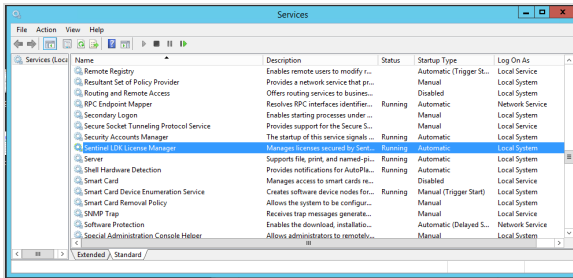
Check the License Tab in CommSrv

1. Open the **Server Configuration (CommSrv)** tool and go to **Licenses** tab. Verify **Use Soft License** is selected.



Check Services for Running Status

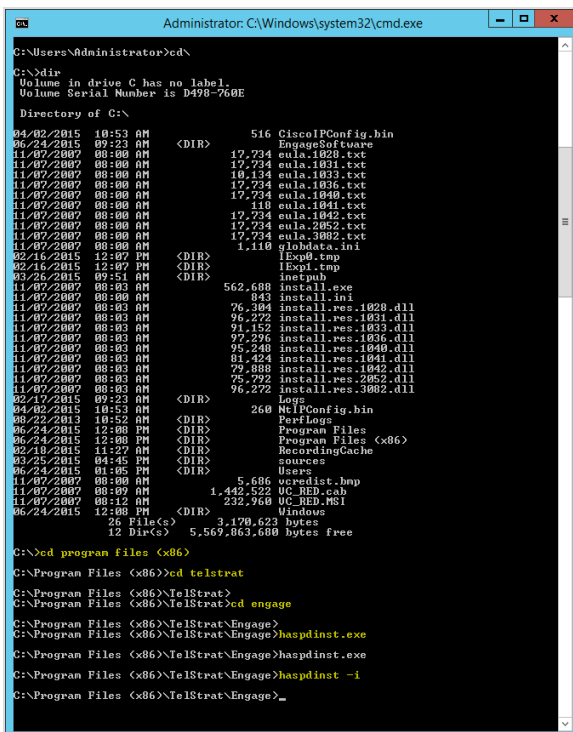
1. Open the **Services** tool on the recording server and verify the *Sentinel LDK License Manager* service is running.



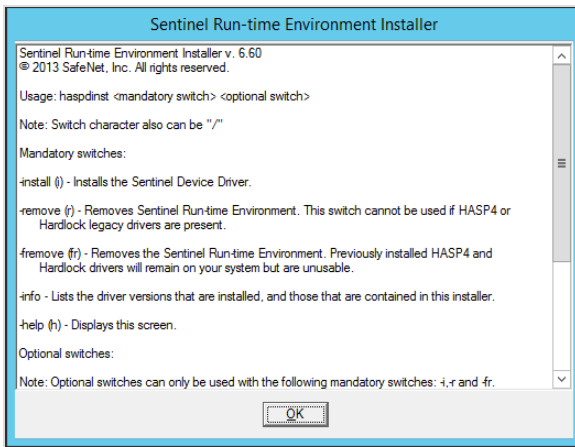
- Restart the **Sentinel LDK License Manager** by right-clicking on the service name to get the pop-up menu and then click **Stop** then **Start**.

Check the Sentinel LDK Installation

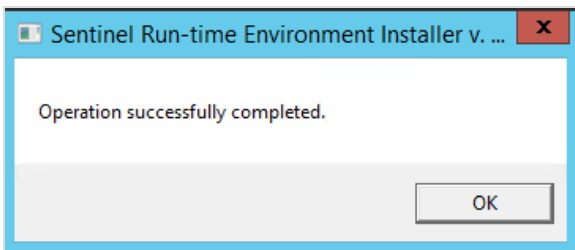
- If this is a new installation and it has never been started, try re-running the **haspdinst.exe** file. Use the **default settings**. From **Start » Run » cmd** to get the **cmd.exe** window.
- Using the Change Directory command (**cd**), navigate through the directories to the Engage directory.



- Enter **haspdinst.exe** in the cmd box and view the program window. Various switches are described. Use the **-i** switch to install the Sentinel program (ex. **haspdinst -i**).



4. Enter **haspdinst -i** in the cmd box. The program will take a moment to install and display the window when complete.



5. If the voice recording server was not or has not been restarted after initial installation, **restart it now**.

10.9.2 TmpInfo.log shows SQL Connection Error 80043c9d

Symptom: The TmpInfo.log file shows the following error:

SQL Connection Error 80043c9d

Re-Attempt #21 to connect to SQL Server PRODMGMT43\ENCACHEX

SQL DMO 'Connect' Error:<BEGIN>

[Microsoft][ODBC SQL Server Driver][SQL Server]Cannot execute as the database principal because the principal "guest" does not exist, this type of principal cannot be impersonated, or you do not have permission.

Cause: This is typically caused when Engage is not configured with the correct SQL login and password information.

Solution: Launch the *Server Configuration* program, go to the *Voice Recorder Database* tab and enter the SQL login and password information. **Restart the TelStrat Voice Recording service.**

10.9.3 TmpInfo.log shows SQL Connection Error 80040000

Symptom: TmpInfo.log file shows the following error:

SQL Connection Error 80040000

Re-Attempt #5 to connect to SQL Server SqlServer\encachex

SQL DMO 'Connect' Error:<BEGIN>

SQL Server does not exist or access denied.

ConnectionOpen (Connect()).

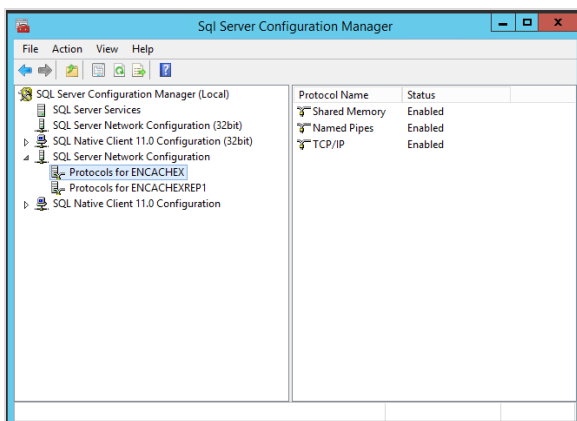
Possible Causes:

Cause: *Firewall Settings are blocking the SQL connection.*

Solution: Confirm with the customer that the firewall settings appropriate for the deployment and voice platform have been made.

Cause: *SQL is not setup to allow remote access.*

Solution: Open the *SQL Server Configuration Manager* and check if TCP/IP is set to Disabled which is the default setting. Change it to **Enabled** . Restart the *SQL Server (server name)* service. The TCP/IP protocol must be enabled in the SQL Server.



10.9.4 TmpInfo.log shows Database 'Config' could NOT be created

Symptom: TmpInfo.log file shows the following error:

ERROR: Database 'Config' could NOT be created successfully - 0x80041432

Cannot create file 'c:\Program Files\Microsoft SQL Server\MSSQL10_50.SQLEXPRESS\MSSQL\DATA\Config_Data.mdf' because it already exists. Change the file path or the file name, and retry the operation.

CREATE DATABASE failed. Some file names listed could not be created. Check related errors.

Cause: This can occur if the Config database *is not attached* in SQL but the Config.mdf file is present.

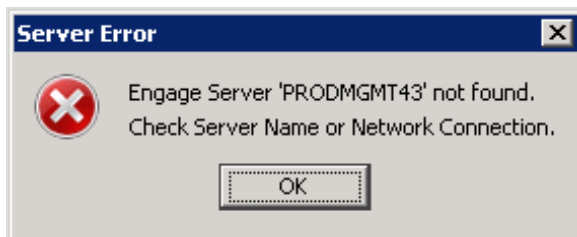
Solution: Attach the Config.mdf file if the config database should already be connected or delete the file and Engage will create a blank database with no configuration (if that is the intent).

10.10 Engage Server Not Found - Dongle Release Mismatch

Another reason to receive the Engage Server Not Found error is a mismatch between the license dongle and the Engage application.

Symptom:

Server Error Warning



Application Started at 06/25/2015 14:36:04 06/25/15 14:36:04

Server Version 4.1.1.1

CServiceModule::InitializeDataMgr():new CDataMgr()... 06/25/15 14:36:04

InitLicenseManager:LIC_PROVIDER_SAFENET 06/25/15 14:36:04

License Server initialized successfully. 06/25/15 14:36:05

Detected VMWare: ESX 06/25/15 14:36:05

INFO: CommSrv Server is running in Virtual Machine Env.

Dongle is programmed for a maximum version of 3.6, App version is 4.1. The Server will now exit. 06/25/15 14:36:05

Cause:

License dongles are programmed to run on purchased releases of Engage applications. If the Engage application release does not match the dongle, the server will not connect.

Solution:

Contact TelStrat Customer Support and request an updated license key that authorizes the newer software release.

10.11 Troubleshoot "Download Service Not Found" Error

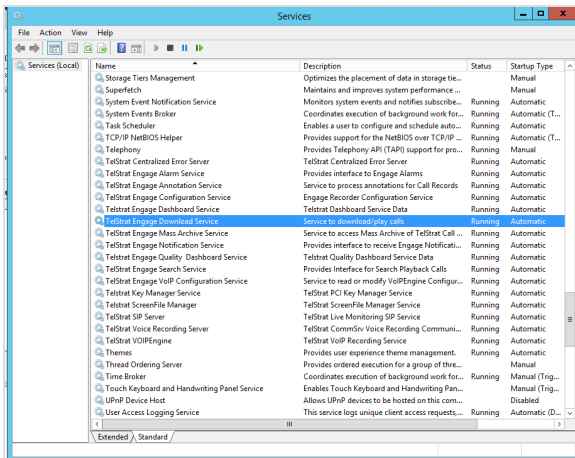
If call playback is not working and/or the **Download Service Not Found** error window is delivered on the screen, there are two areas to check.

Check the TelStrat Engage Download Service state

Engage Services requires setting the **TelStrat Engage Download Service** to *Automatic Mode* and then starting the service. The installation program automatically makes this configuration change as part of the installation. The **TelStrat Engage Download Service** is essential for downloading and playing calls. If the service is not running, no calls can be played.

Verify that the **TelStrat Engage Download Service** is *Running* on the Engage Voice Recorder. The installation program automatically makes this configuration change as part of the installation. To do this:

1. Go to the Engage Server's *Services* tool.
2. Scroll down and find **TelStrat Engage Download Service** and verify that *Running* is in the *Status* column.
3. If the *Status* area is empty, right-click on the **TelStrat Engage Download Service** name and use the drop-down menu and click on *Start*. This should start the service and *Running* should appear in the *Status* column.



Check the Net.TCP Port Sharing Service state:

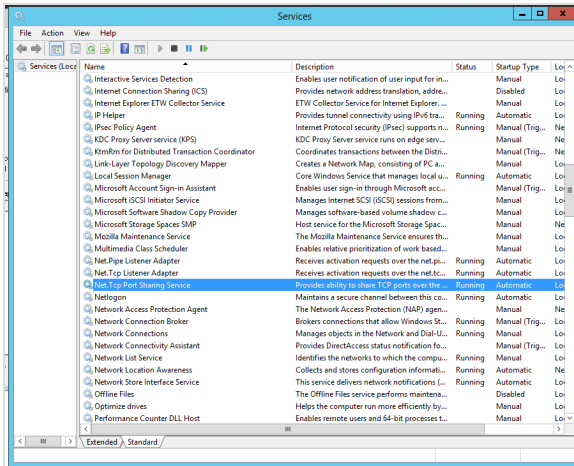
Engage Services requires setting the **Net.Tcp Port Sharing Service** to *Automatic Mode* and then starting the service. The installation program automatically makes this configuration change as part of the installation.

The **Net.Tcp Port Sharing Service** provides the ability to share TCP ports over the net.tcp network.

If this service, **Net.Tcp Port Sharing Service**, is not **Running**, then the Web Client cannot connect to the *TelStrat Engage Download Service* and the *TelStrat Engage Annotation Service* (in Engage Release 4.0.5 or newer) and the Web Client user interface will be unusable.

To check the status of these services:

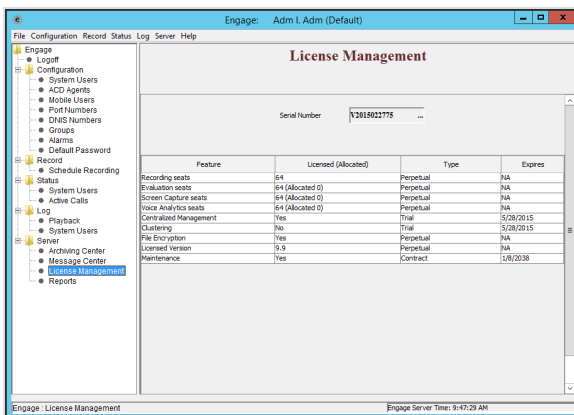
1. Go to the Services tool of the Engage Voice Recorder.
2. Scroll down the list of services and find **Net.Tcp Port Sharing Service** and verify that **Running** is in the *Status* column.
3. If the *Status* area is empty, right-click on the **Net.Tcp Port Sharing Service** name and use the dropdown menu and click on **Start**. This should start the service and **Running** should appear in the *Status* column.
4. Be sure to check that the two associated services (TelStrat Engage Download Service and TelStrat Engage Annotation Service) are in the **Running** state in the *Status* column. If not, right-click on each and click **Start**.



10.12 Troubleshoot License Management

The Engage JAVA client is used to reveal the system's software licenses. The information on a specific server is found by using the menu and navigating to the **Server » License Management** window.

When licenses are not installed or are invalid (out of date, wrong serial number, etc), the Engage system will not function correctly.



Each system comes with a set of various product-related licenses, depending on what was purchased. These licenses are:

- Recording Seats:
- Evaluation Seats:
- Screen Capture Seats:

- Voice Analytics Seats:
- Centralized Management:
- Clustering:
- File Encryption:
- Licensed Version:
- Maintenance:

Symptom: An example of a failure to apply a software license generates repeated alert messages (in the Temp-info.log file) such as:

ILicenseManager::InitLicenses() Failed with error code 1! 05/31/15 12:30:38

InitLicenseManager Failed - Will Retry in 30 second. 05/31/15 12:30:38

ILicenseManager::InitLicenses() Failed with error code 1! 05/31/15 12:31:12

InitLicenseManager Failed - Will Retry in 30 second. 05/31/15 12:31:12

ILicenseManager::InitLicenses() Failed with error code 1! 05/31/15 12:31:46

InitLicenseManager Failed - Will Retry in 30 second. 05/31/15 12:31:46

ILicenseManager::InitLicenses() Failed with error code 1! 05/31/15 12:32:20

InitLicenseManager Failed - Will Retry in 30 second. 05/31/15 12:32:20

Cause: Engage may not be configured to use the software licenses or the software license key may be invalid.

Solution: Verify that the correct and valid software licenses have been installed on the Engage Voice Recorder.

10.13 Troubleshoot Playback Calls

This section provides common troubleshooting of Playback Calls issues.

10.13.1 Audio Playback Fails in IE11, IE10 and IE9

Playback fails in IE11, IE10, IE9. The Timeline displays with 0 (zero) second duration.

If the MP3encoder.dll file is missing on the Engage Record server, the timeline player may show a valid timeline, but the call duration shows 0 (zero) seconds.



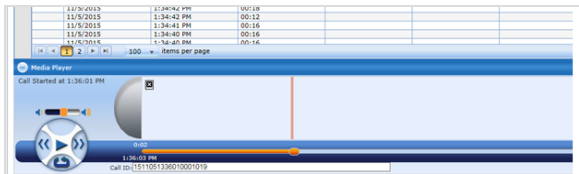
IE11, IE10, and IE9 support playback of .MP3 files only using the timeline player. Engage requires an *MP3encoder.dll* file that is included with the Microsoft Visual C++ 2010 Redistributable Package.

If playback within IE9-IE11 fails and the .MP3 download fails, then install the *Microsoft Visual C++ 2010 Redistributable* package found in the [Windows Pre-reqs](#) folder of the Engage prerequisite software folder.

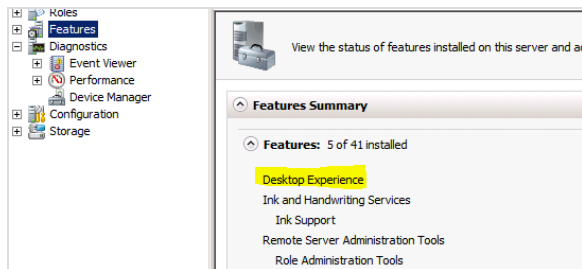
Refer to the Engage Server Pre-Requisite Tasks section of this Server Installation Guide for instructions.

10.14 Timeline Graphic Fails in IE11, IE10 and IE9

Symptom: Graphic is displayed, but audio will not play and timeline displays 0 (zero) second duration.



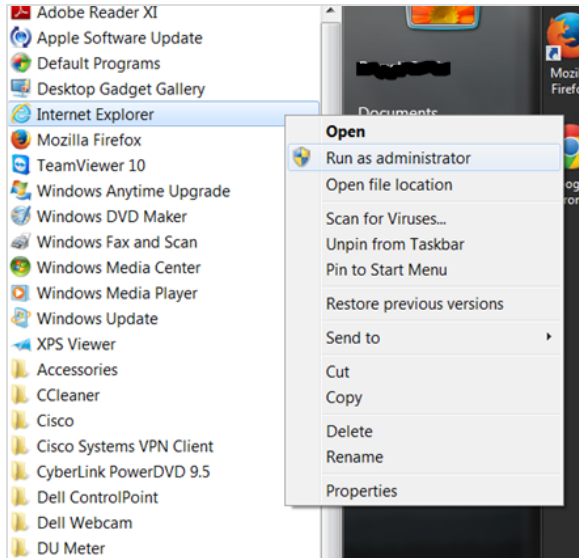
Troubleshooting: Check if the *Desktop Experience* feature is enabled on the server. This is required to support the timeline player graphic for IE9-IE11.



Solution: Install the *Desktop Experience* feature for Windows Server 2008 R2 or 2012.

10 Playback Fails for Administrator

Sometimes, a workstation's current User Account Controls (UAC) settings prevent the Internet Explorer from installing the Active-X player. To repair this:



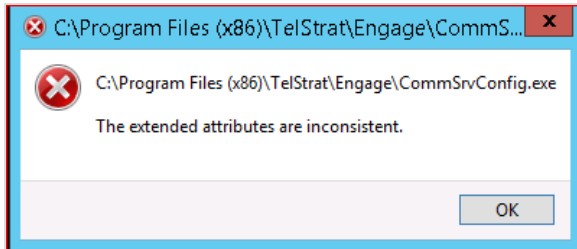
1. Click the **Start** button, go to and right-click on **Internet Explorer**.
2. From the pop-up menu, click on **Run IE as the Administrator**. IE will launch.
3. Logon to the *Engage Web Client* to load the Active-X player.

Once IE is run as an Administrator, playback is available in BOTH administrative and standard user modes.

10.15 Windows Audio Service Crashes Server Config

Symptom:

When using the Server Configuration (CommSrv) program of the Engage server on Windows Server 2012 R2, an error window (*The extended attributes are inconsistent*) can pop up and display.



Cause:

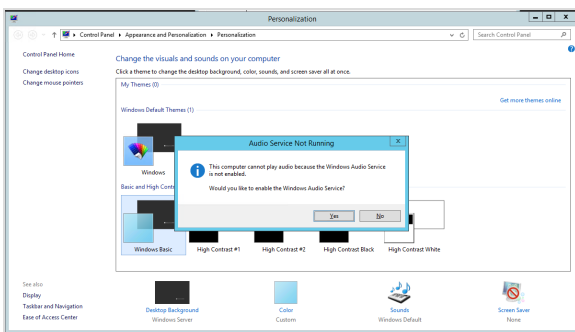
This error indicates that the *Windows Audio* service is not *Running* on the server. The error can occur after trying to launch CommSrv. When changes are being made to a computer by a program via a user, the User Account Control (UAC) process normally provides a audible BEEP and in some cases, an information/request window. When the error occurs, the Windows Audio service is not running, which prevents the playing of the audible sound file, which causes the error.

Solution:

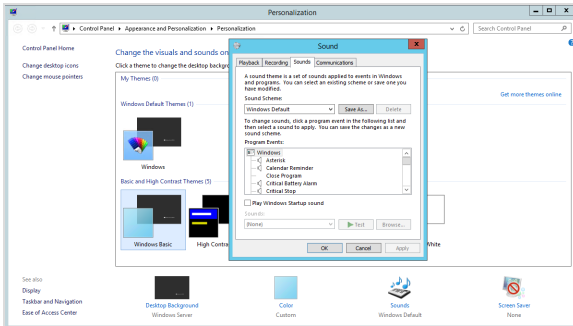
There are two ways to start the *Windows Audio* service:

Use the Desktop Personalization window:

1. Logon to the server.
2. Right-click on the desktop area to get the pop-up menu and click on *Personalize*. Click on the *Sounds* option.



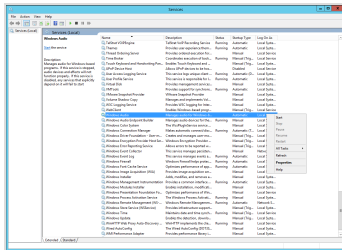
3. The error window **Audio Service Not Running** will appear.
4. Click *Yes* and the **Sound** theme window will appear. Click *OK* to select the *Windows Default* sound theme.



Use the Services Tool:

The *Windows Audio* service can also be started using the **Services** tool.

1. From the **Start** menu, launch the **Services** tool.
2. Scroll down the list of services and right-click on the *Windows Audio* service name to get the pop-up menu.
3. Click on **Start** to start the service.



10.16 Event Monitor not Functioning

The Engage Event Monitor is responsible for delivery of system event messages and content. This important information can be sent to administrators or users using:

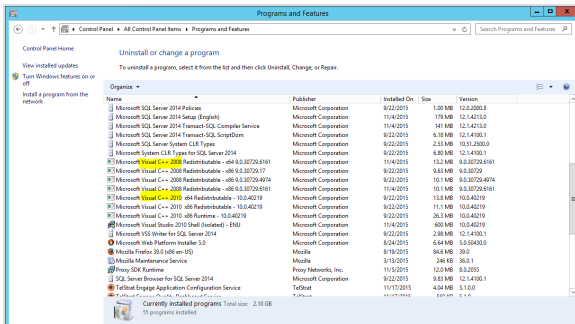
- e-mail addresses.
- SMTP messaging.
- the Web Client's Events button.

The Engage Event Monitor application expects to use installed Microsoft Visual C++ 2008 and 2010 software elements. The complete implementation of the Engage Recording Server requires the following up-to-date Visual C++ components be installed on the server:

- 2008vcredist_x64
- 2008vcredist_x86
- 2020vcredist_x64
- 2010vcredist_x86

If system events are failing to be generated (not being delivered to e-mail addresses, showing up in SMTP messaging or there are no events when using the Web Client's Events button), check for proper installation and most recent versions of the C++ software:

1. Go to the server's **Control Panel**.
2. Locate the software components (ex. with names such as Microsoft Visual C++ 2008 Redistributable - x64...)



3. If the software is missing, reinstall it.

10.17 TALC Card Traces and Commands

Access the TALC through Telnet client.

Go to Edit and hit Start Loggin

Give the file a name

In Debug, type pf 2 port

Leave the session open so it logs all the calls on the port.

When the TALC card is ready to communicate, it displays:

TALC_RDY>

dc 0,s: Dumps the configuration of the card.

displlog shows the events on the board (reset, login, connection to IDVR).

Description of dump elements:

Ex. *IPCFG 192.168.143.134, 255.255.255.0, 192.168.143.254, 0.0.0.0, 255.255.255.0, D*

IP Address: 192.168.143.134

IP Network Mask: 255.255.255.0

IP Gateway: 192.168.143.254

Management IP Address: 0.0.0.0

Management IP Network Mask: 255.255.255.0

Ethernet Full Duplex [E-Enable D-Disable]: D

Ex. *SYSCFG 1,IDVR Beta Card 1*

Board ID: 1

Node Name: IDVR Beta Card 1

Ex. *ACCFG E, 1, 04:00, 16, 0, 4728*

Configuration name: accfg

DN Discovery[E/D]: E

DN Discovery Frequency [1-Per Day 2-Per Week 3-Per Month]: 1

DN Discovery Time [hh:mm]: 04:00

Extension to Dial - Port Number: 16

Extension to Dial - Feature Key: 0

Extension to Dial - DN: 4728

Ex. *PORTCFG 0, E, 1, D, D, N, D, D*

Port Number: 0

IDVR Status [E/D]: E

IDVR CompressionRate[0-G711 1-G723.1]: 1

TAPI Support [E/D]: D

2250Port[E/D]: D

Configure Agent ID ?[Y/N]: N

Beep Tone [E/D]: D

Virtual Phone Recording [E/D]: D

Ex. *FKEYCFG 1,13 EREC ,14 ECS ,9 RDIS ,NC*

Device Number: 1

Feature 1

KeyNo Feature Data: 13 EREC (record)

Feature 2

Key No Feature Data: 14 ECS (Conversation save)

Feature 3

Key No Feature Data: 9 RDIS (Delete Recording)

Feature 4

Key No Feature Data: NC

Config commands

Attribute *rc* : Type *rc* before any of the following *config commands* and the system will print the *current config* for that command.

Dm i

ip: set the IP address of Card

syscfg: set the unit ID, and Node Name

idvrcfg : enable, and set the IP address of server

accfg: set DN Discovery

portcfg: configure a port

fkeycfg: configure key for port

sympdispcfg: symposium configuration

sc y: save configuration

sr 1,y : reset board

us: upload software

uc: upload configuration

DEBUG Commands and Suggestions

wh displays version number of the card and how long the card has been up

pf 4 (port 0 - 15) captures information sent between card & Phone

pf 4 (port 32 - 47) captures information sent between card & PBX

cp 5 (port 0 – 15) snapshot of the phone

cp 085 <port> To see the DN Discovery of the particular port

db 13 5 displays cross connect information

db 2 153 Call start information

db 2 154 detailed call start information

db 2 8 See DND discover run

db 2 184 Agent login

db 8 y IDVR State Machine

db 2 026 Call State Machine

cp 021 <port> To see the Call Bits for the port

cp 022 <port> To see the RSM (Recorder State Machine) for the port – use it for recording problem

ES 1 Network states

Dcb DSP information

NVD

CPP MADN enable disable

TMS (set in seconds) Time stamp (default 60 for 1 minute)

Sdp 13 3 port Beep tone

Sdp 8 3 port ?

sdp: Set Debug Print Level: Type (max=18), Level (max=3), Channel(max=31)

0 : Icon Control

1 : Connect ID

2 : Privacy Override

3 : Line Preference Key (LPK)

4 : Redundant_Indicator

5 : CP Virtual Device

6 : CP Call Handler

7 : CP Call State Machine

8 : CP RSM Manager

9 : CP Recorder State Machine

10 : IDVR Keys

11 : CPND State Machine

12 : Softphone Hotline State Machine

13: Recording Beep Tone

14 : ACD Call Force Tone

15 : Fast Path

16 : KBA Phase II From PBX

17 : Overlay

18 : DC IDVR Call Manager

During a debug session, always do the following:

- When doing traces, annotate what the user is doing. Use special characters (ex. !, @, #, \$, % etc.) to mark the comments.

In debug window:

- **wh**: Get the version, how long the card has been up.

Before closing the debug window and while in the MMI window:

- **dc**: Get the config
- **dlog**: Get the display log

When a customer reports a problem, while communicating with them, always get:

- Card's config
- TNB of the whole slot
- Symptoms of failure
- Exact date/time of failure
- Frequency of failures
- **Finally, get a VERY detailed description describing exactly (as close as possible) what the user is doing (ex. keys being pressed, how many times, lamp status whether on, off or blinking, and any other symptoms) to generate the issue.**