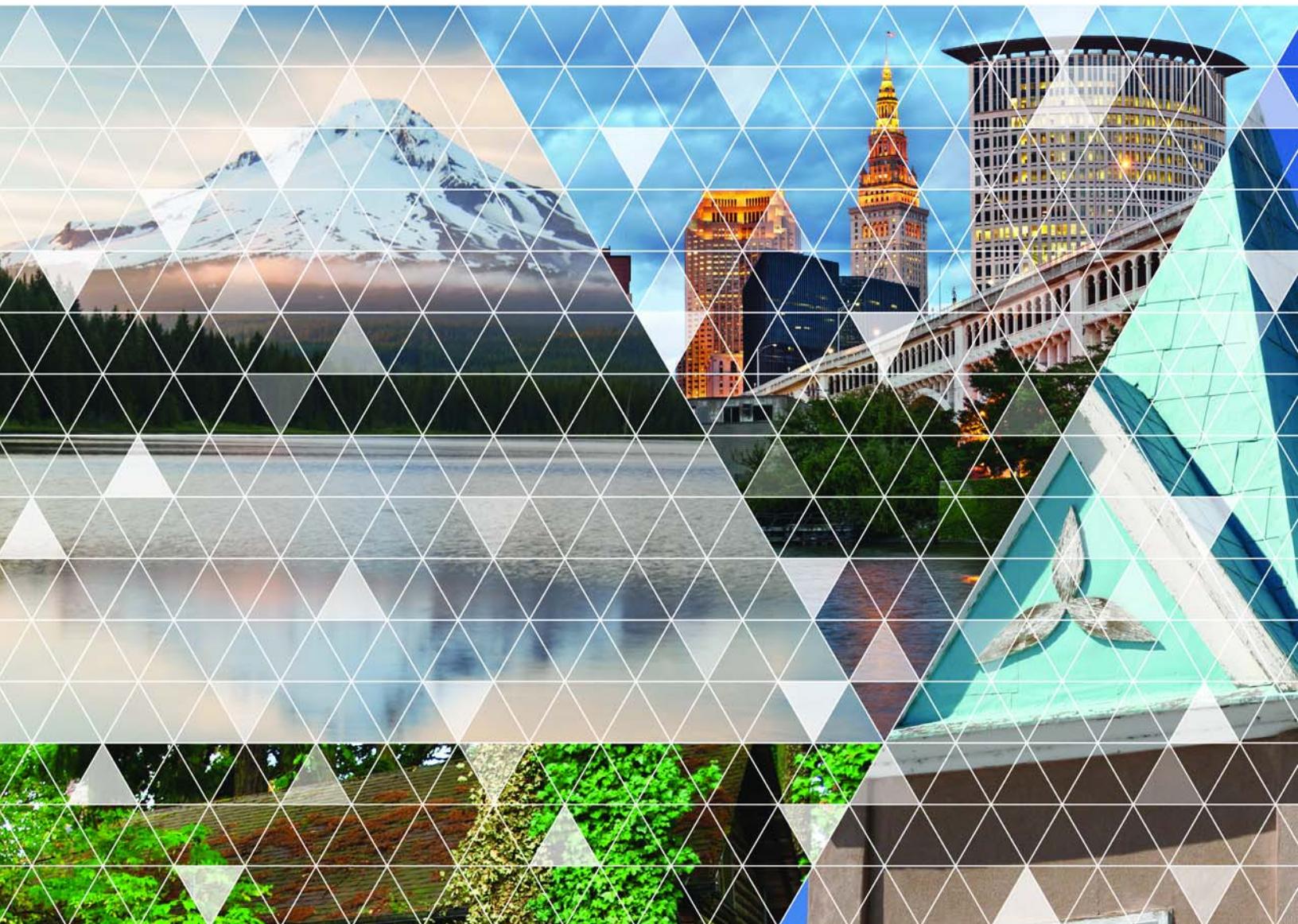


Version 9.3.0

Accela Civic Platform®

Installation Guide



Accela Civic Platform Installation Guide

© 2018 Accela, Inc. All rights reserved.

Accela, the Accela logo, the Accela logo with "Government Software" notation, Accela Automation, Accela Asset Management, Accela Citizen Access, Accela Mobile Citizen Access, Accela ERS, Accela GIS, Accela IVR, Accela Land Management, Accela Licensing, Accela Mobile Office, Accela Public Health and Safety, Accela Service Request, Accela Wireless, Kiva DMS, Kiva Development Management System, 'PERMITS' Plus, SiteSynch, Tidemark Advantage, Civic Platform, Civic Cloud, Civic Hero, E-Boardroom, EnvisionConnect, Envista, GEOTMS, IQM2, Mediataraq, Minutetraaq, PublicStuff, Trusted To Do More, VelocityHall, Vantage360, and other Accela logos, devices, product names, and service names are trademarks or service marks of Accela, Inc. Brava! Viewer is a trademark of Informative Graphics Corporation. Windows is a registered trademark of Microsoft Corporation. Acrobat is a trademark of Adobe Systems Incorporated. Portions copyright 2009 Ching-Lan 'digdog' Huang and digdog software. All other company names, product names, and designs mentioned herein are held by their respective owners.

Version 9.3.0

March 2018

Corporate Headquarters

2633 Camino Ramon
Suite 500
Bishop Ranch 3
San Ramon, CA 94583

Tel: (888) 722-2352
Fax: (925) 659-3201

www.accela.com

Contents

Getting Started.....	6
Introduction.....	7
Understanding the Civic Platform Installation Process.....	7
Planning Your Civic Platform System Deployment.....	8
Planning the Installation.....	8
Preparing the Environment.....	11
Hardware and Software Requirements.....	11
Setting Up Multi-Homed Servers.....	11
Installing the Database.....	12
Remote Installation.....	13
Installing ColdFusion MX 7.0.....	13
Preparing Configuration Settings.....	14
Configuration Checklist.....	14
Backing Up Civic Platform.....	18
Renaming Your Configuration Folder.....	19
Installing Civic Platform Components.....	20
Installation.....	21
Installing the Base Civic Platform 9.0.0.....	21
Manually Upgrading the Civic Platform Database.....	56
Installing the Latest Application Code.....	58
Installation Directory Structure.....	63
Top Level Directory Structure.....	63
Second Level Directory Structure.....	64
Registry Entries.....	65
Services.....	65
Post Installation Configuration.....	66
Importing the License Key.....	66
Starting Windows Services.....	66
Changing the Default Administrator Passwords.....	67
Configuring the Heartbeat Interval.....	67
Clearing the Server Cache for Load-Balanced Servers.....	68
Enabling Additional Security Measures.....	69
Configuring MultiRefs in Result Sets.....	72
Enabling the Facebook Integration.....	73
Configuring the Sent From Email Address for Trust Account Notifications.....	74

Configuring Exchange Server Permissions.....	75
Installation Maintenance.....	78
Modifying or Repairing an Installation.....	78
Removing a Civic Platform Installation.....	80
Troubleshooting.....	83
Error 1603, 1638.....	83
Error 1628, 1607, 1618.....	83
Disk Out of Space.....	84
Installing Additional Server Tools.....	85
Configuring the SMS Adapter.....	86
SMS Adapter Prerequisites.....	86
Deploying the Web Service.....	86
Configuring the Web Service.....	88
Testing the Web Service.....	90
Installing the Ad Hoc Report Tool.....	91
Preparing Your System.....	91
Running the Ad Hoc Report Installer.....	93
Configuring the Ad Hoc Reporting Service.....	100
Deploying Ad Hoc Reports into Another Environment.....	102
Installing Oracle 11g OCI Driver Configuration Tool.....	103
Running the Oracle OCI Driver Configuration Tool Installer.....	103
Modifying an Oracle OCI Driver Configuration Tool Installation.....	107
Removing an OCI Driver.....	109
Upgrading the Database for Nearby Query Support.....	112
Nearby Query Prerequisites.....	112
Running the Nearby Query Installer.....	112
Setting Up Civic Platform Clients.....	114
Browser Settings.....	115
Setting ActiveX Controls.....	115
Pop-up Blocker Settings.....	117
Language Settings.....	119
Trusted Sites and Zones Settings.....	119
Installing Security Certificates.....	123
AEDR Installation and Configuration.....	125
Required Software and Configuration.....	125
Installing the Accela Electronic Document Review (AEDR) Client.....	125
Installing the ComparA Client.....	131
Configuring Adobe Acrobat.....	131
Migrating Document Comments from Version 7.1.0.....	135

Accela Document Scan Installation.....	138
Configuring Your System to Use Accela Document Scan.....	138
Installing Accela Document Scan.....	138
Setting Up a Cashier Station.....	141
Intended Audience and Environment.....	141
Requirements.....	141
Configuring the Cashier Station.....	142
Setting Up Web Browser Security Policy.....	151
Validating the Installation.....	151
Customizing Endorsement Content.....	152
Configuring a Barcode Scanner.....	155

Getting Started

Before you begin installing Civic Platform, review the topics in this section and prepare your environment accordingly.

Table 1: Revision History

Date	Description
March 2018	The 9.3.0 version of this guide updated the "Installing Oracle" section to add sqlnet.ora parameters to support Oracle 12c. Also, when creating the regular Accela and Jetspeed database users during the base installation, the passwords cannot have special characters.

Related Information

[Introduction](#)

[Preparing the Environment](#)

[Preparing Configuration Settings](#)

Introduction

Related Information

[Understanding the Civic Platform Installation Process](#)

[Planning Your Civic Platform System Deployment](#)

[Planning the Installation](#)

Understanding the Civic Platform Installation Process

A basic Civic Platform installation is comprised of the following software components:

- **Web Server**

Civic Platform packages JBoss with Civic Platform components and deploys these to the web server. The web server receives instructions to construct and deliver web pages to a Civic Platform browser-based client, and provides information from the browser-based client to the application server for processing.

- **ColdFusion MX Web Server**

Civic Platform deploys the third-party tool ColdFusion MX to a web server. The ColdFusion MX web server provides the user interface environment for the Classic Admin pages.

- **Application Server**

Civic Platform packages JBoss with Civic Platform components and deploys these to the application server. The application server executes the main functionality of Civic Platform. The application server retrieves and writes record content to the database, and integrates with the web server to send and receive information to and from the client.

- **Database Server**

Civic Platform deploys components into an existing (Oracle or SQL Server) database. The database stores all Civic Platform record content, except for attachments.

You can install the following optional components:

- **Index Server**

The index server provides Civic Platform with the ability to perform global full-text searches across all Civic Platform records. Without the index server, Civic Platform can only perform exact match searches for record metadata within specified application types.

- **Accela Report Writer (ARW) Server**

Generates reports of information stored in the Civic Platform database. ARW uses the same database as Civic Platform.

- **Accela Document Services (ADS) Server**

Provides access to stored documents. ADS uses a different database instance than Civic Platform and ARW.

Planning Your Civic Platform System Deployment

The *Accela Civic Platform 9.0.0 System Planning Guide* contains detailed information to help you determine the appropriate network topology for your agency.

The number of concurrent Civic Platform users provides the single best criterion that predicts system load (number of transactions, searches, and so forth). Refer to the sample topologies for small (less than 50), medium (50 to 200) and large (more than 200) numbers of Civic Platform users provided in the System Planning Guide.

Planning the Installation

The following provides a high level sequence of activities that you should follow when performing a Civic Platform installation. You can determine whether or not to perform the indicated optional tasks based on your system requirements and the task description.

To set up the Civic Platform environment:

1. Review Environment Requirements

Prior to installing or upgrading to a new version of Civic Platform, review the hardware and software requirements of your deployment topology. For information on the environment requirements for the main hosts comprising a Civic Platform deployment, see the “Supported Environments” chapter in the corresponding version of the *Civic Platform Release Notes*.

2. Contact Accela Customer Support

Contact Accela Customer Support to obtain the installation files and supporting product documentation. You need to access one of Accela's authorized FTP sites to transfer the installation file to your target system before proceeding.

3. Obtain Accela Software License Key

Obtain an Accela software license key for the current release. Contact Accela Customer Support at 1-888-722-2352 ext. 5. Office hours are Monday–Friday 4:00am to 6:00pm Pacific Time.

4. Complete a Full Backup

Perform a full backup of your Accela software, database and any adapters. Follow the backup instructions in [Backing Up Civic Platform](#) and your internal guidelines for backing up and storing data.

5. Back Up Your Adapters

If you installed your own customized adapters or any third-party adapters (for example, a payment processing adapter) inside the JBOSS server, back it up. You need to redeploy the adapter after the installation process completes.

6. Remove Existing Civic Platform Instances

Starting with version 7.1.0, Civic Platform supports multiple Civic Platform instances. Only remove existing Civic Platform instances that are not useful (see [Installation Maintenance](#)).

7. Uninstall Conflicting Programs

Remove conflicting programs that use the same port numbers you plan to use for Civic Platform. You can view the current port number usage by the command "netstat -an" or a third-party tool like "fport."

8. Prepare Configuration Settings

Prepare the list of configuration settings you need for your installation (see [Configuration Checklist](#)). Do this before running the installer to make the installation process go more quickly.

To install the Civic Platform base components:

1. Run the Civic Platform Base Installer

Use the Civic Platform installation program to install the family of Civic Platform products and related third-party software. Refer to [Installing a Base Civic Platform](#).

2. Install or update the Civic Platform database

You can use the Civic Platform installer to install a new database, or to update an existing one (see [Managing a Civic Platform Configuration](#)). You can optionally use the Civic Platform Database Update installer or a manual procedure to update an existing database (see [Manually Upgrading the Civic Platform Database](#)).

3. Deploy the Latest Application Code

Run the installer to deploy Civic Platform application code (see [Installing the Latest Application Code](#)).

4. Import the Accela License

Log in to Civic Platform and import the Accela software license key you obtained from Accela Customer Support (see [Importing the License Key](#)).

5. Set Up a Firewall

For Civic Platform and add-on port configuration settings, contact Accela Customer Support at 1-888-722-2352 ext. 5. Office hours are Monday – Friday 4:00am to 6:00pm Pacific Time.

6. Check the Civic Platform Directory Structure

[Installation Directory Structure](#) explains the Civic Platform directory structure.

7. Perform Post Installation Configuration

Modify settings in the application server, the web server for the Civic Platform features to function correctly (see [Post Installation Server Configuration](#)).

To install additional Civic Platform tools and functionality:

1. Configure the SMS Adapter

Configure an SMS adapter web service for integration with SMS text messaging services (see [Configuring the SMS Adapter](#)).

2. Installing the Ad Hoc Report Tool

Install and configure the ad hoc report tool for the ad hoc report feature (see [Installing Ad Hoc Report Tool](#)).

3. Installing OCI Driver Configuration Tool

When the database server is Oracle 11g, if you prefer that Civic Platform servers use JDBC thin driver for connecting with the database, you can install the Oracle OCI driver configuration tool on all the Civic Platform server instances (except for the database server) (see [Installing Oracle 11g OCI Driver Configuration Tool](#)).

4. Upgrade the Civic Platform database for Nearby Query Support

If you want to enable the Nearby Query functionality, you must run the Nearby Query installer to upgrade the database with new geometry information columns (see [Upgrading the Database for Nearby Query Support](#)).

To prepare the Civic Platform client:

1. Configure the Browser

Modify settings in the browser for the Civic Platform features to function correctly (see [Browser Settings](#)).

2. Run the Accela Electronic Document Review Installer

Install Adobe Acrobat X Pro and .Net Framework 4.0 Client Profile, and then run the Accela Electronic Document Review installer (see [Electronic Document Review Client Installation](#)).

3. Install the Accela Document Scan Client

Install the Accela Document Scan client (see [Accela Document Scan Installation](#)).

4. Set Up the Cash Drawer

Set up the cash drawer for printing receipts in point of sale (POS) operations (see [Setting Up a Cashier Station](#)).

5. Install a Barcode Scanner

Install and configure an Intermec SR30 Handheld Scanner on client machines, so users can read and retrieve system generated invoices by scanning barcodes on invoices (see [Configuring Barcode Scanner](#)).

Preparing the Environment

You need to be aware of some basic environment-related requirements and options.

Related Information

[Hardware and Software Requirements](#)

[Setting Up Multi-Homed Servers](#)

[Installing the Database](#)

[Remote Installation](#)

[Installing ColdFusion MX 7.0](#)

Hardware and Software Requirements

For information on the hardware and software requirements for the main hosts comprising a Civic Platform deployment, see the “Supported Environments” chapter in the corresponding version of the *Accela Civic Platform Release Notes*.

Setting Up Multi-Homed Servers

Best practices prescribe installing Civic Platform using a multi-homed configuration. Multi-homed describes a computer host that has multiple IP addresses to connected networks. You configure physical connection between a multi-homed host to multiple data links that can be on the same or different networks.

If you install multiple Accela products on a single physical server, the recommended configuration is to set up a multi-homed environment on that server. IT professionals accomplish this by setting up multiple virtual IP addresses. Each Accela service requires a unique TCP/IPv4 address.

To set up multi-homed servers:

1. Go to the Network properties.
2. Choose **show all connections** or find a place to click in the Network properties.
3. Right-click the network card that you want to set up and choose properties.
4. Click Internet Protocol (TCP/IP) and then click the properties button.
5. Choose “Use the following IP address.”
6. Enter the base IP address for the NIC.
7. Click the **Advanced** tab.
8. Enter the multi-homed IP addresses one at a time in the advanced tab.

Installing the Database

Civic Platform requires an existing Oracle or MS SQL database server and database. If you have not yet installed your database, refer to the Oracle or MS SQL documentation to set up your database. Ensure that your database works well. Check the network connections and driver connections. For more information on the database installation and related preparation work, please refer to the respective database sections below.

Topics

- [Understanding Database Install and Upgrade Prerequisites](#)
- [Installing Oracle](#)
- [Installing MS SQL Server](#)
- [Transparent Data Encryption](#)

Understanding Database Install and Upgrade Prerequisites

Installing or updating the database requires the following information:

For Oracle:

- User with privileges to do database updates
- Password for that user
- TNS name of the database
- sqlplus. You must install sqlplus and make sure it exists in the PATH environment variable.
- (Required only for new installation) Manually grant access on DB packages “DBMS_RANDOM” and “DBMS_LOB” to public.
- (Required only for new installation) Manually create Civic Platform and Jetspeed database table spaces.
- The initial database password for the regular Accela and Jetspeed database user cannot have special characters such as !, #, -, _, etc. If your agency has a security policy that requires passwords to have special characters, passwords can be changed after the Civic Platform installer has created the database users.

For MS SQL Server:

- User with privileges to do database updates
- Password for that user
- Name of database
- Server name or IP address of the machine with the database
- Microsoft SQL server
- The initial database password for the regular Accela database user cannot have special characters such as !, #, -, _, etc. If your agency has a security policy that requires passwords to have special

characters, passwords can be changed after the Civic Platform installer has created the database users.

Installing Oracle

A DBA should choose to install one empty db (SID) while installing the Oracle database server software, or opt to do so during post installation. After the db (SID) installation, the DBA owns the SYS account and password.

The \$ORACLE_HOME/database or \$ORACLE_HOME/dbs directory needs to have at least 2G disk space for storing data files.



Note: If your agency is using Oracle 12c, you must add the following parameters in the sqlnet.ora file:

```
SQLNET.ALLOWED_LOGON_VERSION_SERVER=8
SQLNET.ALLOWED_LOGON_VERSION_CLIENT=8
```

The above sqlnet parameters replaced SQLNET.ALLOWED_LOGON_VERSION, which has been deprecated in Oracle 12c. For reference, see <https://docs.oracle.com/database/121/UPGRD/deprecated.htm#UPGRD52905>.

Installing MS SQL Server

Create a user account with SYSADMIN role and set the default database as master.

The MSSQL residing location (e.g. C:\Program Files\Microsoft SQL Server\MSSQL\Data) need to have at least 2G disk space for storing data files.

Transparent Data Encryption

You can encrypt data at rest using transparent data encryption or other disk encryption technologies. Accela Civic Platform has been successfully tested on Oracle and SQL Server databases that utilize [Transparent Data Encryption \(TDE\)](#).

IMPORTANT: If your agency implements TDE, you must implement it at the tablespace level for Oracle or at the database level for SQL Server.

Remote Installation

If you plan to run the Civic Platform base installer from your local computer, and install the Civic Platform modules to a remote server, please ensure the operating systems of the local and remote computers are the same. Both the operating systems must either be 64 bit or 32 bit.

Installing ColdFusion MX 7.0

The Civic Platform installer provides ColdFusion MX 7.0 or Railo. For ColdFusion MX 7.0, you need to provide your ColdFusion license after completing the installation.

Preparing Configuration Settings

Create a checklist of your system configuration settings and backup your system.

Related Information

[Configuration Checklist](#)

[Backing Up Civic Platform](#)

[Renaming Your Configuration Folder](#)

Configuration Checklist

A Civic Platform installation can use all the configuration settings from a prior Civic Platform instance as is, or use the configuration settings that you modify from a prior Civic Platform instance. You can also enter configuration settings manually, without using configuration settings from a prior installation.

[Civic Platform Component Configuration Parameters](#) lists the configuration parameters for Civic Platform components, along with example values and a space to write in your own values. Review this list and prepare your modifications or new values, before you run the installer.

Table 2: Civic Platform Component Configuration Parameters

Component	Parameter: (with Example Values)	Your Value
General	Have a total of approximately 6 IP addresses available.	
Recommendation	 Note: The actual total of IP addresses depends on whether the Accela core services are installed on separate servers or a multi-homed server.	
ColdFusion MX Web Server	<ul style="list-style-type: none"> • Host: aa.Accela-product.accela.com • IP address: 10.50.2.1 • HTTP port number: 80 • HTTPS port number: 443 • JBoss port bind base: 2 • SSO cookie domain: .accela.com • SMTP mail server: 10.50.1.23 • SMTP mail server port number: 25 	<ul style="list-style-type: none"> • • • • • • • •
Web Server	<ul style="list-style-type: none"> • Host: av.accela-product.accela.com • IP address: 10.50.2.2 • HTTP port number: 80 • HTTPS port number: 443 • JBoss port bind base: 4 	<ul style="list-style-type: none"> • • • • •

Component	Parameter: (with Example Values)	Your Value
Application Server	<ul style="list-style-type: none"> • IP address: 10.50.2.3 • JBoss port bind base: 3 (preset) • SMTP user name: authuser • SMTP user password: password 	<ul style="list-style-type: none"> • • • •
Index Server	<ul style="list-style-type: none"> • IP address: 10.50.2.4 • JBoss bind port base: 6 	<ul style="list-style-type: none"> • •
ARW Server	<ul style="list-style-type: none"> • Host name: reporting.Accela-product.accela.com • IP address: 10.50.2.4 • HTTP port number: 80 • JBoss port bind base: 9 	<ul style="list-style-type: none"> • • • •
ARW Server with Oracle Database	<ul style="list-style-type: none"> • DB TNS name: reporting • DB username: reportUser • DB login password: reportUser • DB IP address: 10.50.0.26 • DB port number: 1521 • DB SID: reporting 	<ul style="list-style-type: none"> • • • • • •
ARW Server with MS SQL Server Database	<ul style="list-style-type: none"> • DB ODBC name: reporting • DB login username: reportUser • DB login password: reportUser • DB server: reporting_sqlserver • DB port number: 1433 • Database name: reporting 	<ul style="list-style-type: none"> • • • • • •

Component	Parameter: (with Example Values)	Your Value
ADS Server	<ul style="list-style-type: none"> IP address: 10.50.2.7 HTTP port: 80 JBoss bind port base: 7 	<ul style="list-style-type: none"> • • •
ADS Server with Oracle Database	<ul style="list-style-type: none"> DB IP address: 10.50.0.26 DB port number: 1521 Service name: proj1 DB username: ads DB login password: adspw 	<ul style="list-style-type: none"> • • • • •
ADS Server with MS SQL Server Database	<ul style="list-style-type: none"> IP address: 10.50.0.35 Port: 1433 Database name: ADS User name: vchtrans Password: vchtrans 	<ul style="list-style-type: none"> • • • • •

Component	Example\Default Port Values	Notes
Report server	<ul style="list-style-type: none"> HTTP: 80 JBoss port bind base: 3 	Note 2
Report server with Oracle database	• DB: 1521	
Report server with MS SQL Server database	• DB: 1433	
Mobile Office server	• DB:1433	
Citizen Access server	• App server: 3080 or 3443	
Accela IVR server	<ul style="list-style-type: none"> Tomcat: 8080 Tomcat shutdown: 8005 App server: 3080 	Note 4
Accela Gateway server	• HTTPS: 443	Note 5
Accela GIS server	• 9080 or 3080	

- **Note 1:** Port Bind Base is the base number for all other ports except HTTP and HTTPS ports. The value should typically be a single-digit or double-digit between 1~65 (such as 2, 3, etc.), and becomes the ‘thousands’ prefix for all other pre-defined values. The ‘Port Bind Base’ concept applies to the setup of other Accela products. Each Accela product if installed on the same server should have a unique base.
- **Note 2:** If the server is on the same host as the application server, they have the same IP address, use a different HTTP port number and HTTPS port number from the ones used for the application server ([Setting Up Multiple-Homed Servers](#)).
- **Note 3:** Application server clients specify port 3080 as the default port for communicating with the application server. Reserve JBoss binding port base 3 for the application server.
- **Note 4:** Use unique port numbers for multiple Tomcat instances.
- **Note 5:** Accela Mobile Gateway can support multiple application servers. Each supported application server uses a different port.

Backing Up Civic Platform

Before you remove a base installation of Civic Platform, make a back-up of your Civic Platform files and registry settings, as described below.

The examples used in this section assume that you install Civic Platform on the D: drive.

Back Up Your Civic Platform Files:

1. Copy the entire D:\Accela folder.
2. Paste it to another location for safe keeping.

Back Up Your Accela Registry Settings:

1. Go to the Windows Registry Editor, via **Start > Run > regedit**.
2. If the Operating System is 32 bit, locate

```
HKEY_LOCAL_MACHINE\SOFTWARE\Accela Inc
```

if the Operating System is 64 bit, locate

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Accela Inc
```

3. Right-click > Export this folder. Save the file as

```
D:\Accela_backup\9.0.0\yourregistryfile.reg
```

Files Automatically Backed Up During Uninstall

When you uninstall a previous version of Civic Platform, the uninstall process automatically creates a backup folder and stores your ServerConfig.properties files in \\Accela_backup\\<version #>. For example, D:\Accela_backup\9.0.0.

You can refer to these configuration files when you perform a fresh installation of Civic Platform. These files contain the ports, the port bind bases, host names, IP addresses, and other crucial information needed when performing a new installation. The original installation location for these files is listed below.

ADS Server:

```
D:\Accela\av.ads\conf\av\ServerConfig.Properties
```

Application Server:

```
D:\Accela\av.biz\conf\av\ServerConfig.Properties
```

ColdFusion MX Web Server:

```
D:\Accela\av.cfmx\conf\av\ServerConfig.Properties
```

Index Server:

```
D:\Accela\av.indexer\conf\av.indexer\ServerConfig.Properties
```

Reporting Server:

```
D:\Accela\av.arw\conf\av\ServerConfig.Properties
```

Web Server:

```
D:\Accela\av.web\conf\av\ServerConfig.Properties
```

Renaming Your Configuration Folder

Starting with version 7.1.0, you can use the configuration of existing Civic Platform instances as the basis for the configuration of a to-be-installed instance. If you plan to use the configuration file from a prior instance, but want to delete the instance, rename the directory that contains the configuration of the existing instance so that the uninstall program does not remove it.

The \$\av.xxx\conf folders contain the configuration files. Rename these folders to prevent the uninstall program from removing them.

Installing Civic Platform Components

This section contains the following topics. Review each topic prior to installing the Civic Platform components.

Related Information

[Installation](#)

[Installation Directory Structure](#)

[Post Installation Configuration](#)

[Installation Maintenance](#)

[Troubleshooting](#)

Installation

Installing Civic Platform involves the following procedures.

Related Information

[Installing the Base Civic Platform 9.0.0](#)

[Manually Upgrading the Civic Platform Database](#)

[Installing the Latest Application Code](#)

Installing the Base Civic Platform 9.0.0

Topics

- [Understanding the Civic Platform Installation Environment](#)
- [Managing a Civic Platform Configuration](#)
- [Installing Civic Platform Components](#)

Understanding the Civic Platform Installation Environment

To install Civic Platform 9.0.0 you must uninstall previous versions and perform a fresh installation of the Civic Platform 9.0.0 base and 9.0.2 application.

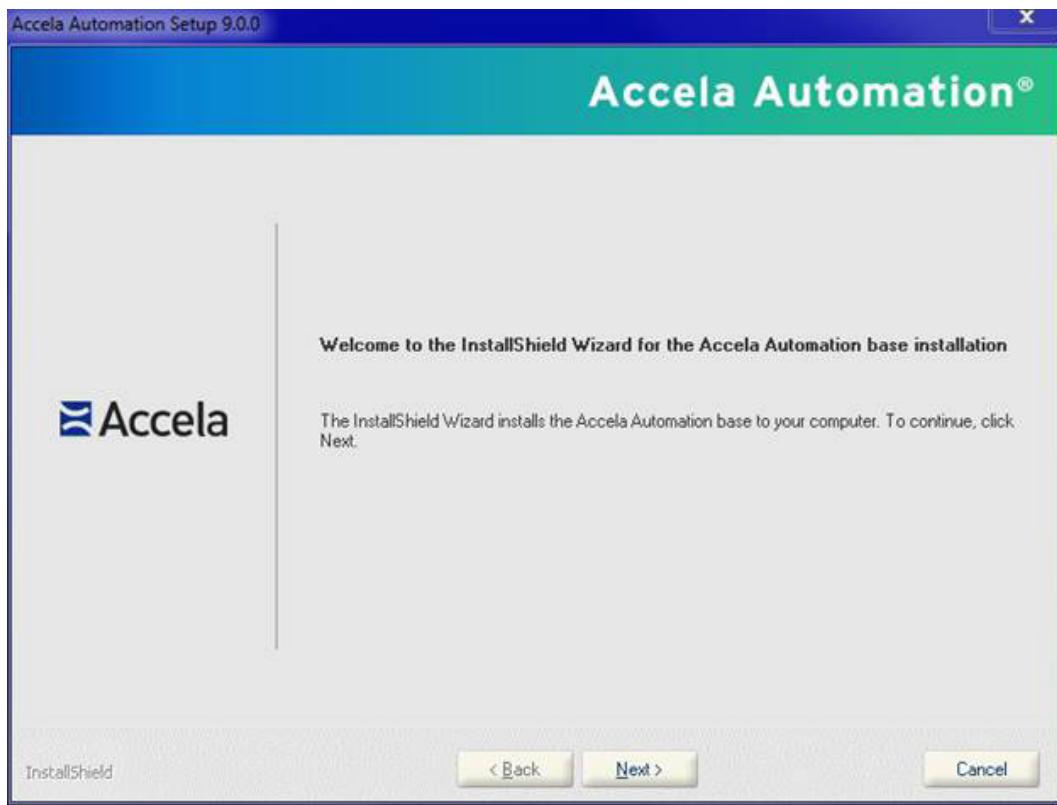
We highly recommend that you do not install Civic Platform 9.0.0 on the same server as any previous version. If you plan to keep your 8.0.x installation, you must install 9.0.0 on a different server.

Using the Configuration Checklist as a Guide

The [Configuration Checklist](#) provides a listing of the configuration parameters associated with a Civic Platform instance. Prior to running the Civic Platform installer, write down the parameter values you want to use for your new installation. You can obtain these parameter values from your previous installation's ServerConfig.Properties files, which are backed up automatically to a folder named Accela_backup when you uninstall the previous version. Refer to [Files Automatically Backed Up During Uninstall](#).

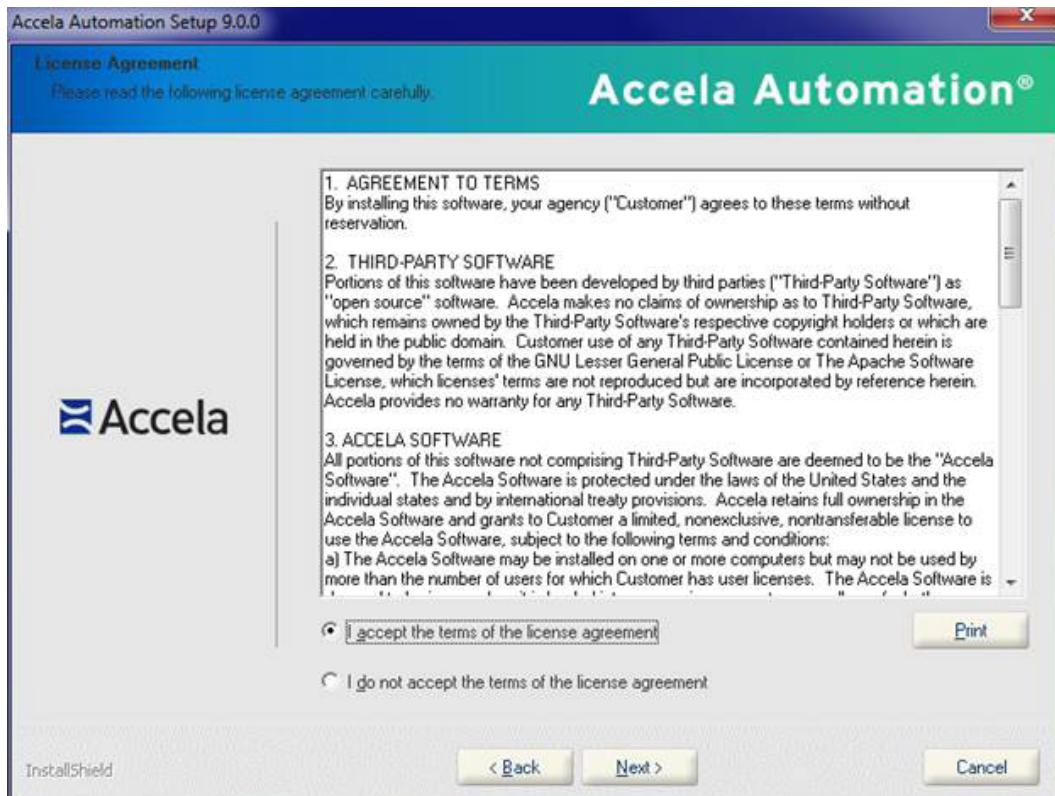
To install the Civic Platform 9.0.0 Base:

1. Back up your current Accela directory. See [Backing Up Civic Platform](#).
2. If you want to use your previous instance to populate certain screens during this installation, rename your configuration folder. See [Renaming Your Configuration Folder](#).
3. Uninstall any previous version of Civic Platform. Refer to [Installation Maintenance](#).
4. Double-click AABase_9.0.0.exe in the setup folder to start the Civic Platform base installer.
The Civic Platform Preparation and Setup screens display.



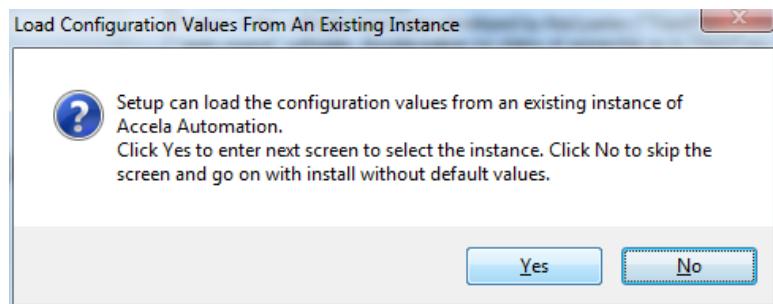
- Click **Next** to continue.

This License Agreement screen displays.



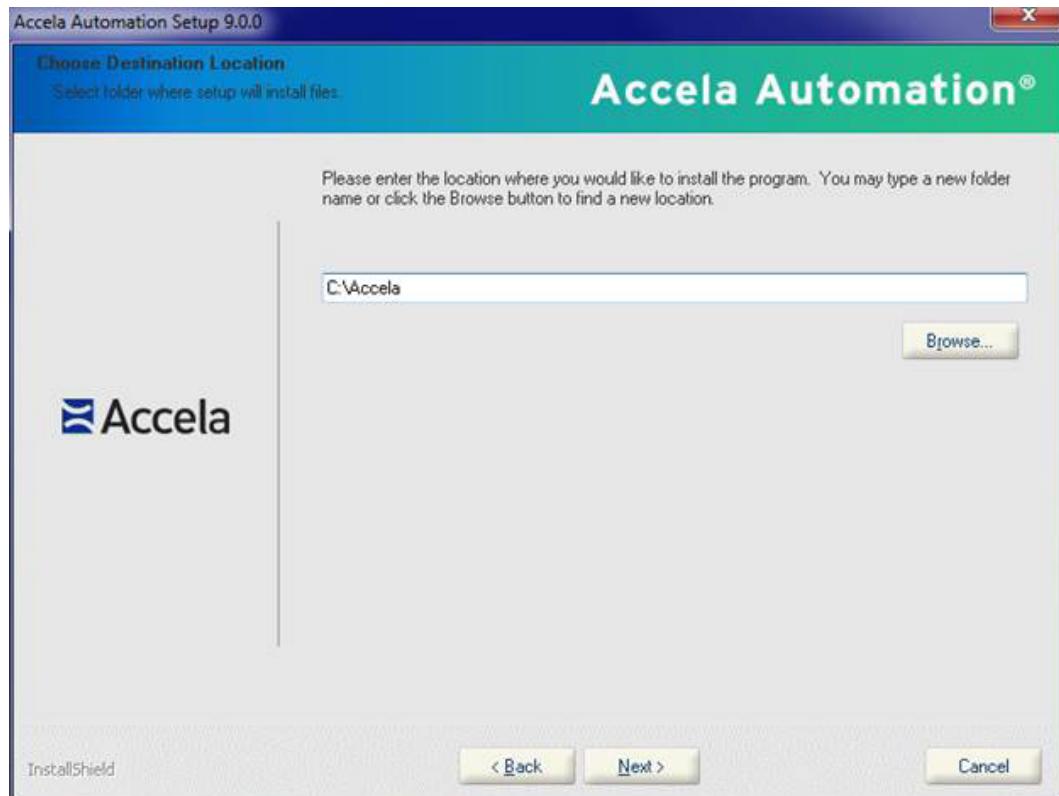
- Accept the terms of the license agreement, and then click **Next**.

Civic Platform displays the Load Configuration Values From An Existing Instance prompt.



7. Click **No** to manually enter the configuration values.

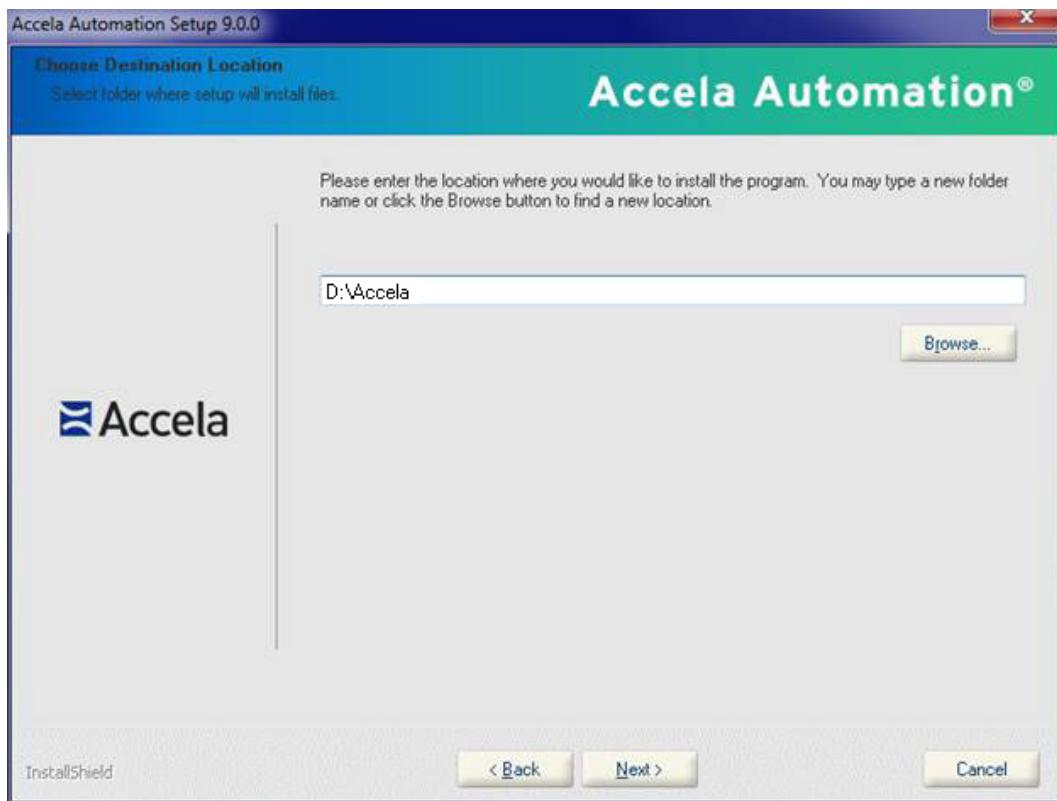
Civic Platform displays the Enter Instance Name screen.



8. Enter the instance name (for example; prod_9.0.0, test_9.0.0, or dev_9.0.0), and then click **Next**.

The installer uses the name as part of the service name. The hotfix installer uses this name (see [Installing the Latest Application Code](#)). The instance name identifies the Civic Platform instance that you are installing; it can be helpful to include the version number in the instance name.

Civic Platform displays the Choose Destination Location screen.



9. By default the destination folder is C:\Accela, however it is best practice to install Civic Platform on a drive designated for data storage, typically the D drive. This can safeguard your Civic Platform implementation, as this drive is not typically effected by automatic Windows updates, and is often scheduled for backups by IT staff, according to best practices.

You can accept the default location or click **Browse** to choose a different location. Do not include spaces in the destination folder name.

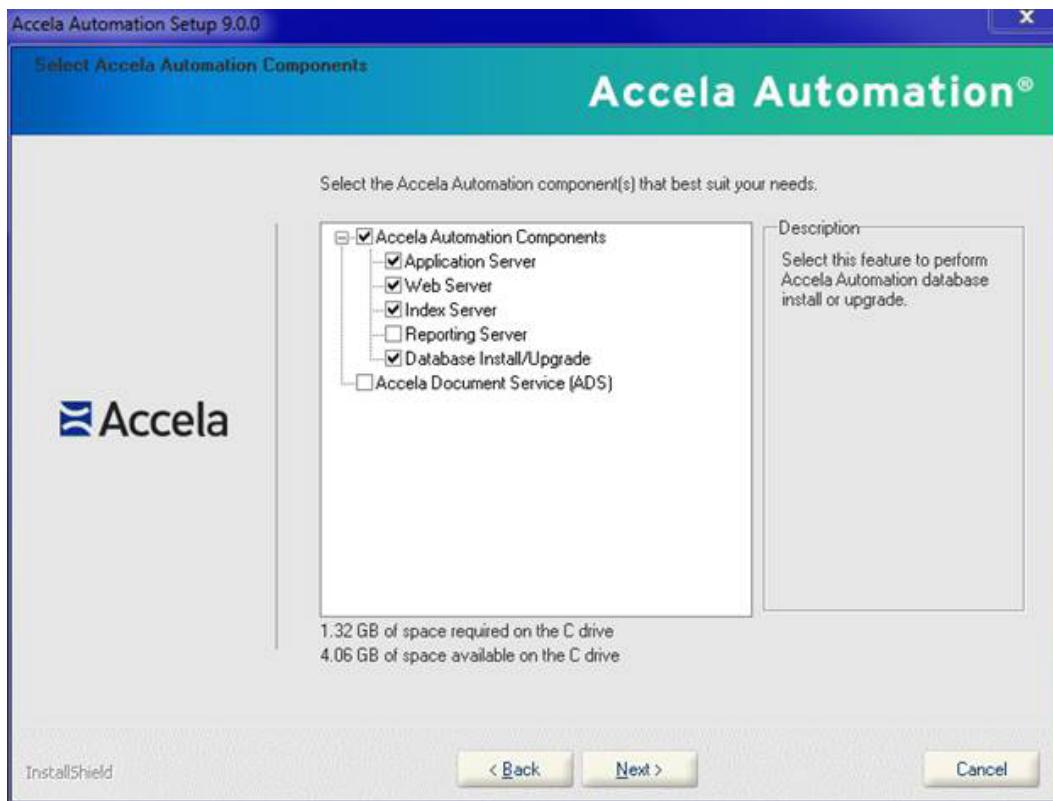
When you're done choosing the destination, click **Next**.

10. Select the Civic Platform components to install (See [Managing a Civic Platform Configuration](#)).

Managing a Civic Platform Configuration

This section provides instructions on how to manage components of your Civic Platform installation. You can add, remove, repair, or configure components.

You access this screen either when you perform a new installation, as is the case for the 9.0.0 installation described in the preceding steps, or when you perform maintenance on an existing installation (see [Installation Maintenance](#)).



1. Perform the steps in the preceding section.
2. Select the **Database Install/Upgrade** option and any other Civic Platform components you want install, and then click **Next**.



Note:

- a) When installing Civic Platform 9.0.0, select the Database Install/Upgrade option in this screen.
- b) If your implementation will be accessed by external users, for example Citizen Access users, you must use full server names *including the domain name* (for example, hostname.domain.com), when installing Civic Platform components.
- c) To install a new database, you must use the Database Install/Upgrade option in this screen. If you are upgrading the database, you can use either the Database Install/Upgrade option or the manual procedure for updating the database (see [Manually Upgrading the Civic Platform Database](#)).

Topics

- [Configuring the ColdFusion MX Web Server and Civic Platform Web Server](#)
- [Configuring the Index Server](#)
- [Configuring the Application Server](#)
- [Configuring the Reporting Server](#)
- [Configuring the Application Server Database](#)
- [Configuring the Reporting Server Database](#)
- [Configuring a New or Upgraded Database](#)

- Configuring the Accela Document Service (ADS)

Configuring the ColdFusion MX Web Server and Civic Platform Web Server

The Civic Platform web server configuration consists of two parts; 1) configuring the optional ColdFusion MX web server, and 2) configuring the Civic Platform web server.



Note:

You can configure ColdFusion as part of a Civic Platform installation or ADS server installation.

To configure the ColdFusion MX web server and web server:

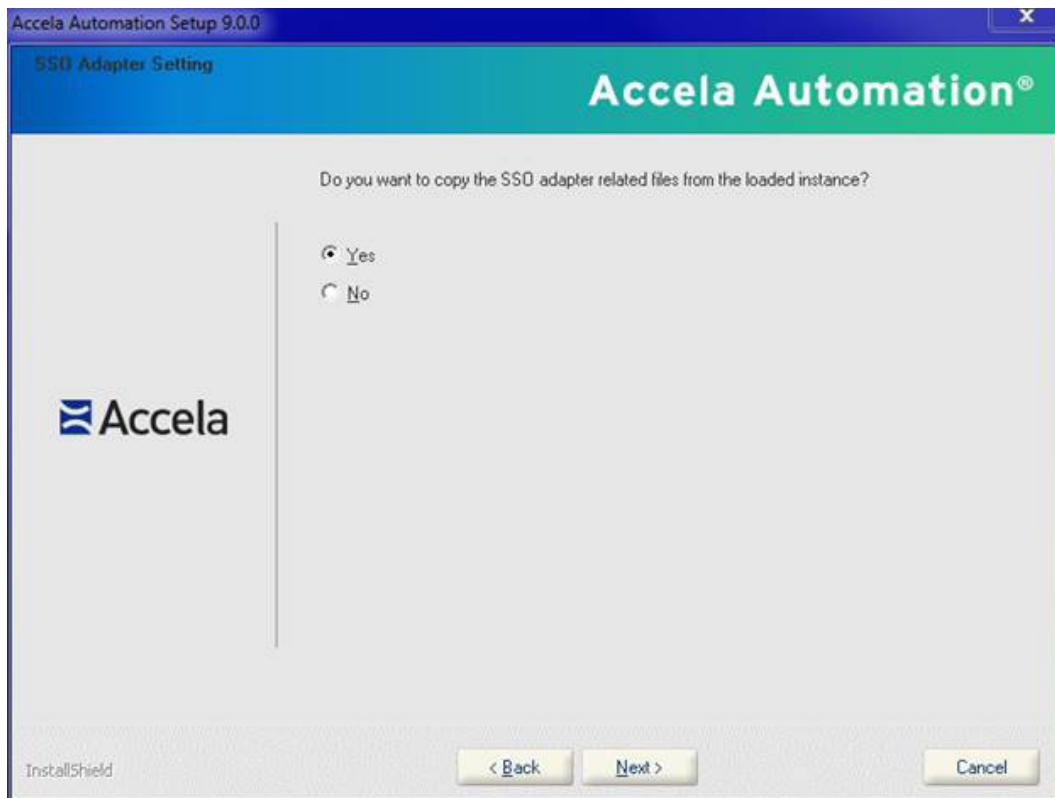
1. Access the web server configuration by selecting the **Web Server or Accela Document Service (ADS)** check box in the Select Civic Platform Components screen (see [Managing a Civic Platform Configuration](#)).
2. If you selected to load configuration values from an existing Civic Platform instance, and the instance contains customized SSO adapter files, the installer requires you to select whether to use the existing SSO adapter files.



Note:

- a) If the installer detects no existing SSO adapter files to copy, the installer skips this step, and copies default SSO adapter files to the web server.
- b) Because the installer copies the SSO adapter files to both the web server and the application server, you must select the same option in the SSO Adapter Setting screen for both the web server installation and the application server installation.

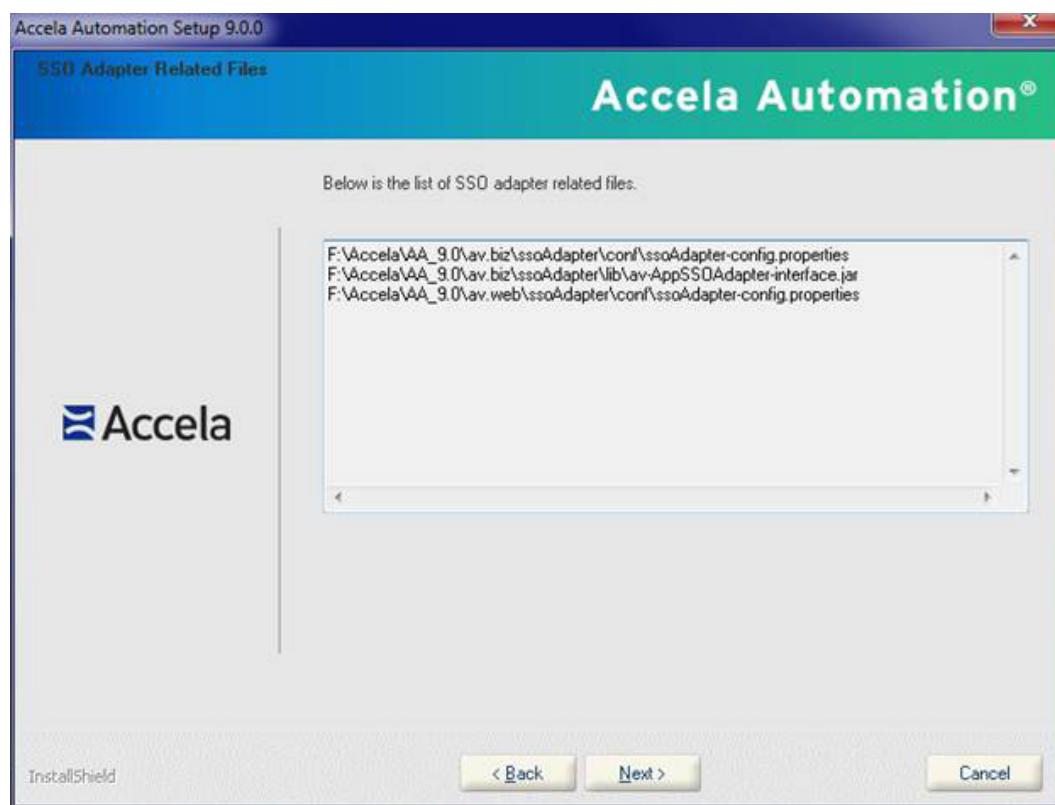
The SSO Adapter Setting screen displays.



- a. Click **Yes** to copy the SSO adapter files from the existing instance.

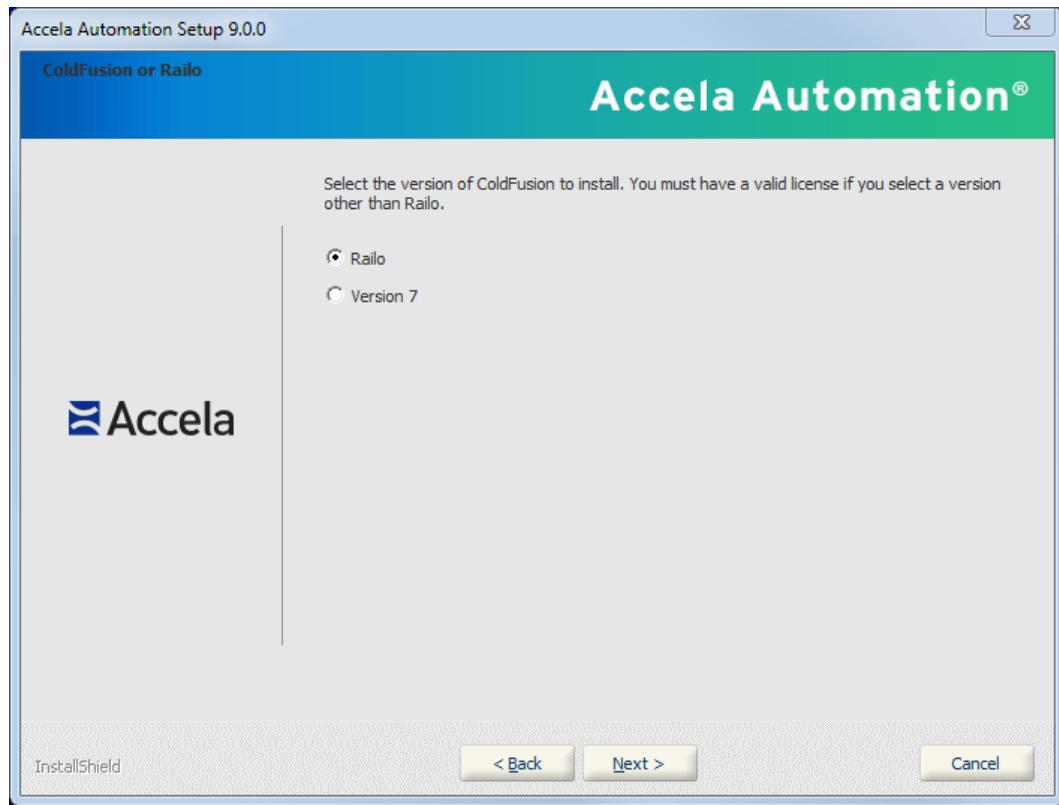
- b. Click **No** to copy default SSO adapter files to the web server.

The SSO Adapter Related Files screen displays.



3. Click **Next**.

The ColdFusion or Railo screen displays.

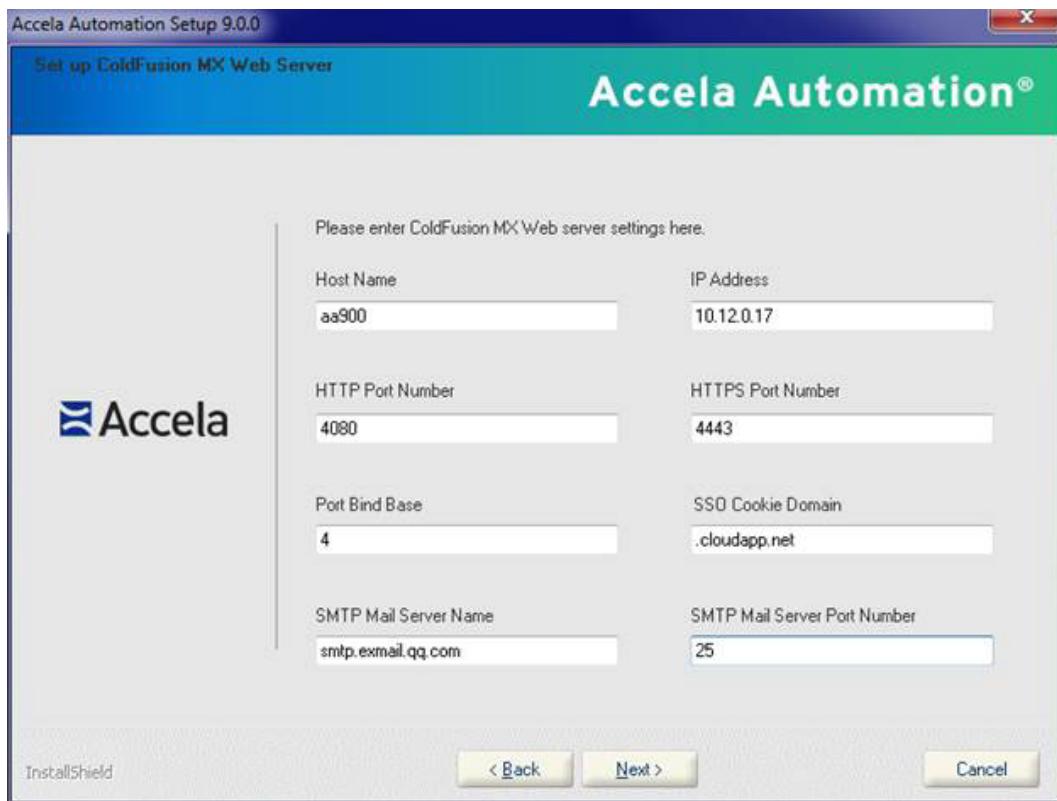


4. Select the ColdFusion version you want to install.

For information on using Railo, refer to the Accela Success Community.

5. Click **Next** to continue.

The Set up ColdFusion MX Web Server screen displays.



6. Enter parameter values for the ColdFusion web server.

You can use the parameter values from your previous installation; these values are stored in \\Accela_backup\\<version>\\av.cfmx\\av.cfmx.ServerConfig.properties. Refer to [Files Automatically Backed Up During Uninstall](#).



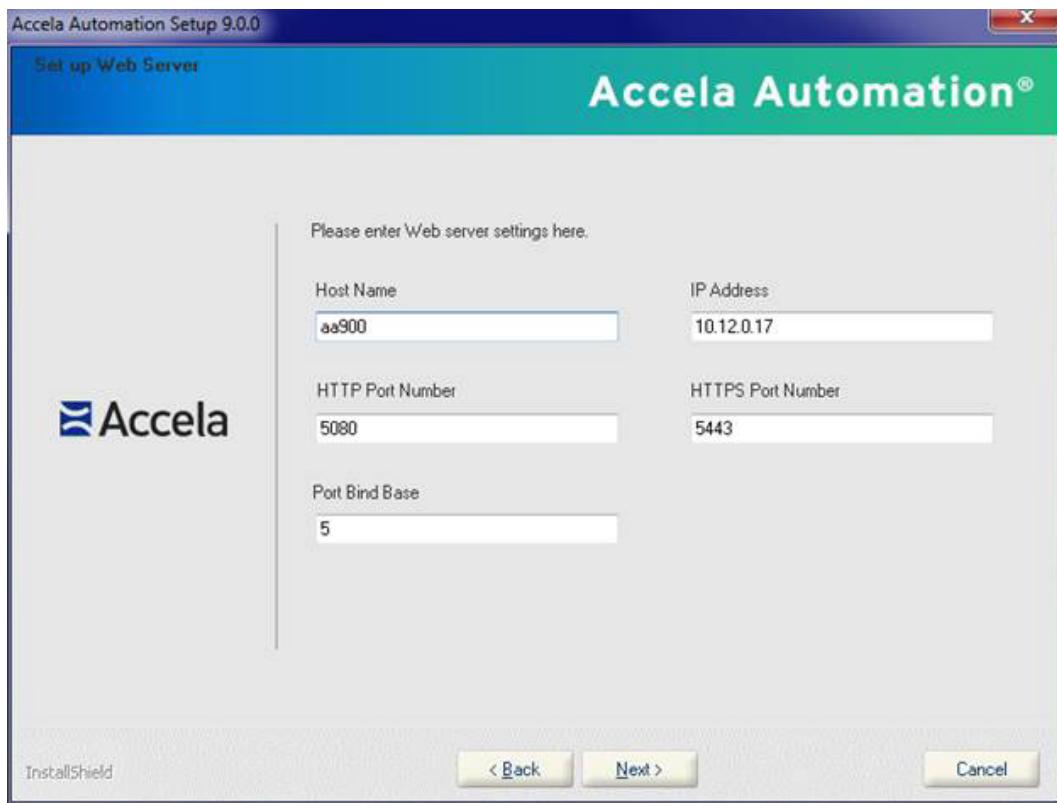
Note:

(1) You must enter values in SSO Cookie Domain, SMTP Mail Server Name and SMTP Mail Server Port Number. The Port Bind Base field is the base number for all other ports except HTTP and HTTPS ports. The value must typically be a single-digit or double-digit between 1~65 (such as 2, 3, etc.), and becomes the “thousands” prefix for all other pre-defined values. The Port Bind Base concept applies to the setup of other Accela products. Each Accela product if installed on the same server should have a unique base.

(2) Use the broadest part of your domain when entering the SSO Cookie Domain values. For example, if your host name is aa.prod.accela.com, your SSO Cookie Domain must be .accela.com.

7. Click **Next to complete the ColdFusion MX web server configuration.**

The Set up Web Server screen displays.



8. Enter configuration parameter values for the Civic Platform web server.

You can use the parameter values from your previous installation; these values are stored in \\Accela_backup\\<version>\\av.web\\av.web.ServerConfig.properties. Refer to [Files Automatically Backed Up During Uninstall](#).



Note:

If the web server is on the same host as the application server, they have the same IP address, use a different HTTP port number and HTTPS port number from the ones used for the application server.

9. Click **Next** to complete the web server configuration.

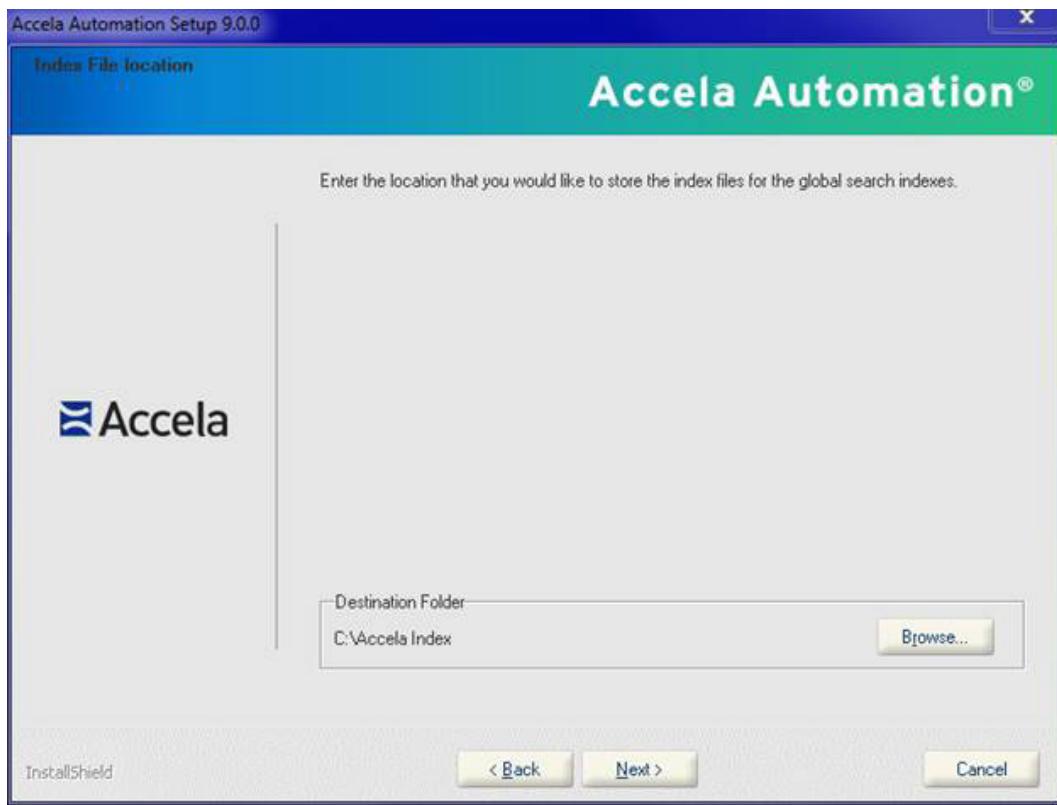
Configuring the Index Server

The index server enables the global search function in Civic Platform.

To configure the index server:

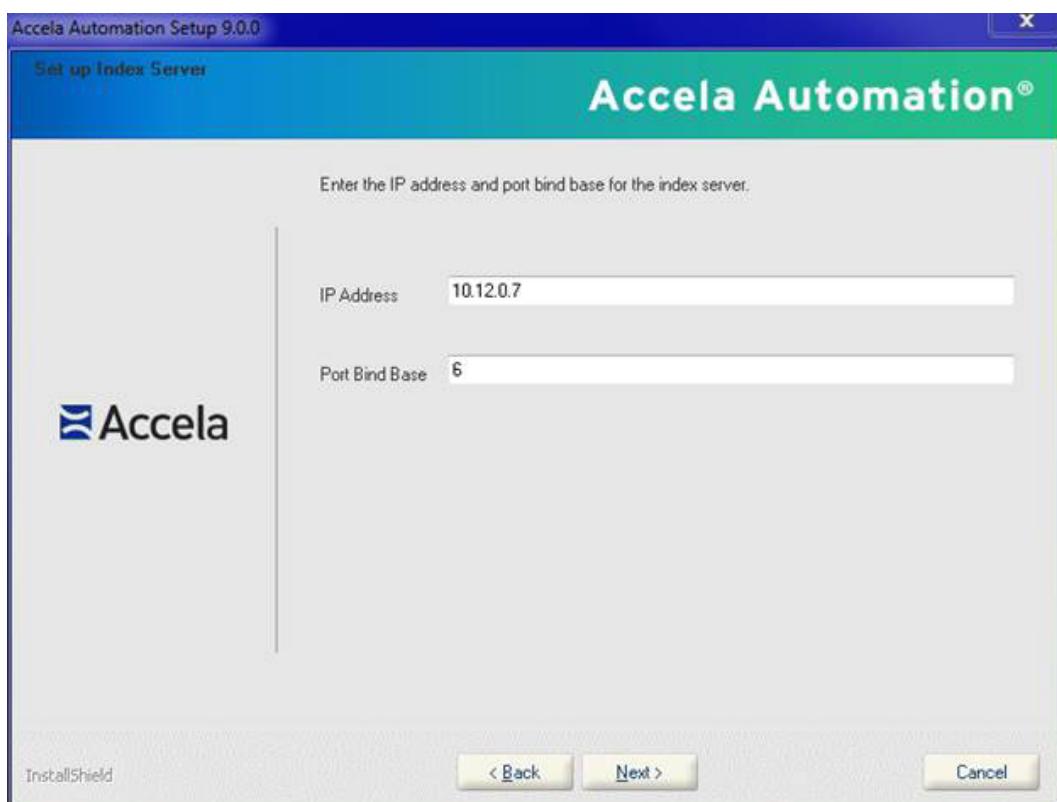
- Access the index server configuration by selecting the Index Server check box in the Select Civic Platform Components screen (see [Managing a Civic Platform Configuration](#)).

The Index File Location screen displays.



2. Click **Browse** and change the folder name from Index to Accela Index, then click **OK**.
3. Click **Next**.

The Set up Index Server screen displays.



4. Enter the IP address and Port Bind Base.

You can use the parameter values from your previous installation; these values are stored in \\Accela_backup\\<version>\\av.indexer\\ServerConfig.properties. Refer to [Files Automatically Backed Up During Uninstall](#).

5. Click **Next to complete the index server configuration.**

Configuring the Application Server

To configure the application server:

1. Access the application server configuration by selecting the **Application Server** check box in the Select Civic Platform Components screen (see [Managing a Civic Platform Configuration](#)).
2. If you selected to load configuration values from an existing Civic Platform instance and the instance contains customized SSO adapter files, the installer requires you to select whether to use the existing SSO adapter files.

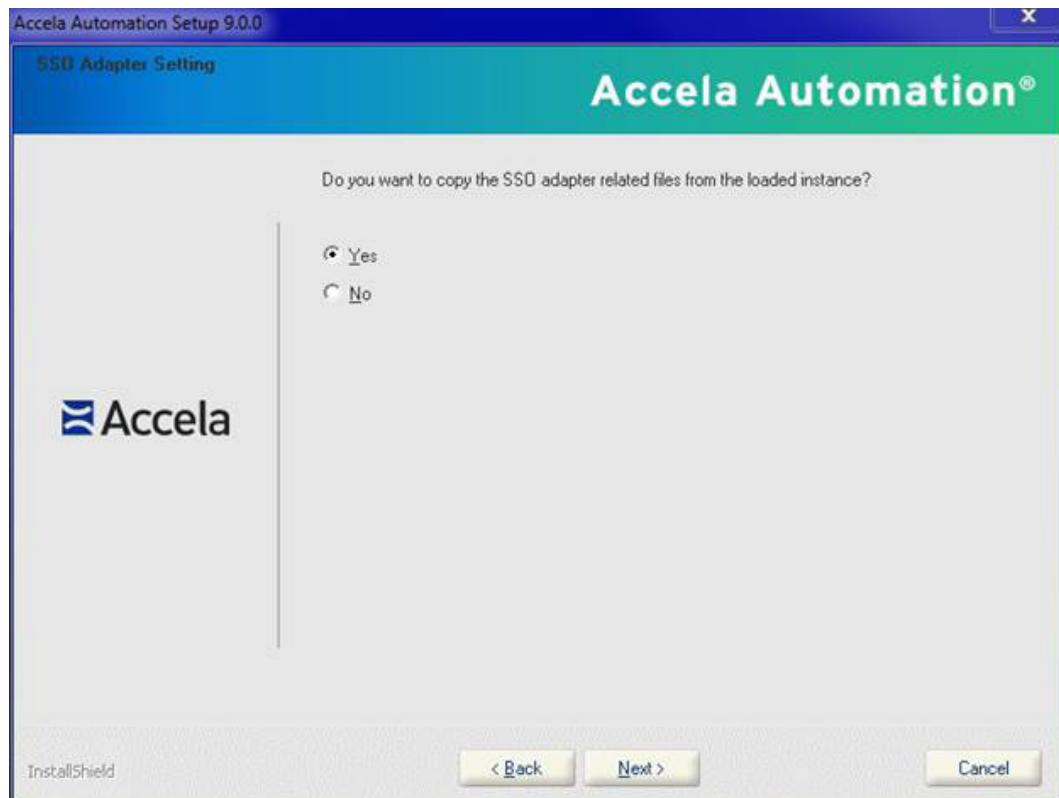


Note:

If the installer detects no existing SSO adapter files to copy, the installer skips this step, and copies default SSO adapter files to the application server.

Because the installer copies the SSO adapter files to both the web server and the application server, you must select the same option in the SSO Adapter Setting screen for both the web server installation and the application server installation.

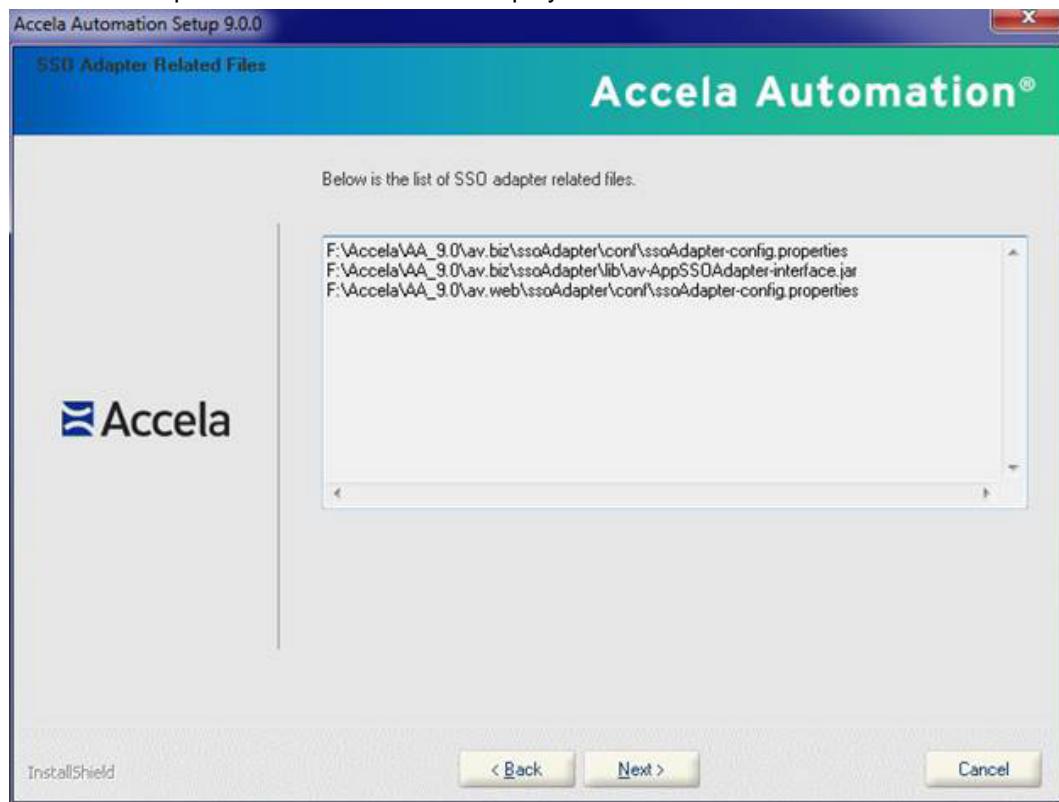
The SSO Adapter Setting screen displays.



a. Click **Yes** to copy the SSO adapter files from the existing instance.

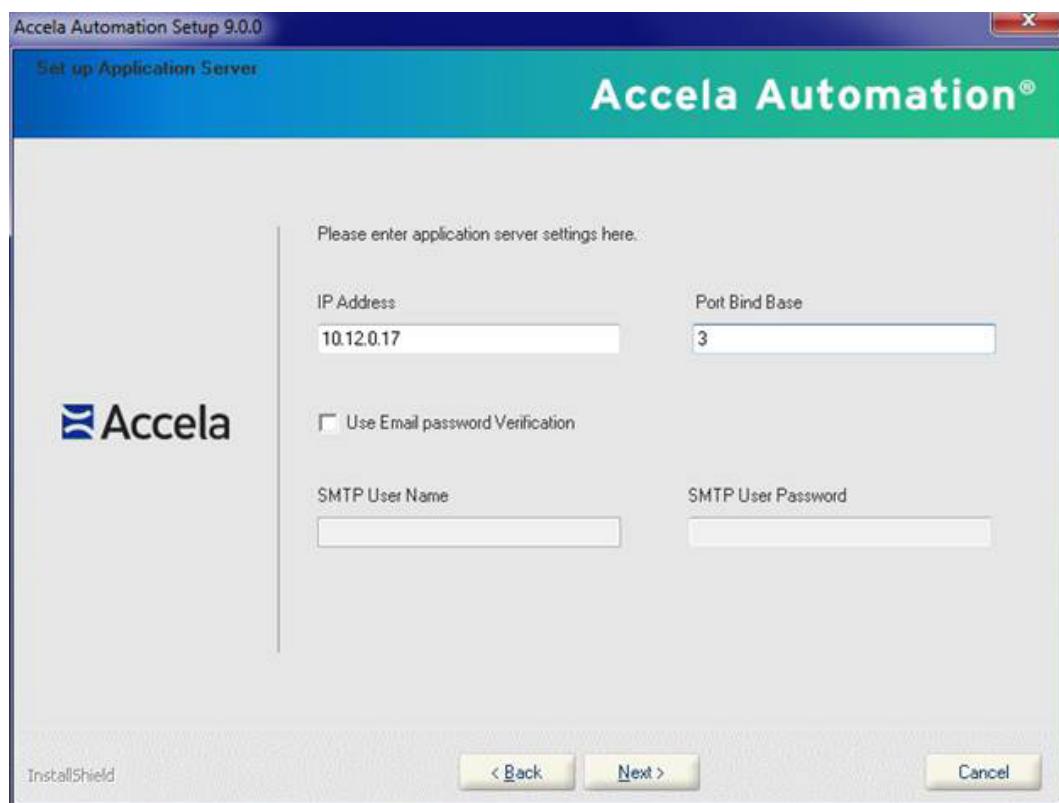
b. Click **No** to copy default SSO adapter file to the web server.

The SSO Adapter Related Files screen displays.



3. Click Next.

The Set Up Application Server screen displays.



4. Enter configuration parameter values for the Civic Platform application server.

You can use the parameter values from your previous installation; these values are stored in \\Accela_backup\\<version>\\av.biz\\ServerConfig.properties. Refer to [Files Automatically Backed Up During Uninstall](#).



Note:

Only select Email password verification if your mail server requires that you use a user name and password to send email. Otherwise leave the check box unchecked and leave the SMTP User Name and Password fields blank.



Note:

The Accela wireless server communicates with the Accela application server through port 3080 in the current Accela hosted solution. Use 3 as the JBoss binding port base for the application server.

5. Click **Next to continue.**

Configuring the Reporting Server



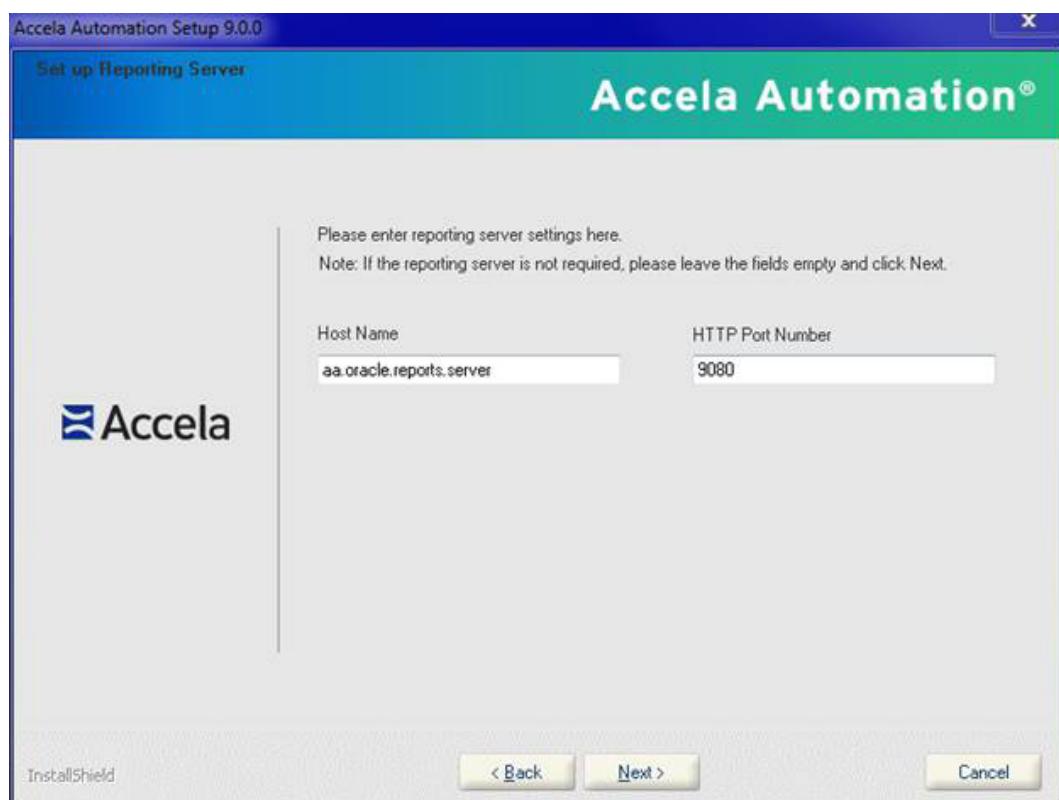
Note:

The reporting server is the same as the Accela Report Writer (ARW) server.

To configure the reporting server:

- Access the application server configuration by selecting the **Reporting Server** check box in the Select Civic Platform Components screen (see [Managing a Civic Platform Configuration](#)).

The Set up Reporting Server screen displays.



- Enter configuration parameter values for the Civic Platform reporting server.

**Note:**

If the reporting server is on the same host as the application server, they have the same IP address, use a different HTTP port number from the one used for the application server.

3. Click **Next** to continue.

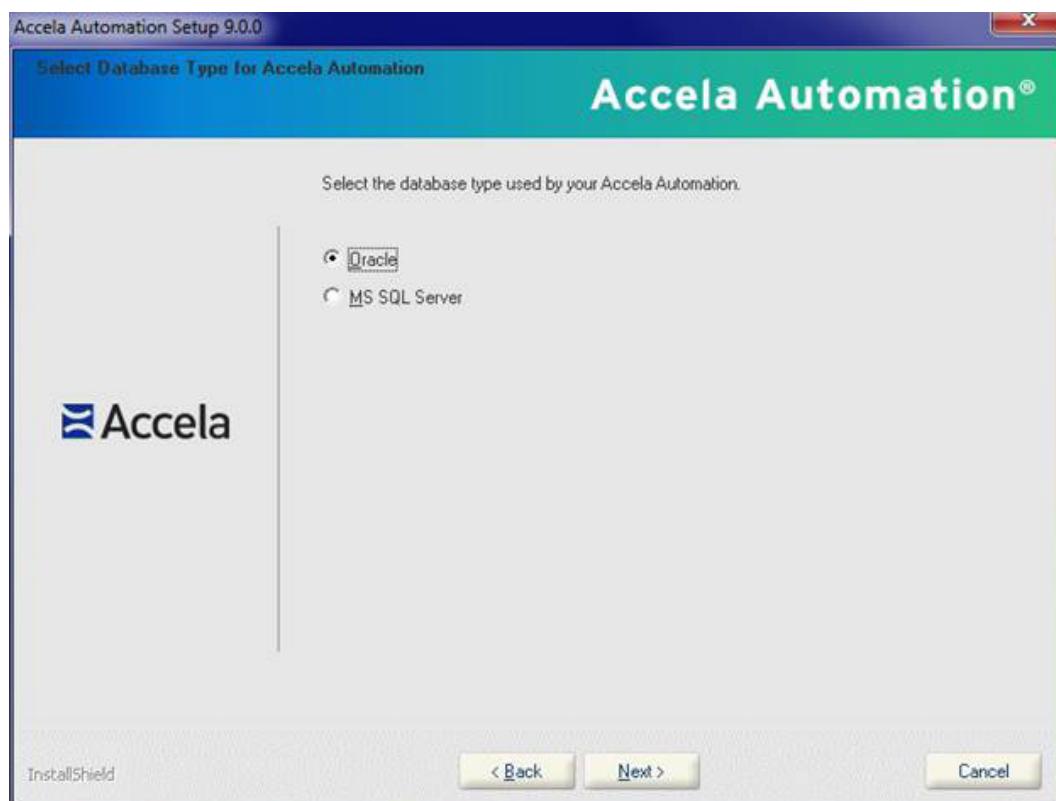
Configuring the Application Server Database

This section provides instructions to configure the application server database when you select the Database Install/Upgrade option (see [Managing a Civic Platform Configuration](#)). This procedure supports configuration of Oracle or SQL Server database servers.

To configure the application server database:

1. Access the application server database configuration by selecting the **Database Install/Upgrade** check box in the Select Civic Platform Components screen (see [Managing a Civic Platform Configuration](#)).

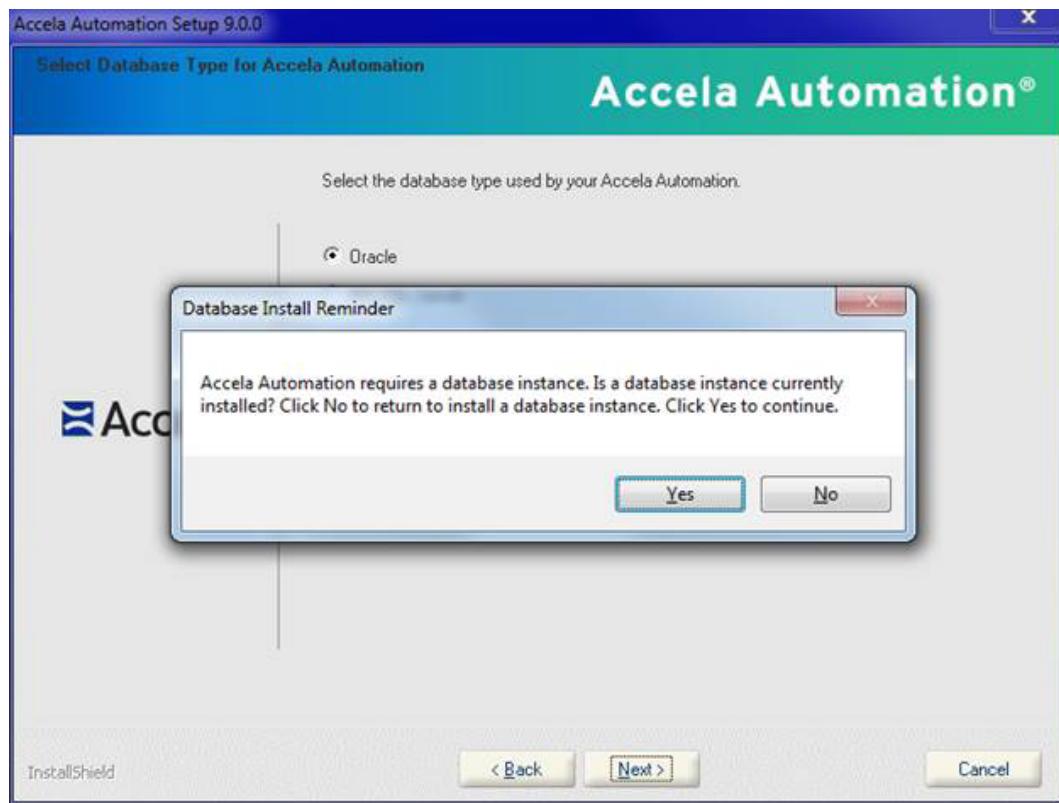
The Select Database Type for Civic Platform screen displays.



2. Select the database server type.

3. Click **Next** to continue.

The Civic Platform installer may prompt you about whether you already installed a database.



4. Click Yes or No.

- Click **No** if you have not yet installed a database.

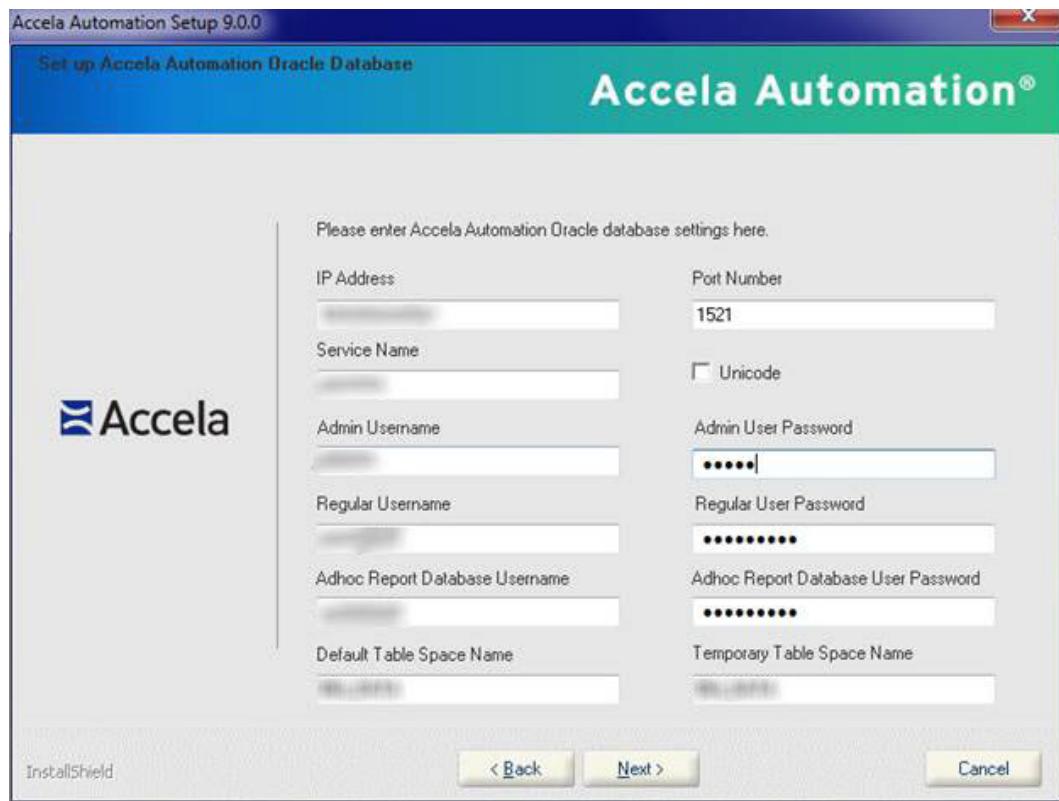
The installer returns to the Select Civic Platform Components window.

Select the Database Install/Update option to install a database (see [Managing a Civic Platform Configuration](#)).

or,

- Click **Yes** if you have an existing instance of a database that you want to upgrade.

5. Configure an Oracle database (see [The Set up Civic Platform Oracle Database screen](#)) or SQL Server (see [The Setup Civic Platform MS SQL Server Database screen](#)) database.



 **Note:** For the **Regular User Password** and **Adhoc Report Database User Password** fields, do *not* include special characters such as !, #, -, _, etc. If your agency has a security policy that requires passwords to have special characters, passwords can be changed after the Civic Platform installer has created the database users.

Figure 1: The Set up Civic Platform Oracle Database screen

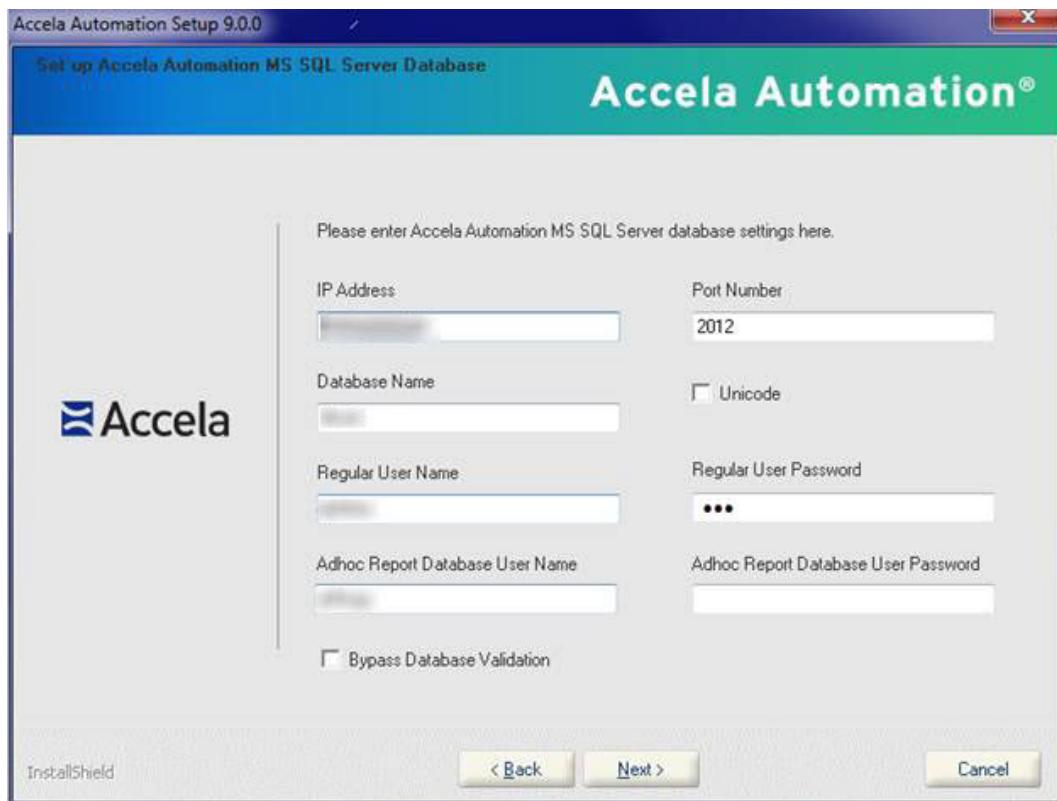


Figure 2: The Setup Civic Platform MS SQL Server Database screen

 **Note:** For the **Regular User Password** and **Adhoc Report Database User Password** fields, do *not* include special characters such as !, #, -, _, etc. If your agency has a security policy that requires passwords to have special characters, passwords can be changed after the Civic Platform installer has created the database users.

6. Enter parameter values for the Oracle database server or the SQL Server database server.

 **Note:**

If you mark **Bypass Database Validation**, the installation program does not validate the database settings before continuing to the next step. **Unicode** is for I18N multilingual support.

7. Click **Next** to continue.

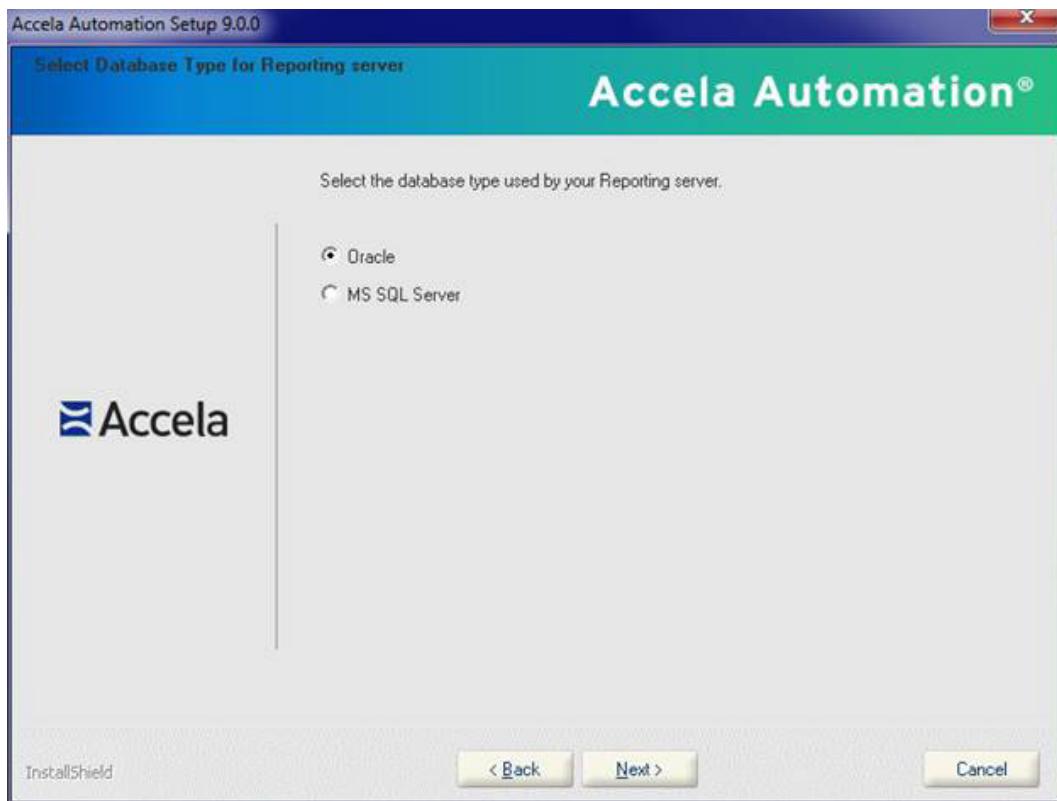
Configuring the Reporting Server Database

This section provides instructions to configure the reporting server database when you de-select the Database Install/Upgrade option (see [Managing a Civic Platform Configuration](#)). This procedure supports configuration of Oracle or SQL Server database servers.

To configure the reporting server database:

1. Access the reporting server database configuration by de-selecting the **Database Install/Upgrade** check box in the Select Civic Platform Components screen (see [Managing a Civic Platform Configuration](#)).

The Select Database Type for Reporting Server screen displays.



2. Select the database server type.

3. Click **Next** to continue.

The Civic Platform installer may prompt you about whether you already installed a database.

4. Click **Yes** or **No**.

- Click **No** if you did not install a database yet.

The installer returns to the Select Civic Platform Components window.

Select the Database Install/Update to install/update a database (see [Managing a Civic Platform Configuration](#)).

or,

- Click **Yes** if you installed a database.

5. Configure an Oracle (see [The Set up Civic Platform Oracle Database screen](#)) or SQL Server (see [The Setup Civic Platform MS SQL Server Database screen](#)) database for the reporting server.

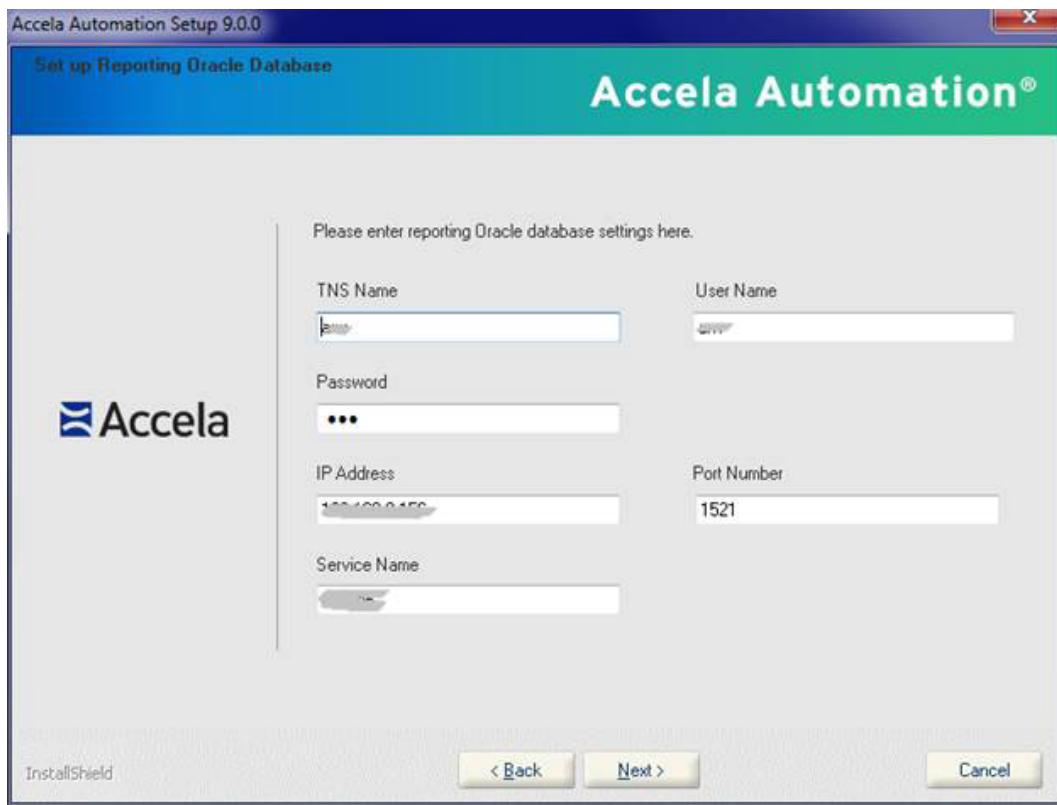


Figure 3: The Set up Reporting Oracle Database screen

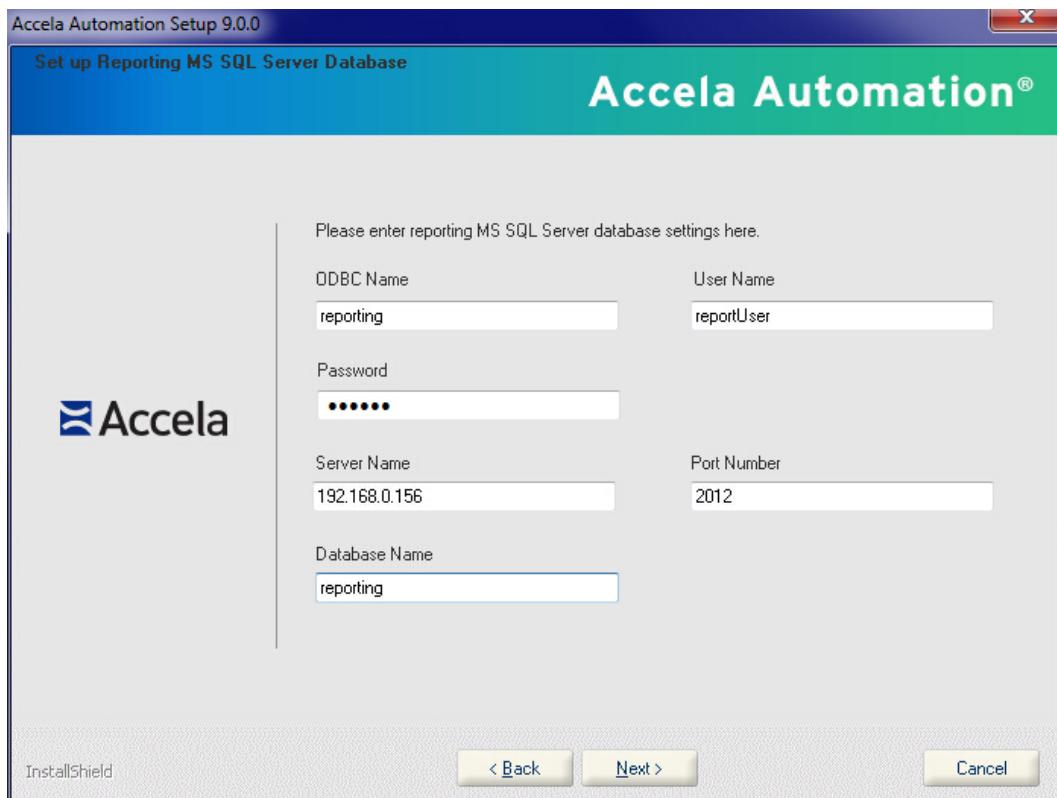


Figure 4: The Set up Reporting MS SQL Server Database screen

6. Enter configuration parameter values for the Oracle database server or the SQL Server database server.
7. Click **Next** to continue.

Configuring a New or Upgraded Database

This section provides instructions to configure the database when you select the Database Install/Upgrade option (see [Managing a Civic Platform Configuration](#)). This procedure supports configuration of Oracle or SQL Server database servers.

After you select the database type (Oracle or MS SQL Server), configure a new or upgraded database.

Configure a new or upgraded Oracle database server:

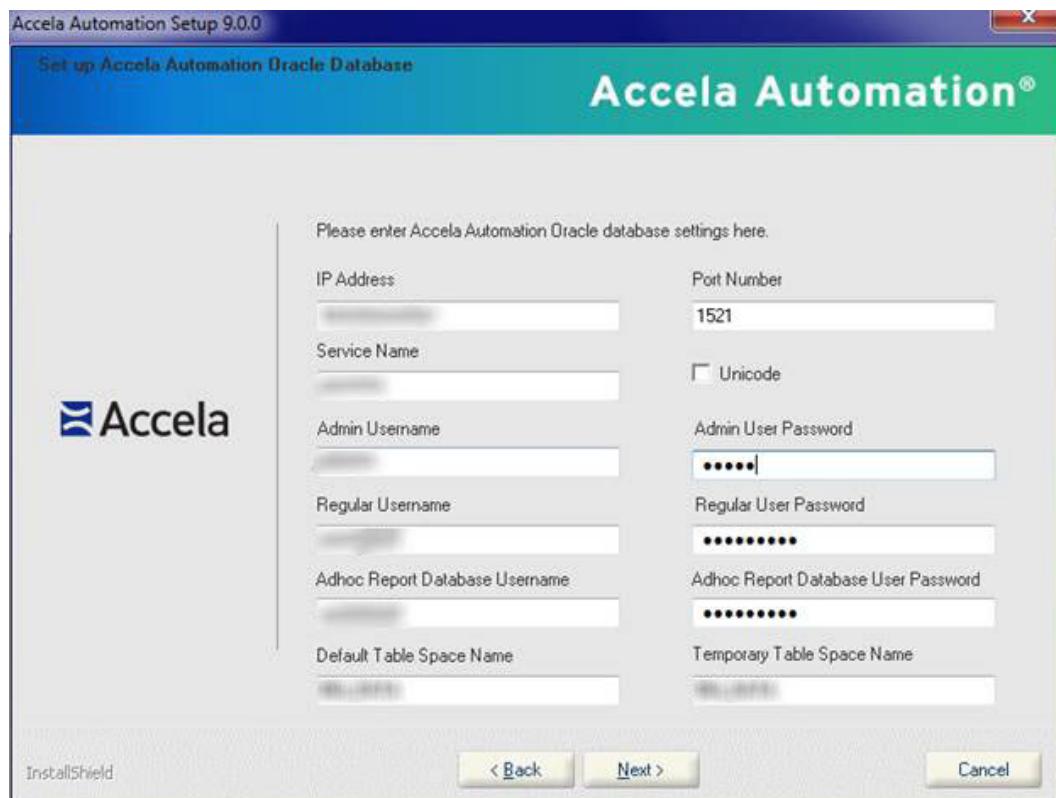


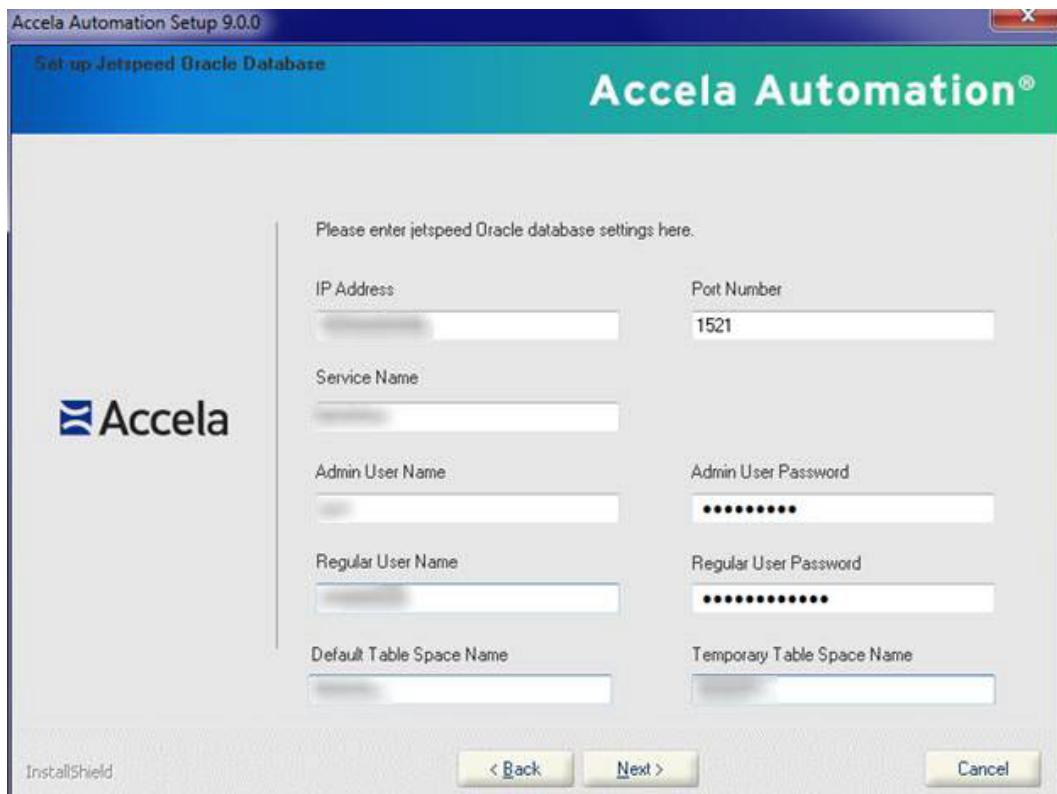
Figure 5: Set up Civic Platform Oracle Database Screen

1. Enter appropriate values for the listed configuration parameters. See [Configuration Checklist](#) for example values.

If the entered database does not exist, the installer creates a new 9.0.0 Oracle database with the entered name. Otherwise, the installer upgrades the existing database to version 9.0.0.

2. Click **Next** to continue.

The Set up Jetspeed Oracle Database screen displays.



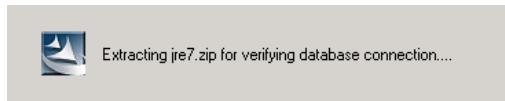
 **Note:** For the **Regular User Password** field, do *not* include special characters such as !, #, -, _, etc. If your agency has a security policy that requires passwords to have special characters, passwords can be changed after the Civic Platform installer has created the database users.

3. Enter appropriate values for the listed configuration parameters. See [Configuration Checklist](#) for example values.

If the entered database does not exist, the installer creates a new 9.0.0 Jetspeed database with the entered name. Otherwise, the installer upgrades the existing database to version 9.0.0.

4. Click **Next** to continue, and verify the database connections and database settings.

The installer displays the following series of message boxes with the verification results of the database settings.



This error message displays if you entered an invalid IP, port number, or service ID.



This error message displays if you entered an invalid SYS user name or password.



This error message displays if you entered an invalid regular, ad hoc, or Jetspeed login user name.



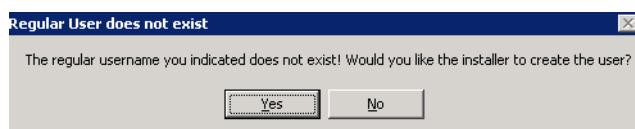
This error message displays if you entered an invalid regular, ad hoc, or Jetspeed login password.



This error message displays if you selected **Database Install/Upgrade** and then entered an invalid regular, ad hoc, or Jetspeed login user name or password.



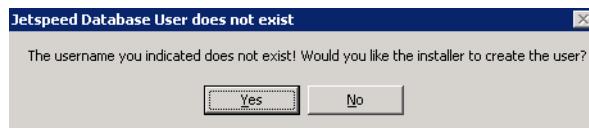
This error message displays if you did not select **Database Install/Upgrade** and entered a new Civic Platform user account.



This error message displays if you did not select **Database Install/Upgrade** and entered a new ad hoc user account.



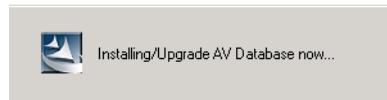
This error message displays if you did not select **Database Install/Upgrade** and entered a new Jetspeed user account.



This error message displays if there are conflicting public synonyms and roles.



This message displays indicating the installer is installing or upgrading the database.



The following command prompt window illustrates the running procedure:

```

It may take several minutes to initialize <upgrade> database ...
Initializing to 7.1.0 database...
Executing: sql\7.1.0\base\oracle\v360\7.1.0_1_create_user.sql
Executing: sql\7.1.0\base\oracle\v360\7.1.0_2_create_table_index_trigger.sql
Executing: sql\7.1.0\base\oracle\v360\7.1.0_3_create_views.sql
Executing: sql\7.1.0\base\oracle\v360\7.1.0_4_create_fun_package.sql
Executing: sql\7.1.0\base\oracle\v360\7.1.0_5_create_public_synonym.sql
Executing: sql\7.1.0\base\oracle\v360\7.1.0_6_grant_table_privs.sql
Executing: sql\7.1.0\base\oracle\v360\7.1.0_7_initial_data.sql
Executing: sql\7.1.0\base\oracle\v360\7.1.0_8_misc.sql
Executing: sql\7.1.0\base\oracle\jetsspeed\turbine-oracle.sql
Executing: sql\7.1.0\base\oracle\jetsspeed\InitJetspeedDB.sql
Upgrading database from 7.1.0 to 7.1.0...
sql\7.1.0\oracle\v360\7.1.0_01_base_tab_oracle.sql script was applied successfully.
sql\7.1.0\oracle\v360\7.1.0_02_base_synonym_oracle.sql script was applied successfully.
sql\7.1.0\oracle\v360\7.1.0_03_base_grant_oracle.sql script was applied successfully.
sql\7.1.0\oracle\v360\7.1.0_04_base_gview_oracle.sql script was applied successfully.
sql\7.1.0\oracle\v360\7.1.0_05_base_quitext_oracle.sql script was applied successfully.
sql\7.1.0\oracle\v360\7.1.0_06_base_rmenuitem_oracle.sql script was applied successfully.
sql\7.1.0\oracle\v360\7.1.0_07_base_misc_oracle.sql script was applied successfully.
sql\7.1.0\oracle\v360\7.1.0_08_base_tab_oracle.sql script has not been applied before.
Now begin executing: sql\7.1.0\oracle\v360\7.1.0_08_base_tab_oracle.sql
sql\7.1.0\oracle\v360\7.1.0_09_base_synonym_oracle.sql script has not been applied before.
Now begin executing: sql\7.1.0\oracle\v360\7.1.0_09_base_synonym_oracle.sql
sql\7.1.0\oracle\v360\7.1.0_10_base_grant_oracle.sql script has not been applied before.
Now begin executing: sql\7.1.0\oracle\v360\7.1.0_10_base_grant_oracle.sql
sql\7.1.0\oracle\v360\7.1.0_11_base_sys_data_oracle.sql script has not been applied before.
Now begin executing: sql\7.1.0\oracle\v360\7.1.0_11_base_sys_data_oracle.sql
sql\7.1.0\oracle\v360\7.1.0_12_base_rmenuitem_oracle.sql script has not been applied before.
Now begin executing: sql\7.1.0\oracle\v360\7.1.0_12_base_rmenuitem_oracle.sql
sql\7.1.0\oracle\v360\7.1.0_13_base_misc_oracle.sql script has not been applied before.
Now begin executing: sql\7.1.0\oracle\v360\7.1.0_13_base_misc_oracle.sql
sql\7.1.0\oracle\v360\7.1.0_14_base_tab_oracle.sql script has not been applied before.
Now begin executing: sql\7.1.0\oracle\v360\7.1.0_14_base_tab_oracle.sql
sql\7.1.0\oracle\v360\7.1.0_15_base_synonym_oracle.sql script has not been applied before.
Now begin executing: sql\7.1.0\oracle\v360\7.1.0_15_base_synonym_oracle.sql
sql\7.1.0\oracle\v360\7.1.0_16_base_grant_oracle.sql script has not been applied before.
Now begin executing: sql\7.1.0\oracle\v360\7.1.0_16_base_grant_oracle.sql
sql\7.1.0\oracle\v360\7.1.0_17_base_sys_data_oracle.sql script has not been applied before.
Now begin executing: sql\7.1.0\oracle\v360\7.1.0_17_base_sys_data_oracle.sql
sql\7.1.0\oracle\v360\7.1.0_18_base_migration_oracle.sql script has not been applied before.
Now begin executing: sql\7.1.0\oracle\v360\7.1.0_18_base_migration_oracle.sql
sql\7.1.0\oracle\v360\7.1.0_19_data_dic_oracle.sql script has not been applied before.

```

5. After the database creation process completes, check the summary information about the executed SQL scripts in the

```
<InstallDir>\installSQLUtility\log\DBUpgradeScriptLog.txt
```

log file.

Configure a new or upgraded MS SQL database:

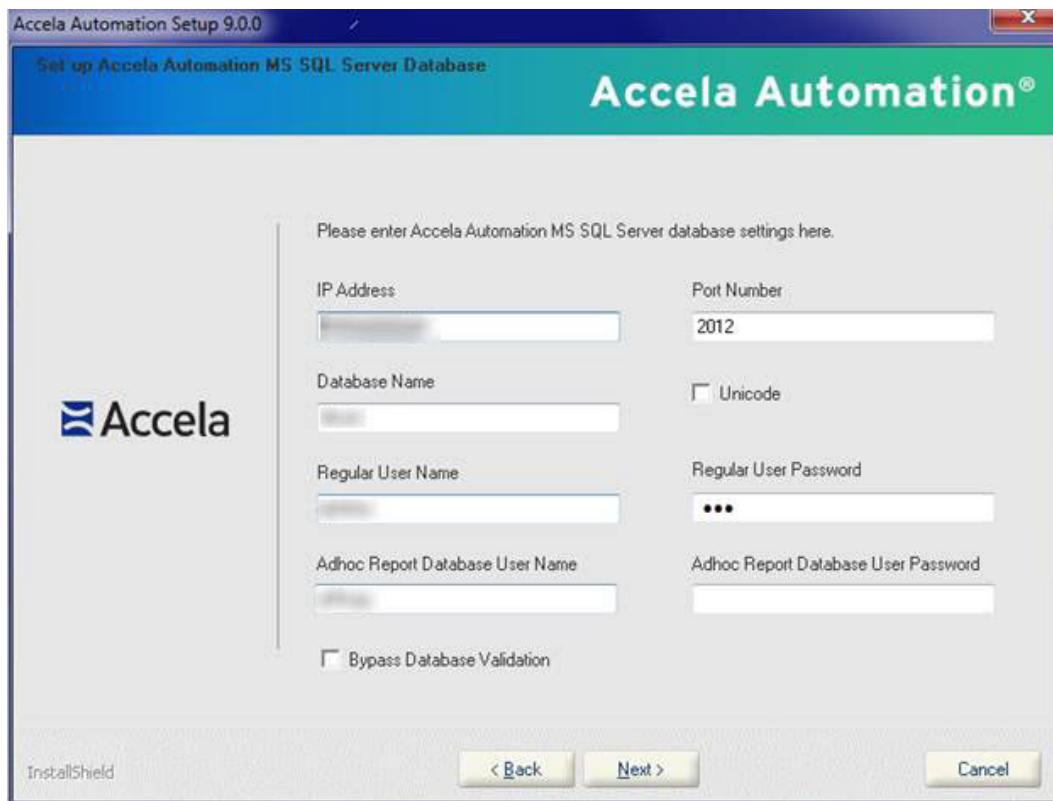


Figure 6: Set up Civic Platform MS SQL Server Database Screen

1. Enter appropriate values for the listed configuration parameters. See [Configuration Checklist](#) for example values.



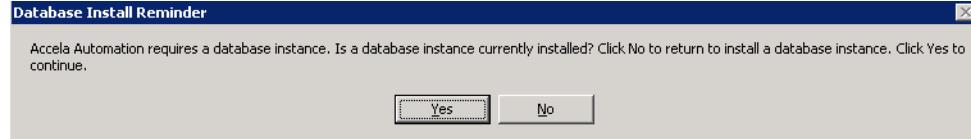
Note:

If you are using MS SQL 2005 you can enter the IP\instance name for the IP address field.

If the entered database does not exist, the installer creates a new 9.0.0 MS SQL Server database with the entered name. Otherwise, the installer upgrades the existing database to version 9.0.0.

2. Click **Next** to continue.

If you selected **Web Server** or **Application Server** components without selecting the **Database Install/Upgrade** component (see [Managing a Civic Platform Configuration](#)), the Database Install Reminder appears in a message box.



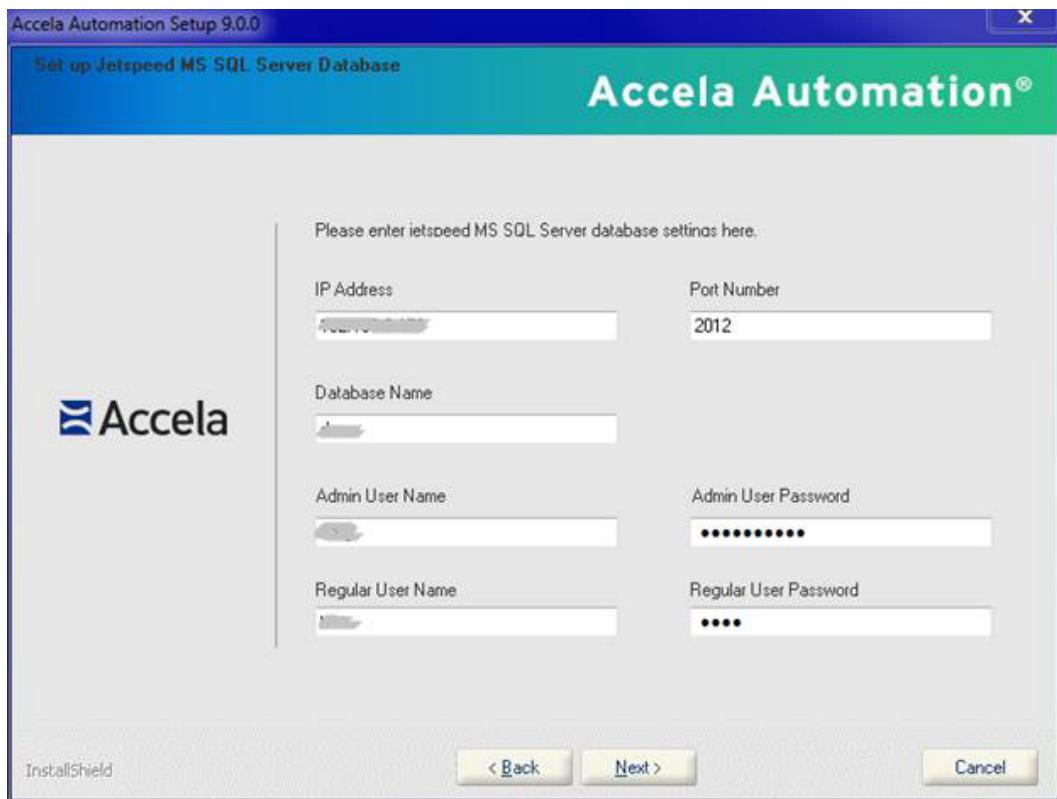
3. Click **Yes** to continue.



Note:

Click **No** to install a Civic Platform database (see [Managing a Civic Platform Configuration](#)).

The Set up Jetspeed MS SQL Server Database screen displays.



- Enter appropriate values for the listed configuration parameters. See [Configuration Checklist](#) for example values.

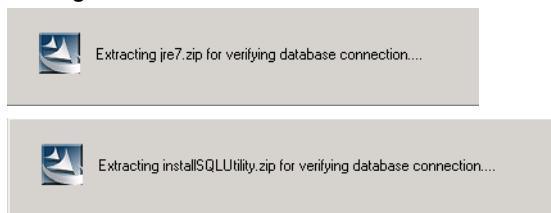


Note:

If using MS SQL 2005 you can enter IP\instance name for the IP address field.

If the entered database does not exist, the installer creates a new 9.0.0 Jetspeed database with the entered name. Otherwise, the installer upgrades the existing database to version 9.0.0.

- Click **Next** to continue.
- The installer displays the following series of message boxes with the verification results of the database settings.



This error message displays if you entered an invalid IP, port number, or database name.



This error message displays if you entered an invalid admin user name or password.



This error message displays if you entered an invalid regular, ad hoc, or Jetspeed login user name.



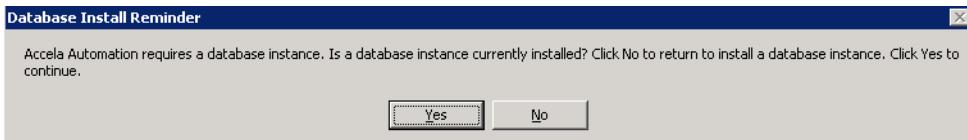
This error message displays if you entered an invalid regular, ad hoc, or Jetspeed login password.



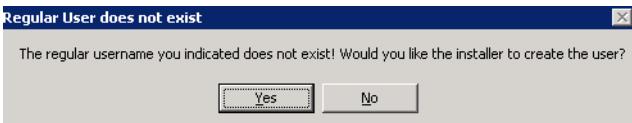
This error message displays if you entered an invalid regular, ad hoc, or Jetspeed login password for the second time.



This message requests that you enter a new Civic Platform database.



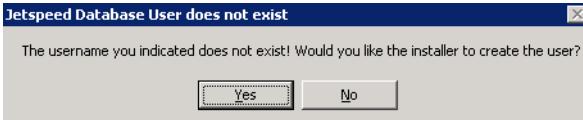
This message requests that you enter a new Civic Platform regular user account.



This message requests that you enter a new ad hoc user account.



This message requests that you enter a new Jetspeed user account.



This message requests that you enter an existing Jetspeed user account for Civic Platform database.



This message requests that you enter an existing Jetspeed user account for Jetspeed database.



This message displays if you entered an invalid database.



This error message displays if you did not select **Database Install/Upgrade**.



The following command prompt window illustrates the running procedure:

```
Executing: sql\7.1.0\base\mssql\v360\7.1.0_5_initial_data.sql
Executing: sql\7.1.0\base\mssql\v360\7.1.0_6_misc.sql
Executing: sql\7.1.0\base\mssql\jetspeed\turbine-mssql.sql
Upgrading database from 7.1.0 ...
sql\7.1.0\mssql\mssql\360\7.1.0_01_base_tab_mssql.sql script was applied successfully
sql\7.1.0\mssql\mssql\360\7.1.0_02_base_synonym_mssql.sql script was applied successfully
sql\7.1.0\mssql\mssql\360\7.1.0_03_base_grant_mssql.sql script was applied successfully
sql\7.1.0\mssql\mssql\360\7.1.0_04_base_gview_mssql.sql script was applied successfully
sql\7.1.0\mssql\mssql\360\7.1.0_05_base_guitem_text_mssql.sql script was applied successfully
sql\7.1.0\mssql\mssql\360\7.1.0_06_base_rmenuitem_mssql.sql script was applied successfully
sql\7.1.0\mssql\mssql\360\7.1.0_07_base_misc_mssql.sql script was applied successfully
sql\7.1.0\mssql\mssql\360\7.1.0_08_base_tab_mssql.sql script has not been applied before
Now begin executing: sql\7.1.0\mssql\mssql\360\7.1.0_08_base_tab_mssql.sql
sql\7.1.0\mssql\mssql\360\7.1.0_09_base_synonym_mssql.sql script has not been applied before
Now begin executing: sql\7.1.0\mssql\mssql\360\7.1.0_09_base_synonym_mssql.sql
sql\7.1.0\mssql\mssql\360\7.1.0_10_base_grant_mssql.sql script has not been applied before
Now begin executing: sql\7.1.0\mssql\mssql\360\7.1.0_10_base_grant_mssql.sql
sql\7.1.0\mssql\mssql\360\7.1.0_11_base_sys_data_mssql.sql script has not been applied before
Now begin executing: sql\7.1.0\mssql\mssql\360\7.1.0_11_base_sys_data_mssql.sql
sql\7.1.0\mssql\mssql\360\7.1.0_12_base_rmenuitem_mssql.sql script has not been applied before
Now begin executing: sql\7.1.0\mssql\mssql\360\7.1.0_12_base_rmenuitem_mssql.sql
sql\7.1.0\mssql\mssql\360\7.1.0_13_base_misc_mssql.sql script has not been applied before
Now begin executing: sql\7.1.0\mssql\mssql\360\7.1.0_13_base_misc_mssql.sql
sql\7.1.0\mssql\mssql\360\7.1.0_14_base_tab_mssql.sql script has not been applied before
Now begin executing: sql\7.1.0\mssql\mssql\360\7.1.0_14_base_tab_mssql.sql
sql\7.1.0\mssql\mssql\360\7.1.0_15_base_synonym_mssql.sql script has not been applied before
Now begin executing: sql\7.1.0\mssql\mssql\360\7.1.0_15_base_synonym_mssql.sql
sql\7.1.0\mssql\mssql\360\7.1.0_16_base_grant_mssql.sql script has not been applied before
Now begin executing: sql\7.1.0\mssql\mssql\360\7.1.0_16_base_grant_mssql.sql
sql\7.1.0\mssql\mssql\360\7.1.0_17_base_sys_data_mssql.sql script has not been applied before
Now begin executing: sql\7.1.0\mssql\mssql\360\7.1.0_17_base_sys_data_mssql.sql
sql\7.1.0\mssql\mssql\360\7.1.0_18_base_migration_mssql.sql script has not been applied before
Now begin executing: sql\7.1.0\mssql\mssql\360\7.1.0_18_base_migration_mssql.sql
sql\7.1.0\mssql\mssql\360\7.1.0_19_data_dic_mssql.sql script has not been applied before
Now begin executing: sql\7.1.0\mssql\mssql\360\7.1.0_19_data_dic_mssql.sql
Finish initializing (upgrading) database. Press ENTER key to continue ...
```

- After the database creation process completes, check the summary information about the executed SQL scripts in the **<InstallDir>\installSQLUtility\log\DBUpgradeScriptLog.txt** log file.

For each database upgrade script, a similar screen like the one below displays.

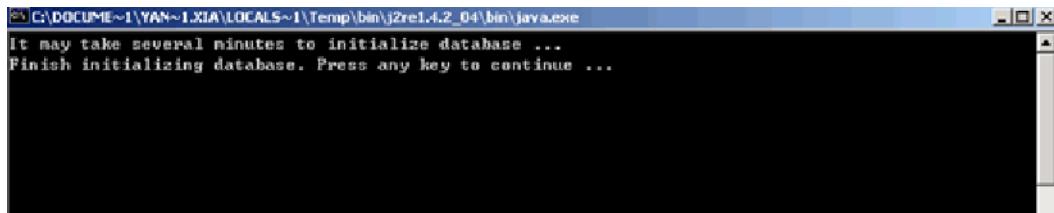


```

Now begin executing: sql\7.0.5-i18n\mssql1\sql\360\7.0.5_23_prod3_tab_mssql.sql
sql\7.0.5-i18n\mssql1\sql\360\7.0.5_24_prod3_sys_data_mssql.sql script has not been applied before.
Now begin executing: sql\7.0.5-i18n\mssql1\sql\360\7.0.5_24_prod3_sys_data_mssql.sql
Upgrading database from 7.0.5 to 7.1.0 ...
sql\7.1.0-i18n\mssql1\sql\360\7.1.0_01_base_tab_mssql.sql script has not been applied before.
Now begin executing: sql\7.1.0-i18n\mssql1\sql\360\7.1.0_01_base_tab_mssql.sql
sql\7.1.0-i18n\mssql1\sql\360\7.1.0_02_base_synonym_mssql.sql script has not been applied before.
Now begin executing: sql\7.1.0-i18n\mssql1\sql\360\7.1.0_02_base_synonym_mssql.sql
sql\7.1.0-i18n\mssql1\sql\360\7.1.0_03_base_grant_mssql.sql script has not been applied before.
Now begin executing: sql\7.1.0-i18n\mssql1\sql\360\7.1.0_03_base_grant_mssql.sql
sql\7.1.0-i18n\mssql1\sql\360\7.1.0_04_base_gview_mssql.sql script has not been applied before.
Now begin executing: sql\7.1.0-i18n\mssql1\sql\360\7.1.0_04_base_gview_mssql.sql
sql\7.1.0-i18n\mssql1\sql\360\7.1.0_05_base_quitext_mssql.sql script has not been applied before.
Now begin executing: sql\7.1.0-i18n\mssql1\sql\360\7.1.0_05_base_quitext_mssql.sql
sql\7.1.0-i18n\mssql1\sql\360\7.1.0_06_base_rmenuitem_mssql.sql script has not been applied before.
Now begin executing: sql\7.1.0-i18n\mssql1\sql\360\7.1.0_06_base_rmenuitem_mssql.sql
sql\7.1.0-i18n\mssql1\sql\360\7.1.0_07_base_misc_mssql.sql script has not been applied before.
Now begin executing: sql\7.1.0-i18n\mssql1\sql\360\7.1.0_07_base_misc_mssql.sql
sql\7.1.0-i18n\mssql1\sql\360\7.1.0_08_base_tab_mssql.sql script has not been applied before.
Now begin executing: sql\7.1.0-i18n\mssql1\sql\360\7.1.0_09_base_synonym_mssql.sql
sql\7.1.0-i18n\mssql1\sql\360\7.1.0_09_base_synonym_mssql.sql script has not been applied before.
Now begin executing: sql\7.1.0-i18n\mssql1\sql\360\7.1.0_10_base_grant_mssql.sql
sql\7.1.0-i18n\mssql1\sql\360\7.1.0_10_base_grant_mssql.sql script has not been applied before.
Now begin executing: sql\7.1.0-i18n\mssql1\sql\360\7.1.0_11_base_sys_data_mssql.sql
sql\7.1.0-i18n\mssql1\sql\360\7.1.0_11_base_sys_data_mssql.sql script has not been applied before.
Now begin executing: sql\7.1.0-i18n\mssql1\sql\360\7.1.0_12_base_rmenuitem_mssql.sql
sql\7.1.0-i18n\mssql1\sql\360\7.1.0_12_base_rmenuitem_mssql.sql script has not been applied before.
Now begin executing: sql\7.1.0-i18n\mssql1\sql\360\7.1.0_13_base_misc_mssql.sql
sql\7.1.0-i18n\mssql1\sql\360\7.1.0_13_base_misc_mssql.sql script has not been applied before.
Now begin executing: sql\7.1.0-i18n\mssql1\sql\360\7.1.0_14_base_tab_mssql.sql
sql\7.1.0-i18n\mssql1\sql\360\7.1.0_14_base_tab_mssql.sql script has not been applied before.
Now begin executing: sql\7.1.0-i18n\mssql1\sql\360\7.1.0_15_base_synonym_mssql.sql
sql\7.1.0-i18n\mssql1\sql\360\7.1.0_15_base_synonym_mssql.sql script has not been applied before.
Now begin executing: sql\7.1.0-i18n\mssql1\sql\360\7.1.0_16_base_grant_mssql.sql
sql\7.1.0-i18n\mssql1\sql\360\7.1.0_16_base_grant_mssql.sql script has not been applied before.
Now begin executing: sql\7.1.0-i18n\mssql1\sql\360\7.1.0_17_base_sys_data_mssql.sql
sql\7.1.0-i18n\mssql1\sql\360\7.1.0_17_base_sys_data_mssql.sql script has not been applied before.
Now begin executing: sql\7.1.0-i18n\mssql1\sql\360\7.1.0_18_base_migration_mssql.sql
sql\7.1.0-i18n\mssql1\sql\360\7.1.0_18_base_migration_mssql.sql script has not been applied before.
Now begin executing: sql\7.1.0-i18n\mssql1\sql\360\7.1.0_19_data_dic_mssql.sql
sql\7.1.0-i18n\mssql1\sql\360\7.1.0_19_data_dic_mssql.sql script has not been applied before.
Finish initializing <upgrading> database. Press ENTER key to continue ...

```

If you run the installer repeatedly, the following DOS window displays.



```

C:\DOCUMENTS~1\YAN~1\XIA\LOCALS~1\Temp\bin\j2re1.4.2_04\bin\java.exe
It may take several minutes to initialize database ...
Finish initializing database. Press any key to continue ...

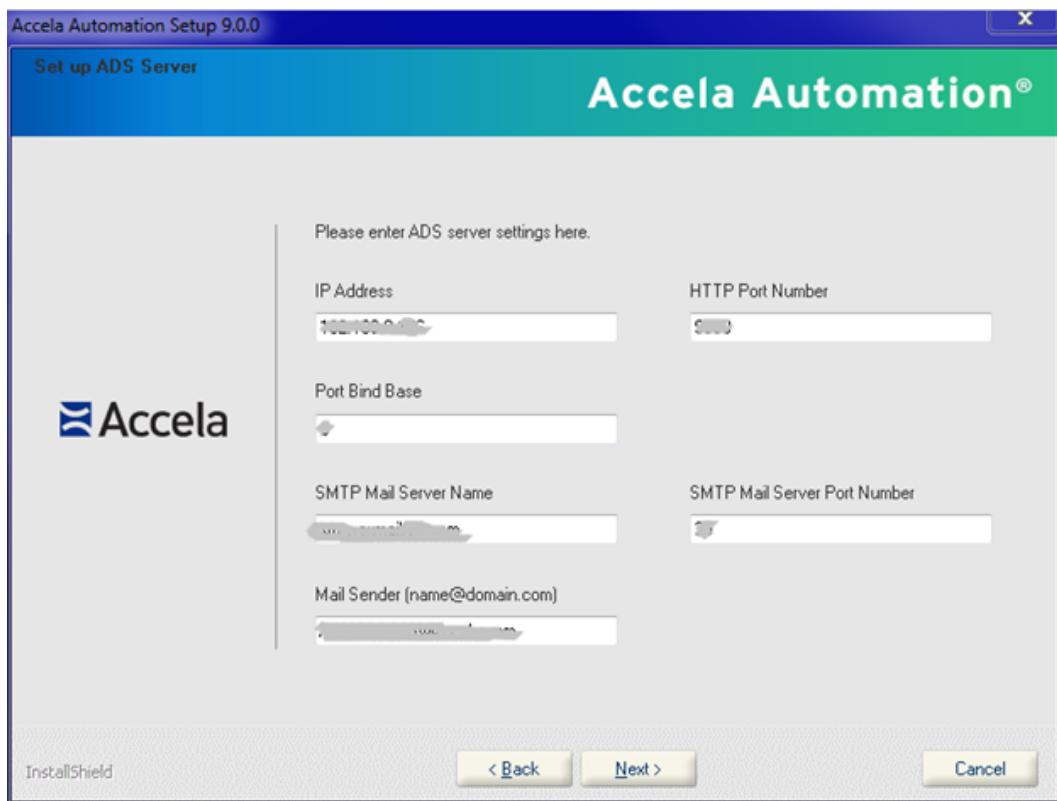
```

Configuring the Accela Document Service (ADS)

To configure the ADS server:

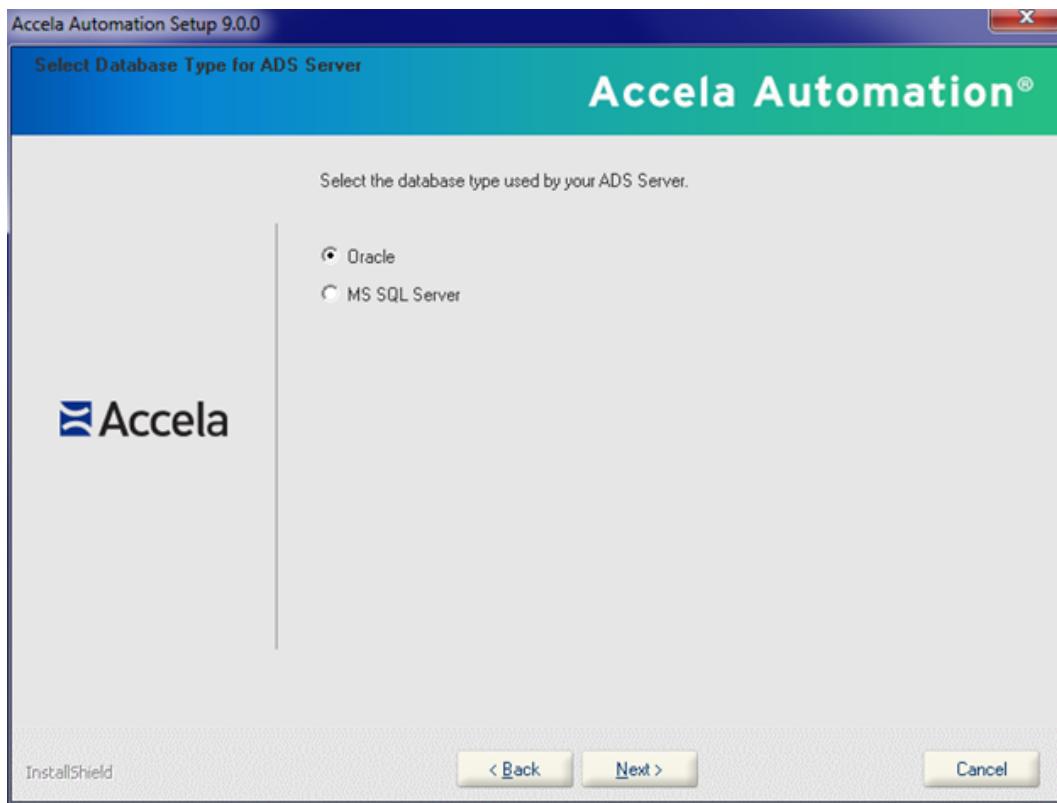
- Access the ADS server configuration by selecting the **Accela Document Service (ADS)** check box in the Select Civic Platform Components screen (see [Managing a Civic Platform Configuration](#)).

The ADS Server Setup screen displays.



2. Enter appropriate values for the listed configuration parameters. See [Configuration Checklist](#) for example values. At a minimum, enter the ADS sever IP Address, HTTP port, and JBoss bind port base number for the ADS server host.
3. Click **Next** to continue.

The Select Database Type for ADS Server screen displays.

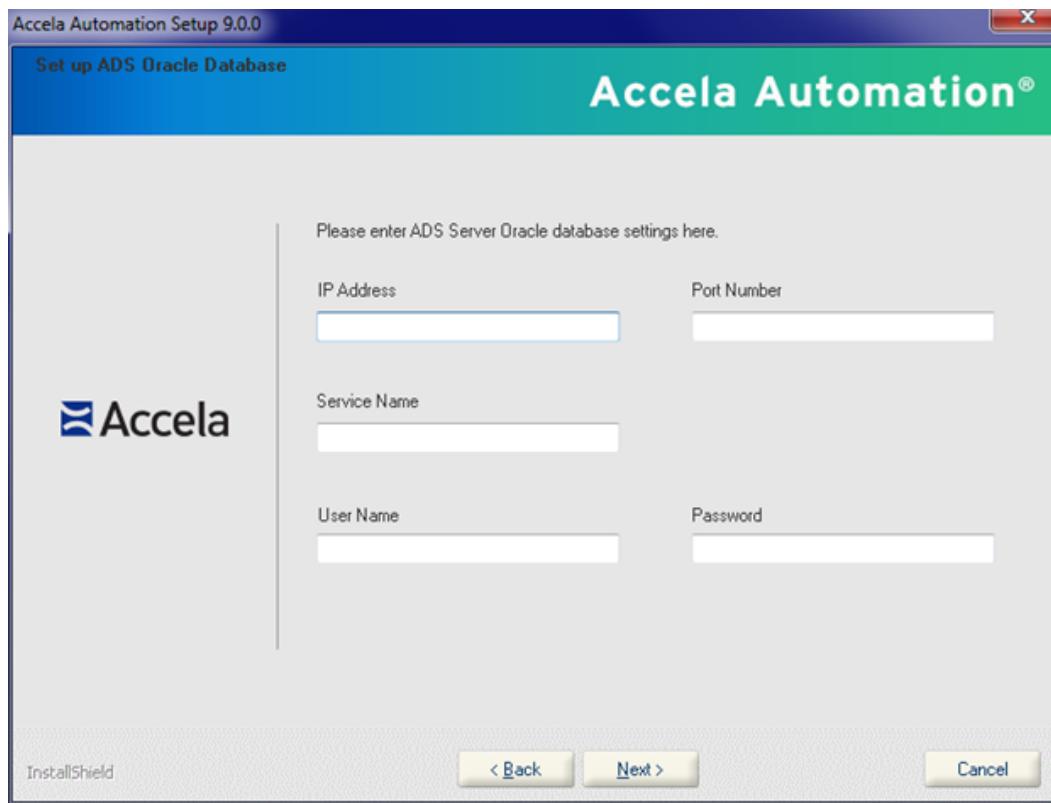


4. Select Oracle or MS SQL Server.

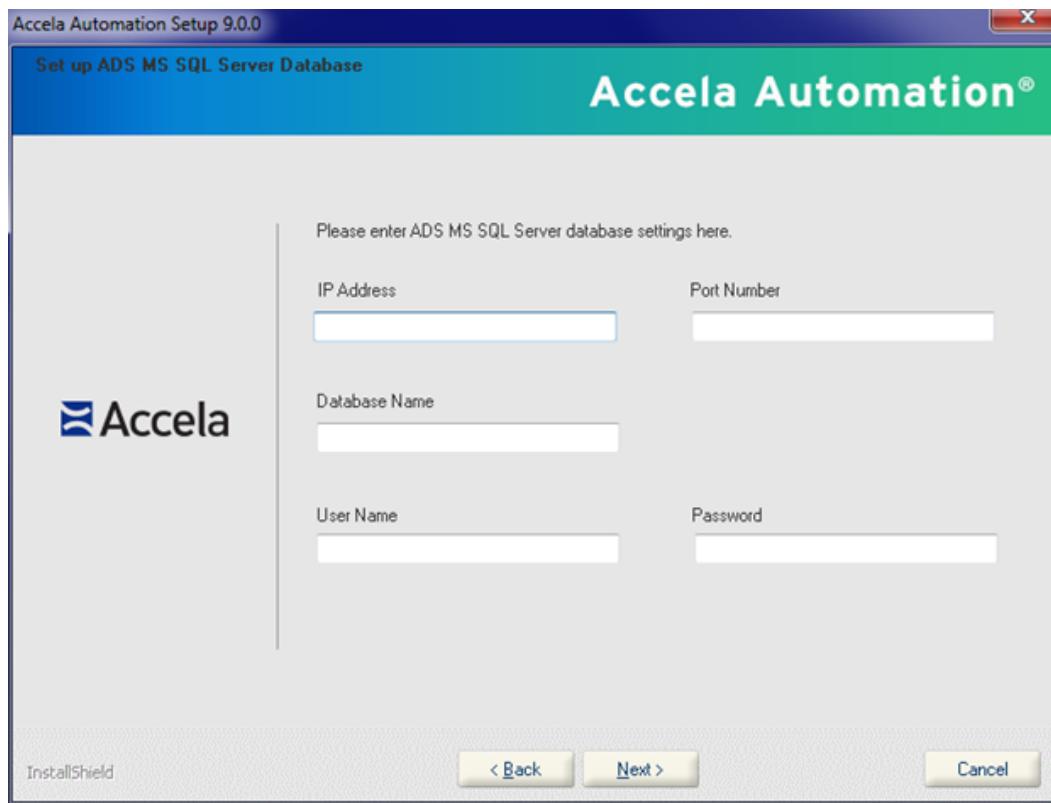
- Select Oracle.

1. Click **Next** to continue.

The Set up ADS Server Oracle Database screen displays.



2. Enter appropriate values for the listed configuration parameters. See [Configuration Checklist](#) for example values.
- Select MS SQL.
 1. Click **Next** to continue.The Set up ADS MS SQL Server Database screen displays.



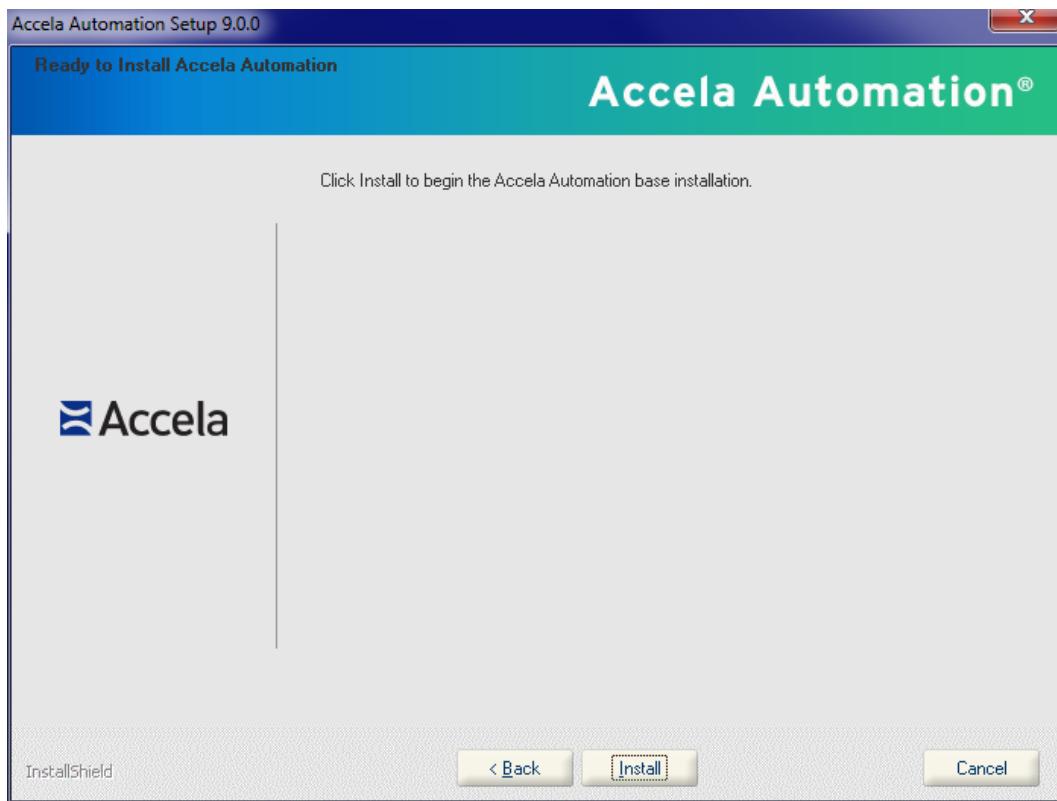
2. Enter appropriate values for the listed configuration parameters. See [Configuration Checklist](#) for example values.
5. The ADS configuration is complete. Click **Next** to continue (see [Installing Civic Platform Components](#)).

Installing Civic Platform Components

To install Civic Platform components:

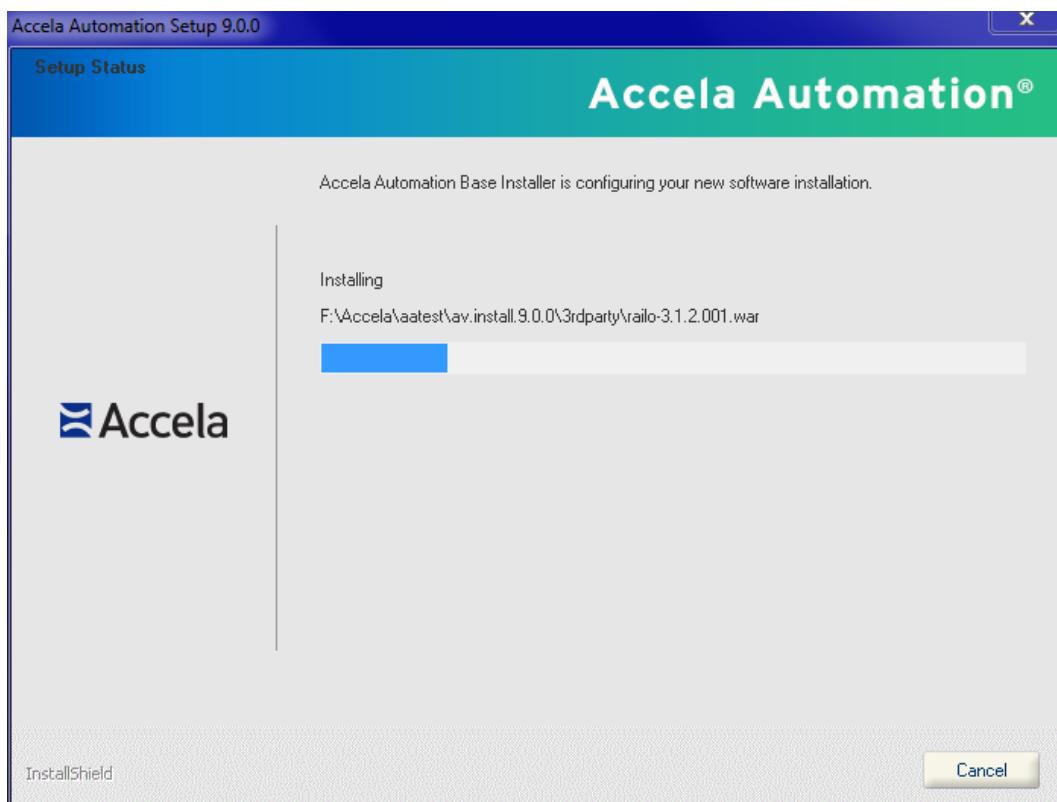
1. Configure the Civic Platform components that you want to install (see [Managing a Civic Platform Configuration](#)).

The Ready to Install Civic Platform screen displays.



2. Click **Install** to start the installation process.

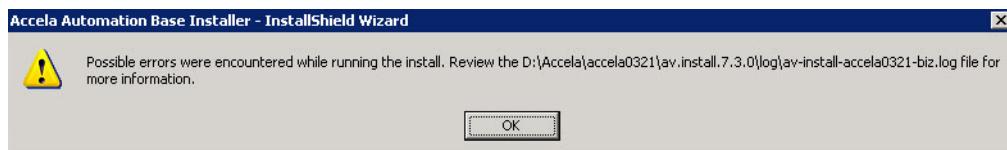
The Setup Status screen displays.



This Setup Status screen shows the progress of Accela Products installation. After the progress bar completes, setup performs actions based on the software components selected to install. The installer either detects an error or completes successfully.

- The installer detects an error.

The Possible errors running install screen displays.



1. Review the log file that the screen indicates.
2. Resolve the problem.
3. Click **Next** to continue.
4. Re-run the installation for the server that failed.



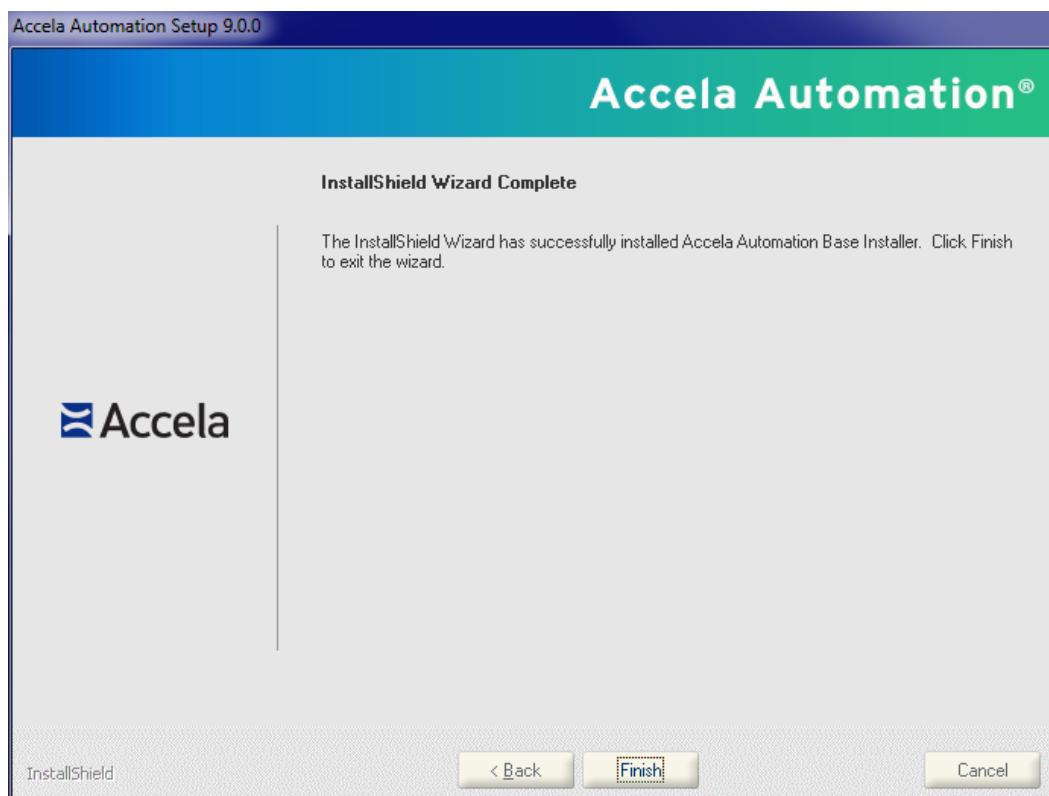
Note:

When re-running the installation, you must select all server components you want to install.

or,

- The installation successfully completes.

The InstallShield Wizard Complete screen displays.



3. Click **Finish** to complete the installation.

4. If required, manually upgrade the Civic Platform database (see [Manually Upgrading the Civic Platform Database](#)).
5. Run the Civic Platform 9.0.2 Application installer (see [Installing the Latest Application Code](#)).

Manually Upgrading the Civic Platform Database

This section provides instructions to manually upgrade the Civic Platform database if you did not choose to have the Civic Platform installer automatically upgrade the database (see [Managing a Civic Platform Configuration](#) or [Configuring the Application Server Database](#)).

Topics

- [Manually Upgrading Database](#)
- [Reviewing Supporting Files](#)

Manually Upgrading the Database

Follow the instruction provided here to manually upgrade an existing 7.1.0 Civic Platform database (or later) to the latest version. If required, upgrade Civic Platform databases earlier than 7.1.0 to 7.1.0 before following this procedure. Refer to the 7.1.0 Accela Automation DBUpdate.pdf document for information on updating Civic Platform databases earlier than 7.1.0 to 7.1.0.

The database update installer extracts SQL script files to the host, sets up batch files to run the SQL scripts, and invokes the scripts to update the database schema or the table data on the specified database. At the end of the upgrade, you can automatically run the database checking scripts and upgrading scripts, or exit the installation and run the scripts manually.

You must install scripts from all previous releases. Refer to the Civic Platform DB Update.pdf, that is applicable to previous releases, to identify other required scripts for your installation.

To manually update the database:

1. If required, install Civic Platform 9.0.0 (see [Installing a Base Civic Platform](#)).
2. Download the installer to the host from which you want to run the installation. The installer file name is *AA_DbUpdate_<release version>_<build_number>.exe*. For example, AA_Db_Update_9.0.1_161221.exe.
3. Run the installer.
4. Click **Next** on the Welcome screen.
5. Read and accept the license agreement by clicking **Next**.
6. Select the directory to copy the database update files to. (The default is C:\Accela\730DbUpdate.)
7. Select the database type you are using (Oracle or MS SQL Server).
8. Click **Yes** or **No** in the pop-up window, “If you are upgrading a multilingual database?”
9. Follow the appropriate steps for your setup:
 - If you select Oracle, enter the following information:

1. User is the Oracle user with privileges to do database updates.
 2. Password is the password for the previous user.
 3. TNSname is the TNS name for the database that you want to upgrade.
 4. Click **Next** after you enter all the information.
- If you select MS SQL Server, enter the following information:
 1. DB Server is the server that the database is running on. Enter the DB Server information in any of the following formats:

IP,Port
ServerName,Port
IP\DBInstanceName
ServerName\DBInstanceName
ServerIP\DBInstanceName, Port
ServerName\DBInstanceName, Port
 2. Click **Next** after you enter the information.
 3. User is the MS SQL user with privileges to do database updates.
 4. Password is the password for the previous user.
 5. DB name is the name for the database that you want to upgrade.
 6. Click **Next** after you enter all the information.

10. Click **Install** to copy the files to your host or **Back** to review your previous settings.

11. Run the scripts automatically or manually.

- Run the scripts automatically by selecting the check boxes to run the database health check scripts after the database upgrade script is successful.
or,
- Run the scripts manually by de-selecting the check boxes to run the database upgrade scripts.

The 9.0.0 scripts are located in the following directories.

Oracle:

```
<installdir>\installSQLUtility\sql\9.0.0\oracle\v360
```

MS Sql:

```
<installdir>\installSQLUtility\sql\9.0.0\mssql\v360
```

Each script contains a release number and sequence number in its name. For example, 9.0.0_3_xxx.sql. The sequence number, 3 in this example, determines the order in which to run the scripts. After the script successfully runs, do not run it again. If a script aborts, until you resolve the problem with the aborted script and run the script successfully, the next script does not run. You can execute this set of scripts by running a BAT file in the version folder, for example, <installdir>\installSQLUtility\sql\9.0.0\run_aa900_oracle.bat.

**Note:**

The scripts create log file in the following directories.

Oracle:

```
<installdir>\installSQLUtility
```

\log

MS Sql:

```
<installdir>\installSQLUtility\log
```

The results of executing these scripts are in the UPGRADE_SCRIPTS database table.

- 12.** After completing the upgrade, install the latest Civic Platform application code (see [Installing the Latest Application Code](#)).

**Note:**

You can run the database installer in remove mode. However, this only removes the SQL script files extracted to your local host. Remove mode does not roll back changes made to the database.

Reviewing Supporting Files

In each version folder, there are two readme text files which describe how to run the scripts manually. For example, the following two files are the readme files in the 9.0.0 version folder:

```
<installdir>\installSQLUtility\sql\9.0.0\readme_900_oracle.txt
<installdir>\installSQLUtility\sql\9.0.0\readme_900_mssql.txt
```

For each version of the database, you can run BAT files to run all SQL script files manually. Before running a BAT file, you need to verify that the correct user/password and database information is in the batch file for your database type. You can execute a set of scripts for the database by running one of the following BAT files in the corresponding version folder.

```
<installdir>\installSQLUtility\sql\9.0.0\run_aa900_oracle.bat
<installdir>\installSQLUtility\sql\9.0.0\run_aa900_mssql.bat
<installdir>\installSQLUtility\sql\9.0.0-i18n\run_aa900_i18n_oracle.bat
<installdir>\installSQLUtility\sql\9.0.0-i18n\run_aa900_i18n_mssql.bat
```

Installing the Latest Application Code

Follow the instructions in this section to install the latest Civic Platform application code to the application server.

The installer unzips code packages to the target directory on the application server, c:\accela\av.deploy for example, and invokes ANT scripts to deploy the application code files (*.ear, *.war, *.jar, etc.) to the JBoss server folders (c:\accela\av.biz\deploy, c:\accela\av.web\deploy, etc.).

To run the latest application code installer:

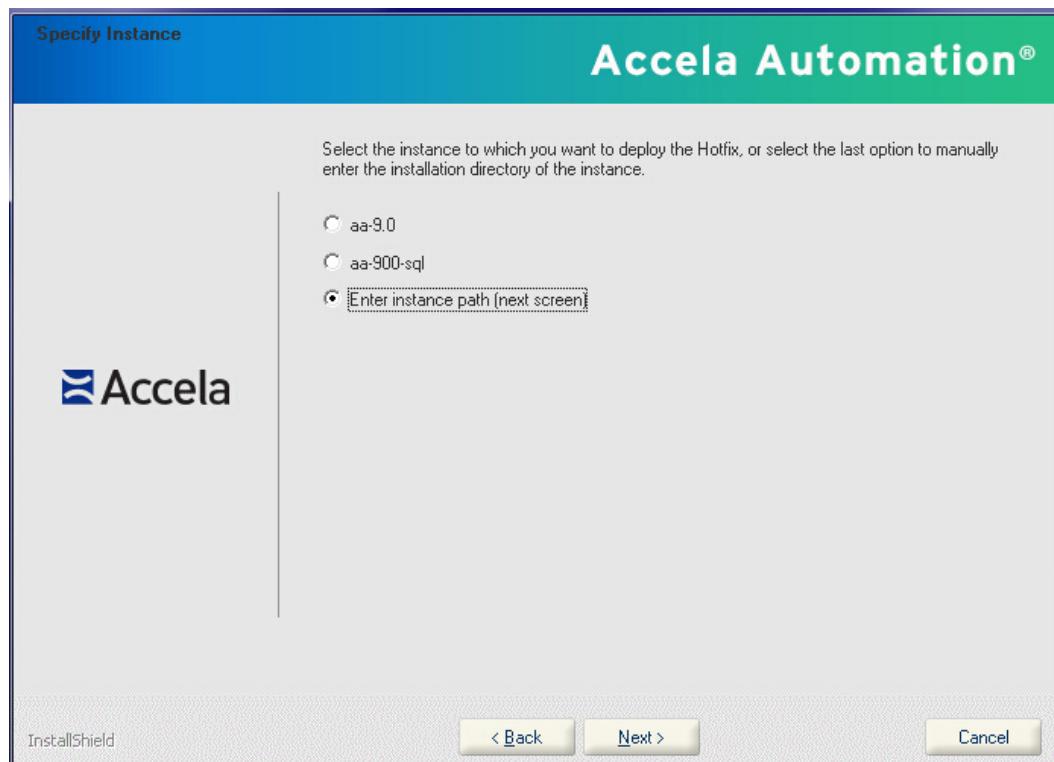
1. Download the installer file to the host from where you want to run the installation.

The set of installation files you downloaded from the FTP site includes the AA_Application_<release version>_<build number>.exe file. For example, AA_Application_9.0.2_170117.exe.

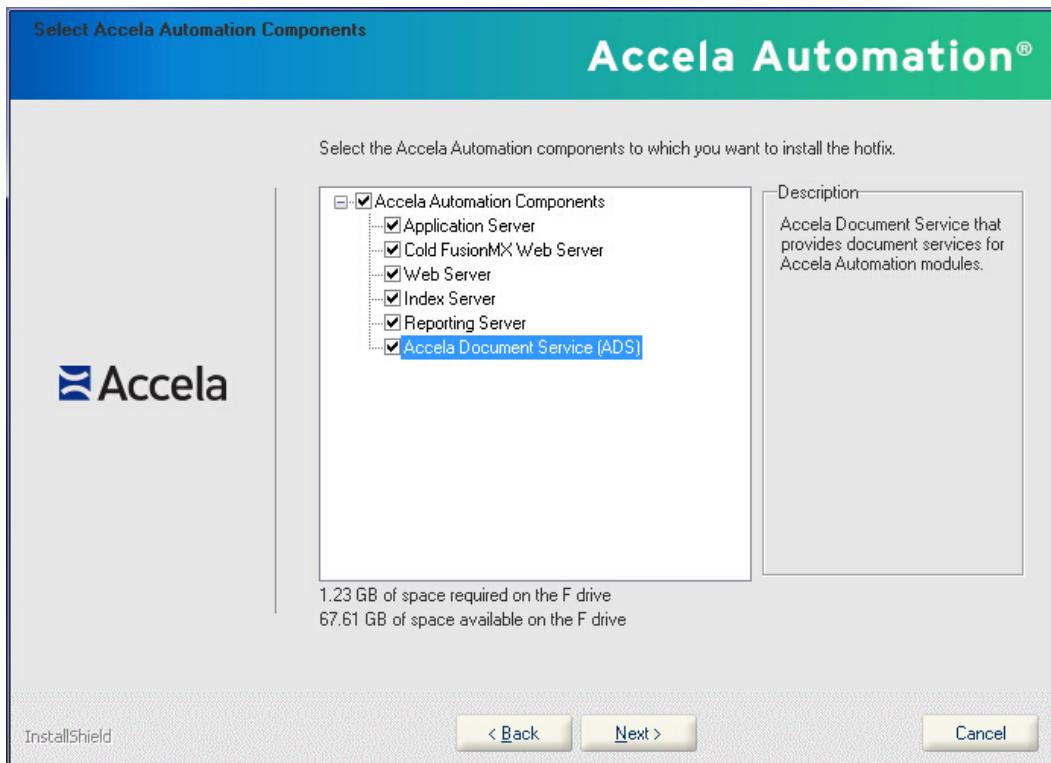
2. Double-click AA_Application_9.0.2_170117.exe to start the installation.

If you have ever run this installer file on the current machine, the installer displays a maintenance screen listing all detected application instances. You can choose whether to install a new instance or maintain an existing instance.

3. If this is the first time you are running the installer on the current machine, the Welcome screen displays.
4. Click **Next**.
5. In the **Specify Instance** screen, select the Civic Platform 9.0.0 base instance, and then click **Next**.

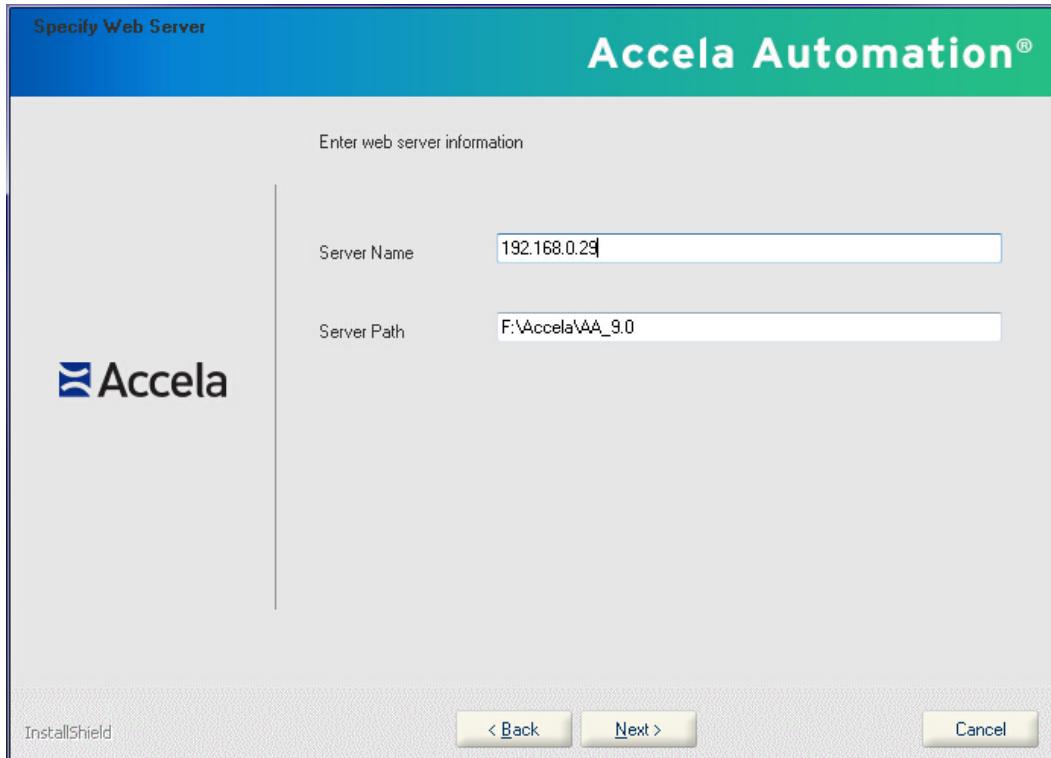


The installer displays the Select Components screen.



6. Select the servers where you want to deploy the new software and then click **Next**.

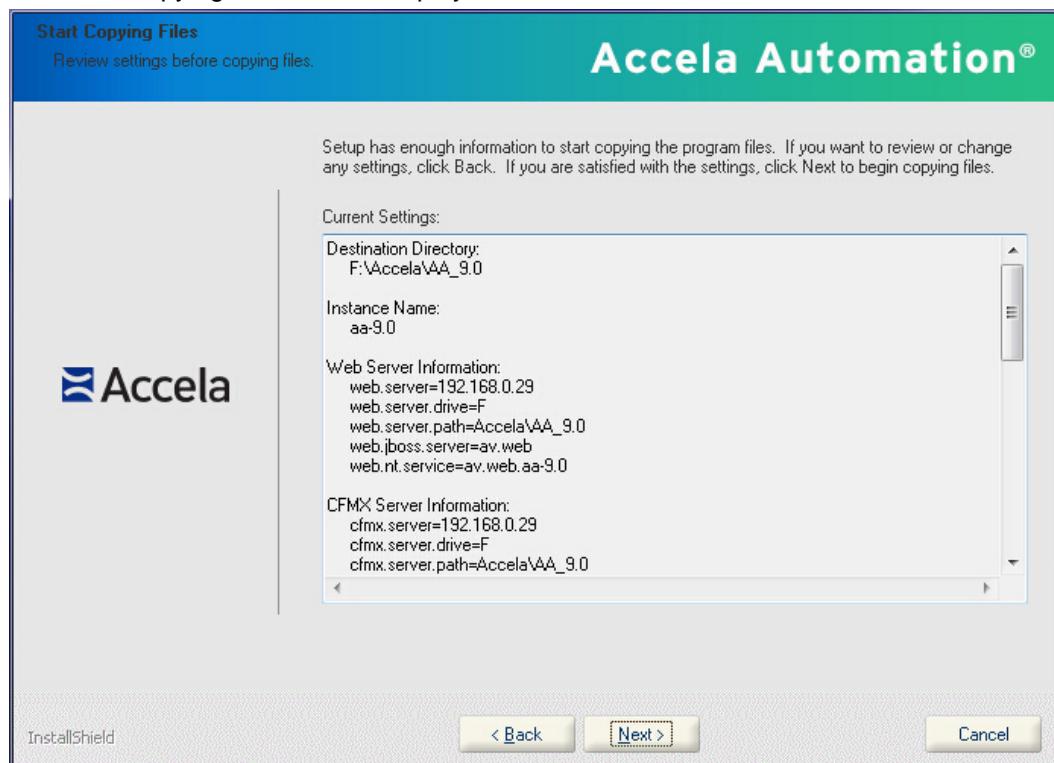
The installer displays the Specify Web Server information screen. This is the first of several Specify <Server Type> screens in the application installation process.



7. Complete these fields for each server component that you specified above, and click **Next** until you see the Start Copying Files screen.

Server Name	Enter the IP Address of the physical server that is running the application.
Path Installed	Enter the path where you installed the application. The folder contains the av.xxx sub folders.

The Start Copying Files screen displays.



8. In the Start Copying Files screen, verify your setup and click **Next**.

The installer installs the application code files on the specified servers and then deploys the application on them.

9. When the deployment is complete, the installer checks the log file for errors.

10. If the log file records any failure, it automatically opens for you to review. Correct any problems in the log file. This log file is located in the <installdir>\av.deploy\log folder. After you resolve the problems, follow to steps 2-8 above to run the installer again.

11. Click the **Finish** button to complete the installation.

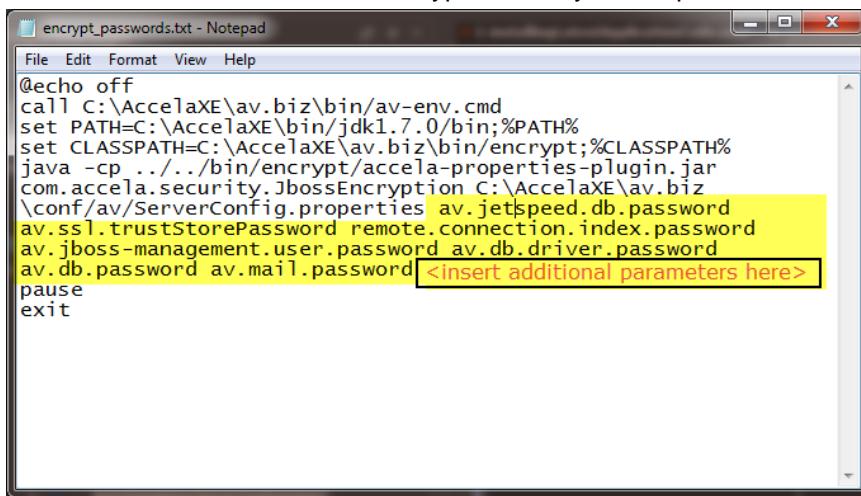
Windows services automatically start upon completion of the installation.

12. If you want to encrypt passwords in configuration files manually, follow these steps:

- a. Locate this BAT file, encrypt_passwords.bat in the bin folder of every server that you deployed in this installation. For example,

```
installdir\av.biz\bin\encrypt_passwords.bat
installdir\av.web\bin\encrypt_passwords.bat
installdir\av.cfmx\bin
\encrypt_passwords.bat
installdir\av.ads\bin\encrypt_passwords.bat
installdir\av.awr\bin\encrypt_passwords.bat
installdir\av.indexer\bin
\encrypt_passwords.bat
```

- b. Double-click the corresponding BAT file to encrypt passwords for the server you want. For example, if you want to encrypt passwords for the av.biz server, locate the **encrypt_passwords.bat** file in the **<installdir>\av.biz\bin** folder and run the BAT file.
13. To validate that the BAT file ran successfully, open the **ServerConfig.properties** file in the **<installdir>\av.biz\conf\av** folder to verify that each property value related to a password is an encrypted text string, and the prefix “encrypted” appears at the beginning of the property name.
14. If there are additional passwords that need to be encrypted in the ServerConfig.properties file you will need to modify the BAT file to include parameters for them, as follows:
- Add the parameters after “\conf\av\ServerConfig.properties “ and before “pause”, as shown in the sample screenshot below.
 - Separate each parameter by a space.
 - Save and re-run the BAT file to encrypt the newly added passwords.



```
@echo off
call C:\AccelaXE\av.biz\bin\av-env.cmd
set PATH=C:\AccelaXE\bin\jdk1.7.0/bin;%PATH%
set CLASSPATH=C:\AccelaXE\av.biz\bin\encrypt;%CLASSPATH%
java -cp ../../bin/encrypt/accela-properties-plugin.jar
com.accela.security.JbossEncryption C:\AccelaXE\av.biz
\conf\av\ServerConfig.properties av.jetSpeed.db.password
av.ssl.trustStorePassword remote.connection.index.password
av.jboss-management.user.password av.db.driver.password
av.db.password av.mail.password <Insert additional parameters here>
pause
exit
```

15. Change the default administrator passwords as described in [Changing the Default Administrator Passwords](#).

Installation Directory Structure

The following topics provide reference information on the Civic Platform folder structure to help you find the location of installed files. Also included are topics regarding the registry and services that are affected by the Civic Platform installer.

Related Information

[Top Level Directory Structure](#)

[Second Level Directory Structure](#)

[Registry Entries](#)

[Services](#)

Top Level Directory Structure

The top level Civic Platform installation directory contains several main subdirectories that store key Civic Platform components. See [Top Level Directory Structure in Civic Platform Destination Folder](#). For description on each directory, see [Civic Platform Top-Level Directory Structure](#).

The top level directory also contains the server cmd files for starting the server services. For example, you can click the run.av.ads.cmd file to start the application server service.



Note:

If you manually start a server service by clicking the cmd file, make sure that the corresponding service in [Services](#) is not started. Otherwise, the server may not function properly due to conflict between the services.

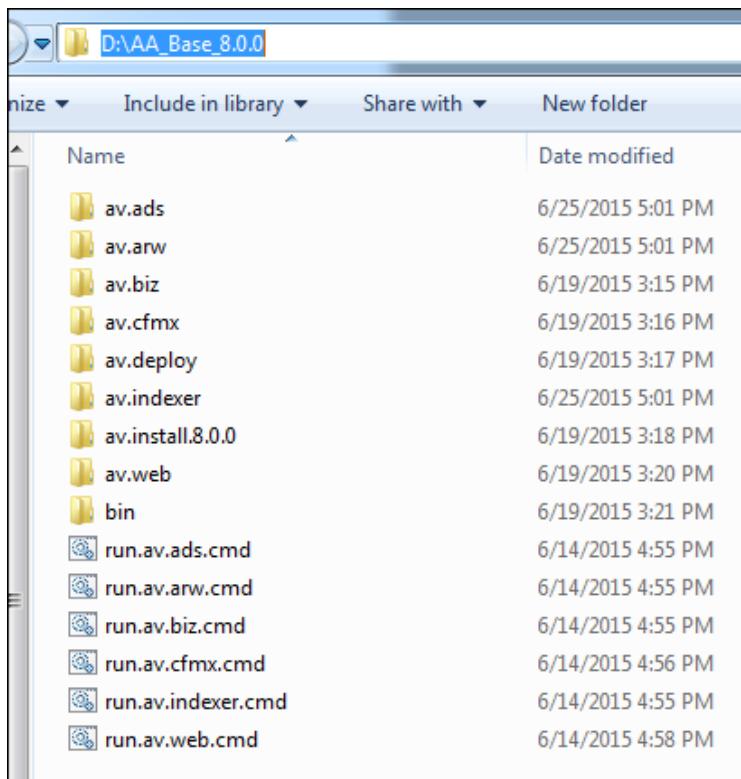


Figure 7: Top Level Directory Structure in Civic Platform Destination Folder

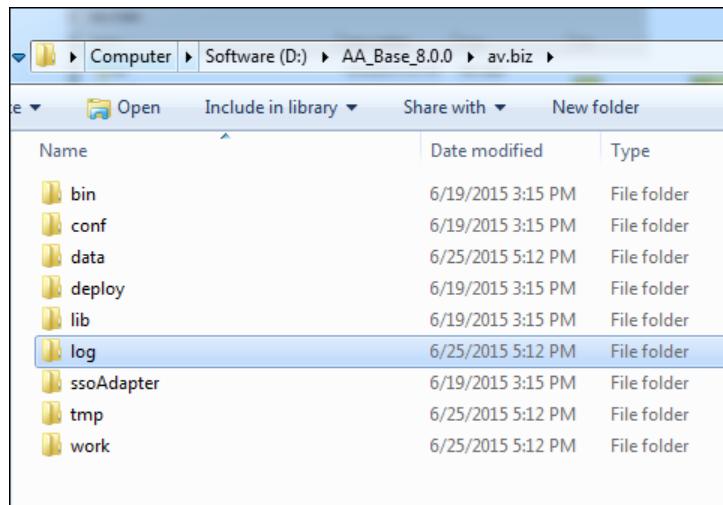
Table 3: Civic Platform Top-Level Directory Structure

Directory	Description
av.ads	Contains the configuration sets for the Accela Document Service component.
av.awr	Contains the configuration sets for the reporting server.
av.biz	Contains the configuration sets for the application server.
av.cfmx	Contains the configuration sets for the ColdFusion MX web server.
av.indexer	Contains the configuration sets for the index server.
av.install.<version_num>	Stores the Civic Platform base installer files.
av.web	Contains the configuration sets for the web server are located under the av.ads directory.
bin	Contains the fundamental utilities for running Java.

Second Level Directory Structure

Under the directory for each Civic Platform component (see [Civic Platform Top-Level Directory Structure](#)), there are a number of subdirectories, bin, conf, data, deploy, lib, log, tmp and work. [Subdirectories in the Application Server](#) shows you the subdirectories for the application server. The other server components have similar subdirectory structure.

For description on each subdirectory, see [Civic Platform Server Configuration Directory Structure](#).

**Figure 8: Subdirectories in the Application Server****Table 4: Civic Platform Server Configuration Directory Structure**

Directory	Description
bin	Contains the fundamental utilities for running the server.
conf	Contains the server configuration file ServerConfig.properties. After installation, you can make changes to ServerConfig.properties for implementing enhanced server functionality. For more information, see Post Installation Server Configuration .
data	This directory is available for use by services that want to store content in the file system.
deploy	This directory is the default location the hot deployment service looks to for dynamic deployment content.

Directory	Description
lib	Contains system libraries.
log	Contains server logs.
ssoAdapter	This directory is available in the application server and web server for supporting the SSO adapter configuration.
tmp	Contains some temporary files.
work	Contains some temporary files.

Registry Entries

Under HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Accela Inc, the Civic Platform installer adds the registry keys as shown in [Civic Platform Registry Keys](#).

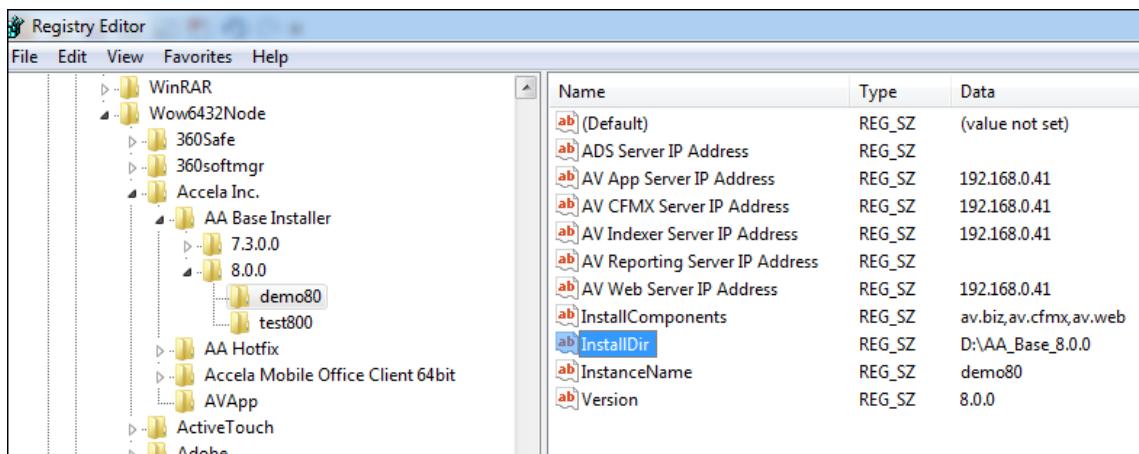


Figure 9: Civic Platform Registry Keys

Services

The Civic Platform installer adds the following services and sets them to “started” when the installation is complete.

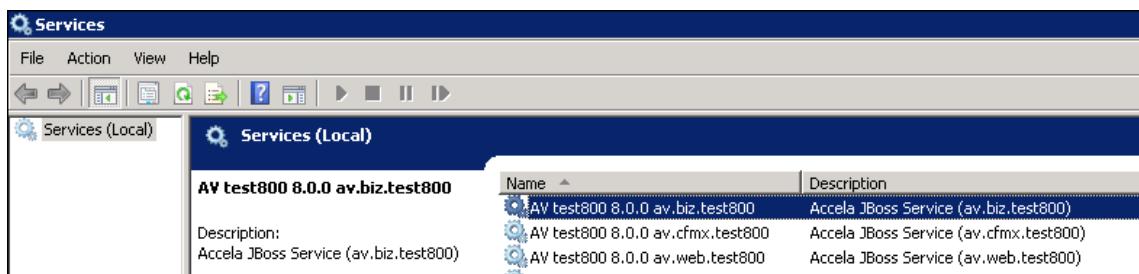


Figure 10: Civic Platform Services

Post Installation Configuration

The following procedures can only be performed after the Civic Platform installation is complete. These procedures require access to Civic Platform Administration or to files/services installed by Civic Platform.



Note:

IMPORTANT: After installing Civic Platform you must change the default administrator passwords. See the topic below for full details.

Related Information

[Importing the License Key](#)

[Starting Windows Services](#)

[Changing the Default Administrator Passwords](#)

[Configuring the Heartbeat Interval](#)

[Clearing the Server Cache for Load-Balanced Servers](#)

[Enabling Additional Security Measures](#)

[Configuring MultiRefs in Result Sets](#)

[Enabling the Facebook Integration](#)

[Configuring the Sent From Email Address for Trust Account Notifications](#)

[Configuring Exchange Server Permissions](#)

Importing the License Key

If you do not have a license key contact Accela Customer Support.

To import your Accela software license key:

1. Log in to Civic Platform.
2. Navigate to the Administration page.
3. Go to **Setup > System Tools** and select **Product License** from the drop-down menu.
4. Import the license key.

Starting Windows Services

Civic Platform installs Windows services on the target machine with display names similar to "AV test 9.0.0 av.ads.test."

These Windows services do not start automatically after installation. An administrator must start the services from the Windows Services console by setting the program to run or from the Command Prompt by executing the run.ads.bat file, located under %Installation Directory%. Running the program from the Command Prompt enables monitoring of the process.

Changing the Default Administrator Passwords

It is imperative that you change the default administrator passwords after performing a new installation of Civic Platform.

To change the default administrator passwords:

1. Log in to Civic Platform Super Agency.
2. For new installations, you must first create the agency before you can change the default administrator passwords.
 - a. Go to **Agency > Add**.
 - b. Refer to the *Civic Platform On-Premise Administrator Supplement* for complete instructions.
3. After you create the agency, change the default password for both of the following users:
 - Super agency admin user
 - Agency admin user
 - a. Navigate to the Classic Administration page.
 - b. Choose **User Profile > User**.
 - c. Locate the user profile you want to change the password for.
 - d. Enter the new password for the user.
 - e. Enter the new password again to confirm it.
 - f. Click **Save**.

Configuring the Heartbeat Interval

The 9.0.3 release includes a configuration file update that enables a heartbeat between the **av.web** and **av.biz** servers to help ensure active connections between the servers. Customers who install the Civic Platform server components **av.cfmx** and **av.web** on different servers must modify their configuration files to decrease the default **HEARTBEAT_INTERVAL** value based on their firewall time-out settings. The value of the **HEARTBEAT_INTERVAL** must be less than the firewall time-out setting to ensure that the server does not time out, by pinging it and keeping it active for users to access before the server times out.

For example, if your firewall time-out setting is 60 minutes (this is typically the default), you must change the **HEARTBEAT_INTERVAL** value to 50 minutes, represented in the configuration file in *milliseconds*. Therefore, the calculation to determine a 50-minute heart-beat ping is as follows: $50 \times 60 \times 1000 = 3000000$. If your firewall is configured with a 30-minute time-out setting, configure the **HEARTBEAT_INTERVAL** for 25 minutes, or 1500000 milliseconds, based on this calculation formula: $25 \times 60 \times 1000$.



Note: If you installed the Civic Platform server components **av.cfmx** and **av.web** on the *same* server, you can skip this procedure.

To set the **HEARTBEAT_INTERVAL** in your environment:

1. Navigate to your installation directory and open the following files in a text editor:

- av.cfmx\conf\av\av-biz-client.xml
 - av.web\conf\av\av-biz-client.xml
2. Locate the existing HEARTBEAT_INTERVAL value which is currently set at 2147483640:

```
<prop key="remote.connection.biz.connect.options.org.jboss.remoting3.  
RemotingOptions.HEARTBEAT_INTERVAL">2147483640</prop>
```

3. Change the HEARTBEAT_INTERVAL value based on the above calculation. For example, change 2147483640 to 3000000 if your firewall time-out setting is 60 minutes; change it to 1500000 if your firewall time-out setting is 30 minutes.
4. After saving the change, restart the JBoss server.

 **Note:** Subsequent hotfix releases include the configuration file with the default value. You must apply the HEARTBEAT_INTERVAL setting when installing the next hotfix release.

Clearing the Server Cache for Load-Balanced Servers

- [Clearing the Server Cache](#)

Clearing the Server Cache

Both load balanced and stand-alone Civic Platform servers can automatically clear the server cache when administrators make changes to system configuration data, such as Standard Choices.

Stand-alone Civic Platform servers do not need any system configuration.

For load balanced Civic Platform servers, administrators must configure av.clearcache.url in every ServerConfig.properties file to enable this feature.

```
av.clearcache.url=URL1,URL2,URL3,URL4,URL5..URL(n)
```

In the configuration line:

- Each URL(n) is one of the values below (note each value must end with the equal sign):

```
$av.biz.url$/av-biz-ws/services/clearCache/cacheName=  
$av.web.url$/portlets/clearCache?cacheName=  
$av.cfmx.url$/clearCache.jsp?cacheName=
```

- The \$av.biz.url\$, \$av.web.url\$, or \$av.cfmx.url\$ in each URL(n) refers to the URL of a server that associates with the current server having the ServerConfig.properties file. Please refer to the table below for the scope of \$av.biz.url\$, \$av.web.url\$, or \$av.cfmx.url\$ for each server type.

Table 5: URLs in ServerConfig.properties

Server Type	ServerConfig.properties Location	Scope of \$av.biz.url\$, \$av.web.url\$ or \$av.cfmx.url\$ in URL(n)
Application Server	\$installdir\$\av.biz\conf\av	The URLs of the web servers and the ColdFusion MX web servers that work with the current application server, and all the other application servers.

Server Type	ServerConfig.properties Location	Scope of \$av.biz.url\$, \$av.web.url\$ or \$av.cfmx.url\$ in URL(n)
Web Server	\$installdir\$\av\web\conf\av	The URLs of the application servers and the ColdFusion MX web servers that work with the current web server, and all the other web servers.
ColdFusion MX Web Server	\$installdir\$\av\cfmx\conf\av	The URLs of the application servers and the web servers that work with the current ColdFusion MX web server, and all the other ColdFusion MX web servers.

Enabling Additional Security Measures

Additional security measures are in place to limit exposure to potential vulnerabilities related to XSS and CSRF security.

To enable additional security measures:

1. To limit exposure to potential vulnerabilities related to XSS and CSRF security, add the following code to the ServerConfig.properties file in \av\web\conf\av\ and \av\cfmx\conf\av\.

```
#Security validation switch
av.security.xss.filter=true
av.security.csrf.filter=true
```

2. To defense phishing from URL redirection, add the following code to the ServerConfig.properties file in \av\web\conf\av\.

```
#Security turn on or off

av.security.xss.filter=true

av.security.xss.phishing.filter=true
```

With the defense, users can only enter external URLs in a URL field provided in Civic Platform and receive error messages when entering external URLs in any other fields.

3. Users must clear their browser cache, including cookies, before accessing the latest Civic Platform.

Importing security certificates for HTTPS connections to the Biz server

The Civic Platform Biz server is installed with a self-signed certificate by default. For HTTPS connections from component IIS servers (such as Citizen Access, Mobile Office, Accela GIS, and Accela Gateway) to the Biz server, your agency can choose to either:

- Use the default Biz server self-signed certificate, which must be imported to the trusted certificate store on the component IIS server(s).
- Use your agency's trusted domain certificate, which must be imported to the trusted certificate store on both the Civic Platform Biz server and the component IIS server(s).

The following procedure describes how to import the Biz server self-signed certificate to the Citizen Access IIS server's Trusted Certificate store. Perform this procedure on each server that needs to connect to the Biz server via https.

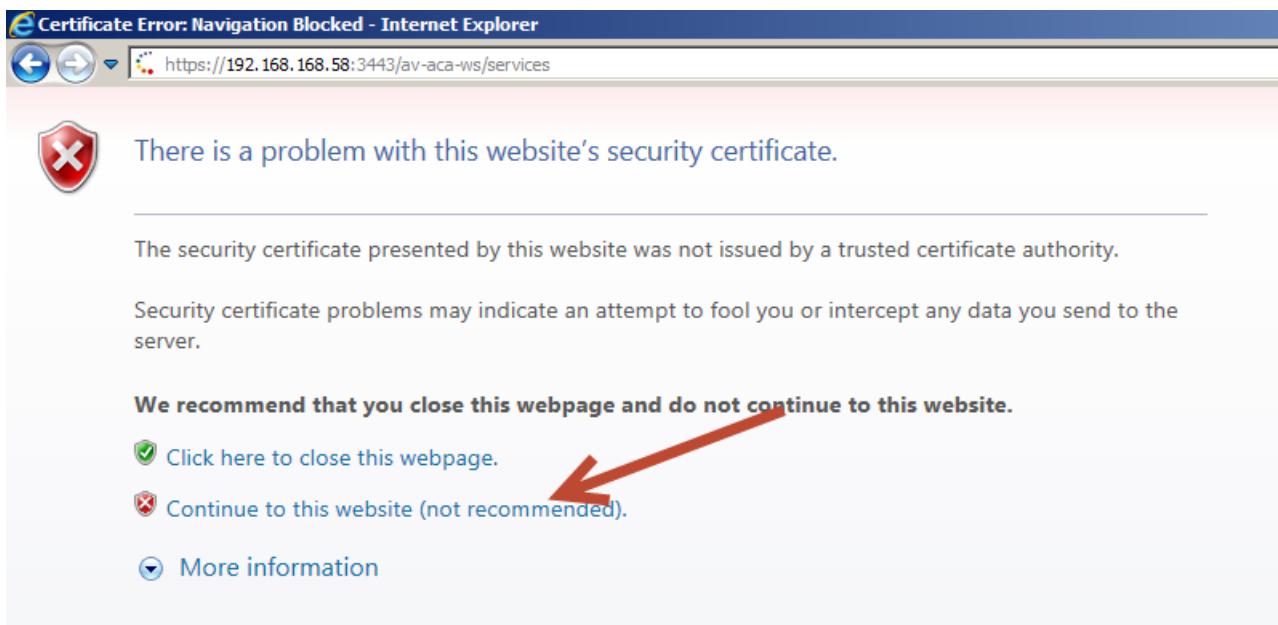


Note: If your agency is using a trusted domain certificate instead of the Biz server's self-signed certificate, perform a similar procedure for importing your agency's trusted domain certificate to the Civic Platform Biz server and component IIS servers.

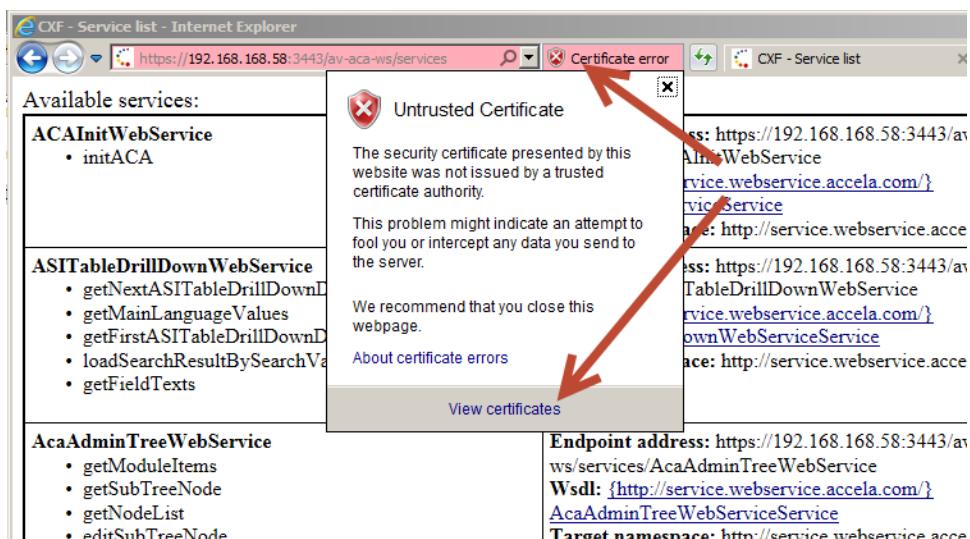
- Get the Citizen Access server URL from the `web.config` file on the Citizen Access server's IIS root folder, as shown below:

```
<website name="wsserver01" url="https://192.168.168.58:3443/av-aca-ws/services" timeout="300">
  <webServices>
    <webservice id="Accela.ACA.WSProxy.EDMSDocumentUploadwebserviceservice" url="/av-aca-ws/service"
      <webservice id="Accela.ACA.WSProxy.spellcheckerwebserviceservice" url="/av-biz-ws/services/sp
    </webServices>
  </website>
</websites>
```

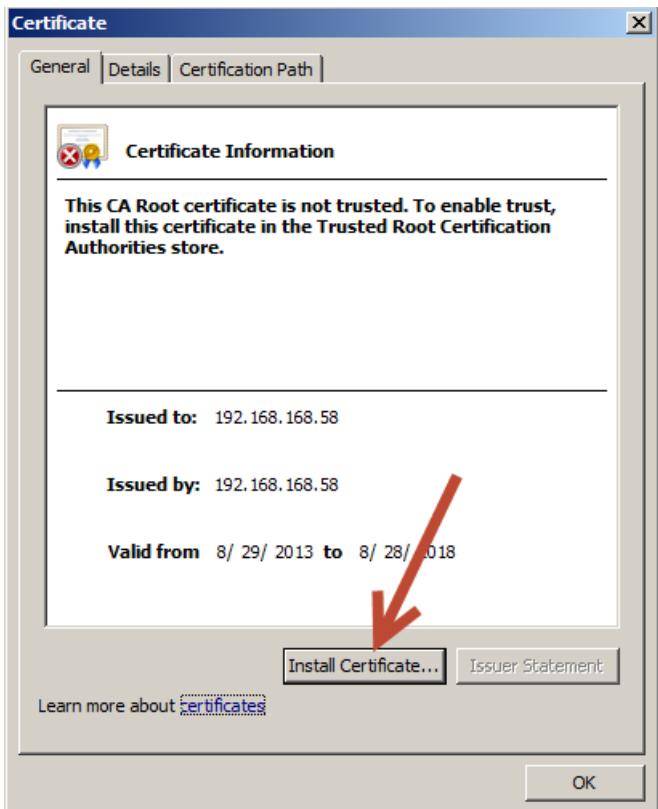
- On a web browser, go to the Citizen Access server URL. When the browser returns a security warning that the certificate cannot be verified, click **Continue to this website...**:



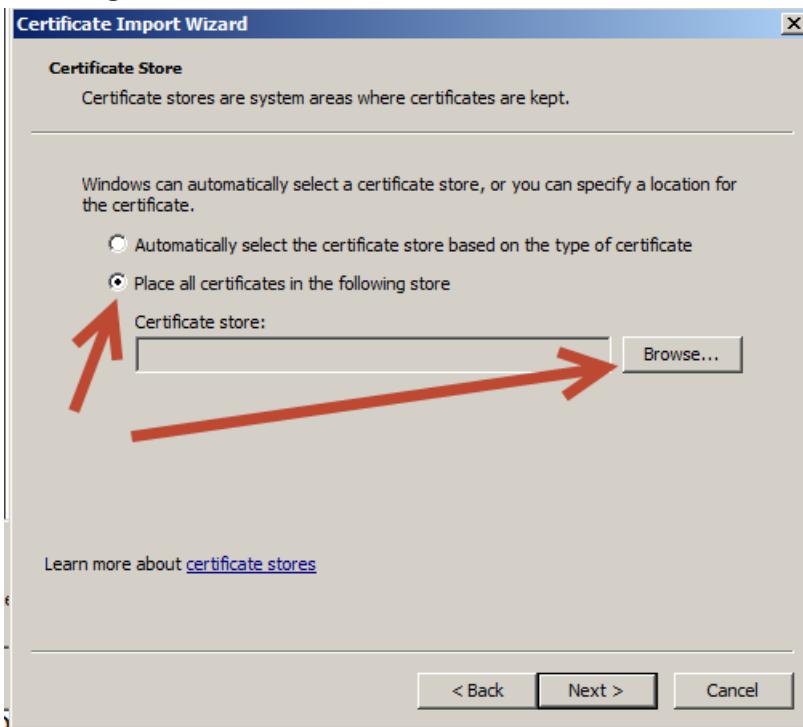
- Click **Certificate Error** next to the address bar, then click **View certificates**:



4. On the **Certificate** window, click **Install Certificate** and click **OK**. If this option is not enabled, close IE and run it again as Administrator.



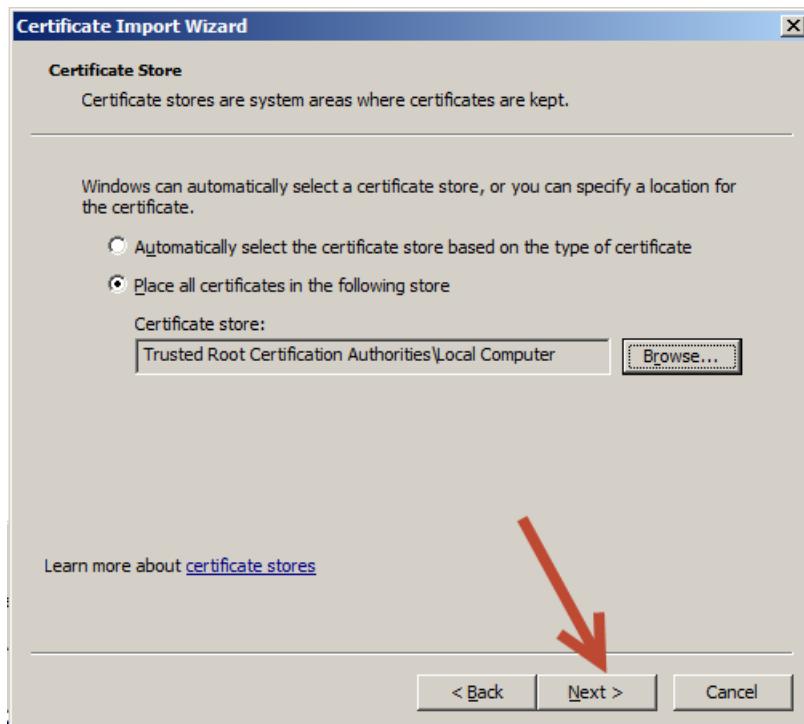
5. Click **Next**, then on the **Certificate Import Wizard** window, select **Place all certificates in the following store**, and click **Browse**:



6. Check the **Show physical stores** checkbox, expand **Trusted Root Certificate Authorities**, select **Local Computer**, and click **OK**.



7. Click **Next**, and then **Finish** to close the wizard.



8. Go to the Citizen Access URL on the browser again to verify that the browser no longer returns a security warning.

Configuring MultiRefs in Result Sets

By default, Civic Platform uses MultiRef data structures in result sets generated by Axis for Web service calls. However, ESB platforms such as Oracle ESB cannot parse result sets with MultiRef data structures. If you want to remove MultiRefs from result sets, configure the following:

- Turn the sendMultiRefs option off in Axis server-config.wsdd.

1. On the application server machine, open the global configuration file \$Install_Dir\$\av.biz\deploy\av-biz.ear\av-biz-ws-0.9.war\WEB-INF\server-config.wsdd.
2. Find the line for the setting sendMultiRefs:

```
<parameter name="sendMultiRefs" value="true"/>
```

Change it to:

```
<parameter name="sendMultiRefs" value="false"/>
```

Add a switch parameter SendMultiRefs in the EDMS Standard Choice Value and set the parameter to False.

Table 6: Standard Choices Configuration

Name	New or Existing	Level	Standard Choice values	Value Description	Description
EDMS	Existing	Agency	<i>EDMS name</i>	EDMS_VENDOR= STANDARD; URL={Your URL goes here}; EDMS_DOCUMENT_SIZE_MAX={Number}MB; ACA_EDMS_DOCUMENT_SIZE_MAX={Number}MB; sendMultiRefs=false	If the parameter sendMultiRefs is True (default value), the EDMS client code sends request content XML with multiRefs data structure elements. If the parameter sendMultiRefs is False, the EDMS client code sends request content XML without multiRefs data structure elements.

Enabling the Facebook Integration

For information about setting up the Accela Facebook integration, see the Social Media Integrations chapter in the Accela Civic Platform Administrator Guide.

To complete the process of setting up the Accela Facebook integration an administrator must modify the web.config file, as described below.

To enable the Accela Facebook integration:

1. Create your agency's ACA-Facebook app, as detailed in the Social Media Integrations chapter in the Accela Civic Platform Administrator Guide.
2. Go to <https://developers.facebook.com> and open your ACA-Facebook app.

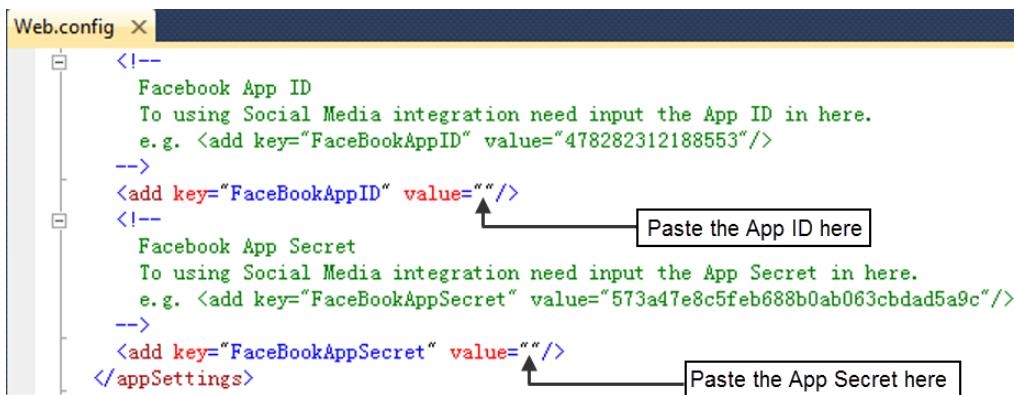
The App Details page displays, with the App ID and App Secret that you need to copy/paste into the web.config file in the next steps.

Apps > City of Progress Citizen Access

Settings

Summary	App ID/API Key 409012695823671	App Secret 73b8bdbf1f378a606c35a95553358e47
	App Namespace cityofprogress	Site URL https://aca.dev.accela.com/facebook-aca/socialmedia/facebookportal.aspx?&fb_source=search&ref=ts
	Site Domain aca.dev.accela.com	Canvas Page http://apps.facebook.com/cityofprogress/
	Canvas URL https://aca.dev.accela.com/facebook-aca/socialmedia/facebookportal.aspx?&fb_source=search&ref=ts	Secure Canvas URL https://aca.dev.accela.com/facebook-aca/socialmedia/facebookportal.aspx?&fb_source=search&ref=ts

3. On the Citizen Access web server, navigate to the web.config file, which resides in the virtual root directory for Citizen Access. For example: \\inetpub\\wwwroot\\<citizenaccess> where <citizenaccess> can be whatever name you choose for the installation directory.
4. Locate the Facebook App ID and Facebook App Secret sections in the web.config file, shown here.



5. In the App ID area, paste the App ID between the empty quotation marks provided; in the App Secret area, paste the App Secret between the empty quotation marks provided.

The following is an example of the finished results:

- <add key="FacebookAppID" value="409012695823671"/>
- <add key="FacebookAppSecret" value="73b8bdbf1f378a606c35a95553358e47"/>

Note that the values in the example text exist as comments only; do not change those values.

6. Save the web.config file and exit.

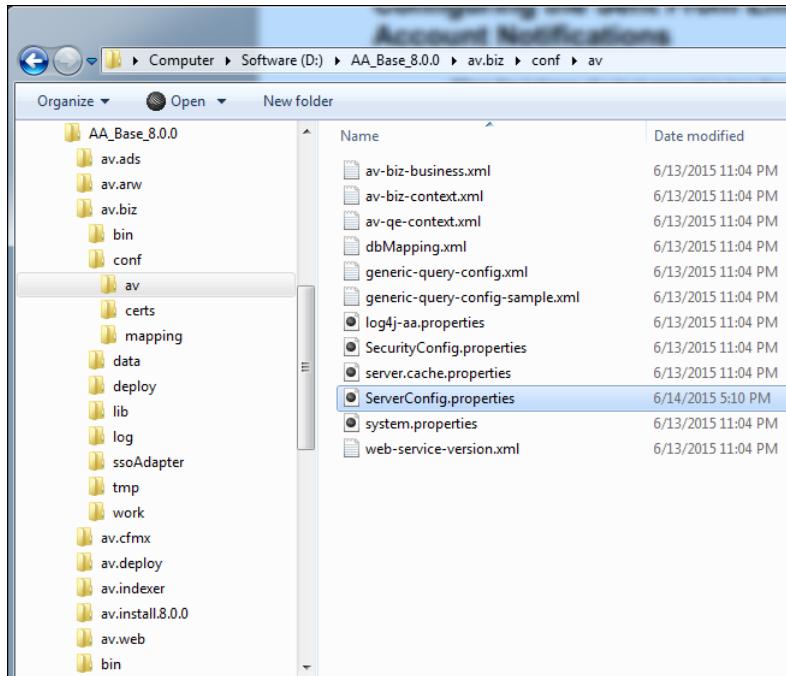
Configuring the Sent From Email Address for Trust Account Notifications

When the balance of a trust account is less than the threshold amount you defined in the trust account, Civic Platform can send a low balance email notification to the trust account manager. To enable this functionality, you must configure the ServerConfig.properties file of your av.biz server to include the sender's email credentials, as described below.

To configure the sender's e-mail address for trust account notifications:

1. On your Civic Platform server, navigate to the av.biz ServerConfig.properties file.

This file resides in the root directory for your Civic Platform implementation, which can be whatever name you choose for the installation directory. Refer to the sample directory structure in the screenshot below.



2. Find the mail server configuration section (use the **ctrl+f** function to search the document), and modify the settings that exist in bold text in the following script:

```
# mail server configuration
av.mail.user=<username> (The username associated with your preferred "Sent
From" email account)
av.mail.password=<password> (The password associated with your preferred
"Sent From" email account)
av.mail.from=Auto_Sender@Agency.com (The preferred "Sent From" email
address that recipients receive notification emails from)
```

3. Save the serverConfig.properties file.
4. Restart the av.biz server. Your changes do not take effect until you restart the server.

Configuring Exchange Server Permissions

To implement communication manager functionality, configure your Microsoft Exchange Server account permissions to enable users to:

- Send Outlook meeting requests on behalf of other users
- View the calendar availability of Outlook users
- Send email notifications on behalf of other users

Topics

- [Email Server Configuration](#)
- [Calendar Server Configuration](#)

Email Server Configuration

In Civic Platform, when agency users send meeting requests in the calendar portlet, the sender is the responsible person that you defined in calendar administration. You must configure your Exchange Server email permissions to allow the default email account to send email on behalf of that responsible person.

To configure default email account permissions on Exchange Server 2007:

1. For the Send Email Permission setting of the default email account that you configured in Communication Manager > General Setting > Email Server Settings, assign permission to send emails on behalf of other accounts.
 - a. Open ExchangeManagementShell.
 - b. Enter the following command:

```
Get-ClientAccessServer | Add-ADPermission -User admin@agency.com -ExtendedRights ms-Exch-EPI-Impersonation
```

To configure default email account permissions on Exchange Server 2010:

1. For the Send Email Permission setting of the default email account that you configured in Communication Manager > General Setting > Email Server Settings, assign permission to send emails on behalf of other accounts.
 - a. Open ExchangeManagementShell.
 - b. Enter the following command:

```
New-ManagementRoleAssignment -Role:ApplicationImpersonation -User: admin@agency.com
```

Calendar Server Configuration

Modify the administrator's account permission to grant access to view Outlook calendar availability of the other agency staff. This enables Civic Platform users who organize meetings to view internal staff availability, provided they are on the same Exchange server.

To configure the defaults of the calendar permissions on Exchange Server 2007:

1. For the Outlook Calendar View Permission setting of the default calendar account that you configured in **Communication Manager > General Settings > Calendar Server Settings**, assign administrator permissions to access other user accounts Outlook Calendar.
 - a. Open ExchangeManagementShell.
 - b. Enter the following command:

```
Add-MailboxPermission -identity John@agency.com -User admin@agencys.com -AccessRights FullAccess
```

To configure the defaults of the calendar permissions on Exchange Server 2010:

1. For the Outlook Calendar View Permission setting of the default calendar account that you configured in Communication Manager > General Settings > Calendar Server Settings, assign administrator permissions to access other user accounts Outlook Calendar.

a. Open ExchangeManagementShell.

b. Enter the following command:

```
Add-MailboxFolderPermission -Identity John@agency.com:\calendar -User  
admin@agency.com -AccessRights Full Access
```

Installation Maintenance

This chapter provides instructions to uninstall, remove, or install new modules to an existing Civic Platform installation, and also the instructions to install a hotfix or feature pack.

When you run a Civic Platform installer a second (or later) time, the installation runs in maintenance mode. Maintenance mode allows the user to modify feature selections from the first-time installation, repair the features already, or remove the entire application. You launch the maintenance process from the Windows Add/Remove Programs utility.

Related Information

[Modifying or Repairing an Installation](#)

[Removing a Civic Platform Installation](#)

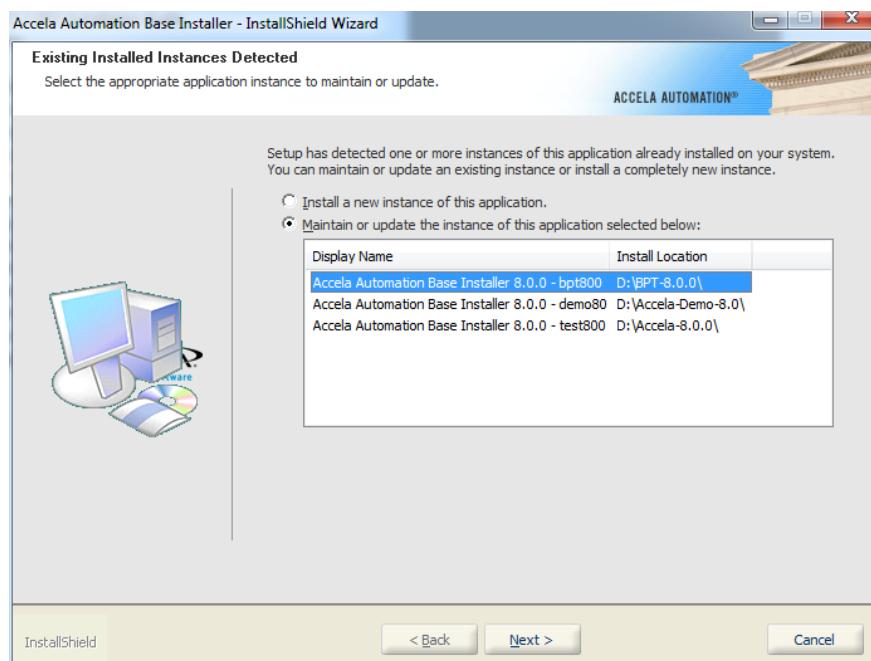
Modifying or Repairing an Installation

To modify or repair an existing installation:

Stop all Civic Platform processes before invoking the Add/Remove Programs utility and close down all Civic Platform files in use. You can stop processes from the Windows services control or the Command prompt.

1. Launch the uninstall program from the Windows Add/Remove Program utility.

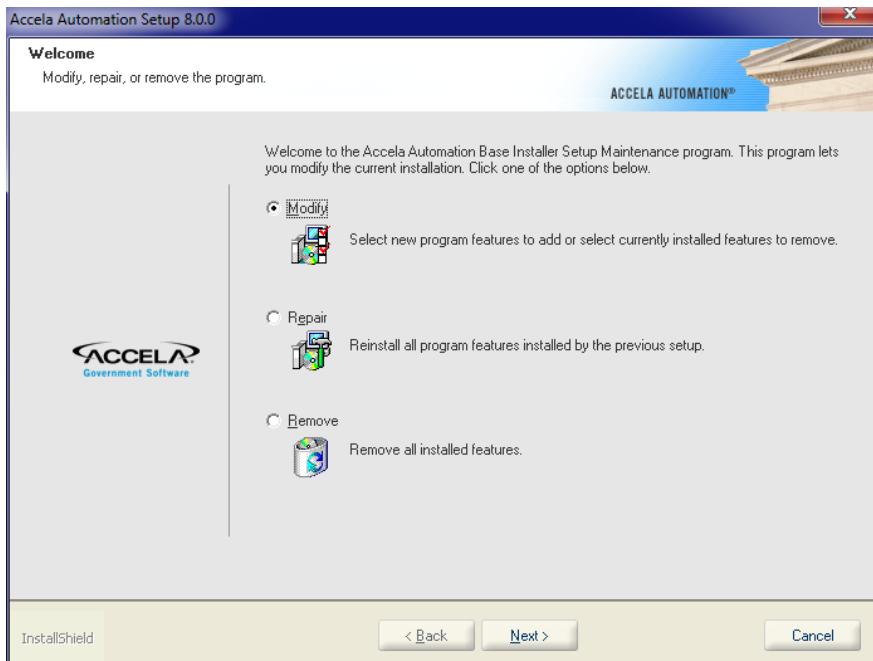
The Civic Platform Base Installer - Install Shield Wizard screen displays.



2. Highlight the instance to maintain or repair and select the option to maintain or update the highlighted instance.

3. Click **Next**.

The Civic Platform Modify/Repair/Remove screen displays.



4. Select Modify or Repair.

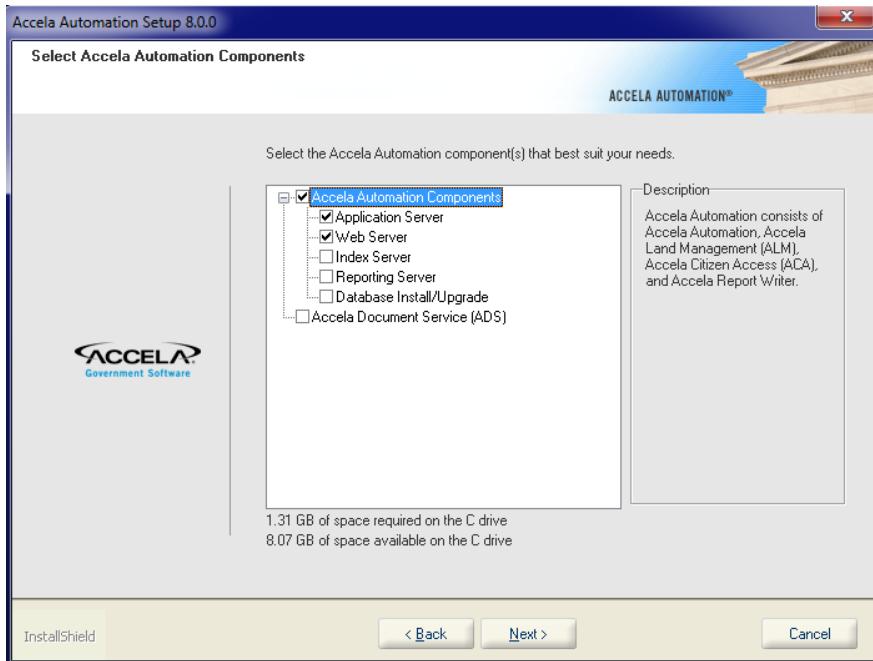
5. Click Next.



Note:
If there is 0.00MB of space required on the E drive, this indicates that you are in the Maintenance mode and you installed all the checked components from the previous installation.

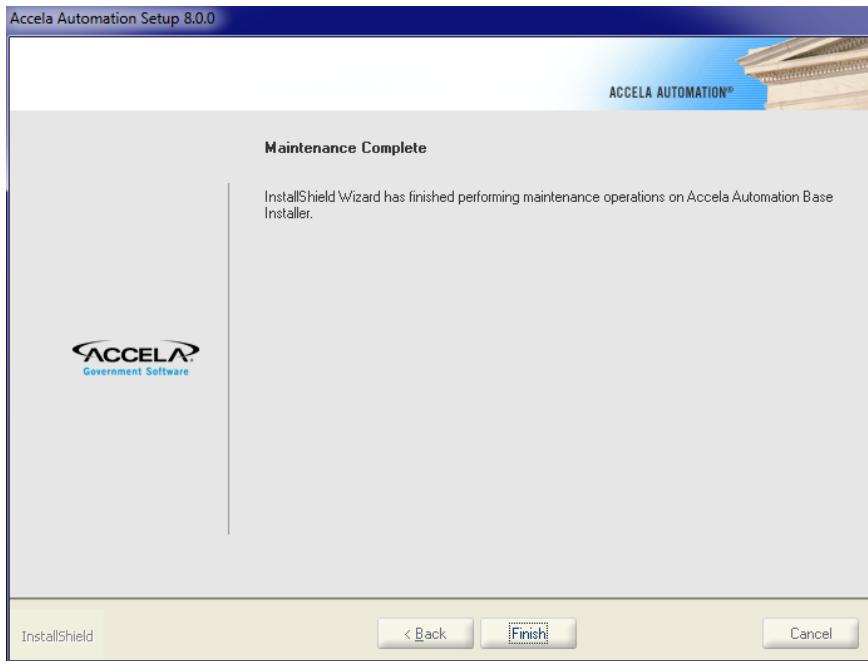
All the previous configuration settings automatically populate the dialogs.

The Select Civic Platform Components screen displays.



6. Click Next to modify or repair the installation.

- See [Managing a Civic Platform Configuration](#) to modify an installation.
- If you repair an installation, the installer automatically repairs the components that you installed. The Maintenance Complete screen displays.



7. Click **Finish** to conclude the activity.

Removing a Civic Platform Installation

You must remove previous versions of Civic Platform base and application prior to installing Civic Platform 9.0.0.

Use the Windows Add/Remove Programs utility to remove a Civic Platform instance.

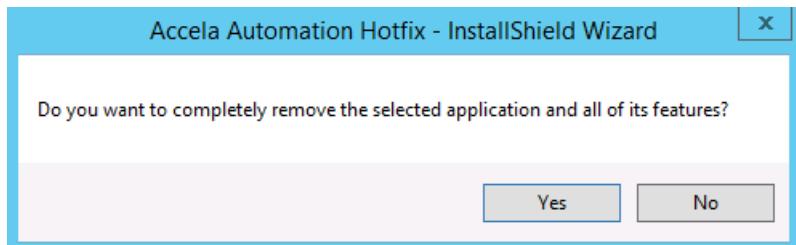
 **Note:** We highly recommend that you do not install Civic Platform 9.0.0 on the same server as any previous version. If you plan to keep your 8.0.x installation, you must install 9.0.0 on a different server.

If you want to use the configuration of the to-be-removed instance as the basis for a new instance, change the name of the configuration folder of the to-be-removed instance first. See [Renaming Your Configuration Folder](#).

Stop all Civic Platform processes before invoking the Add/Remove Programs utility and close down all Civic Platform files in use. You can stop processes from the Windows services application or from the Command prompt.

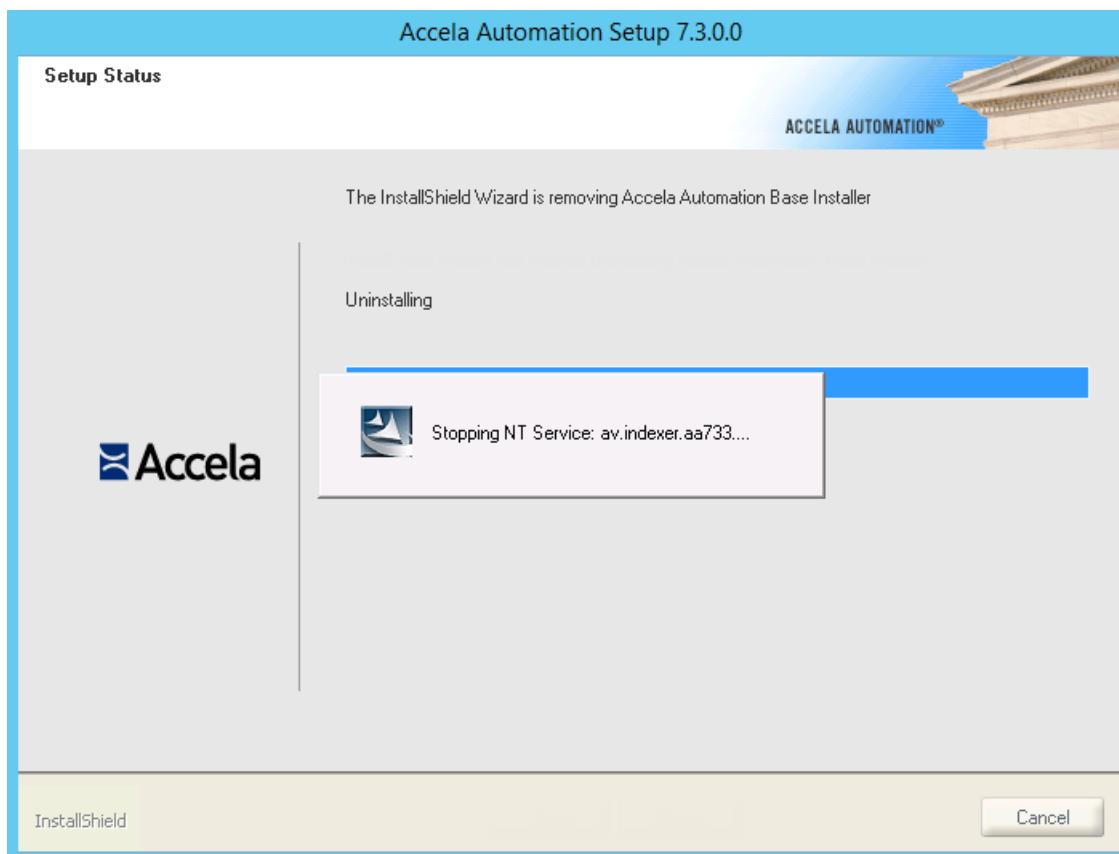
To remove a Civic Platform instance:

1. Go to Control Panel > Programs > Uninstall a Program.
2. Select **Accela Automation Application <version>**, and then click **Uninstall**.
The Install Shield Wizard asks you to confirm the removal.

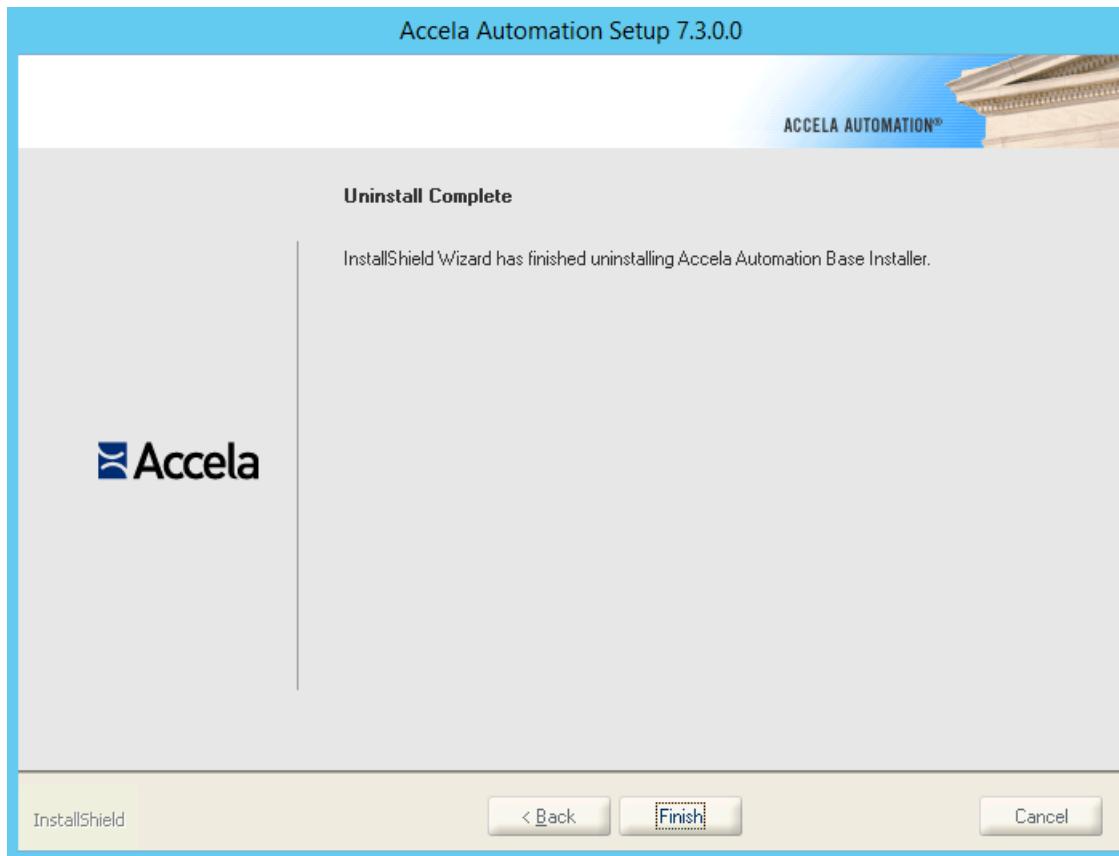


3. Click Yes.

The uninstallation process begins and a series of status messages display.



The Uninstall Complete screen displays.



4. Click **Finish.**

The uninstallation process completes and you are returned to the Control Panel.

5. Repeat these steps for the **Accela Automation Base <version> prior to installing Civic Platform 9.0.0.**

Troubleshooting

Use the recommendations in this chapter to help troubleshoot issues during and after installation.

Related Information

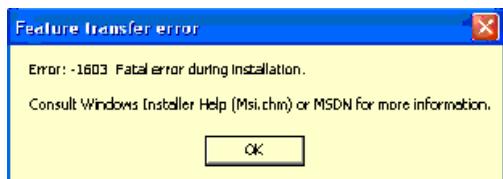
[Error 1603, 1638](#)

[Error 1628, 1607, 1618](#)

[Disk Out of Space](#)

Error 1603, 1638

Error 1603 or 1638 occur if you accidentally start the installer more than one time, which results in more than one IDriver.exe process under your Windows Task Manager.



If the problem persists, cancel the installation and perform the following operation:

Properly register the file msieexec.exe by using the following command line:

```
<WINDOWSFOLDER>\System32\msieexec.exe /REGSERVER
```

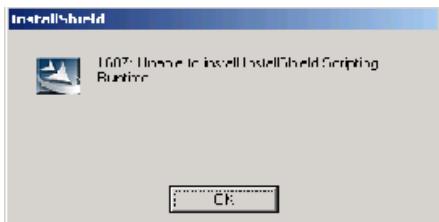
You can enter the command line in the Windows Start | Run dialog, after replacing <WINDOWSFOLDER> with the location of the Windows folder.

Error 1628, 1607, 1618

Error 1628 occurs if you interrupt the installation process.



If you restart the installer, besides error 1603 shown in [Error 1603, 1638](#), error 1607 or 1618 can also occur.



To resolve these errors, go through the common resolution described in [Error 1603, 1638](#).

Disk Out of Space

This error mostly happens when the temp folder on your machine does not have sufficient disk space for the database setup and database upgrade processes. Reserve 3 GB of free disk space for a complete installation of all server components.

When this error occurs, cancel the installation and clear the temporary folder on your machine. Typically, this temporary folder locates on C:\temp. Pay attention to "bin" subfolder. If you cannot delete objects under the temporary folder, restart your host and repeat the delete operation.

Installing Additional Server Tools

You can install additional tools to the server.

Related Information

[Configuring the SMS Adapter](#)

[Installing the Ad Hoc Report Tool](#)

[Installing Oracle 11g OCI Driver Configuration Tool](#)

[Upgrading the Database for Nearby Query Support](#)

Configuring the SMS Adapter

Civic Platform's communication manager feature integrates with SMS text messaging services, enabling you to communicate with agency users by text message.

To implement this integration, you must configure an SMS adapter web service (.wsdl file), provided by Accela.

Related Information

[SMS Adapter Prerequisites](#)

[Deploying the Web Service](#)

[Configuring the Web Service](#)

[Testing the Web Service](#)

SMS Adapter Prerequisites

Prior to configuring the SMS adapter, you must install the following.

- SMS text messaging adapter

Accela provides a sample SMS Adapter, which you can access from the Civic Platform installation directory; for example, D:\AA9.0.0\main-dev\ws-sdk\SMSAdapter\war.

- Apache Tomcat application server

Go to <http://tomcat.apache.org/download-60.cgi>. Download Tomcat and unzip the installation files to your local directory; for example, D:\apache-tomcat-6.0.29.

- JDK 6 or higher.

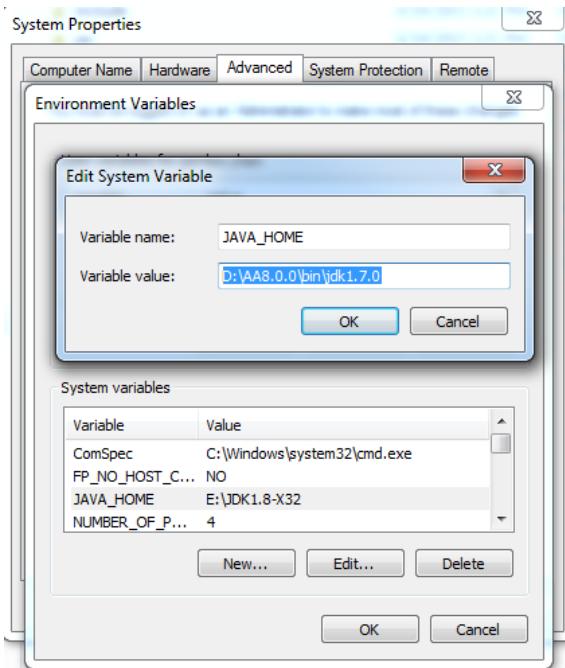
Go to <http://www.oracle.com/technetwork/java/javase/downloads/index.html>. Download and install JDK 6 or higher.

Deploying the Web Service

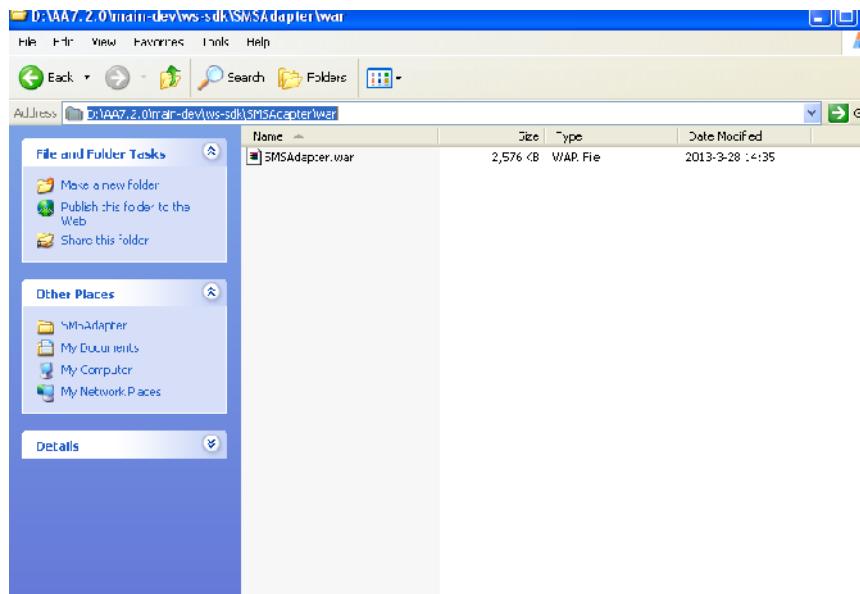
Use the instructions in this section to deploy the web service.

To deploy the web service:

1. Add JAVA_HOME=D:\AA9.0.0\bin\jdk1.7.0 to your system variables.

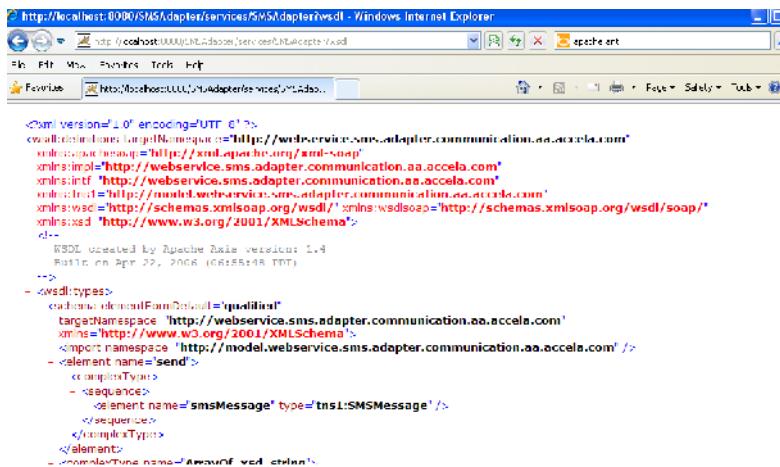


- Get the SMSAdapter.war file from the Civic Platform source code directory; for example, D:\AA_Prod\ws-sdk\SMSAdapter.



- Copy the SMSAdapter.war file to your Tomcat directory; for example, D:\apache-tomcat-6.0.29\webapps.
- Go to D:\apache-tomcat-6.0.29\bin. Double-click startup.bat to start the server.
- Enter the following URL in your browser's address bar: <http://localhost:8080/SMSAdapter/services/SMSAdapter?wsdl>

Your browser displays the web service, indicating that you have successfully deployed the web service.



```

<?xml version='1.0' encoding='UTF-8'?>
<wsdl:definitions name="http://webservice.sms.adapter.communication.aa.accela.com"
    xmlns:tns="http://webservice.sms.adapter.communication.aa.accela.com"
    xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
    xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
    xmlns:types="http://www.w3.org/2001/XMLSchema"
    xmlns:axis="http://axis.apache.org/axis2/java/core/types/">
    <!-- RODEL created by Apache Axis version: 1.4
        Built on Apr 29, 2006 (08:55:48 EDT)
    -->
    <types>
        <element name="send" type="tns:SMSMessage"/>
        <!-- Sequence -->
        <element name="smsMessage" type="tns:SMSMessage"/>
        <!-- Sequence -->
        <element name="request" type="tns:SMSMessage"/>
        <!-- ComplexType -->
        <!-- Element -->
        <!-- Element -->
    </types>

```

Configuring the Web Service

Perform the following steps to configure your web service for use by Civic Platform.

To configure your web service for use by Civic Platform:

1. Configure the standard choice COMMUNICATION_SMS_PROVIDERS.

The Standard Choice value is your SMS provider's name; for example, Message Media.

The information you provide in this standard choice informs the options available in Communication Manager > General Settings > SMS Server Settings.

2. Configure SMS Server Settings:

a. In Civic Platform, navigate to Setup > Communication Manager > General Settings > SMS Server Settings.

SMS Provider	The provider that you configured in the Standard Choice COMMUNICATION_SMS_PROVIDERS.
--------------	--

Adapter URL	The SMSAdapter.wsdl web service location.
-------------	---

Account	The user name for accessing the SMS service provider's website.
---------	---

Password	The password for accessing the SMS service provider's website.
----------	--

Configuring SMS Account Settings in the SMS Adapter

Perform the following steps to configure your SMS Account Settings in the SMS Adapter.

To configure your SMS Account Settings in the SMS adapter:

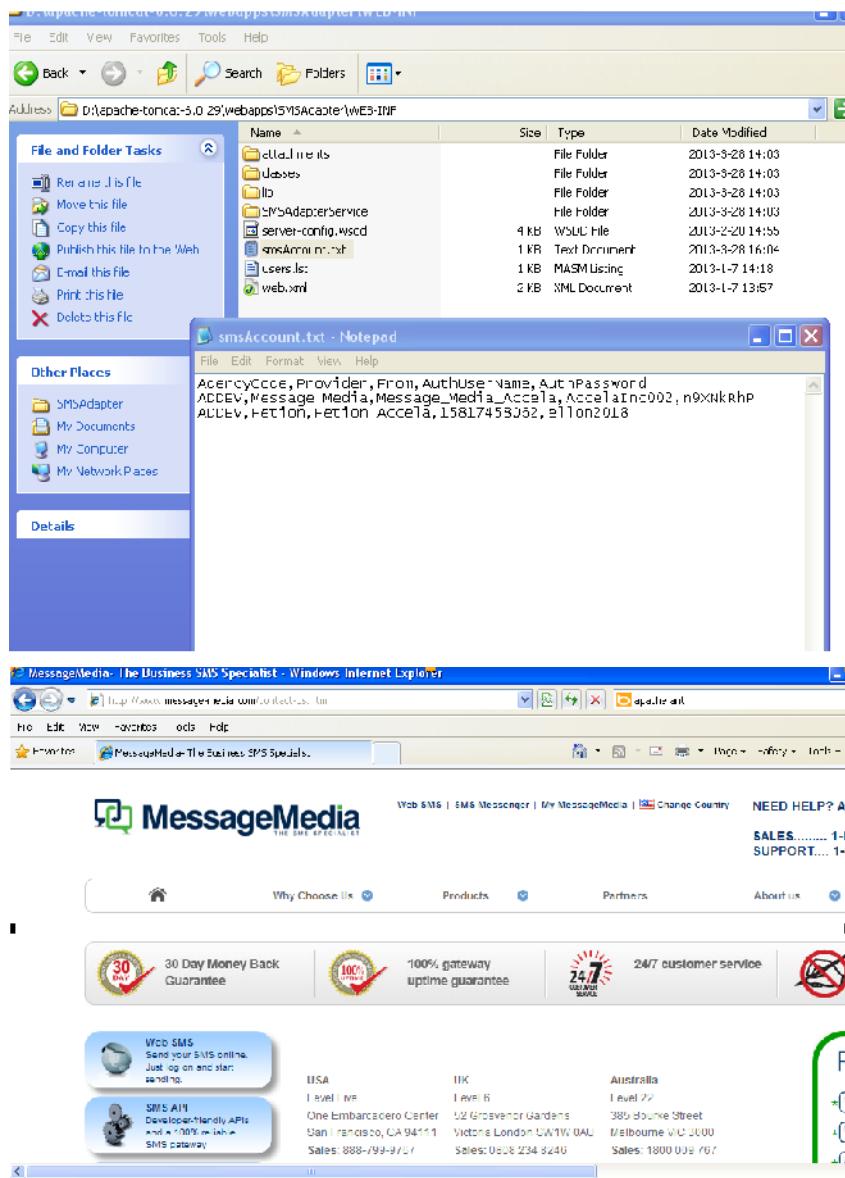
1. Go to D:\apache-tomcat-6.0.29\webapps\SMSAdapter\WEB-INF\smsAccount.txt and add your SMS account information to the smsAdapter.txt file. Use the following parameters.

Agency Code	Your agency code.
-------------	-------------------

Provider	The SMS provider that you configured in SMS Server Settings.
----------	--

From	The phone number that you configured in Communication Manager > Account Settings > SMS Account Detail Tab.
------	--

AuthUserName	The user name of an authorized user of your SMS service provider account. For example, this is the user name for logging in to your Message Media account on the web.
AuthPassword	The password of an authorized user of your SMS service provider account. For example, this is the password for logging in to your Message Media account on the web.



2. Configure communication manager settings:

- Go to **Setup > Communication Manager > Account Settings > SMS Accounts tab**, and complete the configuration settings for your agency.
- Go to **Setup > Communication Manager > General Settings > SMS Server Settings tab**, and complete the configuration settings for your agency.

Refer to the Communication Manager chapter of the *Accela Civic Platform Administrator Guide* for complete details.

Testing the Web Service

Test the web service by sending an SMS text message from Civic Platform.

1. Go to **Record portlet > Communications tab> New SMS**.
2. Complete the fields and send the SMS text message.
3. Check status of the message in the Sent Items folder in communication manager.
 - A Sent status indicates success.
 - A Failed status indicates you need to modify your settings.

Installing the Ad Hoc Report Tool

To use the ad hoc reports feature in Civic Platform, you must install the ad hoc report tool to the ad hoc report server. Some additional configurations are necessary after the installation.

Follow the instructions in this chapter to install and configure ad hoc reports.

Related Information

[Preparing Your System](#)

[Running the Ad Hoc Report Installer](#)

[Configuring the Ad Hoc Reporting Service](#)

[Deploying Ad Hoc Reports into Another Environment](#)

Preparing Your System

Topics

- [System Requirements](#)
- [Server Domain Name Requirement](#)

System Requirements

You can use either Windows Server 2008 R2 or Windows Server 2012 to host the ad hoc report server. The server must meet the following system requirements before you can proceed with the installation.

- If you use Windows Server 2008 R2, install Microsoft Internet Information Server (IIS) 7.x with the default roles and role services.
- If you use Windows Server 2012, install Microsoft Internet Information Server (IIS) 8.x and all the roles and role services as shown in [Required Roles and Services on Windows Server 2012](#).

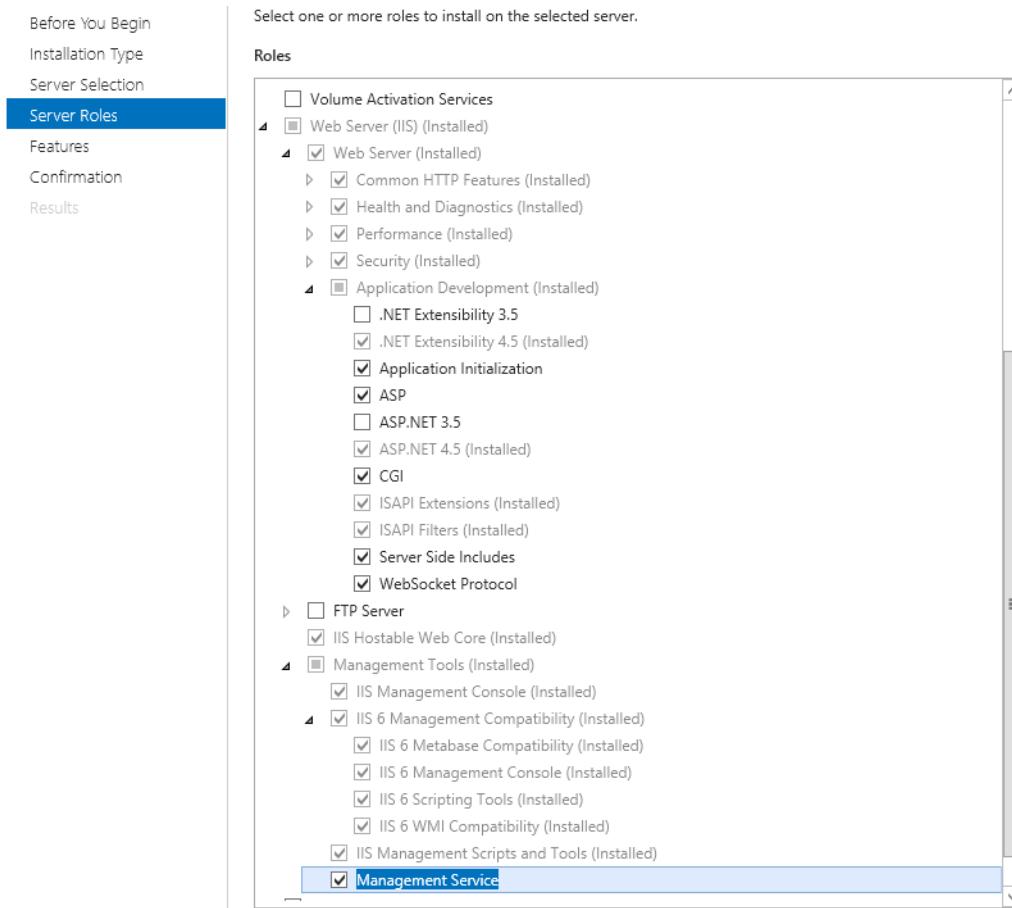


Figure 11: Required Roles and Services on Windows Server 2012

- Microsoft .NET framework 4.0 or 4.5
- If you have an Oracle database:
 - Ensure that Oracle database version is 9i or higher.
 - The TNS name of the Oracle database host must be the server IP address, not the server name.
 - Ensure that you have added the read & execute permission to the %ORACLE_HOME% folder and sub-folders for authenticated users. If you are adding the permission now, remember to restart the server.

Server Domain Name Requirement

Due to Internet Explorer limitation on cross domain access, you must configure the domain names of the ad hoc report server and the Civic Platform web server with identical hierarchical levels, for Civic Platform to successfully access the report server.

Specifically, if the domain name of the Civic Platform web server has 3 hierarchical levels, the domain name of the ad hoc report server must have 3 hierarchical levels as well. For example, if the web server domain name is test-site.accela.com, the ad-hoc report server domain name can be ad-hoc.accela.com, and cannot be ad-hoc.com.

Running the Ad Hoc Report Installer

You can run the ad hoc report installer to install ad hoc report tool to the ad hoc report server.



Note:

Before proceeding, you must contact Accela Customer Support to obtain an ad hoc report license key.

To run the ad hoc report installer:

1. Locate and double-click the ad hoc report installer to launch the installation wizard. The installer file is named Setup_Adhoc_Report_9.0.0_161211.exe.

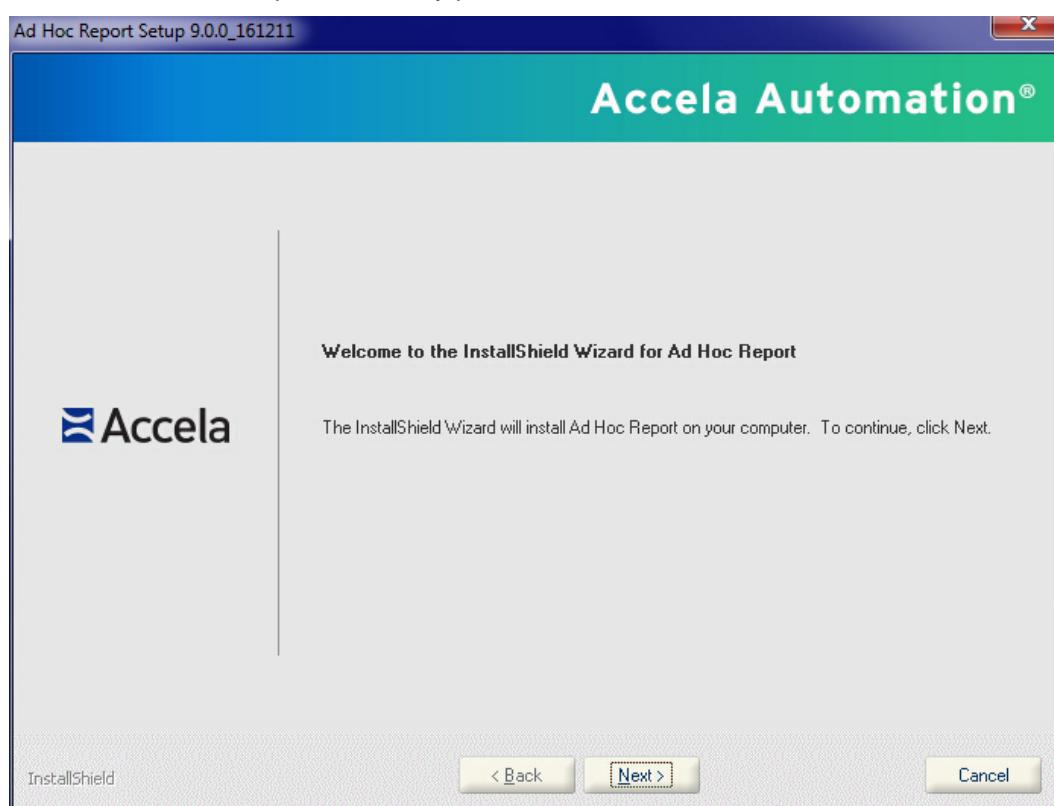
The installer checks whether the server meets the software requirements.

If you run the ad hoc report installer on Windows 2008 R2 and Microsoft .NET framework 4.0 or 4.5 is not installed, the installer attempts to download the Microsoft .NET Framework 4.5 installation file and ask if you want to install Microsoft .NET Framework 4.5.

If you run the ad hoc report installer on Windows 2012 and Microsoft .NET framework 4.0 or 4.5 is not installed, the installer displays a message indicating what is missing and then aborts.

If the server meets all the software requirements, a Welcome screen displays.

To exit the installation process at any point, click **Cancel**.



2. Click **Next**.

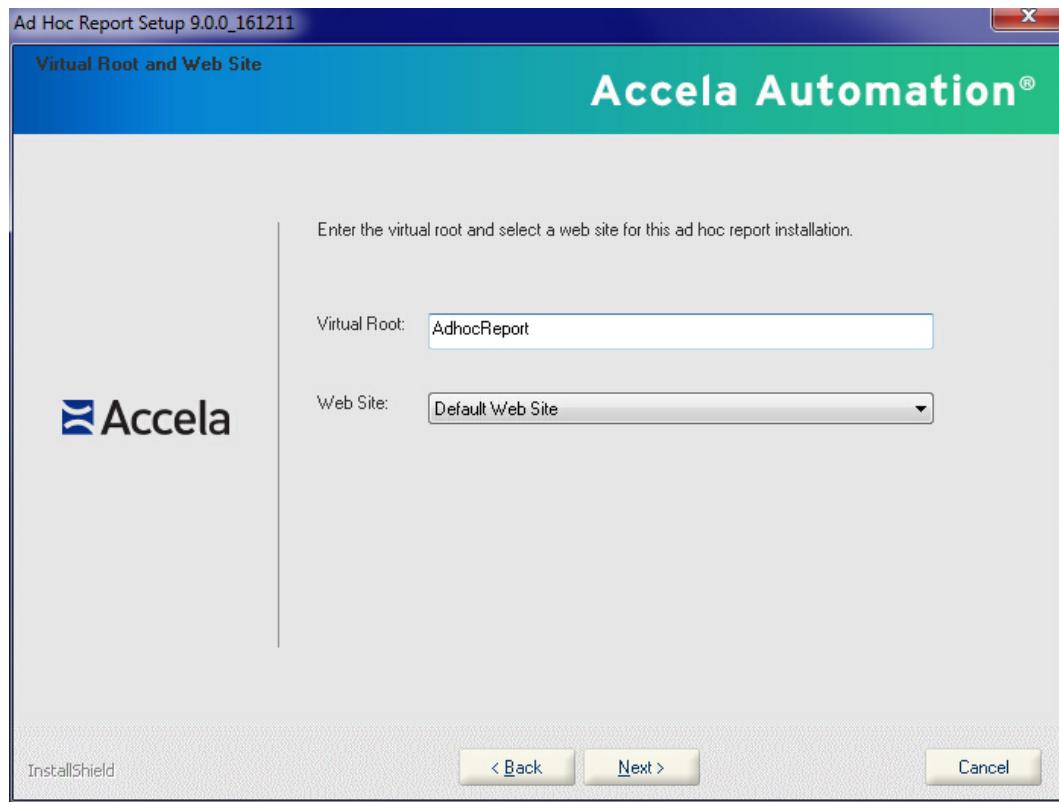
The License Agreement screen displays.

3. Read the license agreement. Use the **Print** button to print the terms of the license agreement, if desired.
4. Click "I accept the terms of the license agreement" to continue.

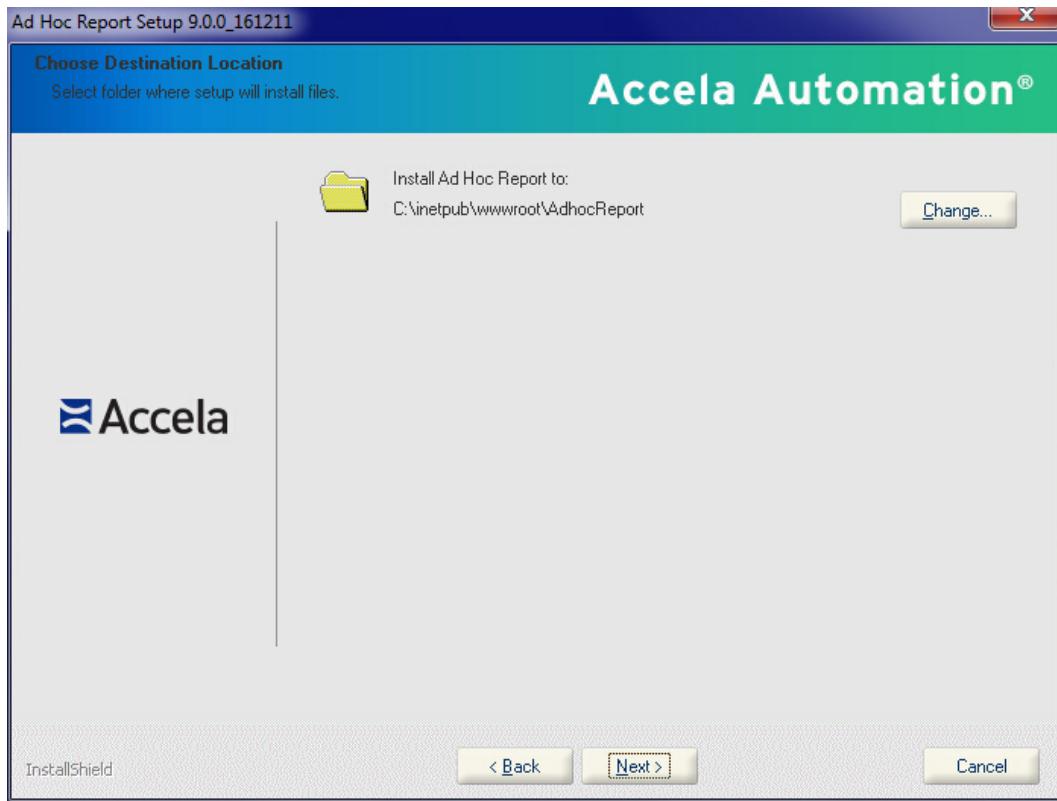
**Note:**

If you do not accept the terms of the license agreement, you are not permitted to continue with the installation.

The Virtual Root and Web Site screen displays.



5. Enter the virtual root and select the website for your ad hoc report application. Click **Next**.
The Choose Destination Location screen displays.



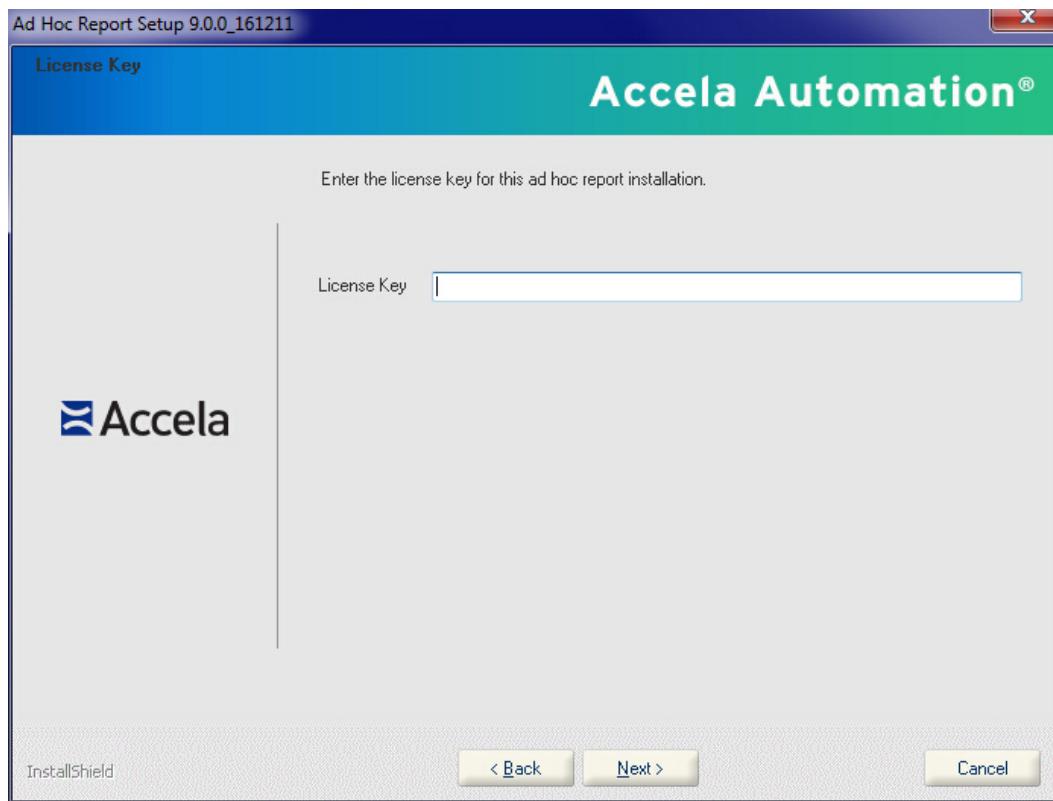
6. To accept the provided installation location

- Click **Next**.

To change the installation location

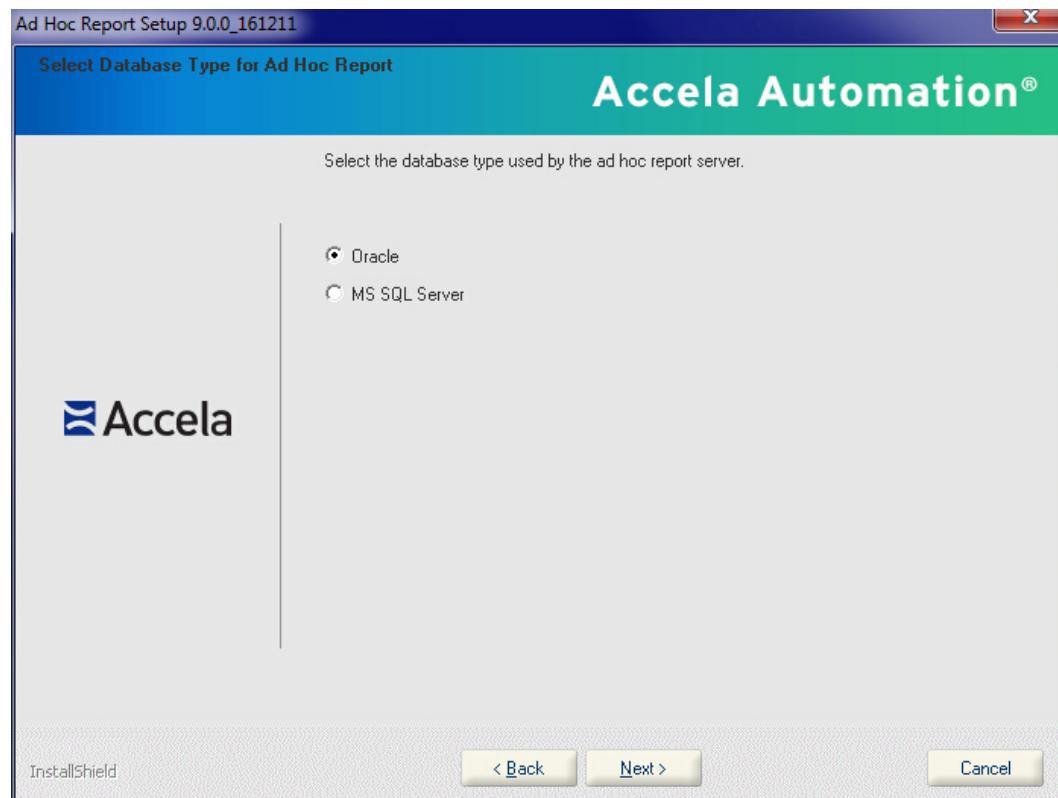
- a. Click **Change....**
- b. Locate and select the destination folder you want to use for the installation.
- c. Click **Next**.

The Enter License Key screen displays.



7. Enter the license key you obtained from Accela Customer Support. Click **Next**.

The Select Database Type for Ad Hoc Report screen displays.



8. Select the database server type, and click **Next**.

The Set up Oracle (or MS SQL) Server Database screen displays.

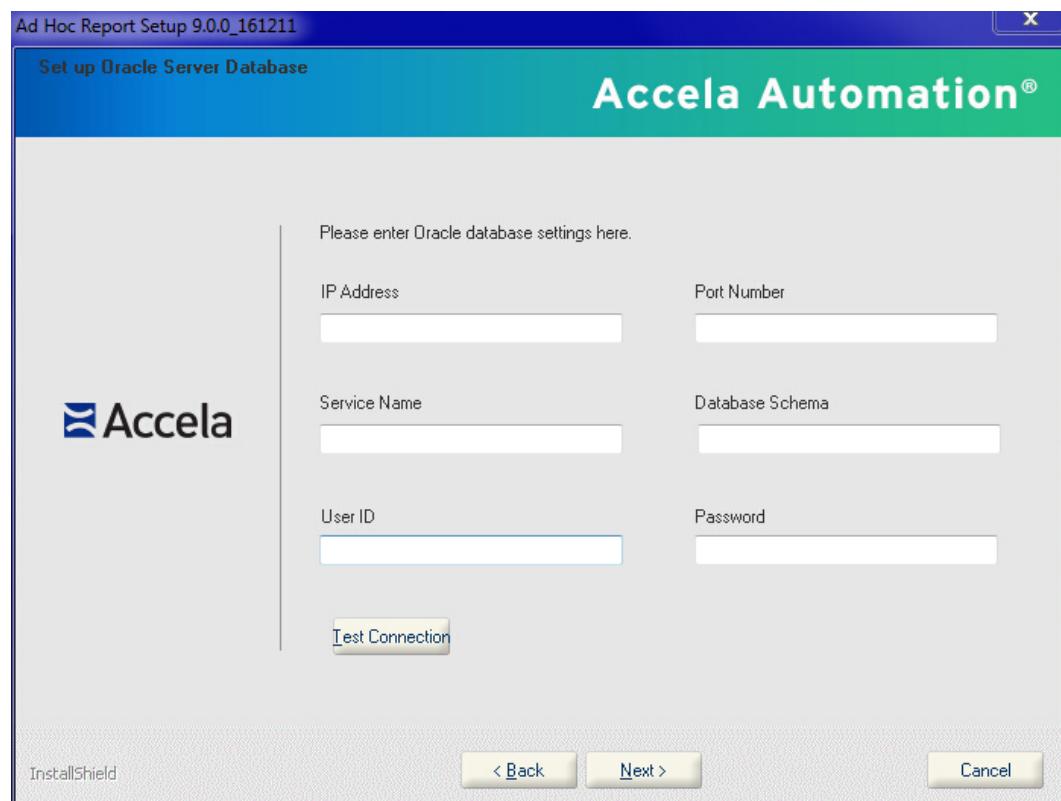


Figure 12: The Set up Oracle Server Database screen

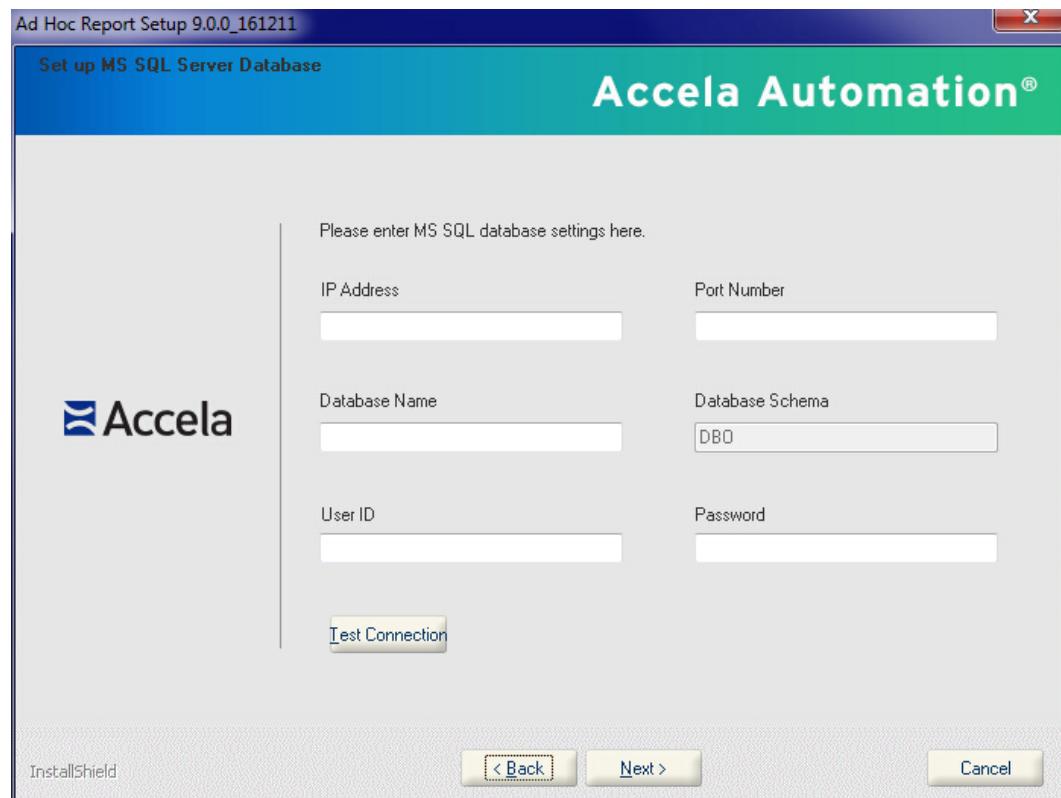
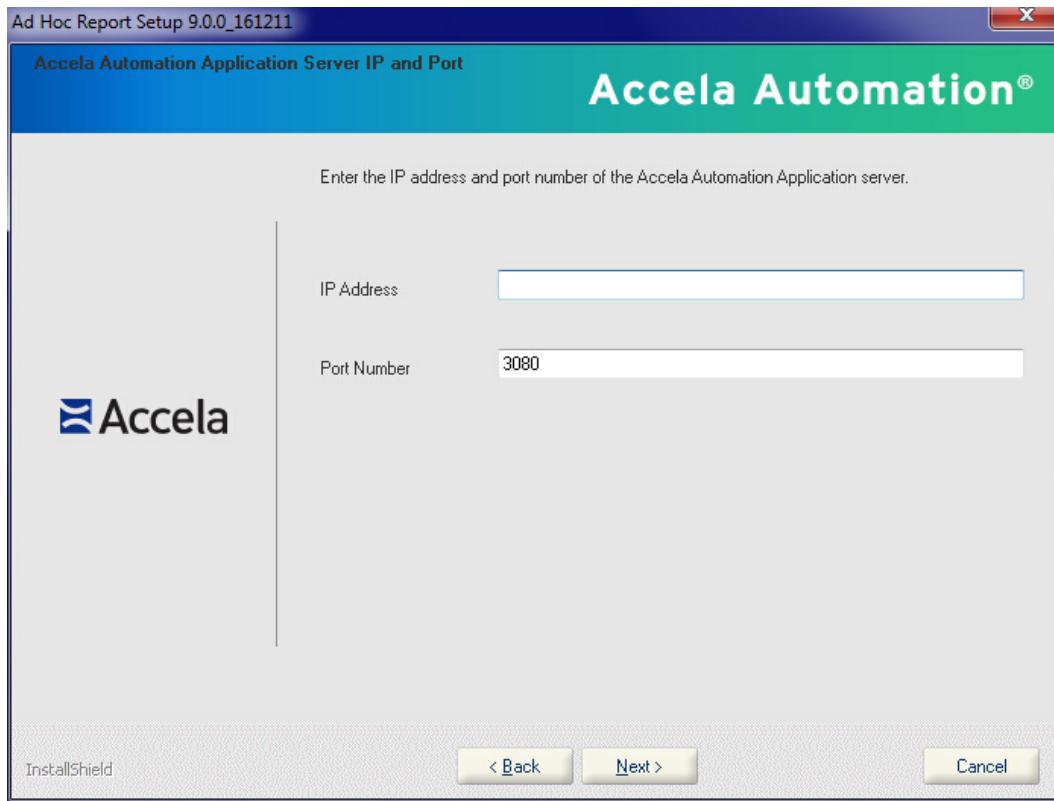


Figure 13: The Set up MS SQL Server Database screen

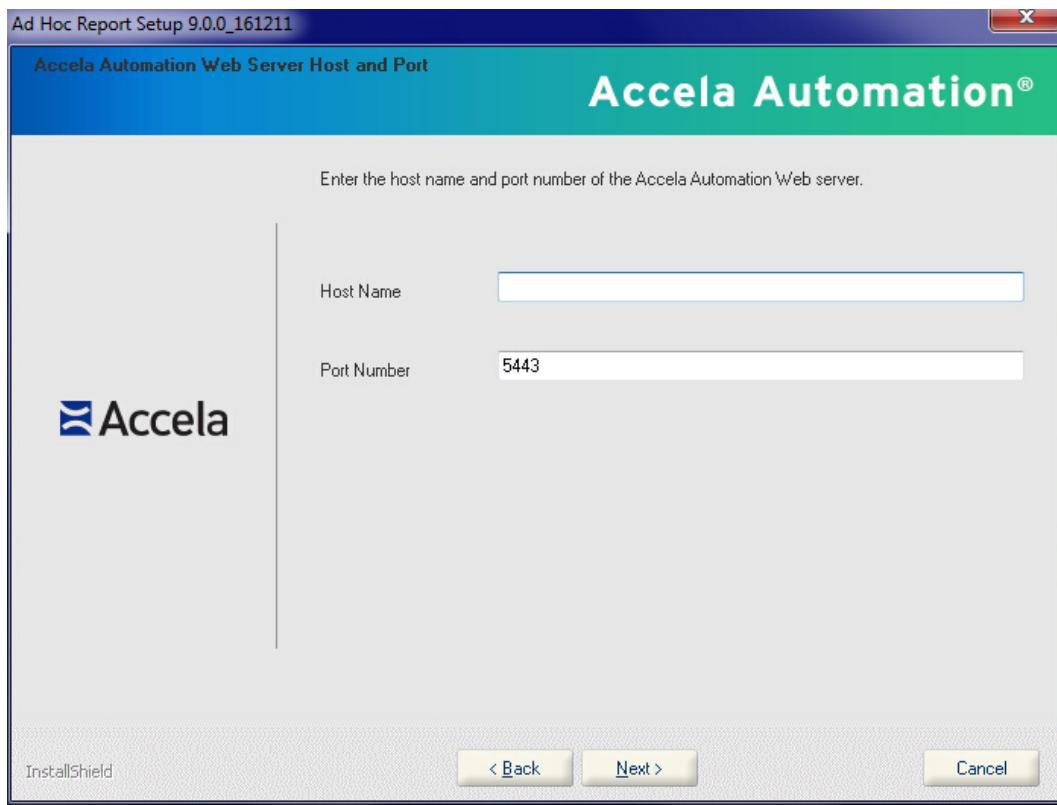
9. Enter parameter values for the Oracle database server or the SQL Server database server, and click **Next**.

The Enter Civic Platform Application Server IP and Port screen displays.



10. Enter the Civic Platform application server IP and port information. Click **Next**.

The Enter Civic Platform Web Server Host and Port screen displays.



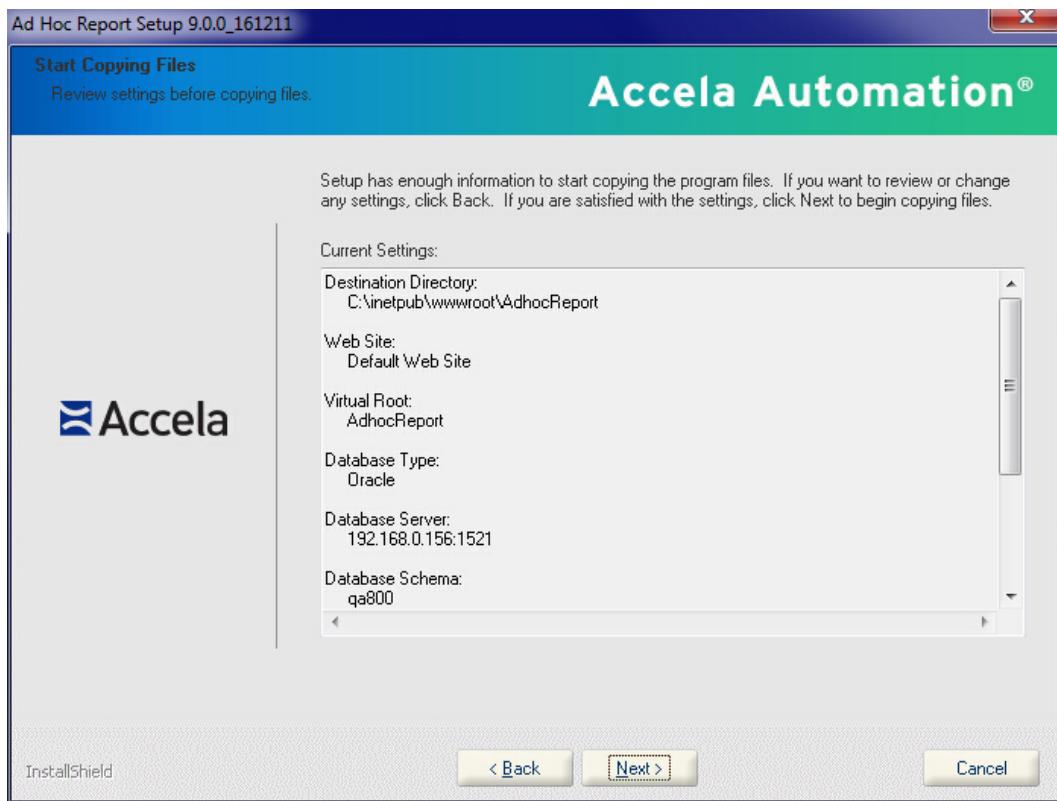
11. Enter the Civic Platform web server host and web server port information. Click **Next**.



Note:

You must enter the domain name of the web server in the Host Name field.

The Start Copying Files screen displays.



12. Click **Next**.

The Setup Status screen displays. A progress bar displays to give you a visual indicator of where the installer is in the process. When the installation is complete, the InstallShield Wizard Complete window displays, indicating that installation is successful.

13. Click **Finish** to complete the installation.

A popup dialog displays with the **InstallerInfo** file content.

14. Follow the instruction in the popup dialog to add the ad hoc report URL as a Standard Choice in the super agency website.

Configuring the Ad Hoc Reporting Service

The following sections provide details on additional setup and configuration for Accela ad hoc reporting.

Topics

- [Adding the Ad Hoc Report Service URL](#)
- [Defining Data Sources](#)
- [Defining a Logo File](#)
- [Configuring Internet Explorer on Users' Workstations](#)

Adding the Ad Hoc Report Service URL

You must go to the super agency website and add the ad hoc report service URL in the Standard Choice ADHOC_REPORT_SETTINGS.

To add the ad hoc report service URL:

1. Open your super agency website, and navigate to Classic Admin Tools > Agency Profile > Standard Choices.
2. Add the Standard Choice using the following settings.

Standard Choice Name	ADHOC_REPORT_SETTINGS
Standard Choice Value	SERVER_URL
Value Desc	Follow the syntax below to build the ad hoc report service URL. Be sure to replace the host and virtual directory with the settings of the new ad hoc report application.

```
http://[host]/[virtual directory]/Report/
Index.aspx
```

For example:<http://aa.server.com/AdhocReportWeb/Report/Index.aspx>

The screenshot shows the 'Standard Choices Item - Edit' page. At the top, there's a navigation bar with 'User ID: ADMIN', 'Admin Tools', 'Daily', and 'ACCELA AUTOMATION®'. Below that is a sub-navigation bar with 'Agency Profile', 'User Profile', 'Property', and 'Help'. The main form area has a title 'Standard Choices Item - Edit' and a subtitle 'Use this form to set up a Standard Choices Item.' It contains fields for 'Standard Choices Item Name' (set to 'ADHOC_REPORT_SETTINGS'), 'Description' (a large text input field), 'Status' (radio buttons for 'Enable' and 'Disable' with 'Enable' selected), and 'Type' (radio buttons for 'System Switch', 'Shared drop-down', 'EMSE', and 'Business Configuration' with 'System Switch' selected). At the bottom, there's a table with columns 'Standard Choices Value', 'Value Desc', and 'Active'. A row is shown with 'SERVER_URL' in the first column, 'http://aa.server.com/AdhocReportWeb/Report/Index.aspx' in the second, and a checked checkbox in the third. Below the table are buttons for 'Update', 'Add', and 'Cancel'.

Defining Data Sources

You need to go to Civic Platform to define data sources for ad hoc reports, and set permissions on ad hoc report data sources.

- By default, the installer installs the standard Civic Platform database views into the database and all views are available for ad hoc reports. If your agency uses Standard Choice ADHOC_REPORT_DB_VIEW to configure additional DB views at a super admin level, Civic Platform appends those database views to the list of standard views and makes the all views available to all agencies. If an agency uses Standard Choice ADHOC_REPORT_DB_VIEW to configure additional DB views at an agency level, only that agency's users have access to the DB views added. Agency-level DB views are in addition to the default DB views and any appended DB views at a super admin level.
- Open Report Manager (**Settings > Ad hoc Data Sources**) and assign permissions either by user group or by module for each data source. See "Setting Permissions on Ad Hoc Report Data Sources" in the Report Manager chapter of the *Accela Civic Platform Administrator Guide*.

Defining a Logo File

You can define a logo file for use in ad hoc reports.

- Add a new Standard Choice Value, AGENCY_LOGO, to the Standard Choice LOGO_TYPE_CATEGORY. See the Standard Choices Reference chapter of the *Accela Civic Platform Configuration Reference*.
- Add the desired logo file using logo type = AGENCY_LOGO. See the “Applying a Logo to Ad Hoc Reports” section in the Logos chapter of the *Accela Civic Platform Administrator Guide*.

Configuring Internet Explorer on Users’ Workstations

Users must set the ad hoc report server IP address as a trusted site in the browser settings to prevent page loading errors. Consult your browser documentation for information about setting up trusted sites.

Deploying Ad Hoc Reports into Another Environment

If your agency wants to create ad hoc reports in a staging environment and then move them to a production environment for use, follow the process described below. Note that the process assumes that you already created the ad hoc report before moving it. For information about creating an ad hoc report, see “Designing a New Report” in the Ad Hoc Reporting chapter of the *Accela Civic Platform User Guide*.



Note:

To deploy ad hoc reports from one environment to another, you must use a 3rd party database application to access to both the source database and the target database. Civic Platform does not provide the ability to work with databases.

1. Use a database application such as MS-SQL or Oracle, to access the source database.
 - In the RADHOC_REPORTS table, locate the XML for the ad hoc report you are migrating to production and copy the XML contents for the report.
2. Access the target database.
 - Add a new row to the RADHOC_REPORTS table, and enter a group and name for the report.
 - Paste the XML contents you copied from the source database into the target database.
 - Locate and change the serv_prov_code in this table (serv_prov_code=TENANTID) so it shows the *current agency serv_prov_code*.
3. Open Civic Platform and navigate to Report Manager.
 - Set permissions as needed for the DB_views used in the report you just moved.
 - If you want to associate a report with a portlet or report list for users to access by clicking a button, add the report in Report Manager, associate it with the portlet or report list portlet, and set appropriate permissions.

For more information, see the Report Manager chapter of the *Accela Civic Platform Administrator Guide*.

Installing Oracle 11g OCI Driver Configuration Tool

If your database server is Oracle 11g, the Civic Platform servers use the default JDBC thin driver for connecting with the database. If you want to switch to the JDBC OCI driver, you need to install the Oracle OCI driver configuration tool on all the Civic Platform server instances (except for the database server), which can be:

- Civic Platform web server
- ColdFusion MX web server
- Civic Platform Application server
- Index server
- Accela Report Writer (ARW) server
- Accela Document Services (ADS) server



Note:

The Oracle OCI driver only works with Civic Platform in Windows Server 2008 64bit and Windows Server 2008 R2 64bit.

Follow the instructions in this section on how to install, maintain, or remove the Oracle 11g OCI driver configuration tool in a Civic Platform server.

Related Information

[Running the Oracle OCI Driver Configuration Tool Installer](#)

[Modifying an Oracle OCI Driver Configuration Tool Installation](#)

[Removing an OCI Driver](#)

Running the Oracle OCI Driver Configuration Tool Installer

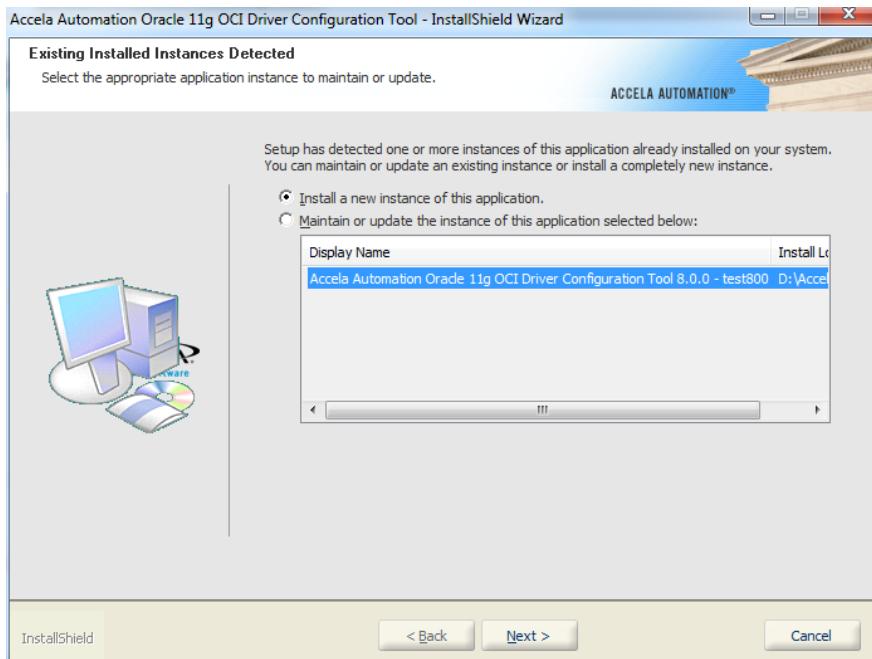


Note:

The Oracle OCI driver configuration tool installer can back up and maintain the modifications that you made to the server configuration files with the Oracle thin driver.

To run the Oracle OCI driver configuration tool installer:

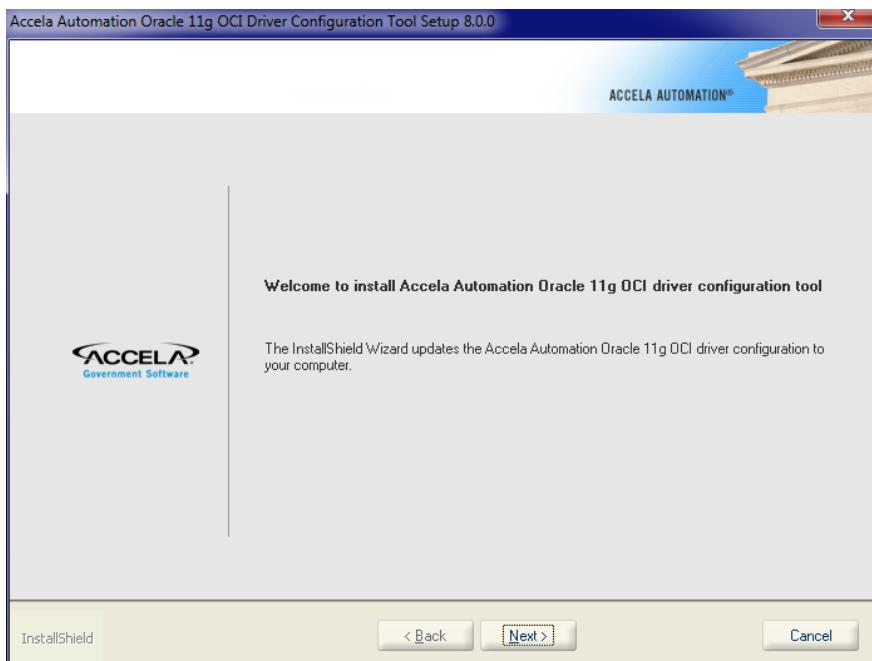
1. Locate and double-click AA_OCI_Driver_Tool_9.0.0.exe to launch the installation wizard.
2. Only if the InstallShield Wizard detects that the Oracle 11g OCI driver configuration tool instance exists, the Existing Installed Instances Detected screen displays.
The Existing Installed Instances Detected screen provides two options for you to either create a new instance or maintain the existing instance.



To exit the installation process at any point, click the **Cancel** button.

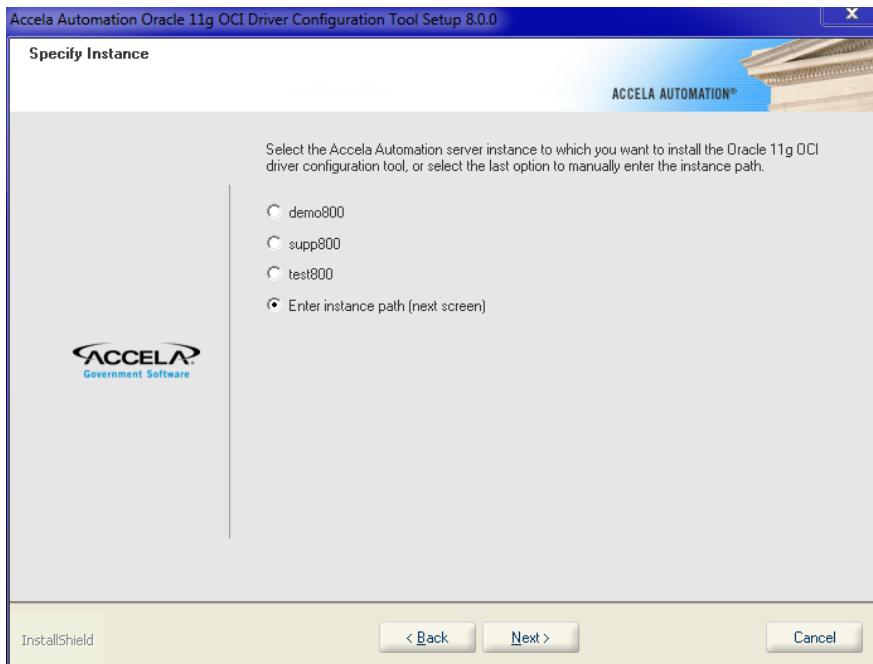
3. Select the option “To install a new instance of this application.”

The Welcome screen displays.



4. Click **Next**.

The Specify Instance screen displays, with all the Civic Platform server instances that the InstallShield Wizard detects.



5. Select the server instance to which you want to install the Oracle OCI driver configuration tool.



Note:

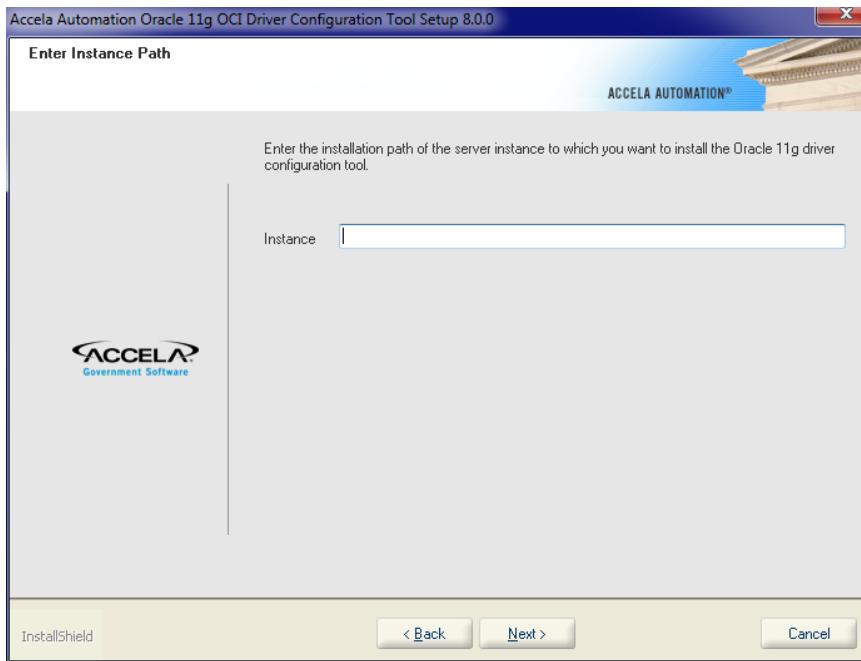
If you installed a Civic Platform server instance remotely from the current machine to another one (for example, computer B), you must go to computer B to install the OCI driver configuration tool on the server instance. Because computer B does not store the installation path of the server instance, you need to enter the path manually.

If you want to install the OCI driver configuration tool on a server instance which the Specify Instance screen does not list, take the following additional steps:

- a. Select the “Enter instance path (next screen)” option.**

- b. Click Next.**

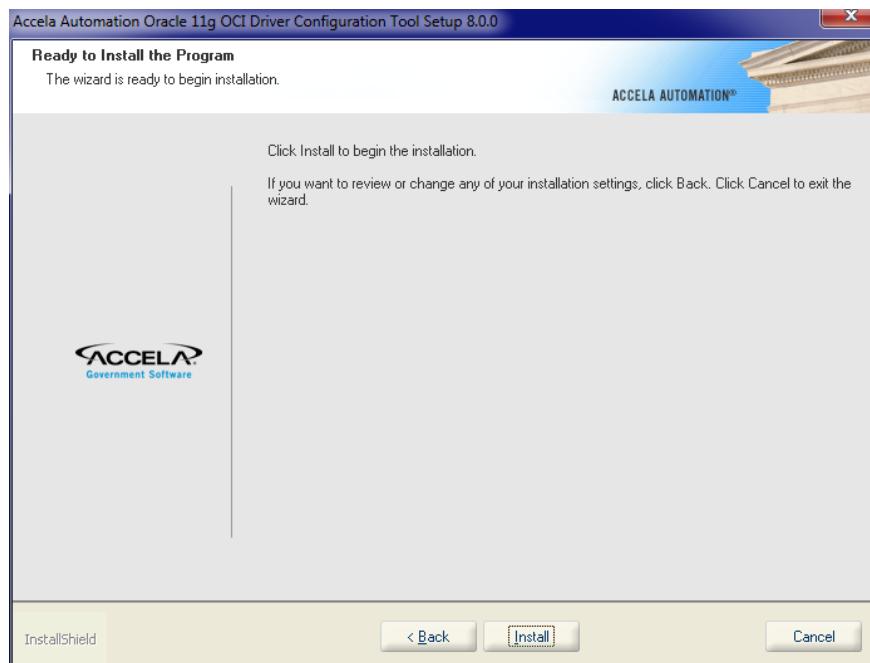
The Enter Instance Path screen displays.



- c. Enter the installation path of the server instance to which you want to install the OCI driver configuration tool.

6. Click Next.

The Ready to Install the Program screen displays.

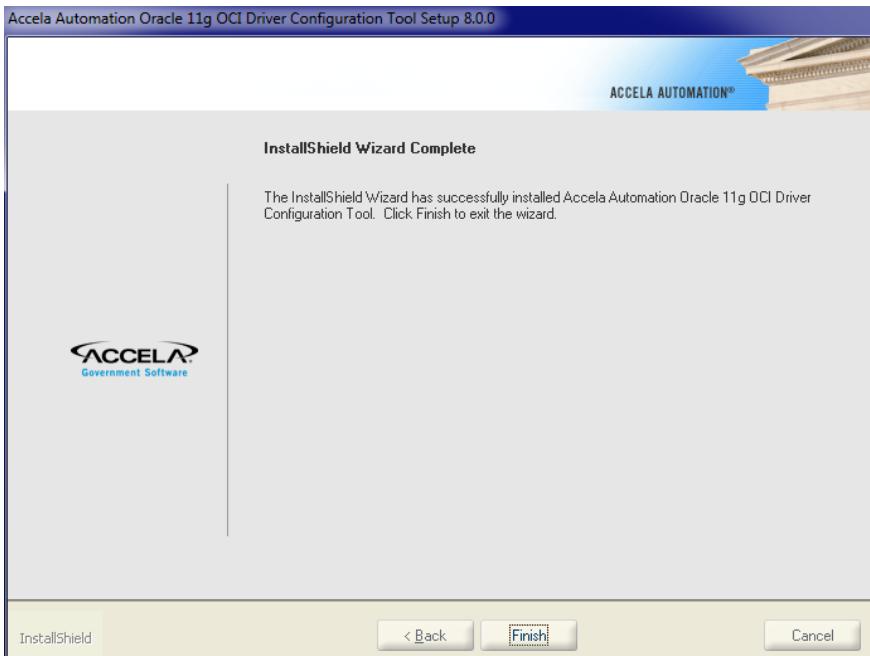


7. Click Install.

If some Civic Platform services are running, the installer stops the services, installs the OCI driver configuration tool, and then starts the services again when the installation is complete.



A progress bar displays to give you a visual indicator of where the installer is in the process. When the installation is complete, the InstallShield Wizard Complete window displays, indicating that installation is successful.

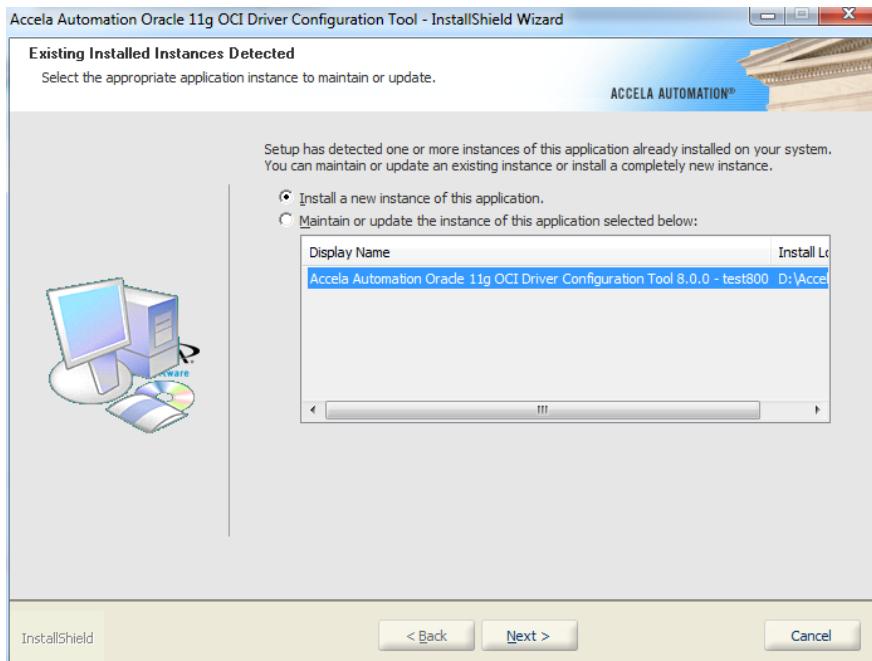


8. Click **Finish** to conclude the activity.

Modifying an Oracle OCI Driver Configuration Tool Installation

To modify or repair an existing installation:

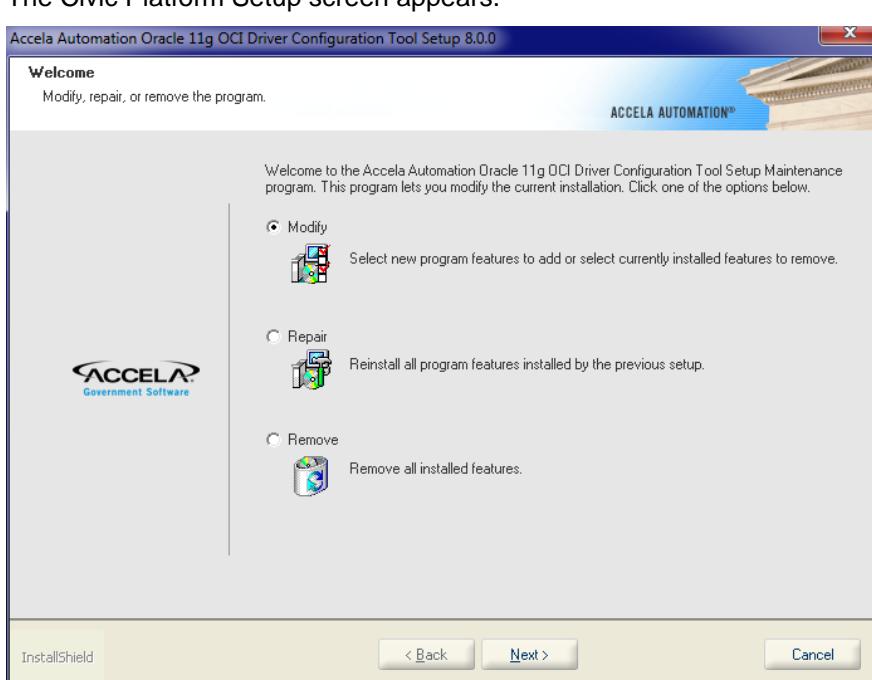
1. Launch the uninstall program from the Windows Add/Remove Program utility.
The Existing Installed Instances Detected screen displays.



2. Highlight the instance to maintain or repair and select the option to maintain or update the highlighted instance.

3. Click Next.

The Civic Platform Setup screen appears.



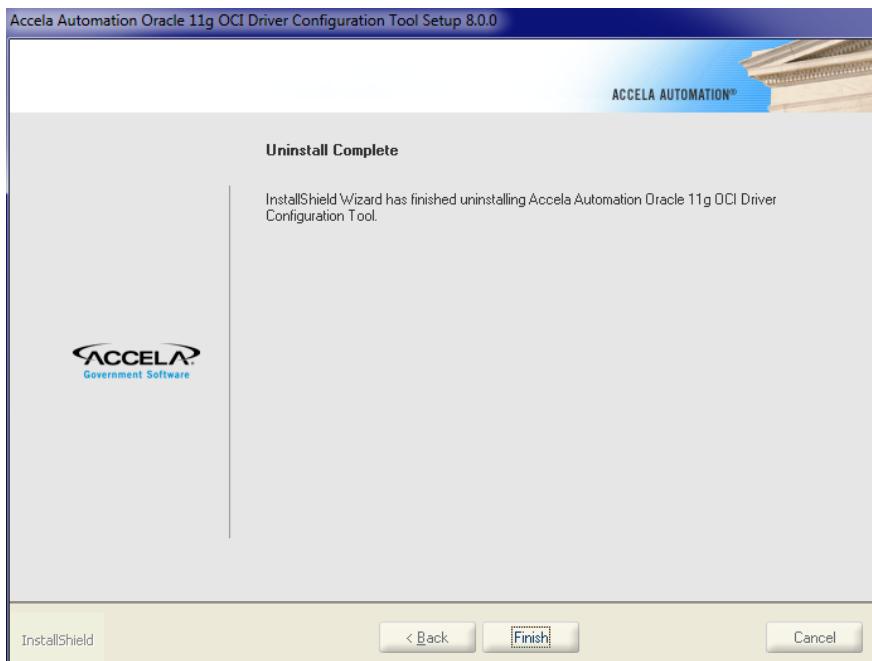
4. Select Modify or Repair.

5. Click Next.

If some Civic Platform services are running, the installer stops the services, re-installs the OCI driver file configuration tool, and then starts the services again after the installation is complete.



A progress bar displays to give you a visual indicator of where the installer is in the process. When the installation is complete, the Maintenance Complete window displays, indicating that the maintenance operation is successful.



6. Click **Finish** to conclude the activity.

Removing an OCI Driver

Use the Windows Add/Remove Programs utility to remove an OCI driver instance configuration tool.

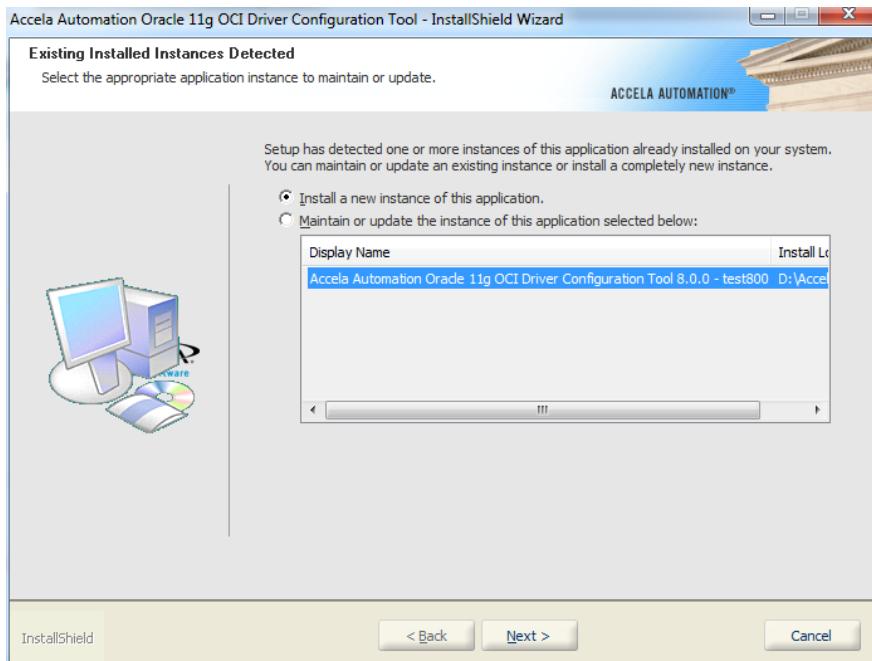


Note:

If you remove an OCI driver instance configuration tool, you lose the modifications that you made to the server configuration files with the Oracle OCI driver.

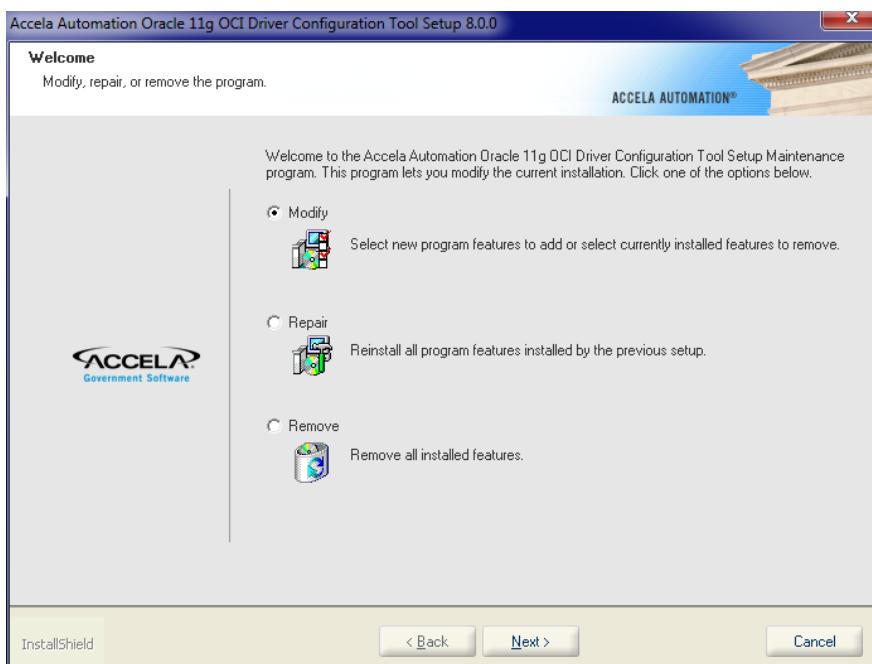
To remove an Oracle OCI driver configuration tool instance:

1. Launch the uninstall program from the Windows Add/Remove Program utility.
The Existing Installed Instances Detected screen displays.



2. Highlight the instance to remove and select the option to maintain or update the highlighted instance.
3. Click **Next**.

The Civic Platform Setup screen appears.



4. Select **Remove**.
5. Click **Next**.

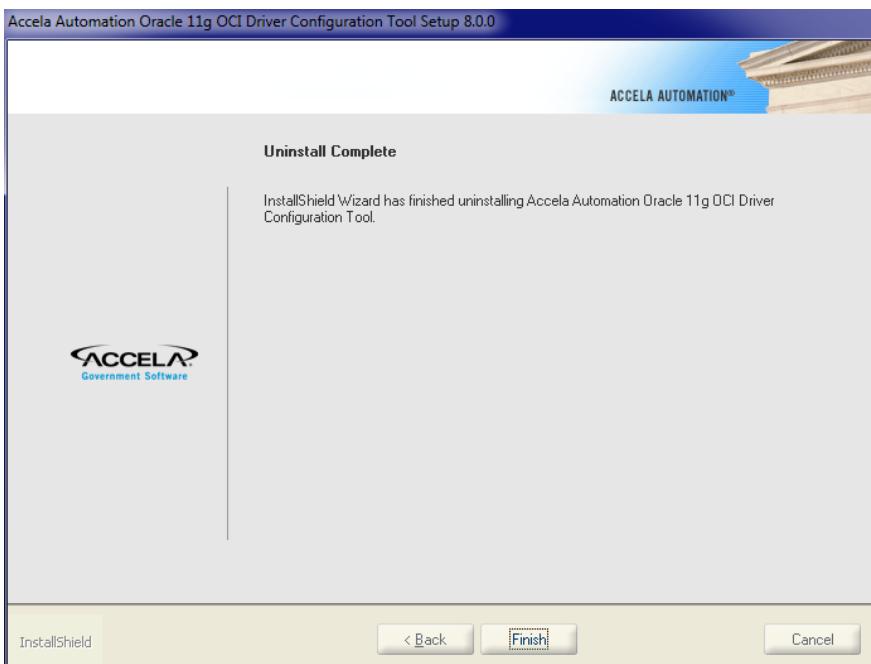
The Confirm Uninstall screen appears.



6. Click Yes.

A screen appears showing that the installer is removing files from the target system.

The Uninstall Complete screen appears.



7. Click Finish to complete the activity.

Upgrading the Database for Nearby Query Support

The Nearby Query functionality enables users to search for records, inspections, and asset condition assessments within maps, within one or more selected GIS features, or near one or more selected GIS features from the legacy Accela GIS map viewer. To enable the Nearby Query functionality, you must run the Nearby Query installer to upgrade the Civic Platform database with new geometry information columns.

After the upgrade, you must complete additional configuration. For more information about the configuration, see “Configuring Global Variable Settings” in the Configuring Agency Settings chapter of the *Accela Civic Platform GIS Administrator Guide*.

Related Information

[Nearby Query Prerequisites](#)

[Running the Nearby Query Installer](#)

Nearby Query Prerequisites

The following are the prerequisites to running the Nearby Query installer.

- The Civic Platform database type is MS SQL Server or Oracle Database 11g.
If your agency uses Oracle Database 11g, ensure you have done all of the following before running the Nearby Query installer.
 - Install the Oracle Locator feature on the database server.
 - Apply the following patches to the database:
p6880880_112000_{\$PLATFORM}.zip
p13901133_112030_{\$PLATFORM}.zip



Note:

If your agency uses Oracle Database 10g, the Nearby Query functionality is not supported, so you do not need to run the Nearby Query installer.

- The machine that you run the Nearby Query installer can connect to the Civic Platform database.
- You have upgraded the Civic Platform database to the latest version.

If your agency has multiple databases, you must run the Nearby Query installer for each database.

Running the Nearby Query Installer

To run the Nearby Query installer:

1. Download the installer to the host from which you want to run the installation. The installer file name is *AA_Enable_Nearby_Query_9.0.0.exe*.
2. Run the installer.
3. Click **Next** on the Welcome screen.

4. Read and accept the license agreement, and then click **Next**.
5. Select the directory to copy the database update files to, and then click **Next**.
The default is C:\Accela\730NearbySearchDbUpdate.
6. Select the database type you are using (Oracle or MS SQL Server).
7. Click **Yes** or **No** to dismiss the confirm message “Are you upgrading a Multilingual database?”
8. Follow the appropriate steps for your setup:

- If you select Oracle, complete the following information and click **Next**:

User	Enter the name of the Oracle user with privileges to do database updates.
Password	Enter the password of the Oracle user.
TNS Name	Enter the TNS name for the database that you want to upgrade.

- If you select MS SQL Server, do the following:

1. Enter the DB Server information in any of the following formats, and then click **Next**.

IP,Port
 ServerName,Port
 IP\DBInstanceName
 ServerName\DBInstanceName
 ServerIP\DBInstanceName, Port
 ServerName\DBInstanceName, Port

2. Enter the following information to connect to the database, and then click **Next**.

User	Enter the name of the MS SQL user with privileges to do database updates.
Password	Enter the password of the MS SQL user.
TNS Name	Enter the name for the database that you want to upgrade.

9. Click **Install** to copy the files to your host or click **Back** to review your previous settings.

10. Do any of the following.

- Mark the **Run DB Update Scripts** check box and click **Finish**.

The Nearby Query installer runs the DB upgrade script against the specified database.

- Clear the **Run DB Update Scripts** check box and click **Finish**.

After you complete the upgrade, you must locate the desired DB upgrade script and run the script manually.



Note:

You can remove the Nearby Query installation. However, this only removes the SQL script files extracted to your local host. Remove mode does not roll back changes made to the database.

Setting Up Civic Platform Clients

You need to perform additional installation procedures for optional clients.

Related Information

[Browser Settings](#)

[AEDR Installation and Configuration](#)

[Accela Document Scan Installation](#)

[Setting Up a Cashier Station](#)

[Configuring a Barcode Scanner](#)

Browser Settings

Users access Civic Platform through a web browser. Some Civic Platform functions use Microsoft ActiveX controls within a web browser. If users do not set the browser security settings properly, then numerous pop-up windows display.

This chapter provides you instructions to change web browser settings, with which you can better manage and minimize pop-up windows. You must set security for each computer's web browser that accesses Civic Platform.

For a list of browsers that Civic Platform supports, refer to the "Supported Environment" chapter in the *Civic Platform Release Notes*.

You can modify several settings on your web browser that impact how Civic Platform runs.

Related Information

[Setting ActiveX Controls](#)

[Pop-up Blocker Settings](#)

[Language Settings](#)

[Trusted Sites and Zones Settings](#)

[Installing Security Certificates](#)

Setting ActiveX Controls

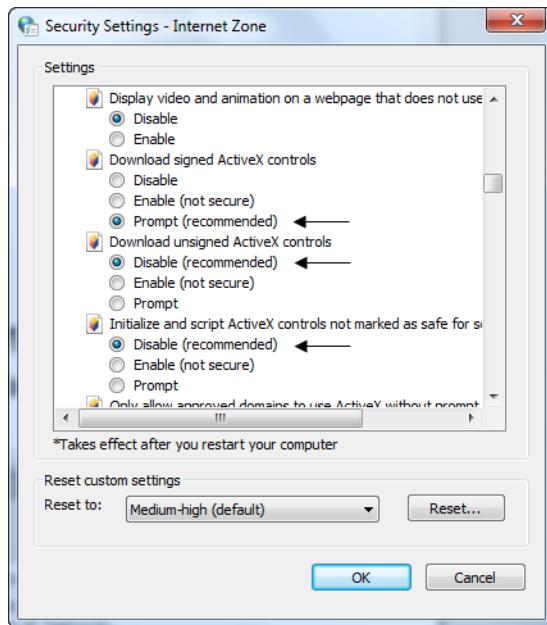
ActiveX is a set of controls that allow a user to interact with and run compatible applications through a browser. Some functions within Civic Platform use ActiveX controls to encapsulate certain functionality.

If you are not using the cashier module, then follow the steps in this section to disable ActiveX controls in your browser, and then restart your browser. If you are using the cashier module, see these steps, [ActiveX Control for Cashiering and Trust Accounts](#).

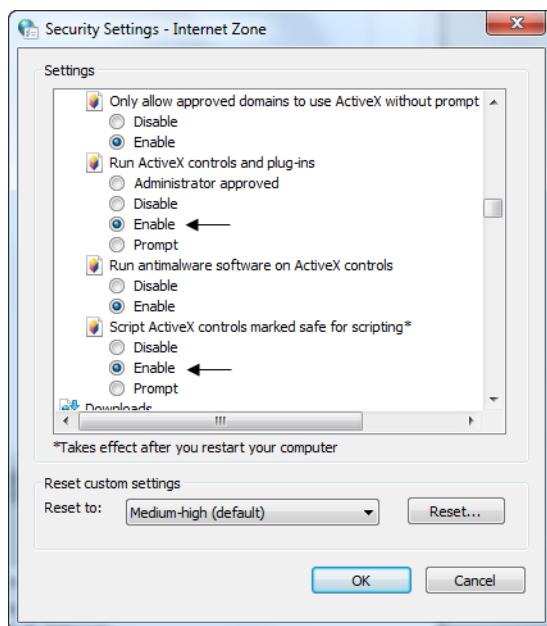
Also, if you are not using the cashier station, and persistent cashier session pop-up windows are displaying, then check to see whether you disabled the cash drawer function identifications (FIDs) as specified in [Cashier Station FIDs and Standard Choices](#). Only agency administrators have access to manage FIDs.

To modify IE security settings for ActiveX:

1. In the web browser, go to the **Tools** menu item and choose **Internet Options**.
2. Click the **Security** tab and click the **Custom** level button. Scroll to the ActiveX controls and plug-ins section.
 Security Settings - Internet Zone window displays.
3. Mark these options under the ActiveX controls and plug-ins section.
 - a. Download signed ActiveX controls, set to **Prompt**.
 - b. Download unsigned ActiveX controls, set to **Disable**.
 - c. Initialize and script ActiveX controls not marked as safe for scripting, set to **Disable**.



- d. Run ActiveX controls and plug-ins, set to **Enable**.
- e. Script ActiveX controls marked safe for scripting, set to **Enable**.



4. Click **OK** to save Security Settings, and restart your browser.
5. Restart your browser for the settings to take affect.
6. Optionally, continue with [Pop-up Blocker Settings](#).

Pop-up Blocker Settings

Pop-up Blocker is a browser feature that lets you limit or block most pop-ups. You can choose the level of blocking you prefer, from blocking all pop-up windows to allowing the pop-ups that you want to see.

If you enable Pop-up Blocker, you get a message saying "Pop-up blocked. To see this pop-up or additional options click here." To minimize the number of pop-ups, you can configure the settings by allowing only pop-ups from the Civic Platform web server.

To set your pop-up blocker settings for your agency's av.web server:

1. In the web browser, go to the **Tools** menu item and choose Pop-up Blocker > and click Pop-up Blocker Settings.

If applicable, click the Google toolbar pop-up blocker Icon to allow pop-ups from the Civic Platform website.

If applicable, click the Yahoo toolbar pop-up blocker Icon to allow pop-ups from the Civic Platform website.

2. In the web browser, go to the **Tools** menu item and choose Pop-up Blocker > and click Pop-up Blocker Settings.

If this option is inactive, select Turn On Pop-up Blocker, and then choose Pop-up Blocker Settings. Pop up Blocker Settings window displays.

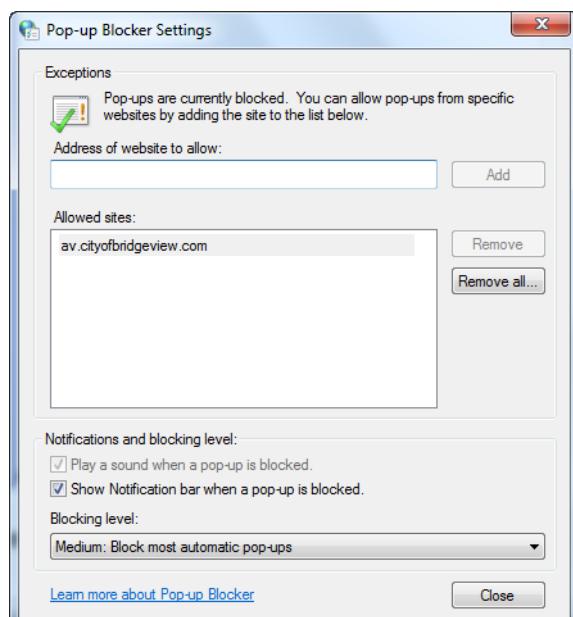
3. Enter your agency's av.web URL into the "Address of websites to allow." Include the https:// or http://. For example, https://av.cityofbridgeview.com.

You can use an asterisk to designate all sites in a particular domain. If you have other cityofbridgeview.com sites, such as http://av.test.cityofbridgeview.com and http://av.beta.cityofbridgeview.com, the browser considers that all the sites are in the secure zone.

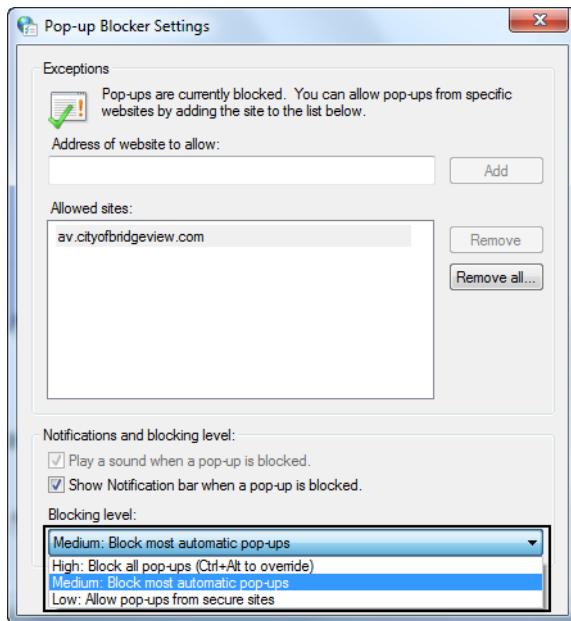
Sites that use secure forms use "https://" instead of "http://" You must add separately the "https://" variant of the URL. So, to cover all sites at cityofbridgeview.com for example, you must add two entries: http://*.cityofbridgeview.com and https://*.cityofbridgeview.com

4. Click the **Add** button.

The browser displays in the Allowed sites list.

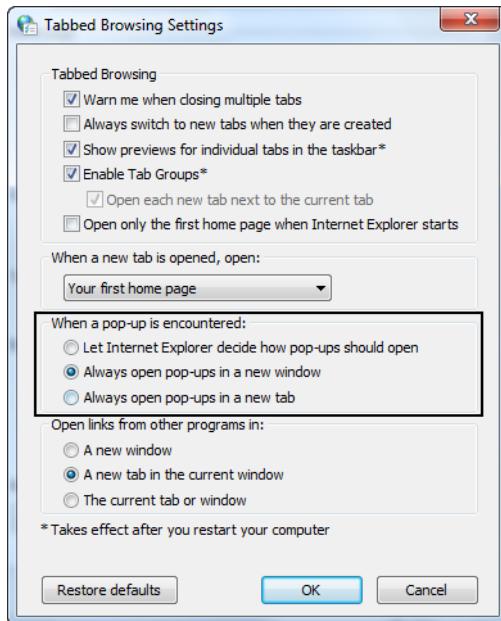


- Under Filter level, select the level to apply to the web browser. Depending on your needs, High: Block all pop-ups can be appropriate.



- Click the **Close** button.
- In the web browser, go to Tools > Internet Options > General tab, and in the Tabs area, click the **Settings** button.

The Tabbed Browser Settings window displays.



- Mark the **Always open pop-ups** in a new window option.
- Click **OK**.

Language Settings

Configure the language settings in Internet Explorer so that English is at the top of the list.

You can add multiple languages to Internet Explorer to display web page and Address bar text correctly. Keep in mind that if you installed languages in Internet Explorer, only those languages are available in websites and the address bar.

To add a language in the web browser:

1. In the web browser, go to the **Tools** menu item and choose **Internet Options**.

The Internet Options window displays.

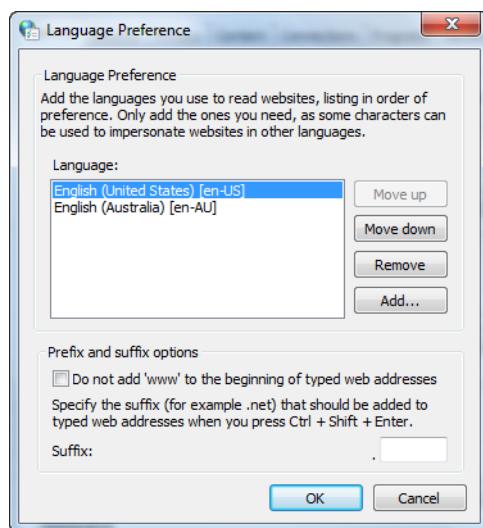
2. Click the **General** tab and click the **Languages** button.

The Language Preference window displays.

3. In the **Language Preference** dialog box, click the **Add** button.

4. In the **Add Language** dialog box, select **English (United States) [en-us]** from the list.

If more than one language exists in the list, place [en-US] as the first one. By default, the Internet Explorer language setting is the same as your operating system language.



5. Click **OK** until the Internet Options closes.

Trusted Sites and Zones Settings

This section explains how you can change browser pop-up settings so to manage and minimize pop-up windows. You must set the security for each computer's browser that accesses Civic Platform.

When using Civic Platform, and particularly using payments, there are two settings that affect the web browser: trusted sites and ActiveX controls. You must add your Civic Platform web server as a trusted site to prevent pop-up window, and also configure the security settings for ActiveX controls to manage the security settings (especially for your cash drawer). In addition, you need to managing the function identifications (FIDs) to ensure that the proper Civic Platform user group has appropriate privileges and limitations.

Set the FIDs for the cashier module correctly for the user group. For example, if you want to eliminate this type of pop-up message: "The cashier session has not been started." from displaying, you can disable FID 8251 Cashier Session for the user group that accesses a specific portlet.



Note:

If the user group does not use the cashier module, you can disable the related Cashier function identifications (FIDs), so "The cashier session has not been started." pop-up message does not display. Refer to [Cashier Station FIDs and Standard Choices](#).

If you set FIDs 8296 Cash Drawer and 8261 Open Cash Drawer to Full Access, then a security warning for opos.cab displays. You need to modify the security settings for Trusted Sites.

If the browser Information bar displays a security setting message, similar to the one shown in [Installing ActiveX Message](#), or in [Printer Add-on with ActiveX Message](#), you can follow both the trusted site and ActiveX control steps in this section to manage security settings for this message.

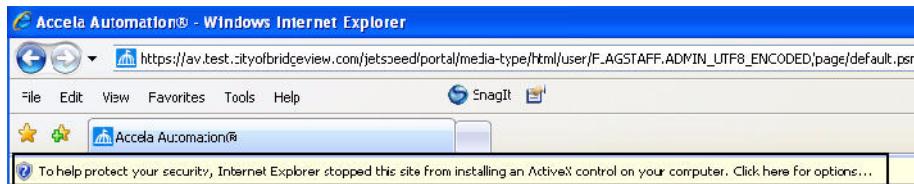


Figure 14: Installing ActiveX Message

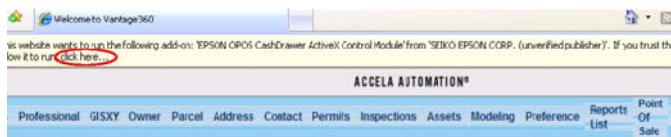


Figure 15: Printer Add-on with ActiveX Message

Topics

- [Accela Server Trusted Site for Cashiering and Trust Accounts](#)
- [ActiveX Control for Cashiering and Trust Accounts](#)

Accela Server Trusted Site for Cashiering and Trust Accounts

The steps in this section can help reduce pop-up windows, namely the opos.cab and printer.cab pop-up messages. Printing custom trust account receipts also require the steps below.

To prevent the security warning for opos.cab and printer.cab (see [opos.cab Unknown Publisher Security Window](#)), or to remove outdated certs when installing ActiveX controls, you must add your Civic Platform web server as a trusted site, and configure the security settings for [ActiveX Control for Cashiering and Trust Accounts](#).

Remember to configure ActiveX controls if you enabled the following FIDs:

- 8296 Cash Drawer
- 8261 Open Cash Drawer
- 8286 Fees Print Receipt Summary

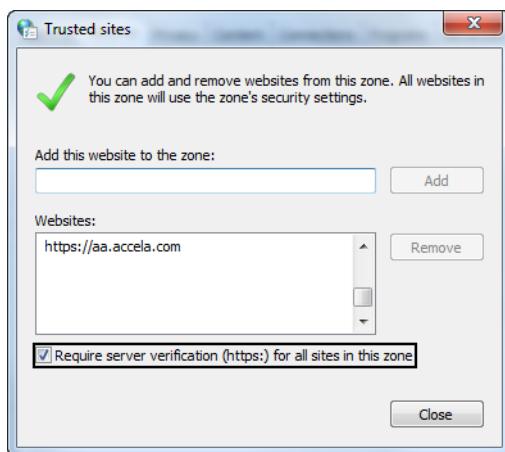
If you are in a portlet but you do not manage payments or do not use the cash drawer in that portlet, check the list of function identifications (FIDs) for cashier sessions and configure each one for the user group. For example, if you need to eliminate this pop-up message: "The cashier session has not been started." from displaying, you must disable FID 8251 Cashier Session for the user group that accesses a specific portlet. Refer to the list of cashier session FIDs in [Cashier Station FIDs and Standard Choices](#).



Figure 16: opos.cab Unknown Publisher Security Window

To set your av.web server and Classic Admin site as trusted sites:

1. In your browser, go to **Tools > Internet Options**.
The Internet Options window displays.
2. Go to the **Security** tab, click the Trusted Sites green check mark, and then click the **Sites** button.
The Trusted Sites window displays.
3. Enter your agency's av.web URL into the websites list. You need to add this server as a Trusted Site when managing payments. Consult with your agency administrator for the address.
4. Click **Add**.
5. Enter your agency's aa.web URL (the URL for your Classic Admin site) into the websites list. To enable detailed trust account receipts you must set your Classic Admin site as a trusted site, as trust account payments leverage Classic Admin functionality. Consult with your agency administrator for this URL.



6. Click **Add**.
7. Clear the check box for "Require server verification (https:) for all sites in this zone."
8. Click **Close** and then click **OK** to save these trusted sites.
9. Continue with the steps in [ActiveX Control for Cashiering and Trust Accounts](#).

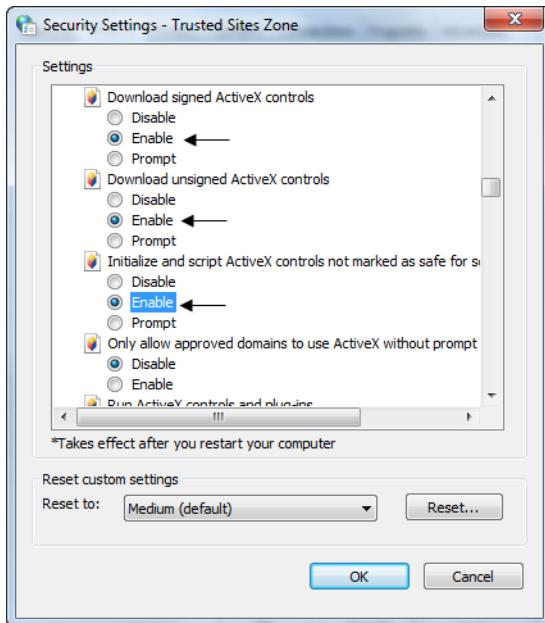
ActiveX Control for Cashiering and Trust Accounts

Follow these steps to manage the security settings of the ActiveX controls for the cash drawer functions and to enable detailed receipt summaries. You must restart your browser when you finish making these changes.

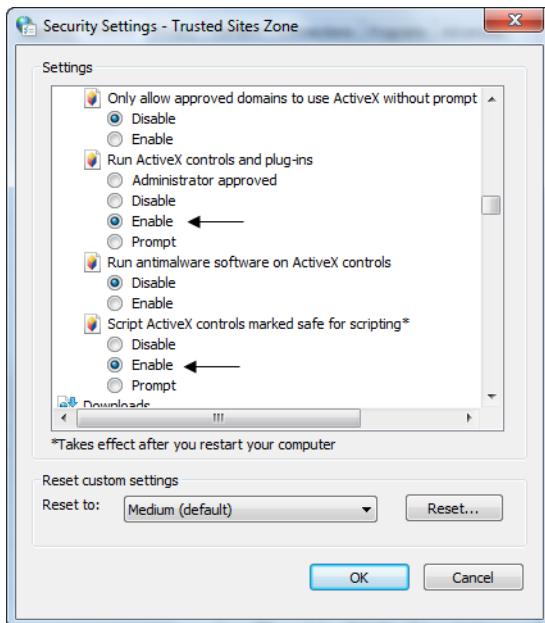
If you are not using the cashier module, then you can disable ActiveX controls in your browser by setting FID 8296 Cash Drawer and FID 8261 Open Cash Drawer to None. These two settings eliminate cashier session pop-up windows.

To modify IE security settings for ActiveX with the cashier module:

1. In the web browser, go to the **Tools** menu item and choose **Internet Options**.
The Internet Options window displays.
2. Click the **Security** tab and click Trusted sites, and click the **Custom Level** button.
The Security Settings - Trusted Sites Zone window displays.
3. Mark these options under the ActiveX controls and plug-ins section.
 - a. Download signed ActiveX controls, set to **Enable**.
 - b. Download unsigned ActiveX controls, set to **Enable**.
 - c. Initialize and script ActiveX controls not marked as safe for scripting, set to **Enable**.



- d. Run ActiveX controls and plug-ins, set to **Enable**.
- e. Script ActiveX controls marked safe for scripting, set to **Enable**.



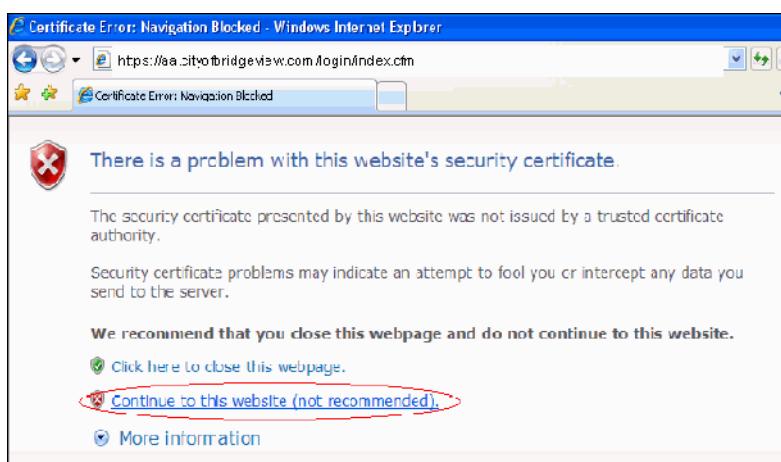
4. Click **OK** to save these Security Settings, and click **OK** to close the Internet Options window.
5. Restart your browser. For these settings to take effect you must restart your browser.

Installing Security Certificates

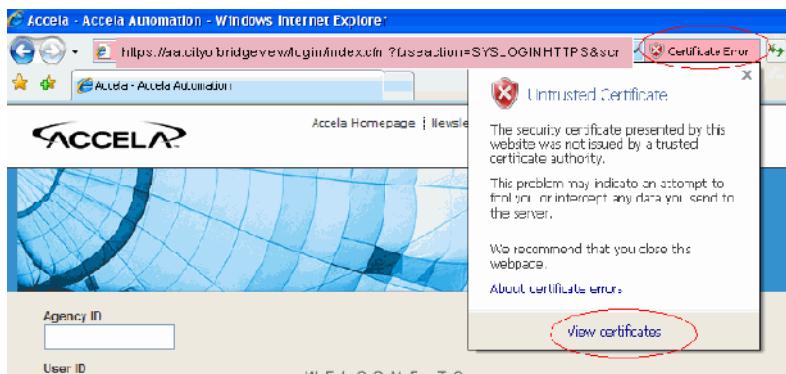
In Civic Platform you must install security certificates. After the installation, the certificate error does not block browser navigation, so that you can easily access Civic Platform.

To install a secure certificate:

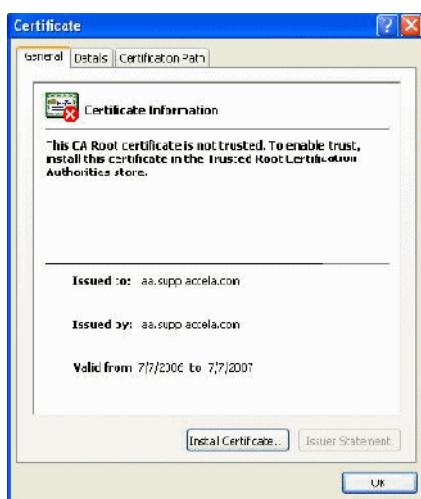
1. Access the Civic Platform address. Your agency administrator provides this URL Address.
Certificate Error - Navigation blocked page displays.



2. Click **Continue to this website** (not recommended).
3. Click the **Certificate Error** button, and then click **View Certificates**.



4. Click the **Install Certificate** button in the **General** tab of the **Certificate** window. After the secure certificate installation completes, click **OK**.



5. Close this browser session. Start a new browser session and log in to Civic Platform. Because you installed the security certificate, the problem should not persist. To eliminate other pop-ups, consider changing your [Pop-up Blocker Settings](#).

AEDR Installation and Configuration

Follow the instructions in this chapter to install and configure Accela Electronic Document Review (AEDR).

 **Note:** The [AEDR Installation and Usage Guide](#) is available on Community. Although it was originally published in 7.2.2, this doc is still highly relevant and useful.

Related Information

[Required Software and Configuration](#)

[Installing the Accela Electronic Document Review \(AEDR\) Client](#)

[Installing the ComparA Client](#)

[Configuring Adobe Acrobat](#)

[Migrating Document Comments from Version 7.1.0](#)

Required Software and Configuration

- Accela Electronic Document Review (AEDR) client, available on Accela's FTP site
- ComparA, a third-party side-by-side comparison tool, available on Accela's FTP site
- Silverlight version 5 or higher
- Adobe Acrobat X Pro
 - Purchase a license or try for free: <http://www.adobe.com/downloads/>.
- .Net Framework 4.0 or 4.5.
- • Download .Net Framework 4.0: <http://www.microsoft.com/downloads/en/details.aspx?FamilyID=e5ad0459-cbcc-4b4f-97b6-fb17111cf544>.
 - Download .Net Framework 4.5: <http://www.microsoft.com/en-us/download/details.aspx?id=30653>.
- Configure Civic Platform FIDs and Standard Choices. See "Electronic Document Review" in the *Civic Platform Configuration Reference*, available via the [Documentation Library](#) on Community.
- Configure Adobe Acrobat. See [Configuring Adobe Acrobat](#) .

Installing the Accela Electronic Document Review (AEDR) Client

Obtain the latest Accela Electronic Document Review installer and the Adobe Acrobat Configuration file (containing Accela-designed custom stamps and other custom tools) from the Accela FTP site. Make note of where you have stored the files.

If you are installing Accela Electronic Document Review on a Windows 7 operating system, contact your IT representative before proceeding to ensure that you have sufficient permissions to install applications on your machine.

Topics

- [Initial Installation](#)
- [Modifying an Installation](#)
- [Removing an EDR Installation](#)

Initial Installation

The Accela Electronic Document Review installation wizard walks you through the installation of Civic Platform Electronic Document Review for Adobe Acrobat Pro to your local machine. You can find an Accela Electronic Document Review Client installer, a proxy server setting tool, and an Acrobat Configuration Files installer that you can use to install Accela-built custom stamp and custom buttons.

Topics

- [Running the Electronic Document Review Client Installer](#)
- [Running the Acrobat Configuration Files Installer](#)
- [Configuring the Proxy Server \(Optional\)](#)



Note:

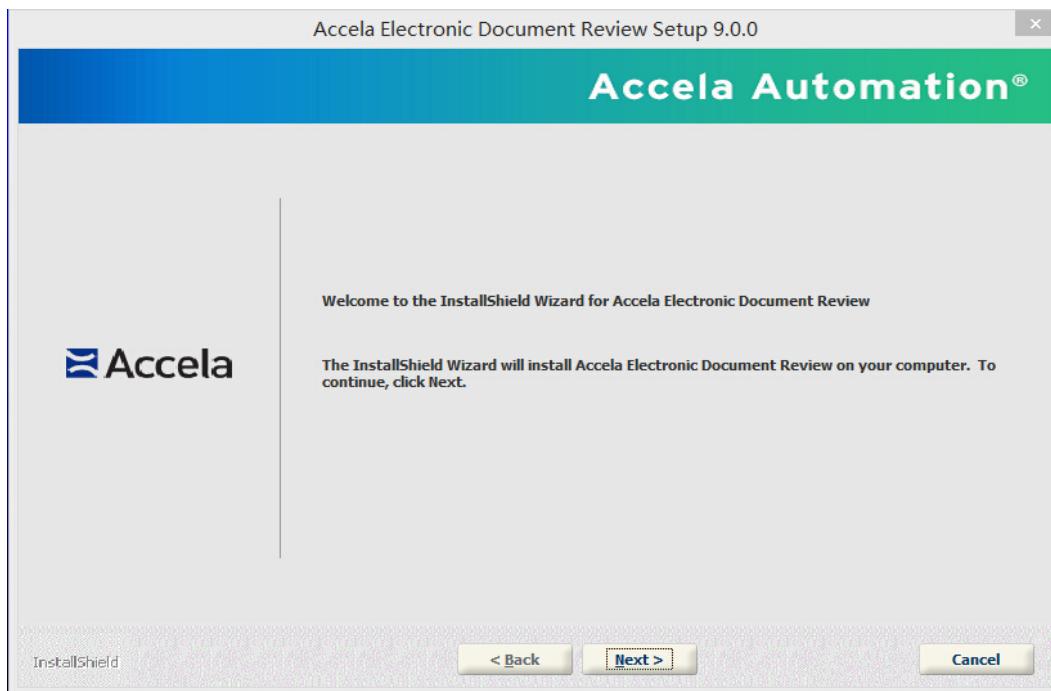
If you have an older version of Accela Electronic Document Review installed, uninstall it before proceeding. See [Removing an EDR Installation](#).

Running the Electronic Document Review Client Installer

To run the Accela Electronic Document Review Client Installer:

1. Locate and double-click *AEDR_Client_9.0.0.exe* to launch the installation wizard.

The installer checks whether you installed .Net Framework 4.0 or 4.5 Client Profile and Adobe Acrobat Pro software. If you did not install the software yet, the installer displays a message indicating what is missing and then aborts. Otherwise, a Welcome screen displays.



To exit the installation process at any point, click the **Cancel** button.

2. Click **Next.**

The License Agreement screen displays.

3. Read the license agreement. Use the **Print button to print the terms of the license agreement if you desire.**

4. Click “I accept the terms of the license agreement” to continue.



Note:

If you do not accept the terms of the license agreement, you are not permitted to continue with the installation.

The Installer Selection screen displays. You can choose to install the Accela Electronic Document Review Client, the Acrobat Configuration Files, or both.

5. Mark the check box for either or both options and click **Next.**

The Choose Destination Location screen displays.

6. To accept the provided installation location:

- Click **Next**.

To change the installation location:

- Click **Change....**
- Locate and select the destination folder you want to use for the installation.
- Click **Next**.



Note:

If your operating system is Windows 7 and you want to install the program to a non-default folder, make sure that you are the owner of the destination folder, and that you have ‘full control’ permissions for that folder. Check these settings by right clicking the destination folder name and selecting **Properties**.

If you are installing the Acrobat Configuration zip file, the “Choose an Acrobat Plug-in zip file” screen displays. See [Running the Acrobat Configuration Files Installer](#) for more information. If not, the “Ready to Install Program” screen displays. Skip to step 2 in [Running the Acrobat Configuration Files Installer](#).

Running the Acrobat Configuration Files Installer

To run the Acrobat Configuration Files Installer to install Accela-built custom stamp and custom buttons:

**Note:**

For the custom stamps/buttons installation, you must organize your files with a proper structure within the zip file, for the installation wizard to correctly read the files in the zip file.

The prescribed folder structure is as follows:

FOLDERNAME.zip\FOLDERNAME\Disciplines\...

For example, if you have a folder named AgencyStamps. The folder structure of this folder should be:

Agency Stamps

> Disciplines

> Parks and Rec> Fire> Zoning

The Parks and Rec, Fire, and Zoning folders contain the stamp files.

You can compress the Agency Stamps folder, and apply the folder name, Agency Stamps, to the zip file.

1. Mark the check box for each set of tools (categorized by discipline) that you want to install, then click **Next**.

The Ready to Install Program screen displays.

2. Click **Install**.

The Setup Status screen displays. When the installation is complete, the InstallShield Wizard Complete window displays, indicating that installation is successful.

3. Click **Finish**.

Configuring the Proxy Server (Optional)

If you access the Civic Platform server through a proxy server, you must perform necessary proxy server configuration with the provided proxy server setting tool, for the Accela Electronic Document Review feature to work successfully.

To configure the proxy server with the proxy server setting tool:

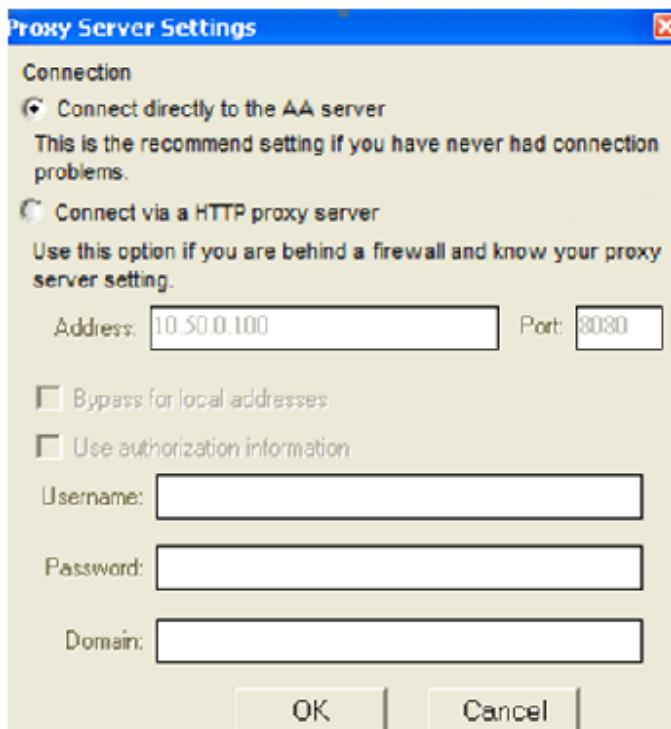
1. Locate and double-click the AccelaDocumentCollaboration.exe located under the \$INSTALL_HOME \Accela\DocReview folder, where \$INSTALL_HOME stands for the installation location of the Accela Electronic Document Review Client.

A program icon displays in the Windows system tray.



2. Right-click the AccelaDocumentCollaboration icon and select "Proxy Server Settings."

The Proxy Server Settings window displays.



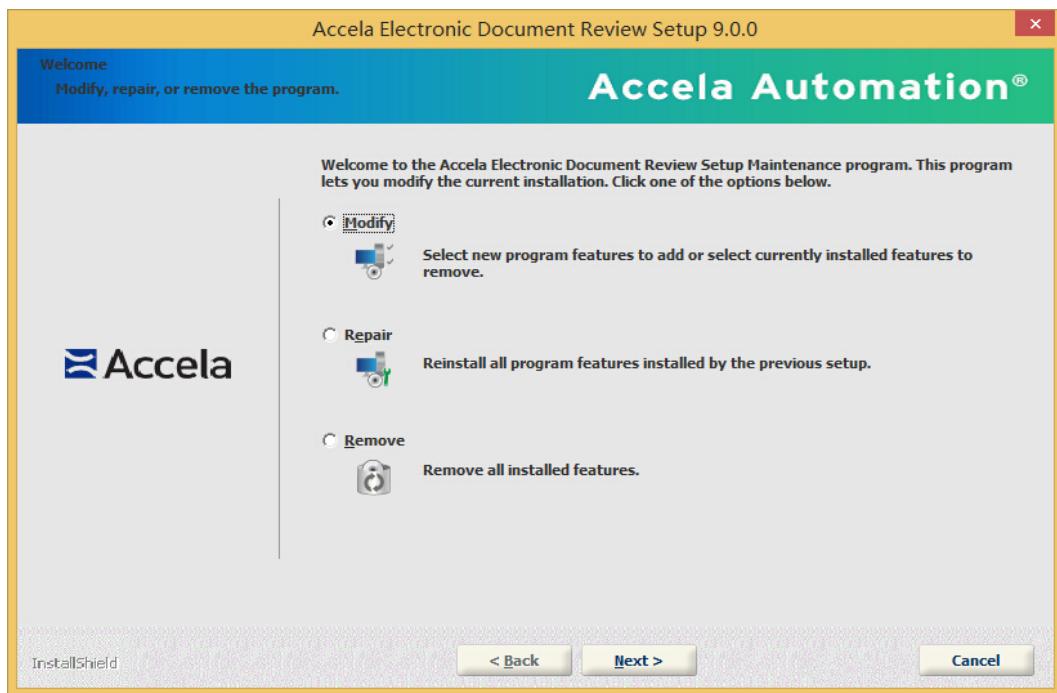
3. Select the connection option. If you select the “Connect via a HTTP proxy server” option, complete the fields as required.

Address and Port	Enter the IP address and port number of the proxy server.
Bypass for local addresses	Check this option if your local machine locates in the same local network as the Civic Platform server.
Use authorization information	Check this option if your proxy server requires a user authentication, and enter the authentication information in the Username, Password, and Domain.

Modifying an Installation

If you have already installed the current version of Accela Electronic Document Review client and/or Acrobat configuration files, and you need to add additional Acrobat configuration files, for example, you can run a modified installation. If you installed an older version, you must remove the existing Accela Electronic Document Review client, and then perform an initial installation using the current version.

1. Locate and double-click *AEDR_9.0.0_<build number>.exe* to launch the installation wizard. The Accela Electronic Document Review Setup Maintenance program launches, and the Welcome page displays.



2. Select **Modify and click **Next**.**

The Installer Selection window appears. If you leave a box unchecked, Accela uninstalls that option. If this is not what you want to do, be sure to mark both check boxes.

3. Select both options and click **Next (see note for prior step).**

The “Choose an Acrobat Plug-in zip (compressed) file to Install” window appears. If you previously installed an Acrobat Configuration zip file, it is pre-selected.

4. See the note about custom stamp zip file organization at the beginning of this section and make sure the zip file containing your custom stamps complies with the listed requirements.

5. Click **Browse to locate and select the zip file you want to use and click **Next**.**

The installer extracts the content from the Acrobat plug-in zip file. The Select Disciplines screen displays. The screen categorizes the Accela-designed buttons and other custom tools by discipline.

6. Mark the check box for each set of tools (categorized by discipline) that you want to install, then click **Next.**

The Ready to Install Program screen displays.

7. Click **Install.**

The Setup Status screen displays. When the installation is complete, the InstallShield Wizard Complete screen displays, indicating that installation is successful.

8. Click **Finish.**

Removing an EDR Installation

Make sure you close Adobe Acrobat and have backed up any custom stamp, button, or other Acrobat tool files that you want to keep before proceeding.

Following the steps in this section removes both the Accela Electronic Document Review Client and any Accela-designed custom stamps and custom buttons that you installed using this installer. The steps do not affect your own custom buttons and custom stamps as long as you used unique naming conventions.

1. Locate and double-click *AEDR_9.0.0_<build number>.exe* to launch the installation wizard.
The Accela Electronic Document Review Setup Maintenance program launches, and the Welcome page displays.
2. Select **Remove** to remove all installed features, then click **Next**.
You need to confirm that you want to completely remove all the installed features.
3. Click **Yes** to continue. Click **No** to exit.
The Setup Status screen displays. When the process is complete, the InstallShield Wizard Complete screen displays, indicating that you removed the application and all components (including all Accela-designed custom stamps and custom tools).
4. Click **Finish**.

Installing the ComparA Client

The side-by-side comparison overlay tool, ComparA, must be installed on each workstation where a user is reviewing plans and documents. The installation location is hard-coded to install ComparA to a pre-defined location so that Civic Platform knows where to find it.

Note: you must install Accela Civic Platform 7.2.2.0.7 or later before installing ComparA.

To run the ComparA Client Installer:

1. Download the ComparA installation files from Accela's FTP site.
2. Launch the installer by double clicking *ComparaSetup2.11.1.msi* (or the latest version).
3. Click **Next**.
The Confirm Installation window displays.
4. Click **Next**.
The installation begins, and a progress bar displays. When the installation is finished, the installer displays "Installation Complete."
5. Click **Close** to complete the installation.
6. Configure the required Civic Platform FIDs and Standard Choices. Refer to "Electronic Document Review" in the *Civic Platform Configuration Reference*, available via the [Documentation Library](#) on Community.

Configuring Adobe Acrobat

If your agency uses Accela Electronic Document Review, you can make modifications to Adobe Acrobat Pro to align its functionality with the types of documents your agency plan to review, and the types of annotations you can use.

This section details both the required steps and several optional steps for you to take to set up Adobe Acrobat Pro for use with Electronic Document Review.

Topics

- [Required Setup](#)
- [Optional Acrobat Setup](#)
- [Best Practices: Adobe Acrobat Tools](#)

Required Setup

Each user must purchase and install Adobe Acrobat Pro separately for interacting with Civic Platform Electronic Document Review and the PDF files associated with projects. Click the following link to download a trial version of Adobe Acrobat Pro, or directly purchase:

<http://www.adobe.com/downloads/>

After the installation, you need to run the Accela Document Review Client Installer to install the Accela plug-ins and document review collaboration client.

Optional Acrobat Setup

Users can personalize the appearance of their PDF annotations, such as modifying them by color, by appearance, and by content.

Topics

- [Modifying your Quick Tools Toolbar](#)
- [Changing the default color/appearance of annotations and drawing markups](#)
- [Changing the name that appears by default in comments](#)
- [Finding your Measuring Tools](#)
- [Creating and Importing Custom Stamps](#)

Modifying your Quick Tools Toolbar

Adobe Acrobat Pro provides you with a number of annotation and graphical tools that you can use when reviewing PDF documents. You can customize the appearance and content of many of these tools, and can also decide how you want to access these tools. The Quick Tools feature gives you the ability to select which tools to appear in your toolbar. You can also elect which tool groups, such as Annotations and Drawing Markups, appear in the side panel. Note that the Civic Platform panel locates in the Tools group and not in the Comments group.

For the best practice recommendations for setting up your toolbar, see [Best Practices: Adobe Acrobat Tools](#).

Changing the default color/appearance of annotations and drawing markups

Repeat the following steps for each annotation and drawing mark-up tool you want to modify.

1. Click **Comment** to open the side panel.
2. Use the **Show/Hide Panels** button to ensure that the Annotations and/or Drawing Markups panels display in your toolbar.
3. Right-click the annotation tool or drawing markup tool that you want to set up.
4. Click **Tools > Default Properties**.
A Properties window displays for the type of tool that you selected.
5. Modify the appearance of the tool as desired using the settings on the Appearance tab.

6. Click **OK** when done.

Adobe Acrobat Pro applies the new settings every time you use the newly modified tool.

Changing the name that appears by default in comments

By default, Adobe Acrobat Pro uses your workstation name to identify you as the author of comments you insert in any document. Follow the steps below to define a different name and specify other identifying information to appear in comments, stamps, and digital signatures.

1. Choose **Edit > Preferences** from the menu in Adobe Acrobat Pro.
The Preferences window displays.
2. In the Categories list on the left side, find and select **Commenting**.
3. Locate and clear the **Always use Log-in Name for Author name** check box.
4. In the Categories list on the left side, find and select **Identity**.
5. Enter the fields on the Identity form with your identifying information.



Note:

You cannot modify the Login Name, which is your workstation login name.

6. Click **OK**.

Finding your Measuring Tools

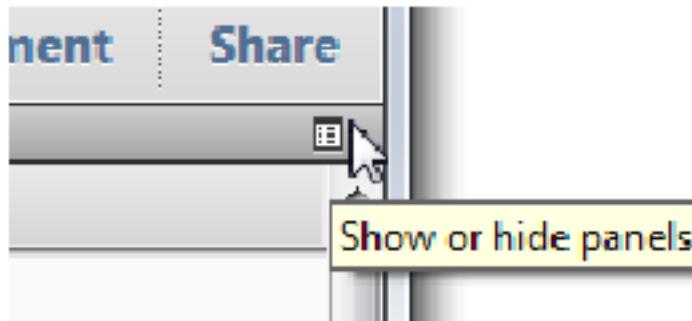
The Measuring Tool button is available on both the toolbar and the side panel. However, Adobe Acrobat Pro may not display it by default. If you do not see the Measuring Tools button and you anticipate that you need not use it, you can add it to your toolbar and/or side panel.

To add the Measuring Tool button to your toolbar:

1. Click the Customize Quick Tools button
The Customize Quick Tools window displays, showing a list of available tools to the left.
2. Click **Tools > Analyze** in the left pane.
3. Select the **Measuring Tool** and move it to the right panel.
4. Click **OK**.

To add the Measuring Tool button to your side panel:

1. Click Tools to display the Tools panel.
2. Click the Show/Hide Panels button to display a menu where you can choose which panels to display.



3. Select Analyze. A check mark next to the name means the panel is visible.
- The Analyze panel displays. The Measuring Tool button is in that panel.

Creating and Importing Custom Stamps

In addition to the standard Adobe Acrobat stamp set and the Civic Platform stamp set provided to you with the Document Review Client Installer, you can create your own stamps and import them for use in Adobe Acrobat Pro. You can use any application with basic graphics tools to create a custom stamp, as long as the application supports printing to PDF. Word is a good option because it supports both text and graphics, and supports saving to PDF.

Custom stamps can be simple graphical images, or they can be complex, incorporating dynamic elements that use data from other sources such as the Identity form in Adobe Acrobat or the time clock on your computer. One option for creating your own stamps is by modifying the sample stamps we have provided. This section provides instructions for modifying an AEDR stamp.

To modify an AEDR stamp:

1. If you have not yet done so, install the custom stamps and custom buttons.
2. Navigate to this folder (or equivalent) on your computer:

```
...Users\yourlogin\AppData\Roaming\Adobe\Acrobat\10.0\Stamps
```

3. Identify the stamp you want to modify, and create a copy.

Note: Do not modify the original pdf files found in the ...\\Acrobat\\10.0\\Stamps folder. Instead, copy/paste the stamp file you want to modify and modify the COPY instead of the original. When you rename the copy, use a unique name.

4. Open the newly created pdf file copy in Adobe Acrobat Pro, and make changes as needed.



Note: You can find useful editing tools in the Quick Tools window which you can access by clicking the **Customize Quick Tools** button in your toolbar. Expand **Tools > Content** in the Quick Tools window to find a number of editing tools you can add to your toolbar. Experiment to see what tools work best for you.

5. Save the modified PDF file to the same folder where the other custom stamps locates (...\\Users\\yourname\\AppData\\Roaming\\Adobe\\Acrobat\\11.0\\Stamps). Do not close the file.

6. Select **File > Properties** to open the Document Properties window.

- In the **Title** field, enter a group name or category name for your stamp. You can enter an existing name or a new name. For example, if you create a series of stamps for the Fire Department to use, you can enter “Fire Department” in the Title field for each stamp you want to include in the group. When you open the Stamps drop-down list, you can see Fire Department > listed. If you select Fire Department, you can see a list of every stamp for which you set Title = Fire Department.
- Click **OK**.

7. Save the document.

To see your stamp in the **Stamp** drop-down list, restart Adobe Acrobat Pro.



Note:

For information about creating dynamic stamps in Adobe Acrobat Pro, check out <http://acrobatusers.com>, which is an Adobe-sponsored user community.

Best Practices: Adobe Acrobat Tools

Accela recommends that users set up their Quick Tools toolbar as shown in the illustration below.



- 1. Customize Quick Tools button** - Click to access Customize Quick Tools
- 2. Add Sticky Note button** - Find in Comment > Annotations
- 3. Draw Rectangle button** - Find in Comment > Drawing Markups
- 4. Draw Cloud button** - Find in Comment > Drawing Markups
- 5. Measurement button** - Find in Tools > Analyze
- 6. Accela Check In Revisions button** - Find in Third-Party Plug-Ins > Plug-In Add-On Tools
- 7. Accela E-Codes button** - Find in Third-Party Plug-Ins > Plug-In Add-On Tools
- 8. Accela Publish Comments button** - Find in Third-Party Plug-Ins > Plug-In Add-On Tools
- 9. Accela Get Updates button** - Find in Third-Party Plug-Ins > Plug-In Add-On Tools
- 10. More Insert Options drop-down button** - Find in Tools > Pages
- 11. Crop button** - Find in Tools > Pages
- 12. Stamps drop-down button** - Find in Comment > Annotations
- 13. Sign Document button** - Find in Tools > Sign & Certify
- 14. Bates Numbering drop-down button** - Find in Tools > Pages

Migrating Document Comments from Version 7.1.0

The 7.1.0 version of Electronic Document Review (EDR) stores document comments in separate XML files on the server (by Adobe) with the document. The 9.0.0 version of EDR stores document comments stored in the database, which gives you the ability to use them in reports.

If your agency implemented Electronic Document Review (EDR) 7.1 and you are upgrading to Civic Platform 9.0.0, you must migrate all of the document comments stored in these XML files on the server to your Civic Platform database. This migration is a one-time process.



Note:

Running this migration possibly affects users who are working online. Accela recommends that you run the process after working hours.

To migrate 7.1.0 document comments from XML to the database:

Pre-migration:

1. Add the migration URL to the link portlet in Civic Platform for security purposes. The URL to use is [https://servername:port\]/portlets/migration/documentcommentindex.jsp](https://servername:port]/portlets/migration/documentcommentindex.jsp), where servername and port are

your agency's Civic Platform server name and server port number. For instructions on adding a URL to a link portlet, see the Link Portlets topic in the Accela Civic Platform Administrator Guide.

Migration:

1. Click the main link configured for Civic Platform administration.



Note:

If you did not follow the instructions in the pre-migration step to add the URL to the Link Portlets list, you can open the migration by typing the address. An address example is [https://servername:port\]/portlets/migration/documentcommentindex.jsp](https://servername:port]/portlets/migration/documentcommentindex.jsp), where **servername** and **port** are your agency's Civic Platform server name and server port number.

Make sure you also log in to Civic Platform using the same session as migration window uses.

2. Click the **Agency Profile > Link Portlets** link.

3. Click the Document Comment Migration link you created.

The Document Comment Migration detail portlet displays.

4. Choose the Links tab, then click the URL.

The Document Comment Migration window displays.

Document Comment - Migration.

Use this form to migrate the document comments.

Agency Code:

ADDEV

Start migration

Stop migration

NOTE:

- Please click "Start Migration" button to launch a migration task.

5. Confirm the Agency Code value, then click the Start migration button.

Civic Platform begins the migration. The status of the process displays in the window. When the migration is complete, the message indicates the process is complete. Click the Stop Migration button at any time to halt the process.

Document Comment - Migration.

Use this form to migrate the document comments.

Please wait while migrating

Remainder: 115

Agency Code:

ADDEV

[Start migration](#)

[Stop migration](#)

NOTE:

- Please click "Start Migration" button to launch a migration task.

Accela Document Scan Installation

To use the Accela Document Scan feature in Civic Platform, you must install .Net Framework 4.0 or 4.5 in your local machine, followed by the Accela Document Scan client.

Accela Document Scan uses TWAIN driver functionality to communicate with scanners, so your scanner must be TWAIN-compliant, and applicable scanner software that includes the TWAIN drivers must be installed on the workstation where you plan to use Accela Document Scan.

Follow the instructions in this chapter to install and set up Accela Document Scan.

Related Information

[Configuring Your System to Use Accela Document Scan](#)

[Installing Accela Document Scan](#)

Configuring Your System to Use Accela Document Scan

You need to have installed .Net Framework 4.0 or 4.5. Click this link to obtain the .Net Framework 4.0 install package: <http://www.microsoft.com/downloads/en/details.aspx?FamilyID=e5ad0459-cbcc-4b4f-97b6-fb17111cf544>. Click this link to obtain the .Net Framework 4.5 install package: <http://www.microsoft.com/en-us/download/details.aspx?id=30653>.

Installing Accela Document Scan

To install Accela Document Scan:

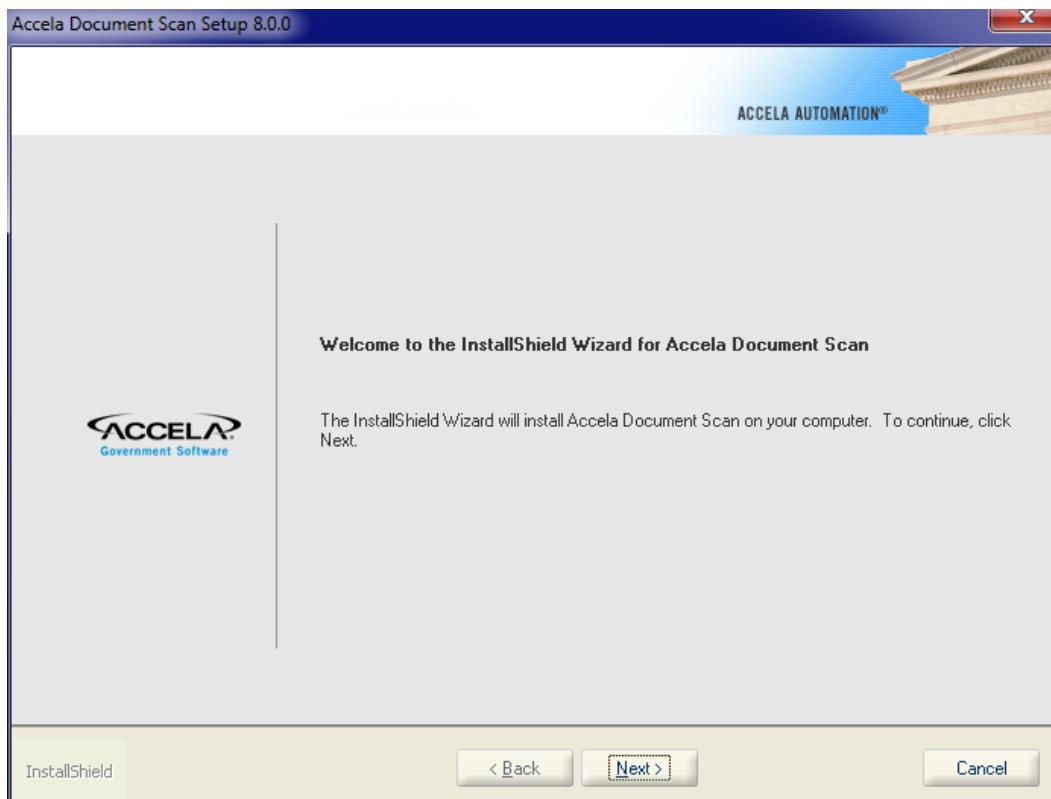
1. Get the Accela Document Scan client installer (*Accela_Document_Scan_Client_9.0.0.exe*) from the Accela FTP site and copy it to the workstation.
2. Confirm that the workstation is attached to at least one TWAIN-compliant scanner, and that the applicable scanner software has been installed on the workstation.
3. Locate the installer in your file browser, and double-click the file to launch the client installer.



Note:

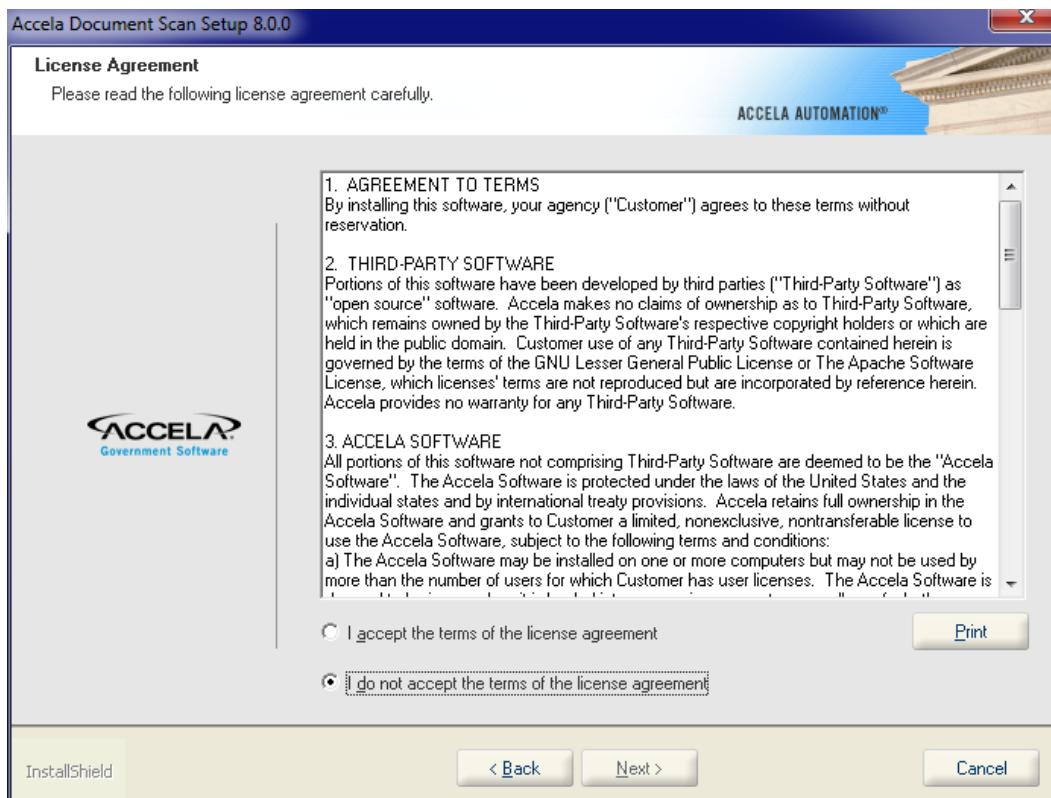
If the workstation runs on a Windows 7 operating system, you may see a security warning message displayed, asking you if you want to allow Accela Document Scan to make changes to your computer. Click **Yes** to continue with the installation.

The InstallShield Wizard for Accela Document Scan launches and the Welcome screen displays.



4. Click **Next.**

The License Agreement page displays.



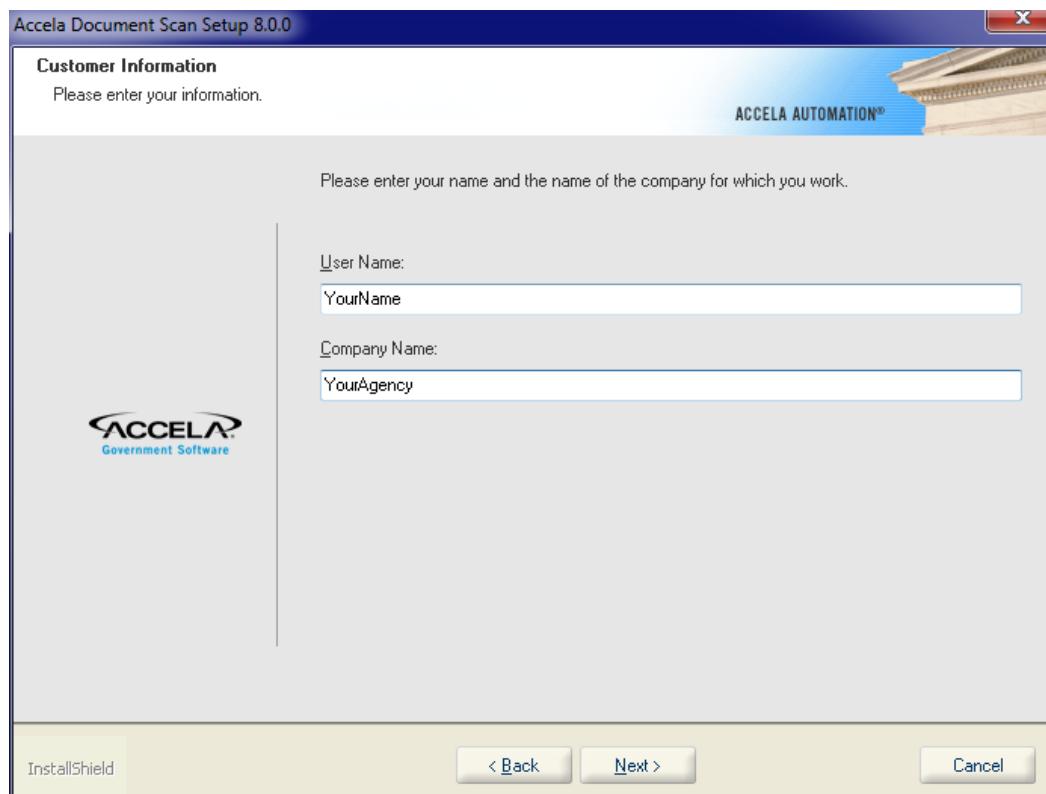
5. Read the agreement and select “I accept the terms of the license agreement” to continue.

**Note:**

If you do not want to accept the terms of the agreement, the installation cannot proceed. Click Cancel to exit the installer.

6. Click Next.

The Customer Information page displays.



7. Enter your name and the name of your agency in the boxes provided.

8. Click Next.

The Installation wizard checks scanner availability and then lists available scanners.

9. From the drop-down list, choose the scanner you want to use for the current workstation.

10. Click Next.

The Choose Destination Location window displays.

11. Click Browse if you want change the location where you want to install Accela Document Scan. Otherwise, click Next to accept the default installation location.

The Ready to Install window displays.

12. Click Install to proceed with the installation.

13. Click Finish when the installation completes.

Setting Up a Cashier Station

This chapter provides instructions for setting up a cashier station, which includes configuring a cash drawer and a slip printer. This enables cashiers to print receipts for point-of-sale (POS) transactions, process payments, endorse checks, and track the balance of funds in their cash drawer. Civic Platform is compatible with electronic cash drawers and with the Epson TM-U675P multi-function slip printer.

The Epson TM-U675P printer is the only printer that can work with cashier stations.

Related Information

[Intended Audience and Environment](#)

[Requirements](#)

[Configuring the Cashier Station](#)

[Setting Up Web Browser Security Policy](#)

[Validating the Installation](#)

[Customizing Endorsement Content](#)

Intended Audience and Environment

The intended audience for this chapter is Accela Services staff, who typically implement Civic Platform's cashier station functionality. You must have access to the Accela FTP site, so you can download the necessary files and necessary components to implement the feature.

The instructions in this chapter can work well with Windows XP Professional, SP 3.

Example Use Case

You can capture the amount of money in a cash drawer when starting and ending a cashier session by setting the Standard Choice CASH_DRAWER_STARTING_ENDING_BALANCE to Yes.

When a user starts taking payments by clicking the New Session button, a prompt displays requiring them to enter the starting cash amount in the drawer. Users must also enter an amount in the drawer when they finish a cashier session. These amounts display on the transaction list to assist users when they figure out the balance for the day. The starting and ending balances display on the Cashier Session Report.

Requirements

Verify that you have all the necessary hardware components and software components before you begin the configuration.

The slip printer can operate independently of the cash drawer, so an agency can choose not to implement cash drawer functionality, depending on their requirements. The cash drawer, however, is dependent on the slip printer. You must connect the slip printer to the workstation with a special cable called a "Kwick Kable," which looks like a flat telephone cord.

Topics

- [Hardware](#)
- [Software](#)

Hardware

This feature requires the following hardware components:

- Workstation (PC or laptop)
- Epson TM-U675P multi-function slip printer
- ERC-32B black printer ribbon
- Connection cord from workstation to a printer with USB port compatibility
- Roll of receipt paper
- Connection cord from the printer to the cash drawer (Epson RJ-12 Drawer 1 “Kwick Kable”)
- Printer-driven electronic cash drawer

Software

This feature requires the following software components:

- Windows XP Professional SP3, or Windows 7 32-bit.
- Other required software components: Refer to the *Accela Enterprise Software Fact Sheet* for a list of required software for the workstation. This document is available from the Accela Customer Support team.

Configuring the Cashier Station

There are six general tasks to configure a cashier station. The following is an outline, with references to the corresponding sections of this document:

1. Set the FIDs for the feature. See [Cashier Station FIDs and Standard Choices](#).
2. If you are connecting the printer to the workstation through the LPT port, you must configure the workstation's parallel port which can enable plug-and-play detection. See [Configuring Parallel Ports](#).
3. Download and install the necessary printer drivers associated with this feature. For Windows XP workstations, these drivers are available for download on the Accela FTP site. For Windows 7 workstations, you must download the drivers from a trusted internet site. See:
 - [Installing the Epson Advanced Driver](#)
 - [Installing the OPOS Driver](#)
 - [Installing the OPOS Driver Service Pack \(Windows XP Only\)](#)
4. Set the web browser security policy. See [Setting Up Web Browser Security Policy](#).
5. Validate the installation. See [Validating the Installation](#).
6. Customize the content of the endorsements that print on the backs of checks, according to the agency's business objectives. See [Customizing Endorsement Content](#).

**Note:**

Do not connect the printer to the workstation until . If you do, the drivers automatically selected when attaching the printer to the workstation install automatically and cause numerous problems. If the incorrect drivers install on the workstation, you must remove them.

Topics

- [Cashier Station FIDs and Standard Choices](#)
- [Configuring Parallel Ports](#)
- [Installing the Epson Advanced Driver](#)
- [Installing the OPOS Driver](#)
- [Installing the OPOS Driver Service Pack \(Windows XP Only\)](#)

Cashier Station FIDs and Standard Choices

See the *Accela Civic Platform Configuration Reference* for details setting FIDs and standard choices.

FIDs

- 8107-Cashier Supervisor
- 8108-Cashier Payment
- 8296-Cash Drawer
- 8261-Open Cash Drawer
- 8251-Cashier Session
- 8259-Cashier Session Supervisor
- 8286-Fees Print Receipt Summary
- If the agency chooses not to implement a cash drawer, set FID 8296-Cash Drawer and 8261-Open Cash Drawer to None to eliminate pop-up windows.

Standard Choices

- **ENABLE_PAYMENT_ENDORSEMENT**

Set this standard choice value to Yes to display the Print Application Endorsement button on the receipt summary of a record (Record > Payment tab > Check receipt number > receipt summary).

- **PAYMENT_REMITTER_CONTACT_TYPE**

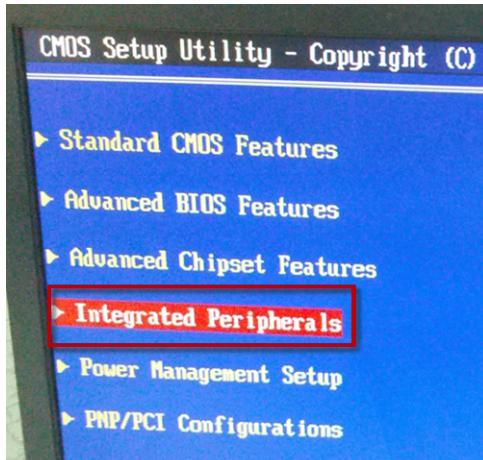
This standard choice defines a “remitter” contact type, which displays on the check endorsement page. Set the value of this standard choice to a valid contact type, for example, Applicant. You must map this standard choice value to an existing contact type, which you define in the standard choice CONTACT_TYPE.

Configuring Parallel Ports

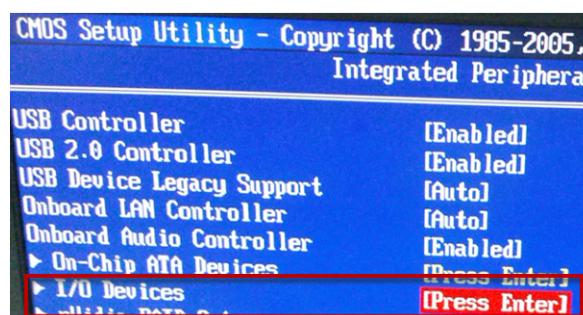
If you are connecting the printer to the workstation through the LPT port on the workstation, you must configure the workstation’s parallel port. Parallel port configuration enables plug-and-play detection.

To configure to use parallel ports:

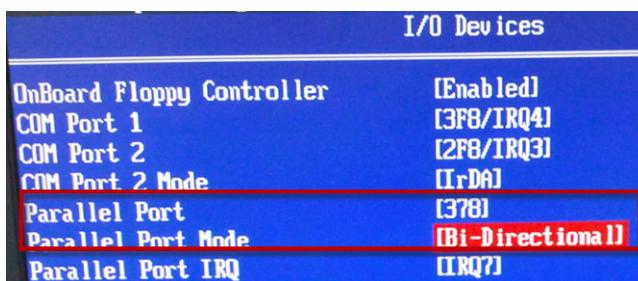
1. Restart the computer; during reboot, press the appropriate key to enter Setup mode, which is often the Delete key.
The workstation displays the CMOS Setup Utility page.
2. Select Integrated Peripherals, as shown in this sample screen.



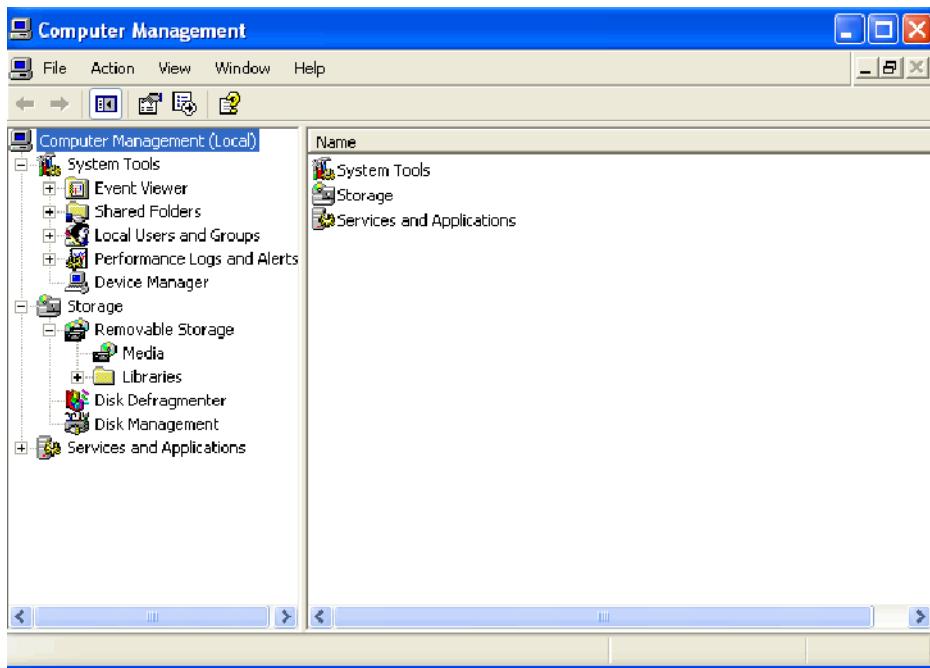
3. Select I/O Devices, as shown in this sample screen.



4. Set the parallel port to 378 and set the parallel port mode to Bi-Directional, as shown in this sample screen.



5. Restart the computer again, this time without pressing any keys.
6. Navigate to **Control Panel > Administrative Tools > Computer Management**.
The workstation displays the Computer Management window.

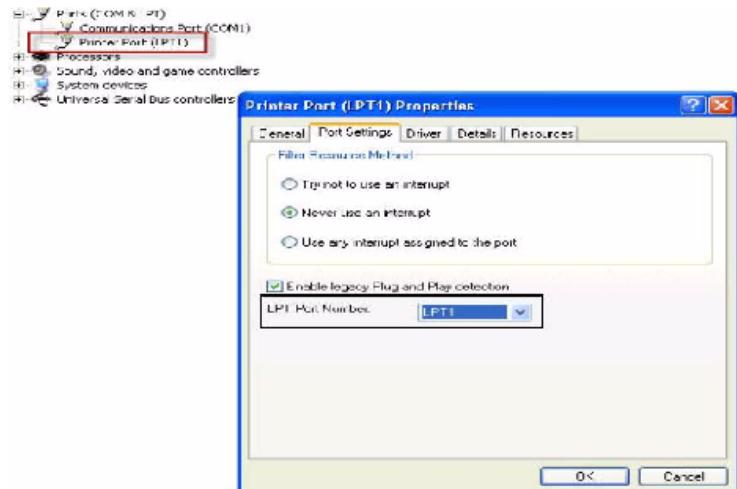


7. Navigate to System Tools > Device Manager > Ports > ECP Printer Port (LPT1).

The ECP Printer Port (LPT1) window displays.

8. Select the Port Settings tab.

9. Mark the Enable legacy Plug and Play detection check box and select LPT1 from the drop-down list.



10. Click OK and close all windows.

Installing the Epson Advanced Driver

For the workstation to communicate correctly with the Epson printer, you must install the appropriate printer drivers. The first driver that you must install is the Epson Advanced Driver.

Do not attach the printer to the workstation until instructed to do so. If you do, the workstation automatically selects drivers to run the printer which are incorrect and you must remove them.

**Note:**

Do not connect the printer to the workstation until . If you do, the drivers automatically selected when attaching the printer to the workstation install automatically and cause numerous problems. If the incorrect drivers install on the workstation, you must remove them.

To install the Epson advanced driver:**1. Download the appropriate driver:**

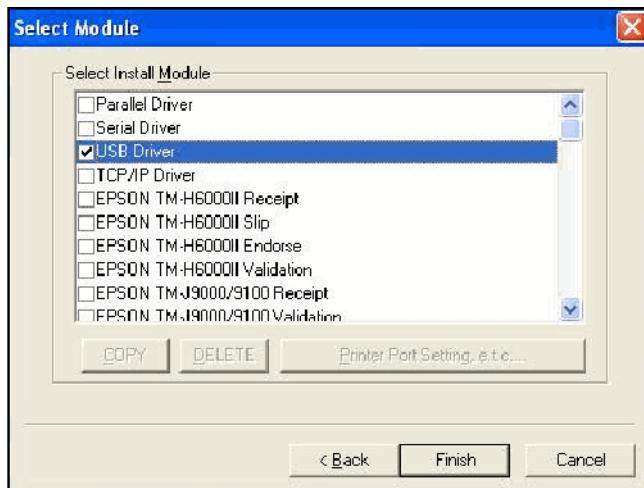
- Windows XP: ATM_301cE.exe. This driver is available on the Accela FTP site.
- Windows 7: APD_453E.exe. You must perform an internet search for this driver and download it from a trusted site.

2. Extract the contents of the zip file and double-click the executable file to run it.**3. Choose the operating system (Windows XP or Windows 7) and language.****Note:**

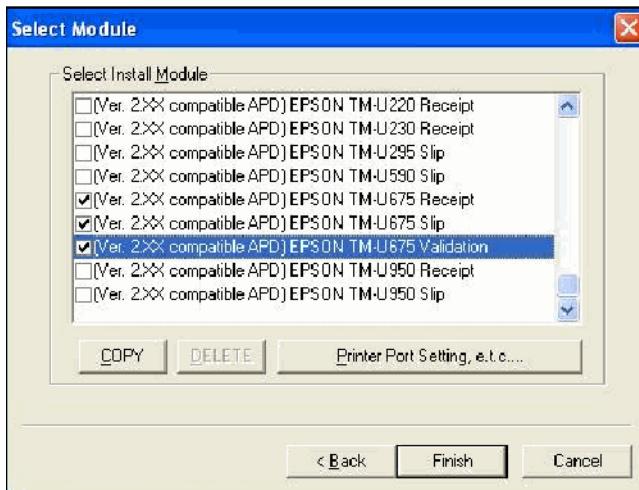
The remaining screens and steps are for a Windows XP Professional SP3 workstation. If you are configuring a Windows 7 workstation, the screens differ from these examples.

4. When prompted, specify one of the following check boxes:

- USB Driver
- Parallel Driver (only if you are [Configuring Parallel Ports](#)).

**5. Scroll down this same list in the Select Module window and mark these check boxes for (Ver. 2.XX compatible APD) EPSON TM-U675P.**

- a. Mark the Receipt check box for (Ver. 2.XX compatible APD) EPSON TM-U675.
- b. Mark the Slip check box for (Ver. 2.XX compatible APD) EPSON TM-U675.
- c. Mark the Validation check box for (Ver. 2.XX compatible APD) EPSON TM-U675.



6. For each of the (Ver. 2.XX compatible APD) EPSON TM-U675 modules (Receipt, Slip, and Validation), set up the Printer Port Settings.
 - a. Highlight the (Ver. 2.XX compatible APD) EPSON TM-U675 module and click the **Printer Port Setting, etc.** button.
 - b. Mark the option for the applicable Port Type. **USB** for USB port and **Parallel LPT1** for Parallel mode.
 - c. Perform the printer port settings for each of the Slip, Receipt, and Validation (Ver. 2.XX compatible APD) EPSON TM-U675 list items.
7. Click **Finish**.
8. Set the default printer to the Receipt printer.
 - a. Navigate to Control Panel > Printer & Faxes.
 - b. Click the Receipt printer, then right-click and choose **Set as Default Printer** from the drop-down list.
 - c. Exit the Control Panel.
9. Shut down the computer.
10. Connect the Epson Printer to the Workstation with the USB cord or parallel connection cord.
11. Start the computer. Verify that the printer can successfully print a test document.

Installing the OPOS Driver

After you install and test the Epson Advanced Driver, install the OPOS drivers.

For Windows XP workstations, you must install the OPOS driver and its associated service pack. For Windows 7 workstations, you only need to install one OPOS driver, as described below. Follow the instructions below for a successful OPOS base driver installation.

To install the OPOS driver:

1. Download the appropriate driver:
 - Windows XP: OPOSADK250E.exe. This driver is available on the Accela FTP site.
 - Windows 7: ADK270ER3.exe. You must perform an internet search for this driver and download it from a trusted site.

**Note:**

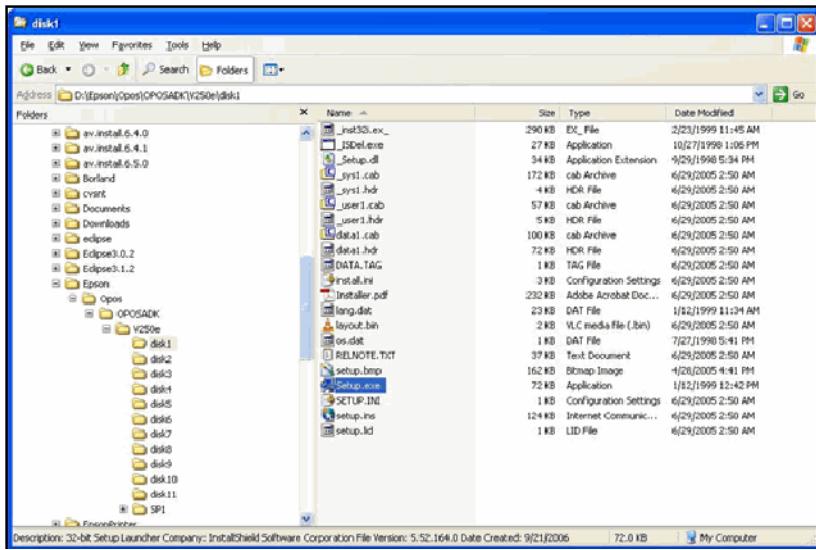
The remaining screens and steps for a Windows XP Professional SP3 workstation. If you are configuring a Windows 7 workstation, the screens differ from these examples.

2. Unzip the

OPOSADK250E.zip

file.

3. Go to Epson > OPOS > OPOSADK > V250e > disk1.



4. From the disk1 folder, run

setup.exe

5. Choose the following settings:

- a. When the release note displays, close the note.**

The workstation displays a window with a question about the parallel I/F.

- b. When prompted for parallel I/F (interface), answer **No** for USB connection or **Yes** for Parallel mode, depending on your configuration.**

6. When prompted, restart the computer.

Installing the OPOS Driver Service Pack (Windows XP Only)

This procedure is not applicable to Windows 7. If you are configuring a Windows 7 workstation, skip this step.

After you install the OPOS base driver, as described in the previous section, install the OPOS driver service pack. Follow the instructions below for a successful OPOS driver service pack installation.

To install the OPOS driver service pack:

1. Download the OPOSADK250ESP1.exe driver from the Accela FTP site.

2. Unzip the

OPOSADK250ESP1.zip

file.

3. Browse to **OPOSADK > V250e > SP1 > disk1**.

4. From disk1, run the

setup.exe

file.

5. Restart the computer.

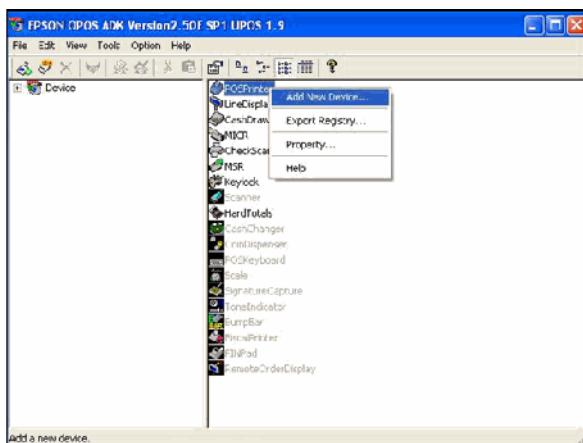
6. Navigate to **Start > All Programs > OPOS > Setup POSv2.00**.

7. Run the OPOS setup utility.

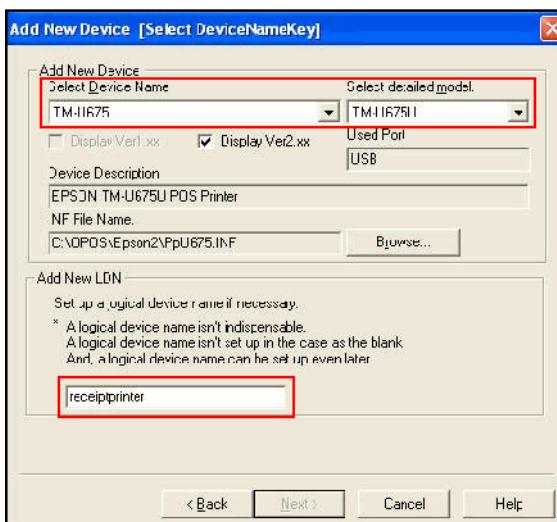
The workstation displays the EPSON OPOS ADK Version 2.5E SP1 UPOS window.

8. Add a new device to POSPrinter

a. From the device node, right-click POSPrinter and choose Add New Device from the menu.

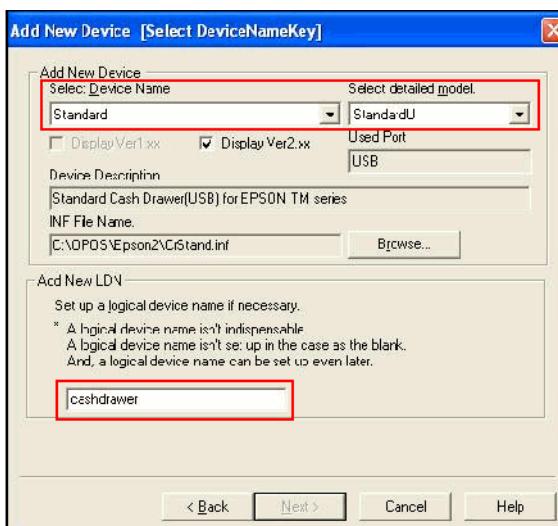


The Add New Device [Select DeviceNameKey] page displays.



b. Choose TM_U675 from the Select Device Name drop-down list.

- c. Choose the applicable TM-U675 option from the **Select detailed model** drop-down list. Use TM-U675U for USB port and TM-U675P for parallel port.
 - d. Type *receiptprinter* for the New LDN Name. Do not change this name, you must enter it exactly as shown in the sample screen.
 - e. Click **Finish**.
9. Add a new device to the cash drawer.
- a. From the device node, right-click Cash Drawer and choose **Add New Device** from the menu. The Add New Device [Select DeviceNameKey] page displays.



- b. Choose Standard from the Select Device Name drop-down list.
- c. Choose the applicable Standard option from the **Select detailed model** drop-down list. Use StandardU for USB port and StandardP for parallel port.
- d. Type *cashdrawer* for the New LDN Name. Do not change this name, you must enter it exactly as shown in the sample screen.
- e. Click **Finalize**.



Note:

If you get an error message indicating that you assigned another device (POS Printer) to the port, click OK. It is okay for the POS Printer and the Cash Drawer to share the same port because the POS Printer passes through the cash drawer commands.

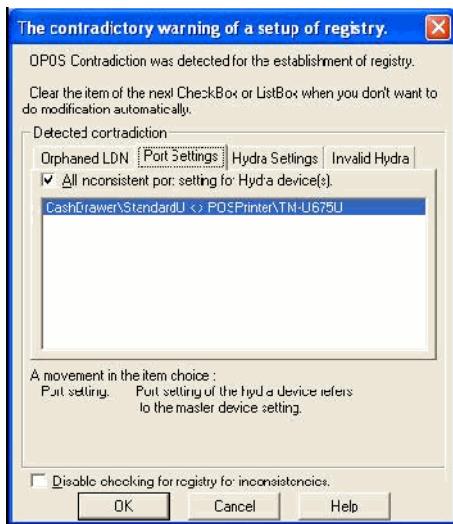


Figure 17: Contradictory Warning of a Setup of Registry:

Setting Up Web Browser Security Policy

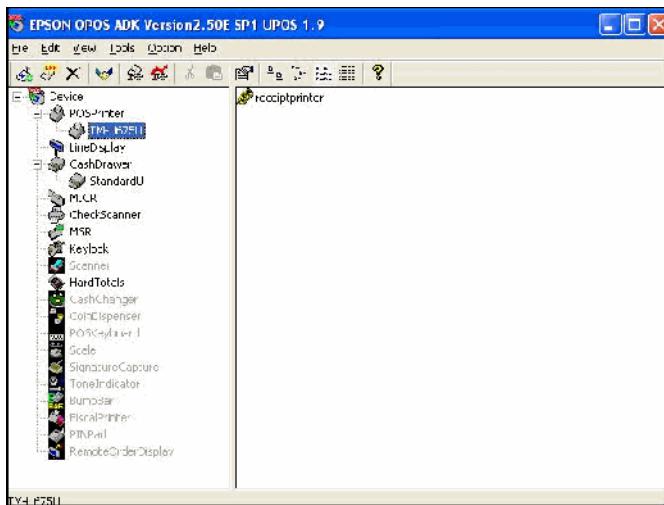
Civic Platform generates receipts with a browser pop-up feature when users process a payment in a cashier session. You cannot view or print receipts unless you set Civic Platform as a trusted site, enable Active X features and scripting, and disable pop-up blockers from Microsoft Internet Explorer (IE), Google Toolbar, and Yahoo Toolbar.

Follow the instructions in [Trusted Sites and Zones Settings](#) to set up the browser security policy, and then restart your browser.

Validating the Installation

Use the procedure in this section to verify that the Epson TM-U675P printer and electronic cash drawer installation are successful and that the components function properly.

1. Verify that the POSPrinter directory displays receiptprinter, and that the CashDrawer directory displays cashdrawer in the Devices area of your Windows file system.



2. Download the OPOS-test.exe driver from the Accela FTP site.

3. Unzip the

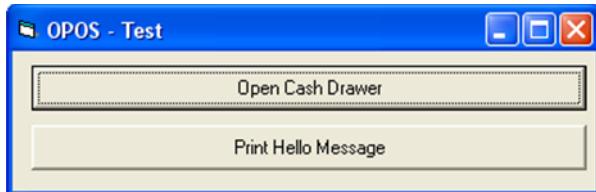
OPOS-test.zip

file and run the

OPOS-test.exe

file.

The following screen displays.



a. Click **Open Cash Drawer** to test opening the cash drawer electronically.

If the cash drawer does not open, review the installation steps and verify that you have performed the installation correctly.

b. Click **Print Hello Message** to test the receipt printer data output.

If the Hello Message does not print, review the installation steps and verify that you have performed the installation correctly.

Customizing Endorsement Content

You can customize the content of the endorsements that you print from the slip printer, with the following procedure. You can print endorsement details on checks and applications.

To customize the endorsement fields that print from the slip printer:

1. In Civic Platform, navigate to Setup > Agency Profile > Content Customize.

2. Select one of the following endorsement types, then customize the text of the endorsement content, using the variables listed in [Endorsement Type Variables](#).

Endorsement Type	Product Navigation Path
APPLICATION_ENDORSEMENT	Record/POS > Payment/Refund
CHECK_ENDORSEMENT	Record/POS > Payment/Refund
SET_CHECK_ENDORSEMENT	Set/Sets > Payment and Sets/Refund
TRANSACTION_CHECK_ENDORSEMENT	Payment Processing > Payment/Refund
TRUSTACCOUNT_CHECK_ENDORSEMENT	Trust account > Deposit/Withdraw

3. From the product paths indicated for each of the endorsement types:

- a. Make a payment or refund by check method.
- b. Go to the receipt summary.
- c. Click the check endorsement button and go to the endorsement detail page.
- d. Click the print button.

The endorsement prints with the slip printer.

Table 7: Endorsement Type Variables

Endorsement Type	Supported Variables
APPLICATION_ENDORSEMENT	<ul style="list-style-type: none"> \$\$transNBR\$\$: Transaction number \$\$permitNBR\$\$: Record ID \$\$contactName\$\$: Contact name \$\$contactType\$\$: Contact type \$\$refContactID\$\$: Reference contact ID \$\$todayDate\$\$: Today's date \$\$businessDate\$\$: Business date
CHECK_ENDORSEMENT	<ul style="list-style-type: none"> \$\$permitNBR\$\$: Record ID \$\$transNBR\$\$: Receipt customized number \$\$adminFeeDue\$\$: Add Fee \$\$cashDrawerID\$\$: Cash drawer ID \$\$totalAmtPaid\$\$: Total Payment Amount \$\$totalInvoice\$\$: Total invoice \$\$totalPaid\$\$: Total paid \$\$balance\$\$: Total invoice less total paid \$\$todayDate\$\$: Current Date \$\$receiptNbr\$\$: Receipt Number \$\$payerRefContactID\$\$: Remitter contact ID \$\$payerContactType\$\$: Remitter type \$\$payerName\$\$: Remitter name

Endorsement Type	Supported Variables
SET_CHECK_ENDORSEMENT	<ul style="list-style-type: none"> \$\$setId\$\$: Set ID \$\$setName\$\$: Set name \$\$transNBR\$\$: Receipt customized number \$\$adminFeeDue\$\$: Add Fee \$\$cashDrawerID\$\$: Cash drawer ID \$\$totalAmtPaid\$\$: Total Payment Amount \$\$totalInvoice\$\$: Total invoice\$\$totalPaid \$\$: Total paid \$\$balance\$\$: total invoice - total paid \$\$todayDate\$\$: Current Date \$\$receiptNbr\$\$: Receipt Number
TRANSACTION_CHECK_ENDORSEMENT	<ul style="list-style-type: none"> \$\$transNBR\$\$: Receipt # \$\$forPermitNbr\$\$: Permit ID \$\$forPOSTransNbr\$\$: POS ID \$\$totalAmtPaid\$\$: Payment Amount \$\$cashDrawerID\$\$: CashDrawerID \$\$sessionNbr\$\$: Session Nbr \$\$todayDate\$\$: Date/Time \$\$businessDate\$\$: Business Date \$\$paymentMethodAndAmount\$\$: Amount
TRUSTACCOUNT_CHECK_ENDORSEMENT	<ul style="list-style-type: none"> \$\$transNBR\$\$: Receipt Number \$\$accountNBR\$\$: Account Number \$\$businessDate\$\$: Business Date \$\$todayDate\$\$: Today \$\$transType\$\$: Transaction Type \$\$amount\$\$: Amount \$\$tenderType\$\$: Tender Type \$\$accountBalance\$\$: Account Balance \$\$cashDrawerID\$\$: Cash Drawer ID \$\$sessionNbr\$\$: Cashier Session Number \$\$transComments\$\$: Transaction Comments \$\$refNBR\$\$: Reference Number

Configuring a Barcode Scanner

The payment processing portlet in Civic Platform allows users to read and retrieve system generated invoices by scanning barcodes on each invoice. It is an efficient way for users to process multiple records for payments.

The Intermec SR30 Handheld scanner is the only scanner that Civic Platform supports for the barcode scanning feature. This section guides you to install and configure an Intermec SR30 Handheld Scanner in your local machine. For information on integrating barcodes in payment reports, see "Using Barcodes in Payment Reports" in the "Report Manager" chapter in the *Accela Civic Platform Administrator Guide*.

To install and configure the Intermec SR30 Handheld Scanner:

1. Follow the steps in the *Intermec SR30 HandHeld Scanner User Guide* to install and configure the scanner. You can get the manual here: http://epsfiles.intermec.com/eps_files/eps_man/934-017.pdf.

To configure the Intermec SR30 Handheld Scanner, you need to use their EasySet tool to enable and disable symbologies for your scanner. EasySet is available on the Intermec website at www.intermec.com/EasySet.

2. Use EasySet to initialize the scanner for integration with Civic Platform.

- a. Start EasySet.

The first time you start EasySet, the Select Product dialog box appears. If the Select Product dialog box does not appear, choose **Product > Select**, or click the product icon in the upper left corner.

- b. Activate Code 39 with the following steps.

- a. Select **Code 39** under **Symbologies**;

- b. Click **active (*)** under **Code 39**.

- c. Scan the generated barcode.

- c. Activate special key interpretation with the following steps.

- a. Select **Code 39** under **Symbologies**;

- b. Click **special keys interpretation** under **Code 39**.

- c. Click **active (*)** under **special keys interpretation**.

- d. Scan the generated barcode.

- d. Set the start/stop characters to be not transmitted.

- a. Select **Code 39** under **Symbologies**;

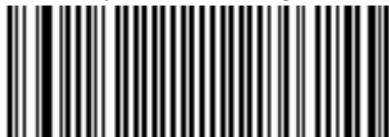
- b. Click **start/stop** under **Code 39**.

- c. Click **not transmitted (*)** under **start/stop**.

- d. Scan the generated barcode.

3. Scan the barcode depicted below to resolve the conflict between the shortcut key Ctrl+Shift_j with the shortcut key for the Feeds bar in Internet Explorer 8.

postamble - USB - keyboard HID - compose: <CR>



\60\02\42\01\00\00\01\00\22\40