This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Workspace Desktop Edition Deployment Guide

Deployment overview

4/2/2026

Deployment overview

Contents

- 1 Deployment overview
  - 1.1 ClickOnce deployment
  - 1.2 Non-ClickOnce deployment
  - 1.3 Customization package deployment
  - 1.4 ClickOnce deployment principles
  - 1.5 Security constraints

Workspace can be deployed in one of three ways, depending on whether you want a ClickOnce or a non-ClickOnce deployment. Optionally, you can choose to install the developer package to customize and extend the capabilities of Workspace. Refer to Table - **Workspace Install Mode Deployment Packages** for the list and description of items that are installed by the Workspace Deployment Application.

Workspace Install Mode Deployment Packages

Package name	Purpose	Folder contents
Prepare a ClickOnce package	Enables IT and administrators to install the Workspace ClickOnce package on a WebServer.	The Workspace folder contains the following folders or files: • `Workspace`: Workspace application • `WorkspaceDeploymentManager`: Deployment Manager application • `WebPublication`: `publish.htm` (bootstrap for client side) and `setup.exe` (prerequisites)
Install Workspace Developer Toolkit	Intended for developers, testers, or those who are demonstrating the application. It contains all the deliverables, including the API references, Workspace, Deployment Manager, and Samples.	The destination folder contains the following folders or files: • `Bin`: List of assemblies (DLLs) available for customization of Workspace (API) • `Doc`: API Reference documentation • `Workspace`: Workspace application • `WorkspaceDeploymentManager`: Deployment Manager application • `WebPublication`: `publish.htm` (bootstrap for client side) and `setup.exe` (prerequisites) • `Samples`: Samples of extensions for developers
Install Workspace application	Intended for agents, testers, or those who are demonstrating the application. It contains only the agent application.	The destination folder contains the following folder: • `Workspace`: Workspace application.

ClickOnce deployment

ClickOnce enables a safe and secure workflow that enables agents to be authenticated and then granted access only to specific privileges. Initially, agents are given a URL (through email, a corporate portal, or a desktop shortcut) that links to the ClickOnce server. When they navigate to the server, the Workspace application is downloaded to their workstation. The application automatically starts, and agents are prompted to authenticate through the login window. When upgrades are made available, they are automatically delivered to agents upon login.

The basic steps for a ClickOnce deployment are as follows:

1. Perform the Procedure: Installing Workspace Deployment Package on the Windows operating system, which guides you through the steps for installing Workspace on your Windows web server from the Workspace CD/DVD.
2. Deploy the ClickOnce package on your web server by using the following Procedure: Deploying the Workspace downloadable package (ClickOnce) on your web server.
3. Start the application bootstrap to install, upgrade, or start the application.
4. Test the client application by using the following Procedure: Configuration verification: Testing the client.

Non-ClickOnce deployment

You can install Workspace on a workstation without a ClickOnce deployment. This installation includes only the agent application. This installation option is used mainly to test Workspace on your system, not for enterprise-wide deployment.

The basic steps for a Non-ClickOnce deployment are as follows:

1. Perform the Procedure: Installing the Workspace application on a client desktop, which guides you through the steps for installing Workspace on an end-user desktop from the Workspace CD/DVD.
2. Start the application.
3. Test the client application by using the following Procedure: Configuration verification: Testing the client.

(Optional) To use Kerberos Single Sign-on (SSO):

1. Install Workspace by using the basic Non-ClickOnce above.
2. Modify the Configuration Server host, port, and application name parameters in the `interactionworkspace.exe.config` property file to conform with your system. This file is in the Workspace directory on the Workspace CD/DVD.

   Workspace requires that you specify the unique Service Principal Name (SPN) that is used in each Configuration Server and Configuration Server Proxy that will handle SSO requests from UI applications. Edit the `login.kerberos.service-principal-name` option in the `interactionworkspace.exe.config` property file to add the following line:

```
<appSettings>
  ...
  <add key="login.kerberos.service-principal-name" value="<SPN Name>"/>
  <add key="login.url" value="tcp://<host><port>/AppName" />
  <add key="login.connections.parameters.isenable" value="false" />
  ...
 </appSettings>
```

3. Add the customization resources that are required for your final installation.
4. Prepare your final package by using the updated file set.
5. Push the package to the agent workstations by using your desktop technology.

Customization package deployment

You can install the Workspace application, API references, Deployment Manager, and Samples on a development workstation as follows: Perform the Procedure: Installing Workspace Customization on the Windows operating system, which guides you through the steps for installing Workspace Customization on a development workstation from the Workspace CD/DVD.

ClickOnce deployment principles

ClickOnce provides a smooth experience for both the user and the network administrator. The user launches the application by using either a URL or a desktop icon. The URL can be provided to agents by email, a corporate portal, a desktop shortcut, or other means. This simple method enables you to install the Workspace application on every workstation easily.

When an agent accesses the URL the Interaction Workspace application is downloaded to the agent's workstation; it automatically starts and the login window is displayed.

For subsequent application starts, the agent can reuse the initial URL or execute the application through a desktop icon or through the `Start` menu.

If a hot fix or update is required or made available on the server, Workspace automatically upgrades the next time that the agent starts the application without you having to push-out a fix or update to every user.

> **Important**
>
> During deployment, you can specify whether agents can reject the Workspace upgrade.

ClickOnce enables you to deploy a security-enabled centralized WebService. Microsoft ClickOnce deployment technology that simplifies the privilege of publishing Windows-based applications to a web server or other network file share.

ClickOnce eliminates the need to reinstall the entire application whenever updates occur. Updates are provided automatically when an agent logs in. Only those portions of the application that have changed are downloaded to the client.

ClickOnce applications are entirely self-contained, they do not rely on shared resources. This means that you can update other resources without any impact on Interaction Workspace, or you can update Workspace without breaking other applications.

Another advantage of ClickOnce is that administrative permissions are not required for the update to be installed. The update is installed automatically from the server when an authorized client logs in.

Scenarios: ClickOnce principles

The following three scenarios demonstrate the utility of the ClickOnce approach to application and system security management:

- Initial installation
- Application patch
- Update of agent privilege permissions

The application patch and permission-update scenarios can occur simultaneously.

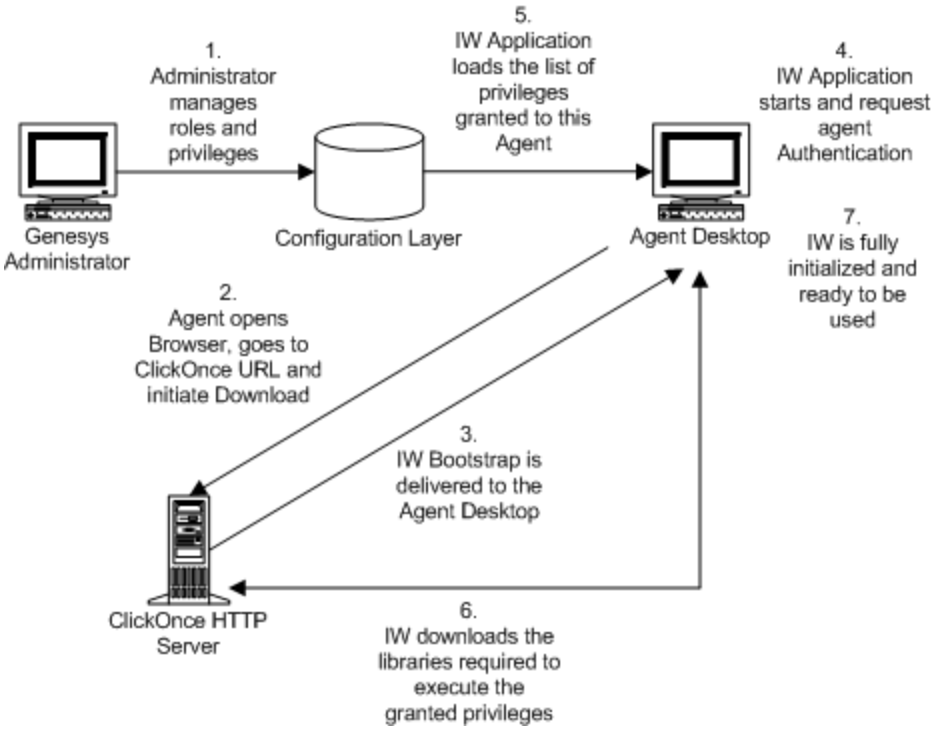
Initial installation

For the initial installation onto the client workstation, the following prerequisites must be met:

- The Workspace application must be installed as a ClickOnce package on the HTTP Server that enables ClickOnce.
- Microsoft .NET Framework 4.5 must be installed on the client workstation.

The Figure - **Initial ClickOnce installation of the Workspace (IW) application** shows the steps in a typical first installation of Workspace in a ClickOnce environment:

1. The administrator manages the roles and privileges of the contact center agent by using Genesys Administrator Extension and stores the configurations in the Configuration Layer. Through email, the corporate portal, or other notification, agents are provided with the application URL.
2. Agents use the URL to go to the ClickOnce HTTP Server and initiate the download.
3. The Workspace Application Bootstrap is delivered to the agent workstation; then the Workspace application launches and agents are prompted for authentication information. **Note:** Agents provide their credentials and are authenticated on the network.
4. The Workspace application starts and requests agent authentication.
5. The Workspace application loads the list of privileges that are granted to each agent, based on agent authentication.
6. The Workspace application then downloads the libraries that are required to execute the granted privileges.
7. Workspace is fully initialized and ready to be used.



Initial ClickOnce installation of the Workspace application

Applying a patch

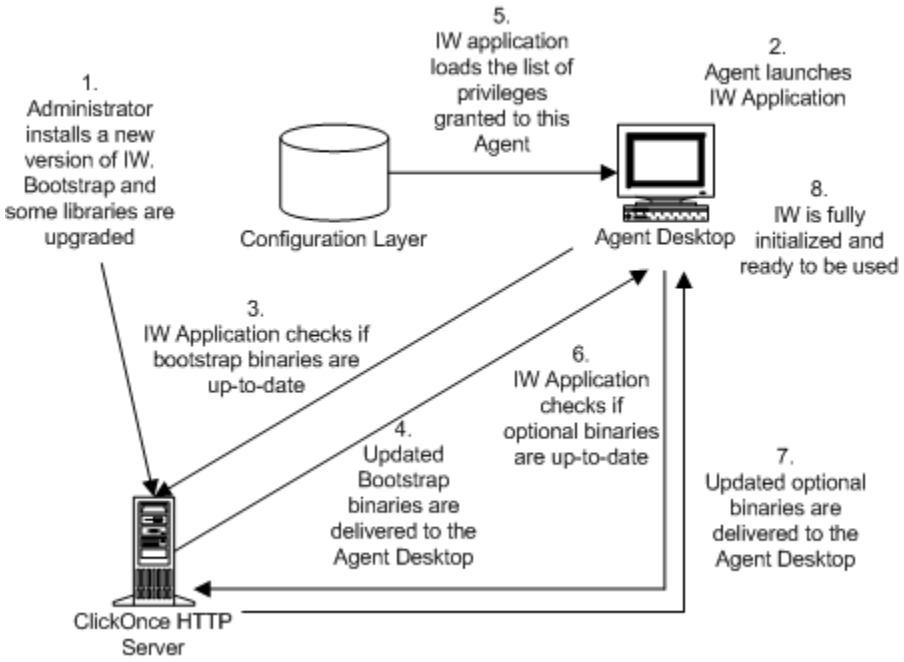
To apply a patch to the installation on the client workstation, the following prerequisites must be met:

- The agent has run Workspace and has been successfully authenticated at least once on the current workstation.
- Privileges that are granted to the agent have not been changed since their previous authentication.

The Figure - **Patching of the Workspace application through ClickOnce** shows the steps in a typical patch installation of Workspace in a ClickOnce environment:

1. The administrator installs a new version of the Workspace Bootstrap and upgrades one or more libraries.
2. Agents launch the Workspace application on their desktop by using the URL or by double-clicking the desktop icon. The agent is authenticated.
3. The Workspace application checks the ClickOnce HTTP Server to determine if the bootstrap binaries are up to date.
4. The updated bootstrap libraries are delivered to the agent workstation.
5. The Workspace application loads the list of privileges that are granted to each agent, based on agent authentication.
6. The Workspace application checks the ClickOnce HTTP Server to determine if the optional binaries are up to date.
7. Updated binaries, if any, are delivered to the agent workstation.

8. The Workspace application is fully initialized and ready for agent use.



Patching of the Workspace application through ClickOnce

Limitation of patching with ClickOnce

Because of the architecture of Workspace and the underlying Platform SDK and Enterprise Services on which it is built, patches are applied to groups of assemblies, not just to a single assembly. Therefore if one assembly in a group is updated, the whole group must be patched.

Update agent privilege permissions

To update the Workspace installation on the client workstation with updated privilege permissions, the following prerequisites must be met:

- The agent has run Workspace and has been successfully authenticated at least once on the current workstation.
- The Workspace application has not been upgraded on the ClickOnce server since the previous login.

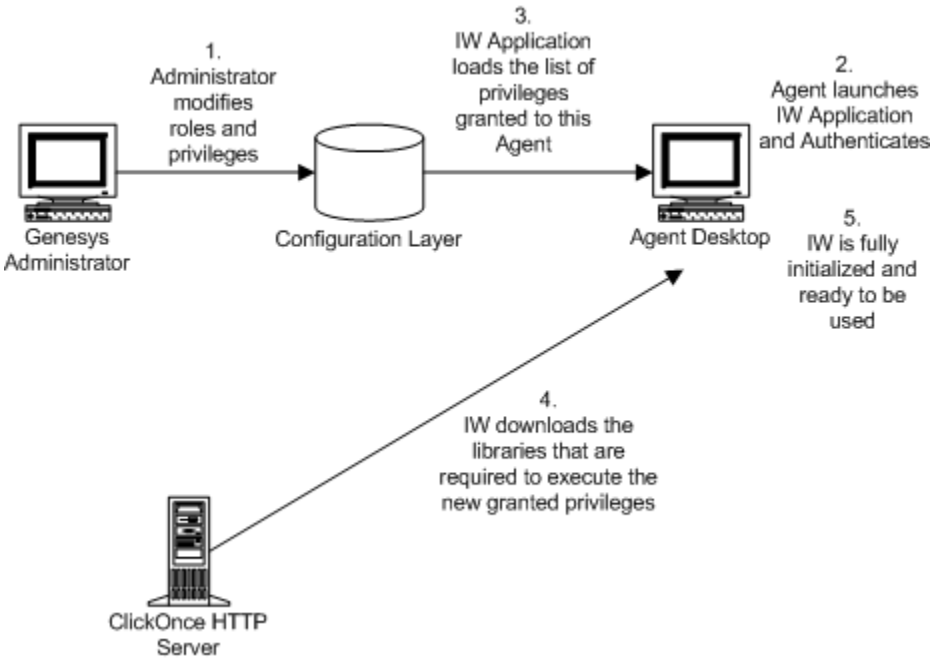
Privilege updates while the agent is not logged in

The Figure - **Update of the agent's role through ClickOnce** shows the steps in a typical privilege-permission upgrade of Workspace in a ClickOnce environment if the agent is *not* already logged in:

1. The administrator modifies the roles and privileges of the contact center agent by using Genesys Administrator Extension and stores the modified configurations in the Configuration Layer.
2. Agents launch the Workspace application on their desktop by using the URL or by double-clicking the desktop icon. The agents are authenticated.
3. The Workspace application loads the list of privileges that are granted to each agent, based on agent

authentication.

4. The Workspace application then downloads the missing libraries that are required to execute the new granted privileges.
5. Workspace is fully initialized and ready for agent use.



Update of the agent's role through ClickOnce (IW = Workspace)

Privilege updates while the agent is logged in

If new privileges are granted to the agent while the agent is logged in, the additional libraries will not be downloaded to the agent's workstation; however, if privileges are removed, this change is taken into account immediately to ensure security.

ClickOnce updates for shared workstations

If multiple users share the same workstation, the download behavior depends on whether each agent has a unique account or whether all agents share the same account.

If each agent has a unique account, then updates are downloaded by account. Therefore, each user will have to download updates. The advantage of this scenario is that multiple agents with different roles can share the same workstation without compromising security.

If all users share a generic account, then only a single instance of the application is downloaded. This means that each user will have the same role as that assigned to the first user to download the application.

Security constraints

To deploy Workspace, three deliverable subsets are installed on the agent workstation:

- Prerequisites: Microsoft .NET Framework 4.5.
- Mandatory executable: Workspace Application Bootstrap (`.exe` file and mandatory DLL assemblies).
- Optional assemblies: The list of optional assemblies depends on the privileges that are granted to the agent who logs in to the application.

The .NET Framework and service pack are not installed through the ClickOnce system; they are installed by the ClickOnce Bootstrap application (see the Figure - **Initial ClickOnce installation of the Workspace application** and Figure **Patching of the Workspace application through ClickOnce**). Therefore, more rights are required on the target computer to install the prerequisite than to install Workspace.

The Workspace Application Bootstrap and the optional assemblies are pure ClickOnce deliverables; therefore, the full ClickOnce security model applies to these installables. However, the .NET Framework does not have the same security constraints. Therefore, Genesys recommends that you deploy the agent application in two phases:

1. Installation of .NET Framework by the administrator **by using the ClickOnce Bootstrapper**, or **by using the standard network distribution**.
2. Installation of Workspace by the agents at the initial login.

You can find more information about ClickOnce security at this URL: http://msdn.microsoft.com/en-us/library/76e4d2xw(VS.80).aspx

Code Access Security

Code Access Security (CAS) is a mechanism that limits system access to the permissions that are granted to each code. CAS protects resources and operations and enables you to grant permissions to assemblies — giving a high degree of control over what resources the assemblies can access. For example, restrictions can be applied to file-system locations, the registry, and specific name spaces.

Setting Code Access Security permissions

You must set CAS permissions for both the Workspace ClickOnce application and the zone from which the application will be installed (for example, your local intranet, the Internet, and so on).

Workspace must be defined as a Full Trust application. A Full Trust application is granted all access to any resource. Granting this level of permission is necessary because some of the embedded DLLs require Full Trust permissions. If Workspace is not defined as a Full Trust application, execution failures will occur when the application tries to access a restricted resource.

Machine Access Security

The Workspace application, which is deployed by ClickOnce, uses CAS permissions. This means that Workspace might require more permissions than are allowed by your security policy. In this case, ClickOnce will allow an automatic elevation of privileges. However, if the publisher is not trusted, a Machine Access security warning is prompted, but no security warning is prompted if the publisher of

Interaction Workspace is trusted.

> **Tip**
> ClickOnce supports Windows Vista User Account Control (UAC); therefore no additional messages are displayed.

ClickOnce and installation security

The minimum class privilege for running a ClickOnce application is `User`. A `Guest` account cannot deploy a ClickOnce application through the network. If an agent is logged in with a `User` account, ClickOnce will automatically elevate the privileges for installing the application on the agent's workstation. If the publisher of ClickOnce deployment is Trusted, the installation will run without any prompting; however, if the publisher is not Trusted, the agent will be prompted to Trust the publisher of the deployment.

ClickOnce and location security

To deploy an application via ClickOnce, the ClickOnce HTTP server must be in a Trusted Zone, such as your local intranet, or be listed in Trusted Sites.

ClickOnce and publisher security

You must consider two publishers when you are deploying a ClickOnce application: the publisher of the application and the publisher of the deployment.

The Workspace Deployment Wizard updates some application files; therefore, the application manifest must be signed after these updates. The Workspace Deployment Wizard must be enabled to sign both the application and deployment manifests.

To sign the manifests, the Workspace Deployment Wizard requires a security certificate. The same security certificate can be used to sign both manifests.

Certificate deployment overview

You must provide a permanent certificate that is used to sign the Workspace installer manifest. This certificate is pointed to during installation. You can obtain your own certificate by one of the following methods:

- Generate a self-signed certificate by using the `Makecert.exe` file.
- Purchase a third-party verified certificate
- Generate a certificate by using Windows Certificate Server

> **Tip**
> The certificate can be stored on the client side and the server side in the Windows

> domain. The certificate must be on the target workstation. The certificate can be declared at the Network level.

Refer to the *Genesys 8 Security Deployment Guide* to review a detailed procedure about how to create a certificate.

Deploying certificates on a workstation

The Workspace Deployment Wizard requires you to do one of the following:

- Provide a security certificate.
- Generate a self-signed security certificate in the Workspace Deployment Wizard.

You must retain the Certificate file for all upcoming updates. If the updated version is signed by a different certificate, ClickOnce will consider it as a new installation, which means that you will have to uninstall the previous version by using `Add/Remove Programs` command *on each client workstation*.

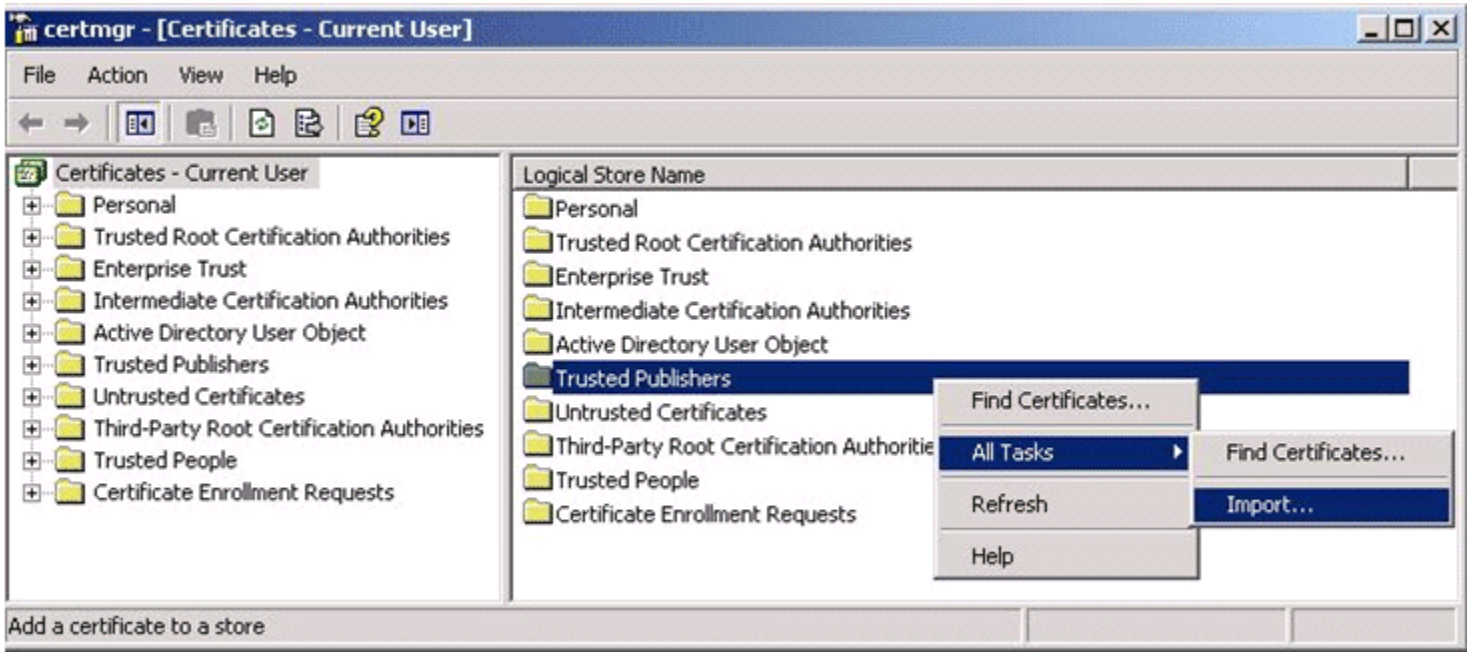
Application and deployment signing cases

The Table - **Summary of the Cases for Signing the Application and the Deployment for the Integrator and the User** provides a summary of the cases for signing the application and the deployment for the Integrator and the User, along with the impact for the user.

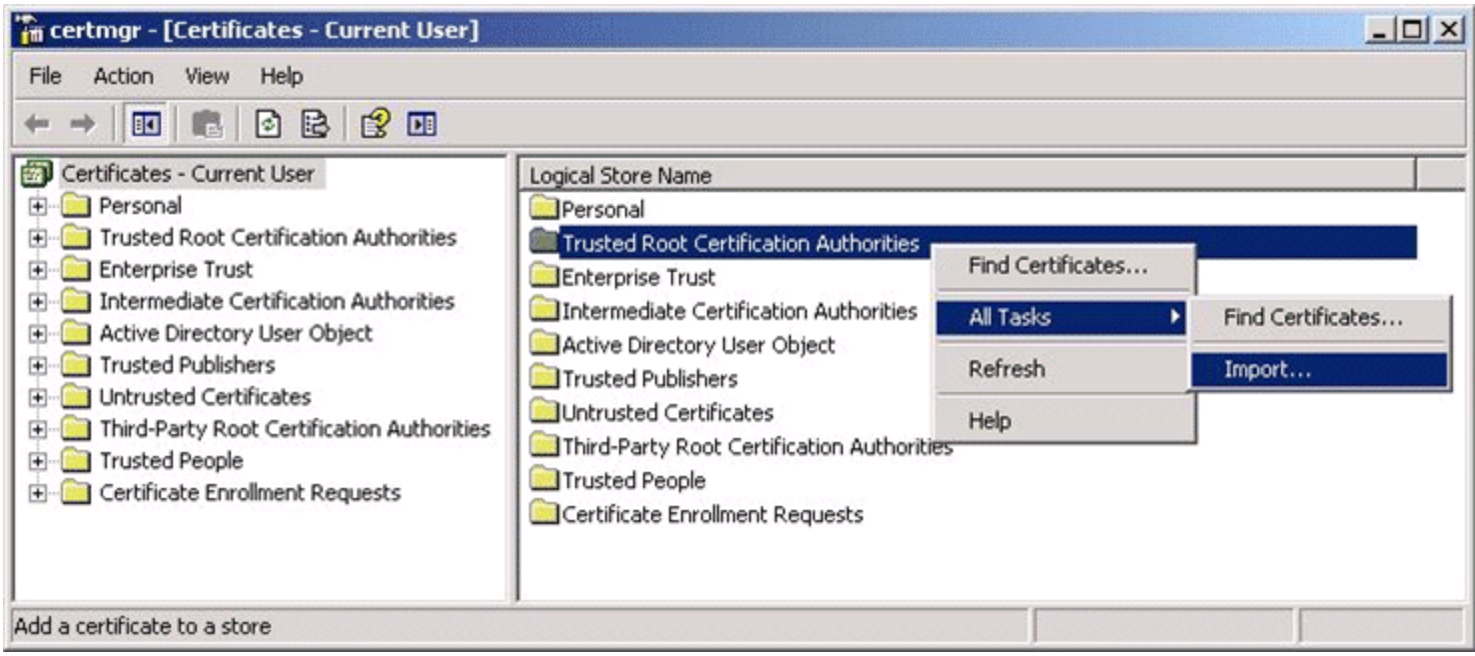
Summary of the Cases for Signing the Application and the Deployment for the Integrator and the User

	Integration	User administration	User impact
Application Verisign Certificate	Non-modifiable application		A prompt to trust the known publisher is displayed.
		Add the certificate in Trusted Publishers store (see Figure - **Importing a Trusted Publisher**).	No warning is displayed.
Application Self-Certification	Non-modifiable application		A prompt to trust the unknown publisher is displayed.
		Add the certificate in the Trusted Root Certification Authorities store (see Figure - **Importing a Trusted Root Certification Authority**) and in the Trusted Publishers store (see Figure - **Importing a Trusted Publisher**).	No warning is displayed.
Deployment Verisign Certificate	N/A	Sign the Deployment.	A prompt to trust the known publisher is

	Integration	User administration	User impact
			displayed.
		Sign the Deployment and Add the certificate in the Trusted Publishers store (see Figure - **Importing a Trusted Publisher**).	No warning is displayed.
Deployment Self-Certification	N/A	Sign the Deployment.	A prompt to trust the unknown publisher is displayed.
		Sign the Deployment and Add certificate in the Trusted Root Certification Authorities store (see Figure - **Importing a Trusted Root Certification Authority**) and in the Trusted Publishers store (see Figure - **Importing a Trusted Publisher**).	No warning is displayed.



Importing a Trusted Publisher



Importing a Trusted Root Certification Authority

Trusted publishers

For a publishers to be consider a Trusted Publisher, the following criteria must be met:

- The publisher certificate must be installed in the Trusted Publishers certificate store on the user's computer.
- The issuing authority of the publisher certificate must have its own certificate installed in the Trusted Root Certification Authorities certificate store (This is already included in Verisign).

If the issuer of the certificate is not in the Trusted Root Certification Authorities certificate store, or if the publisher is not in the Trusted Publishers certificate store, the user will be prompted with a dialog box that asks for confirmation. For more information on Trusted Publisher certificates, refer to the following article: http://msdn.microsoft.com/en-us/library/ms996418.aspx

Deploying certificates on the network

There are two methods for deploying certificates over a network to a large number of client workstations:

1. Active Directory domain
2. `certmgr.exe` tool

Active Directory domain

If you run in an Active Directory (AD) domain, use the AD Group Policy Objects (GPO) to distribute certificates centrally. For the root Certificate Authorities (CA) certificate, add a GPO to AD, and then link to the appropriate level (usually the domain level).

1. Go to: Computer Settings>Windows Settings>Security>Public Key Policies.
2. Add the root CA certificate under Trusted Root Certification Authorities.

Next you must distribute the trusted publisher. Add a GPO to AD and link at the appropriate level (usually for the organizational unit that should trust the application).

1. Go to User Settings>Windows Settings>Internet Explorer Maintenance>Security>Authenticode Settings.
2. Click Import.
3. Click Modify.
4. Enable the Lock down Trusted Publishers feature to prevent users from modifying their Trusted Publisher certificate store.

After the standard GPO-replication-to-clients occurs, every client trusts your CA and the Trusted Publisher certificate. Users will not receive Trust challenges for applications that are signed with corporate certificates. For more information on this topic, refer to the following technical article: http://msdn.microsoft.com/en-us/library/aa719097.aspx#clickonce_topic6

certmgr.exe tool

You can use the certmgr.exe tool to install the certificate on each client workstation. See the following technical article for more information: http://msdn.microsoft.com/en-us/library/ms996418.aspx#clickoncetrustpub_topic5

Modifying agent workstations

Installation of Workspace results in the following modifications to your agent workstations:

- Workspace is added to the Start menu.
- Workspace is added to the Add/Remove Programs group in the Control Panel.
- The Workspace icon is added to the desktop.
- ClickOnce stores the application binaries and associated data files in directories that it creates and manages in the user-profile Local Settings folder or other location.

To determine the folder locations at which ClickOnce has stored the application binaries, launch Workspace, and open the About dialog box from the Help menu. Press Ctrl-Click on the Genesys icon to display hidden buttons that enable you to access the exe, data, log, and GC folders.

Nothing is added to the Program Files folder or the registry. No administrative rights are required for the agent to install the application.