



Ceedo Virtualization Technology Overview

Ceedo's unique approach to application virtualization enables multiple applications to be virtualized together to create a virtual workspace that separates the applications, settings and data from the operating system, while allowing them to interact with one another.

January 2010

Table of Contents

Introduction	3
Application Installation: The Challenge	4
Approaches to Achieve 'No-Install'	5
Developing 'Portable Applications'	6
Using Application Virtualization	6
Ceedo's Approach – Application Workspace Virtualization	7
The Ceedo Technology	9
The Ceedo Virtualization Layer	10
The Virtualization Layer logic	11
The Virtual File System.....	12
The Virtual Registry	13
The Ceedo Compatibility Layer	13
The Ceedo Cross Application Bus	14
Creating a Virtual Workspace	14
Security Considerations.....	15
Summary	17

Table of Figures

Figure 1 - The Ceedo Sphere & Supported Devices	3
Figure 2 - Standard Application Virtualization	7
Figure 3 – Ceedo Workspace Virtualization.....	8
Figure 6 – a Virtual Workspace of Applications	9
Figure 4 – Standard Windows Application - Installed	10
Figure 5 – Standard Windows Application Using Ceedo's Virtualization Layer	11

Introduction

Ceedo Technologies, Ltd. has developed a technology that allows IT administrators to easily virtualize a suite of standard off-the-shelf Windows™ applications and deploy them to users' PCs. Using this technology, IT administrators can easily set-up, update and teardown Windows application environments to employees – even for home use, and for subcontractors. Within minutes, users can access an entire workspace of the applications they need and are accustomed to working with. Applications are launched from a handy launch bar or fully integrated into the user's Windows UI, as if they were actually installed on the PC.

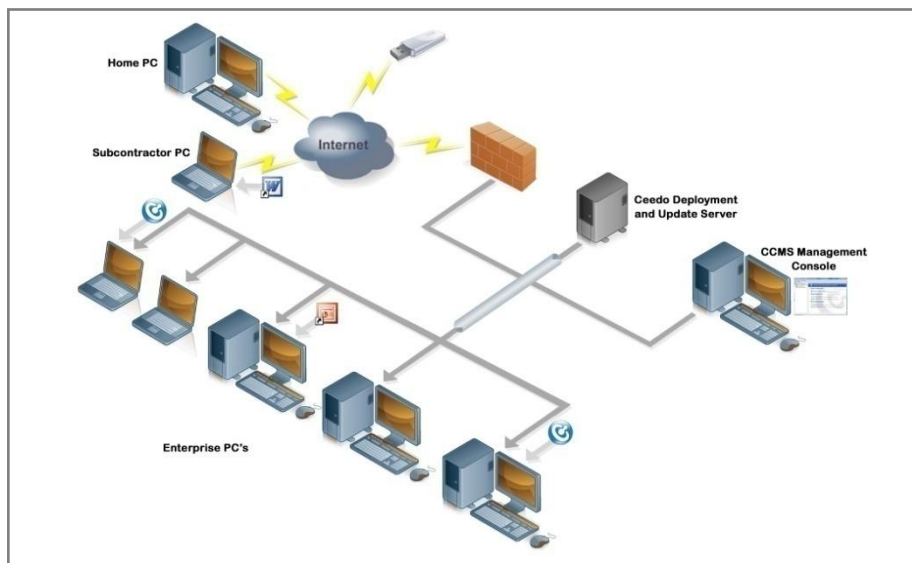


Figure 1 - The Ceedo Sphere & Supported Devices

The Ceedo virtual workspace launches on any Windows host PC without the need to pre-install software, drivers or agents. Ceedo's virtual workspace runs on top of, and leverages the existing Windows OS on the host PC. It works fully in user mode, enabling operation on locked-down PCs.

Ceedo's virtualization layer mediates between the operating system and the Ceedo-installed applications, making it possible to reinstall the operating system without having to re-install the applications, while keeping all user settings and data intact.

This process ensures business continuity during operating system migration (i.e., from Windows XP to Windows Vista, or Windows Vista to Windows 7), or during failure and disaster recovery. Using Ceedo's Client Management System (CCMS), both the Ceedo Virtualization Layer and the applications that run on top of it can be automatically updated over a LAN or WAN.

This document examines the challenges associated with Windows application management and the complexities arising from the need to install applications into the

Windows environment. Further, it details the core components of Ceedo's virtualization technology which addresses these challenges by enabling a suite of standard Windows applications to run on a host PC without installation.

Application Installation: The Challenge

Most Windows applications use the Windows persistent storage mechanism, including the Windows file system and the Windows registry to store status and settings, creating strong ties between the applications and the underlying operating system. These ties become an obstacle when there is a need to move the application to another computer, update the underlying operating system, or manage the applications remotely.

Following is a review of typical application installation requirements:

A typical Windows application requires an installation process to register and bind the application's binaries, resources and configuration to the host PC's Windows environment. The installation process usually performs the following operations:

- Copying files to the application folder (which typically resides under C:\Program Files).
- Copying files to the Windows shared folders (usually C:\Windows or C:\Program Files\Common Files).
- Registering Dynamic Link Library (DLL) files and COM objects.
- Creating application shortcuts in the Windows Start Menu.
- Storing some registration and default settings for the application in the Windows Registry.
- Preparing and registering the uninstall mechanism for uninstalling the application.
- Updating some Windows settings such as file association, automatic startup, etc.

All the information stored during the installation phase is later used by the installed application during the execution phase to ensure proper functioning of the application. When the application executes, it first confirms that all of its binaries (EXE, DLL, and OCX) have been loaded correctly. This involves checking the Program Files folders, Windows folders, COM objects (which are read through the Registry classes values), and other files. During the execution phase, a typical application routinely accesses these files and registry values, performing read and write operations.

The fact that an application must be installed on a particular operating system on a host PC in order to operate, and must be un-installed to be completely removed from the system, creates several complexities for end-users and IT managers:

- The installation process consists of several steps and is a lengthy process:
 - It requires users to wait until the installation completes prior to using the application.

- Some installations require rebooting the PC which resets the user's environment and can be disruptive to work.
- IT managers, when installing manually, waste valuable time waiting for the required set of applications to be installed on a host PC.
- When a user migrates to another computer because of a computer failure or a hardware upgrade, all of the user's applications must be re-installed on the new PC and then re-configured. This step can typically take anywhere from a few hours to a few days to complete, depending on the complexity of the configuration.
- Installed applications are not portable. Users often transfer files to a USB drive and continue to work on another PC. However, since the applications cannot be transferred and used at another location, some of the files on the USB drive may not be usable due to missing file associations.
- When an organization decides to upgrade their current Windows operating system version (i.e., migrate from Windows XP to Windows Vista, or Vista to Windows 7), it is a common best practice to perform a 'clean install' of the operating system for performance reasons. This means installing the operating system from scratch, which requires the applications to be re-installed as well. This is also the case when purchasing and deploying new PCs, typically an ongoing process in any organization.
- Since all applications use common file locations, conflicts are often created between DLLs and other application files which share the same name. Conflicts are also caused when applications require different versions of the same system resources (i.e., .NET, Java VM, etc.).
- Managing, updating and removing applications remotely by the enterprise IT department is a complex task:
 - It requires running an additional installation process with the difficulties mentioned above.
 - When regression issues are discovered on some PCs, it is difficult to undo an update. Consequently, IT managers put off updating applications.

Enabling applications to run on a host PC without requiring installation alleviates many of these issues. The end result is flexible and simplified IT processes due to the streamlining of application deployment and management.

Approaches to Achieving “No-Install”

Following are some of the conventional approaches to enable applications to run on Windows PCs without the need for installation.

Developing “Portable Applications”

One method of avoiding application installation is to re-write the application itself, in a way that will not use any Windows persistence services. Such modified applications, often called 'Portable Applications,' do not use the Windows registry, do not store files in the standard Windows folder, and do not use any 3rd party ActiveX components or COM objects.

The benefits of “Portable Applications” are:

- Applications can run without installation.
- Applications can be 'ported' from PC to PC (i.e. being able to carry them and run them directly from a USB drive).

The difficulties with this approach are:

- Modifications can only be made by the developer of the application who has access to the source code, and not by a 3rd party ISV, integrator, or the enterprise itself.
- Modifications usually require a lot of time, are expensive and are not practical for the enterprise itself unless the developer is determined to pursue this option.
- Modification requires the application developer to create propriety methods for information storage that do not depend on Windows registered resources - more time has to be spent developing, debugging and documenting these methods.
- The use of proprietary persistence services prevents the interaction between applications and operating system components in using common resources such as ActiveX controls, which lengthens development time and prevents taking advantage of improved application performance usually associated with common resources.

Using Application Virtualization

A better approach is to use virtualization technology to “tweak”the application's behavior at runtime without the need for source code modification. Virtualization is a very broad term which refers to the abstraction of computer resources. When applied to applications, virtualization means that the resources required for the application's execution are abstracted from the application itself. These resources are actually mapped onto 'virtual' resources, which are stored in a location that does not depend on, or relate to the host PC's persistent storage. This approach leaves the applications unchanged, yet independent of a particular host PC; the application can run on any PC as long as the virtual resources are available.

Standard application virtualization technology implements a virtualization layer between each application and the operating system, as illustrated in Figure 2 below.

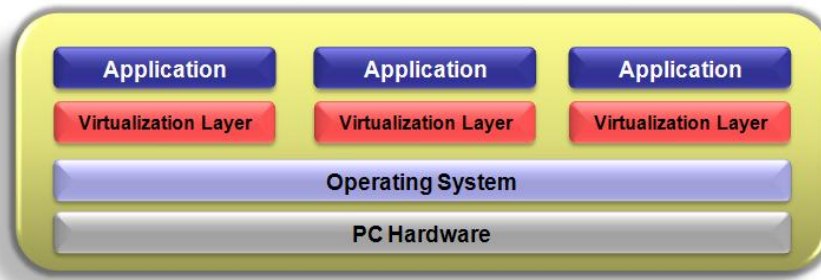


Figure 2 - Standard Application Virtualization

The benefits of standard application virtualization are:

- Applications can run without installation on the host PC and can be ported from PC to PC.
- Applications do not require modification, making the technology practical and economical for organizations allowing them to use the technology with any application.

There are two main obstacles to this approach:

- First, each virtualized application is isolated in its own 'bubble,' not only from the installed applications on the host, but also from other virtualized applications, so virtualized applications cannot interact with one another, or launch one another. This prevents application suites such as Microsoft Office, for example, from embedding an Excel worksheet in a Word document or a PowerPoint presentation.
- Second, most application virtualization solutions require an offline packaging process called 'Application Sequencing.' This process is partially manual, considered somewhat of an *art*, and does not always complete successfully, adding a degree of complexity and uncertainty to the application deployment process.

Ceedo's Approach – Application Workspace Virtualization

Ceedo has developed Workspace Virtualization, which is an enhancement of Application Virtualization. Ceedo's solution solves the application installation problem in an improved, more streamlined manner, avoiding some of the difficulties caused by standard application virtualization.

Workspace Virtualization is an extension of Application Virtualization. It virtualizes a full 'workspace' which includes several applications, application settings and user data. In the virtual workspace, applications can interact with one another, launch one another, and can have specific user settings for each application that are separate from the application itself and from the underlying operating system. Storing the user's personalized application settings and data as part of the virtualized environment enables

them to be easily moved, together with the applications themselves, to another operating system or another physical PC.

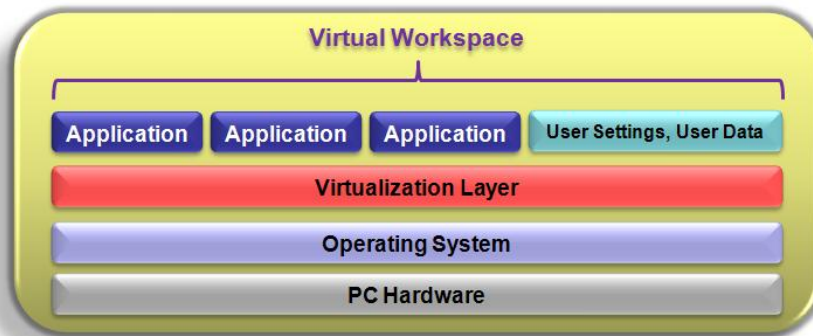


Figure 3 – Ceedo Workspace Virtualization

In contrast to Application Virtualization, Workspace Virtualization does not require an offline packaging or sequencing process. Virtualized application images are created by simply running the application's standard setup file through the Ceedo Runtime Virtualization Engine, which virtualizes the application in runtime and adds it to the workspace. After the application is added into the workspace, application plug-ins and additional applications can be added without modifying the existing applications in the workspace.

Offline virtualization and direct deployment of applications is supported as well. For deployment of applications into a workspace without running the Ceedo Runtime Virtualization Engine included in the workspace, a separate tool allows an IT administrator to use the same Runtime Virtualization Engine for a quick and simple 'offline' virtualization process. The IT administrator can then remotely add the virtualized application to workspaces that have already been deployed to a PC in the field, a network drive, or to a USB drive.

The benefits of Ceedo's Application Workspace Virtualization are:

- Applications can run without installation on the host PC and can be ported from PC to PC.
- Applications do not require modification, making the technology practical and economical for organizations since they can use the technology with any application.
- Applications can interact with one another as they typically do on Windows PCs.
- The workspace carries the user application settings; thus re-creating a user environment on a new PC becomes a very quick and simple process of moving the workspace to the new PC.

- The application virtualization process is very simple and intuitive. It can be done centrally by the IT administrator, or policy permitting, by end-users themselves

The Ceedo Technology

The Ceedo virtual workspace relies on the following capabilities to virtualize applications and allow them to seamlessly work within any Windows environment:

1. A policy-based hooking mechanism to hook API calls made by applications.
2. A dynamic context-based State Machine to determine the handling behavior for hooked API calls.
3. An alternate registry database for storing application keys and a virtual file system for storing application files and data files.
4. A compatibility layer for allowing applications to work across multiple Windows versions.
5. A cross-application bus for inter-application communications.

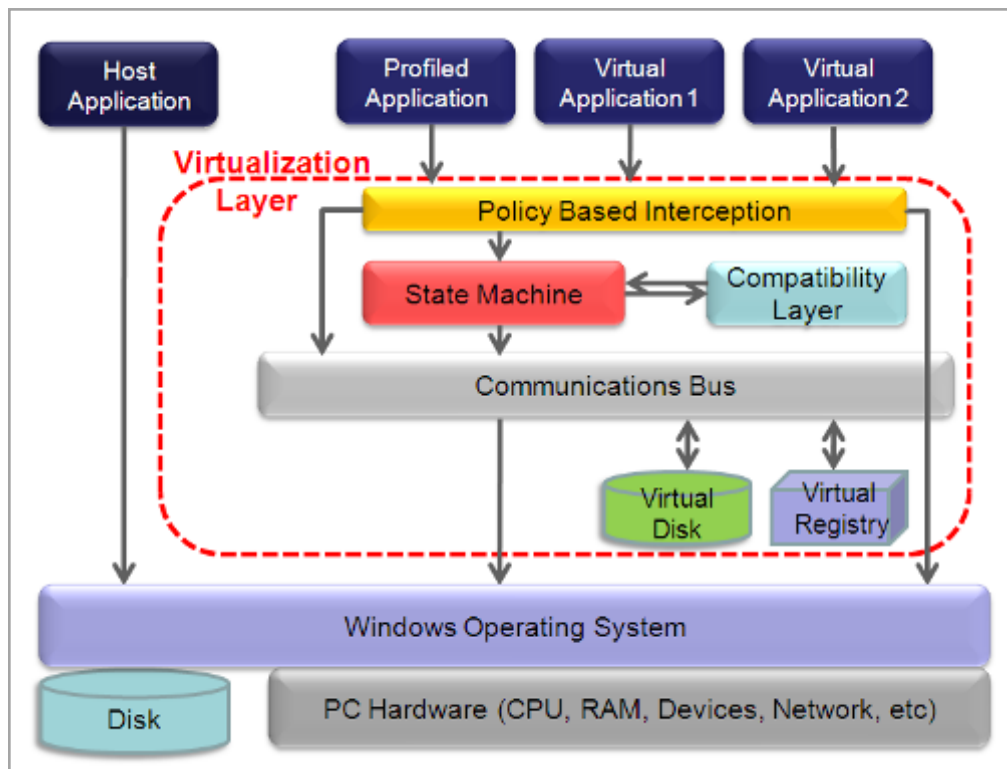


Figure 4 – a Virtual Workspace of Applications

Figure 4 illustrates how a Virtual Workspace of applications functions on a PC using Ceedo's Virtualization Layer. When the Virtual Workspace is executed on a host PC, the Ceedo Virtualization Layer is loaded into memory and is responsible for all 'behind the scenes' operations.

The Ceedo Virtualization Layer

The Ceedo Virtualization Layer is responsible for redirecting and managing the inherent ties between an installed application and the underlying operating system, and acts as a 'mini operating system' for the Virtual Workspace.

The Virtualization Layer intercepts API calls from applications to the operating system, and handles these calls according to a complex set of pre-defined rules. Win32 API calls are the 'behind the scenes' messages that applications use to communicate with the Windows operating system.

There are many types of Win32 API calls. For the purpose of this document, we will divide these into three groups:

- Registry API calls (direct registry get/set commands, DLL/COM objects registration, and more).
- File System API calls (save/load files from various operating system folders such as the C:\Windows folder, the C:\Program Files directory, user profile folders, etc.).
- Other calls (memory, processes, visual, peripherals, and many more).

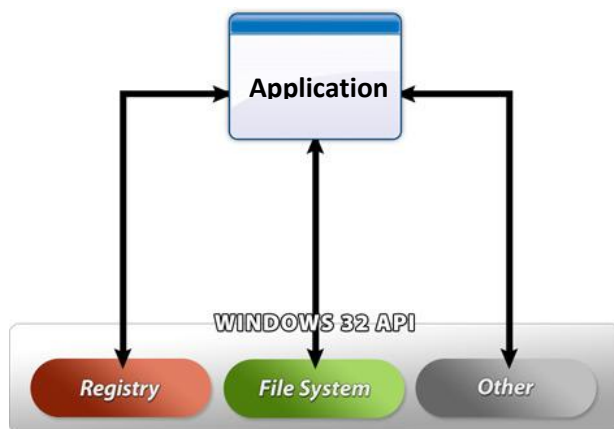


Figure 5 – Standard Windows Application - Installed

Figure 5 shows the normal behavior of a standard Windows application installed on a Windows operating system. Through Win32 API calls, the application interacts with the operating system to perform various functions.

To achieve the effect of virtualization (making the application independent from a particular PC or operating system installation), the Ceedo Virtualization Layer intercepts these API calls and changes their behavior. Intercepting API calls is performed by the Ceedo Virtualization Layer without using system drivers or services, and therefore, work will without requiring administrative privileges. This enables a Virtual Workspace to be launched by employees in an enterprise in *user mode*. For mobility solutions, this enables instant usage of a Ceedo Virtual Workspace from the Web, or from a portable drive on

public PCs at airports, Internet cafés, public schools and other remote locations, even if they are 'locked-down.'

The Virtualization Layer uses a policy developed by Ceedo to determine which API calls to intercept. API-intercepted calls for each application are determined during the application virtualization process in which the set-up of the application is used to create a virtual instance of the application, and to determine hooking for the application.

Calls that do not need to be intercepted are passed to Windows for normal handling. Intercepted calls are passed to the Ceedo Virtualization Layer for handling. The Ceedo Virtualization layer uses its State Machine to determine how to react and respond to each call.

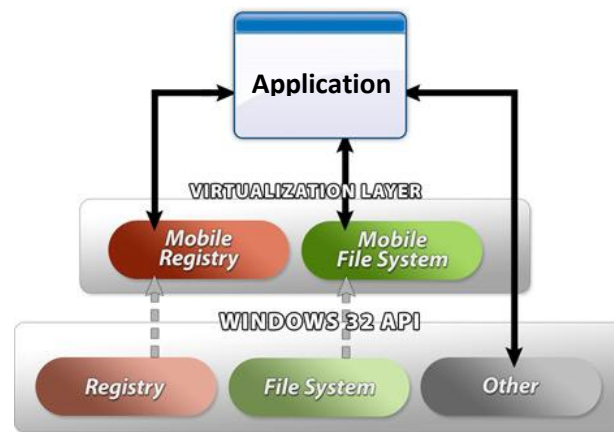


Figure 6 – Standard Windows Application Using Ceedo's Virtualization Layer

Figure 6 shows the flow of API calls from a standard Windows application intercepted by the Ceedo Virtualization Layer. The Virtualization Layer only intercepts API calls that eventually result in Windows registry or file system read or write operations while all other calls remain untouched, and are passed through to be handled directly by the underlying Windows operating system. Intercepted calls are handled internally by the Ceedo Virtualization Layer through its Virtual File System and Virtual Registry.

The end result is that the separation between the application and the operating system is achieved with very little performance overhead. It is typically about 2-3% and is not noticeable by end-users. In fact, since applications can run on 'cleaner' PCs, in reality they may actually run faster if the PC has not had many applications directly installed on it, compared to running on PCs that have many installations on them.

The Virtualization Layer logic

Ceedo uses a State Machine for receiving input from multiple API functions hooks and changing their behavior when appropriate in order to maintain a virtualization layer independent of the underlying operating system and to be transparent to the upper level applications.

The logic implemented in the Ceedo Virtualization Layer determines the result of each operation performed by the applications in the Virtual Workspace. One of the factors affecting this logic is the mode in which the application is running. The Ceedo Virtualization Layer supports two central modes: **Install Mode** and **Run Mode**.

Install Mode

The typical use of Install Mode, as the name suggests, is for installing applications into the Ceedo Virtual Workspace. Install Mode is the default execution mode of the application setup files which are activated through the Ceedo Runtime Virtualization Engine.

When in Install Mode, the Ceedo Virtualization Layer limits the exposure of the application to resources that exist on the PC, so the application will not depend on these resources when it executes, and to ensure the setup installs all required components for the application to function into the virtual environment.

For example, if an application setup needs to copy a DLL to the Windows System folder, and first checks if that DLL already exists, the Ceedo Virtualization Layer will hide the existence of the DLL from the application setup, to ensure it will be copied to the Virtual File System by the setup program. This guarantees the DLL will always be available to the application, even if it is running on a different PC where the DLL does not exist.

Run Mode

When in Run Mode, the Ceedo Virtualization Layer allows some utilization of the host PC resources, ensuring that this utilization is carried out in read-only mode. In Run Mode application requests to components and read requests of attribute values from the host PC are granted. This ensures the proper operation of applications, and allows utilization of resources or other applications that are installed on the host PC. For example, it permits the user the utilization of DirectX hardware resources from the host PC when running graphic-intensive applications. This allows optimization of resource usage and excellent performance of the virtualized applications.

The Virtual File System

The Ceedo platform maintains a Virtual File System, which is designed to mimic the structure of the Windows file system. It provides the pre-defined environment that Windows applications and installers expect to find, so applications running over the Ceedo Virtualization Layer perceive the Ceedo Virtual File System as if it were a part of the host machine's file system.

The Ceedo Virtual File System can be listed, read, written to, or loaded. Equally, files from the host's file system can be listed, read and loaded, however, they cannot be written to. If the Ceedo virtualization engine detects an application call to create a file or open a file for writing, the engine will redirect the call to a file on the Virtual File System instead of a file located in the host PC's file system. This creates a 'sandbox,' ensuring

that any changes remain within the confines of the Virtual File System, making the workspace private and secure since no information is written to the host PC's permanent storage.

The Ceedo Virtualization Layer uses the Virtual File System intensively. When an application is installed by running its setup file through the Ceedo Runtime Virtualization Engine, all files are written to the Virtual File System. During the execution phase of an application, when an application requests loading a DLL, the Ceedo Virtualization Layer first searches the Virtual File System, and if it exists, loads the DLL.

If the DLL does not exist in the Virtual File System and the IT security policy permits it, the DLL can be loaded from the host PC's file system. This ensures that the application can work anywhere without actually being installed locally, as the Virtual File System carries all its resources. Further, it allows applications to utilize common Windows components, or alternatively, use some of the host PC's resources (printers, Internet connection, etc.).

The Virtual Registry

The Ceedo Virtual Registry is somewhat similar in operation to the Virtual File System. Through the Ceedo Virtualization Layer, applications can only read values from the host PC's registry, while all write operations are performed only to the Ceedo Virtual Registry. Similar to the Virtual File System, if the Ceedo Virtualization Layer intercepts a call to retrieve a registry value, it first searches for that value in the Ceedo Virtual Registry, and returns the value if it exists. If the value does not exist in the Ceedo Virtual Registry, a complex set of rules is applied to determine if the Ceedo Virtualization Layer will search for that value in the host PC's registry.

These rules take into account the type of the value (application value, Windows value, Internet Explorer value, etc.) and the mode the application is running in. If the Ceedo Virtualization Layer determines that it needs to search the host PC's Registry, it will do so, and if the value exists, it will be returned to the application. Otherwise, the reply to the application will be 'value not found.' The writing mechanism is less complicated, since all registry keys are written to the Ceedo Virtual Registry. This ensures that all of the data the application has written to the registry is stored and is accessible within the Ceedo Virtual Workspace.

The Ceedo Compatibility Layer

The Ceedo compatibility layer allows moving virtual applications smoothly between different versions of the Windows operating system. This layer allows applications to function across operating system versions by exposing the same API and behavior expected by each application, regardless of the underlying operating system it is currently running on.

This is done by abstracting assembly stores, system environment variables, services handling mechanisms, OS internal techniques, special folders, and additional items from

the application. The end result is that an application installed on Windows XP, for example, and moved to Windows Vista, will continue functioning as if it is running on Windows XP. Ceedo will translate all variables and operations to appear as if they are occurring on Windows XP; this is what allows the application to function in such a case. The same methods apply for running across versions of Windows 2000, Windows XP, Windows Vista, Windows 2003 and Windows 2008 servers.

In essence, the compatibility layer hides the real operating system from the applications and presents the expected operating system façade to the application, allowing it to correctly interact with it. The compatibility layer acts as a translator between the language of the expected operating system calls and the actual operating system present.

Using the compatibility layer, Ceedo allows the virtualizing of an application by the IT administrator, and then deploying it to any Windows operating system used within the organization or outside of it.

It allows for:

- High flexibility of usage of software resources within or outside an organization.
- Makes upgrading operating systems simpler due to the ease of porting the user applications and environment between them.
- Enhances forward compatibility of applications. For example, many applications compatible with Windows XP but not with Windows Vista, can work on Windows Vista after being virtualized by Ceedo.

The Ceedo Cross Application Bus

The Ceedo cross-application bus allows for inter-application communications. It allows virtual applications to interact as if they were actually installed on the Windows operating system. It also allows the virtual applications to interact with the installed applications on the PC.

During setup time of an application, the cross-application bus manages all the registrations required by standard applications to connect to Windows and provide information to other applications.

During run time, the cross-application bus reacts to application requests, finds the requested information, and provides it to applications. It allows applications, for example, to use a COM object added by another application, even one residing on the PC itself, if the Ceedo policy allows for its use.

Creating a Virtual Workspace

By virtualizing a full suite of standard Windows applications, the Ceedo Virtualization Layer creates an integrated Virtual Workspace of applications that is detached from the PC. Since the Ceedo Virtualization Layer presents the same Virtual File System and

Virtual Registry to all applications running on top it, the applications can recognize and interact with one another.

For example, if Adobe Acrobat Reader is installed in Ceedo, all other applications installed in Ceedo will be able to use Acrobat freely, and PDF files will be automatically associated with the Acrobat application within the Ceedo Virtual Workspace. Similarly, if the user receives an email with a link to a website and a browser is installed in the Ceedo Virtual Workspace, the Ceedo Virtualization Layer will ensure the e-mail application recognizes that browser, and clicking the link in the e-mail will launch the Virtual Workspace browser application instead of the browser installed on the host PC.

In addition, due to the request fall-through ability of the virtualization layer, applications can access locally installed resources and applications on the PC. This allows the virtual applications to function and behave as if they were actually installed on the host PC.

In reference to the example above, if a guest application needs to open a PDF file, the Ceedo Virtualization Layer first searches the virtual registry to verify if another guest application is registered to handle PDF files (through the virtual file associations list) exists. If such an application is found, the Ceedo Virtualization Layer will launch it to open the PDF file. If not, the Ceedo Virtualization Layer, policy permitting, will transparently search for such an application on the host PC, and if detected, will launch that application from the host PC. At the same time, the host PC remains fully-functional and is able to execute applications installed locally.

Security Considerations

A Windows PC is an inherently insecure environment. It is susceptible to attack by malware that can corrupt applications and compromise confidential data. To effectively deal with PC security issues, Enterprise IT typically maintains a homogenous, locked-down PC environment at the cost of severely limiting user flexibility and customization.

Ceedo's philosophy is to preserve user flexibility and allow the user to securely run a centrally managed set of rich client applications on a PC that is not under the physical control of the Enterprise. Ceedo has partnered with leading security vendors to implement layers of security that enable deploying and running a Ceedo workspace with a high degree of security.

- **Physical device security** – For a customer who wants to run a Ceedo Workspace from an external, USB storage device, Ceedo has partnered with device vendors such as SafeNet/Aladdin, SanDisk, IronKey, and others whose devices can be deactivated in the event of loss or theft. In addition to requiring user credentials to launch the Application Workspace, a time-based policy can be implemented from within the Ceedo workspace to automatically initiate lock down if a certain time period has elapsed in which the device has not done an online validation ping. Devices that have been tested with Ceedo also include a feature that will automatically lock down or initiate a self-destruct sequence if a certain number of unauthorized or invalid logon attempts have been exceeded.

- **Data encryption** – All or part of a Ceedo environment can be encrypted using the most advanced available hardware and/or software-based encryption technologies such as 128 or 256 bit AES encryption. Especially when using hardware-based encryption, decryption keys are safeguarded, and the entire environment is isolated from potential OS security flaws of a host PC.
- **Environment security** – The Ceedo environment can be readily configured to protect against malware intrusion into the Ceedo environment by user actions such as e-mail and browsing, or from the host PC on which the Ceedo environment is run, host PC validation prior to running the workspace. When started, the Ceedo client will verify that the host PC is running an up-to-date antivirus and operating system before being allowed to run.
- **Isolation from host** – The Ceedo workspace can be isolated from the host PC on which it is running so that all data is written to the Ceedo workspace and not to the host PC, thereby preventing unintended leaking of information. This includes writing by applications of which the user is often unaware, such as history, log files, cookies, temporary files and other information that can be used to identify or track a user. In this manner, both actions by the user, such as saving files, and underlying writing actions by applications, all remain in the workspace. In addition, Ceedo can be configured to stop a user from saving information to the host PC from any applications running inside the workspace.
- **User authentication (2-factor, OTP)** – Enterprises use various means of user authentication to support usage scenarios both within and outside of corporate office locations. Effective use of sophisticated user-authentication technology such as one-time passwords (OTPs), USB tokens and public key infrastructure (PKI) is often effectively limited by the need for installation and configuration on the user's PC, and the resulting support overhead. With Ceedo, robust user-authentication can be implemented as part of the Ceedo workspace and launched on any host PC where the workspace is run. Within the Ceedo workspace, the various means of authentication can be tightly coupled 2-factor authentication, allowing use of tokens, digital signatures and certificates as security underpinning for secure email, browsing, and other applications, in a manner that is almost transparent to the end user.
- **Encrypted communications** – For highly mobile workers and business partners, secure access to corporate resources is a threshold requirement. A Ceedo workspace supports configuration with industry-standard, virtual private network (VPN) technology to ensure the security of all communications. As with all resources implemented in a Ceedo environment, the VPN can be tested in an offline scenario so that when the production Ceedo workspace image is deployed to the end-user, no further configuration or support is required.

Summary

Throughout this document we have seen the many challenges faced by today's IT departments created by the need for application installation. Ceedo's virtualization technology provides a unique solution to meet these challenges by allowing IT administrators to quickly and easily deploy and mobilize applications suites and later update them without the need for installation. This simplifies by an order of magnitude the complexities of managing PCs and allows for new usages of PCs and applications.

With the implementation of various layers of security, the Ceedo workspace affords the end-user and the enterprise a full set of applications tightly coupled with industry-standards information security. Ceedo's technology enables this marked improvement by using virtualization and remote management capabilities to address these IT issues.

In this document, we have delved into the virtualization segment of Ceedo's technology, which is the basis of making this possible. Ceedo's virtualization technology allows the virtualization of a full suite of standard, off-the-shelf Windows applications, and full interaction between the applications. Ceedo's virtualization technology does not require a complex application sequencing process, and fully works in user mode, allowing it to be seamlessly deployed and run on any PC, including locked-down PCs.

The future is clear – virtualization technology will improve the way we work and the IT processes we rely on. Ceedo's virtualization products aim at making this future possible today. Ceedo's products provide IT administrators with cost-effective PC management solutions for office and employee home-office environments.

Market proven, Ceedo's virtualization technology has already been deployed to over four million users worldwide, successfully creating the ultimate managed virtual workspace.

To learn more, visit our website at www.ceedo.com.