Realtime
publishers

The Shortcut Guide[tm] *To*

User Workspace Management

sponsored by

RES
software

Greg Shields

Realtime
publishers

Copyright Statement

Realtime
publishers

Chapter 2: Personalization Equals Content + Context

I spent time today walking the hallways of a business not unlike your own. In its rows of cubicle walls, grey-and-blue color schemes, and ergonomic furniture, I found hundreds of different computers. Laptops, desktops, monitors both CRT and LCD, printers and peripherals, even a few mobile devices—room after room of equipment that enables this business to function.

And as I was walking through those hallways, the IT professional in me took over by default. My inner IT pro pondered the administrative work required to support each piece of equipment. Each requires an operating system (OS), patching, applications and updates, along with the occasional troubleshooting and technical support. Accomplishing each of these tasks requires smart thinking paired with software solutions.

That business was full of equipment that enables it to operate, but at the same time, the equipment itself requires special care and feeding. In the end, that's our job in IT: managing the special care and feeding of all that equipment. Systems administration is what we think about when we get up in the morning, and it's the last thing on our minds as we drift off to sleep. We live, eat, and breathe technology along with technology's "equipment."

And then I paused for a minute, and found myself pondering not the equipment but instead the people. For a moment I stopped thinking of those laptops and desktops with my IT professional's eye. I stopped thinking of that equipment as *equipment*, and instead considered it as do the people who use it: To everyone else in the business, t*hat equipment is merely an extension of their job role.*

Suddenly, the culture of business outside the walls of IT became clear. We in IT are programmed to think of the equipment we manage as problems to be solved—devices to which we apply troubleshooting support. But to the rest of the business' employees, that equipment is an extension of themselves. They use their desktops to communicate with customers and business partners, write memos, and draw up spreadsheets. They lug their laptop through airports to present at meetings and conferences. They think of printers not as devices in need of toner and IP addresses; rather, the printer enables them to convert soft copy documents to hard for sharing with others.

It was then that I realized the crucial component in this serendipity: With everyone else in our business, *it's the personality that matters*. Lacking personality, that computer becomes little more than a strange device they don't understand. Lacking personality, users don't know how to interact with their equipment or they fear even touching it. Without a personality, their computers become objects for your IT group to deal with and cease being personal.

The Misalignment Between IT and Users

There's a misalignment between IT and users in many companies. In these businesses, the IT organization sees itself as a technology-first group of people. Their mission is to ensure consistent and secure access to applications and data. When servers or desktops experience a problem, IT is the group called in to work the fix. IT's success in these companies is usually measured by the number of work orders they close each month or how many days they can operate without a major outage.

This focus is critically important. Desktops and servers that go down absolutely impact the functionality of business, as do applications that break when they aren't updated or patched appropriately. But it is exactly this equipment-centric focus that brings its own set of problems.

Consider my frustration in Chapter 1's first few pages. There, I explained the problems I experienced in upgrading just a single workstation from Windows Vista to Windows 7. Upgrading the OS was a simple process, taking only about 30 minutes and zero effort. But transferring over the user's personal information—their desktop shortcuts, important files, browser bookmarks, and the like—consumed another three-and-a-half hours.

That user's personal files may have been of little importance to me; my task was merely to upgrade their desktop. And yet to the user, *those personal files are worth substantially more than any new OS.* If that user can't find the shortcut to their accounting spreadsheet or their connection to the office printer, a new OS does them little good. And, in fact, the new OS might actually hinder their ability to do their job.

That's why personality—and the preservation of personality, no matter how our users might connect—is so incredibly important. Users in a business must be able to accomplish their given job. And no matter how many newfangled access methods we create to connect users to applications and data, *no solution is complete without considering the user's workspace.* Elevating this consideration from an afterthought to one of primary importance is the first step in eliminating the misalignment between IT and users.

Defining Personalization

This realization is perfectly positioned for this guide's discussion on User Workspace Management. Personalization and the preservation of personalization across access methods effectively represent a central tenet of User Workspace Management. The practices and software solutions that fulfill User Workspace Management are primarily laid into place to ensure that personality is seamlessly delivered no matter how that user might connect. Chapter 1 discussed some of the mechanics of how this might work, with a further discussion to occur later in this chapter.

Where Chapter 1 left off was in the explanation of personalization itself. Put simply, personalization is about *getting the right content to the right people in the right circumstances*. This definition is exceptionally precise in the way it describes such a system. To help you better understand, let's deconstruct each of its salient points in the following sections.

The Right Content

Digging under the covers of the Windows OS, you'll find thousands (if not more) of different configurations that aggregate to create a personalized desktop. These thousands of configurations, as shown in Figure 2.1, represent printers, desktop, bookmarks, network configurations, personal files and folders, and even application settings. All of these individual personality configurations represent the content that a user expects to be present on their computer when they log in.
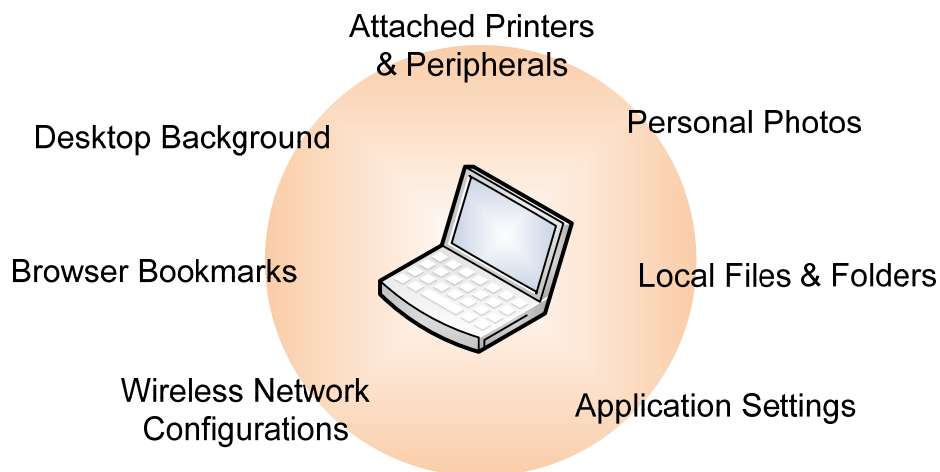
Figure 2.1: There are many configurations that combine to create personality.

The "personal" in this content's personalization stems from the fact that each of these settings tends to be uniquely created by each individual user. As such, each user will realize a different set of settings as they organically construct their workspace over time.

Think for a minute about the different workspaces you might see today in your own computing environment. As you walk through the hallways of your business, you might see one user with a solid red background. Another might display a picture of that user's children. Look at the composition of any two desktops and you'll see a different set of icons, a few of which are positioned there by IT but most which have been created by the individual user.

Those substantial differences between each user's workspace are what make the computer comfortable to work with. For example, every time that John uses the link on his desktop to find his spreadsheet, he grows just a bit more comfortable with doing his job. Every time that Jane double-clicks Microsoft Outlook, she knows that it is already populated with the correct configuration and will quickly bring forth her email.

Yet those substantial differences also pose a problem to the unprepared IT organization. The collection of individual user settings can be spread across many locations on that computer. They're stored in files, within the registry, even within Active Directory (AD) itself. This spread of configurations across multiple applications and data structures makes capturing the data challenging. *Essentially, without a very smart system, you'll never be able to decouple the environment in the ways that Chapter 1's promising mobility requires.*

> **You Could Script This, But…**
>
> You might be thinking to yourself at this point, "The number of places where users store their data isn't all that large. I could create a script to accomplish this data gathering." Absolutely, you could, but would you want to?
>
> There are long-term risks in custom script creation not considered by many IT professionals as they choose to build solutions themselves. First, although collecting this data may be easy, the repositioning of it onto replacement equipment is much more difficult. Managing and maintaining custom scripts over time can itself be a full-time job. Changes to OSs and applications require extra effort. All of these combine to create a situation where a well-meaning script creator finds themselves in support of a fully-fledged application.
>
> Further, as you'll discover in a minute, there is more to personality management than simple migration from one access point to another. A true User Workspace Management solution will also include administrative toolsets that enable IT control over portions of personality, while others are left to users. Accomplishing that requires far more than any simple script.

That's why User Workspace Management solutions become such useful tools for the aligned IT organization. These solutions have been built with the logic to seek out and capture each user's personal information from across the many locations where it can be stored. Different than a "profile," where presence or absence of user data is an all-or-nothing thing, User Workspace Management solutions granularly capture and deliver the right content to wherever it is needed.

The Right People

And yet "the right content" is only the first step, because a fully-unmanaged environment presents its own set of problems. Think about what can happen when your users' content is left completely to their own decisions. Such a practice unnecessarily exposes the environment to risk.

This chapter has talked about the need for user workspace preservation no matter what the access point. But what if those configurations are inappropriate or even dangerous to the business computing infrastructure? What if some outside force, such as malware or an ill-informed user, has configured their computer in a way that hurts themselves and the business rather than helping it?

It is because of these problematic situations that most IT environments choose to proactively manage personality in some way. When IT can prevent certain applications from installing, they at the same time protect themselves against licensing violations and the introduction of bad code. When IT creates a baseline for application settings or customizes application settings for each individual user, they at the same time enforce corporate policies for the protection of the environment. Each of these proactive management elements are laid into place to ensure that the right people are interacting with the right content.

The problem with traditional approaches to proactive management stems from the nature of policies themselves. Due to limitations in how policies can be applied and enforced, many IT organizations that want to control certain elements of personality ultimately find themselves forced to control all elements of personality. In order to ensure that desktops have the right software, IT must itself do all the installing. In order to protect desktops from bad personality configurations, IT must enforce settings that cannot be overwritten. Although the net result is a more-secured environment, *it is at the same time a more-sterile environment, devoid of all the elements that make the computer personal and comfortable.*

Delivering the right content to the right people requires a solution that splits the control of personality elements. On one side are the individual users and their settings. On the other sits the IT organization and the business, each with its own charter and set of policies to be enforced. An effective User Workspace Management solution should, like what is shown in Figure 2.2, enable the configuration of a desktop and its applications to be divided in some way between these two groups.
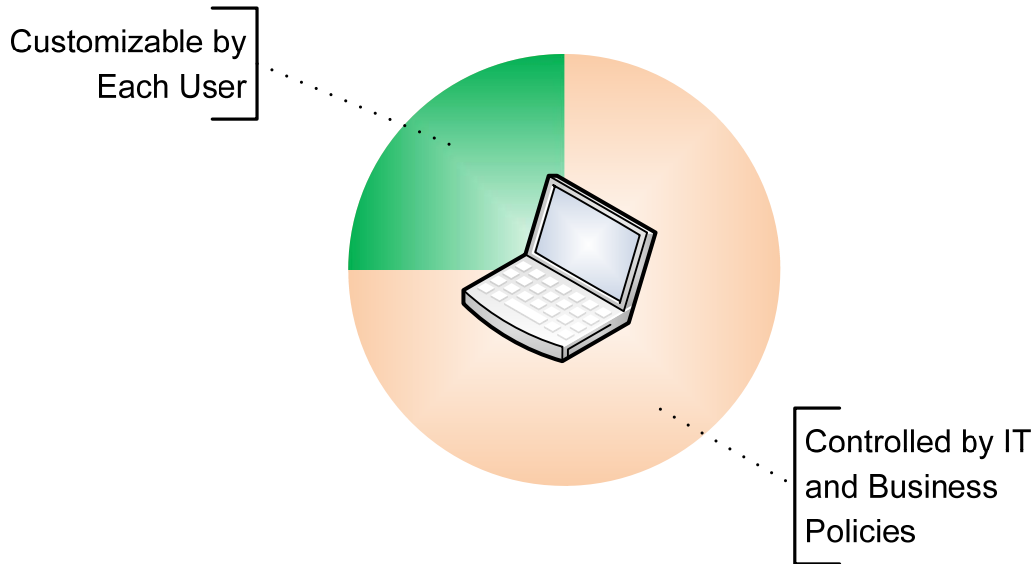
Figure 2.2: Today's computing environments require a split of control between those that are customizable by the user and others that are defined by IT and business policies.

Consider how this separation of responsibility might improve your environment:

- Users can be given the ability to adjust their desktop settings but are prevented from modifying security settings.

- Users can be given the ability to adjust configurations for Microsoft Word and Office, while those for Microsoft Outlook are defined by IT.

- Users can be given the ability to install applications but only those that have been prepackaged and made available by the IT organization.

- Different users can be assigned different application configurations based on a combination of who they are along with established IT policy.

Building an environment like these enables IT to maintain the necessary lockdowns that prevent data disclosure, theft, or loss. At the same time, users are also given the ability to personalize their desktops as they see fit.

The Right Circumstances

Completing this chapter's definition of personality is the recognition that certain content also only makes sense within the right context. Like a joke at a funeral or a comic strip on the front page of the paper, sometimes content doesn't make sense or is inappropriate based on the circumstances of its consumer.

This idea of "circumstances" is based on the recognition that personalization is really the intersection of content plus context (see Figure 2.3). As discussed in the previous section, that context can be based on the individual.

Personalization is
Delivering
Context-appropriate
Content

Content

User
Workspace
Management

Context   Security
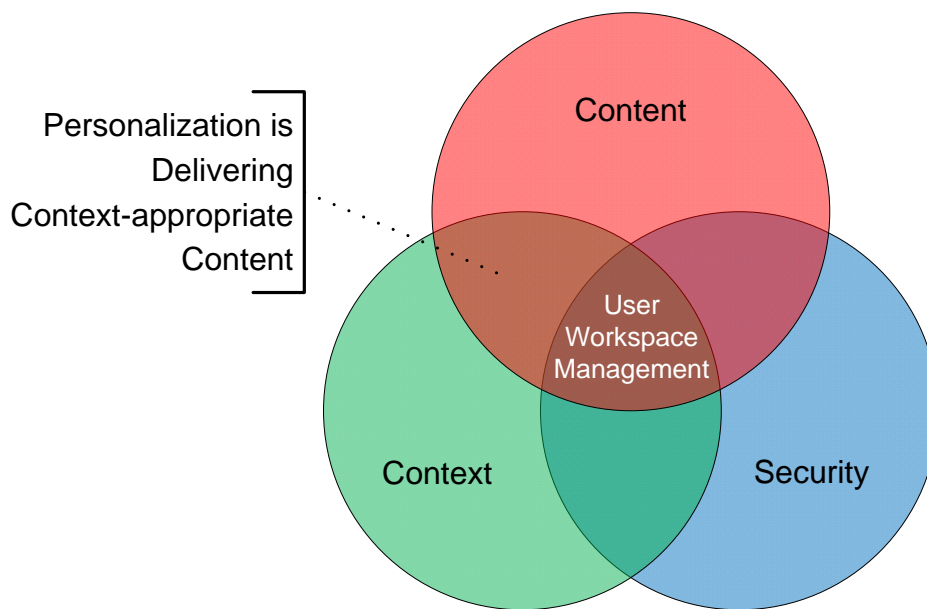
Figure 2.3: Personalization is the intersection of content and context.

For example, Bob the Accountant should get a set of configurations simply because he is Bob and because he is also an accountant. Who Bob is determines some level of how his workspace is managed. But "who Bob is" only defines one of the two important things about Bob's connection to the office network today. *The other part can be simply described as "where Bob is."* Think for a minute about how this second factor could be addressed. You'll find that there are a number of elements that could describe where Bob is.

Bob's Location

If Bob is connecting to the environment from within the environment, it can be reasonably assumed that he is using a protected connection. Thus, by connecting from his desktop computer, IT can enable the highest level of access to applications and data. Conversely, if Bob connects via Remote Desktop Services or Citrix XenApp from his home computer, that location is fully-unprotected. IT should be able to restrict the applications and data to which Bob has access.

Yet these two situations represent only the two opposites of locations where Bob could connect. What if he's connecting via a conference room or a kiosk computer in the lunchroom? Should these partially-protected locations get special restrictions as well? A well-designed User Workspace Management solution will be able to granularly define which settings Bob should get based on the location from which Bob connects.

Bob's Device

Making decisions based strictly on Bob's location only partially defines his context. For example, how should IT configure Bob's experience when he logs in from his company-supplied laptop but via his home network connection? Should the content that is delivered to Bob's connection be different than if his connection is from his uncontrolled home computer?

How do any of these decisions change when Bob's device is not a physical device but a logical one? If Bob is connecting via Remote Desktop Services or Citrix XenApp, should he get a different level of resource access than if he uses a VPN client? Further, should Bob's hosted virtual desktop via Citrix XenDesktop or VMware View get a completely different configuration than any of the previously mentioned scenarios?

Other classes of devices have even more special requirements. Consider today's proliferation of enterprise-worthy mobile devices. With these, should Bob's configuration be adjusted further to support the capabilities of these devices? As these devices are more likely to be lost or stolen, should Bob be given more limited access to data? Can Bob's connection be reconfigured such that the device retains no data whatsoever? For all of these questions, likely the answer is "yes."

When Bob Connects

Each of these are questions that must be answered to fully construct Bob's context. Yet a third element might need to be included in the calculation as well: *When is Bob connecting?* Here, should Bob's connection be adjusted for the times of day when Bob really shouldn't be attaching to work. Should applications that need special administrative access be restricted from Bob during the evening hours?

A User Workspace Management solution that provides time-of-day manipulations can also be a handy solution for IT. Such a solution can enable IT to perform maintenance on portions of the IT environment, all the while seamlessly repositioning incoming user connections to alternative hardware, connection mediums, or servers. The net result is a reduced sense of downtime, with downed services being seamlessly fulfilled through surviving alternatives.

In any of these situations, the "when" that is associated with Bob's connection can have a dramatic difference on the resources he is given. To be fully functional for these requirements, your chosen User Workspace Management solution should include the support for time-based configuration decisions.

Summing it Up

When you start summing up all of the above intersections, getting the right content to the right people in the right circumstances delivers some very interesting advantages to the IT environment. Consider a few of the following situations that result from the deployment of an effective User Workspace Management solution:

- Jane is allowed to manage her wireless settings while out of the office, and those same settings are defined while she's within the LAN. Her settings can be automatically configured to the proper settings for her local wireless LAN, no matter which building she's in.

- The configuration of Brian's hosted virtual desktop can be locked down much tighter than his primary desktop. With many virtual desktops sharing the same physical host, this extra lockdown ensures that IT gets greater virtual machine consolidation.

- Eloise's laptop needs to interact with her business' Exchange server both when she's in the office and on the road. That configuration can be automatically and seamlessly adjusted as her network connection changes to ensure she's always in contact with her email.

- Dan is promoted from Call Center Phone Operator to Call Center Manager, an activity that happens often with the high turnover rate of employees. He is immediately granted access to the set of restricted Manager applications simply by adding him to a new group.

The Power of Pervasive

We're not done yet. All of this capacity for managed and semi-managed personalization only works when it can be applied everywhere. It is for this reason that you will often see the buzzword *pervasive personalization* tagged to User Workstation Management solutions. Although you might scoff at the buzzwords as simple marketing material, in actuality, this term well describes the tactics that smart solutions in this space are using today.

The "pervasive" in pervasive personality describes the fact that a well-designed User Workspace Management solution must be able to deliver personality everywhere. No matter if you're using traditional desktops, server-based computing, hosted virtual desktops, or any combination thereof, such a solution must seamlessly flow the user's workspace across each technology.

This statement means that a User Workspace Management solution has a big role to fill. Think for a minute about the different mechanisms IT has at its disposal to connect users with their applications and data. For example, consider Figure 2.4—these *workspace delivery systems* can run atop many different software platforms.
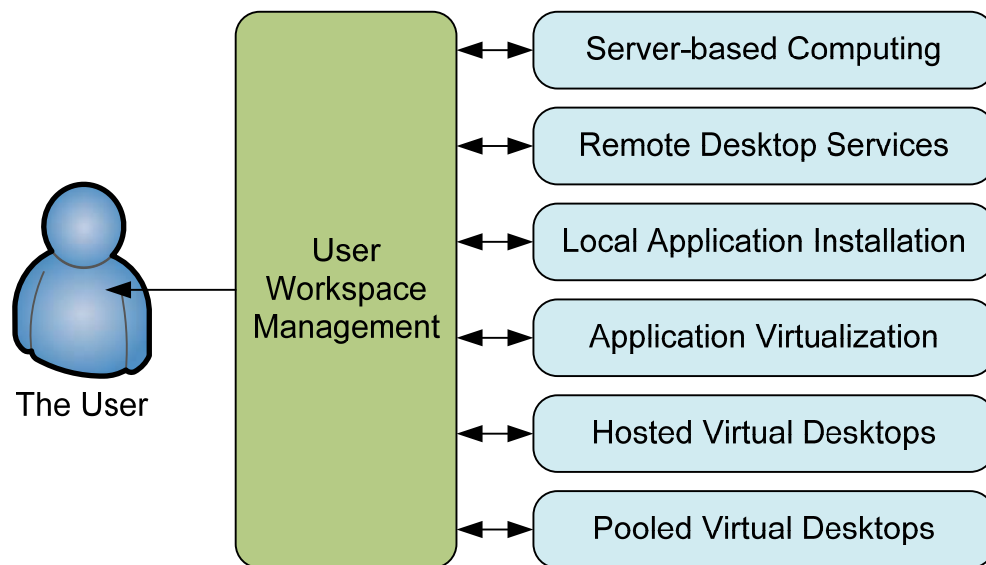
Figure 2.4: An effective User Workspace Management solution can sit in front of any workspace delivery system.

Server-Based Computing and Remote Desktop Services

Server-based computing and Remote Desktop Services use session-based architectures to enable multiple users to share resources on the same server. Microsoft's Terminal Services and Remote Desktop Services, as well as Citrix's XenApp, are three of the primary examples in use today. These technologies can deliver either a single application or a full desktop to connecting users. Here, a user's workspace can be delivered to the session as it is created when the user logs in.

Local Application Installation

In combination with an automated application installation solution, prepackaged applications can be made available for automatic installation by users when needed. Users based on their role and requirements can be assigned applications—along with their associated customizations—which follow them across the desktops they use.

Application Virtualization

Superior to local application installation is the ability to decouple and encapsulate applications from the OS entirely. This process is at a high level similar to the kind of decoupling and encapsulation that User Workspace Management accomplishes with user personality. Different here is that the applications themselves are just-in-time delivered to users as they are needed, negating the need for manual effort by IT.

Hosted Virtual Desktops

Also referred to as VDI environments, hosted virtual desktops commonly link users to specific virtualized desktops that reside within the data center. By virtualizing the desktop, users can effectively access that desktop from anywhere, while IT gains greater control over its security and configuration. Here, user personality can be highly managed to ensure resources are not oversubscribed and virtual desktops interact appropriately with each other.

Pooled Virtual Desktops

Similar to hosted virtual desktops, pooled virtual desktops instead connect users randomly to a pool of available and similarly-configured desktops. Here is where user personality delivery can bring great value, with applications, customizations, and data just-in-time applied to a generic OS instance as the user logs in. Once the user is finished with their session, those settings can be returned to a database for later distribution.


Creating Pervasive Personalization

Every business today leverages at least one of the above six infrastructures. Even the most nascent of businesses tends to start with traditional desktops that are configured through local software installation. Those with greater levels of IT maturity find themselves eventually adding other technologies to extend application and data access or to improve the delivery of services. Evolving through server-based computing, virtual desktops, and application virtualization architectures, businesses today often find themselves supporting many access points all at once.

Consider how these access points create complexities in some areas while they reduce complexity in others. For example, perhaps a business has determined that it needs to enable access to a set of applications over the Internet. Some of those applications function well atop Microsoft's Remote Desktop Services. Other applications, for reasons of performance or incompatibility, don't work well within this technology's session-based architecture. For the company's second set of applications, a deployment to pooled virtual desktops is necessary to get around the incompatibilities.

Environments like this with multiple access points are common. The workflow of a business creates the need for application and data access through multiple technology architectures. The problem, however, in being successful with this everything-for-everyone mindset has been in synchronizing the requisite personality information.

The solution for this problem occurs when a User Workspace Management solution is laid in front of each technology architecture. Figure 2.5 shows the use case for this architecture in relation to this section's example. Here, the user needs to access Application A atop Remote Desktop Services technology. That same user needs to simultaneously access Application B atop a pooled virtual desktop. Lacking a User Workspace Management solution, that user would be forced to re-create their workspace with each new access point. Conversely, with a centralized User Workspace Management solution in place, personality information is seamlessly synchronized between the two connections.
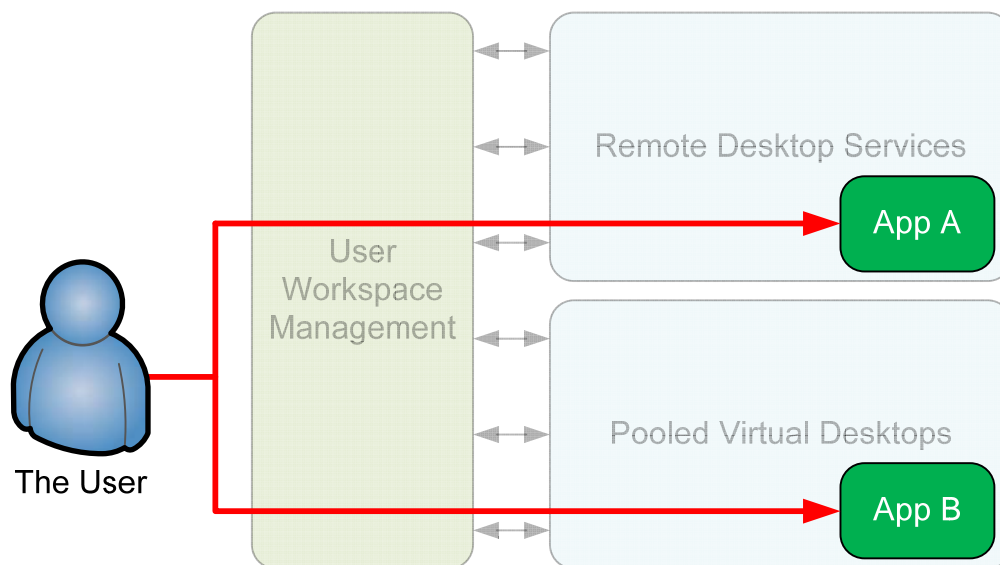
Figure 2.5: Deploying User Workspace Management in front of delivery architectures solves the personality synchronization problem.

The mechanisms that enable this synchronization are illustrated in Figure 2.6. In this image, a user has the option of selecting any of the available technology architectures available to them: laptop, desktop, virtual desktop, Remote Desktop Services session, and so on. Each of these potential targets for the user's attention is preinstalled with a software agent for the User Workspace Management solution.
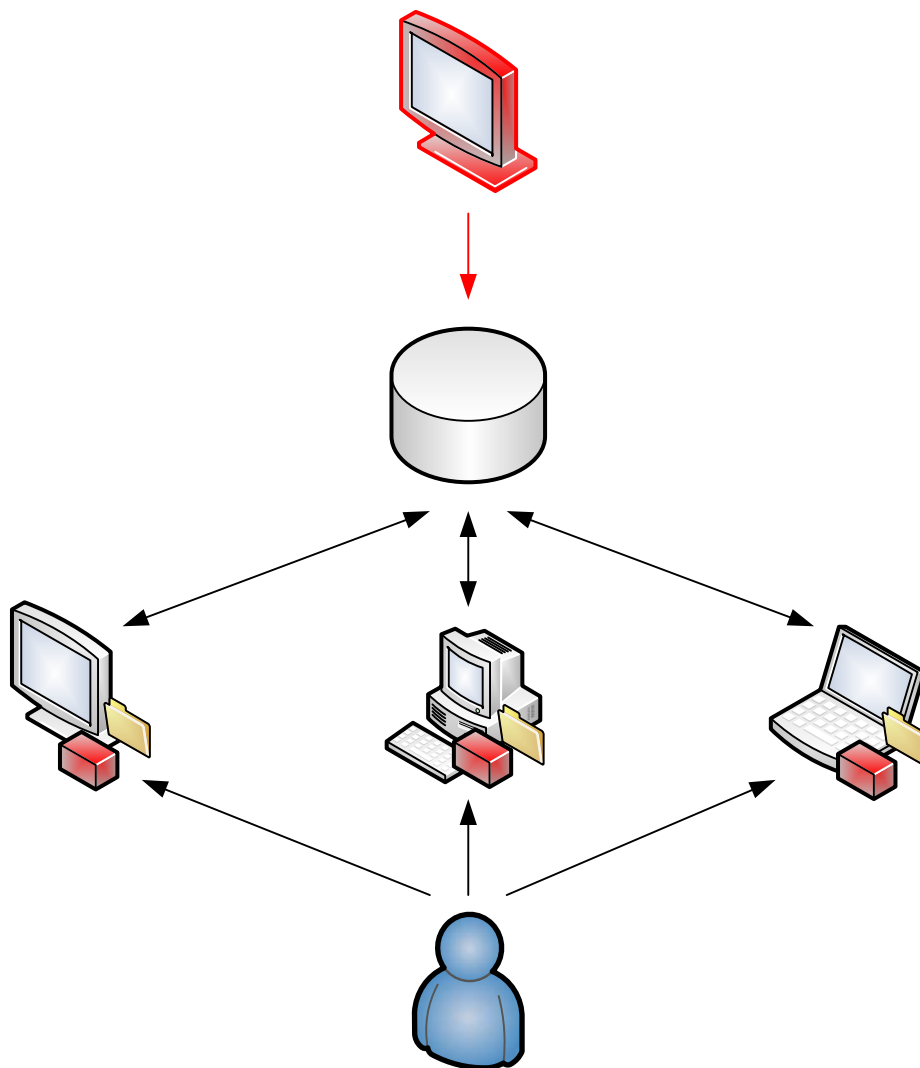
Figure 2.6: Centralizing user personality data into a database enables its delivery to any technology.

That agent communicates with a centralized database where user configurations are stored. The configurations are comprised of those that are created by each individual user (their "personality" data) along with other policy-driven configurations that have been defined by IT and business policies. The management workstation at the top represents the mechanism by which administrators can enact change to configurations.

Because configurations are regularly replicated between individual devices and the centralized database, any changes can be swiftly distributed to other devices as they are identified by the User Workspace Management solution. Effectively, when a user makes a change within one technology architecture, it can be assumed to be available within the others within a reasonable amount of time. The same holds true for administrators, who can modify their policy-driven configurations and assume that they will be quickly applied across all technology architectures.

Realtime
publishers

Incorporating Run Books into Personalization

It should be obvious at this point that there are innumerable ways in which user workspaces can be controlled. With an effective User Workspace Management solution in place, the biggest limitation lies only within the administrator's imagination.

The challenge is in actually converting a desired state or configuration into a set of code that is actionable within target technology infrastructures. Recognizing that you want a policy and actually creating that policy can be difficult without the right set of tools.

It is because of these hurdles that many User Workspace Management solutions include Run Book Automation features. These features enable the creation of "building blocks" of configurations, which can be logically linked to create a policy. Figure 2.7 shows how five building blocks are linked into a run book. That run book, along with its configurations, is ultimately deployed to a set of target computers through the User Workspace Management solution.
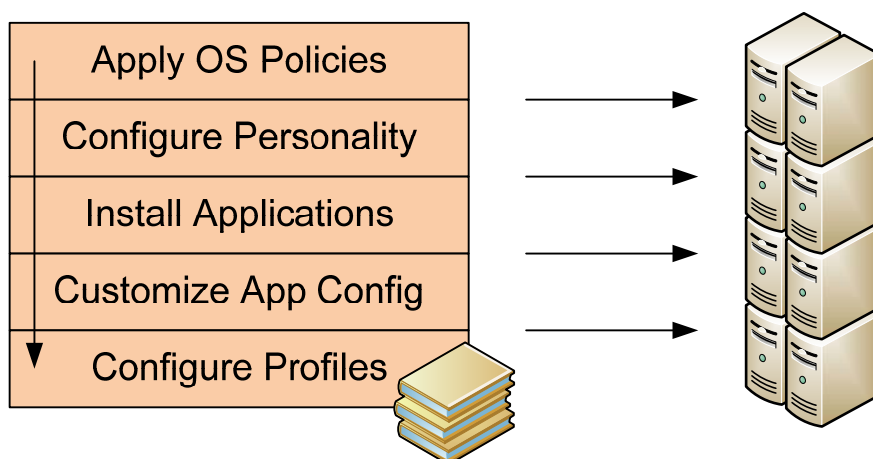
Figure 2.7: Run Book Automation uses building blocks to enact change to user workspaces.

Run books and Run Book Automation are particularly handy in environments where extreme levels of configuration experience, such as advanced scripting techniques, have not yet developed. To aid these environments, Run Book Automation solutions often include preconfigured building blocks that can be easily linked to create a needed configuration. Because the building block itself is the logical item of interaction, it abstracts the underlying code. The result is that virtually any configuration can be created without needing to understand the details of the code beneath. When considering a User Workspace Management solution, take a look through its building blocks to verify that they include the configurations you need for your own environment.

User Workspace Management Facilitates Workplace Satisfaction

In the end, the goal of any User Workspace Management solution is the assurance of user satisfaction. Keeping your fellow employees happy is a primary responsibility of any support organization like Information Technology. By implementing a User Workspace Management solution, you ensure that your users will retain the same comfortable experience across a range of technology infrastructures. At the same time, your IT organization gains the ability to modify or expand the environment without fear of interrupting your users' daily tasks.

You'll notice back in Figure 2.3 that a complete discussion on User Workspace Management requires the intersection of not two but three different elements. This chapter has introduced the first two in its discussion on content and context; also needed is a conversation on the security implications. Chapter 3 of this guide will discuss the benefits of tying security to *people* as opposed to *devices* by using a User Workspace Management solution.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit
http://nexus.realtimepublishers.com.

Realtime
publishers