VDI-in-a-Box 5.4

Nov 16, 2016

About VDI-in-a-Box

VDI-in-a-Box overview
About this release
Fixed issues
Known issues
Server requirements
User device requirements
Optional components

Get started

Download and extract the VDI-in-a-Box Manager
Create and configure the grid
Create the first Windows image
Create the first template from the published image
Assign templates to users, groups, and IP addresses
Test the connection as a user

License VDI-in-a-Box

Manage VDI-in-a-Box

Manage images
Install the Desktop Agent manually
Manage templates
Manage desktops
Manage personal desktops
Back up and restore personal desktops
Generate desktops from a pool of MAC addresses
Manage user sessions
Log on to the VDI-in-a-Box appliance
Manage servers
Manage a grid
Use VDI-in-a-Box with Active Directory
Configure VDI-in-a-Box kiosks
Configure user devices as kiosks
Configure generic user accounts
Configure shared user accounts
Manage SSL certificates
Collect logs

Manage optional components
Configure secure remote access using Citrix NetScaler Gateway
Configure secure remote access using the Microsoft Remote Desktop Gateway
Manage printing
Configure Profile management
Use StoreFront with VDI-in-a-Box
Use Citrix App Controller with VDI-in-a-Box
Optimize Microsoft Lync calling
Manage the Citrix Desktop Lock
Configure smart card authentication
Manage antivirus software
Use HDX features and enhancements

Access VDI-in-a-Box from user devices
Configure Windows, Mac, and Linux devices to access VDI-in-a-Box virtual desktops
Configure iOS devices to access VDI-in-a-Box virtual desktops
Configure Android devices to access VDI-in-a-Box virtual desktops
Use thin clients to access VDI-in-a-Box virtual desktops
About VDI-in-a-Box

Nov 16, 2016

Citrix VDI-in-a-Box consists of a single virtual appliance that provides all of the functionality needed to create, provision, manage, and load balance virtual desktops. It has a built-in connection broker, load balancer, user manager, and desktop provisioning server. It does not require separate shared storage, high-speed interconnects, or multiple management servers. The appliance runs on commodity servers running a hypervisor such as Citrix XenServer, Microsoft Hyper-V, or VMware ESXi, and you manage it through a single console.

Citrix Receiver helps provide VDI-in-a-Box desktop users with secure connections to a high-definition personalized user experience. Powered by Citrix HDX technologies, VDI-in-a-Box provides a superior user experience with Flash multimedia and applications, 3D graphics, webcams, audio, and branch office delivery. Although the desktops run on remote servers, the user experience is equivalent to that of a local Windows desktop. Both pooled and personal desktops are available, so users can install their own applications and store profile data. From the user's perspective, logging on to a virtual desktop is the same as logging on to a local desktop.

This section provides general information about VDI-in-a-Box, which you should read before using the product:

- For a general overview of VDI-in-a-Box, including concepts and terminology, read VDI-in-a-Box overview.
- For information on new features in this release, read About this release.
- For details of any known issues in this release, read Known issues.
- For the system requirements for servers and user devices for this release, read Server requirements and User device requirements.
- For a summary of the optional components, such as NetScaler Gateway and Profile management, that you can use with this release, read Optional components.
VDI-in-a-Box overview

Nov 16, 2016

Citrix VDI-in-a-Box consists of a single virtual appliance that provides all the functionality needed to create, provision, manage, and load balance virtual desktops. The VDI-in-a-Box appliance, known as VDI-in-a-Box Manager or vdiManager, runs as a virtual machine on a hypervisor. vdiManager creates and manages virtual desktops on the local physical server by communicating with the local hypervisor.

A typical VDI-in-a-Box deployment might look like this:

Each vdiManager can be set up to run as a single physical server or it can be a part of a collection of physical servers referred to as a VDI-in-a-Box grid. Each vdiManager in a grid performs the following functions:

- Creates virtual desktops from a template. A template consists of:
  - An image that includes a Windows operating system, a set of applications, and the VDI-in-a-Box Desktop Agent, which communicates with the vdiManager about user connections and desktop health. Multiple templates can use the same image.
  - Policies that specify characteristics such as how many desktops to create, the number of virtual CPUs and how much RAM to allocate to them, whether local USB peripherals can be accessed by the virtual desktop, and the desktop refresh policy.

A grid can contain multiple templates and images.
To provide access to virtual desktops, you assign individual users, user groups, or a range of IP addresses to the template on which the desktops are based. Desktop assignment can therefore be either user-based or location-based. You can also make any template the default template for the grid; this means that any user who logs on but has not been assigned a template is provided with a desktop based on the default template.

- Balances the load across the grid. vdiManagers create desktops across servers running vdiManager based on how many desktops are currently running on each server and the availability of computing resources (memory and cores) on each server. When a user logs on, vdiManager provisions a desktop from a lightly loaded server.
- Provides high availability. vdiManager instances on physical servers communicate with each other to share key operational and configuration information. For instance, VDI-in-a-Box templates and images are stored on multiple servers so they are not lost if a physical server fails. When a physical server fails, the remaining servers in the grid have the necessary information to create extra desktops to replace those on the failed server. When the failed server is repaired and rejoins the grid, the key operational and configuration information is sent to it and it then resumes desktop provisioning.

Citrix recommends that you have a grid consisting of N+1 servers where N servers are capable of handling the regular load and 1 server is available to absorb the load in case one server in the grid fails. This means that if a single server fails, grid operations are not adversely affected.

- Brokers connections so that a user can log on to any server in the grid.
- Provides a web-based interface, the VDI-in-a-Box console, used to configure and manage servers running vdiManager, desktops, templates, images, users, and the grid, all at the grid level. In the VDI-in-a-Box console, the grid appears as one logical server running vdiManager. It is also possible to view the status and activity of each server individually when required. When you update vdiManager on one server, vdiManager distributes the changes to all servers in the grid.

VDI-in-a-Box is designed to work without shared storage. A direct access storage device for each server is sufficient. You can, however, use shared storage on some platforms; for further information, see http://support.citrix.com/article/CTX137401.

User authentication and user data

VDI-in-a-Box allows you to choose between Active Directory and Workgroups.

VDI-in-a-Box uses Active Directory for authentication and a simple network file system to hold user data.

For Windows domain environments, Active Directory service is required to provide user authorization and authentication.

Active Directory can also be used to provide "roaming profiles," keeping user application configurations and their My Documents folders in a central location outside of the desktop. With this approach users are presented with a personalized desktop each time they log on. While the use of roaming profiles is optional, it provides personalization that makes the user
experience for virtual desktops nearly identical to that for a physical desktop. Use of third-party profile management tools with VDI-in-a-Box requires only the deployment of their agents on each VDI-in-a-Box image. If profiles are large, ensure the feature is configured to reduce network load at logon and use features such as redirected folders.

Each server running vdiManager requires sufficient local storage to keep images, templates, and configuration information needed for a highly available system. VDI-in-a-Box does not back up user data stored on virtual desktops. Typical usage is to create desktops dynamically from a template and destroy them based on a refresh policy. A simple network file system is sufficient to keep user data outside the desktop.

For sites using Workgroups, VDI-in-a-Box includes a user database for authentication.
About this release

Nov 16, 2016

VDI-in-a-Box 5.4 provides support for Windows 8.1 virtual desktops and Windows Server 2012 R2 Hyper-V. It also includes a range of enhancements that increase VDI-in-a-Box's flexibility and a range of power tools for administrators.

Fixed issues

Known issues

Windows 8.1 virtual desktops

Create Windows 8.1 desktops and run them on any supported hypervisor.

Windows Server 2012 R2


VMware vSphere ESXi 5.5

VMware vSphere ESXi 5.5 Hypervisor is now supported.

Built-in HTML5 device support

Use devices running HTML5-capable browsers to access VDI-in-a-Box desktops without StoreFront. This allows devices such as Chromebook to access VDI-in-a-Box desktops without additional server components.

Multiple computer domains

If you use Active Directory as a user database, you can place the computer objects for VDI-in-a-Box desktops in more than one domain. This allows you to separate your users into different domains and meet regulatory or compliance requirements in your organization. For more information, see Use VDI-in-a-Box with Active Directory.

StoreFront smart card support

Users can log on using smart cards when accessing desktops through StoreFront from non-domain-joined Windows devices.

SSL certificate multiple host names

You can specify multiple host names on a single SSL certificate, which is more cost-effective than using a wildcard certificate. This enables you to specify the grid IP FQDN as the common name and add subject alternate names for the FQDNs of the individual vdiManagers. For more information, see Manage SSL certificates.

Install existing SSL certificates

Install existing SSL certificates through the Manage SSL Certificate wizard. For more information, see Manage SSL certificates.

Follow-me desktops

Time-share user devices among multiple user names where each user name is shared by a group of users: in a classroom or lab environment, for example. In previous releases of VDI-in-a-Box this was achieved through setting your entire grid to...
generic user mode. You now have the flexibility to support shared user accounts and dedicated user accounts in the same VDI-in-a-Box grid just by clearing a check box on an individual template. For more information, see Configure shared user accounts.

Generic user mode is now reserved solely for avoiding user name verification after the user logs on to a desktop. For more information, see Configure generic user accounts.

Image save as

You can save an existing image under a new name. This gives you the flexibility to easily create backups, or experiment with different image settings.

If you need to pilot a new version of an image for a pooled desktop, you can update an existing image, save it with a different name, then edit an existing template to use this image. When testing is complete it’s easy to either continue using the updated image, move back to the previous version, or create subsequent versions if you need to continue testing.

For more information, see Manage images.

Change images for pooled-desktop templates

You can edit an existing template for pooled desktops and base it on a different image, provided the image is compatible with the template properties and existing desktops. This enables you to test new versions of images, as described above. For more information, see Manage templates.

Remote Assistance support

Launch Windows Remote Assistance from the vdiManager console, enabling administrators or support staff to share users' screens and shadow their sessions. For more information, see Manage user sessions.

Wizard-driven migration to Citrix XenDesktop

If you need to move your entire VDI-in-a-Box deployment to XenDesktop, this easy-to-use wizard exports your images and generates PowerShell scripts that you can run to migrate all template configurations and user assignments to a XenDesktop deployment. For more information see Migrate to XenDesktop.
VDI-in-a-Box 5.4 Fixed Issues

Nov 16, 2016
VDI-in-a-Box 5.4.8

Compared to: VDI-in-a-Box 5.4.7

VDI-in-a-Box 5.4.8 contains all fixes that were included in previous releases of VDI-in-a-Box, plus the following, new fixes:

- With the account lock threshold set to “2” (allowing users to enter incorrect credentials twice before the account is locked), the account is actually locked after just one incorrect authentication attempt.
  
  [#599576]

- After upgrading to Java 8 Version 51, the option to enter user credentials is missing from the Java client.
  
  [#605372]

- Clicking an application icon multiple times in rapid succession can result in the creation of multiple, separate session logons.
  
  [#616773]

- This release introduces support for a separate management network of traffic to mitigate a Java deserialization issue. For more information, see Knowledge Center article CTX218826.
  
  [#625885]

- This fix updates an internal component. For more information, see Knowledge Center article CTX206991.
  
  [#625886]

- This fix updates an internal component. For more information, see Knowledge Center article CTX200355.
  
  [#644238]

- This fix updates an internal component.
  
  [#649142]

- This fix updates an internal component.
  
  [#649147]

VDI-in-a-Box 5.4.7
Compared to: VDI-in-a-Box 5.4.6
VDI-in-a-Box 5.4.7 contains all fixes that were included in previous releases of VDI-in-a-Box, plus the following, new fixes:

- Multiple sessions might be unexpectedly assigned to a user when reconnecting to a session. This can happen when the desktop health check fails to respond within the timeout value.
  
  [#588070]

- This fix updates an internal communications component of VDI-in-a-Box.
  
  [#573435]

VDI-in-a-Box 5.4.6

Compared to: VDI-in-a-Box 5.4.5

VDI-in-a-Box 5.4.6 contains all fixes that were included in previous releases of VDI-in-a-Box, plus the following, new Security and other fixes:

- This fix addresses a security vulnerability. For more information, see Knowledge Center article CTX200355.
  
  [#534163]

- This fix addresses a security vulnerability. For more information, see Knowledge Center article CTX200491.
  
  [#542444]

- This fix addresses a security vulnerability. For more information, see Knowledge Center article CTX200391.
  
  [#542442]

- Grid IP not retained in a single server grid after appliance reboot.
  
  [#0491855]

- Chrome update impact on HTML5 client for VDI-in-a-Box 5.4.x.
  
  [#544407]

- VDI-in-a-Box web-console login for Active Directory user accounts causes accounts getting locked before the lockout threshold is met.
  
  [#546782]

- VDI-in-a-Box Manager sometimes fails to display network label in ESX.
  
  [#546783]

- Multiple user sessions are created when user logs in from NetScaler Gateway and the grid is in generic mode.
  
  [#563112]

VDI-in-a-Box 5.4.5

Compared to: VDI-in-a-Box 5.4.4

VDI-in-a-Box 5.4.5 contains all fixes that were included in previous releases of VDI-in-a-Box, plus the following, new Security
and other fixes:

- This fix addresses a security vulnerability. For more information, see Knowledge Center article CTX200217. [#506018]
- This fix addresses a security vulnerability. For more information, see Knowledge Center article CTX200238. [#511619]

VDI-in-a-Box 5.4.4
Compared to: VDI-in-a-Box 5.4.3
VDI-in-a-Box 5.4.4 contains all fixes that were included in previous releases of VDI-in-a-Box, plus the following, new Security and other fixes:

- This fix addresses a security vulnerability. For more information, see Knowledge Center article CTX140605. [#467879]
- This fix addresses a security vulnerability. For more information, see Knowledge Center article CTX140876. [#482393]
- Any user or administrator who knows the instance id of a desktop can access that desktop. [#467866]
- Instance sort Intermittently throws an exception that causes logon failures. [#467878]
- A broken image parcel file causes manual-refresh desktops to be deleted. [#467876]

VDI-in-a-Box 5.4.3
Compared to: VDI-in-a-Box 5.4.2
VDI-in-a-Box 5.4.3 contains all fixes that were included in previous releases of VDI-in-a-Box, plus the following, new fixes:

- On-hold desktops cannot be reassigned to users who are members of a user group rather than registered as named users. [#450965]
- SSL certificates do not migrate from VDI-in-a-Box 5.3 to VDI-in-a-Box 5.4.x. [#439269]
- Desktops based on templates scheduled to refresh during the morning are refreshed at noon. [#453103]
VDI-in-a-Box 5.4.2
Compared to: VDI-in-a-Box 5.4

VDI-in-a-Box 5.4.2 contains all fixes that were included in previous releases of VDI-in-a-Box, plus the following, new fixes:

- The management console provides only RDP connection if the Advanced Property **Check if Citrix Receiver is installed on client** is disabled.
  
  [#437811]

- Session reliability does not work if the desktop connection through NetScaler Gateway is interrupted for longer than 10 seconds.
  
  [#430565]

- You cannot create personal desktops after saving an image with VMXNet 3 NIC.
  
  [#432970]

- The management console does not work when Internet Explorer is in compatibility mode.
  
  [#430759]

- You cannot select the **Delete computer name from AD** option when creating a template.
  
  [#430015]

- Smart card authentication fails on Windows 8.1 desktops.
  
  [#424941]

VDI-in-a-Box 5.4
Compared to: VDI-in-a-Box 5.3.6

VDI-in-a-Box 5.4 contains all fixes that were included in previous releases of VDI-in-a-Box, plus the following, new fix:

- Smart card authentication through StoreFront 2.0 is not supported.

  [#398290]

For a list of issues fixed in VDI-in-a-Box before Version 5.4, see [VDI-in-a-Box 5.x - Issues Fixed in This Release](https://docs.citrix.com).
Known issues

Jan 13, 2014
This topic contains:

- General issues
- Third-party issues
- Globalization issues

For a list of previous known issues that have been fixed in this version of VDI-in-a-Box, see http://support.citrix.com/article/CTX134622.

General issues

- COM port mapping does not work. To resolve this issue, contact Citrix Support to obtain the relevant hotfix. [432105]
- Repeated connections to a Windows desktop in Workgroup mode that involve HTML5 Receiver may result in an inaccessible desktop. This issue does not occur in Active Directory mode. To avoid this issue, when working in this scenario ask users to log off after using a desktop and have a refresh policy of ‘On logout’ to dispose of used desktops. [424882]
- If user imports a VM that has a stale IDE registry entry without the corresponding hard disk, and it is saved as an image, personal desktops provisioned from it may become broken during the initial personal vDisk update. To avoid this issue, start with a new imported VM created from an ISO. [414012]
- Sessions fail when launched using Receiver for HTML5 through StoreFront 2.0. To avoid this issue, use StoreFront 2.1. [425916]
- The Citrix license may not be visible in the About dialog box after it has been uploaded to VDI-in-a-Box. If this occurs, restart the VDI-in-a-Box Manager on which the license was uploaded, reconnect to the VDI-in-a-Box Manager, and click About to see the license. [300849]
- Personal desktops using Multiple Activation Key (MAK) activation consume a new activation each time the personal desktop is refreshed or reset. [317240]
- File and printer sharing firewall exceptions are not created for the domain when you create a draft image from a base image that was a member of a workgroup before it was imported. To work around this issue, from the Control Panel go to System and Security > Windows Firewall > Allowed Programs and select File and Printer Sharing in the Domain column. [325619]
- Disabling the multiple data stores feature after it has been enabled does not remove or block the additional data stores. All data stores remain available. To remove the additional data stores, from the VDI-in-a-Box Manager Console, click the Servers tab and click the server to be configured. In the Server Properties dialog box, click Configure and in the Select datastores section, set all data stores to the same data store. [310168]
- The HDX connection to a VDI-in-a-Box desktop running Windows 7 using a VMware ESX/ESXi hypervisor may fail. This can happen if VMware Tools has been updated on the image after the VDI-in-a-Box Desktop Agent was installed. To resolve this issue, disable the display adapter VMware SVGA 3D, which is added as part of the VMware Tools installation. [318109]
- Dialog boxes may occasionally flicker in Internet Explorer. The workaround is to reload the page after refreshing the browser cache. [347445]
- When you are installing a new Desktop Agent on an image for a static Windows 2008 desktop, an error message (error 1953) appears. The message may appear behind the active dialog box, so you should actively monitor the installation process. To work around this, click OK in the message dialog box; a silent re-try takes place and the Desktop Agent installs successfully. [398287]
This issue has now been documented in Configure Profile management.

Third-party issues

If after installing a hotfix on XenServer, all the desktop instances provisioned from an image fail to start or you cannot edit that image, a possible reason is that an old version of XenServer Tools is mounted in the DVD of the published image (XenServer template) and the provisioned VMs from that template. Use the XenCenter console to eject the DVD from each affected VM and the XenServer template (VDI-in-a-Box published image); to do this, in the Storage tab of the VM/XenServer template in the XenCenter console click Eject on DVD Drive 1.

Globalization issues

Non-English versions of Windows Server 2012 cannot be imported as desktop images unless .NET 3.5.1 is already installed on the VM. Windows Server 2012 R2 desktops do not have this prerequisite. [428061]

VDI-in-a-Box does not support non-ASCII characters in ESXi hypervisor items. [318690]

VDI-in-a-Box does not support Surrogate Pairs characters in hypervisor items such as VM name or Network Adapter name. [318681]

A Simplified Chinese, Traditional Chinese, or Korean Windows Server 2008 R2 environment migrated from VDI-in-a-Box 5.1.x, 5.2.x, or 5.3 to 5.4 has a status of “broken” if the firewall on the Hyper-V server blocks SMB ports (for file and printer sharing). To resolve this issue, uninstall the Hyper-V connector and manually install the VDI-in-a-Box 5.4 version. [327239]

The user name displayed on the log on screen in an RDP session contains corrupted characters if the name includes non-ASCII characters. [321966]

VDI-in-a-Box does not support non-ASCII characters for the user name when the VDI-in-a-Box Java Desktop Client is started from a command prompt window. If possible, launch the Java Desktop Client with a web browser by typing https://IPaddress/dt/vdiclient.jnlp in the Address box. [297880]
Server requirements

Apr 22, 2014

This topic describes the software you need on your servers to run VDI-in-a-Box. It also provides information on sizing your servers.

Supported hypervisors

VDI-in-a-Box implements its own clustering. Citrix therefore recommends not enabling your hypervisor's own clustering/pooling feature.

**Citrix XenServer**
- Citrix XenServer 6.2 Platinum, Enterprise, Advanced, and Free editions
- Citrix XenServer 6.1 Platinum, Enterprise, Advanced, and Free editions

Note: Servers in a XenServer pool are not supported by VDI-in-a-Box.

To optimize usage of space on your servers, consider using the XenServer Thin Provisioning feature.

**Microsoft Hyper-V**
- Microsoft Hyper-V Server 2012 R2
- Microsoft Hyper-V Server 2012
  - If your hypervisor is Microsoft Hyper-V Server 2012 or Microsoft Hyper-V Server 2012 R2 and does not have access to the internet, you must manually install .NET Framework 3.5 before installing the Citrix VDI-in-a-Box for Hyper-V Connector. At a command prompt, type:

  ```
  DISM /Online /Enable-Feature /FeatureName:NetFx3 /All /LimitAccess /Source:hyper_v_iso_location\sources\sxs
  ```

  where `hyper_v_iso_location` is the location of your Hyper-V installation media.

- Microsoft Hyper-V Server 2008 R2 with Service Pack 1
- Microsoft Windows Server 2008 R2 with Service Pack 1, Enterprise edition, with Hyper-V role enabled
  - Dynamic Host Configuration Protocol (DHCP) server – supported
  - Active Directory – supported
- Windows Server 2008 R2 with Service Pack 1 Server Core, with Hyper-V role enabled
  - Dynamic Host Configuration Protocol (DHCP) server – supported
  - Active Directory – supported

Note: Windows Server 2008 R2 with Service Pack 1, Standard edition is not supported by VDI-in-a-Box for use with Hyper-V.

Citrix does not recommend using Internet Information Services (IIS) with Hyper-V and VDI-in-a-Box. However, if you do use this combination, you must add an IIS SSL binding in the IIS Manager. Refer to your Microsoft documentation for details of how to do this. The VDI-in-a-Box SSL binding on port 9875 must remain, and you must restore your other bindings (including the one on 443) manually.

**VMware ESXi or VMware vSphere**
- VMware Essentials license or greater is required.
  - Note: If you are evaluating Citrix VDI-in-a-Box and have downloaded a free version of ESXi from the VMware Web site, do not install the license key that comes with that version. If you install this license key, the APIs required for Citrix VDI-in-a-Box to work with the hypervisor close and the setup process ends. Leave the license selection as Evaluation Mode (No License Key). Convert to a paid hypervisor license during the trial period.
Virtual desktop operating systems

- VMware ESXi 5.5
- VMware ESXi 5.1 Update 2

Virtual desktop operating systems

- Windows 8.1 Enterprise and Pro editions, 32-bit or 64-bit versions.
- Windows 8 Enterprise and Pro editions, 32-bit or 64-bit versions.
- Windows 7 with Service Pack 1, Professional and Enterprise editions, 32-bit or 64-bit versions.
- Windows 7 N is not supported.
- Windows XP with Service Pack 3, Professional edition, 32-bit version
- Windows Server 2012 R2, Full Standard edition, 64-bit version
- Windows Server 2008 R2 with Service Pack 1, Enterprise edition, 64-bit version

Windows Virtual Desktop Access Volume License is needed to access virtual desktops. Retail license editions of Windows operating systems (for example Windows 8.1 Enterprise evaluation) are not supported. Please refer to http://www.microsoft.com/licensing/software-assurance/windows-virtualization.aspx for licensing details.

Web browsers for accessing the vdiManager console

Use the following Web browsers to access the VDI-in-a-Box Manager (vdiManager) console:

- Windows Internet Explorer 10, 9, and 8
- Google Chrome
- Mozilla Firefox
- Safari

Sizing your servers

Server sizing calculators are available. Citrix recommends that you use them when sizing servers for your VDI-in-a-Box deployment:

- Partners: Go to http://www.citrix.com/skb, click VDI-in-a-Box, and then click Citrix VDI-in-a-Box 5.4 Server Sizing Tool.

Networking

vdIManager and all provisioned desktops should reside on the same network.

For Hyper-V deployments, only a single virtual switch is supported. If multiple virtual switches are configured on different subnets, then the first active virtual switch will be assigned for desktops.
User device requirements

Nov 05, 2013

VDI-in-a-Box provisioned desktops can be accessed from a Web browser, Citrix Receiver, or the VDI-in-a-Box Java Desktop Client.

- **Required** — Install Citrix Receiver on the user device to access VDI-in-a-Box desktops. You can download it from [http://receiver.citrix.com](http://receiver.citrix.com). Citrix Receiver is available for a wide range of user devices including Windows, iPhone, iPad, Android, Mac, Blackberry, and Linux.

  Note: Citrix recommends using Receiver for Windows 4.x when connecting to VDI-in-a-Box desktops from a Windows user device.

- **Optional** — If you want to use the VDI-in-a-Box Java Desktop Client on a user device running Windows, Mac, or Linux, you must also install the Java Runtime Environment (JRE), which you can download from [http://www.java.com](http://www.java.com).

  To use the Desktop Lock, user devices must be running Windows XP or Windows 7 and have Receiver Enterprise edition installed.

Use the following Web browsers to access VDI-in-a-Box provisioned desktops from user devices:

- Internet Explorer 10, 9 and 8
- Google Chrome
- Mozilla Firefox
- Safari
- Opera

You can also access desktops from a wide range of thin clients that are certified either HDX Ready or HDX Ready Premium. Citrix recommends the HDX Ready Premium thin clients for running multimedia and unified communications applications. For the details of the HDX Ready program, see [http://www.citrix.com/cms/idc/hdx-ready-program](http://www.citrix.com/cms/idc/hdx-ready-program). For the list of available HDX Ready and HDX Ready Premium thin clients, see [http://www.citrix.com/ready/](http://www.citrix.com/ready/) and search in the thin clients category.

**HTML5 devices**

VDI-in-a-Box has built-in HTML5 Receiver client support. You can connect to a VDI-in-a-Box desktop from any device running an HTML5-compatible browser (Chromebook, for example) without installing Citrix Receiver. You can also connect through StoreFront 2.1.

Note: Windows XP desktops are not supported.

If you use Active Directory as your user database, you must create a Citrix Group Policy Object (GPO) to set “WebSockets connections” allowed, and link that GPO to the OU in which the base image for the desktop resides.

If you use VDI-in-a-Box in workgroup mode you must add the following setting to the base image for the desktop:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICAPolicies]
"AcceptWebSocketsConnections"=dword:00000001
"WebSocketsPort"=hex(0):
"WSTrustedOriginServerList"=hex(0):
```

HTML5 Receiver is the default Receiver on Chromebooks. However, if you want to use the HTML5 Receiver on other devices instead of the installed Receiver, use the HTML5 Receiver URL:

```
http(s)://vdiMgrIP-or-hostname/html5
```

instead of the regular URL:

```
http(s)://vdiMgrIP-or-hostname
```
You can also connect through StoreFront 2.1 with Receiver for Web.
Optional components

Feb 13, 2014

This topic describes optional components and products that you can use to enhance your experience of VDI-in-a-Box, depending on the use cases and organizational environment you are working with.

- **Secure remote access.** VDI-in-a-Box works with NetScaler Gateway or Remote Desktop Gateway to provide secure remote access.
  Secure remote connections from user devices to virtual desktops are supported for the following product versions:
  - Citrix Access Gateway VPX 5.0.x
  - Citrix NetScaler Gateway 10.1
  - Remote Desktop Gateway with Remote Desktop Connection 6.1, 7.x, or 8.x.
  For more details, see [Configure secure remote access using Citrix NetScaler Gateway](https://docs.citrix.com) and [Configure secure remote access using the Microsoft Remote Desktop Gateway](https://docs.citrix.com).

- **Profile management.** Citrix recommends that you use Citrix Profile management with your VDI-in-a-Box deployment so that user data can be stored separately from virtual desktops and can persist across desktop refreshes.
  Download Profile management from the VDI-in-a-Box download page. For more details, see [Configure Profile management](https://docs.citrix.com).

- **Citrix StoreFront.** StoreFront integrates with your existing Citrix deployment enabling you to deliver Windows applications and virtual desktops to any device through a unified self-service storefront.
  VDI-in-a-Box supports StoreFront 2.x and 1.2. Citrix recommends you use version 2.x.
  For more details, see [Use StoreFront with VDI-in-a-Box](https://docs.citrix.com).

- **Citrix XenMobile (Enterprise or App edition).** Citrix App Controller allows you to access all your business resources including virtual desktops, mobile apps, SaaS apps, and data, from one central place.
  For more details, see [Use Citrix App Controller with VDI-in-a-Box](https://docs.citrix.com).
  To access VDI-in-a-Box desktops, you must use App Controller 2.8.

- **Citrix HDX RealTime Optimization Pack for Microsoft Lync.** This provides a highly scalable solution for delivering real-time audio-video conferencing and USB or VoIP enterprise telephony through Microsoft Lync in VDI-in-a-Box environments.
  Download the pack from the VDI-in-a-Box download page. This optimization pack is not compatible with the Citrix Desktop Lock because the two components require different versions of Receiver.
  For more details, see [Optimize Microsoft Lync calling](https://docs.citrix.com).

- **HDX Optimization Pack for Google Earth.** This pack improves the visual quality of images generated by the Google Earth application.
  For more details, see [HDX Optimization Pack for Google Earth](https://docs.citrix.com).

- **Citrix Desktop Lock.** Use the Desktop Lock to turn your existing user devices into thin clients by blocking access to the local operating system.
  This allows you to repurpose existing machines and avoid purchasing new thin clients.
  Download the Desktop Lock from the VDI-in-a-Box download page. The Desktop Lock requires Citrix Receiver 3.4 Enterprise edition.
  Products and features that require later versions of Receiver, such as the Citrix HDX RealTime Optimization Pack for Microsoft Lync, are therefore not compatible with the Desktop Lock.
  For more details, see [Manage the Citrix Desktop Lock](https://docs.citrix.com).

- **Smart cards.** VDI-in-a-Box supports smart card authentication. For more details, see [Configure smart card authentication](https://docs.citrix.com).
**Application virtualization.** VDI-in-a-Box works with application virtualization solutions such as XenApp to provide flexibility in meeting your desktop and application virtualization needs. VDI-in-a-Box can deliver any application through a virtual desktop; you can install the applications your users need on the master images used to provision desktops. In cases where this is not sufficient, you can enable your users to connect to XenApp applications directly from a VDI-in-a-Box desktop by installing Citrix Receiver on the image and configuring it to point to the XenApp store. You can also use StoreFront to access applications.

**VMware vCenter.** vCenter is not required to operate a VDI-in-a-Box grid. VDI-in-a-Box has a built-in connection broker, load balancer, user manager, and desktop provisioning server that allow you to manage all the servers in the grid as one logical server. In addition, VDI-in-a-Box provides linked clones to reduce storage without vCenter. However, if you use vCenter to monitor your ESX servers, you can continue to do so with VDI-in-a-Box running on ESX. To do so, make the vCenter information known to the grid so that VDI-in-a-Box can interoperate with vCenter.
Get started with VDI-in-a-Box

Nov 14, 2014

Before installing VDI-in-a-Box, make sure you have the following available:

- One or more servers running one of the following hypervisor systems:
  - Citrix XenServer/XenCenter
  - Microsoft Hyper-V/Hyper-V Manager
  - VMware ESXi/vSphere Client
- The administrator user name ('root' for XenServer and ESXi) and password for the hypervisors.
- A Dynamic Host Configuration Protocol (DHCP) server.
- If you are using MAK activation, you must have a Windows Volume License key.
- If you are using KMS activation, you must have an active KMS server that has already activated at least 25 desktops.
- If your network uses Microsoft Active Directory, you must have the user name and password of an Active Directory user with read, write, and modify privileges for computer accounts and read privileges for user accounts.

The topics that follow describe how to quickly set up an initial VDI-in-a-Box deployment consisting of a single-host grid, a master image, and a machine catalog of pooled desktops.

The steps are:
1. Download and extract the VDI-in-a-Box Manager
2. Create and configure the grid
3. Create the first Windows image
4. Create the first template from the published image
5. Assign templates to users, groups, and IP addresses
6. Test the connection as a user
Download and extract the VDI-in-a-Box Manager

Apr 06, 2015

Separate packages are provided on the Citrix web site for each supported type of hypervisor. Downloading them, extracting the relevant version of the VDI-in-a-Box Manager, and importing it into your hypervisor, are described in the following topics.

Download and extract the VDI-in-a-Box Manager to XenServer

Download the VDI-in-a-Box virtual appliance, called VDI-in-a-Box Manager (vdiManager), for use with Citrix XenServer from the Citrix web site.

The download package, VDI-in-a-Box_XenServer_v5_4_x.zip, contains the vdiManager file, vdiManager_Xen_v5_4_x.xva. About 6 GB of disk space is needed to extract vdiManager.

Note: Be sure to download and extract the file to a location accessible with Citrix XenCenter.

2. If you are not already logged on to My Account, do so now. If you open the Download page without having logged on, you are unable to download the product software.
3. Click Downloads.
4. From the products list, select VDI-in-a-Box.
5. From the download type list, select Product Software.
6. Click Find. The VDI-in-a-Box product software page appears.
7. Click the version of the product you want to download. The product version page appears.
8. From the Appliances section, for the version that matches your hypervisor, click Download. The End-User License Agreement appears.
9. Accept the agreement. The Download Manager window opens.
10. Click Download Now.
11. Click Install and save the zip file. The Download Manager downloads the zip file.
12. From the zip file, extract the vdiManager file.

To import vdiManager

When the vdiManager file is extracted, import it into Citrix XenCenter. For details on importing with XenCenter, see your XenServer documentation. When the import process is finished, vdiManager appears in the XenCenter management console as a virtual machine.

Important: Do not import more than one vdiManager per hypervisor. Doing so may result in excessive CPU, RAM, disk, and network consumption, and cause system non-responsiveness.

Download and extract the VDI-in-a-Box Manager to Microsoft Hyper-V

Download the VDI-in-a-Box virtual appliance, called VDI-in-a-Box Manager (vdiManager), for use with Microsoft Hyper-V from the Citrix web site.

The download package, VDI-in-a-Box_Hyper-V_v5_4_x.zip, contains the vdiManager file, vdiManager_Hyper-V_v5_4_x.exe. About 6 GB of disk space is needed to extract vdiManager. In addition to installing vdiManager, the vdiManager file configures Microsoft Hyper-V to work with VDI-in-a-Box, including enabling the Hyper-V Manager role, if it is not already set.
Note: Be sure to download and extract the file to a location accessible with Microsoft Hyper-V.

2. If you are not already logged on to My Account, do so now. If you open the Download page without having logged on, you cannot download the product software.
3. Click Downloads.
4. From the products list, select VDI-in-a-Box.
5. From the download type list, select Product Software.
6. Click Find. The VDI-in-a-Box product software page appears.
7. Click the product version you want to download. The product version page appears.
8. From the Appliances section, for the version that matches your hypervisor, click Download. The End-User License Agreement appears.
9. Accept the agreement. The Download Manager window opens.
10. Click Download Now.
11. Click Install and save the zip file. The Download Manager downloads the zip file.
12. From the zip file, extract the vdiManager file.

**Import the vdiManager into Hyper-V**

1. Start vdiManager_Hyper-V_v5_4_x.exe by double-clicking the icon or at a command prompt. The Citrix VDI-in-a-Box for Hyper-V Setup wizard appears. The wizard will install:
   - Citrix VDI-in-a-Box for Hyper-V Connector
     Note: Use the Citrix VDI-in-a-Box for Hyper-V Connector delivered with this version of VDI-in-a-Box. Earlier versions are not supported.
   - Citrix VDI-in-a-Box Manager appliance
2. Click Next. The Select Destination Location page appears.
   Note: Do not import a vdiManager onto a Hyper-V server that already has a vdiManager on it. Doing so updates the Hyper-V Connector on the server, making it incompatible with the existing grid and causing the grid to stop functioning.
3. Accept the default location for the VDI-in-a-Box installation and click Next. The Select Additional Tasks page appears.
4. Leave Create Citrix VDI-in-a-Box manager virtual appliance selected, then click Install.
   Note: If you want to be able to manage the virtual desktops from a remote device, select Enable Hyper-V Remote Administration.
   The installation process begins. When it completes, the Welcome to Citrix VDI-in-a-Box for Hyper-V page appears.
5. Click Close, then Finish. On the device running Hyper-V Manager, or an alternative management console, the vdiManager appears in the hypervisor list of virtual machines as vdiManager_timestamp.
   Important: Do not import more than one vdiManager per hypervisor. Doing so may result in excessive CPU, RAM, disk, and network consumption, and cause system non-responsiveness.

**Download and extract the VDI-in-a-Box Manager to VMware ESXi**

Download the VDI-in-a-Box virtual appliance, called VDI-in-a-Box Manager (vdiManager), for use with VMware ESXi from the Citrix web site.

Download and extract the VDI-in-a-Box Manager to VMware ESXi

Download the VDI-in-a-Box virtual appliance, called VDI-in-a-Box Manager (vdiManager), for use with VMware ESXi from the Citrix web site.
The download package, VDI-in-a-Box_ESX_v5_4_x.zip, contains the vdiManager file, vdiManager_ESX_v5_4_x.ova. About 6 GB of disk space is needed to extract vdiManager.

Note: Be sure to download and extract the file to a location accessible with VMware vSphere Client.

2. If you are not already logged on to My Account, do so now. If you open the Download page without having logged on, you are unable to download the product software.
3. Click Downloads.
4. From the products list, select VDI-in-a-Box.
5. From the download type list, select Product Software.
6. Click Find. The VDI-in-a-Box product software page appears.
7. Click the version you want to download. The product version page appears.
8. From the Appliances section, for the version that matches your hypervisor, click Download. The End-User License Agreement appears.
9. Accept the agreement. The Download Manager window opens.
10. Click Download Now.
11. Click Install and save the zip file. The Download Manager downloads the zip file.
12. From the zip file, extract the vdiManager file.

To import vdiManager

When the vdiManager file is extracted, import it into VMware vSphere Client. For details on importing with VSphere Client, see http://www.vmware.com/. When the import process is finished, vdiManager appears in the vSphere Client management console Inventory view as a virtual machine.

Important: Do not import more than one vdiManager per hypervisor. Doing so may result in excessive CPU, RAM, disk, and network consumption, and cause system non-responsiveness.
Create and configure the grid

Aug 06, 2013

Configure the VDI-in-a-Box grid when VDI-in-a-Box Manager (vdiManager) has been imported into your hypervisor and is available in its management console.

The grid unites servers running vdiManager, allowing load balancing and ensuring high availability of virtual machines on the servers.

Enable JavaScript and cookies on your browser.

To open the vdiManager console for first time setup

These steps may vary slightly depending on your Web browser.

1. In your hypervisor, ensure vdiManager is started and in a powered-on state.
   Note: If you have not already done so, make a note of the vdiManager IP address.
2. In your Web browser's URL box, type https://<vdiManagerIPaddress>/admin/ and press Enter. A security warning about the Web site's certificate may appear.
3. Accept the certificate as trusted and continue. If additional warnings appear, accept those, too. The Citrix VDI-in-a-Box Administrator Login page appears.
4. On the Citrix VDI-in-a-Box Administrator Login page, in the Username box, type vdiadmin.
5. In the Password box, type kaviza and click Log On. The Citrix VDI-in-a-Box Administrator Login page appears.
6. To accept the EULA, select I have read and accept the terms of use, then click Next. The Welcome page, showing the four high-level steps necessary to complete virtual desktops, appears.

To set up the hypervisor

1. On the Welcome page, click Get Started. The Set up your Hypervisor and VDI-in-a-Box Grid page appears.
2. Click Continue. The Hypervisor page of the VDI-in-a-Box Initial Set up wizard appears.
3. In the IP Address box, type the IP address of the server running your hypervisor.
4. In the User Name and Password boxes, type your user name and password. The user account must have root privileges.
5. Click Next. The Datastore page of the VDI-in-a-Box Initial Set up wizard appears.

To set up the data store and network label

The data store contains your desktop images, virtual desktops, and personal vDisks (the personalized data and applications used for personal desktops).
1. On the Datastore page, select the data store and network label.

2. Click Next. The data store information is saved and the Grid page of the VDI-in-a-Box Initial Set up wizard appears,
allowing you to create a new grid or join an existing grid.

To select a new or existing grid

Create a new grid when setting up a new VDI-in-a-Box environment. You must associate it with a database containing the users and groups who will be accessing the VDI-in-a-Box virtual machines. The database can be your Active Directory server or a locally stored database called a workgroup.

Join an existing grid when expanding a VDI-in-a-Box environment.

To create a new grid and assign a database

1. On the Grid page, select Create a new VDI-in-a-Box grid and click Next. The Configuration page of the VDI-in-a-Box Initial Set up wizard appears.

2. In User Database, select VDI-in-a-Box workgroup or Microsoft Active Directory. If you selected Microsoft Active Directory, you must provide additional information. If you selected VDI-in-a-Box workgroup, you do not need to provide this information.
The External Management check box appears only if your hypervisor is VMware ESXi.

3. If you selected Active Directory, in the IP Address box, type the IP address hosting the database.
4. If you selected Active Directory, in the Domain box, type the DNS domain.
5. If you selected Active Directory, in the User Name and Password boxes, type your user name and password. The user should have Domain Administrator privileges; if this is not possible, see http://support.citrix.com/article/CTX136282 for details of the minimum permissions needed if you use a Domain User account instead.
6. If your hypervisor is VMware ESXi, follow these steps. If your hypervisor is XenServer or Hyper-V, continue to step 7:
   1. If VMware vCenter manages servers in the grid, select vCenter manages servers in this grid.
   2. In the IP Address box, type the IP address of the server running vCenter.
   3. In the User Name and Password boxes, type your vCenter user name and password. The user must have Domain Administrator privileges.
7. Click Next. The question “Have you reserved a dedicated IP address for VDI-in-a-Box Manager?,” appears.

8. Select Yes or No and click Done. The Generate a Base Desktop Image page appears. You now need to create a Windows image and import it into VDI-in-a-Box as a base for generating desktops; for details, see Create the first Windows image.

To join an existing grid
1. In the VDI-in-a-Box Initial Set up wizard, on the Grid page, select Join a VDI-in-a-Box server on an existing grid and click Next. The Configuration page of the VDI-in-a-Box Initial Set up wizard appears.
2. On the Configuration page, in the IP Address box, type the IP address of the vdiManager in the existing grid.
3. On the Configuration page, in the User Name and Password boxes, type your vdiManager console user name and password.
4. Click Next. The grid configuration process is finished.
Create the first Windows image

Nov 25, 2013

After you have created your VDI-in-a-Box Manager (vdiManager) and associated it with a data store, database, and grid, you can create your first Windows image.

Use your hypervisor to create a new virtual machine running one of the supported Windows operating systems. Refer to your hypervisor documentation for details.

When creating the virtual machine, be sure that it meets the following conditions:

- The virtual machine is running one of the supported Windows operating systems.
- Remote Desktop Connection (RDP) functionality must be enabled on the virtual machine.
- The virtual machine has only one network interface card (NIC) and it is assigned to Device 0.
- The virtual machine has only one disk image with a maximum size of 65 GB. By default, the maximum image size is 65 GB. If you need to increase the maximum image size, you must increase the size of the export folder as described in http://support.citrix.com/article/CTX138113.
- The virtual machine must be started and in a powered on state before importing into VDI-in-a-Box.
- The virtual machine has at least 4 GB of space available, or 8 GB if you plan to provision personal desktops.

Note: For Hyper-V Server 2012 R2, only Generation 1 virtual machines are supported.

To prepare for importing the image

You must complete the following steps outside VDI-in-a-Box. See the respective manufacturers’ documentation for details.

1. Enable the Local Administrator account on the virtual machine. This step is not necessary if the VM is running Windows XP.
2. Install your hypervisor’s management tools on the virtual machine. See the hypervisor manufacturer’s documentation for details.
3. If desired, join the virtual machine to a domain.
   Note: The virtual machine can be a member of a workgroup.
4. Log on to the virtual machine as the local administrator and enable remote connections for your users.
5. Enable File and Printer Sharing in firewall settings to allow remote agent installation. See the firewall manufacturer’s documentation for details. Ensure that your network is identified as a private or domain network.
6. If the VM is running Windows XP, in the Advanced Setting section of the View dialog box (My Computer > Tools > Folder Options > View), disable Use simple file sharing.

To import the Windows virtual machine

If the Generate a Base Desktop Image page is not currently displayed in your Web browser, navigate to your new vdiManager (https://<vdiManagerIPaddress>/admin/) and log on.

1. On the Generate a Base Desktop Image page, click Continue.
2. On the Import new VM page, select the virtual machine you want to use as an image.
3. In the New Image Name box, type a name for the imported virtual machine. 
   Note: The name should be different from the name of the source image.
4. In the Description box, type a description of the virtual machine.
5. Leave the Install Agent manually check box cleared. Citrix recommends you select manual installation only if you 
   require custom installation of agent components, or as a fallback if automatic installation does not work in your 
   deployment environment. For details of how to install the agent manually, see Install the Desktop Agent manually.
6. Click Import. The Specify Administrator Credentials dialog box appears.

   ![Specify Administrator Credentials](https://docs.citrix.com)

   Note: If the VM is running Windows XP, the option for selecting a local user with administrator privileges is not available.
7. Select whether to provide credentials for an administrator or a local user with administrator privileges. 
   Important: If you select to use the credentials for a local user with administrator privileges, disable the Microsoft 
8. Type the user name and password for an account with administrator privileges on the image and click OK. The import 
   and Desktop Agent installation process begins creating a draft image, and a status page appears showing the progress. 
   The Edit Image page of the Import new VM wizard appears.

To edit the draft image

Add any necessary updates, settings, or patches as well as any applications to be included in the image. A checklist is
provided to help ensure the image meets all prerequisites for producing desktops.

1. On the Edit Image page, click Connect.

![Edit Image page](image1)

2. In the Citrix VDI-in-a-Box Log in dialog box, provide your administrator credentials for the image and click Log in.

![Citrix VDI Log in](image2)

3. Edit the image as necessary and log off.
4. In the Citrix VDI-in-a-Box Log in dialog box, click Cancel to close it.
5. On the Edit Image page, click View. A list of prerequisites, in question format, appears. 
   
   Note: The prerequisites vary based on hypervisor and image operating system.
6. Click Yes to indicate each prerequisite has been met.
7. When all prerequisites have been met, click Done. The prerequisites close and the Edit Image page appears.
8. Click Next. The Prepare Image page appears.

To prepare the image
On the Prepare Image page, select whether the image will be used to generate pooled or personal desktops. For details about personal desktops, see Manage personal desktops. An image prepared for use with a personal desktop can also be used to generate pooled desktops. However, if you intend to use an image to generate pooled desktops only, prepare it using the Pooled desktops option to avoid adding unnecessary personal vDisk settings.

1. On the Prepare Image page, in the Domain name box, if it is active, select the domain or workgroup.
2. In the optional Organizational unit (OU) box, type the organization unit to which the image will apply.
3. Select Pooled desktops or Pooled and personal desktops.
4. Click Prepare. The Confirm message appears.
5. Click Confirm. The Confirm message and the Prepare Image page close. A status page appears showing the progress. A test desktop is created based on the prepared image and the Test Image page appears.

To test the prepared desktop image

Use the test image to verify the prepared draft image is suitable for generating your desktops and that users can connect to their desktops through HDX and RDP. The test image and any changes made to it are deleted when the draft image is saved. If you experience problems with connecting to the test image or if you need to make changes to the draft image, use the Back button to again edit and prepare the draft image.
1. On the Test Image page, click Connect. Note that you cannot save the image until you have connected to it. The Connect to the draft image dialog box appears.

2. In the Connect to the draft image dialog box, select Use Citrix HDX and click Connect. The Citrix VDI-in-a-Box Log in dialog box appears.

3. Provide user credentials and click Log in to log on to the test image through an HDX connection. The test image opens through an HDX connection.

4. Verify that the installed applications are functioning properly and the required group policies are applied.

5. If your grid is configured with Active Directory, log off and log on as a domain user to test access.

6. Log off from the test image. The test image closes.

7. In the Citrix VDI-in-a-Box Log in dialog box, click Cancel to close it.

8. On the Test Image page, click Connect.

9. In the Connect to the draft image dialog box, select Use Microsoft RDP and click Connect. The test image opens through an RDP connection.

10. Log on to the test image to verify the RDP connection works properly and then log off. The test image closes.


12. In the Confirm message, click Confirm. The Confirm message and Test Image page close. A status page appears showing the progress. The Create Desktop Templates from the Base Image page appears. For details of how to create
templates, see Create the first template from the published image.
Create the first template from the published image

Oct 04, 2013

Use templates to create uniform virtual desktops. Templates consist of an image and policies:

- The image contains the operating system and applications that run on the desktop. One image can be used by multiple templates.
  
You must create and publish at least one image before creating a template.

- Policies are characteristics such as how many desktops to create and how much RAM to allocate. You set policies while you are creating the template.

This topic describes the simplest way to create a template, using the default configuration options, which provide you with a template for pooled desktops. Full details of all the options you can choose from when configuring a template are provided in Manage templates.

1. If the Create Desktop Templates from the Base Image page is not currently displayed in your Web browser, navigate to your new VDI-in-a-Box Manager (https://<vdimanagerIPaddress>/admin/) and log on.
2. In the Create Desktop Templates from the Base Image page, click Continue. The Template Information page of the Create a New Desktop Template wizard appears.

3. In the Template Name box, type a name for the template.
4. From the list of available images, select the image you want to associate with this template.
5. In the Description box, type a description of the template.
6. The desktops created from this template will have names made up of a prefix and a suffix:
   - In the Prefix box, provide a prefix, which can include numbers, letters, and hyphens (-).
   - In the Suffix box, provide a suffix, which must be between one and four numeric characters. Leading zeros are allowed.
The combined prefix and suffix can be up to 15 characters.

7. Click Next. The Template Policies page appears.

8. In the Maximum desktops box, type the maximum number of desktops to deploy from this template.

9. In the Pre-started desktops box, type the number of desktops that should be started and available for users upon logon. You must pre-start at least one desktop.

10. Click Save.

11. Click Close. The number of desktops designated for pre-start are started and the Assign Users to Desktops page appears. For details of how to assign users, groups, and IP addresses to desktops, see Assign templates to users, groups, and IP addresses.
Assign templates to users, groups, and IP addresses

When you have created your templates, you can assign them to users, user groups, and IP addresses. Users and groups can have multiple templates assigned to them. When templates are assigned to an IP address, such as for a kiosk, all users logging on at that kiosk receive the same desktop.

If a user has not been assigned a template and logs on, that user receives the default template. If you have not specified a default template, that user's credentials are rejected.

If the Assign Users to Desktops page is not currently displayed in your Web browser, navigate to your VDI-in-a-Box Manager (https://<vdiManagerIPaddress>/admin/) and log on.

To assign templates to user groups

1. On the Assign Users to Desktops page, click Continue. The Users page appears. It contains tables for user groups, users, and IP addresses.
2. At the User Groups table, click Add. A row for a new user group entry appears in the User Group table.

3. In the Group Name box, type the name of the group to which you want to assign a template. If Active Directory is used as the user database, type the first characters of the group name and press Enter to select from matching groups.
4. In the Description box, type a group description.
5. Select the templates you want to assign to the group, then click Save.
6. Repeat these steps to assign templates to additional groups.

To assign templates to users

1. At the Users table, click Add. A row for a new user entry appears in the Users table.

2. In the User ID box, type the user ID of a user to whom you want to assign a template. If Active Directory is used as the user database, type the first characters of the User ID and press Enter to select from matching IDs.
   
   Note: First Name, Last Name, and Group are optional and automatically filled in if the user and full information are in Active Directory.
3. Select the templates you want to assign to the user, then click Save.
4. Repeat these steps to assign templates to additional users.

To assign templates to incoming IP addresses
1. At the IP Addresses table, click Add. A row for a new IP address entry appears in the IP Addresses table.

2. In the IP Address Ranges box, type the ranges of the user device IP addresses to which you want to assign a template. Addresses can be added as individual addresses (192.168.23.143), prefixes (192.168), or ranges (192.168.10.174-204). Separate entries with new lines or spaces.

3. From the templates list, select the template you want to assign to the IP address.

4. Click Save. The IP address is added to the table.

5. Repeat these steps to assign additional templates to IP addresses.

   Note: Once a template is assigned, it cannot be assigned again until the existing assignment is terminated.

To edit template assignments

1. In the VDI-in-a-Box console, select the Users page.

2. Point to the user group, user, or IP address whose template you want to edit and click Edit.

3. Edit as necessary and click Save.
Test the connection as a user

Aug 06, 2013

After setting up a template, creating desktops from the template, and assigning them to users, log on to a desktop as a user to ensure the connection works correctly. To do this, you must first install the latest version of Citrix Receiver, if you have not already done so. If you plan to use the Java Desktop Client, you must also install Java SE Runtime Environment (JRE) 6 or 7.

To prepare your user device

Prepare your user device for testing by installing Citrix Receiver to take advantage of the HDX connections.

- If it is not already installed, from https://www.citrix.com, download Citrix Receiver following the directions provided at that web site.
- If you plan to use the Java Desktop Client, ensure you have JRE 6 or 7 installed on the user device. If necessary, obtain the latest version from https://www.java.com, following the directions provided at that web site.

To connect to the desktop

These steps may vary slightly depending on your web browser.

Note that if you use VDI-in-a-Box in Workgroup mode, as opposed to through Active Directory, users have to enter their credentials twice: once to connect to vdiManager and again to log on to Windows.

1. Start your web browser.
2. In the web browser address box, type https://<vdiManagerIPaddress>/.
   A security warning about the web site’s certificate may appear.
3. Accept the certificate as trusted and continue.
4. In the Citrix VDI-in-a-Box page, in the Username box, type your user name.
5. In the Password box, type your password and click Log On.
6. Click the desired desktop. You are connected to the virtual desktop.

To connect to the desktop through the VDI-in-a-Box Java Desktop Client from a web browser

These steps may vary slightly based on the web browser you are using.

1. Start your web browser.
2. In the web browser address box, type https://<vdiManagerIPaddress>/dt/vdiclient.jnlp. A security warning about the web site’s certificate may appear.
3. Accept the certificate as trusted and continue. Depending on which web browser you are using, the Opening vdiclient.jnlp dialog box appears.
4. If the Opening vdiclient.jnlp dialog box appears, ensure Open with is selected and Java(TM) Web Start Launcher (default) appears from the list next to it, then click OK.
5. In the Citrix VDI-in-a-Box Client dialog box, type your user credentials and click Log On. If multiple templates are assigned to the user, the Select a Desktop dialog box appears.
6. Select the desktop you wish to test by clicking Connect. You are connected to the virtual desktop.

To connect to the desktop though the VDI-in-a-Box Java Desktop Client from a command prompt

These steps may vary slightly based on the user device you are using.

1. Open the Command Prompt window.
2. Type the command: javaws https://<vdiManagerIPaddress>/dt/vdiclient.jnlp.
3. Press Enter.
4. In the Log on dialog box, in the User name box, type your user name.
5. In the Password box, type your password and click Log On. If multiple templates are assigned to the user, the Select a Desktop dialog box appears.
6. Select the desktop you wish to test by clicking Connect. You are connected to the virtual desktop.
You can manage VDI-in-a-Box licensing through a Citrix license server, or you can manage licensing locally.

**Note**

A paid VDI-in-a-Box license includes an Enterprise level XenServer license. When you upload a VDI-in-a-Box production license to the vdiManager, a XenServer Enterprise license is automatically enabled on the underlying XenServer hypervisor.

VDI-in-a-Box operates on a concurrent user licensing model. When a user launches a desktop, a license is requested and checked out to the desktop that the user is using. When the user logs off or disconnects from the session, the license is checked back in and is available for another user. Desktops in the following categories, as viewed on the vdiManager console, count as a concurrent user: In Use, On Hold, and any personal desktop assigned to a user. When a personal desktop is assigned to a user, that desktop is reserved for that user until it is destroyed. It is treated as a concurrent desktop in use, even when the user has logged off.

Obtain your license file

1. When you purchase VDI-in-a-Box you receive an email that contains a license code and a link to My Citrix. Click the link.
2. On the landing page that appears, everything is preconfigured; do not select options from the drop-down lists. Click Continue.
3. On the next page, click Confirm.
4. On the next page, to access the license file, click Download.

Manage licensing through a Citrix license server

To connect to the license server:

1. Install a Citrix license server. For details of how to do this, see Licensing Your Product. Make a note of the license server's IP address and the License Server Manager port number.
2. In the Admin tab of the vdiManager console click Advanced Properties.
3. Scroll to the License Server section, enter the IP address and port number of the Citrix license server, then click OK.
4. Refresh the page, then click About. The license server address appears in the About VDI-in-a-Box dialog box:

For more details of managing licensing through a Citrix license server, see Licensing Your Product.

Manage licensing locally
To upload a license file:
1. In the Admin tab of the vdiManager console click Grid Maintenance, then click OK.
2. Click Grid and License Upgrade.
3. Click Choose File.
   ![Grid and License Upgrade](image)
   1. Navigate to the license file and click Open.
   2. Click Submit.
   3. After you have uploaded the license, refresh the page, then click About. The license details appear in the About VDI-in-a-Box dialog box:
   ![About VDI-in-a-Box](image)

The following table shows the results of upgrading from a VDI-in-a-Box evaluation license to a Citrix permanent license:

<table>
<thead>
<tr>
<th>Existing license</th>
<th>New license uploaded</th>
<th>What happens</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDI-in-a-Box evaluation license (30 day, 10 concurrent users)</td>
<td>Citrix permanent license</td>
<td>Citrix permanent license immediately replaces VDI-in-a-Box evaluation license</td>
</tr>
<tr>
<td>VDI-in-a-Box evaluation license (30 day, 10 concurrent users)</td>
<td>Citrix non-permanent (evaluation/not for resale) license with 10 or more concurrent users</td>
<td>Citrix non-permanent license immediately replaces VDI-in-a-Box evaluation license</td>
</tr>
<tr>
<td>VDI-in-a-Box evaluation license (30 day, 10 concurrent users)</td>
<td>Citrix non-permanent (evaluation/not for resale) license with less than 10 concurrent users</td>
<td>VDI-in-a-Box evaluation license stays until it expires. Citrix non-permanent license takes effect afterward</td>
</tr>
</tbody>
</table>
The following table shows the results of upgrading from a Citrix permanent license to another Citrix license:

<table>
<thead>
<tr>
<th>Existing license</th>
<th>New license uploaded</th>
<th>What happens</th>
<th>Expiration displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix permanent license with &lt;number&gt; of concurrent users</td>
<td>Citrix permanent license with &lt;number&gt; or more concurrent users</td>
<td>Both licenses take effect with the concurrent users added together</td>
<td>Permanent</td>
</tr>
<tr>
<td>Citrix permanent license with &lt;number&gt; of concurrent users</td>
<td>Citrix permanent license with less than &lt;number&gt; concurrent users</td>
<td>Both licenses take effect with the concurrent users added together</td>
<td>Permanent</td>
</tr>
<tr>
<td>Citrix permanent license with &lt;number&gt; of concurrent users</td>
<td>Citrix non-permanent license with &lt;number&gt; or more concurrent users</td>
<td>Both licenses take effect with the concurrent users added together until the non-permanent license expires</td>
<td>Permanent</td>
</tr>
<tr>
<td>Citrix permanent license with &lt;number&gt; of concurrent users</td>
<td>Citrix non-permanent license with less than &lt;number&gt; concurrent users</td>
<td>Both licenses take effect with the concurrent users added together until the non-permanent license expires</td>
<td>Permanent</td>
</tr>
</tbody>
</table>
Manage VDI-in-a-Box

Apr 26, 2013
This section contains information about configuring and managing VDI-in-a-Box.

- Manage images
- Manage templates
- Manage desktops
- Manage user sessions
- Manage servers
- Manage a grid
Manage images

Oct 21, 2013
You can create a new image either by copying a published image and editing the copy, or by adding a completely new image.
To update an image, edit a published image.

To save an image under a different name, follow the instructions below for updating an image, then edit the name and description before saving it. Note that after an image has been saved under a different name, existing personal desktops cannot change to the new image. For more details of updating templates to use different images, see Manage templates.

You can export a copy of a published image to use as a XenDesktop master image for creating desktop catalogs, or to use when transferring an image between different VDI-in-a-Box deployments. The VM created has the VDI-in-a-Box desktop agent removed but retains any applications and settings.
Note: For details of how to move your VDI-in-a-Box deployment to XenDesktop, see http://support.citrix.com/article/CTX136081.
You can use Microsoft's System Preparation Utility (sysprep) as an alternative to the VDI-in-a-Box preparation tool. To display a check box to select sysprep on the Prepare Image page of the Import new VM wizard, from the Admin tab, click Advanced Properties, then select Show sysprep option on prepare dialog. Note that you must use the VDI-in-a-Box preparation tool to prepare an image for use with a personal vDisk.

To create a new image from a published one
Use this procedure to copy an image to create a new image with different settings or applications.

1. In the vdiManager console, click the Images tab.
2. In the row of the image you want to copy, click Copy.
3. In the Copy to new image dialog box, type a name and description for the new image and then click OK.
4. When the Images page shows the status for the new image as “Running,” click Edit, then follow the instructions in the Edit image wizard. For help with the wizard, see Create the first Windows image.

To create a completely new image
1. In the vdiManager console, click the Images tab.

2. Click Add, then follow the instructions in the wizard. For help with the wizard, see Create the first Windows image.

To update an image

Use this procedure to apply changes such as software updates to a published image.

1. In the vdiManager console, click the Images tab.
2. In the row of the image you want to update, click Edit, then click Confirm. A draft image, based on the image you want to update, is created.
3. When the Images page shows the status for the draft image as “Running,” click Edit, then follow the instructions in the Edit image wizard.
4. From the Edit Image wizard, connect to the image to add any necessary updates, settings, or patches as well as any applications to be included in the deployed image.
5. Log off from the draft image and follow the instructions in the wizard. After you save the new draft image, it becomes the new version of the published image and the previous version of the image is deactivated. The image changes are propagated to the desktops based on the associated template refresh policies.

To fix an image

Use this procedure if vdiManager reports that an image stored on one or more servers in a multi-server grid is not the same on all servers. In that case, the image status changes to “broken” and desktops are not generated from it until the image is fixed.

1. In the vdiManager console, click the Images tab.
2. In the Status column, click the Published link, then under the Fix column, click the icon.
3. Click Confirm.

To export an image

Use this procedure to export a published image for use as a XenDesktop master image or to transfer an image between different VDI-in-a-Box deployments.

1. In the vdiManager console, click the Images tab.
2. Click the name of the image you want to export. The Image Properties dialog box appears.
3. Click Export. The Export Image dialog box appears.
4. Select the data store on which you want to store the image, enter a name for the exported VM, then click Export.
   Note: Characters in the exported VM name can be only letters, numbers, underscores, hyphens, periods, and spaces. You are notified that the image has been queued for export.
5. The new VM that is being created appears on the Images page. To monitor progress details, click View. When you are exporting an image, errors may occur during the process. To ensure you are aware of these, in the Recent Tasks and Events panel, click on the relevant export task to display its status history. When the export is complete, the progress box closes and a message appears confirming that the export has been successful.
6. Log on to the new VM and check the Add/Remove programs list to make sure all Citrix components have been removed. If they have not, manually remove them before using the exported image.
Install the Desktop Agent manually

Dec 20, 2012

The VDI-in-a-Box Desktop Agent resides on each desktop created from the image. vdiManager communicates with the desktop through the agent. The Desktop Agent is automatically installed when the draft image is being imported into the VDI-in-a-Box Manager (vdiManager). The Desktop Agent on existing images is automatically updated when they are migrated from one version of VDI-in-a-Box to another.

If the automatic installation fails, you can manually install the Desktop Agent. When you are importing an image you can also choose to manually install the Desktop Agent.

To manually install the Desktop Agent on a draft image

These steps may vary slightly depending on your Web browser.


2. Click Copy to clipboard, copy the resultant URL to download the Desktop Agent, and click OK. The URL should be in this format: https://vdimanager ip address/dt/dtagent

3. Click Connect. The logon screen of the image appears.

4. Log on to the desktop, start a Web browser, and paste the URL copied in Step 2 into the Web browser URL box and press Enter. A security warning about the Web site's certificate may appear.

5. Accept the certificate as trusted and continue. The Install the Desktop Agent page appears.
1. Please verify the following information before proceeding:
   - Make sure that the image is member of the correct domain or workgroup.
     (If not, please add the image to the correct domain/workgroup. Doing so will require you to reboot the image before proceeding. In which case, save the USB at this page.)
   - Make sure that the Windows firewall or an anti-virus software is not blocking TCP ports 1494, 2598, 3389, and 8000.
   - Make sure that the remote desktop access is enabled for the desktop users by adding the desktop users to the Remote Desktop Users group.
   - Make sure that the anti-virus versions of Citrix VDI-in-a-Box Desktop Agent, Citrix Virtual Desktop Agent, or Citrix PodICA are not installed on the image.

2. Install the Desktop Agent.

3. Once the Desktop Agent is installed, close this window and return to VDI-in-a-Box setup.

6. Verify the information listed in Step 1 of the Install the Desktop Agent page.
7. Click Install. The File Download - Security Warning dialog box appears.
8. Accept any security warnings that may appear. The Citrix VDI-in-a-Box Desktop Agent Setup wizard, which installs the agent, appears.
9. Click Install.
   Important: During the installation process, the Citrix VDI-in-a-Box Desktop Agent Installation and Configuration dialog box appears. The messages in this dialog box may pause, indicating success or failure of individual steps in the installation process. Do not click any buttons in this dialog box or interrupt the installation. When the process is complete the dialog box closes.
   The image automatically restarts following the successful Desktop Agent installation.
Manage templates

Nov 22, 2013

This topic provides guidance about the options you can choose from when configuring a template. The options are listed in the order in which they appear on your screen.

To edit a template, click the Templates tab, click the name of the template you want to edit, make your changes, then click Save.

Type a name and description for the template, and select the image you want to base the template on.

If the template is for personal desktops, you cannot change the image on which the template is based.

Establish naming patterns for all desktops generated by your template by setting computer names with prefixes and suffixes.

The prefix and suffix can combine to be up to 15 characters long. The suffix must be at least one numeric character and can be up to four numeric characters.

Use leading zeros in the suffix to hold places for up to four digits. The number generated by the suffix increases with each virtual desktop. For example, if you set the computer prefix to ‘Sales’ and the suffix as 0000 and generate two virtual desktops, they will be called Sales0000 and Sales0001. If leading zeros are not included in the suffix, they will not be included in the resulting names. For example, a suffix value of 1 would produce Sales1, Sales2, Sales3, and so on.

Citrix recommends allocating at least 1536 MB of memory for Windows 8, Windows 7, Windows Server 2012, and Windows Server 2008 R2 desktops. For Windows XP desktops, a minimum of 512 MB of memory is required and 1 GB of memory is recommended.

Select the number of virtual cores for each desktop.

To allow users to access peripherals that are on or attached to their local device, select the relevant check box. Note that:

- If you select Smart cards, users must access desktops through smart cards. If a user attempt to access a desktop without smart card authentication, the desktop is locked.
- If you select Other USB devices, this allows users to access locally attached USB devices such as webcams and scanners in their virtual desktop. Changes to this setting are applied on virtual desktop startup; they are not applied to existing running desktops.

Color depths lower than 32-bit are available only on Windows 7 desktops and Windows XP desktops. To be able to select lower color depths on Windows 7 desktops, you must first enable the Legacy graphics mode policy as follows:

- If you are using Active Directory, set up a Citrix Group policy to enable Legacy graphics mode for Active Directory
If you are using Workgroup, set up the following registry key in the image:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\GraphicsPolicies]
"LegacyGraphicsMode"=dword:00000001
```

To select lower color depths on Windows XP desktops, no policy set up is needed: just select the relevant depth from the drop-down list.

Select this check box to display the Desktop Viewer for HDX connections and the connection bar for full-screen RDP connections. This setting is applied only when the user connects from Windows-based devices.

If your published image has a Key Management Service (KMS) activation key, Citrix recommends selecting Reset the activation timer (KMS clients).

If you are using Key Management Service (KMS)-based activation for your desktops, there must always be 25 desktops with unique Client Machine IDs (CMID) requesting activation from the KMS server. The KMS server will not activate any desktop if there are fewer than 25 desktops with unique CMIDs. To ensure that your desktops have unique CMIDs, select Reset the activation timer (KMS clients).

Specify the maximum number of desktops that can be deployed from the template. This number represents the total of the number of desktops to which users can be connected at any one time, including the number of pre-started desktops ready for use.

Pre-started desktops are in a powered-on state and ready for use as soon as the user logs on. When you specify a number of desktops for pre-start, VDI-in-a-Box maintains that number as users log on. For example, if you specify five pre-started desktops in the template, there will always be five virtual desktops started and waiting for your users. When two users log on to their desktops, VDI-in-a-Box starts two more desktops to maintain the requested five pre-starts. This continues until your stated maximum number of desktops for the template is reached.

You must pre-start at least one desktop or users will not be able to access a desktop.

For testing purposes, Citrix recommends setting a maximum of two desktops with one pre-started desktop.

If you select to create a template for pooled desktops, the following options are available. Note that if you are editing an existing template, you cannot change it from a pooled desktop template to a personal desktop template.

- **Refresh desktop**
  
  The refresh method determines when users' desktops are replaced with a fresh desktop matching the template:
  
  - **On logout**: Refreshes the desktop each time the user logs off. This does not apply to administrators; for debugging reasons, the 'administrator' account is allowed to log on and off without triggering desktop lifecycle events.
  
  - **Scheduled**: Refreshes at a set day and time on a daily, weekly, or monthly basis. You can include desktops in use at the scheduled time. If you exclude in-use desktops, they are replaced when the user logs off following the scheduled refresh.
This is a useful option in situations where a site has multiple shifts (classrooms, helpdesk and support setup, for example): if you provision sufficient additional desktops to handle the period of transition between the two groups of users, you can avoid the potential boot storm caused by the current shift logging off.

- Scheduled or on logout: Refreshes at a set day and time and each time the user logs off. This is useful in environments where users log on to desktops for extended periods.
- Manual: Refreshes only through your action. This setting results in a persistent or static desktop, one which remains with the user indefinitely. Users can add applications and other modifications with the expectation that they will be available with each log on. This type of desktop has some limitations:
  - Users are not able to take advantage of any base image update without destroying and recreating the desktop.
  - A static desktop is attached to a particular server and cannot be moved to a different server, so if the server is down, the user has no access to the desktop.
  - A static desktop cannot be refreshed at the template level through a Refresh action: unlike the other desktops provisioned from the template, it has to be refreshed individually.
Because of these limitations, Citrix recommends using personal desktops instead of manually refreshed pooled desktops. For details of personal desktops and best practices to follow when using them, see Manage personal desktops.

- Do not reassign desktops 'On hold' to new users
  You can allow users to hold desktops so that when they log off the desktop cannot be reassigned to anyone else. When this happens, the desktop appears as On Hold in the Session tab, and when the user connects again, he will log on to the same desktop; the desktop then becomes active again.

- Enable fast refresh of desktops
  By default, the refresh process is completed as quickly as possible when users log off. Citrix recommends disabling this option only for troubleshooting purposes if you experience issues with desktop refresh.
  This option is not available for manually refreshed desktops.

- Desktops follow users to other access devices
  This option is selected by default: if a user disconnects from a desktop then logs on at another device, they get the same desktop.
  If you are working in an environment where users need a fresh desktop every time they log on, clear this check box. For example, if you have selected generic user mode and want a template for generic rather than personal users, by clearing this check box you ensure that users who log on using the same generic user name always get different desktops. When a user disconnects, if they log on again under the same user name at a different device they get a fresh desktop. For information about configuring generic user accounts, see Configure generic user accounts.

  Note: If you created a template using VDI-in-a-Box 5.3 or earlier, with generic user mode enabled, then this check box is cleared by default. To edit the template and make it suitable for use by personal rather than generic users, select the check box. Make sure there are no user sessions running on desktops that use this template before you make any changes.

If you select to create a template for personal desktops, the following option is available. Note that if you are editing an existing template, you cannot change it from a personal desktop template to a pooled desktop template
- Personal disk size. Ensure that you specify sufficient space to host any user-installed applications, and, if you are not using Profile management, sufficient space for the user settings. The valid range is between 10 and 60 GB.
If you change the size of the personal disk after creating a template, note that the change applies only to personal desktops created after the change has been made, not to existing desktops. For information on changing the personal disk size for existing desktops, see http://support.citrix.com/article/CTX136156.

For more details of personal desktops and best practices to follow when using them, see Manage personal desktops.

Select this option to make this template the default template for the grid. This overrides any existing default template.

If a user has not been specifically assigned a template, when they log on they will be allocated a desktop based on this template. If no default template for the grid has been specified, they will not be able to log on.
Manage desktops

Nov 05, 2013

Pooled desktops refresh according to the refresh policy configured for the template. Force a refresh as follows.

1. From the VDI-in-a-Box Manager (vdiManager) console, from the Desktops tab, click Summary.
2. In the Refresh column, click the link for the template entry.

![VDI-in-a-Box Manager Console](image)

The Confirm dialog box appears, identifying the refresh policy.

![Confirm Dialog Box](image)

3. Click Confirm to immediately refresh those desktops currently in use or click Cancel to refresh the desktops according to their established refresh policies.

Note that you cannot force a refresh on a personal desktop in this way. To manage personal desktops that are in use, click User Sessions, then Actions. For general information on updating personal desktops, see Manage personal desktops.

1. From the vdiManager console, from the Desktops tab, click User Sessions.
2. Click Actions for the user entry you want to act upon.
The Actions menu appears.

The menu omits Restart and Shut Down if the desktop refresh policy is set to "On logout." Shadowing users is described in Manage user sessions.

3. Select the action you want to take and then click Confirm.

A desktop in an unknown state has the status Broken and is not available to users. Causes for broken desktops:

- Typically, broken desktops are unable to start Windows due to a missing or incorrect startup configuration, such as an incorrect product key or domain credentials. Use a console client to see if the broken desktop is waiting on user input.
- The server is too heavily loaded to start new desktops.
- The disk space on the data store is full.
- There are no available MAC addresses.
- The template image no longer exists.

Before destroying a broken desktop, determine the problem, repair the desktop, and then test the desktop to ensure that working desktops replace the broken ones.

1. From the vdiManager console, from the Desktops tab, click Summary. Alternatively, click the Servers tab and then click Desktops.
2. Click the number link in the Broken column and then click Destroy.
3. Click Confirm.
Manage personal desktops

**Nov 05, 2013**

The personal desktop feature retains the single image management of pooled desktops while allowing users to install applications, change their desktop settings, and store data.

Personal desktops are available for published images running Windows 8.x or Windows 7 (32-bit and 64-bit editions).

Note: Windows 8.x personal desktops are not supported on Microsoft Hyper-V Server 2008 R2.

Note: The first time a user logs on to a Windows 8.x personal desktop, the logon process takes longer than usual: between 5 and 10 minutes. This is because the Metro apps are installed the first time a user logs on.

Unlike pooled desktops, where users lose their customization and personal applications when the desktop refreshes, personal desktops retain those changes. This means administrators can centrally manage their base images while providing users with a customizable desktop experience.

Personal desktops allow this flexibility because they are composed of two separate virtual hard disks: a personal vDisk and the published image. Any changes made by users, such as changing their profiles or installing applications, are saved to the personal vDisk. The content of the personal vDisk is blended at runtime with the content from the published image to provide a unified experience. The two virtual disks are visible on the personal desktop through Windows Explorer and other applications.

Citrix recommends storing profile data on a network-attached storage (NAS) server along with the use of a profile management application such as Citrix Profile management, included with VDI-in-a-Box. If you use Profile management, Citrix recommends disabling Profile Redirection in the personal desktops. As a result, profile data is saved to Profile management only, bypassing the personal vDisk and eliminating the backup copy. To create a backup, see Back up and restore personal desktops. To disable profile redirection, see [http://support.citrix.com/article/CTX131553](http://support.citrix.com/article/CTX131553).
VDI-in-a-Box provisions personal desktops by always prestarting them based on template configurations:

1. A linked clone is created for the new desktop based on the image specified by the template.
2. An empty personal vDisk is created. It is then linked to the underlying linked clone using the inventory process, which involves creating an inventory for the image and synchronizing it with the personal vDisk.
3. The personal desktop is created. It consists of three layers: the image, the linked clone, and the personal vDisk.
4. The personal desktop is prepared and started.

When a user tries to connect to the personal desktop, VDI-in-a-Box passes an ICA handle to the user's device and the user can then log on.

1. Create a Windows 8 or Windows 7 image as described in the Get Started section, making sure that you select Pooled and personal desktops when you are preparing the image.

Citrix recommends the following best practices when creating images for personal desktops:

- Disable automatic Windows updates in the published images. Updating images centrally ensures consistency and permanence across your environment.
- Add CtxPvd.exe and CtxPvDsSvc.exe, located under C:\Program Files\Citrix\Personal vDisk\bin, to the list of processes whose activities should be excluded from scanning by antivirus software.

Inventory operations and image update operations involve significant file I/O. These operations comprise scanning and creating a large number of files. If antivirus scanning is enabled during the personal vDisk inventory or image update operation, this can slow down the process significantly.

2. Create a template as described in the Get Started section, making sure that you select Personal desktop on the Policies page. When you specify the personal disk size, ensure that you specify sufficient space to host any user-installed applications, and, if you are not using Profile management, sufficient space for the user settings. The valid range is between 4 and 60 GB.

You can edit the template and change the size of the personal disk after creating a template, but note that the change applies only to personal desktops created after the change has been made, not to existing desktops. For information on changing the personal disk size for existing desktops, see http://support.citrix.com/article/CTX136156.

Updates to the published image are received by the personal desktop as soon as the user logs off. The image refreshes without modifying the personal vDisk. However, refreshing a personal desktop can take up to an hour; Citrix therefore strongly recommends that you update the images used by personal desktops only during off-hours, and after all users have logged off from their personal desktops. This ensures that users do not experience any downtime after the maintenance period.

After updating a personal desktop image, make sure that all the personal desktops provisioned from the image were refreshed to the latest version. The current image version and the personal vDisk version should be identical.

To find the current image version:

1. In the vdiManager console, click the Servers tab.
2. Click Images.
3. Check the image version. The current image has a green indicator. A yellow indicator means that an image transfer is in progress.

To find a personal desktop's current personal vDisk version:

1. In the vdiManager console, click the Desktops tab.
2. Click the User Sessions tab.
3. Select the Show all sessions check box.
4. Click on the VM name.
5. Scroll down to find the personal disk version.

You can use a shared storage data store to provide high availability for personal vDisks. For information on how to configure VDI-in-a-Box and your hypervisor to use shared storage, see http://support.citrix.com/article/CTX136080. Note: VDI-in-a-Box cannot make use of shared storage when running on XenServer or Windows Server 2008-based hypervisors.
Back up and restore personal desktops

Aug 30, 2012

Protect your users' profiles and applications by backing up their personal desktops. The restored backup is attached to a fresh desktop generated from the published image to form a new personal desktop.

The following steps apply when using XenServer, Hyper-V, or ESXi.

1. Obtain the personal disk name of the personal desktop you are backing up: From the Desktops tab, on the User Sessions page, in the row containing the personal desktop, click the VM Name, make note of the personal disk name and click Close.

![Desktop Details - BuildA0004](image)

2. Shut down the personal desktop: From the Desktops tab, on the User Sessions page, in the row containing the personal desktop, click Actions and then click Shutdown.

Use Citrix XenCenter for the following steps.

1. Export the personal desktop to another location accessible to XenServer.
2. Import the exported OVF or XVA file to another server on your VDI-in-a-Box grid.
3. Detach the personal disk from the published image, and then delete the published image. The personal disk is stored, unattached to an image and available when needed.

Perform the following tasks on the Windows-based device used for Hyper-V management.

1. Map to Drive C of the Hyper-V server hosting the personal desktop being backed up.
2. Map to Drive C of the Hyper-V server on which the personal desktop would be restored.
3. From the data store containing the personal disk images, copy the personal disk to the server on which it would be restored.

Note: By default, personal disks are stored in C:\ProgramData\Citrix\VIAB\PVD.
Use VMware vSphere for the following steps.

1. Connect separate instances of vSphere to the server hosting the personal desktop being backed up and the server on which the backup will be stored.
2. From the server hosting the personal desktop, from the PVD folder, download the personal disk. Two separate files, `<PersonalDiskName>.vmdk` and `<PersonalDiskName>-flat.vmdk`, are downloaded.
3. From the server that will store the backup, upload both files to the PVD folder.

The following steps apply when using XenServer, Hyper-V, or ESXi.

1. From the vdiManager console, from the Desktops tab, select the User Sessions page.
2. In the row for the damaged desktop, click Actions and then click Repair. The data stores are searched for a matching copy of the selected personal desktop. If found, a confirmation message appears stating that you are about to repair a personal desktop by destroying the damaged copy and replacing it with the found copy.
3. Click Confirm. VDI-in-a-Box restores the backed up copy on the server on which it was stored.
Generate desktops from a pool of MAC addresses

Aug 30, 2012

Generate desktops with a specified range of Media Access Control (MAC) addresses if your Dynamic Host Configuration Protocol (DHCP) policies assign IP addresses to MAC addresses or assign free IP addresses only to MAC addresses from a known range. The MAC address pool applies to all desktops, draft images, and test images generated throughout the VDI-in-a-Box grid.

**Pre-requisites:**

- Verify there are enough MAC addresses in the pool to handle all the desktops and draft images that are planned in the grid.
- Verify that external systems, such as DHCP, that the MAC address pool is intended to serve can handle all of the MAC addresses in the pool. The pool assigns addresses to desktops randomly.

Note: VDI-in-a-Box does not verify that an assigned MAC address is unique in a network, except within the desktops in the grid. If a server leaves a grid that has MAC addresses assigned to desktops, the original grid does not track that the MAC addresses are assigned to desktops and so can reassign them.

1. From the VDI-in-a-Box Manager (vdiManager) console, from the Admin page, click Advanced Properties.
2. Scroll to the MAC Address Pool section and provide the starting address and range length. The MAC address range must be in the following format: 00:50:56:[0-3]:xx:xx.

![Advanced Properties](image)

**Figure:** Advanced Properties for MAC Address Pool
Manage user sessions

Oct 04, 2013

You can manage various aspects of user sessions:

1. From the vdiManager console, from the Admin tab, click Advanced Properties, then scroll to the User Session section.

2. Customize user sessions as follows:
   - To change the dimensions of the desktop window, use Desktop session default width and Desktop session default height. By default, desktops open in full-screen mode. These properties do not apply to connections made with Citrix Receiver.
   - To require users to enter a password to log on to a desktop, select Require users to re-enter password on Windows logon screen. By default, this setting is not enabled.
   - To save users' credentials in the Java Desktop Client, select Retain user credentials in the VDI-in-a-Box Java Desktop Client. By default, this setting is not enabled, causing the users' credentials to be cleared after logon.
   - To set the amount of time a user session can be idle before it is automatically ended, use Log off idle user session from the web console. The default setting is five minutes.
   - To prevent users restarting active or on-hold desktops, clear Users can restart "active" or "on hold" desktops assigned to them. This setting is enabled by default.

3. To save updated settings, click OK.

You can use Remote Assistance to share your users' desktop screens and shadow their actions for troubleshooting purposes.

Note: Session shadowing is not supported for Windows XP desktops.

For Remote Assistance to work on a desktop, the Configure Solicited Remote Assistance group policy must either be enabled or left unconfigured.

To launch Remote Assistance:

1. Launch the vdiManager console from a Windows desktop.
2. From the Desktops tab, select User Sessions.
3. Click Actions for the relevant session, then click Shadow.
   
   Note: The user must be connected to the session you want to shadow.

4. After the connection initializes, a dialog box prompts you to save the .msrcincident file.
5. Open the .msrcincident file with the Windows Remote Assistance viewer, if the file is not already selected by default.
6. Take a note of the access password displayed in the vdiManager console.
7. Enter the access password in the Windows Remote Assistance viewer. A confirmation prompt appears on the user's desktop.
8. Instruct the user to click Yes to allow you to shadow the session.
9. For additional control, request the user to share keyboard and mouse control.
Log on to the VDI-in-a-Box appliance

Apr 26, 2013

You can use the hypervisor console or a Secure Shell (SSH) client, such as PuTTY, to log on to the VDI-in-a-Box appliance. This enables you to:

- Change the password for the appliance
- Obtain detailed logs for troubleshooting purposes

Initial credentials for the appliance are:

- User name: kvm
- Password: kaviza123

Citrix recommends changing the default password in the production environment. Change credentials for user names kvm and root from their initial password "kaviza123" by logging on as each of those users and using the passwd command.

Important: When changing these passwords, do so for each VDI-in-a-Box Manager (vdiManager) in the grid. Passwords are associated with the vdiManager appliances, not the entire grid.

1. From your hypervisor console or an SSH client, open the vdiManager.
2. Using the account whose password is to be changed, log on to the vdiManager.
3. At the command prompt, type passwd and press Enter.
4. When prompted, type the current password and press Enter.
5. When prompted type the new password and press Enter.
6. When prompted, type the new password again for confirmation and press Enter. A message confirming the successful password change appears.
Manage servers

Apr 13, 2015

You can manage various aspects of server performance:

1. From the vdiManager console, from the Admin tab, click Advanced Properties, then scroll to the Miscellaneous section.

2. To optimize server performance, use the following properties:
   - To set the maximum load assignable to a server, use **Max server load (90%)**. If server failure causes desktop load to be shifted, the remaining servers on the grid will not take on a load beyond this setting, avoiding overloading. The default setting is 90% of a server's capacity.
   - To set the maximum capacity of desktops that each server will start at one time, use **Max number of starting desktops**. If the creation of a new desktop would cause the number of starting desktops to exceed this number, the system delays startup of the new desktop. This addresses performance problems due to starting too many desktops at one time. The default setting is 20; setting it to 0 disables any restriction on how many desktops can be started at one time.
   - To set the maximum number of personal desktops each server will start at one time, use **Max number of starting personal desktops**. If the creation of a new desktop would cause the number of starting desktops to exceed this number, the system delays startup of the new desktop. This addresses performance problems due to reintegrating too many personal disks with their base images at one time.

3. To save updated settings, click **OK**.

VDI-in-a-Box offers flexible data storage options to enable you to maximize performance in different types of deployment:

- By default, images, desktops, and personal vDisks (the personalized data and applications used for personal desktops) are all stored on the same data store. You specify this when you first configure your grid.
- On Microsoft Hyper-V, VMware ESXi and VMware vSphere, you can configure three separate data stores. This allows separate storage of images, desktops and personal vDisks.
- On XenServer, you can configure two separate data stores. Desktops and images must be on one data store, with personal vDisks on the other data store.

Important: Data is not moved when you change data stores. While reference points are maintained to objects in data stores you have left, the objects remain there. Plan any moves carefully and conduct them as infrequently as possible.

1. In the VDI-in-a-Box Manager (vdiManager) console, from the Admin page, click Advanced Properties.
2. Scroll to the Miscellaneous section and click **Enable multiple datastores** and then **OK**.
3. Click the Servers tab and then the server you want to update. The Server Properties dialog box appears.
4. Click **Configure**. The Configure Server dialog box appears.
5. In the Select datastores section, select data stores for your images, desktops, and personal vDisks.
   - Note: For XenServer, the option to select a separate data store for desktops is not available, because they have to be stored in the same location as images.
You must immediately update the VDI-in-a-Box server configuration parameters if any of the following credentials change: hypervisor, Active Directory, or domain controller. For environments in which account credentials change regularly, Citrix recommends using accounts that remain fixed.

<table>
<thead>
<tr>
<th>Component</th>
<th>To update in the vdiManager console</th>
<th>Impact if not changed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor credentials</td>
<td>Click the Servers tab, click the server name, and then click Configure.</td>
<td>VDI-in-a-Box cannot communicate with the hypervisor.</td>
</tr>
<tr>
<td>User Active Directory or domain controller credentials</td>
<td>Click the Users tab and then click Configure.</td>
<td>VDI-in-a-Box cannot authenticate users.</td>
</tr>
<tr>
<td>Computer Active Directory or domain controller credentials</td>
<td>Click the Admin tab, and then click Additional Domain for Desktops. Additional Domain for Desktops is enabled only if you have configured separate user and computer domains, as described in Use VDI-in-a-Box with Active Directory.</td>
<td>VDI-in-a-Box cannot authenticate computers.</td>
</tr>
</tbody>
</table>

If the IP address of the underlying hypervisor changes on a server on which you are running VDI-in-a-Box, you need to change the address in the vdiManager, otherwise VDI-in-a-Box will cease to function.

1. Destroy all pooled desktops except for any with the manual refresh policy (static desktops):
   1. Desktops are unavailable during this process, so coordinate the downtime with the users.
   2. Log on to the vdiManager console.
3. Set the number of pre-started desktops to zero for each template for pooled desktops: click the Templates tab, click the template name, click Next, in Pre-started desktops type 0, then click Save.

2. Publish or destroy all draft images. Make sure that no images are being transferred before proceeding to the next step:
   1. Click the Images tab.
   2. Ensure no draft or test images are listed.

3. Shut down all personal desktops (desktops for which user changes are saved on a personal vDisk) and static desktops: click the Desktops tab, click User Sessions, click Actions for each desktop you want to shut down, then click Shutdown.

4. Deactivate the server: in the vdiManager console, from the Servers tab, click the server, then click Deactivate.

5. Put the grid into maintenance mode: click the Admin tab, click Grid Maintenance, then click OK.

6. Change the hypervisor address at the hypervisor level.

7. In the vdiManager console, from the Servers tab, click the server, and then under Hypervisor Settings click Configure.

8. Delete the existing IP address, type the new one, type the password, and save.

9. Take the grid out of maintenance mode: click the Admin tab, click Grid Maintenance, then click OK.

10. Activate the server: from the Servers tab, click the server, then click Activate.

11. To ensure that vdiManager is operating correctly, under Advanced Actions, click Self Test. This should result in the message 'Server checks out fine' appearing in the console.

12. Reprovision any pooled desktops: for each pooled desktop template, click the Templates tab, click on the template name, click Next, in Pre-started desktops type the number of pre-started desktops you want, then click Save.

13. Restart any personal desktops: click the Desktops tab, click User Sessions, then for each personal desktop click Actions and select Restart.
Manage a grid

Jan 06, 2014

1. Import and power on the vdiManager appliance.
2. Note the IP address of the vdiManager and then use a web browser to log on to the vdiManager console (https://IPaddress/admin).
3. Follow the directions in the VDI-in-a-Box Initial Set up wizard to configure the hypervisor and join it to the grid, as described in Get started with VDI-in-a-Box. Desktops from other servers are not migrated to the new server. Desktops are created on the new server as needed to satisfy policy requirements.

When you remove a server from the grid, it becomes the only server in a new grid. It is no longer connected to the rest of the servers in the old grid and does not share its load.

1. Deactivate the server to remove all desktops running on it: From the Servers tab, click the server, and then click Deactivate.

2. Click Confirm.
3. After the server status changes to deactivated, click the Servers tab, click the server, and then click Leave Grid.

1. Put the grid in maintenance mode: from the Admin tab, click Grid Maintenance, then click OK.
2. On the Admin page, click Grid and License Upgrade. The Grid and License Upgrade dialog box appears.
3. Click Choose File. Navigate to the upgrade or license file, and click Open.
4. Click Submit. When the upgrade completes, the server status changes to Success.
5. When prompted, log on to vdiManager.
6. Take the grid out of maintenance mode: from the Admin tab, click Grid Maintenance, then click OK.

1. Let your users know when maintenance is to occur and when they must log off.
2. Citrix recommends backing up any personal desktops. (See Back up and restore personal desktops.)
3. Put the grid in maintenance mode: from the Admin tab, click Grid Maintenance and then click OK.
4. After all users log off and personal desktop backups are complete, deactivate all servers in the grid: from the Servers tab, click the server, click Deactivate, and then click Confirm. Deactivating a server deletes all desktops, including those in use, and immediately shuts down the server so that it no longer provisions desktops. Only the personal desktops remain, with a status of "On Hold."
5. Use the hypervisor console to power off the personal desktop virtual machines. To identify those desktop sessions, go to Desktops > User Sessions and look for "On Hold" entries in the Status column.
6. Shut down the vdiManager virtual machines: from the Servers tab, click the server, then click Shutdown. The servers are now ready for maintenance performed from the hypervisor.

1. Use the hypervisor console to power on all vdiManager virtual machines.
2. When all vdiManagers are running, log on to the vdiManager console and take the grid out of maintenance mode: from the Admin tab, click Grid Maintenance, then click OK. On the Servers tab, the Recent Tasks and Events section should display the message "Server checks out fine" for each server.
3. Activate each server: from the Servers tab, click the server, then click Activate.

Prerequisite:

- A static IP address that is not already assigned.

1. Put the grid in maintenance mode: from the Admin tab, click Grid Maintenance, then click OK.
2. Deactivate the server so that it is not running any desktops: from the Servers tab, click the server, click Deactivate, then click Confirm.
3. Shut down any draft or test desktops on the server: from the Desktops tab, on the User Sessions page, in the row for each desktop, click Actions, Shutdown, then Confirm.
4. From the Servers tab, click the server name, then click Modify.
5. In the VDI-in-a-Box Manager Network Settings dialog box, click Static IP configuration, enter the static IP address, then click OK. The Notification dialog box appears indicating that the change to the network configuration was successful and that the vdiManager has been restarted.
6. Click Close.
7. Take the grid out of maintenance mode: from the Admin tab, click Grid Maintenance, click OK.

Rather than having user devices access virtual desktops through the IP address of specific servers on the grid, you can assign a single virtual IP address to the entire grid. Access requests made to this address are sent to the primary server in the grid. If that server is unavailable, the virtual IP address is assumed by another server in the grid.
The grid-wide IP address must be a static IP address selected from the same subnet pool used for the other servers in the grid.

Note that you cannot use the grid-wide IP address to log on to the management console.

1. From the Admin tab, click Advanced Properties.
2. Scroll to the Grid section and in the Grid IP address box, type the static IP address you are assigning to the grid and click OK.

Resetting vdiManager to factory settings is irreversible. It deletes all the desktops, templates, images, and environment information from the grid and deletes the base image files physically stored on the data store of the hypervisor.

1. Verify that you are logged into the vdiManager console for the server you plan to reset.
2. Remove the server from the grid. Resetting a server to factory settings is not allowed on a server in a grid.
3. From the Admin tab, click Reset Server. After the reset is complete, you are logged off from the vdiManager console. The next time you log on, the Welcome to VDI-in-a-Box page appears. For information about setting up vdiManager, refer to Get started with VDI-in-a-Box.

1. If the server is part of a grid, remove it from the grid.
2. Reset vdiManager to factory settings.
3. From the hypervisor console, shut down the vdiManager virtual machine and remove it from the host. See the hypervisor manufacturer's documentation for details.

You can synchronize the clocks of the vdiManagers in your grid by connecting to a Network Time Protocol (NTP) server. A result of using NTP is consistency of log time stamps.

1. From the Admin tab, click Advanced Properties.
2. Scroll to the Grid section and in the NTP server box, type the IP address of the Network Time Protocol (NTP) server and click OK. Within an hour, the clocks on all servers on the grid are synchronized. The NTP server and the servers on the grid then synchronize hourly.

3. Configure NTP on your hypervisor, using the same NTP server as in Step 2. For details, see http://support.citrix.com/article/CTX134279.

The grid time is necessary for grid communication, such as refresh schedules. By default, the grid time is the time on the first server in the grid. Grid time is not tied to a clock and can be set to what you choose. Grid time is synchronized across all the servers in the grid every 24 hours.

Note: If the use of an NTP server is enabled, the Grid Time may be changed as NTP synchronization occurs. While this inaccuracy will self-correct when the Grid Time synchronizes, Citrix recommends checking and, if necessary, resetting Grid Time immediately after enabling NTP and again an hour later.

1. From the Admin tab, click Grid Time. The Set Grid Time dialog box appears.

2. Accept the current date and time or click in the New Date and Time box and, from the calendar that appears, select a new date.

   Note: Be sure to follow the mmm dd, yyyy hh:mm:ss [AM | PM] format.

3. If you selected a new date, edit the time to reflect the current time.

4. Click Save.
Use VDI-in-a-Box with Active Directory

Oct 30, 2013
VDI-in-a-Box provides two options for user authentication: you can set up Workgroup mode for user authentication using VDI-in-a-Box's built-in user database, or you can use Active Directory. This topic provides details of how to use Active Directory with VDI-in-a-Box.

When using VDI-in-a-Box with Active Directory you should continue to manage users through Active Directory. Most of your users will already be members of Active Directory security groups. This means you can just add these security groups to VDI-in-a-Box and assign desktop templates to these groups instead of individual user accounts. VDI-in-a-Box allows you to add both groups and users; for details of how to assign templates, see Assign templates to users, groups, and IP addresses.

You may want to add individual user accounts to VDI-in-a-Box when you are in a lab environment or test phase where only a few users will be accessing desktops. For a production environment with fewer than 20 users it is manageable to add users instead of security groups, but Citrix does not recommend this. Active Directory is designed for central management and control of users, so there is no need to manage users in two places.

VDI-in-a-Box supports Active Directory default domain accounts and nested groups:
- You can add Active Directory built-in security groups and user accounts to VDI-in-a-Box. This is a good solution if you plan to provide the same VDI-in-a-Box desktop template to all your users. Simply add the Domain Users group to VDI-in-a-Box and assign a desktop template to this group. You can do the same for Administrator, Domain Admins, and any other built-in account.
- Nested groups support is useful when users are members of groups that are members of other groups. If all the member users need access to the same VDI-in-a-Box desktop template(s), just add the main group containing all the other groups and user accounts. For example you may have a group called Sales, which contains many member groups such as East Coast Sales, Midwest Sales, West Coast Sales. Each of these groups contains multiple user accounts. To give the same VDI-in-a-Box desktop to all the Sales users, regardless of their location and specific role, add Sales to VDI-in-a-Box and assign a desktop template to this group. Now all the groups and user accounts under Sales have access to this desktop template.

VDI-in-a-Box never adds, updates, or deletes user and group objects in Active Directory. Its interaction with Active Directory users and groups is read-only.

Each VDI-in-a-Box desktop requires a valid computer object and account in Active Directory for a trust relationship to exist and to allow for users to authenticate. A computer object is also created for a draft image for testing purposes, but this object is deleted immediately after the image is published.

By default all computer objects are placed in the Active Directory Computers container (with the exception of Domain Controllers). Citrix recommends that you create a new Organizational Unit (OU) for VDI-in-a-Box desktops; this allows for separation of virtual desktops and the ability to apply different group policies. You can place VDI-in-a-Box desktops in different Organizational Units at the image level. You can create different OUs and child OUs for each image if you wish; this is especially useful for change management and test environments.

You can specify the Distinguishing Name (DN) as part of the VDI-in-a-Box Prepare Image task. For example there could be a domain called company.com where you have created an OU called VDIdesktops. You would type the following DN into
the OU field: OU=VDIdesktops,DC=company,DC=com

VDI-in-a-Box itself does not add computer objects into Active Directory. That is done by the desktops as they join the domain. VDI-in-a-Box does remove computer objects from Active Directory, but only transient computer objects that will not be reused by later desktops.

You can apply Group Policies to VDI-in-a-Box virtual desktops. Keep this in mind when troubleshooting, because certain GPOs may interfere with VDI-in-a-Box virtual desktop behavior. For example if you have a group policy that disables TCP Ports 1494 and 2598 you cannot connect to desktops using HDX.

To reduce problems and to prevent performance issues from occurring with VDI-in-a-Box virtual desktops, block inheritance of group policies that are not applicable. Ensure that your virtual desktops comply with your organization's IT and Security policies, but try to reduce the amount of policies being applied to the virtual desktops.

To troubleshoot group policy issues, use standard Microsoft GPO troubleshooting steps. Tools such as RSOP (Resultant Set of Policy) and GPResult can help find the root cause of many Group Policy issues.

Active Directory can also be used to provide roaming profiles, keeping user application configurations and their My Documents folders in a central location separate from the desktop. Citrix Profile management is available to VDI-in-a-Box users, but roaming profiles are still often an appropriate solution for simple use cases.

You can either use the same domain for desktops and users, or, if your organization uses multiple domains for computers and users, you can place desktops in a different domain from users. You can also choose to divide your desktops between more than one domain.

For example, you might have a scenario where there is one Active Directory forest with multiple domains. A single domain, such as computers.company.com, is used to store all computer objects, both physical and virtual, regardless of their location. A domain, such as users.company.com, has a trust relationship with other domains, such as east.users.company.com and west.users.company.com. The actual user accounts are on the respective region's user domains, but with a correctly configured trust relationship between the user domain and computer domain, users are able to authenticate to computer objects residing in the computers.company.com domain.

If your user domain has subdomains, the users and groups in the subdomains can also authenticate with VDI-in-a-Box, provided the Global Catalog and trust relationships between the domains are correctly configured. For further details, see http://support.citrix.com/article/CTX136845.

1. In the VDI-in-a-Box Manager (vdiManager) console, from the Admin page, click Advanced Properties.
2. Scroll to the Miscellaneous section. click Specify alternate domains or workgroup for desktop and then OK.
3. On the Admin page, click Manage Computer Domains, then in the Manage Computer Domains dialog box click Add. The Specify Additional Domain for Desktops dialog box appears.

4. In the Domain name box, type the name of the domain for desktops.
5. In the User name and Password boxes, type the administrator credentials for the domain.
6. Click Add, type the IP address for the domain, and click Save to add the address to the IP addresses list.

7. To specify additional domains, repeat steps 4 to 6.
8. Click Save, then Close.
After you have configured additional domains for desktops, you can select them when preparing images.

If you have configured additional desktop domains, you can edit or delete them. You cannot edit or delete the domain that contains your users.

1. On the Admin page click Advanced Properties, then Manage Computer Domains.

![Manage Computer Domains](image)

2. To edit a domain, click its name. When the details of the domain appear, edit them, then click Save. Note that to change a domain's IP address you must delete the existing address and add a new one.

   To delete a domain, click Delete.

3. Click Close.

Use Active Directory failover to ensure your grid continues to fully function, even if the primary server fails.

VDI-in-a-Box begins using the first Active Directory server you listed. If that server fails, VDI-in-a-Box moves to the next Active Directory server in the list. This process is repeated, as necessary, with each Active Directory server in your list. Periodic checks of the primary server are made and, if it has recovered, VDI-in-a-Box activity automatically resumes on it.

Important: To ensure uninterrupted desktop provisioning, each Active Directory server in the list should contain identical data and be synchronized. VDI-in-a-Box does not provide a mechanism to ensure synchronized operations among the Active Directory servers.

1. From the vdiManager console, from the Users tab, click Configure.

![vdiManager console](image)

The Specify Domain dialog box appears.
2. Click Add, type the IP address of an Active Directory server in your grid, and click Save.

The IP address is added to the IP addresses list.

3. Repeat Step 2 for each Active Directory server you want to add to the list.
4. Click the arrows to move servers up or down the list.
5. In the Password box, type your domain password and click Save.
Configure VDI-in-a-Box kiosks

Sep 02, 2013

The VDI-in-a-Box kiosk feature allows you to convert user devices into a kiosk system that you deploy wherever you need standard desktops, such as in conference rooms, school labs, or nurses' stations at hospitals. You deploy a VDI-in-a-Box kiosk to IP address ranges as a user device location rather than to a user or group name.

Like any VDI-in-a-Box virtual desktop, a kiosk is based on a template. To establish connectivity between a desktop and user device, assign a template to the IP address of the user device.

You can set up a user device so that a user connects to the desktop through Citrix Receiver (recommended), a web browser, or the VDI-in-a-Box Java Desktop Client.

If a user disconnects from a kiosk-assigned desktop, they are automatically logged off after two minutes and cannot reconnect to the same desktop.

If a user leaves their desktop connection on one device, goes to another device and tries to connect to the desktop, they get a new desktop.

Note: In a conflict between kiosk and user settings, the kiosk settings take priority.

You cannot access VDI-in-a-Box kiosks through StoreFront.

There must be no HTTP proxy (for example Access Gateway Enterprise Edition) between the user device and vdiManager when kiosk mode is used.

Plan the number of templates needed for the kiosks, based on:

- Whether the kiosks can use the same desktop policy or need different ones.
- The IP addresses of the user devices. You assign a template to an IP address or a range of IP addresses.
  
  Example: You are deploying VDI-in-a-Box kiosks for the existing computers in the Engineering and Art labs of a school district. Define a template for each lab, assigning the IP address range of the computers in the Engineering lab to the Engineering kiosk template and the IP address range of the computers in the Art lab to the Art kiosk template. This setup ensures that a student logging in from either lab will receive the appropriate desktop.

- Maintain separate templates for use in kiosk deployments. By using kiosk-specific templates only for kiosk device assignments and not for individual user or group assignments, you can manage and monitor the kiosk sessions efficiently.
- Consider implementing daily refresh policies.
- For kiosks in public areas and conference rooms:
  - Set the refresh policy to On logout to ensure that each new user gets a fresh desktop.
  - Since it takes time to generate new desktops, prepare the image using the Fast desktop refresh option to allow quick provisioning of the desktops when users log out.
  - To keep a reasonable number of desktops in a pre-started or new state, adjust the Maximum desktops policy count to exceed the number of user devices.
  - If the load is heavy and desktop re-generation on each use is too resource intensive, use the Scheduled refresh
method to ensure that the desktops are refreshed every night. In this case, the maximum number of desktops does not need to exceed the number of kiosks.

- **Determine how many desktops to pre-start.** Pre-started desktops are in a powered-on state and at the logon prompt, ready for use. Pre-starting desktops eliminates the need for users to wait for virtual desktops to start. When you specify a number of desktops for pre-start, VDI-in-a-Box maintains that number as users log on. For example, if you specify five pre-started desktops in the template, five virtual desktops are started and available for your users. When two users log on to their desktops, VDI-in-a-Box starts two more desktops to maintain the requested five prestarts. This continues until your stated maximum number for the template is reached.

- **Observe caution if you change desktop template assignments for kiosks.** The reassignment delivers new desktops to the user device while retaining the old desktops in VDI-in-a-Box. Identify these orphaned kiosk sessions and remove them through the VDI-in-a-Box console Desktops > User Sessions tab.
Configure user devices as kiosks

Nov 04, 2013
To configure user devices as kiosks, follow these steps:
1. Assign a template to each user device IP address or range of addresses.
2. Set up each user device to operate as a kiosk.
3. Verify the kiosk connection.

1. In the vdiManager console, click the Users tab.
2. At the IP Addresses table, click Add.
3. In the IP Address Ranges box, type the user device IP addresses to assign to a template. You can specify individual addresses (192.168.23.143), prefixes (192.168), or ranges (192.168.10.174-204). Separate entries with new lines or spaces. You can also use an asterisk (*) to represent all IP addresses, such as 172.*.
4. Select a template to assign to an IP address or range. You can assign only one template to a user device.

The following table shows sample IP address assignments for the Engineering and Art labs, a break room, and a library at a school district.

<table>
<thead>
<tr>
<th>IP address ranges</th>
<th>Template name</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.30-50</td>
<td>Engineering Lab</td>
<td>A separate template is required for the two labs, to accommodate the two IP address ranges.</td>
</tr>
<tr>
<td>192.168.1.1-20</td>
<td>Art Lab</td>
<td></td>
</tr>
<tr>
<td>192.168.2.11</td>
<td>Break Room</td>
<td>The user device in the Break Room requires its own template. If that device had an IP address starting with 192.168.3, the Library template could be used for it.</td>
</tr>
<tr>
<td>192.168.3</td>
<td>Library</td>
<td>All user devices with IP addresses starting with 192.168.3 and 192.168.4 use the Library template.</td>
</tr>
<tr>
<td>192.168.4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. If you want users’ credentials entered from kiosks to be verified by Active Directory: from the Admin page select Advanced Properties, then in the User Sessions section select Authenticate AD users in kiosk mode. By default, kiosk credentials are not verified through the VDI-in-a-Box logon screen; they are expected to be authenticated by the desktop.

The supported connection methods for kiosk operation are the same as for non-kiosk desktops: Citrix Receiver (recommended), a web browser, and the VDI-in-a-Box Java Desktop Client. For configuration details, refer to the eDocs topics for your user devices in Access VDI-in-a-Box from user devices.

If you use the Java Desktop Client, consider including it in the end device start-up script so that the client launches when the user device restarts. Alternatively, create a shortcut to the client: Open a command window on the user device, enter javaws --viewer, right-click the Java Desktop Client entry, and choose Install Shortcuts. If you have multiple vdiManagers...
consider creating a shortcut to each one so that a user has options if a VDI-in-a-Box appliance is offline.

**Launching the Java Desktop Client with a common user name and password**

To pass a default user name (such as “guest”) and password so that the user can connect directly to the desktop without entering credentials, use the command:

```
javaws https://IPaddress/dt/vdiclient.jnlp?"username=kioskuser&password=kioskpassword"
```

In VDI-in-a-Box console, go to the Desksops > User Sessions tab. The User ID and client IP address entries start with an asterisk (*) so you can easily search for and sort kiosk entries.
Configure generic user accounts

Nov 05, 2013

Generic user mode enables you to bypass the verification and enforcement of the user name of the logged on user account with the user who requested the desktop. This is useful in several situations:

- If your user authentication database is a product other than Active Directory or Workgroup (the authentication methods currently supported by VDI-in-a-Box)
- If in your organization computers reside in a different domain from users, there is a one-way trust relationship between users and computers, and VDI-in-a-Box cannot have access to the user domain
- If you want to enable your users to call up a set of templates using a generic user name and then log on to a desktop with their real credentials

In VDI-in-a-Box 5.3 and earlier, generic user mode was used both for bypassing user authentication when the user logs on to a desktop, and for setting up shared user accounts. When you selected generic user mode, ‘follow me’ access to desktops was automatically disabled for the entire grid, so all users always got a fresh desktop every time they logged on.

As from version 5.4, generic user mode is used only for bypassing user authentication, as described in this topic. ‘Follow me’ access is controlled at the template level using a new check box: Desktops follow users to other access devices.

If you used generic user mode in previous versions to bypass user authentication, after upgrading to version 5.4 you can continue to work in generic user mode and use your existing templates. If you need to create new templates, make sure you clear the Desktops follow users to other access devices check box as described below in 'To configure generic user accounts'.

If you used generic user mode in previous versions to set up shared user accounts, after upgrading to version 5.4 you should clear the Enable generic user check box in Advanced Properties. You do not need to edit any templates that you created in generic user mode in previous versions: ‘follow me’ access is automatically disabled on these templates. For information on configuring and using shared user accounts in VDI-in-a-Box 5.4 onwards, see Configure shared user accounts.

1. Configure the grid: from the vdiManager, from the Admin tab, click Advanced Properties.
2. Scroll to the User Session section and select Require users to re-enter password on Windows logon screen.
3. Scroll to the Miscellaneous section and select Enable generic user.
4. Create the desktop images and templates for the generic accounts by following the VDI-in-a-Box image and template creation procedures.
   The desktops may join either Windows Workgroup or a Windows domain.

   When you are creating templates for generic users, clear the Desktops follow users to other access devices check box. This ensures that anyone logging on to a desktop based on this template gets a fresh desktop every time they log on.
   Note: If you created templates using VDI-in-a-Box 5.3 or earlier, with generic user mode enabled, ‘follow me’ access is disabled on those templates by default. However, remember that when you create new templates using version 5.4, you must clear the check box manually. If you do not, users who log on using a generic user account then log on to a desktop using their own credentials will be unable to access disconnected active or ‘on hold’ desktops.
   Be sure to install the necessary Windows authentication software components on the image.

5. Add the generic user accounts:
1. Click the Users tab and then, in User Groups, click Add.
2. Type the User ID for the generic account.
3. Select the templates you want to assign to the group.
4. Click Save.
6. Test the configuration:
   1. Log on to vdiManager with a generic user account.
   2. Click the template assigned to the generic user.
   3. Make sure the user is prompted to enter the user name again on the desktop's logon (Windows GINA) screen.
   4. Enter a user name that's different from the generic user account user name.
   5. Make sure the desktop is still accessible after five minutes of remoting.

If a user disconnects from an active desktop, they cannot access that desktop again, either from the same device or another one. They can access an 'on hold' desktop again if they connect from the same device.
Configure shared user accounts

Nov 05, 2013

Shared user accounts are useful in settings such as classrooms or labs where you have a group of users who need to access a class/lab-specific desktop using the same user ID.

For example, in a school a group of third grade students use the classroom from 10 until 12; they all use the ‘Grade3’ user account which gives them access to two templates, one for Math applications and one for Science applications. Each student logs on to a device, selects the template they want from the list, and is given their own desktop. At 12 this group of students leave the classroom and a group of fourth grade students use the same classroom and the same devices. They all use the ‘Grade4’ user account, which gives them access to templates for History and Geography applications. When the students log on, they are each given a fresh desktop.

In VDI-in-a-Box 5.3 and earlier, generic user mode was used both for bypassing user authentication when the user logs on to a desktop, and for setting up shared user accounts. When you selected generic user mode, ‘follow me’ access to desktops was automatically disabled for the entire grid, so all users always got a fresh desktop every time they logged on.

As from version 5.4, generic user mode is used only for bypassing user authentication, as described in Configure generic user accounts. ‘Follow me’ access is controlled at the template level using a new check box: Desktops follow users to other access devices.

If you used generic user mode in previous versions to set up shared user accounts, after upgrading to version 5.4 you should clear the Enable generic user check box in Advanced Properties. You do not need to edit any templates that you created in generic user mode in previous versions: ‘follow me‘ access is automatically disabled on these templates.

1. Create the desktop images and templates for the shared user accounts by following the VDI-in-a-Box image and template creation procedures.
   When you are creating templates for shared user accounts, ensure that Refresh Desktop is set to On logout (the default) and clear the Desktops follow users to other access devices check box. This ensures that anyone logging on to a desktop based on this template gets a fresh desktop every time they log on.
   
   Note: If you created templates using VDI-in-a-Box 5.3 or earlier, with generic user mode enabled, ‘follow-me‘ access is automatically disabled on those templates.
   
   Be sure to install the necessary Windows authentication software components on the image.

2. Add the shared user accounts:
   1. Click the Users tab and then, in User Groups, click Add.
   2. Type the User ID for the shared account.
   3. Select the templates you want to assign to the group.
   4. Click Save.

3. Test the configuration:
   1. Log on to vdiManager using a shared user account from a user device.
   2. Keep the connection on and log on to vdiManager with the same shared user account from another user device.
   3. Verify that both remote desktop sessions are accessible at the same time.
Clearing the check box `Desktops follow users to other access devices` essentially provides a unique desktop for each pairing of a user ID and a user device. This impacts disconnecting and logging off in the following ways:

- If a user logs on to a device and is given a desktop, then logs on using the same user ID to a different device, they get a different desktop.
- If a user disconnects or logs off from a device, then another user logs on to that device using a different ID, the second user will get a different desktop.

Citrix recommends that you set up your templates so that desktops are refreshed 'on logout' (the default setting). If you use a different refresh policy, then when a user disconnects or logs off, the desktop they have been using is not destroyed and may be given to the next user who logs on to the device using the same user account and template.

If some users need continuous access to the same desktop when they log off and log back on again, you can configure a separate template for their desktops: leave `Desktops follow users to other access devices` selected when you create or edit the template, and assign the template to a personal user name rather than a shared one. This ensures that any user who connects to a desktop based on this template will be able to reconnect to the same desktop if they disconnect from one device then log on at another. If you are editing an existing template, make sure there are no user sessions running on desktops based on this template before making the change.
Manage SSL certificates

Oct 17, 2013

SSL certificates are required for communication over HTTPS. SSL certificates can be self-signed, or signed by a trusted certificate authority (CA).

VDI-in-a-Box includes a self-signed certificate. Self-signed certificates do not require payment, but bear in mind the following points:
- You have to install them on all your user devices in order for them to be trusted by those devices. This makes them a practical solution for small deployments but less effective for enterprise-level deployments.
- Browsers require a trusted certificate. A self-signed certificate results in a browser warning message appearing every time you connect to a virtual desktop or to the vdiManager console.
- If your users log on through StoreFront, a trusted certificate is required.

VDI-in-a-Box provides a wizard that enables you to:
- Create a new Certificate Signing Request (CSR) and install a CA-issued SSL certificate
- Create and install a self-signed SSL certificate for a Fully Qualified Domain Name (FQDN)
- Upload an existing SSL certificate in PKCS12 format
- Distribute certificates to all servers in the grid

1. From the vdiManager console, click the Admin tab.
2. Click Manage SSL Certificate.
3. Click Create CSR.
4. Complete the request details then click Create. You can specify more than one FQDN; for example, you may want to have a single certificate that covers a NetScaler Gateway server, the grid IP address, and all the servers in the grid. To do this, select Specify multiple host names, then type the names of the additional servers separated by semicolons. You can use IP addresses or regular DNS host names. A confirmation message appears, which provides the name of the request file.

5. Click Download. The request file is downloaded to your computer.

Send the completed CSR to a CA. The CA verifies that the CSR is valid and authentic, then issues a CA-signed certificate containing the CSR's information. This certificate is returned to you with root and intermediate certificates.

If you are prompted for a server type during certificate submission or download, specify 'tomcat'.

When the CA has sent you the relevant certificates, you can install them on a server.

1. Put the grid into maintenance mode: from the vdiManager console, click the Admin tab, click Grid Maintenance, then click OK.
2. From the Admin tab, click Manage SSL Certificate.
3. Click Install Cert.
4. Click Browse, then browse to the certificates' location.
5. You must upload the certificates in order from the root through the necessary intermediates to the issued CA-signed certificate, otherwise the upload fails. To upload a file, select it, then click Choose.

6. Click Install (note that this button is dimmed until you have uploaded all the necessary files). The certificates are installed and a confirmation message appears on the screen. 
   Note: Installing the SSL certificate restarts the vdiManager service.
7. Click Close.
8. Take the grid out of maintenance mode: from the Admin tab, click Grid Maintenance, then click OK.
1. Put the grid into maintenance mode: from the vdiManager console click the Admin tab, click Grid Maintenance, then click OK.
2. From the Admin tab, click Manage Certificate.
3. Click New self-signed certificate.

4. Click Generate.
5. Complete the details, then click Create.
6. The certificates are installed and a confirmation message appears on the screen.
   Note: Installing the SSL certificate restarts the vdiManager service.
7. Click Close.
8. Take the grid out of maintenance mode: from the Admin tab, click Grid Maintenance, then click OK.
9. Install the certificates on all user devices in order for them to be trusted by those devices.

You can upload existing SSL certificates, provided that they are in a PKCS12 container. The container must include:
- The complete certificate chain (root certificate, intermediate certificate(s), and the server certificate)
- The private key for the certificate
- The password

1. Put the grid into maintenance mode: from the vdiManager console click the Admin tab, click Grid Maintenance, then click OK.
2. From the Admin tab, click Manage Certificate.
3. Click Existing certificate.
4. Click Upload Cert.
5. Browse to the certificate's location, type the password, then click OK.
6. The certificate is uploaded and a confirmation message appears on the screen.
   Note: Uploading the certificate restarts the vdiManager service.
7. Click Close.
8. Take the grid out of maintenance mode: from the Admin tab, click Grid Maintenance, then click OK.

After you have installed an SSL certificate on one server, you can distribute it to all the other servers in the grid. Do this if all the servers are addressed with the same host name, perhaps because you are using the grid IP address or because you have a load balancer in front of the servers in the grid. You are responsible for making sure that a CA-issued certificate can legitimately be placed on multiple hosts.

1. Put the grid into maintenance mode: from the vdiManager console click the Admin tab, click Grid Maintenance, then click OK.
2. On the server on which the certificate is already installed, from the Admin tab, click Manage Certificate.
3. Click Distribute, then after confirmation that the certificates have been distributed, click Close.
   Distributing the certificate across the grid restarts all the receiving vdiManager services. Allow about five minutes for the vdiManagers to complete the installation process before making any changes to the grid.
4. Take the grid out of maintenance mode: from the Admin tab, click Grid Maintenance, then click OK.

Note that if you add a new server to the grid, you must redistribute the SSL certificate so that the new server also has the single grid-wide certificate.
Collect logs

Nov 04, 2013

Logs are automatically produced for various components of VDI-in-a-Box. You can download them for use in troubleshooting and to assist support teams in solving issues.

Debug logs for each appliance in a VDI-in-a-Box grid are produced automatically. They are also available in syslog format, so you can use third-party tools to analyze them.

You can download debug logs either for an individual server, or for the whole grid:
1. In the vdimanager console, click the Admin tab.
2. Click Download Debug Log.
3. Select whether to download logs for only the server you are working on or for the entire grid, then click OK.
4. You can either open the log file or save it to a specified location.

Debug log files are named yyyymmdd_vdiMgrIPaddress_debug.tar.gz, where yyyymmdd represents the current date, and vdiMgrIPaddress represents the IP address of the VDI Manager that generated the debug log file.

To collect all virtual machine logs and zip them, at a command prompt type collectVdiLogs.

Logs are generated in the system temp folder (%temp%).

For domain join issues, the file at c:\Windows\debug\NetSetup.LOG is useful. The standard collected logs mentioned previously contain only part of this file.

For connectivity issues needing more detail than is available in the standard collected logs, see the following:
• For PortICA logging: http://support.citrix.com/article/CTX118837
• For WorkstationAgent logging: http://support.citrix.com/article/ctx117452

Note that VDI-in-a-Box uses the same HDX components as XenDesktop. Because of this, logs for connectivity issues are the same for the two products.
Manage optional components

Oct 22, 2013
This section describes the following optional components and products that you can use to enhance your experience of VDI-in-a-Box:

- Citrix NetScaler Gateway
- Remote Desktop Gateway
- Printing
- Citrix Profile management
- Citrix StoreFront
- Citrix App Controller
- Citrix HDX RealTime Optimization Pack for Microsoft Lync
- Citrix Desktop Lock
- Smart cards
- Antivirus software
- Citrix HDX features
Configure secure remote access using Citrix NetScaler Gateway

Nov 04, 2013

To provide remote users with secure connections to virtual desktops, use Citrix NetScaler Gateway 10.1 with VDI-in-a-Box. NetScaler Gateway is a secure application access solution for Citrix XenServer, Microsoft Hyper-V, or VMware ESXi that provides secure access to desktops while allowing users to work from anywhere. NetScaler Gateway eliminates the need for remote users to configure a virtual private network (VPN) connection and log on to it before logging on to the desktop. Single sign-on is available for users connecting through the VDI-in-a-Box web interface.

For supported versions, see Optional components.

For detailed configuration instructions specific to VDI-in-a-Box, see http://support.citrix.com/article/CTX134315. For NetScaler Gateway information, see NetScaler Gateway.

If you use the VDI-in-a-Box Java Desktop Client to access virtual desktops, you cannot use NetScaler Gateway.

Note: The procedure for configuring the connection to NetScaler Gateway provided in this topic enables single sign-on, which is available from VDI-in-box 5.3 onwards. If you have previously configured the connection but want to update it to enable single sign-on, add the NetScaler Gateway virtual server IP address before the FQDN in NetScaler Gateway Addresses (IP and FQDN), as described in Step 4 of the procedure.

- Configure the VDI-in-a-Box Grid IP address as described in the section ‘To provide high availability with a grid-wide virtual IP address’ in Manage a grid. This allows a single entry on NetScaler Gateway without the need for the Load Balancing feature.
  The Grid IP address provides automatic failover of the VDI-in-a-Box web interface as well as connection brokering roles on a local area network (LAN) and through NetScaler Gateway.

- You must have NetScaler Gateway platform licenses.

Perform the setup described in the NetScaler Gateway 10.1 documentation:
1. Download the virtual appliance for NetScaler Gateway 10.1.
2. Import the virtual appliance onto a supported hypervisor.
3. Configure NetScaler Gateway basic settings, including NetScaler IP (NSIP) for management, and install a NetScaler Gateway Platform License.

The number of configured gateways must not exceed the number of NetScaler Gateway virtual server instances on the NetScaler.
1. In the vdiManager console, from the Admin tab, click Advanced Properties.
2. Add the Grid IP address.
3. Scroll to the Gateways section.
4. In NetScaler Gateway Addresses (IP and FQDN), for each NetScaler Gateway virtual server, type the following: virtual server IP address, fully qualified domain name: port number

Separate the entries with semicolons. For example:


Note: To enable single sign-on, you must ensure that you enter the virtual server IP address. If you enter only the FQDN and port number, remote access without single-sign on is configured.

5. In NetScaler Gateway SNIP addresses, type the list of Subnet IP (SNIP) or Mapped IP addresses of the NetScaler Gateway servers, separated by semicolons. Specify the same number of NetScaler Gateway servers in the same order as listed in the external gateways list. For example: 172.16.1.1;172.16.1.2

6. Click OK.

Create a NetScaler Gateway virtual server for the VDI-in-a-Box grid. You can create multiple NetScaler Gateway virtual servers on a single NetScaler appliance, allowing access to multiple separate VDI-in-a-Box grids.

1. Log on to the NetScaler Gateway appliance by opening a web browser and navigating to the NetScaler IP address.

2. Provide a host name, Subnet IP address, and one or more DNS addresses. The Subnet IP address is the internal IP address of the NetScaler Gateway server. For production environments, the DNS should be an external-facing DNS that will be used to redirect http to https requests based on the FQDN, if this is enabled in the NetScaler Gateway Settings section. You can change the NetScaler Gateway administrator password from here.

3. Complete the rest of the setup wizard using the default values.

4. Under Update Licenses, click Browse to choose and upload a NetScaler Gateway platform license.

5. Click Continue, then Done.

6. Save the configuration when prompted, then restart the NetScaler Gateway appliance.

7. Log back on to the NetScaler Gateway web console.

8. To open the NetScaler Gateway Setup page, click Get Started.

9. Complete the NetScaler Gateway Setting section, providing an IP address and name to use for the NetScaler Gateway virtual server.

10. Complete the Certificates section, selecting the Install Certificate or Use Test Certificate option. You can create certificates using the NetScaler > Configuration > SSL section or third-party certificate tools.
Note: SSL certificates are required only on Netscaler Gateway, not in vdiManager.

11. Complete the LDAP Authentication section, providing the Active Directory domain in which your user accounts are stored. Click Continue.

12. Configure the Enterprise Store Settings section:
   2. For Deployment Type, select Web Interface.
   3. For XenApp Services Site URL, type the URL of the VDI-in-a-Box grid IP address as follows:
      https://vdiGridIP/dt/PNAgent/config.xml
      Note: You must begin the URL with https://
   4. For Single Sign-on Domain, provide the Active Directory domain in which your user accounts are stored.
   5. For Secure Ticket Authority, type the Secure Ticket Authority URL, including the Grid IP address, in the following format: https://<vdiGridIPaddress>/dt/sta.
      Note: Begin the Secure Ticket Authority URL with https://.

13. Verify the NetScaler Gateway virtual server configuration: in the NetScaler Configuration > NetScaler Gateway > Virtual Servers section, double-click the virtual server created and review the settings. Repair any issues before proceeding.

14. Return to the NetScaler Gateway web console, click Configuration, then click Save. This ensures that that running configuration is saved to disk in case a restart is required.

To allow mobile devices to connect to VDI-in-a-Box desktops through NetScaler Gateway, a Citrix Receiver session policy is required. For details of how to create this policy, see the 'More Information' section in http://support.citrix.com/article/CTX134315.

Use Citrix Receiver to connect to VDI-in-a-Box desktops through NetScaler Gateway. See the Receiver section of eDocs for details on setting a server URL option with several user devices. Use the following URL to connect: https://accessgatewayfqdn/dt/PNAgent/config.xml. Specify the same user name used to access desktops through the vdiManager console.

Important: PNA in PNAgent must be upper-case.
Configure secure remote access using the Microsoft Remote Desktop Gateway

Nov 04, 2013
Remote access to VDI-in-a-Box desktops is available through the Microsoft Remote Desktop Gateway. The Remote Desktop Gateway must be set up in the demilitarized zone. It must be in the same domain as the virtual desktops to which it provides remote access. The vdiManager must be configured with the Remote Desktop Gateway's IP address.
Note: For details on configuring the Remote Desktop Gateway, see http://support.citrix.com/article/CTX134286.
For supported versions, see Optional components.

1. In the vdiManager console, from the Admin page, click Advanced Properties.
2. Scroll to the Gateways section.

3. In External Microsoft Remote Desktop Gateway addresses, type the list of external fully qualified domain names (FQDN) of the Remote Desktop Gateway(s), including the port and separated by semicolons. For example: www.gateway1.com:443;www.gateway2.com:443
4. In Internal Microsoft Remote Desktop Gateway IP addresses, type the list of internal IP addresses of the Remote Desktop Gateways, separated by semicolons. Specify the same number of Remote Desktop Gateways in the same order as listed in the external gateways list. For example: 192.0.2.5;192.0.2.20
5. Click OK.
This topic describes the options for managing printing with VDI-in-a-Box.

The simplest way to give your users access to printers is to enable printer redirection. This connects all the printers available on the user device to the virtual desktop. This works for all types of printers including local, network, and wireless. Because these printers are already configured on the user device there is no need to configure or install drivers on the virtual desktops. If, however, the user device cannot connect to the required printer (thin clients, for example), then you need to consider the other options described in this topic.

To enable printer redirection:
1. In the vdiManager console, click the Templates tab.
2. Click the name of the template you want to edit.
3. Under Connect these devices to the VDI-in-a-Box desktop, select Printers.
4. Click Next, then on the next page click OK.

This section describes the two ways to use print drivers with VDI-in-a-Box: the Citrix Universal Print Server and vendor print drivers. Depending on how HDX print policies are configured, you can use a combination of native drivers and the Universal Print Server. This may be necessary when the Universal Print Server is used by most printers, but some specialized printers require native print drivers.

VDI-in-a-Box does not currently support the HDX policies to assign default printers, session printers, or assign printers based on client IP address. Other policies, including Citrix Universal Print Server policies, are supported by VDI-in-a-Box.

Use the Universal Print Server to reduce print driver clutter and to improve bandwidth consumption during print jobs. It allows a single generic driver called the Universal printer driver to be used on VDI-in-a-Box virtual desktops. You can download the Universal Print Server package from the VDI-in-a-Box download page. For more details of the Universal Print Server package, including detailed installation instructions, see the XenDesktop 7 printing documentation.

Note: The Universal Print Server is not supported on Windows Server 2012.

The procedure below is an overview of how to install the Universal Print Server for use with VDI-in-a-Box:
1. Download the Universal Print Server package from the VDI-in-a-Box download page.
2. Unzip the contents and place them on a network share for easy access.
3. Install the Citrix HDX Group Policy Management package onto a Windows 2008 R2 Server.
4. Install the UPServer component on the same Windows 2008 R2 Server. This also enables the Printing and Document Services role.
5. Configure a Citrix HDX Printing Group Policy.
6. Check that the Citrix Print Manager service starts on the desktops: open services.msc, and confirm that the Citrix Print Manager Service has started.

If the Citrix Print Manager service does not start on the desktops, complete the following steps. These instructions use Windows Task Scheduler to start the Citrix Print Manager service on the desktops, but you can use Group Policy and logon...
scripts instead.
1. Select to edit the image.
2. Log on to the draft image as an administrator.
3. Create a new batch file containing the file command:
   ```bash
   net start cpsvc
   ```
4. Save the batch file to a location such as the C:\ drive. Do not save it in the administrator's profile.
5. Open Windows Task Scheduler.
6. Create a new task and give it a name; for example, Citrix Print Service. Enter the following information:
   - General tab: in the Security options, change the User or Group to include all domain users and to run whether the user is logged on or not. Select the correct operating system in the Configure for dropdown menu.
   - Triggers tab: Click New, then select the option to begin the task at startup.
   - Action tab: Select the option to start a program. Click Browse, then select the batch file created in step 3.
7. Save the task.
8. Return to the vdiManager console to save and publish the image, then check that the task runs as scheduled.
9. When the image is published, log on to a published desktop, open services.msc from the Windows Start menu and confirm that the Citrix Print Manager Service has started.

Use vendor drivers only in the following situations:
- If the Universal Print Server is not available
- If you need to use a specialized printing device that is not compatible with the Universal printer driver
- If you are deploying VDI-in-a-Box in workgroup mode and no Active Directory exists in the environment

If the only option is to install the vendor drivers on the VDI-in-a-Box images, you do this in the same manner as on a physical computer. This works with local, network, and wireless printers.

To reduce the need for end-user interaction, you can install the print drivers on the VDI-in-a-Box image. If you are using a print server you can also deploy the drivers from the server. In a print server scenario, it is not always necessary to install the drivers on the image because the drivers are installed during user sessions when a printer is connected. However, this can consume additional bandwidth and users may not have permissions to install software or drivers on the virtual desktop.

You can assign printers to specific computers or users in Active Directory. The methods described here usually require a Windows server with the Print and Documents Services role in combination with a print driver (vendor or Citrix Universal printer driver) and HDX Group Policy Management.

Location-based printing, also known as proximity printing, allows the user to access a different printer from the one they normally use, typically based on the physical location of the user device or possibly Active Directory membership.

Active Directory and Group Policy allow you to configure location-based printing without the need for third-party solutions. There are two basic requirements for deploying printers using these methods: (1) Windows Server domain controller, (2) Windows Server with Print and Documents Services role. These roles do not have to reside on the same Windows Server but they can do so.

The first step is to decide whether to use the Citrix Universal Print Server or vendor drivers. The steps described in this section apply to using the Universal Print Server or vendor-supplied drivers.
The next step in the process is to decide how to assign printers:

- For small VDI-in-a-Box deployments it may make sense to filter group policy based on OU. For example, a customer may have three distinct user groups requiring three images, each with different installed applications. You could create an OU named VDI-Desktops, and three child OUs named Finance, Sales, and Engineering. You would then join the three images to the respective OUs within Active Directory and assign printing group policies to each OU.
- For most VDI-in-a-Box deployments it is easier to assign printing group policies based on group membership. In many cases there may only be a few images, all joined to the same OU. You can create a GPO for each set of printers to be used by specific groups of users. This is a good solution when network printers are already deployed by location based on group membership. An example would when printers are deployed by department because the users sit near each other. In this case you would create a GPO with an assigned printer and then filter it based on group membership. This way each member of the group has access to the printers from their virtual desktop.
- You can also assign printers based on client IP addresses. However, you should do this only if you are using static IP addresses, segmented DHCP scopes (or static/reserved IP addresses) for specific locations or departments, or in kiosk-type situations.

The following example describes a VDI-in-a-Box deployment where Windows Server 2008R2 is used as a domain controller and print server. The Citrix Universal Print Server has been installed and configured to reduce print driver clutter, and the administrator has decided to deploy network printers to the virtual desktops based on Active Directory group membership. Each department already has its own network printer(s) configured on the Windows server using the Printer and Documents Services role.

1. Create an OU called VDI-Desktops. The DN is OU=VDI-Desktops,DC=company,DC=com.
2. Install the Citrix Universal Print Server components onto the Windows server. This includes the HDX Group Policy Management component.
3. Install and configure VDI-in-a-Box with one image:
   1. Install the Citrix UPCIent component.
   2. Prepare the image and join it to the VDI-Desktops OU.
4. Create templates named Finance Desktop, Marketing Desktop, and Inside Sales Desktop for the three departments that will use VDI-in-a-Box desktops. Ensure that the Printer Redirection item is disabled.
5. Open the Group Policy Management Editor on the domain controller.
6. Create a new GPO assigned to the VDI-Desktops OU and configure Citrix policy to use the Citrix Universal Print Server.
7. Create a new GPO for each department in the VDI-Desktops OU and use a naming convention that is easy to understand, such as Finance - Citrix Printers.
8. Select each departmental printing GPO and adjust the Security Filtering to include only the respective groups. For example, remove Authenticated Users and add the Finance Security Group to the Finance - Citrix Printers GPO. Do this for all the departments.
10. Click Print Servers > Server Name > Printers.
11. Right-click the printer used by the Finance department and select Deploy with Group Policy.
12. For GPO name, click Browse and select the Finance - Citrix Printer GPO found in the VDI-Desktops OU.
13. Select the option to deploy this printer to computers this GPO applies to and click Add.
14. Click OK and repeat steps 11-13 for each department.
15. Start desktops for each VDI-in-a-Box template.
16. Log on to each of the departmental desktops to confirm the printer(s) have been installed and can be used by printing a test page.

You can write custom logon scripts to connect network printers based on client location. VDI-in-a-Box writes the client
device IP address into the registry, allowing you to use a script to assign a network printer based on this registry key. This solution can be used with most network print server deployments or with the Citrix Universal Print Server.

The client IP address is written to the following registry location:

HKEY_LOCAL_MACHINE\SOFTWARE\Kaviza\dtagent\endPointAddress

The data field for endPointAddress can be extracted and used by a script. An example would be a school with Computer Science and Biology labs where students are able to bring their own laptops. Each lab has its own DHCP scope, allowing you to write a script that assigns the Computer Science network printer to VDI-in-a-Box desktops only when students are connected from the Computer Science network. The same happens for the Biology lab, even if a student disconnects from the Computer Science lab and reconnects to the VDI-in-a-Box desktop from the Biology lab.
Configure Profile management

Nov 04, 2013

To apply user personalization settings to virtual desktops, use Citrix Profile management with VDI-in-a-Box. Profile management consolidates and optimizes user profiles to minimize management and storage requirements. Profile management applies to any user location or user device, providing users with fast logons and logoffs.

The use of Profile management with VDI-in-a-Box is subject to the Profile management end-user license agreement (EULA).

Prerequisites

- A VDI-in-a-Box grid
- A Windows 7 or later image published through vdiManager
- A shared folder on a file server where users have read and write permissions

Citrix recommends that you always use the latest versions of VDI-in-a-Box and Profile management to ensure you get the full benefit of any new features.

To install and configure Profile management for VDI-in-a-Box

Plan the deployment and perform the setup described in the Profile Management topics for your version in eDocs.

Do not install the Profile management on VDI-in-a-Box servers. Install it on the images that you use to create virtual desktops.

To configure VDI-in-a-Box images for Profile management

For each image used to create desktops, set the Organizational Unit (OU) to the one configured with the Group Policy Object (GPO) template.

1. To view the OU set for an image: Click the Images tab and then click the image name.
2. To set the OU for an image:
   1. Click the Images tab, click the edit link for the image, and then click Confirm.
   2. In the Edit draft image wizard, enter the Organizational unit (OU).
After you save the new draft image, it becomes the new version of the published image and the previous version of the image is deactivated. The image changes are propagated to the desktops based on the associated template refresh policies.

Optimize your use of Profile management

To ensure that your VDI-in-a-Box deployment operates as effectively as possible and that no data is lost, Citrix recommends that you always configure certain optional Profile management settings: active write back and profile streaming.

To enable active write back

Active write-back ensures that profile updates are regularly synchronized during a session; the default is for updates to be saved only when the user logs off, which, for desktops that are regularly refreshed, means that updates made during a session may be lost. At log-off minimal profile data (if any) then needs to be synchronized. Another benefit of enabling this setting is that if a virtual desktop fails or is reset instead of being correctly shut down, files will have been synchronized.

For details of how to configure active write-back, see the documentation for the version of Profile management that you are using.

To enable profile streaming

Profile streaming ensures that user profile contents are fetched only when needed, which has the following benefits:

- Speeds up logon times because the entire user profile is not loaded at logon.
- Uses less network bandwidth because the entire profile does not need to be synchronized from the user store to the virtual desktop each time a user logs on to a new desktop.

For details of how to configure profile streaming, see the documentation for the version of Profile management that you are using.
Use StoreFront with VDI-in-a-Box

Sep 30, 2013
This topic describes how to install and configure StoreFront for use with VDI-in-a-Box. It also lists requirements and any limitations to bear in mind when using StoreFront to access VDI-in-a-Box virtual desktops.

StoreFront is a unified application and data store that allows Windows, web, SaaS and mobile applications to be aggregated and delivered to any user on any device anywhere. This single point of aggregation allows you to deliver VDI-in-a-Box desktops alongside other data types, including XenApp applications and XenDesktop virtual desktops.

StoreFront support for VDI-in-a-Box includes Single Sign-on for both local and remote connections, as well as strong two-factor authentication through NetScaler Gateway Enterprise Edition. This allows for a more secure deployment while improving the user experience. StoreFront also enables you to easily deploy Citrix Receiver and related components to Windows and Mac user devices.

For supported versions, see Optional components.

For more details about StoreFront, see StoreFront.

StoreFront requirements and limitations

Only virtual desktops from grids that have been configured to use Active Directory can be accessed through StoreFront; desktops that use workgroup mode are not available through StoreFront.

StoreFront must be in the same forest as the servers running VDI-in-a-Box.

If you intend using HTTPS to secure connections between StoreFront and VDI-in-a-Box, you must install SSL certificates on your VDI-in-a-Box servers before configuring StoreFront. For details of how to create a certificate request and install certificates, see Manage SSL certificates.

You cannot access VDI-in-a-Box kiosks through StoreFront.

To install and configure StoreFront 2.x

1. Install StoreFront as described in the StoreFront documentation.
2. If the StoreFront management console is not already open after installation of StoreFront, click Start > All Programs > Citrix > Citrix StoreFront.
3. In the results pane of the Citrix StoreFront management console, click Create a new deployment.
4. Specify the base URL to be used to access the StoreFront services and then click Next to set up the authentication service, which authenticates users to VDI-in-a-Box servers.
5. On the Store Name page, specify a name for your store and click Next.
7. In the Add Delivery Controller dialog box, specify a name that will help you to identify the deployment (for example, VIAB Grid) and select VDI-in-a-Box.
8. Click Add, then type in the IP addresses of your VDI-in-a-Box servers.
   For fault tolerance, if you are using the VDI-in-a-Box grid-wide virtual IP address feature, type in only the grid virtual address. If you are not using this feature, type in at least two server IP addresses to enable fault tolerance through StoreFront, listing the entries in order of priority to set the failover sequence.
9. From the Transport type list select the type of connections for StoreFront to use for communications with the servers.
To send data over unencrypted connections, select HTTP. If you select this option, you must make your own arrangements to secure connections between StoreFront and VDI-in-a-Box. User connections to StoreFront, however, are encrypted regardless of this selection, provided the StoreFront site is configured with HTTPS.

To send data over secure HTTP connections using SSL or Transport Layer Security (TLS), select HTTPS. StoreFront validates SSL certificates, so you must have installed trusted certificates on all VDI-in-a-Box servers to use HTTPS. Note: If you are using HTTPS, ensure that the server names you specify in the Servers list match exactly (including the case) the names on the certificates for the servers.

10. Specify the port for StoreFront to use for connections to VDI-in-a-Box. The default port is 80 for connections using HTTP, and 443 for HTTPS connections.

11. Click OK. Repeat Steps 6 to 11, as necessary, to list additional deployments on the Delivery Controllers page. Click Next.

12. On the Remote Access page, specify whether and how users connecting from public networks can access the store through NetScaler Gateway:
   - To make the store unavailable to users on public networks, select None. Only local users on the internal network will be able to access the store. If you select this option, continue to Step 24.
   - To make only resources available through the store available to users on public networks through NetScaler Gateway, select No VPN tunnel. Users log on directly to NetScaler Gateway and do not need to use the NetScaler Gateway Plug-in.
   - To make the store and other resources on the internal network available to users on public networks through an SSL virtual private network (VPN) tunnel, select Full VPN tunnel. Users require the NetScaler Gateway Plug-in to establish the VPN tunnel.

   If you configure remote access to the store through NetScaler Gateway, the pass-through from the NetScaler Gateway authentication method is automatically enabled. Users authenticate to NetScaler Gateway and are automatically logged on when they access their stores.

13. If you enabled remote access, list the NetScaler Gateway deployments through which users access the store. Click Add.

14. On the General Settings page, specify a name for the NetScaler Gateway deployment that will help users to identify it. Users see the display name you specify in Citrix Receiver, so you should include relevant information in the name to help users decide whether to use the deployment. For example, you could include the geographical location in the display names for your NetScaler Gateway deployments so that users can easily identify the most convenient deployment for their location.

15. Enter the URL of the user logon point or virtual server for your NetScaler Gateway deployment in the Gateway URL box. Specify whether the logon point or virtual server is hosted on a standalone NetScaler Gateway appliance or an Access Controller server that is part of an NetScaler Gateway cluster.

16. Select the version of NetScaler Gateway you are using.

17. Unless you are configuring remote access through an NetScaler Gateway Enterprise Edition deployment, click Next and continue to Step 19. For NetScaler Gateway Enterprise Edition deployments, specify the subnet IP address of the NetScaler Gateway appliance. The subnet address is the IP address that NetScaler Gateway Enterprise Edition uses to represent the user device when communicating with servers on the internal network. This can also be the mapped IP address of the NetScaler Gateway appliance. StoreFront uses the subnet IP address to verify that incoming requests originate from a trusted device.

18. From the Logon type list select the authentication method used for Citrix Receiver users accessing their desktops and applications through NetScaler Gateway Enterprise Edition:
   - If users are required to enter their domain credentials, select Domain.
   - If users are required to enter a tokencode obtained from a security token, select Security token.
   - If users are required to enter both their domain credentials and a tokencode obtained from a security token, select
Domain and security token.

- If users are required to enter a one-time password sent by text message, select SMS authentication.
- If users are required to use smart cards, select Smart card.

Click Next.

19. If you are configuring StoreFront for an NetScaler Gateway cluster, on the Appliances page list the IP addresses or fully qualified domain names of the NetScaler Gateway appliances in the cluster and click Next.

20. On the Secure Ticket Authority (STA) page, specify the URL for a server running the STA. Enter URLs for multiple STA servers to enable fault tolerance, listing the servers in order of priority to set the failover sequence. If you are using the VDI-in-a-Box grid-wide virtual IP address feature, you need specify only the grid virtual address to enable fault tolerance. Important: The paths for VDI-in-a-Box servers must include /dt/sta after the IP address. For example https://203.0.113.2/dt/sta

The STA issues session tickets in response to requests for connections to VDI-in-a-Box servers. These session tickets form the basis of authentication and authorization for access to resources.

21. If you want to keep disconnected sessions open while Citrix Receiver attempts to reconnect automatically, select the Enable session reliability check box. If you configured multiple STAs and want to ensure that session reliability is always available, select the Request tickets from two STAs, where available check box.

When the Request tickets from two STAs, where available check box is selected, StoreFront obtains session tickets from two different STAs so that user sessions are not interrupted if one STA becomes unavailable during the course of the session. If, for any reason, StoreFront is unable to contact two STAs, it falls back to using a single STA.

22. Click OK to configure remote user access to the store through your Access Gateway deployment.

23. Repeat Steps 13 to 22, as necessary, to list additional NetScaler Gateway deployments on the Remote Access page. If you add multiple deployments, specify a default NetScaler Gateway appliance to be used to access the store.

24. On the Remote Access page, click Create and then, when the store has been created, click Finish.

StoreFront automatically establishes a trust relationship between the new store and the authentication service.

The URL for users to access the Receiver for Web site for the new store is displayed. The Receiver for Web site enables users to access their desktops through a Web page.

Your store is now available for users to access with Citrix Receiver and through the Receiver for Web site. After creating the store, further options become available in the Citrix StoreFront management console.

By default, the store is configured to specify that Citrix Receiver Updater for Windows and Citrix Receiver Updater for Mac...
users accessing the store receive plug-in updates directly from the Citrix Update Service on the Citrix web site. The specific plug-ins included depend on the configuration of the store.
Use Citrix App Controller with VDI-in-a-Box

Jul 05, 2013

App Controller allows you to access all your business resources including virtual desktops, mobile apps, SAAS apps, and data, from one central place.

If you have an existing App Controller setup, you can easily add VDI-in-a-Box desktops to the other resources you provide to your end users through App Controller.

Note: VDI-in-a-Box only supports desktop access through App Controller using CGP. Access without CGP is unsupported. For supported versions, see Optional components.

To configure App Controller for use with VDI-in-a-Box

1. Log on to the App Controller management console.
2. Click the Apps & Docs tab.
3. In the Apps & Docs panel, click Windows Apps.
4. For Host, type the IP address or host name of your VDI-in-a-Box server. For example: 192.0.2.9
5. For Port, type 443
6. For Relative Path, type /dt/PNAgent/config.xml
7. Select Allow secure access.
8. Click Save.

For more information on App Controller, see App Controller.
Optimize Microsoft Lync calling

Oct 22, 2013
If you have Microsoft Lync deployed in your environment, and your users make Lync calls from their virtual desktops, use Citrix RealTime HDX Optimization Pack to improve the quality of the audio and video associated with the calls. The Lync optimization pack channels audio and video components of Lync calls to local resources for efficient processing and high quality playback.

The Lync optimization pack consists of two components:

1. You install HDX RealTime Media Engine on your users’ devices.
2. You install HDX RealTime Connector on your users’ virtual desktops.

You can download the Lync optimization pack from the VDI-in-a-Box download pages.

For important information about the Lync optimization pack, such as system requirements, installation instructions, and configuration tips, see the following topics in eDocs: HDX RealTime Optimization Pack for Microsoft Lync.
Manage the Citrix Desktop Lock

Oct 29, 2013

The Citrix Desktop Lock locks down the user device so that users can access only their VDI-in-a-Box virtual desktop; they cannot interact with the local desktop.

The user must have only one template assigned.

For Single Sign-on to work, the user device must be in the same domain as the VDI-in-a-Box grid.

To install the Desktop Lock:

1. Ensure you have read User device requirements so that you know your environment is appropriate.
2. Log on to the user device with administrator credentials.
4. Download CitrixDesktopLock.msi from the VDI-in-a-Box download page on the Citrix web site.
5. Open a command prompt and install Receiver as follows:
   CitrixReceiverEnterprise.exe /includeSSON
   ADDLOCAL="ReceiverInside,ICA_Client,SSON,USB,DesktopViewer,Flash,PN_Agent,Vd3d" SERVER_LOCATION="my.vdi-grid" ENABLE_SSON="Yes"
   
   where my.vdi-grid is the URL of your VDI-in-a-Box grid.
6. When the Receiver installation has completed, click Cancel when you are prompted for credentials to log on to the Citrix application.
7. Double-click CitrixDesktopLock.msi, then follow the wizard steps for installing the Desktop Lock.
8. When the installation has completed, click Close.
9. When prompted, restart the user device. If you then log on using your domain user credentials, your VDI-in-a-Box desktop opens immediately, just as if it were your local desktop.
Configure smart card authentication

Nov 04, 2013

VDI-in-a-Box supports smart card authentication, enabling users to log on to virtual desktops by using a smart card reader. To log on, users insert a smart card in the reader and enter their smart card Personal Identification Number (PIN). If users remove their smart cards during a session, they are forced to log off.

Prerequisites

- Install the device driver for the smart card on the draft image before you publish the image and provision desktops from it.
- Select Smart cards check box for the template, as described in the instructions below.
- Active Directory:
  - The VDI-in-a-Box grid and the desktops must all be in the same domain.
  - Configure Group Policy for smart card removal behavior. For example, you can set it to force user logoff from the user device when the smart card is removed. This ensures that Citrix Receiver is unloaded and reset for subsequent use.
- User device requirements:
  - Supported Windows-based operating system.
  - If the devices are to connect to vdiManager directly, they need to join the same domain as the grid and the desktops. Receiver Enterprise must be installed and configured with the vdiManager's PNAgent address as follows: http(s)://<vdiManagerIP-or-hostname/dt/PNAgent/config.xml; whether you use http or https and how you specify the vdiManager depends on the version of Receiver you are using.
  - The devices can be in a different Organizational Unit (OU) from the desktops.
  - If the devices are to connect through StoreFront 2.x, they must have Receiver 4.x installed. Configure StoreFront's store to enable pass-through with smart card authentication. The devices can join the same domain as the grid and the desktops, or they can be in Workgroup.
  - Note: To use smart cards in an environment where the user devices cannot be in an Active Directory domain (for example non-Windows thin clients), see the section 'To configure smart card authentication for non-Windows user devices' below, which also describes the limitations of this type of configuration.

To configure smart card authentication for Windows user devices

1. Plan the templates needed for smart card authentication. Desktops based on a template configured for smart cards require a smart card for access. Users who attempt to connect to such desktops without a smart card are denied access.
2. Create one or more templates configured for smart cards:
   1. Click the Templates tab and then click the Add link.
   2. In the Create a New Desktop Template wizard, specify the template information as usual.
   3. Select the Smart cards check box.
4. Click Proceed and then click Next.
5. Specify the template policies and then click Save.
3. Assign users or groups to the new templates. These users and groups must have their information embedded in their smart cards. For help, refer to Assign templates to users, groups, and IP addresses.
4. If the devices are to connect directly to vdiManager, configure Citrix Receiver Enterprise on the user devices: open Receiver, select Server Options, then for Logon Mode select Pass-through authentication. If the devices are to connect through StoreFront, configure StoreFront to enable pass-through with smart card authentication by specifying LogonMethod as smartcard_sson. Configure Receiver 4.x on the devices to point to the StoreFront store. When the user inserts their smart card in the reader, Receiver automatically reads the user name from it and the user only has to enter their PIN to log on.
5. Test smart card authentication on a user device:
   - For a device that connects directly to vdiManager, insert a smart card in the reader and enter your PIN to log on to the device. You should then be able to launch desktops without reentering your PIN.
   - For a device that connects through StoreFront, insert a smart card in the reader and enter your PIN to log on to the device. You should then be able to launch desktops without reentering your PIN. If you log on to the device using your user name and password, you need to enter your smart card PIN to launch desktops.

To configure smart card authentication for non-Windows user devices

1. Import the image on which your template will be based.
2. When you are editing the image, enable the image's standalone mode by editing the following registry entry (of type REG_DWORD): ForceVdaStandaloneMode. Set this to 1 to enable standalone mode. For x86 this is in HKLM\SOFTWARE\Citrix\VDI\HDX Connector Service. For x64 this is in HKLM\SOFTWARE\Wow6432Node\Citrix\VDI\HDX Connector Service. Caution: Editing the Registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.
3. Create a generic user in Active Directory with a complex password.
4. In the vdiManager console, click Admin, then Advanced Properties.
5. Select Enable generic user and Require users to re-enter username and password on Windows logon screen.
6. When you have created the template (remembering to select the Smart cards check box), assign the generic user and the smart card user to it.
7. Without inserting the smart card, log on to Receiver on the user device with the generic user name, leaving the password blank. The desktops available to that user are displayed.

8. Launch a desktop. The desktop logon screen appears.

9. Insert your smart card and enter your PIN, then your selected desktop appears.
Manage antivirus software

Sep 22, 2015
VDI-in-a-Box provides an inherently secure environment by centralizing data and utilizing disposable pooled desktops or persistent personal desktops. Administrators choosing to provide additional security through antivirus software deployment should take steps to avoid the following issue, which is frequently encountered when running antivirus software in a VDI environment.

The software is running on pooled desktops that are destroyed every time the user logs off from the desktop. If the user logs on to a desktop and the antivirus software detects that the virus definitions are out of date, a new set of virus definitions is downloaded. When the user logs off from the desktop, the newly downloaded definitions are destroyed with the desktop and a new desktop will be generated with the outdated definitions from the image. The next time the user logs on, the virus definitions need to be downloaded yet again, and the definitions download grows larger and larger until the image has been updated with the latest definitions.

To avoid this issue, virus definitions should be stored separately from desktops in a central location that all desktops can point to. There are many antivirus programs designed specifically for virtualized environments that do this by default; some traditional antivirus programs also support this.

For information on compatible antivirus software, see https://citrixready.citrix.com.
Use HDX features and enhancements

Jun 18, 2013
Citrix HDX includes a broad set of technologies that provide a high-definition user experience for today’s media-rich user environments.

For information on how to configure and use these HDX features and enhancements, see Deliver high definition user experience with HDX. Note that VDI-in-a-Box does not support HDX3D Pro.

To configure HDX policies through Group Policy settings

Many HDX features are configurable through Group Policy settings. If your network environment includes Active Directory and you have the appropriate permissions to manage Group Policy, you can use the Group Policy Editor to configure HDX policies settings. The HDX policy settings template for Active Directory is available for download from the VDI-in-a-Box downloads page.

In the Group Policy Editor, you access policies and settings by clicking Citrix Policies under Computer Configuration or User Configuration in the tree pane.
Access VDI-in-a-Box from user devices

Oct 10, 2013

Users access Citrix VDI-in-a-Box virtual desktops through their user devices. Protocols, such as Citrix's HDX or Remote Desktop Connection (RDP), are used to communicate between the user device and virtual desktop. A client-side protocol agent and a server-side protocol agent are required to make the connection between the user device and the virtual desktop.

Protocols supported by VDI-in-a-Box

VDI-in-a-Box supports the following protocols:

- **HDX**
  - HDX is the default protocol.
  - No separate license is required.
  - HDX provides a high-definition user experience.
  - HDX provides better multimedia support while using less bandwidth.
  - HDX is suitable for remote access over a WAN.
- **Remote Desktop Connection (RDP) 6.1, 7.x, and 8.x**
  - RDP is suitable for LAN deployments.
  - RDP 8 support includes support for RemoteFX without hardware GPU-assisted rendering.
  - Note: For best results when using RDP 7 or 8, Citrix recommends running Windows 7 or Windows 8 respectively on both the virtual desktop and the user device.

Access VDI-in-a-Box virtual desktops

Users access VDI-in-a-Box virtual desktops in any of three ways:

Important: All access methods require Citrix Receiver on the user device except for access through a locked-down device, such as Chromebook, that can support HTML5 Receiver.

- **Web browser**
  - Web browsers support both HDX and RDP, although some configuration is required to use each protocol. Devices that do not have Citrix Receiver pre-installed (Chromebook for example) can use HTML5 Receiver if their browser supports HTML5. Use the HTML5 Receiver URL:

    http(s)://vdiMgrIP-or-hostname/html5

  - instead of the regular URL:

    http(s)://vdiMgrIP-or-hostname

- **Citrix Receiver**
  - Citrix Receiver allows direct access to VDI-in-a-Box desktops through an HDX connection without the use of a Web browser or Java client.
  - Receiver connects to VDI-in-a-Box desktops on Windows, Mac, Linux, iOS, and Android platforms.
  - With Citrix Receiver, older and low-end thin clients that do not have browsers can be used to access VDI-in-a-Box virtual desktops. Mobile devices, such as the iPad, can also be used with Receiver to access VDI-in-a-Box virtual desktops without requiring a Web browser or Java client.

- **VDI-in-a-Box Java Desktop Client**
- The Java client automatically checks for updates and refreshes itself as needed.
- The client requires the Java Runtime Environment.
- The client switches to an RDP connection if an HDX connection is not available.

Note that if you use the VDI-in-a-Box Java Desktop Client to access virtual desktops, you cannot use NetScaler Gateway.

Compare client access

<table>
<thead>
<tr>
<th>Client</th>
<th>Accesses virtual desktop</th>
<th>Automatic RDP connection started if there is no HDX</th>
<th>Kiosk*</th>
<th>Integrated error messages</th>
<th>Automatic failover to healthy vdiManager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Receiver</td>
<td>Y</td>
<td>Not applicable</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web browser</td>
<td>Y</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>VDI-in-a-Box Java Client</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

Note: If the grid-wide virtual IP address feature is active, automatic failover is available for all three access methods. See Manage a grid for details.

*The kiosk option is useful for libraries, nurses' stations, and anywhere you want to place a public user device with the desktop assigned to the device and not to the user logging on. All users receive the same desktop, based on the purpose of the kiosk.

Log on from a user device

The following figure shows a basic logon sequence between a Web browser on a user device and a server with VDI-in-a-Box Manager. An HDX session between the user device and a specific virtual desktop on the server is being created using Receiver. Once the connection is created, the session traffic takes place between Receiver and the virtual desktop only. The same sequence applies when the Java client is used.
Configure Windows, Mac, and Linux devices to access VDI-in-a-Box virtual desktops

Nov 01, 2013

Prerequisites

Install the appropriate Citrix Receiver on the user device in order for it to access VDI-in-a-Box desktops. You can download Receiver from http://receiver.citrix.com/?ntref=citrixdotcomdownloads.

For Linux devices, you must also install rdesktop, which you can download from http://www.rdesktop.org.

If you are using the VDI-in-a-Box Java Desktop Client you must also install the Java Runtime Environment (JRE), which you can download from https://www.java.com.

To configure user devices to access VDI-in-a-Box desktops with a web browser

These steps may vary slightly depending on your web browser.

1. Start your web browser.
2. In the web browser address box, type https://<vdiManagerIpaddress>. A security warning about the web site's certificate may appear.
3. Accept the certificate as trusted and continue. The VDI-in-a-Box Log On page appears.
4. Create a desktop shortcut to the VDI-in-a-Box logon page through the web browser.

To configure user devices to access VDI-in-a-Box desktops with Citrix Receiver

You can use Citrix Receiver on user devices to connect to VDI-in-a-Box desktops. See the Receiver section of eDocs for details on setting a server URL option.

Use the following URL: http(s)://<vdiManagerIpaddress-or-hostname>/dt/PNAgent/config.xml; whether you use http or https and how you specify the vdiManager depends on the version of Receiver you are using.

Use the user name you use for accessing desktops through the vdiManager console.

To configure user devices to access VDI-in-a-Box desktops with the VDI-in-a-Box Java Desktop Client

1. Ensure you have installed the JRE on the device.
2. You can access the Java Desktop Client either through your browser, by typing https://<vdiManagerIpaddress>/dt/vdiclient.jnlp in the browser address bar, or through a command prompt or terminal window as follows:
   1. Open a command prompt or terminal window on your device.
   2. At the command or Terminal prompt, type javaws https://<vdiManagerIpaddress>/dt/vdiclient.jnlp. A security warning about the web site's certificate may appear.
3. Accept the certificate as trusted and continue.
   Note: To avoid this error, either install a trusted certificate on the vdiManager or do not use https and use http://<vdiManagerIpaddress>/dt/vdiclient.jnlp. This does not compromise security because only the jnlp file is downloaded through http. The credentials are still sent to the vdiManager over a secure https connection.
4. If additional security warnings appear, accept them and continue. The VDI-in-a-Box Client dialog box appears.
5. Create a desktop shortcut to the VDI-in-a-Box Java Desktop Client.
1. Open a command or terminal window on the device.
2. At the command or terminal prompt, type `javaws -viewer`. The Java Cache Viewer window appears.
3. Right-click the JavaClient entry and select `Install Shortcuts`. 

Configure iOS devices to access VDI-in-a-Box virtual desktops

Aug 17, 2012

Prerequisites

- Integrate the Citrix VDI-in-a-Box grid with Active Directory for user authentication.
- Assign at least one template to users accessing desktops from iOS devices (iPads and iPhones).

To configure an iOS device to access VDI-in-a-Box virtual desktops

For details related to Citrix Receiver for iOS, see the Receiver for iOS section of eDocs (Receiver for iOS).

1. Download and install Receiver for iOS from the iTunes App Store.
2. Open the New Account screen to configure accounts manually for Citrix Receiver for mobile devices) and in Address, type the address to the VDI-in-a-Box Manager (vdimanager) in the following format:
   https://<vdimanagerIPaddress>/dt/PNAgent/config.xml
3. Tap Next. The Verified screen appears.
4. Complete the Verified screen and tap Save. A list of the desktops available to the configured user appears.

To access VDI-in-a-Box virtual desktops with an iOS device

1. On the Accounts screen, tap the VDI-in-a-Box account you want to open.
2. On the Enter Credentials screen, type your user credentials and tap OK.
   Note: Depending on the account settings, the user password may be saved, in which case this step is skipped.
3. A list of the available desktops for the account appears.
4. Tap the desired desktop. You are connected to the virtual desktop.
Configure Android devices to access VDI-in-a-Box virtual desktops

Aug 16, 2012

Prerequisites

- Enable HDX on the Citrix VDI-in-a-Box grid.
- Enable and license the VDI-in-a-Box HDX Gateway.
- Integrate the Citrix VDI-in-a-Box grid with Active Directory for user authentication.
- Assign at least one template to users accessing desktops from Android devices.

To configure an Android device to access VDI-in-a-Box virtual desktops

For details related to Citrix Receiver for Android, see the Receiver for Android section of eDocs.

1. Download and install Receiver for Android from the Android Market.
2. Open the Add Account screen and in Address, type the address of the VDI-in-a-Box Manager (vdiManager) in the following format: https://<vdiManagerIPAddress>/dt/PNAgent/config.xml. A security warning about the Web site's certificate may appear.
3. If the security warning message appears, tap Accept. An error message appears.
5. On the Add Account page, type the Username and Domain, and tap Add.
   Caution: If desired, the user's password can also be typed here. This saves the password and allows the user to connect to the VDI-in-a-Box desktop with no identity verification.
   The new account is added to the Accounts list.

To access VDI-in-a-Box virtual desktops with an Android device

1. On the Citrix Receiver Accounts list, tap the VDI-in-a-Box account you want to open.
2. Type your password.
   Note: If the user password was saved during the configuration process, this step is skipped.
3. Type your user credentials and tap Log On. You are connected to the virtual desktop.
Use thin clients to access VDI-in-a-Box virtual desktops

Dec 05, 2012
VDI-in-a-Box supports a wide variety of thin clients from leading vendors such as HP and Dell Wyse. Citrix has established the Citrix Ready framework to help you choose the right thin client for your VDI-in-a-Box deployment. Citrix Ready is a verification program for Citrix partners including thin client vendors to ensure interoperability between their products and Citrix products such as VDI-in-a-Box. Select the thin clients that achieve basic Citrix Ready status or the more stringent HDX Ready status to ensure successful VDI deployment in your environment. More information about HDX Ready and Citrix Ready thin clients is at http://www.citrix.com/ready/.
Upgrade and migrate

Mar 27, 2014
You can upgrade or migrate to VDI-in-a-Box 5.4. You can also migrate from VDI-in-a-Box to XenDesktop.

To upgrade or migrate to VDI-in-a-Box 5.4

If you are using a version of VDI-in-a-Box prior to 5.4, the following upgrade and migration paths to version 5.4 are supported:

- If you are using VDI-in-a-Box 5.3.x or 5.2.x, you can upgrade to version 5.4. For details, see Upgrade to VDI-in-a-Box 5.4.x.
- If you are using VDI-in-a Box 5.1.x, you must migrate to version 5.3, as described in Migrate from VDI-in-a-Box 5.1.x to 5.3, then upgrade to version 5.4.
- If you are using VDI-in-a-Box 5.0.x, you must migrate to version 5.2.1, as described in Migrate from VDI-in-a-Box 5.0.x or 5.1.x to VDI-in-a-Box 5.2, then upgrade to version 5.4.

Migration or upgrade from any other version is not supported.

To upgrade VDI-in-a-Box with new hotfix packages

For information on how to upgrade VDI-in-a-Box with new hotfix packages, see http://support.citrix.com/article/CTX140490.

To migrate to XenDesktop

If you are using VDI-in-a-Box 5.4 or later, you can migrate to XenDesktop using a wizard. For further details, see Migrate to XenDesktop. If you are using an earlier version of VDI-in-a-Box, see http://support.citrix.com/article/CTX136081 for details of how to migrate to XenDesktop.
Upgrade to VDi-in-a-Box 5.4.x

Oct 25, 2013
The following steps describe how to upgrade VDI-in-a-Box 5.3.x or 5.2.x to VDI-in-a-Box 5.4.x. If you need to move from any other version of VDI-in-a-Box to 5.4, please see Upgrade and migrate for details of supported paths. Important: To avoid issues caused by running VDI-in-a-Box in an unsupported environment, upgrade your hypervisor to the latest supported version for the currently deployed VDI-in-a-Box version before upgrading VDI-in-a-Box. For more information on which hypervisor versions are supported, see the System Requirements topic for the relevant release.

To download the VDI-in-a-Box upgrade file

2. If you are not already logged on to My Account, do so now. If you open the Download page without having logged on, you are unable to download the product software.
3. Click Downloads.
4. From the products list, select VDI-in-a-Box.
5. From the download type list, select Product Software.
6. Click Find. The VDI-in-a-Box product software page appears.
7. Click VDI-in-a-Box 5.4. The VDI-in-a-Box 5.4 page appears.
8. From the Upgrade section, for 5.3 to 5.4 or 5.2 to 5.4, click Download.
9. Click Download Now.
10. Navigate to a location to download HF_VDI_inabox_5.4.x.tar and click Save.

Before you upgrade

Before you upgrade your entire grid, Citrix strongly recommends that you either ensure you have a backup server running the existing version of VDI-in-a-Box or that you pilot the upgrade on a single server.

To build a backup server

1. Back up all the assigned personal desktops as described in Back up and restore personal desktops.
2. Remove a server from the grid:
   1. On the Servers tab, click the server name.
   2. Click Leave Grid.
   3. Using the vdiManager console on the server that has left the grid, on the Servers tab click the server name, then click Shutdown.
3. Upgrade the rest of the grid as described in this topic.
4. Restore the shutdown personal desktops from the removed server on the remaining servers in the grid, as described in Back up and restore personal desktops.
5. Test the upgraded grid. If it works without any issues:
   1. Upgrade the backup server.
   2. Reset it: on the Admin tab, click Reset.
   3. Join the server to the grid as described in Create and configure the grid.
   If there are issues with the upgraded grid, contact Citrix support, who will rebuild the grid using your backup server and backed-up personal desktops.

To build a pilot upgrade server

1. Back up all the assigned personal desktops as described in Back up and restore personal desktops.
2. Remove a server from the grid:
   1. On the Servers tab, click the server name.
   2. Click Leave Grid.
   3. Using the vdiManager console on the server that has left the grid, on the Servers tab click the server name, then click Shutdown.
3. Upgrade the pilot server as described in this topic.
4. Test the upgraded pilot server.
5. Upgrade the old grid.
6. Reset the pilot server on the Admin tab, click Reset.
7. Rejoin the pilot server to the upgraded grid as described in Create and configure the grid.

To upgrade VDI-in-a-Box

1. If necessary, upgrade your hypervisor to the latest supported version.
2. Put the grid in maintenance mode: from the vdiManager console, on the Admin page, click Grid Maintenance and then click OK.
3. Destroy all pooled desktops except for assigned static desktops.
   1. Desktops are unavailable during an upgrade, so coordinate the downtime with the users.
   2. Log on to the vdiManager 5.3.x or 5.2.x console.
   3. Set the number of pre-started desktops to zero for each template for pooled desktops: click the Templates tab, click the template name, click Next, in Pre-started desktops type 0, then click Save.
4. Publish or destroy all draft images. Make sure that no images are being transferred before proceeding to the next step:
   1. Click the Images tab.
   2. Ensure no draft or test images are listed.
5. Shut down all assigned personal desktops and assigned static desktops: click the Desktops tab, click User Sessions, click Actions for each desktop you want to shut down, then click Shutdown.
6. Deactivate all servers in the grid: click the Servers tab, click the desired server, click Deactivate, then click Confirm.
7. On the Admin page, click Grid Upgrade. The Grid Upgrade dialog box appears.
8. Click Choose File, navigate to the upgrade file, and click Open.
9. Click Submit. When the upgrade completes, the logon page appears
10. Log on to vdiManager.
11. Take the grid out of maintenance mode: from the Admin page, click Grid Maintenance, and then click OK.

When you have completed the VDI-in-a-Box upgrade, check the system requirements for the new version for more information about which hypervisor versions are supported. You can then upgrade to any newly supported hypervisor version.

To upgrade existing images

After upgrading VDI-in-a-Box, you must update your existing images.

Note: If you have upgraded your hypervisor, you must install the latest version of the hypervisor tools on your images.

Note: If you are using Citrix Profile management with VDI-in-a-Box, you must update your images to at least version 5.0.
1. Log on to one server's vdiManager console and click the Images tab. All your images are displayed with a yellow warning triangle next to them.
2. Click on the warning triangle next to the first image. You are prompted to confirm that you want to create a new draft image.
3. Click Confirm.
   The Edit Image page appears.

4. Make any additional edits to the image you require, such as adding new applications, and click Next.
5. Complete the Prepare Image and Test Image pages. For details about these pages, see Create the first Windows image.
6. On the Test Image page, click Save. A message appears stating that continuing will save the prepared image and distribute it to other servers in the grid.
7. Click Confirm. The updated image is published and ready to be deployed based on your refresh policies.
8. Repeat the above steps for each of your published images.

To refresh desktops

Following the upgrade of VDI-in-a-Box and the update of your images, you must refresh all your desktops.
1. Restart personal desktops: click the Desktops tab, click User Sessions, then for each personal desktop click Actions and select Restart.
   Note: When a personal desktop is restarted, if you have upgraded your hypervisor tools, the desktop will automatically have the upgraded version of the tools.
2. Activate all servers in the grid: click the Servers tab, click the relevant server, then click Activate.
3. Reprovision pooled desktops: for each pooled desktop template, click the Templates tab, click on the template name, click Next, in Pre-started desktops type the number of pre-started desktops you want, then click Save.
4. Update static desktops (manually refreshed desktops) one at a time.
   Caution: Do not do this with personal desktops: this may destroy the personal vDisk.
   1. Restart the desktop.
   2. From your hypervisor, log on the desktop as an administrator. Citrix recommends using a local administrator account.
   3. If you have upgraded your hypervisor, install the corresponding version of the hypervisor tools.
   4. From the Control Panel, uninstall the currently installed Desktop Agent. The virtual machine restarts.
   5. From the hypervisor, log on to the same desktop as an administrator.
   6. In the virtual machine's web browser, type the address of the Desktop Agent (https://<IPaddress>/dt/dtagent/) into the URL box.
   7. Follow the on-screen instructions.
   8. Repeat the on-screen instructions.
8. Repeat these steps for each static desktop in the grid.

To upgrade user devices

After upgrading VDI-in-a-Box you must upgrade Citrix Receiver on user devices to ensure the best user experience. Citrix recommends that you always use the latest version of Receiver to benefit from the latest HDX features and capabilities.

You should also upgrade the firmware on thin clients to the latest version. Please contact the thin client manufacturer to
Migrate to XenDesktop

Dec 16, 2013
If you need to migrate your VDI-in-a-Box deployment to XenDesktop, use the Migrate to Citrix Studio wizard to:

- Export images quickly and easily to XenDesktop. The images are exported as running VMs, with all the VDI-in-a-Box-specific software removed, including the desktop agent.
- Generate PowerShell scripts to create machine catalogs and delivery groups in Studio that match your VDI-in-a-Box template settings and user assignments.

Prerequisites

- VDI-in-a-Box 5.4 or later.
- XenDesktop 7 or later, with Studio installed and configured, a database, and an available host (in XenDesktop, the host is the hypervisor that hosts the master images and VMs).

Citrix recommends that you have VDI-in-a-Box and XenDesktop on the same host. If they are on different hosts, you have to migrate the images to the XenDesktop host after exporting them.

If you are using an earlier version of VDI-in-a-Box, see http://support.citrix.com/article/CTX136081 for details of how to migrate to XenDesktop.

Limitations

Machine catalogs and delivery groups corresponding to templates for personal desktops and static desktops are created in XenDesktop, but existing desktops based on these templates are not transferred. When users of these desktops log on to XenDesktop, they receive new desktops based on the VDI-in-a-Box settings, but they need to reinstall any user-installed applications.

To migrate your deployment

1. In the vdiManager console, click Admin:

2. Click Migrate to Citrix Studio:
3. Select the images you want to export. These images will be exported as running VMs on the host on which you are running the wizard.

4. Select the data store for the VMs. This must be a data store on the host on which you are running the wizard.

5. Click Next:

6. Enter the FQDN of your XenDesktop delivery controller, and change the port number if necessary.

7. Click Next.

The images that will be exported are listed together with the templates that use them:
Note the following points about pooled desktop templates:

- **Refresh policies**
  The 'Manual' refresh policy corresponds to statically assigned desktops in XenDesktop: a dedicated local machine is created for the user and changes are saved on the local disk. 'On logout' and 'Scheduled or on logout' refresh policies correspond to randomly assigned desktops.

- **Do Not Reassign Desktops 'On hold' to New Users**
  If this setting is selected in the template, statically assigned desktops are created in XenDesktop. If the setting is not selected, randomly assigned desktops are created.

8. Click Migrate.
   The images are exported and the browser downloads the PowerShell script to your browser's default download location.
   You can monitor the status of the image export from the Images tab in the vdiManager console:

9. Prepare the images for XenDesktop as described in the documentation for your version of XenDesktop. This includes installing the relevant hypervisor tools and the Virtual Desktop Agent on the images.

10. Ensure the images are on a host that is part of the XenDesktop environment.

11. Run the PowerShell script on the delivery controller. The script creates machine catalogs and delivery groups with the settings used in your VDI-in-a-Box deployment:
You can now open Studio, see your migrated environment, and manage it from there:
VDI-in-a-Box reference information

May 22, 2015
This topic provides reference information for use when planning and implementing your VDI-in-a-Box deployment.

Communication ports and protocols

For details of the communication ports and protocols used by each component, see http://support.citrix.com/article/CTX135153.

Services

The following tables provide information about the services installed with VDI-in-a-Box:

**Desktop VM**

<table>
<thead>
<tr>
<th>Service name</th>
<th>Short name</th>
<th>Account</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix VDI Agent Service</td>
<td>vdiAgent</td>
<td>\vdiAgentUser(network)</td>
<td>Performs all managed VM life cycle operations and reports the state of various attributes to VDI Controller at regular intervals. Watches for logons, logoffs, connections, and disconnections.</td>
</tr>
<tr>
<td>Citrix VDI Agent Monitor Service</td>
<td>vdiAgentMonitor</td>
<td>\vdiAgentMonitorUser (network)</td>
<td>Monitors vdiAgent to ensure it is running. Responsible for all install, uninstall, or update operations.</td>
</tr>
<tr>
<td>Citrix HDX Connector Service</td>
<td>VdiHdxConnectorSvc</td>
<td>Network Service</td>
<td>Controls the Citrix Virtual Delivery Agent service for brokering HDX connections to the desktop.</td>
</tr>
</tbody>
</table>

**Hyper-V**

<table>
<thead>
<tr>
<th>Service name</th>
<th>Short name</th>
<th>Account</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix VDI-in-a-Box Hyper-V Connector</td>
<td>vdiHVConnector</td>
<td>.\kaviza (Network)</td>
<td>Securely exposes the Windows Hyper-V WMI interface for VDI Controller to communicate with the hypervisor.</td>
</tr>
</tbody>
</table>