Citrix® 2.1 Synchronizer™ Setup and Usage Guide

This document serves as a guide for Synchronizer system administrators for the Citrix XenClient 2.1 release.

Publication date 29 November 2011
# Table of Contents

1. Synchronizer Overview ................................................................................................................................. 1  
   1.1. Devices .................................................................................................................................................. 1  
   1.2. Users ................................................................................................................................................. 1  
      1.2.1. User Groups .......................................................................................................................... 1  
      1.2.2. User Roles .......................................................................................................................... 2  
   1.3. VM Images ......................................................................................................................................... 2  
      1.3.1. VM Image Modes .................................................................................................................. 2  
      1.3.2. VM Image Assignments ..................................................................................................... 2  
      1.3.3. VM Image Backup ............................................................................................................. 3  
      1.3.4. Creating and Deploying VM Images ............................................................................... 4  
      1.3.5. VM Image Versions ............................................................................................................. 4  
2. Planning your Synchronizer Deployment ........................................................................................................... 5  
   2.1. Network and Firewall Configuration ................................................................................................. 5  
   2.2. VM Image Repository Storage ....................................................................................................... 6  
3. Installation and Upgrade ................................................................................................................................. 7  
   3.1. Installing Synchronizer .................................................................................................................... 7  
   3.2. Upgrading Synchronizer To a New Version .................................................................................... 9  
4. Configuring the Synchronizer ........................................................................................................................... 11  
5. Administration .............................................................................................................................................. 14  
   5.1. Synchronizer Web Interface Overview .......................................................................................... 14  
   5.2. Managing Users and Groups ...................................................................................................... 16  
      5.2.1. Managing Local Users and Groups .................................................................................. 16  
      5.2.2. Managing AD Users and Groups .................................................................................... 18  
      5.2.3. Changing the User Name Registered With Synchronizer .............................................. 19  
   5.3. Managing VM Images ....................................................................................................................... 19  
   5.4. Managing VM Image Assignments ............................................................................................... 21
Chapter 1. Synchronizer Overview

Citrix Synchronizer for XenClient is the server-based application for IT administrators to manage XenClient virtual machine (VM) images, users, and their XenClient devices. It:

- Stores XenClient VM images.
- Provides secure backup facilities.
- Offers management capability of users and their XenClient devices.
- Allows you to set policy about how a VM image can be used, for example, which USB devices can be used with the VM on a XenClient device.
- Simplifies the maintenance and secure distribution of VM images and applications to users.

You can register a XenClient device with a Synchronizer instance during XenClient installation, or in Citrix Receiver for XenClient after installation. Registering with a Synchronizer instance creates a record of the XenClient device in the Synchronizer database. Once the device is registered the user can:

- Download VM images that have been assigned to them.
- Back up VMs if policy allows. VM backup can also be set to occur automatically at fixed intervals.
- Upload new VMs or new VM versions to Synchronizer.

**Note**

Users cannot upload new versions of a VM unless they are explicitly enabled to do so by a Synchronizer Admin user.

The rest of this chapter defines Synchronizer terms and concepts.

1.1. Devices

A device is a laptop or desktop that has XenClient installed on it. Synchronizer keeps track of the relationship between devices and users, and enables secure communications between devices and Synchronizer.

1.2. Users

A Synchronizer user is an individual with a XenClient device. Synchronizer enables you to create users locally, or link in existing Microsoft Active Directory (AD) users.

When a user registers with Synchronizer for the first time, a record of their XenClient device is created and they are registered as the owner of the device.

VM images managed by Synchronizer can be assigned to a user for use on any registered device.

1.2.1. User Groups

Synchronizer enables you to create groups of users locally, or link in existing AD user groups. This allows you to assign a VM image to a number of users with similar application needs. As an example, you might want to create a VM image for all the users in the accounting department that contains the particular applications they need to do their work.
1.2.2. User Roles

You can assign either a **Standard** role or an **Admin** role to a Synchronizer user. A user with **Admin** rights can:

- Upload VMs to Synchronizer, creating a new VM image
- Log in to and use the Synchronizer web interface

Users assigned the **Standard** role cannot log in to the Synchronizer web interface and can only work with VM images that have been assigned to them.

1.3. VM Images

A VM image consists of files stored in the Microsoft Virtual Hard Disk (VHD) format. XenClient makes use of VHD chaining to allow a single large VHD to act as a parent to a large set of copy-on-write (CoW) children. This approach is also used to efficiently store subsequent versions of VM image files and backups of user data. By default, the image files are stored in an image repository that is created when Synchronizer is installed. You can change the image repository to a network directory exported by NFS using the Synchronizer web interface.

A VM image does not run on Synchronizer. When you run a VM on your device, it runs locally on the XenClient hypervisor from the XenClient device hard disk. When a VM is backed up or uploaded to Synchronizer, the VM image data is encrypted using AES CBC 128-bit encryption. A new key is created each time an upload is initialized. The client keys are stored in a secure user key store, protected by the device key and the user passphrase. A copy of the keys is also kept securely in Synchronizer.

1.3.1. VM Image Modes

When you create a new VM image, you set the VM Image mode. This can be either **Static VM Image Mode**, **Static VM Image Mode with the user profile only backed up**, or **Dynamic VM Image Mode**.

- **Static VM Image Mode** VM images are stored by the Synchronizer as a distinct set of VHDs. On your XenClient device, this VM runs like a traditional laptop would. In **Static VM Image Mode**, you can make changes, for example, installing software or updating your operation system, without affecting other users, and your changes remain when you reboot the device.

- **Static VM Image Mode** VM images with the user profile only backed up splits the system part of the image (operating system and applications) from the user part of the image, again storing them on the Synchronizer as a distinct set of VHVs. On your XenClient device, this VM also runs like a traditional laptop would. In this mode, you can make changes, for example, installing software or updating your operation system, without affecting other users, and your changes remain when you reboot the device. This allows you to use Synchronizer to back up user data and to use traditional Windows distribution tools for handling updates to the operating system and application layer.

- **Dynamic VM Image Mode** VM images in this mode have their system and application files maintained as one set of VHVs which is shared by multiple users. Each user assigned one of these VMs gets an additional VHD with their own user data, but the system and applications are left intact. If a user runs a VM created from such an image, only changes made to their user folders remain after a reboot. All other changes, for example any software they might have installed, are lost because the changes are never made to the system part of the image. This allows IT to provide VM images which retain their integrity over time, which of course prevents users from being able to alter their systems. Synchronizer is used instead of traditional Windows distribution tools for handling updates to the operating system and application layer as well as the user data.

1.3.2. VM Image Assignments

When you assign a VM image to a user, this enables the user to download a specific VM image version to their registered XenClient device and run it there.
When creating an assignment, you can specify policy and configuration settings that describe what the VM is capable of when it is running on a client device. You can control:

- Whether the user can manually backup the VM.
- How long the user can use the VM for before contacting Synchronizer. (This functionality automatically disables a lost or stolen device after the allocated time expires without contact with Synchronizer.)
- How often the XenClient device will automatically check to see if there is updated VM policy, disk, or version available for them.
- Whether the user can change VM properties.
- The allocation of device resources, for example, how much RAM the VM should use.
- If the VM disk image should be encrypted.
- The types of USB devices that can be used with the VM.
- Whether the VM can access a wired or wireless network.
- How the user can use system audio and optical media devices.
- Whether the user can upload a new, modified version of the VM to Synchronizer. This option allows the user to maintain the VM image. For example, you might want one software engineer to maintain a VM with the optimum settings and software for software development, which can then be assigned to other software engineers in the team.

You can, for example, disallow the connection of external USB hard drives, optical media, and wireless networking to inhibit the user installing unauthorized software. Similarly if the user device comes with a built-in optical media device with write capacity, VM policy can be used to disable the ability to write to optical media, thus ensuring that sensitive data does not leave the network.

### 1.3.3. VM Image Backup

The object of VM backup is to ensure that, should a device be lost, a new device can be obtained and the VM image downloaded on to it, ensuring that significant data loss is avoided. Backups are not versioned; they are simply a record of the VM state at the time that the last backup was performed.
You can set the frequency of automatic VM backup during VM image assignment. You can also enable users to make manual backups if desired.

For a Windows VM in Static VM Image Mode, you can also choose during VM image assignment whether a backup should back up both user data and system data or only the user data. For Windows in Dynamic VM Image Mode, only the user data is backed up, as the system data is already backed up automatically due to the nature of Dynamic VM Image Mode.

### 1.3.4. Creating and Deploying VM Images

Using XenClient with Synchronizer involves the five stages described below to create new VM images, and deploy them onto client devices.

**To Create and Deploy a VM Image:**

1. Register the XenClient device with Synchronizer. See the Procedure: “To Connect a XenClient Device to Synchronizer” for more information.
2. Install and configure an operating system and a set of applications in a VM on the XenClient device. See the XenClient Setup and Usage Guide for information about how to do this.
3. Using Citrix Receiver for XenClient, upload the VM to Synchronizer. This creates a VM image that can be assigned to multiple users. See the Procedure: “To Upload a VM to Synchronizer” for more information.
4. Using the Synchronizer web interface, assign a VM image version to a user or user group. See the Procedure: “To Assign a VM Image” for more information.
5. The XenClient user can download VM images to create new VMs from the set of VM images that have been assigned to them. See the XenClient Setup and Usage Guide for information about how to do this.

### 1.3.5. VM Image Versions

VM images are versioned sequentially. The procedure for creating a new VM image version is:

**To Create a new VM Image Version:**

1. Assign the VM image to a user or administrator, ensuring that you set the assignment policy to Allow users to author new versions of this image and Allow user(s) to change properties.
2. The user then downloads the assigned VM image to a XenClient device.
3. Once the new VM version is prepared, the user uploads the new VM version to Synchronizer, keeping the same VM name.

You can then trial the new VM versions with a select group before editing the assignment of users still using the old version and assigning them the tested version.
Chapter 2. Planning your Synchronizer Deployment

This chapter discusses some of the considerations involved in planning a successful Synchronizer deployment. The number of users that a Synchronizer server can support with reasonable quality of service depends on a number of factors, including:

- Frequency of image backup
- Average size of VM images
- Synchronizer VM memory assigned
- The availability of VM image repository space, either local storage or NFS storage
- Internal network speed

There is no theoretical limit on the number of users that can be supported by any given Synchronizer instance. There is however a hard limit set on the maximum number of current transfers of VM image data between Synchronizer and XenClient devices, which is calculated as a function of the available amount of RAM. This is because the encryption and decryption of VM images is computationally expensive, so that to ensure reasonable transfer speeds for connected users, users attempting to exchange data with Synchronizer are put into a queue after the hard limit of concurrent transfers has been reached.

To increase the number of allowed concurrent transfers, increase the RAM allocated to the Synchronizer VM. It may also be useful to maintain separate Synchronizer instances, each supporting types of XenClient user with similar VM image and backup needs. If you allow connections from outside the internal network (for example to support remote backup for mobile workers) it may also be sensible to maintain separate Synchronizer instances for such users, where typically the bottleneck of transfer speeds will be the upload speed of the user connection. Such a Synchronizer instance may well therefore be able to support more concurrent transfers than the limit calculated by Synchronizer.

2.1. Network and Firewall Configuration

The following figure illustrates the ports that are used for communication between the Synchronizer server, XenClient devices, and the Synchronizer web interface. From within the local network, the Synchronizer web interface connects to the Synchronizer server over port 8443 (by default; if this has been reconfigured, use the appropriate port in the discussion below), and XenClient users connect to the Synchronizer server over port 80 or port 443. From outside the local network, XenClient users connect to Synchronizer over port 443 (if you choose to allow connections from outside the network).
2.2. VM Image Repository Storage

VM images data is stored either in a local VM disk or an NFS repository. By default a small, approximately 20GB disk is provisioned during Synchronizer installation. To increase the amount of available storage, either increase the size of the virtual disk of the XenServer host server using the XenCenter management interface, or use the Synchronizer web interface to provision NFS storage instead. See the Procedure: “To Add an NFS Image Repository” for information about how to use an NFS storage repository for VM image storage.
Chapter 3. Installation and Upgrade

This chapter explains how to install or upgrade Synchronizer. See Section 1: “Known Issues” in Citrix® XenClient™ 2.1 Synchronizer™ Release Notes for any known issues that might affect your installation.

Synchronizer is provided as a Xen Virtual Appliance (XVA) file, which can be imported into XenServer. If you do not already have XenServer in your environment, you will need to install XenServer onto a physical server to host your Synchronizer. You can download XenServer for free from www.citrix.com.

**Note**

Synchronizer is supported on XenServer 5.6 or later.

### 3.1. Installing Synchronizer

**Note**

The following installation and upgrade procedures might differ depending on which version of XenServer you are using. This procedure is relevant for XenServer 5.6.

Before you begin, please ensure that:

1. You have a username and password of an Administrator user of Active Directory, if you are going to link to an Active Directory server for user authentication.
2. You have some idea of how much storage space will be needed for VM images, and set up sufficient storage in an NFS share, or in the case of local storage, ensure that there is sufficient free space.
3. You have decided on an FQDN for your Synchronizer server, whether to use a static IP address or DHCP, and configured your DNS appropriately.

**Note**

Due to a limitation in third-party software used by XenClient, the FQDN must start with a letter character. Number or symbols are not allowed at the beginning of a Synchronizer FQDN.

**To Download, Import, and Prepare the Virtual Appliance:**

The following procedure assumes that you are working on a Windows machine that has XenCenter installed.

1. Download the Synchronizer appliance from http://www.citrix.com/xenclient/tryit. This is a compressed archive which contains a .xva file.
2. Uncompress the file and double-click the .xva file to import it into XenCenter.
3. XenCenter launches, and the **Import Source** page of the **Import** wizard is displayed.
4. Click the **Next** button. The **Home server** page is displayed.
5. Choose a pool or a server on which to start the Synchronizer VM, then click **Next**.
   
   The **Storage** page is displayed.
6. Choose a storage repository on which the imported virtual disks of the VM will be created, then click **Import**.
   
   The **Importing VM...** progress bar is displayed. After a short time, the **Network** page of the **Import** wizard is displayed.
7. Select the network that you want the VM to have access to, then click **Next**.
The Finish page is displayed.

8. At the bottom of the Finish page is a checkbox labeled Start VM after import which is checked by default. Uncheck this if you want to increase the size of the virtual disk assigned to hold your VM images (which is 18GB by default). You can then choose to increase the size of the virtual disk before starting the VM and stepping through the various steps of the Synchronizer installation.

You can also change the virtual CPU properties and virtual memory assigned to the appliance at this point (the default RAM assigned is 1 GB).

If you do start the VM automatically after the import operation is finished, you can always shut it down to resize the virtual disk and change CPU and memory properties afterwards.

9. Click Finish to exit the wizard.

The import process begins. This can take several minutes. When the VM is finished being imported, it will appear under the selected host node, or under the node of the host which the system chose if you selected a pool to import it into rather than a specific host.

10. If you want to change the properties of the Synchronizer VM or resize the virtual disk to be used for VM image storage, complete the following steps. If not you can continue to the next step.

   a. If you do want to resize the virtual disk for the VM, select it on the left pane, then click the Storage tab, then select the virtual disk named xt-data-vol and click the Properties button.

   b. The Properties dialog box is displayed for the selected virtual disk.

   c. Click Size and Location on the left side, and use the Size control to set the disk size to the desired value.

   d. Click the OK button.

      The dialog box closes and, after a few moments, the Size column in the Storage tab is updated to the new size.

   e. If you do want to modify the CPU properties, select the VM on the left pane, then click the General tab.

   f. Click the Properties button at the top of the window. The Properties dialog box of the selected VM is displayed.

   g. Click CPU and Memory on the left side.

      Use the Number of VCPUs control to set the number of virtual CPUs to the desired value. You can also set the VCPU priority and the amount of RAM to be assigned to the Synchronizer VM on this page.

      **Note**

      1024 MB is the default amount of memory, but Synchronizer can work with as little as 256 MB, so you can reduce the amount of RAM if desired.

   h. Click OK.

   i. If you changed the VM memory or the Number of VCPUs setting the VM General Changes dialog box is displayed, stating that the VM must be restarted for the new settings to take effect. Click the OK button to dismiss this dialog box.

   j. If required, right-click on the VM and select Reboot, then click Yes to confirm the reboot action.

11. If your VM is not already started, right-click on the VM and select Start.

12. Once the Synchronizer VM has started, click the Console tab to access the command line console.

13. Initial installation steps are performed and the VM boots. Once the VM has booted the Synchronizer for XenClient console is displayed, which guides you through the rest of the Synchronizer installation process.
14. The **End User License Agreement** screen is displayed. Press **Enter** to accept the license agreement.

15. On the next screen, enter and confirm a root password for the VM and press **Enter** to continue.

16. On the next screen, select the **IP address configuration mode**. Select **DHCP** to enter the hostname allocated to this VM by a DHCP server or **Static** to set up a static IP address, hostname and DNS server configuration. Press **Enter** to confirm your chosen network settings. The **Configuring network...** message is displayed.

**Note**

If the Synchronizer FQDN cannot be resolved, due to incorrect DNS settings for example, an appropriate IP address will be chosen and used as the Synchronizer URL.

17. When the system has completed writing the network configuration, the **Customize certificate attributes** screen is displayed. Use this screen to configure the details of the certificate to be used for HTTPS communication with the Synchronizer VM. Fill in the desired values and then press **Enter**. The **Installing certificates...** message is displayed.

18. On the next screen, enter and confirm an administrator password to be used for accessing the Synchronizer web interface as the admin user, and press **Enter** to continue. The **The initial Synchronizer setup process is complete** message is displayed alongside the Synchronizer web interface FQDN. Press **Enter** to continue.

19. The **Synchronizer for XenClient** configuration console is displayed. This is the standard console to be used for changing Synchronizer configuration, which is automatically displayed in the **Console** tab of the VM in XenClient whenever the Synchronizer VM is booted.

### 3.2. Upgrading Synchronizer To a New Version

If you are running Synchronizer 2.0, you can upgrade it to the current version. The upgrade file is available for download from the Citrix website.

**Note**

If you are running Synchronizer 1.0 Service Pack 1, you must upgrade it to Synchronizer 2.0 before upgrading it to the current version. You cannot upgrade 1.0 Service Pack 1 to the current version directly.

If you are running Synchronizer 1.0, you must upgrade it to Synchronizer 1.0 Service Pack 1, and then upgrade it to Synchronizer 2.0 before upgrading it to the current version. You cannot upgrade 1.0 to the current version directly.


Download the 1.0 SP1 upgrade from [https://www.citrix.com/English/ss/downloads/details.asp?downloadId=2306797&productId=2300325](https://www.citrix.com/English/ss/downloads/details.asp?downloadId=2306797&productId=2300325).

In addition, from time to time Citrix might make service packs for Synchronizer available for download from the Citrix website.

**Note**

Synchronizer 2.1 supports XenClient devices running version 2.1 and version 2.0 of XenClient.

To upgrade your Synchronizer to a newer version, follow this procedure.

**To upgrade Synchronizer to a newer version:**

1. Transfer the upgrade file `synchronizer_upgrade.zip` file to the Synchronizer appliance via ftp, scp or wget. For example, from the Synchronizer console, as the root user:
wget <path to zip file>/synchronizer_upgrade.zip

2. Once the file has been transferred to the Synchronizer appliance, unzip it with the following command:

    unzip synchronizer_upgrade.zip

3. Run the upgrade script:

    ./upgrade.sh

4. Reboot the Synchronizer VM.

    Note

    Be sure to transfer the zip file over to the Synchronizer appliance and unzip it there. Do not unzip it on another computer first, then transfer the unzipped files and run the upgrade script - it will fail on a MD5 checksum error if you do that.
Chapter 4. Configuring the Synchronizer

Upon installation, the Synchronizer is configured with information provided during the installation process. You might need to reconfigure some of the settings. This chapter describes how to do that. The procedures below are performed using the Synchronizer for XenClient console.

To access the console, click the Console tab of the Synchronizer VM in XenCenter. To make changes to configuration you will be prompted to log in as the root user.

**To Join an AD Domain:**

1. In the console, follow the menu path Active Directory Settings.
2. Enter the FQDN of your AD server, the Organizational Unit (if necessary), the User Name and the Password.
3. Press Enter.

**To Change the Synchronizer timezone:**

1. In the console, follow the menu path Timezone > Set Timezone. A list of Regions is displayed.
2. Select the Region of your desired timezone and press Enter. A list of cities with the selected region is displayed.
3. Select the City of your desired timezone and press Enter. An message is displayed stating that the timezone has been changed. Press Enter to dismiss the message.

**To Configure the Management Interface:**

1. In the console, follow the menu path Network and Management Interface > Configure Management Interface > Configure Network Interface.
2. Select the type of configuration desired and press Enter. If you are using a static IP address without DHCP, enter the IP address, netmask, gateway and hostname. Press Enter.

3. Press Enter to accept the configuration changes.

To Configure a DNS Server:

This information is typically configured during installation, but it can be added or edited later as described below. You can add new nameservers, remove existing nameservers, edit the name of the local domain, and edit the DNS search list.

1. In the console, follow the menu path Network and Management Interface > Configure DNS resolver. The following dialog box is displayed:

   ![DNS Configuration](image)

   Add or Remove Nameserver Entries
   
   Add a Nameserver
   Remove a Single Nameserver
   Remove All Nameservers
   Update local domain name
   Update search list for host-name lookup

   <Enter> OK <Esc> Cancel

   (Note that if no nameservers are currently configured on the Synchronizer, only Add a Nameserver, Update local domain name, and Update search list for host-name lookup are displayed.

2. Select the relevant operation and press Enter.

3. Follow the instructions and provide the relevant information for the operation you have selected and press Enter.

To Change Admission Control Settings:

The Admission control settings control the maximum number of XenClient devices that can connect to your Synchronizer server at the same time. By default at installation time, the mode is set to Automatic, which sets a fixed number of clients that can connect (the number depends on the hardware available to the Synchronizer). You can change the mode to Manual and decrease increase this number to a maximum allowed value of 50.

There is also Disconnect grace period with a default of 180 seconds. A client holds an admission slot while performing a transfer and gives up the slot when the transfer completes. However, there are times when a transfer might be interrupted (intermittent network connectivity, or perhaps the user has manually paused the transfer). The Disconnect grace period allows the client to maintain its admission slot and resume transfer.

1. In the console, select Admission Control Settings and press Enter.

2. Select the admission control setting mode, Manual or Automatic, then press Enter.

3. If you chose Manual in the previous step, enter the desired number of Maximum connections (the default is 25), then press Enter. Enter the desired number of seconds for the Disconnect grace period (the default is 180 seconds) and press Enter again.

   If you chose Automatic in the previous step, you are only prompted to edit the desired number of seconds for the Disconnect grace period. Press Enter.

4. An "updating settings" message is displayed, then a "configuration successful" message. Press Enter to dismiss the message.
To Change The Root Password:

1. In the console, follow the menu path Authentication > Change Root Password.
2. Enter the old password, the new password, and then confirm the new password and press Enter.

To Change the Synchronizer Web Interface Admin User Password:

1. In the console, follow the menu path Admin UI > Change Admin UI Password.
2. Enter the new password, confirm the new password and press Enter.

To Configure the Default Port for the Synchronizer web interface:

When installed, the port on which the administrators access the Synchronizer web interface is set to Port 8443. If you need to change this, perform the following steps.

1. In the console, follow the menu path Admin UI > Change Admin UI Port.
2. Enter the desired port number and press Enter.

   Note

   The port number should be in the range of 1024 to 49151.

3. Press F8 to accept the configuration changes.
4. On completion, a "configuration successful" message is displayed. Press Enter to dismiss this message.

To Regenerate the CA Certificates:

   Note

   Regenerating a CA certificate also cause a new SSL certificate to be generated. This is to ensure that there is never a situation where a valid CA certificate exists but no SSL certificate exists.

1. In the console, follow the menu path SSL Certificate > CA Certificate.
2. Enter the certificate attributes and press Enter. The Generate Certificate dialog is displayed. Press Enter to continue. The Installing Certificates... dialog is displayed.
3. On completion, a "certificate installation successful" message is displayed. Press Enter to dismiss this message.

To Regenerate the Web Server SSL Certificates:

1. In the console, follow the menu path SSL Certificate > SSL Certificate for Web Server.
2. Enter the certificate attributes and press Enter. The Generate Certificate dialog is displayed. Press Enter to continue. The Installing Certificates... dialog is displayed.
3. On completion, a "certificate installation successful" message is displayed. Press Enter to dismiss this message.
Chapter 5. Administration

This section contains the procedures required for administering Synchronizer, using the Synchronizer web interface, which can be accessed by pointing a web browser at the Synchronizer server host name over HTTPS. Citrix recommends using one of the following browsers:

- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Firefox 3.6
- Firefox 4
- Firefox 5
- Firefox 6

5.1. Synchronizer Web Interface Overview

To connect to the Synchronizer web interface, enter the DNS host name of the Synchronizer VM in your browser address bar and connect over HTTPS. Log in using the administrator username admin and the administrator password.

By default XenClient devices connect to Synchronizer over port 443 and also port 80 if HTTP bulk transfer is enabled. See Section 5.8: “Enabling VM Image Download and Upload Over HTTP” for more information about HTTP bulk transfer. An Admin user logs in to Synchronizer over port 8443 (by default; if this has been reconfigured, use the appropriate port in the discussion below). This allows the corporate firewall to be configured to reject traffic to port 8443 that comes from outside of the corporate network. An attempt to log in to the Synchronizer web interface over port 443 will automatically be redirected to port 8443. If you are not using trusted certificates it is therefore possible that your browser will prompt you twice to accept untrusted certificates, once when the initial attempt to connect is made over port 443 and again when the attempt to connect is redirected to port 8443, before allowing access to the Synchronizer web interface.

After logging in successfully, the Welcome to Synchronizer for XenClient dialog box is displayed. This dialog box contains some useful information to quickly get you started working with Synchronizer. To dismiss this dialog, click the cross at the top right. If you do not want to see this dialog every time that you log in, check the Don't show at logon checkbox before dismissing it. You can view this dialog box at any time by clicking Settings and then clicking the Show Help button.

Next, the VM Images screen is displayed. When the Synchronizer web interface is first displayed, only the admin user is listed, and there are no VM images or devices.
Figure 5.1. Synchronizer Web Interface After Installation:

To navigate through the Synchronizer web interface, click on the buttons along the top to access the corresponding pages.

<table>
<thead>
<tr>
<th>Button</th>
<th>Page description</th>
</tr>
</thead>
</table>
| Images | The **Images** page shows a list of available VM images in the image library. You can select and assign them to users and view their disk usage. Also on this page you can:  
• Filter the images displayed by entering text in the **Search images** text box. All images that contain the text that you enter in their name or description will be displayed.  
• View the number of VMs deployed in the graph on the left hand side.  
• Click the **Disk Space Usage** button to display a graph of how much disk space the VM images are taking up on the Synchronizer VM disk. |
<p>| Users  | The <strong>Users</strong> page shows a list of available users and groups. Here you can add new local users and groups and link in users and groups from AD. If you click on a user in the <strong>Users</strong> list, the <strong>User Details</strong> page is displayed. Here you can edit user information, delete this user, view a list of devices and VMs assigned to this user, assign new VM images to the user, edit VM policy, and revoke VM assignments. If you click on a group in this list the <strong>Group Details</strong> page is displayed. Here you can edit group information, delete a group, view a list of group users and VMs assigned to this group, assign new VM images to the group, edit VM policy, and revoke VM assignments. Also on this page you can filter the users and groups displayed by entering text in the <strong>Search Users</strong> or <strong>Search Groups</strong> text box. |</p>
<table>
<thead>
<tr>
<th>Button</th>
<th>Page description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices</td>
<td>The <strong>Devices</strong> page shows a list of registered devices along with users and device vendors, and allows you to delete a device or mark a device as missing.</td>
</tr>
<tr>
<td>Activity</td>
<td>The <strong>Activity</strong> page shows a list of active VM image transfers or a system log.</td>
</tr>
</tbody>
</table>
| Settings | The **Settings** page shows a list of available image repositories and registration PINs. From here you can add new image repositories, edit existing image repositories, enable or disable the registration PIN feature, add new registration PINs, edit registration PINs, delete registration PINs and search registration PINs by name or description. Also on this page you can:  
  - Click the **Generate Diagnostic Report** button to generate a status report.  
  - Click the **Show Help** button to view a short help screen (the same one displayed when you connect to the Synchronizer through the web interface) which contains useful information to help you get started using Synchronizer. |

### 5.2. Managing Users and Groups

Synchronizer users and groups can be managed using the Synchronizer web interface, or in AD.

#### 5.2.1. Managing Local Users and Groups

A local user exists entirely in the Synchronizer database.

**To Create a Local Synchronizer User:**

1. In the Synchronizer web interface, click **Users**.
2. Click **Add Local User**. The **Add Local User** dialog is displayed.

3. Enter the user details.
4. To grant the user **Admin** rights, select **Admin** from the **Role** dropdown list. **Admin** rights allow the user to publish VMs to Synchronizer and log in to the Synchronizer web interface.
5. To grant the user access to Synchronizer, select **Allow** from the **VM Image access** dropdown list. Select **Not specified** to use the access settings of a group to which the user belongs instead, or **Deny** to deny the user access for the time being.

   **Note**
   
   An **admin** user automatically has full access.

6. Click the **Add** button.

**To Delete a Local Synchronizer User:**

Deleting a local user has the following effects:

- The user name field in the Synchronizer records of all the user’s XenClient devices is set to empty and the devices becomes unregistered.
- All VMs on the user device become unmanaged.
- All VM image assignments for the user are deleted.

1. In the Synchronizer web interface, click **Users**.
2. Click on the user name.
3. Select **Delete User** from the dropdown list in the **User Details** box. The **Delete User** dialog is displayed.
4. Click **Delete User** to confirm.
5. If desired, delete the records of the user's devices.

**To Create a Synchronizer User Group:**

To make the management of VM images easier, Synchronizer supports user groups. An administrator can assign a VM image or a set of VM images to a group of users that have similar computing needs.

1. In the Synchronizer web interface, click **Users**.
2. Click the **Groups** tab.
3. Click **Add Local Group**.

   ![Add Local Group](image)

4. Enter a name for the group in the **Name** text box.
5. Enter a description of the group in the **Description** text box.
6. To grant users in the group access to Synchronizer, select **Allow** from the **VM Image access** dropdown list. Select **Not specified** to use the access settings of the individual users instead, or **Deny** to deny the group access for the time being.
7. Click **Add**.
To Add a User to a Group:

Once a group has been created, you can add new users to it, who will inherit the VM images already assigned to
the group.

**Note**

Synchronizer does not support adding both local and AD users to the same group.

**Note**

XenClient does not provide the facility to edit the membership of AD groups. Any changes to AD groups or
users must be performed using your interface to AD.

1. In the Synchronizer web interface, click **Users**.
2. Click the **Groups** tab.
3. Click the group that you want to add the user to.
4. Click **Edit Group**. The **Edit Group Membership** window is displayed.
5. Select the user or users that you want to add to the group in the list on the left. You can hold down Ctrl and
click to add multiple users.
6. Click **Add selected** to add the selected users.
7. To grant users in the group access to Synchronizer, select **Allow** from the **VM image access** dropdown list.
   Select **Not specified** to use the access settings of the individual users instead, or **Deny** to deny the user
group access for the time being.
8. Click **OK**.

To Delete a Local Synchronizer User Group:

Deleting a local user group also deletes all VM image assignments to the group.

1. In the Synchronizer web interface, click **Users**.
2. Click the **Groups** tab.
3. Click on the group name.
4. Select **Delete Group** from the dropdown list in the **Group Details** box. The **Delete Group** dialog is displayed.
5. Click **Delete Group** to confirm.

5.2.2. Managing AD Users and Groups

To Link in an Existing AD User:

You can link in an existing AD user to Synchronizer. When the user logs in they will be authenticated against the AD
server.

**Note**

This feature is only available in the web interface if your Synchronizer is connected to an AD server.

1. In the Synchronizer web interface, click **Users**.
2. Click **Link AD User**. The **Add Link to Domain User** window is displayed.
3. Enter the **AD Username**.
4. Select the user role from the **Role** dropdown list.
5. To grant the user access to Synchronizer, select **Allow** from the **VM Image access** dropdown list. Select **Not specified** to use the access settings of a group to which the user belongs instead, or **Deny** to deny the user access for the time being.

6. Select the Domain from the **Domain (NETBIOS)** dropdown list.

7. Click **Link**. Synchronizer connects to the AD domain specified, and creates the link if a valid user has been specified.

**To Link in an Existing AD User Group:**

You can link in an existing AD user group to Synchronizer. When a user in this group logs in they will be authenticated against the AD server.

![Note]

This feature is only available in the web interface if your Synchronizer is connected to an AD server.

1. In the Synchronizer web interface, click **Users**.
2. Click the **Groups** tab.
3. Click the **Link AD Group** button. The **Add Link to Domain Group** window is displayed.
4. Enter the **AD Group Name**.
5. To grant the group access to Synchronizer, select **Allow** from the **VM Image access** dropdown list. Select **Not specified** to use the access settings specified in the user settings instead, or **Deny** to deny the user group access for the time being.
6. Select the Domain from the **Domain (NETBIOS)** dropdown list.
7. Click **Link**. Synchronizer connects to the specified AD domain, and creates the link if a valid group name is entered.

### 5.2.3. Changing the User Name Registered With Synchronizer

If the user name of an AD user with a device that is registered with Synchronizer changes, it is necessary to manually change the user name under which the device is registered on the XenClient device itself. To do this, press **Ctrl+Shift+t** in Citrix Receiver for XenClient to open a control domain console. Then run the following command:

```plaintext
set_platform_username <new_username>
```

This changes the user name on the device so that the user can authenticate with Synchronizer using the new credentials.

![Note]

Installing Microsoft Windows Server 2003 Service Pack 1 (SP1) on your Domain Controller is known to change authentication behavior so that users can authenticate using their old password for up to an hour after changing it. For more information about this issue and for a workaround, see [http://support.microsoft.com/kb/906305/en-us](http://support.microsoft.com/kb/906305/en-us).

### 5.3. Managing VM Images

To add an image to the image repository, you will need an existing VM on a XenClient device. Connect the device to Synchronizer, and then upload the VM to create a new VM image. See the Section 4.1: “Installing VMs on XenClient” in *Citrix® XenClient™ 2.1 Setup and Usage Guide* for information about how to install a VM on a XenClient device.

**To Connect a XenClient Device to Synchronizer:**

1. In Citrix Receiver for XenClient, click **System**. The **System Settings** dialog box is displayed.
2. Click **Synchronizer** on the left side of the dialog box.
3. Click **Register**. The **Register with Synchronizer** wizard is displayed.
4. Enter the FQDN or IP address of the Synchronizer server and click **Next**.
5. Ensure that the Synchronizer Identification Code in the dialog box is the same as the one displayed during Synchronizer installation.
   
   If the Synchronizer has the Registration PIN feature enabled, enter the PIN in the **Registration PIN** field.
   
   Click **Next**.
6. Press **Ctrl + Alt + Backspace** and enter your Synchronizer user name and password. Press **Enter** to complete the connection process.

**To Upload a VM to Synchronizer:**

To upload a VM to a Synchronizer, you must be connected as a user whose account has the Admin role, or as a user whose account has the Standard role and whose policies have been set to allow them to upload VMs.

1. On the XenClient device, shut down the VM that you want to upload to the Synchronizer.
2. Hover your mouse over the VM icon and click **Details** to open the VM details window.
3. Click **Upload VM**. The **Upload to Synchronizer** dialog box is displayed.
4. Enter a **VM name** and **Description**.
5. Select the VM image mode. See Section 6.1: "VM Image Modes" for more information about VM image modes.
6. Click **Finish**.
7. The transfer of the image to the Synchronizer commences, and a progress bar is displayed. (A similar progress bar is displayed in the Synchronizer web interface if you click **Activity**).

**To Delete a VM Image:**

Deleting a VM image removes the VM from Synchronizer. Any deployed VMs that are based on the VM image will become unmanaged by Synchronizer as soon as the client device connects to Synchronizer. All versions and backups of the VM image are deleted, as are any VM image assignments of the deleted VM image.

1. In the Synchronizer web interface, click **Images**.
2. Click on the name of the VM image you want to delete.
3. Click the **Delete VM Image** button. The **Delete VM Image** dialog box is displayed.
4. Click **Delete VM** to confirm the deletion.

**To find VHDs associated with a VM Image:**

To figure out which VHDs are related to a VM, use the following command to output the paths of all VHDs related to a specific VM name and version.

- At the console for the Synchronizer appliance, run the following command as root:

```
get-vm-disks -n <vm_name> -v <version>
```

The paths to all the VHDs associated with the specified VM are displayed.

**Note**

Use double quotes around `<vm_name>` if it contains whitespaces.
5.4. Managing VM Image Assignments

To Assign a VM Image:

Once a VM has been uploaded to Synchronizer, it is shown on the VM images screen. You can now assign this VM image to users or groups, which allows them to install it on their device.

1. In the Synchronizer web interface, click Images to display a list of the available VM image images.
2. Click Assign of the relevant VM image. The Assign VM image window is displayed.
3. Select either User or Group from the Assign To drop down menu, then select a specific user or group from the User or Group drop down menu.
4. Click Continue.
5. The VM image page of the wizard is displayed. Select the VM and the VM version to be assigned.
6. Click Continue. The Policy page of the wizard is displayed. Here you can set VM policy.
7. On the General page, you can set the following:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>The amount of virtual RAM to assign to the VM.</td>
</tr>
<tr>
<td>Enable Disk Encryption</td>
<td>If enabled, the contents of the VHD files used by the VM will be encrypted using the AES XTS (256-bit) cypher.</td>
</tr>
</tbody>
</table>

**Note**
Disk encryption is only applied when a VM is first deployed to a device. Editing an assignment at a later point will not cause the disk to be encrypted.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable 3D Graphics</td>
<td>If enabled, the VM will have 3D graphics support enabled. Note that this means that the client device this image is assigned to can only run one VM at a time.</td>
</tr>
<tr>
<td>Enable Autoboot</td>
<td>If enabled, the VM will automatically boot when its host device is booted.</td>
</tr>
<tr>
<td>Enable Power Control</td>
<td>If enabled, when the VM is powered down or restarted, the host device will also be powered down or restarted.</td>
</tr>
<tr>
<td>Allow users(s) to change properties</td>
<td>If enabled, allows users to change VM properties in Citrix Receiver for XenClient.</td>
</tr>
</tbody>
</table>

8. Click **Network** and select whether or not to enable **Wired** and **Wireless** access for this user.

9. Click **Devices** and select which classes of USB devices are allowed to be used.

**Warning**

Because many USB devices are composite USB devices which expose multiple devices of different device classes, not allowing a particular device class can affect the ability of the user to use USB devices which one otherwise might expect to work. For example, some USB modems initially present themselves as mass storage devices to allow the user to install drivers contained on the mass storage embedded in the device. It is only after the drivers are installed that the USB modem is recognized as a USB modem. However, if mass storage USB is disallowed under the policy you set, the user will not be able to install the drivers and will therefore not be able to use the USB modem.

<table>
<thead>
<tr>
<th>USB device class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio</td>
<td>Devices for interfacing external audio devices (microphones, audio line level signals, etc.) to the computer. Select the level of enablement using the radio buttons.</td>
</tr>
<tr>
<td>Optical Drive</td>
<td>The onboard optical drive, for example Blu-ray drive. Select the level of enablement using the radio buttons.</td>
</tr>
<tr>
<td>Allow these USB Devices</td>
<td>Audio USB devices.</td>
</tr>
<tr>
<td>Allow these USB Devices</td>
<td>Devices for capturing still images (cameras, scanners).</td>
</tr>
<tr>
<td>Allow these USB Devices</td>
<td>USB printers.</td>
</tr>
<tr>
<td>Allow these USB Devices</td>
<td>External hard drives, DVD burners, USB sticks, etc.</td>
</tr>
<tr>
<td>Allow these USB Devices</td>
<td>Devices for capturing video data (web cams, digital video cameras).</td>
</tr>
<tr>
<td>Allow these USB Devices</td>
<td>All devices which do not have a standard USB class ID.</td>
</tr>
</tbody>
</table>
10. Click **Synchronizer** and set the following properties:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lease Expiration</strong></td>
<td>14 days</td>
<td>The number of days that the VM image is leased to the user. If the user does not authenticate with the Synchronizer before the lease time expires, the leased VM shuts down and the <strong>REMOTE LOCKED</strong> message is displayed. Connecting to and authenticating with Synchronizer will renew the lease. To ensure that lease times are not renewable, the administrator of the Synchronizer needs to manually revoke the assignment of the VM image to the user when they wish the lease to expire and not be renewable anymore. Enter 0 if you do not want to use a lease time for this assignment.</td>
</tr>
<tr>
<td><strong>Update Schedule</strong></td>
<td>60 minutes</td>
<td>The interval, in minutes, that the registered XenClient device will check for policy updates from the Synchronizer.</td>
</tr>
<tr>
<td><strong>Backup Contents</strong></td>
<td>All-Data</td>
<td>By default all data is backed up. For Windows VMs, setting this property to <strong>User-Data</strong> causes only the user directories of the VM to be backed up.</td>
</tr>
<tr>
<td><strong>Allow Manual</strong></td>
<td>Disabled</td>
<td>Allows the user to manually perform VM backups.</td>
</tr>
<tr>
<td><strong>Automatically</strong></td>
<td>Disabled</td>
<td>Enables automatic VM backups. If enabled, specify the number of hours that will elapse before the VM image will next be backed up automatically in the provided text box.</td>
</tr>
</tbody>
</table>

11. Click **Advanced** and set the following property:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allow users to author new versions of this image</strong></td>
<td>Enabled for users with the admin role; disabled for other users</td>
<td>Sets whether the user can upload a VM to the Synchronizer.</td>
</tr>
<tr>
<td><strong>Enable seamless application support</strong></td>
<td>Enabled</td>
<td>Sets whether seamless application support is enabled.</td>
</tr>
</tbody>
</table>

12. Click **Finish**.

If you want to change any of the user settings for this assignment, click on the user or group in the **Users** list, then click **View**, **Edit**, or **Revoke** next to the image name in the **Actions** column.

**To Edit an Assignment:**

1. In the Synchronizer web interface, click **Users** or **Groups**.
2. Click the relevant user or group name.
3. Next to the relevant assignment in the **Available Assignments** table, select the **Edit** action. Follow the steps of the **Assign VM Image** wizard to edit the assignment.
Note

Disk encryption is only applied when a VM is first deployed to a device. Editing an assignment at a later point will not cause the disk to be encrypted.

To Revoke an Assignment:

Revoking an assignment causes all the details of the assignment to be permanently erased from Synchronizer. Once the lease time of the VM expires, the user no longer be able to use it.

1. In the Synchronizer web interface, click Users or Groups.
2. Click the relevant user or group name.
3. Next to the relevant assignment in the Available Assignments table, select the Revoke action.
4. The Revoke Assignment? dialog is displayed. Click Revoke to permanently revoke the assignment.

5.5. Working with Devices

The Devices page lists all devices registered with the Synchronizer, displaying the Model, Vendor, User Name, Status, and Version of XenClient for each.

To ensure that sensitive data is not compromised when a device is lost or stolen, XenClient provides the ability to mark the device as "lost" and remotely ensure that managed VMs on the missing device cannot be started.

To Mark a Device as Lost:

1. In the Synchronizer web interface, click Devices.
2. Click Mark as Lost next to the lost device and click Yes.

When the VM next connects to Synchronizer the status of all managed VMs on the device is changed to Remote Locked, all managed VMs are forcibly shut down, and no managed VMs can be booted.

Warning

As with a bare-metal operating system, if a managed VM is attempting to update using Windows Update while it is forcibly shut down, the VM may suffer from corruption caused by the interruption to the update.

To Delete a Device:

1. In the Synchronizer web interface, click Devices.
2. Next to the device in the All Devices table, select the Delete action.
3. The Delete Device? dialog is displayed. Click Delete Device to permanently delete the selected device.

Filtering the Devices List

On the left side of the screen are table filters that can be applied to the devices list.

<table>
<thead>
<tr>
<th>Table Filters</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Not checked last any days</td>
</tr>
<tr>
<td>□ Lost in last any days</td>
</tr>
<tr>
<td>□ From vendor any with model any</td>
</tr>
<tr>
<td>□ Where XenClient version is any</td>
</tr>
</tbody>
</table>
You can filter the list by any combination of the following:

<table>
<thead>
<tr>
<th>Filter</th>
<th>How to use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not checked last any days</td>
<td>Click the checkbox to filter the list to show only devices that have not been checked for a specified number of days. To specify the number of days, click on the word any in the filter text and type the desired number into the field that appears.</td>
</tr>
<tr>
<td>Lost in last any days</td>
<td>Click the checkbox to filter the list to show only devices that have been lost for a specified number of days. To specify the number of days, click on the word any in the filter text and type the desired number into the field that appears. If you do not specify the number of days, it will display all devices that have ever been lost.</td>
</tr>
<tr>
<td>From vendor any with model any</td>
<td>Click the checkbox to filter the list to show only devices from a specified vendor and of a specified model. To specify the vendor, click on the first instance of the word any in the filter text and type the desired vendor name into the field that appears. Likewise, to specify the model, click on the second instance of the word any in the filter text and type the desired model name into the field that appears. If you do not specify either of these names, the list will display all devices. For example, if you specify the vendor Dell Inc. but do not specify the model, the list will display all Dell models.</td>
</tr>
<tr>
<td>Where XenClient version is any</td>
<td>Click the checkbox to filter the list to show only devices running a specified version of XenClient. To specify the version, click on the word &lt;any&gt; in the filter text and type the desired version into the field that appears. If you do not specify the version, devices of any version are displayed.</td>
</tr>
</tbody>
</table>

You can use these filters in combination. For example, if you wanted to show just the Dell devices that were running version 1.0, you would select the checkboxes for the last two filters, type "Dell Inc." for the vendor in the first, and type "1.0" for the version in the second.

### 5.6. Working With Image Repositories

By default, Synchronizer is installed with a local image repository with 18G of space. You can add NFS image repositories using the Synchronizer web interface.

**Note**

The local image repository size cannot be modified from the Synchronizer web interface. It must be changed by resizing the virtual disk of the Synchronizer appliance in XenCenter, as described in the Synchronizer installation procedure.

**To Add an NFS Image Repository:**

1. In the Synchronizer web interface, click Settings.
2. Click Add Image Repository.
3. Enter a name to identify the repository in the Name text box.
4. Enter the IP address or DNS name of the NFS server, for example, nfs.mycompany.com in the Server Address text box.
5. Enter the path to the exported share on the server (for example, /exports/xc-images) in the Server Path text box.
6. Enter and standard Linux mount options you want to use in the Mount Options text box.
7. Click OK.
8. All new VM images will be put in the new network image repository.

5.7. Registration PINs

In some cases you might want an additional level of security for your Synchronizer, in addition to requiring users to provide their username and password. Synchronizer includes a means for adding registration PINs that users will be required to provide upon registering their devices. The PINs are autogenerated.

PINs are added and managed in the Settings page.

To Add a Registration PIN:

1. On the Settings page, in the Registration PINs section, click the Add Registration PIN button. A dialog box appears.
2. In the Number of devices field, enter a number (or use the increment/decrement control on the right). The default is 1.
   In the Expiry field, if the Enabled checkbox to its right is checked, enter a date in the form yyyy-mm-dd (or use the calendar button to the right and choose a date from the calendar control that is displayed). By default the expiry date is enabled and set to 30 days from now.
   In the Description field, type some descriptive text.
   All of these fields are required.
3. Click OK. The dialog box closes and the new PIN is added the list in the Registration PINs section.

Once you have added a PIN, you still need to enable its use.

To Enable the Use of Registration PINs:

• Click the button on the top right of the Registration PINs section to set its state to ON.

To Disable the Use of Registration PINs:

• Click the button on the top right of the Registration PINs section to set its state to OFF.

5.8. Enabling VM Image Download and Upload Over HTTP

Because VM images are encrypted for transfer, it may be safe to change the default HTTPS mode of transfer to use HTTP instead. Doing so will decrease the load on your Synchronizer server and should increase the speed of image transfer between XenClient clients and the Synchronizer server.

Warning

Using HTTP presents a risk that the HTTP session token could be intercepted and used maliciously. This includes the risk that the token could be used by an attacker to overwrite Synchronizer data. Citrix recommends taking appropriate steps to mitigate this risk if you choose to enable transfer over HTTP.

To Enable VM Image Transfer Over HTTP:

1. In XenCenter, click the Console tab of your Synchronizer VM and select Local Command Shell from the console menu.
2. The local command shell opens. Log in with the root user credentials.
3. Enter the command:

```bash
vi /xt/config/site.conf
```

4. Change the line:

```python
imagelibrary.bulk_transfer_scheme = "https"
```

5. To read:

```python
imagelibrary.bulk_transfer_scheme = "http"
```

6. Type

```bash
exit
```

and press Enter to quit the local command shell.

7. Reboot the Synchronizer VM from either the console menu or from the XenCenter VM menu.

VM images will now transfer using HTTP over port 80.

5.9. Using a Local VHD Cache to Accelerate VM Download from Synchronizer

When a VM download from Synchronizer is initiated, XenClient attempts to locate VHDs in an attached optical disk or USB drive which would otherwise have to be downloaded from Synchronizer. Using a local VHD cache in this manner can greatly speed up the installation of a VM image onto a device. Use the following procedure to create a local VHD cache:

**To Prepare a Local VHD Cache:**

1. Create, prepare, and upload a VM to Synchronizer.

2. To identify which VHD files are used by the VM, open the local command shell in the console on your Synchronizer appliance, then run the following command:

```bash
get-vm-disks -n "<vm_name>" -v <version>
```

**Note**

Use double quotes around `<vm_name>` if it contains whitespace.

The paths to all the VHDs associated with the specified VM are displayed.

3. Copy the VHDs to a USB drive or burn them to an optical disk. The USB drive must be formatted with an NTFS filesystem. For DVDs, please burn the VHDs to a UDF filesystem. Ensure that:

- The VHD filenames are not changed.
- The VHD files are present in the root folder of the medium.

It is also possible to cache a portion of a VHD file if it is too large for the cache medium. For example, if you have a 4.3 GB VHD file and a 4 GB USB drive, you can use the `split` command in a console on your Synchronizer server:

```bash
split -b 4000M <vhd_filename> xenclient
```

to split the VHD into two files, xenclientaa and xenclientbb:

```bash
ls -lh
```

```bash
total 8.6G
```
You can then rename `xenclientaa` to `example.vhd` and put it on the cache medium. When a download is initiated, XenClient first searches for a USB drive that contains a portion or all of the required VHD(s), then for a optical media drive, and then that falls back to downloading any remaining VHDs or portions thereof from Synchronizer.

**Note**

For successful VHD cache reading, it is essential that only the first portion of any VHD is present on the cache medium. For example, putting the `xenclientab` file onto the cache medium will cause the image transfer to fail.

4. Assign the VM image to a user.

5. Insert the USB device or optical disk into the user’s XenClient device, and initiate the VM image download.

### 5.10. Backing up Synchronizer and its VM images

Citrix recommends backing up your Synchronizer environment. This includes the Synchronizer virtual appliance itself, including its metadata about users, assignments, etc., and the XenClient VM images that you are managing with it.

In a typical environment, the XenClient VM images will be on shared storage. You can just back these up by whatever means you currently use. For example, you can periodically rsync the images to a remote filer.

For the Synchronizer appliance itself and its database, and also any VM images that you might be saved on local storage, we recommend the following procedure.

**To Back Up a Synchronizer:**

1. In XenCenter, right-click on the Synchronizer appliance and choose **Shut Down**.

2. When the Synchronizer is no longer running, right-click and this time choose **Take Snapshot**. In the dialog box that appears, provide a Name and Description for the Snapshot, and make sure the Snapshot mode is set to **Snapshot the virtual machine’s disks**.

3. When the snapshot is completed, click on the **Snapshots** tab, select the snapshot you just took, click the **Actions** button above, and select **Export to a File** from the menu. You can then browse to a desired location available to the machine your XenCenter is running on, give the export file a name, and click **Save**.

   The export operation will take some time.

   **Note**

   Starting with XenServer 5.6 Feature Pack 1, you can automate snapshotting and archiving (exporting) of virtual machines if you have the XenServer Platinum Edition. See the **VM Protection and Recovery** section in the *XenServer 5.6 Feature Pack 1 Administrator’s Guide* for details.

4. Once the Synchronizer export is complete, back up the exported appliance Snapshots remotely as you would back up the VM images.

To restore your environment after a disaster, first restore the XenServer pool where the Synchronizer will reside. Next, restore the shared storage for the VM images. Finally import the backed-up appliance into the XenServer pool and start it. Assuming the environment has been restored to the same state as it was in before the failure, the information in the Synchronizer database should properly point to the VM images and your Synchronizer installation should be up and functioning again.
Chapter 6. Advanced Synchronizer Features

6.1. VM Image Modes

XenClient VMs can be uploaded to a Synchronizer server to create a library of VM images that can be deployed to XenClient users.

A XenClient VM image stored on a Synchronizer server exists in one of the following managed modes:

- **Static VM Image Mode**

  A traditional image of the entire VM stored as a single VHD file. You can make changes to a VM based on this image (for example, installing software or updating the operation system) without affecting other users, and your changes remain when you reboot the device. With this type of VM Image, initial deployment of the image is made with Synchronizer and ongoing updates can be made in the traditional manner using existing Windows distribution tools.

- **Static VM Image Mode with User Profile only backed up**

  The user profile of the VM alone is uploaded to the Synchronizer as a separate VHD from the rest of the system. You can make changes to a VM based on this image (for example, installing software or updating the operation system) without affecting other users, and your changes remain when you reboot the device. With this type of VM Image, initial deployment of the image is made with Synchronizer, and the user profile is thereafter backed up to the Synchronizer. Ongoing operating system and application updates can be made in the traditional manner using existing Windows distribution tools.

- **Dynamic VM Image Mode**

  The user profile of the VM is stored as a separate VHD from the rest of the system. You can make changes to a VM based on this image without affecting other users, but only changes made in the user profile remain when you reboot the device; the operating system and applications revert to the state they were stored at when the image was last saved. With this type of VM Image, deployment and ongoing image updates are made with Synchronizer. Existing Windows distribution tools are not useable with these images.

The mode is chosen when you first upload the VM to a Synchronizer.

To Author a VM in Static VM Image Mode:

1. Shut down the VM that you want to use as a template for the Dynamic VM Image Mode VM.

2. Hover your mouse over the VM icon and click **Details** to open the VM details window.

3. Click **Upload VM** near the top right side of the VM details box. An **Upload to Synchronizer** dialog box appears.

4. Enter a VM Image Name and a Description for the VM.

5. Select the Static radio button and leave the **Allow backup of user profile only** checkbox unchecked.

6. Click **Finish**.
To Author a VM in Static VM Image Mode with User Profile only backed up:

Note

Only Synchronizer users with Admin rights can upload VMs to Synchronizer.

1. Shut down the VM that you want to use as a template for the Dynamic VM Image Mode VM.

Note

The VM must not already be registered with Synchronizer.

2. Hover your mouse over the VM icon and click Details to open the VM details window.

3. Click Upload VM near the top right side of the VM details box. An Upload to Synchronizer dialog box appears.

4. Enter a VM Image Name and a Description for the VM.

5. Select the Static radio button and check the Allow backup of user profile only checkbox.

6. Click Finish.

To Author a VM in Dynamic VM Image Mode:

1. On a XenClient device, ensure that you are connected to Synchronizer as a user with Admin rights.

2. Shut down the VM that you want to use as a template for the Dynamic VM Image Mode VM.

Note

The VM must not already be registered with Synchronizer.

3. Hover your mouse over the VM icon and click Details to open the VM details window.

4. Click Upload VM.

5. Enter a name and description for the VM, and select Dynamic.

6. Click Finish. The VM is uploaded to Synchronizer in Dynamic VM Image Mode.

7. Once the VM is uploaded, you need to create a second version of the VM before assigning it to users.

When a VM based on a newly-created (version 1) Dynamic VM Image Mode is first started, VM to users, its operating system detects the new disks and automatically installs new driver software, which requires a reboot to finish. Because this driver software cannot persist on reboot for a user unless he has Admin rights, if you were to assign the freshly-created VM to users, their VM would need to reboot again each time they restarted it. To avoid this, you need to create a second version of the Dynamic VM Image Mode VM to assign to users.

Note

Disable 3D graphics in the policy when assigning Dynamic VM Image Mode VMs. If 3D graphics is enabled, the physical GPU will be visible to the VM. If the VM image was authored on a machine with a different GPU, then Windows won’t have the driver for the host GPU installed. As a result, Windows will install the driver for the new GPU and prompt for a reboot. After reboot, the system disk will be wiped and the process will repeat.

Similar to the GPU, XenClient passes the optical drive directly through to the VM, which also results in drivers being installed (users will see a notification in the systray when the install completes), but does not prompt for a reboot.

8. If Save changes for reboots is not set to Enabled, click Edit and enable it, then Click Save.

9. Start the VM. When the VM has started, the required drivers install automatically.
10. Reboot the VM to complete the proper installation of the required drivers.

11. Before shutting down the VM and publishing the next version, you should apply all the current Windows updates, rebooting again if necessary. Then, turn off automatic updating for Windows if it is not already disabled. You probably would also want to configure the Windows Firewall at this time.

   Any applications you want the image to have will also need to be installed. Consider that some of the applications will have their own settings for automatic updating that will be an annoyance for users of the image if you leave them enabled.

12. When the VM is fully prepared, shut down the VM.

13. Hover your mouse over the VM icon and click Details to open the VM details window.

14. Click Upload VM.

15. From the Operation pulldown, select Upload new version of current VM, then click Finish.

16. Once the VM is uploaded, this version is ready to assign to users.

   **Note**
   The user must manually join an AD domain if required after downloading a Dynamic VM Image Mode VM.

When the upload is complete, you can assign this VM to users just like any other VM. However, when the user boots the VM, a copy of the VM VHD file is created, which is used as the file system for that user session. Any changes that the user makes in their user folders are preserved, but when the machine is rebooted, any applications installed and the operating system itself will be reverted to the state they had at first boot.

To update a Dynamic VM Image Mode VM, use the following procedure:

**To Update a Dynamic VM Image Mode VM:**

1. In Synchronizer, assign the Dynamic VM Image Mode VM image to your administrator user account.

2. On your XenClient device, in Citrix Receiver for XenClient, create a new VM from Synchronizer, selecting the Dynamic VM Image Mode VM image.

3. Hover your mouse over the VM icon and click Details to open the VM details window.

4. Click the Synchronization tab.

5. From the Operation pulldown, select Upload new version of current VM, then click Finish.

6. Click Save.

7. Start the VM and perform maintenance work. When you are finished, shut down the VM.

8. In Synchronizer, assign the new version of the VM to the relevant user(s), editing the VM policies if desired. The assigned users will be updated with the new version automatically when their XenClient device is restarted or on the schedule defined in the VM policies.
Chapter 7. Troubleshooting

This section describes some solutions for common problems. You may also want to visit the XenClient forums at http://forums.citrix.com/forum.jspa?forumID=1292 for solutions not found in this chapter.

7.1. Changing the Role of a User to Admin Outside of the Synchronizer web interface

Through the Synchronizer web interface it is possible to remove the admin privilege from all users, including the admin user. If this happens to you, there is a command line script make-user-admin that you can run to grant yourself admin user rights.

To Grant a User Admin Rights:

1. In XenCenter, click the Console tab of your Synchronizer VM and select Local Command Shell from the console menu.
2. The local command shell opens. Log in with the root user credentials.
3. Run the following command:
   ```
   make-user-admin
   ```
   The following output is displayed:
   
   This program will grant Synchronizer admin privileges to a user of your choice. Provide the user information at the prompt below:

   1) To specify a local synchronizer user, simply enter the username with no prefix. e.g. 'jane'

   2) To specify a synchronizer user that is linked to an AD user, prefix the username with the NETBIOS name of the domain and a backslash character. e.g. 'MYDOMAIN\jane'

   Enter username (CTRL-C to cancel):

4. Enter the username as prompted and press Enter.
   
   The user role is changed in the Synchronizer database to have admin privileges.

5. Type
   ```
   exit
   ```
   and press Enter to quit the local command shell.

7.2. VM Upload Issues

Use the following procedures to troubleshoot VM upload issues.

To Fix VM Upload Failure due to Insufficient Space:

1. In XenClient, shutdown the Synchronizer VM.
2. Click the Storage tab.
3. Select the `xt-data-vol` virtual disk and click Properties.
4. Click Size and location and increase the disk size.
5. Click OK and restart the Synchronizer VM.

### 7.3. VM Locked Issues

When the lease time of a VM expires and you cannot contact a Synchronizer server, the VM is put into a locked state and cannot be booted. Use the following procedure to unlock a locked VM. This procedure requires the root password set at XenClient installation time.

**To Boot a Locked VM:**

1. In Citrix Receiver for XenClient, press Ctrl + Shift + t to open a control domain console window.
2. Run the `xec-vm` command to get the name of the locked VM:

```
xec-vm
```
3. Run the following two commands:

```
UUID=`xec-vm --name <locked_vm_name> get uuid`
db-write /vm/${UUID}/backend/state/operation READY
```
4. Press Ctrl + q to refresh Citrix Receiver for XenClient.

### 7.4. AD Issues

If you encounter problems linking in AD users and groups, first check that the username is spelled correctly. If you are still unable to link in a user or group, try restarting the AD link services by using the following procedure:

**To Restart the AD Client Services:**

1. In XenCenter, click the Console tab of your Synchronizer VM and select Local Command Shell from the console menu.
2. The local command shell opens. Log in with the root user credentials.
3. Run the command:

```
/sbin/ad-link-restart
```
4. Type `exit` and press Enter to quit the local command shell.

If you are still unable to link in a user or group, check to assure that AD and the Synchronizer server are getting the same time from their clocks. If there is a problem with time synchronization between them, an error message "Unable to create user: Unable to find specified user or group" will be displayed.
Licenses

1. FastCGI

This package was debianized by Davide Puricelli (evo) <apurice@tin.it> on Sat, 3 Jun 2000 22:50:10 +0200.

It was downloaded from http://www.fastcgi.com/

Copyright:

Copyright (c) 1995-1996 Open Market, Inc.

Authors:

- Patches for Apache-1.1 provided by Ralf S. Engelschall <rse@en.muc.de>
- Patches for Linux provided by Scott Langley <langles@vote-smart.org>
- Patches for suexec handling by Brian Grossman <brian@SoftHome.net> and Rob Saccoccio <robs@ipass.net>

1.1. Mod_fastcgi License Terms

This FastCGI application library source and object code (the "Software") and its documentation (the "Documentation") are copyrighted by Open Market, Inc ("Open Market"). The following terms apply to all files associated with the Software and Documentation unless explicitly disclaimed in individual files.

Open Market permits you to use, copy, modify, distribute, and license this Software and the Documentation solely for the purpose of implementing the FastCGI specification defined by Open Market or derivative specifications publicly endorsed by Open Market and promulgated by an open standards organization and for no other purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions.

No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this Software and Documentation may be copyrighted by their authors and need not follow the licensing terms described here, but the modified Software and Documentation must be used for the sole purpose of implementing the FastCGI specification defined by Open Market or derivative specifications publicly endorsed by Open Market and promulgated by an open standards organization and for no other purpose. If modifications to this Software and Documentation have new licensing terms, the new terms must protect Open Market’s proprietary rights in the Software and Documentation to the same extent as these licensing terms and must be clearly indicated on the first page of each file where they apply.

Open Market shall retain all right, title and interest in and to the Software and Documentation, including without limitation all patent, copyright, trade secret and other proprietary rights.

OPEN MARKET MAKES NO EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE SOFTWARE OR THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL OPEN MARKET BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY DAMAGES ARISING FROM OR RELATING TO THIS SOFTWARE OR THE DOCUMENTATION, INCLUDING, WITHOUT LIMITATION, ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OR SIMILAR DAMAGES, INCLUDING LOST PROFITS OR LOST DATA, EVEN IF OPEN MARKET HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS". OPEN MARKET HAS NO LIABILITY IN CONTRACT, TORT, NEGLIGENCE OR OTHERWISE ARISING OUT OF THIS SOFTWARE OR THE DOCUMENTATION.
Index

Symbols
XenClient
  devices, 1
  VM images, 1

A
Active Directory (AD), 1
AD users and groups, 18
Administering Synchronizer, 14
Assignments
  assigning VM images, 21
  editing, 23
  revoking, 24
Authoring VM images, 4, 23, 29

B
Backing up Synchronizer deployment, 28
Backing up VM images, 3

C
Changing admin user password for the web interface, 13
Changing admission control settings for Synchronizer VM, 12
Changing default port for web interface, 13
Changing root user password, 13
Changing Synchronizer timezone, 11
Changing Synchronizer VM properties, 8
Configuration
  DNS server settings, 12
  Management network interface, 11
  Network and firewall, 5
Console, 11
Copy-on-write (CoW), 2

D
Devices
  definition, 1
  deleting, 24
  filtering, 24
  marking as lost, 24
DNS server settings for Synchronizer, 12
Dynamic VM Image Mode, 2

E
Enabling VM Image transfer over HTTP, 26

I
Image repositories, 25
  adding, 25

J
Importing Synchronizer xva, 7
Installation, 7

K
Joining the Synchronizer to an AD domain, 11

L
Linking AD user, 18
Linking AD user group, 19

M
Management network interface, 11

N
Network and firewall configuration, 5
NFS image repository, 25

P
Planning Synchronizer deployment, 5

R
Regenerating CA certificates, 13
Regenerating web server SSL certificates, 13
Registration PINS
  adding, 26
  disabling, 26
  enabling, 26
Resizing Synchronizer VM image storage virtual disk, 8

S
Static VM Image Mode, 2, 2
Synchronizer
  administration, 14
  Changing VM properties, 8
  connecting, 19
  Image repositories, 25
  installing, 7
  Network and firewall configuration, 5
  overview, 1
  Planning deployment, 5
  Resizing VM image storage virtual disk, 8
  VM image repository, 6
  VM images, 2
  web interface overview, 14

T
Timezone, changing, 11
Troubleshooting, 32
  Active Directory issues, 33
  changing role of user to admin outside of Synchronizer web interface, 32
  locked VM issues, 33
VM upload issues, 32

**U**
Upgrading Synchronizer to a new version, 9
Uploading VM to Synchronizer, 29

User groups
- creating, 17
- definition, 1
- deleting, 18

User name
- changing, 19

Users
- adding to a group, 18
- administration, 16
- changing registered user name, 19
- creating, 16
- definition, 1
- deleting, 17
- linking AD group, 19
- linking AD user, 18
- roles, 2

**V**
Virtual Hard Disk (VHD), 2

VM Image Modes
- Dynamic VM Image Mode, 29
- Static VM Image Mode, 29
- Static VM Image Mode with user profile only backed up, 29

VM image repository, 2

VM images
- assigning, 2, 21
- associated VHDs, 20
- creating, 19
- definition, 2
- deleting, 20
- deploying, 4
- Dynamic VM Image Mode, 2
- Static VM Image Mode, 2
- Static VM Image Mode with user profile only backed up, 2
- updating, 31
- uploading, 20

VM Policies, 21
- Advanced, 23
- Allow users(s) to change properties, 22
- Allowing manual updates, 23, 23
- Backup contents, 23
- Enable 3D Graphics, 22
- Enable Autoboot, 22
- Enable Disk Encryption, 21
- Enable Power Control, 22
- Lease expiration, 23

Memory, 21
Network access, 22
Synchronizer, 23
Update schedule, 23
USB devices, 22

VMs
- authoring in Dynamic VM Image Mode, 30
- authoring in Static VM Image Mode, 29
- authoring in Static VM Image Mode with user profile only backed up, 30
- Image modes, 29
- Uploading image to Synchronizer, 29

**W**
Web interface, 14

**X**
Xen Virtual Appliance (XVA), 7
XenCenter, 6, 7, 11
XenServer, 6, 7, 28
Citrix Worldwide

Worldwide headquarters
Citrix Systems, Inc.
851 West Cypress Creek Road
Fort Lauderdale, FL 33309
USA
T +1 800 393 1888
T +1 954 267 3000

Regional headquarters

Americas
Citrix Silicon Valley
4988 Great America Parkway
Santa Clara, CA 95054
USA
T +1 408 790 8000

Europe
Citrix Systems International GmbH
Rheinweg 9
8200 Schaffhausen
Switzerland
T +41 52 635 7700

Asia Pacific
Citrix Systems Hong Kong Ltd.
Suite 3201, 32nd Floor
One International Finance Centre
1 Harbour View Street
Central
Hong Kong
T +852 2100 5000

Citrix Online division
5385 Hollister Avenue
Santa Barbara, CA 93111
USA
T +1 805 690 6400

http://www.citrix.com

About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) is a leading provider of virtual computing solutions that help companies deliver IT as an on-demand service. Founded in 1989, Citrix combines virtualization, networking, and cloud computing technologies into a full portfolio of products that enable virtual workstyles for users and virtual datacenters for IT. More than 230,000 organizations worldwide rely on Citrix to help them build simpler and more cost-effective IT environments. Citrix partners with over 10,000 companies in more than 100 countries. Annual revenue in 2009 was $1.61 billion.

©2011 Citrix Systems, Inc. All rights reserved. Citrix®, Citrix XenClient™, Citrix XenServer™ are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. Microsoft® and Windows® are registered trademarks of Microsoft Corporation in the United States and/or other countries. UNIX® is a registered trademark of The Open Group in the United States and other countries. All other trademarks and registered trademarks are property of their respective owners.