# Contents

1. **Introduction** ........................................................................................................... 3  
   1.1 How to use this Guide .......................................................................................... 3  
   1.2 Before You Start ................................................................................................. 4  
      1.2.1 About the Acano virtualized solution ....................................................... 4  
      1.2.2 Host requirements for the Acano virtualized solution ............................. 4  
      1.2.3 MMP differences in a virtualized deployment .......................................... 5  

2. **Installation** ........................................................................................................... 6  
   2.1 VMWare ............................................................................................................... 6  
   2.2 Hyper-V ............................................................................................................. 7  

3. **Configuration** ...................................................................................................... 8  
   3.1 Creating your own Administrator Account ...................................................... 8  
   3.2 Setting up the Network Interface for IPv4 ....................................................... 8  
   3.3 Adding Additional Network Interface(s) ......................................................... 9  
   3.4 Creating the Web Admin Interface Certificate .............................................. 10  
   3.5 Configuring the Web Admin Interface for HTTPS Access ............................ 13  

4. **Getting and Entering a License File** ................................................................... 15
1 Introduction

The Acano virtualized solution is run on either 2.1 VMWare ESXi or 2.1 Microsoft Hyper-V.

1.1 How to use this Guide

Follow this guide to install the Acano solution as a virtual deployment running the Acano solution Release 1.6 software. Then see one of the Deployment Guides for other set up and configuration information (depending on whether you are setting up a resilient solution or not). Note that this guide is written for experienced Hyper-V and VMWare administrators.

Figure 1: Acano solution installation and deployment documentation

In addition to this guide, the material shown in the figure below can be found at the Acano Documentation & software page. If you need any technical assistance with the configuration, or you want to report a suspected bug, email support@acano.com.
1.2 Before You Start

1.2.1 About the Acano virtualized solution

The Acano virtualized solution for VMWare is provided as an .ovf file. This is a template that sets up a new VM with a single network interface, 16GB RAM and a virtual disk containing the Acano solution application.

A VHD disk image is also provided for Microsoft Hyper-V users.

After installation a fully functioning Acano solution is available:

- For example, users, routing and dial plans work in exactly the same way as the Acano Server deployment and therefore coSpaces, contacts and calls work in the same way also.
- Upgrading between VM versions follows the normal procedure in the release notes.
- An Acano virtualized solution can be run as a complete solution or as a Core or Edge deployment only (see the Deployment Guides for details). The same .ovf file or disk image is therefore used to install all these options.

Note: Although the functionality of an Acano Server deployment and a virtualized deployment are identical for users, the two deployments are not interchangeable. For example, it is not possible to create a backup from one deployment and roll it back on the other. There are other minor differences when using the MMP – see below.

1.2.2 Host requirements for the Acano virtualized solution

<table>
<thead>
<tr>
<th></th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server manufacturer</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>Processor type</td>
<td>Intel Nehalem microarchitecture</td>
<td>Intel Xeon 2600 v2 or newer</td>
</tr>
<tr>
<td></td>
<td>AMD Bulldozer microarchitecture</td>
<td></td>
</tr>
<tr>
<td>Processor frequency</td>
<td>2.0GHz</td>
<td>2.5Ghz</td>
</tr>
<tr>
<td>RAM</td>
<td>1GB per core</td>
<td>1GB per core</td>
</tr>
<tr>
<td>Storage</td>
<td>100GB</td>
<td>100GB</td>
</tr>
<tr>
<td>Hypervisor</td>
<td>VMWare ESXi 5.0 Update 3</td>
<td>VMWare ESXi 5.1 Update 2, 5.5 Update 1</td>
</tr>
<tr>
<td></td>
<td>Hyper-V 2012</td>
<td>Hyper-V 2012, 2012 R2</td>
</tr>
</tbody>
</table>
Recommended Core VM configurations:

<table>
<thead>
<tr>
<th>720p30 call legs</th>
<th>CPU configuration</th>
<th>RAM configuration</th>
<th>Example systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>Dual Intel E5-2680v2</td>
<td>32 GB (8x4GB)</td>
<td>Cisco UCS C220 M3 Dell R620 HP DL380p Gen8</td>
</tr>
<tr>
<td>40</td>
<td>Dual Intel E5-2650v2</td>
<td>32 GB (8x4GB)</td>
<td>Cisco UCS C220 M3 Dell R620 HP DL380p Gen8</td>
</tr>
<tr>
<td>25</td>
<td>Single Intel E5-2680v2</td>
<td>16 GB (4x4GB)</td>
<td>Cisco UCS C220 M3 Dell R620 HP DL380p Gen8</td>
</tr>
<tr>
<td>15</td>
<td>Single Intel E5-2640v2</td>
<td>8 GB (4x2GB)</td>
<td>Cisco UCS C220 M3 Dell R620 HP DL380p Gen8</td>
</tr>
</tbody>
</table>

In addition:

- All memory channels should be populated
- Out-of-bond-management systems configured to share a network port must be disabled
- Where available, hyperthreading should be enabled on the host
- The host must be dedicated to the Acano VM
- An activation key for your Acano virtualized solution is required. Without this activation key the Acano solution’s Call Bridge will only support a limited number of simultaneous calls. To obtain the activation key, you need the MAC address of your virtual server. Therefore instructions are provided in this guide at the appropriate time

1.2.3 MMP differences in a virtualized deployment

The MMP Command Reference details the full set of MMP commands in both deployment models. A summary of the differences is:

- There is a shutdown command that must be used to shutdown the VM rather than using vSphere power button
- The concept of a serial number does not apply to a virtualized solution; therefore the MMP serial command will not return a serial number
- Similarly the health command is not available in the virtualized deployment
- Other commands such as dns no longer require an interface, or cannot take “mmp” as the interface
2 Installation

Follow the appropriate section depending on which type of VM host you are using.

2.1 VMWare

Note: For every release of the Acano virtual solution, there will be an ovf folder for a new deployment, and an upgrade image (.img) for upgrading to the latest release. For a new installation follow this section; for an upgrade follow the release notes.

1. Obtain and download all files in the ovf folder from the Acano FTP site.
2. In the vSphere Client go to File > Deploy ovf Template.
3. Browse to the .ovf file and select it.
4. Follow the wizard instructions. The settings that must be selected are:
   a. Name the new VM.
   b. Select a Virtual disk storage folder to hold the VM disk.
   c. Ensure Power On After Deployment is not selected.

   Note: Depending on how your virtual host is set up, some of the wizard settings may not be displayed or may not be selectable.

5. When you see the message Completed successfully, click Close.
   The new Acano virtual machine is listed in the vSphere client.
6. Select the Acano virtual machine
7. From the Getting Started tab, select Edit Virtual Machine settings and CPUs.
   a. Edit VM settings and choose CPUs. Set Number of Virtual Sockets to 1.
   b. Set Number of Cores per Socket to one of the following:
      - On a dual processor host with hyperthreading, set Number of Cores per Socket to the number of logical cores minus 2.
      - On a dual processor host without hyperthreading, set Number of Cores per Socket to the number of logical cores minus 1.
      - On a single processor host, set Number of Cores per Socket to the number of logical cores.

     The number of logical cores can be found in the vSphere Client, ESXi Summary page. For the 40 call leg configuration above (Dual Intel E5-2650v2) the value will be 30.
8. Click Power on.
9. Open the vSphere Console tab.
   When the process is complete, you see the acano login prompt.
10. Log in with the user name “admin” and the password “admin”. You will be asked to change the admin password.
    You are now logged into the MMP. Go on to Network Configuration.
2.2 Hyper-V

Note: For every release of the Acano virtual solution, there will be a virtual hard drive image (.vhd) for new deployments and an upgrade image (.img) for upgrading existing deployment to the latest release. For a new Hyper-V deployment follow this section, for upgrade see the Release notes.

1. Download the .vhd file from the Acano FTP site and upload it to your Hyper-V datastore.
2. In Hyper-V Manager, select the host you want to home this VM on, then from the Action pane/ menu, create a new VM using New > Virtual Machine.
3. Follow the wizard instructions. The settings that must be selected are:
   a. Name the new VM.
   b. Select Use an Existing Virtual Hard Disk, and browse to the .vhd file above.
4. Click Finish.
   The new Acano virtual machine is created and listed.
5. Select the Acano virtual machine, and configure its Settings from the Action pane/ menu.
6. Select Processor to configure it.
   a. Set the Number of Virtual Processors to one of the following:
      • On a dual processor host with hyperthreading, set Number of Cores per Socket to the number of logical cores minus 2.
      • On a dual processor host without hyperthreading, set Number of Cores per Socket to the number of logical cores minus 1.
      • On a single processor host, set Number of Cores per Socket to the number of logical cores.
      For the 40-call leg configuration above (Dual Intel E5-2650v2) the value will be 30.
   b. In Resource Control, configure:
      i. Virtual machine reserve (percentage) to 100.
      ii. Virtual machine limit (percentage) to 100.
      iii. Relative weight to 100.
7. Select Memory and ensure that startup RAM is configured to the recommended requirements above.
8. Click Apply and Start the Acano Virtual Machine.
9. Select the Acano virtual machine and click Connect.
   When the process is complete, you see the acano login prompt.
10. Log in with the user name “admin” and the password “admin”. You will be asked to change the admin password.

You are now logged into the MMP. Go on to Network Configuration below.
3 Configuration

3.1 Creating your own Administrator Account

For security, create at least one new admin account with the following MMP command (see the MMP Command Reference for details).

user add <name> admin

You will be prompted for a password which you must enter twice. Log in with the new account - you will be asked to change your password.

Note: You must have at least two admin level accounts at all times: then if you lose the password for one account you can still log in with the other one and reset the lost password. We recommend that you create two new accounts and then delete the default “admin” account; because the username “admin” is not very secure.

Note: From R1.1 any MMP user account at the admin level can also be used to log into the Web Admin Interface. There is no separate Web Admin Interface command for creating users any longer.

3.2 Setting up the Network Interface for IPv4

Note: Although these steps are for IPv4, there are equivalent commands for IPv6. See the MMP Reference for a full description.

In the Acano solution virtual deployment, there is only one network interface initially but up to 4 are supported (see the next section). The initial interface is “a”, equivalent to interface A in the Acano Server deployment. (The MMP runs on this interface in the virtual deployment.)

1. Configure the Network Interface speed using the following MMP commands.

   To set network interface speed, duplex and auto-negotiation parameters use the iface command e.g. to display the current configuration on the Admin interface, in the MMP type:

   iface a

   To set the interface to 1GE, full duplex type:

   iface a 1000 full

   and to switch auto negotiation on or off, type:

   iface a autoneg <on|off>

   We recommend that the network interface is set to auto negotiation unless you have a specific reason not to.

2. The “a” interface is initially configured to use DHCP. To view or reconfigure the IP settings:

   a. Go on to step b if you are using static IP addresses.

      To find out the dhcp configured settings, type:

      ipv4 a
Go on to step 3.

b. Configure to use static IP addresses (skip this step if you are using DHCP)

Use the `ipv4 add` command to add a static IP address to the interface with a specified subnet mask and default gateway. For example, to add address 10.1.2.4 with prefix length 16 (netmask 255.255.0.0) with gateway 10.1.1.1 to the interface, type:

```
ipv4 a add 10.1.2.4/16 10.1.1.1
```

To remove the IPv4 address, type:

```
ipv4 a del
```

3. Set DNS Configuration

a. To output the dns configuration, type:

```
dns
```

b. To set the application DNS server type:

```
dns add forwardzone <domain name> <server IP>
```

Note: A forward zone is a pair consisting of a domain name and a server address: if a name is below the given domain name in the DNS hierarchy, then the DNS resolver can query the given server. Multiple servers can be given for any particular domain name to provide load balancing and fail over. A common usage will be to specify "." as the domain name i.e. the root of the DNS hierarchy which matches every domain name, i.e. is the server is on IP 10.1.1.1

```
dns add forwardzone . 10.1.1.33
```

c. If you need to delete a DNS entry use:

```
dns del forwardzone <domain name> <server IP>
```

for example:

```
dns del forwardzone . 10.1.1.33
```

### 3.3 Adding Additional Network Interface(s)

The Acano virtualized solution supports up to four interfaces (a, b, c and d).

If required, you can add a second network interface on VMWare.

1. In the vSphere Client, open the Getting Started tab.
2. Select Edit Virtual Machine Settings.
3. Add an Ethernet Adapter with type VMXNET3 in the usual way.

To do the same on Hyper-V.

1. In the Hyper-V Manager, select the Acano Virtual machine, and select Settings
2. Select Add Hardware.
3. Add an Ethernet Adapter with type Network Adapter in the usual way.
3.4 Creating the Web Admin Interface Certificate

The Web Admin is only accessible through HTTPS, you need to create a security certificate to install onto the Acano solution so you can enable the Web Admin Interface and be able to log into it.

The information in step 1 below assumes that you trust Acano to meet requirements for the generation of a private key. If you prefer, you can generate the private key and the certificate externally using a public Certificate Authority (CA), and then load the externally generated key/certificate pair onto the MMP of the Acano Server using SFTP. Go to Configuring the Web Admin Interface for HTTPS Access.

Note: if testing your Acano solution in a lab environment, you can generate a key and a self-signed certificate on the Acano Server. Self-signed certificates are not recommended for use in real deployments (see http://en.wikipedia.org/wiki/Self-signed_certificate). To create a self-signed certificate and private key, log in to the MMP and use the command:

```
pki selfsigned <key/cert basename>
```

where `<key/cert basename>` identifies the key and certificate which will be generated e.g. "pki selfsigned webserver" creates webserver.key and webserver.crt (which is self-signed).

Then go to Configuring the Web Admin Interface for HTTPS Access.

1. Follow this step if you trust that Acano meets the requirements for generation of private key material. This step explains how to generate a private key and the associated Certificate Signing Request with the MMP `pki csr` command, export them for signing by a CA, and then copying the signed certificate file on to the Acano Server.
   a. Log in to the MMP and generate the private key and certificate signing request:

```
pki csr <key/cert basename> [=<attribute>:<value>]
```

where:

- `<key/cert basename>` is a string identifying the new key and CSR (e.g. "xmpp" results in "xmpp.key" and "xmpp.csr" files)

and the allowed but optional attributes are as follows and must be separated by a colon:

- **CN**: the commonName which should be on the certificate. Use the FQDN defined in DNS A record as the Common Name. Failure to do this will result in browser certificate errors.
- **OU**: is Organizational Unit
- **O**: Organization
- **L**: Locality
- **ST**: State
- **C**: Country
- **emailAddress**

Use quotes for values that are more than one word long, for example:

```
pki csr example CN:example.com "OU:Accounts UK" "O:My Company"
```

b. Send the CSR to one of the following:

- To a Certificate Authority (CA), such as Verisign who will verify the identity of the requestor and issue a signed certificate.
• To a local or organizational Certificate Authority, such as an Active Directory server with the Active Directory Certificate Services Role installed.
  
  i. Transfer the file to the CA.
  
  ii. Issue the following command in the command line management shell on the CA server replacing the path and CSR name with your information:

  `certreq -submit -attrib "CertificateTemplate:WebServer" C:\Users\Administrator\Desktop\certcsr.pem`

  iii. After entering the command, a CA selection list is displayed similar to that below. Select the correct CA and click OK.

  ![Certification Authority List](image)

  iv. Do one of the following:

  • If your Windows account has permissions to issue certificates, you are prompted to save the resulting certificate, for example as webserver.pem. Go on to step c below.
  
  • If you do not see a prompt to issue the resulting certificate, but instead see a message on the command prompt window that the 'Certificate request is pending: taken under submission', and listing the Request ID as follows. Note the RequestID and then follow the steps below before going on to step c below.

  `C:\Users\Administrator>certreq -submit -attrib "CertificateTemplate:WebServer" C:\Users\Administrator\Desktop\demokitcsr.pem
Active Directory Enrollment Policy
<0B05DBB7-591F-4C77-AFEC-39BE47B0F7B5>
ldap:
RequestID: 8
RequestID: "8"
Certificate request is pending: Taken Under Submission (0)`

  v. Using the Server Manager page on the CA, locate the Pending Requests folder under the CA Role.
vi. Right-click on the pending request that matches the Request ID given in CMD window and select All Tasks > Issue.

![Server Manager](image1.png)

vii. The resulting signed certificate is in the Issued Certificates folder. Double-click on the certificate to open it and open the Details tab (see right).

![Certificate Details](image2.png)

viii. Click Copy to File which starts the Certificate Export Wizard.

ix. Select Base-64 encoded X.509 (.CER) and click Next.

x. Browse to the location in which to save the certificate, enter a name such as cacert and click Next.
xi. Rename the resulting certificate to `cacert.pem`.

   c. Transfer both the certificate (e.g. `webserver.crt`) to the MMP of the Acano Server using SFTP.

   **CAUTION**: If you are using a CA with the Web Enrolment feature installed, you may copy the CSR text including the BEGIN CERTIFICATE REQUEST and END CERTIFICATE REQUEST lines to submit. After the certificate has been issued, copy only the certificate and not the Certificate Chain. Be sure to include all text including the BEGIN CERTIFICATE and END CERTIFICATE lines and paste into a text file. Then save the file as your certificate with a .pem, .cer or .crt extension.

### 3.5 Configuring the Web Admin Interface for HTTPS Access

Note: The deployment automatically sets up the Web Admin Interface to use interface A.

2. Establish a SSH connection again to the MMP and sign in.

3. If you want to use a different interface, enter the following commands to configure the Web Admin Interface:
   ```
   webadmin certs webserver.key webserver.crt
   webadmin listen a 443
   webadmin restart
   webadmin enable
   ```

   Note: Be sure to use the same names as the certificates you uploaded.
4. Test that you can access the Web Admin Interface, i.e. enter your equivalent of https://acanoserver.mycompany.com (or the IP address) in your browser and login using the MMP user account you created earlier.

You see the following banner “This Acano Call Bridge …” showing you that the virtual server has not been activated yet. After you upload a license file (in the next section), the banner is removed.

![Acano Call Bridge Banner](image)

Note: Any two interfaces of Acano solution must not be put into same subnet. The only exception is that the ADMIN interface of a physical Acano Server can be on the same subnet as one of the other interfaces (A to D)—and is probably a common deployment.
4 Getting and Entering a License File

The Acano solution virtualized deployment requires a license file; otherwise you will only be able to create a few calls simultaneously. The license file is for the MAC address of your virtual server. Follow the steps below.

1. Log in to the MMP and enter the following command to find the MAC address:
   \texttt{ipv4 a}

2. Email the MAC address to support@acano.com and ask for a license file.

3. After a license file is returned by email, transfer the license file to the MMP using SFTP. The file must be named “acano.lic”

4. To apply the license you need to restart the Call Bridge. However, you must configure the Call Bridge certificates and a port on which the Call Bridge listens before you can do this. These steps are part of the Acano solution configuration and described in both of the Acano solution deployment guides.

   When the license file has been applied and you sign into the Web Admin Interface, the banner should not appear.

---

Note: You are now ready to configure the Acano virtualized solution. See:

- the Acano solution Deployment Guide if you are deploying on a single host or a split Core/Edge deployment
- the Acano solution Scalability & Resilience Guide if you are deploying multiple single, Core or Edge servers that you will cluster

Remember to use the \texttt{shutdown} command rather than using vSphere power button when you want to shut down.