This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Business Edition Premise Provider's Guide

On-site installation

12/19/2025

On-site installation

> **Important**
> The following steps must occur *at the customer site*, as they require specific customer network information.

<multistep> Required licenses=

> **Important**
> You require the following licenses before installing Business Edition Premise. If you do not have all required licenses, do not proceed with the installation steps.

- Three Windows Server 2008 license keys for activating Windows when starting each VM.
- One Genesys software license for either 100 or 300 agents.
- One Business Objects Enterprise (BOE) version 3.1 license key.
- One Microsoft SQL Server 2008 R2 64-bit license with 50 client access.

|-| Provision the network= Provision the network to include:

- Five IP addresses within a single subnet and available on the Windows domain running DNS/DHCP services for the Virtual Machines (VMs); you also need to assign five hostnames for the VMs for entry into a DNS server
- One IP address within a management control subnet for Dell iDRAC configuration, to enable hardware alarming via email (the address must be able to access the customer corporate email server)
- One IP address within the same subnet and available on a Windows domain running DNS/DHCP services for ESXi 5.1 server.

|-| Set up hardware monitoring= Your Dell server includes an Integrated Dell Remote Access Controller (iDRAC) that monitors the server hardware and can send email notifications to help you avoid the data loss that *will* occur if two drives in the RAID array fail.

> **Warning**
> **Failure to monitor the health of your RAID array can result in loss of data.** Ensure that you set up Dell hardware monitoring with email notification.

To configure the iDRAC to send email notifications:

1. Ensure that you have configured your iDRAC. See the section "iDRAC Settings Utility" in the Dell Owner's Manual for your R720 or R420.
2. Use a browser to log into the Dell iDRAC at `https://IP address/login.html`, where *IP address* is the management interface IP address or DNS entry name. Enter the username and password that you specified when configuring the iDRAC.
3. Navigate to **Alerts > Alerts Filter**. Ensure that *only* **System Health**, **Storage**, **Warning**, and **Critical** are checked. Uncheck the other five items. Click **Apply**.
4. Under **Alerts and Remote System Log Configuration**, check the **Email** box in the heading for *each* of the 8 pages.
5. Select the **SNMP and E-Mail Settings** tab. Under **Destination E-mail Addresses**, add up to four addresses to receive alert emails. Check **State** for each address. Click **Apply**.
6. Under **SMTP (E-Mail) Server Address Settings**, enter the IP address or FQDN/DNS name of the corporate email server (authentication is optional). Click **Apply**.
7. Under **Destination E-mail Addresses**, click **Send** to send an email alert to each of the configured accounts.
8. Verify that each account received the test email.
9. Return to the **Alerts** tab. Enable alerts and click **Apply**.

|-| Configure the server=

1. Configure the external interfaces:
   - Media Gateway/SBC: add network bandwidth and provision the network infrastructure
   - Agent phones: add network bandwidth and provision the network and phones
   - Organization email (if the customer selects the email option): provision the network
   - Organization backend servers (optional): provision the network and security information
     - Organization Network Management System (optional): provision the network and security information
2. For the optional email package, set up an account for the ESJ server to connect with the corporate email server to pick up incoming email.
   - Meet network voice requirements:
     - 50ms between particular endpoints
     - MOS > 4
     - R factor > 70
     - network jitter < 40ms
     - RTP packet loss 0
3. The customer is responsible for the following:
   - Completing a backup of the system after installation
   - Updating Genesys One credentials after installation
   - Installing anti-virus software consistent with corporate guidelines (Genesys does not recommend anti-virus software running on hosts with SIP RTP messaging as it can affect voice quality)

- Enabling security policies/firewall per corporate guidelines
- Installing updates
- Being aware that FTC regulations may require that Outbound Contact Server (OCS) audit logs be stored for up to 24 months. Due to storage limitations, the log zip utility on the Core VM is configured to only retain these logs for a maximum of 60 days. Customers must move these logs to external storage before the 60-day expiration.

|-| Update DHCP and DNS servers for ESXi= Power on the ESXi server (if needed) and retrieve its MAC address (for setup in a DHCP server to assign an IP address and in a DNS server so the host name of the ESXi server can be associated to the assigned IP address when first connected to the network):

1. Open the ESXi console for your ESXi server and go to **<F2> Customize System/View Logs > Configure Management Network > Network Adapters/<D> View Details**. Copy the MAC address.
2. Log into the customer DHCP server. In the Command window, replace the existing MAC address for the ESXi server.
3. Restart the DHCP server.
4. Update the customer DNS server with new host name of the ESXi server and the IP address assigned from the customer pool of addresses and given out by their DHCP server.

|-| Update DHCP and DNS servers for VMs= Before you power on the VMs, retrieve their MAC addresses (from VM properties) to populate the DHCP server and update the DNS server:

1. In the vSphere Client inventory, right-click each virtual machine and select **Edit Settings > Network adapter 1** to view its MAC address. Copy each address.
2. Log into the DHCP server. In the Command window, replace the existing MAC address for each VM.
3. Restart the DHCP server.
4. Update the customer DNS server with the new host names of the VM servers and the IP addresses assigned from the customer pool of addresses and given out by their DHCP server.

|-| Configure NTP to synchronize VMs= Configure an NTP (network time) daemon to synchronize the customer VMs.

1. In the vSphere Client, select the ESXi server, and then select the **Configuration** tab.
2. From the **Software** menu, click **Time Configuration** and select **Properties**.
3. Select **NTP Client Enabled** and then click **Options**. The **NTP Daemon (ntpd) Options** window opens.
4. In the **NTP Daemon Options** window, do the following steps:
   - Under **General**, select **Start and stop with host**.
   - Under **NTP Settings**, add an NTP Server in the customer time zone (the NTP Server website lists available NTP servers) and select **Restart NTP service to apply changes**.
   - Click **OK**.
5. Click **OK** again to close the **Time Configuration** window.

|-| Power on the Core VM=

1. Power on the Core VM (this step must take place before you power on any of the other VMs).
2. In Windows setup, enter the locale and product key, accept the license terms, and change the password. (For localized versions, you must first select a language before proceeding with Windows setup.)
3. Confirm that the dialog for changing the user password at the first login appears. The Windows desktop loads and the tuneup script automatically runs.

|-| Configure the VM using the tuneup script=

1. After the tuneup script launches automatically, enter values when prompted:
   - Host naming scheme:
     - Select 1 to use default host names (`g1-core-p, g1-ui-p, g1-db-p, g1-aux-p, g1-gvp-p`). Use this option for environments that you do not plan to extend and if the default naming convention suits your needs.
     - Select 2 to use default host names with custom suffixes (such as `g1-core-p-env1`). The script prompts you for the suffix. Use this option if default names with suffixes agree with your host naming convention. **Important:** The suffix can contain no more than 4 characters.
     - Select 3 to use custom names for each host (such as `newyork-core` and `newyork-ui`). The script prompts you for each name, which should identify the role of the host (core, ui, db, aux, or gvp). Use this option if you need to conform to a customer naming convention. **Important:** Each host name can contain no more than 15 characters.
   - Domain configuration (this setting defines how the FQDN of the hosts is presented in Genesys Configuration; Genesys software uses these names when establishing network connections):
     - Select 1 to have the tuneup script use the domain name that it detects automatically.
     - Select 2 (Other domain name) to enter the domain name manually. When prompted, enter the domain name.
     - Select 3 if your environment does not require a domain name.
   - Rename? Yes
   - Reboot? Yes

Important: Ensure that the Core VM fully restarts before you proceed.

To verify that the IP address is correct, run the Windows command `ipconfig/all`. If the host received proper IP configuration from your DHCP Server, the values will match your network settings.

To verify that the server can reach the remote host, ping an external server (such as a server you plan to use for your agent desktops) by running the command `ping` *`remote host name or IP address`*. The remote host must be reachable via ping and the output of the ping command looks similar to this example (note the shortened output and sample IP addresses; ping times may vary):

```
Pinging agent-desktop.domain.com [1.2.3.4] with 32 bytes of data:

Reply from 1.2.3.4: bytes=32 time<1ms TTL=128

Reply from 1.2.3.4: bytes=32 time<1ms TTL=128

Reply from 1.2.3.4: bytes=32 time<1ms TTL=128
```

```
Reply from 1.2.3.4: bytes=32 time<1ms TTL=128

Ping statistics for 1.2.3.4:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

From the remote host you just pinged, open the console window and issue the following command:

`ping` *`Core VM name or IP address`*

The Core VM host must be reachable and the output of ping command must look similar to the example in the previous substep.

> **Tip**
>
> If you enter incorrect information during the tuneup script configuration, Genesys recommends that you redeploy the Core VM and begin the tuneup script configuration again. If you made a snapshot of the Core VM prior to entering any data for the tuneup configuration script, you can revert to that snapshot. This approach can also be applied to the other VMs; however, if you redeploy the Core VM (or revert to a snapshot), you must also redeploy the other VMs.

|-| Apply licenses and configuration changes= **WATCH:** To view a short demonstration of the license

application, click the Genesys icon below:

In the **Initial Configuration Tasks** window in the vSphere client on the Core VM:

1. Set the time zone in the format *Continent/City or Region*. For a list of time zones, see the TZ column in List of tz database time zones.
2. Set up Genesys License Manager by placing the Flex LM license file (acquired earlier) in the **GCTI\ flexlm** folder.

> **Important**
>
> Altering the Windows Operating System Regional settings (other than time zone) may result in a failure when attempting to apply the MS SQL Server 2008 license key at the completion of the BEP installation.

3. To add the Microsoft SQL Server 2008 R2 64-bit license:
   - Go to **Start > All Programs > Microsoft SQL Server 2008 R2 > Configuration Tools > SQL Server Installation Center (64-bit)**
   - Select **Maintenance**.
   - Select **Edition Upgrade**, and click **OK** to begin the setup.
   - Click **Next** through the Setup Support Rules.
   - Enter the Product Key, and click **Next**.
   - Accept the license terms, and click **Next**.
   - Select the Instance, and click **Next**.
   - Click Upgrade.
4. If your environment uses a domain, you can add it by doing the following:
   - Click **Provide computer name and domain**.
   - In the **System Properties** window, click **Change**.
   - In the **Computer Name/Domain Changes** window, select **Domain** and enter the domain name.
   - Click **OK**.
5. Reboot the VM.

|-| Verify the Genesys services=

1. Click **Start**.
2. To verify this step, enter `Services` in the **Search programs and files** dialog box.
3. Select **Services** and locate groups of services with names starting with `Genesys` in the list of local services.
4. Check the status and startup type of these services. All Genesys services are in status *Started*, with startup type *Automatic*.

|-| Enter Configuration Manager details=

1. On the console of the Core VM, click **Start** and select **All programs > Genesys Solutions > Start Configuration Manager**.
2. In the dialog box, enter:
   - User name: `default`
   - Password: `password`
   - Application: `default`
   - Host name: `localhost`
   - Port: 8888

Before proceeding to the next step, ensure that Configuration Manager starts and its main window displays Environment and Resources objects. |-| Configure db, aux, and gvp VMs=

1. Configure the db, aux, and gvp VMs, beginning with the **db** VM (do not configure the **ui** VM until the next step):
   - Power on each VM. In Windows setup, set the locale and the product key, accept the license terms, and change the password. (For localized versions, you must first select a language before proceeding with Windows setup.) To verify, use the same criteria as for the core server.
   - The tuneup script automatically launches. When prompted:
     - Enter the Primary Core Host IP address (do not use the host name).
     - Enter Yes to rename and restart the VM. Ensure that each VM fully restarts before you proceed.
2. Configure the time zone settings:
   - **For DB VM only:** The time zone is configured as part of the tuneup script. Set the time zone for GIM in the format *Continent/City or Region*. For a list of time zones, see the TZ column in List of tz database time zones.
   - **For all VMs:** In the **Initial Configuration Tasks** window, click **Set time zone**. Configure the time zone in the format *Continent/City or Region*. For a list of time zones, see the TZ column in List of tz database time zones.
3. If your environment uses a domain, select **Provide computer name and domain > Change** and enter the domain name.
4. In the Windows security window, enter the administrator ID and password.
5. Restart the VM.

|-| Configure ui VM=

1. Power on the **ui** VM. In Windows setup, set the locale and the product key, accept the license terms, and change the password. To verify, use the same criteria as for the core server.
2. The UI tuneup script automatically launches. When prompted:
   - Enter the Primary Core Host IP address.
   - Enter Yes to rename and restart the VM.
3. The **tuneup_boe.bat** script launches automatically. Enter the BOE license code (which Genesys does not provide).
4. Wait for the BOE tuneup script to finish and close (the script can take 30 minutes or more to complete).
5. In the **Initial Configuration Tasks** window, set the time zone in the format *Continent/City or Region*. For a list of time zones, see the TZ column in List of tz database time zones.
6. If your environment uses a domain, select **Provide computer name and domain > Change** and enter the domain name.
7. In the Windows security window, enter the administrator ID and password.
8. Restart the VM.

|-| Configure BOE for GI2=

> Important

> This step is only required for Business Edition Premise version 8.1.100.20. If you have a later version, you can skip this step.

1. To configure BOE for GI2, open the ui VM after the ui VM fully restarts for the second time.
2. Open Business Objects Universe Designer and log in with these credentials:
   - System: *`your ui host name`*`:6400`
   - User: `administrator`
   - Password: `G3n35y5`
   - Authentication: `Enterprise`
3. Create a connection, **MSSQL 2008 > JDBC**, that uses these values:
   - Connection name: `GI2-JDBC`
   - Username: `sa`
   - Password: `G3n35y5!`
   - Server host: *`your db host name`*`:1433`
   - Database: `gim_etl`
4. Import Universe from the folder **Interactive Insights > 8.1.1**.
5. In the Universe Parameters window, specify the new GI2-JDBC connection.
6. Export the Universe.

|-| Backup the VMs= Genesys recommends that you backup the VMs by exporting them to an external location or device.

1. Open the vSphere Client.
2. For each VM, do the following:
   - Power off the VM.
   - In the vSphere client, highlight the target VM and select **File** > **Export** > **Export OVF Template**.
   - For the file format, select `Single File (OVA)`.
   - Specify the output file name and location.
   - Export the file.

</multistep>

Next: Deploy the routing applications.