imprivata®

Product Documentation

Virtual Appliance Guide

Imprivata OneSign

Table of Contents

About this Guide

NOTE:
Beginning with 24.1, Imprivata OneSign and Imprivata Confirm ID have been renamed to Imprivata Enterprise Access Management.

Some interfaces in the Imprivata Admin Console, Imprivata Appliance Console, and documentation may retain the older Imprivata OneSign and Imprivata Confirm ID product names.

You can host and manage Imprivata virtual appliances using VMware and Microsoft Hyper-V virtualization software. Imprivata virtual appliances hosted on these platforms are formatted using the industry-standard Open Virtualization Format (OVF).

You can also host and manage Imprivata virtual appliances on Nutanix and Microsoft Azure.

This guide is applicable to:

- All maintained versions of Imprivata Enterprise Access Management (formerly Imprivata OneSign and Imprivata Confirm ID).
- G4 (fourth generation) and G3 (third generation) virtual appliances.

Appliance System Requirements and Guidance

Review the following before you begin.

> **NOTE:**
> To deploy an Imprivata G4 (fourth generation) appliance on Microsoft Azure, skip this topic and instead see Deploy G4 Appliances on Azure for appliance guidance.
>
> To deploy an Imprivata G3 (third generation) appliance on Microsoft Azure, skip this topic and instead see Deploy a G3 Appliance on Azure for appliance guidance.

System Requirements

System requirements vary by the appliance generation. For appliance system requirements, see the *Supported Components* in the Imprivata Environment Reference.

The release introduction history of supported appliances is:

- Imprivata OneSign 7.11 and later releases require G4 (fourth generation) appliances.
- Imprivata OneSign 7.10 introduced the General Availability (GA) release of the G4 appliance to all customers, including for G3 or G2 enterprise migrations to G4.

  Imprivata OneSign 7.10, 7.9, and 7.8 supported either G3 or G4 appliances, but not both G3 and G4 appliances on the same enterprise.
- Imprivata OneSign 7.8 introduced the Controlled Availability (CA) release of the G4 appliance to select customers or on request.
- All maintained releases of Imprivata OneSign, up to 7.10, required G3 appliances.

Unsupported

The following virtual appliance configurations are not supported:

- The cloning of appliance virtual machines is not supported.
- Infrastructure-level snapshots of appliance virtual machines are not supported.

Considerations for Storage Level RAID Protection

While most customers will want to use RAID 5, Imprivata recommends RAID 1+0 or RAID 10 for any appliances that are experiencing a challenge with throughput, especially G4 database appliances.

Number of Appliances to Deploy

> **NOTE:**
> For specific questions about enterprise configuration or additional guidance, contact Imprivata services or support.

G4 Appliances

The number of appliances appropriate for a G4 enterprise depends on many factors, including user counts, authentication methods, and other issues.

First, consider the two G4 appliance types and the limits on their numbers per enterprise:

- Database appliances host the databases, perform database replication, service endpoint agent requests, and contain all audit data.
  - Enforced maximum of two database appliances per enterprise.
  - The first two appliances configured are always database appliances.
- Service appliances exclusively service endpoint agent requests.
  - Recommended maximum of four service appliances per enterprise.
- Recommended maximum of six total appliances per enterprise. Adding more appliances beyond six typically does not yield performance improvements.
- No audit appliances.

For G4 appliances, Imprivata recommends three standard deployment options: two-, four-, and six-appliance enterprises. The two-appliance enterprise offers three different CPU and RAM configuration options for scale.

Recommended Options	2 Appliance Enterprise			4 Appliance Enterprise	6 Appliance Enterprise
Database appliances	2	2	2	2	2
CPUs per appliance	4	8	8	8	8
RAM (GB) per appliance	8	16	32	16	16
Service appliances				2	4
CPUs per appliance				2	2
RAM (GB) per appliance				8	8
Total appliance CPUs in enterprise	**8**	**16**	**16**	**20**	**24**
Total appliance RAM in enterprise	16	32	64	48	64

Recommended Options	2 Appliance Enterprise			4 Appliance Enterprise	6 Appliance Enterprise
Number of user sessions supported (in optimal conditions)	22,000 to 28,000	28,000 to 36,500	36,500 to 47,500	47,500 to 62,000	62,000 to 80,000+

NOTE:
Regarding the last row of the table above: If many or most users use Virtual Desktop Infrastructure (VDI) applications and/or desktops, then the number of user sessions can be double or triple the number of online users for the enterprise.

IMPORTANT:
If you change the amount of RAM per appliance, it increases the storage required in your hypervisor environment for the virtual memory swap file for powering on the virtual appliance. Ensure that you have allocated enough storage to accommodate the change. Otherwise, powering on the virtual appliance will fail.

IMPORTANT:
For OneSign 7.11 and later releases, G4 appliances ship with *four* CPUs by default. When deploying new G4 *service* appliances, manually remove two CPUs. These defaults and requirements do *not* apply to G4 appliances on Azure. For information on G4 appliances on Azure, see Deploy G4 Appliances on Azure.

- The base two-appliance G4 enterprise, having 4 CPUs and 8 GB RAM per appliance, totaling 8 CPUs and 16 GB RAM for the enterprise, can be equated to a base two-appliance G3 enterprise that can accommodate 22,000 to 28,000 user sessions.

  Each additional column or step in the G4 table above yields approximately a 30% improvement in throughput.
- Odd numbers of appliances are recommended only when migrating from a G3 or G2 enterprise to a G4 enterprise, when the original enterprise has an odd number of appliances.
  - Migrations require the same number of G4 appliances in your new G4 enterprise as you have in your existing G3 or G2 enterprise, to support the enterprise export from G3 or G2 and import into G4.
  - For a migration with an odd number of appliances, after you transition your G4 enterprise to production, Imprivata recommends that you transition to a standard deployment configuration.
- Selecting an optimal enterprise configuration depends on knowing your total number of users and endpoints in your environment, usage patterns to identify peak activity periods, and disaster recovery needs that may stretch the topologies and halve the resources for active/active type setups.

There are many factors that affect performance including authentication types, multi-factor authentication methods, EPCS (electronic prescription of controlled substances) workflows, underlying hardware options for hosting the virtual machines that host the appliances, underlying network topology, and more.

Newer high performing systems may yield better throughputs, and conversely older systems may yield poorer performance.

- For customers with active G3 enterprises larger than two appliances, the rule of thumb is to first count the total number of CPUs in your current deployment. Then in the G4 table above, in row **Total appliance CPUs in enterprise**, find a G4 configuration with a matching CPU count.

G3 Appliances

The number of appliances appropriate for a G3 (third generation) enterprise depends on numerous factors, including user session counts, authentication methods, network topology, site configuration, and failover requirements.

- In general, using the fewest appliances necessary to meet these requirements is optimal.
- Only add appliances for redundancy or disaster recovery.
- Before adding appliances to the enterprise, consider scaling up by adding cores to the appliance beyond the preset two cores.
- The maximum number of cores per appliance is eight (8).
- Include audit appliances in the active mix of appliances servicing authentication requests.
- Approximately 11,000 to 14,000 user sessions can be supported per appliance, depending on workflows.

NOTE:
If many or most users use Virtual Desktop Infrastructure (VDI) applications and/or desktops, then the number of user sessions can be double or triple the number of online users for the enterprise.

Examples

- For 22,000 to 28,000 user sessions, use an enterprise of two appliances, with two cores each.
- For 28,000 to 48,000 user sessions, use an enterprise of two to three appliance, with four cores each.
- For 48,000 to 100,000 user sessions, use an enterprise with three appliances, with four to eight cores each.

Network Services Configuration

The Imprivata appliance supports the initial assignment of the following:

- IP address, subnet mask, and default gateway.
- DNS servers.

- NTP servers from the NTP Pool Project.

IP Address and Default Gateway Configuration

As part of the initialization process, an IP address, subnet, and default gateway are initially assigned.

This is achieved using either DHCP, if enabled in your environment, or later using the Imprivata Appliance Console when adding the appliance to a network. If required, you can change the settings using one of the following:

- The Imprivata Appliance Console before running the Imprivata appliance configuration (setup) wizard.
- The Imprivata Appliance Console (https://<appliance IP address>:81/) after completing the appliance configuration (setup) wizard.

> **NOTE**: If DHCP is used to assign these values, be sure to take the necessary steps to prevent duplicate IP address conflicts on the DHCP network. The Imprivata appliance requires a static IP address.

DNS Server Configuration

As part of the initialization process, up to three DNS servers are initially assigned.

- This is achieved using either DHCP, if enabled in your environment, or using the Imprivata Appliance Console.
- If required, the appliance configuration (setup) wizard lets you change these settings as part of the initial setup of the network services. Additionally, after the appliance has been added to the enterprise, you can use the Imprivata Appliance Console (**Network** > **Name Resolution**) to update them.

NTP Server Configuration

As part of the initialization process, the following servers from the North American pool are configured by default:

- 0.north-america.pool.ntp.org
- 1.north-america.pool.ntp.org
- 2.north-america.pool.ntp.org

If required, the appliance configuration wizard lets you change these settings as part of the initial setup of the network services. Additionally, after the appliance has been added to the enterprise, you can use the Imprivata Appliance Console (**Network** > **NTP**) to update them.

> **NOTE**: If you choose to change the defaults, configure at least two external internet-based NTP servers for redundancy. Internal NTP servers are not recommended.
>
> Using an internal NTP server or a Windows Server as an NTP source is not recommended. Windows does not correct any offset that may occur. Windows will keep adding to the offset and eventually an error will occur.

Deploy a VMware Appliance

The following sections detail how to install a virtual appliance to VMware and add it to the network.

Deploying the Imprivata OVF template

To deploy the appliance:

1. From your fulfillment letter, download and extract the Imprivata Virtual Appliance RAR file.

   NOTE: If deploying to VMware ESXi 6.7, deploy one appliance at a time. Deploying multiple appliance in parallel can result in the process timing out.

2. In the vSphere Client, click **File** > **Deploy OVF template**.
3. Follow the **OVF Deploy Template** wizard to complete the deployment. Consider the following:
   - ESXi 6.7 only — Select both the OVF and VMDK files.
   - When prompted to customize **Networking Properties**, either select DHCP if enabled in your environment, or leave all values blank and then later network the appliance using the appliance configuration (setup) wizard.
   - When prompted to review the settings, be sure that **Power on after deployment** is not selected before you finish the deployment.

NOTE: For more information on deploying an OVF template, see the VMware vSphere documentation.

Disabling the vApp Options

To disable the vApp options:

1. In the vSphere Client, right-click the virtual appliance, click **Edit Settings**, and open the **Options** tab.
2. Click **vApp options**, and select **Disable**.

   A message appears that prompts you to confirm the action.
3. Click **Yes**, and then click **OK**.

Adding the Appliance to the Network

To add the appliance to the network:

1. Power on the appliance, and open the console to start the appliance initialization scripts.
   - The initialization scripts run in the background and do not display progress. The time to complete is approximately 15 minutes.
   - The Imprivata Appliance Console displays the IP address, subnet mask, and gateway that is initially assigned to the appliance. For more information, see Appliance System Requirements and Guidance.
2. (Optional, or if DHCP is unavailable on your network) If required, you can add or change the network configuration manually:
   a. At the **login** prompt type **menu**, and then press **Enter**.
   b. Type **1**, and then press **Enter** to assign or reassign the values.

   > **NOTE**: If you receive a database error message when trying to log in, the appliance has not finished initializing.
3. Exit the Imprivata Appliance Console.
4. In a web browser, enter https://<*appliance_IP_address*>:81 to complete the setup using the appliance configuration (setup) wizard.

Accessing the Virtual Appliance Functions

You access the virtual appliance function menu from the Imprivata virtual appliance menu. Not all menu options are available until you complete the Imprivata Configuration Wizard.

To access the Imprivata virtual appliance menu:

1. Open the virtual machine console.
2. Select **Login** and press **Enter**.
3. At the login prompt, enter **menu** and press **Enter**. If prompted, enter the menu password and press **Enter**. The Imprivata virtual appliance functions menu opens.

The menu options are:

- **Configure Network** — Lets you change the default gateway for the appliance. It is for installation only. Change this setting from the Network tab under the Network page of the Imprivata Appliance Console.
- **Reset SSL** — Clears all SSL information, including the optional SSL 2.0 setting.
- **Reset Administrator password for Imprivata Appliance Console**— Resets the Administrator password to *admin*. You cannot reset the Super Administrator password.
- **Modify Password for this menu** — Lets you set or clear the password for this menu.

- **Restage** — Resets the appliance to factory settings. Contact Imprivata Customer Support for assistance with restaging an appliance.
- **Restart** — Restarts the appliance. It is best to restart the appliance by using the Imprivata Appliance Console **System** page > **Operations** tab > **Reboot/shutdown options** > **Reboot this appliance**, unless the Imprivata Appliance Console is unreachable.
- **Shutdown** — Shuts down the appliance. The Virtual Machine is still deployed in the VMware host.
- **Quit**

Troubleshooting

Verify the RAR File Download

Verify that the files were not corrupted during download.

1. In the Imprivata Virtual Appliance RAR file, there should be three files:
   - .mf - a manifest files, containing checksums for the OVF and VMDK files.
   - .ovf - the virtual machine template file, containing a description of the virtual machine.
   - .vmdk - the virtual machine hard disk file.
2. Open the .mf file in a text editor. It is formatted similar to the following example:

   ```
   SHA1(imprivata6.2.ovf)= a956be53480a2d6f4ca43a9c6ef46fba2e326150
   SHA1(system-disk1.vmdk)= a2bedcb3bfb14e7bbbf5ad481d58104aa1ec79ba
   ```

3. Run a hash of each of these two files to verify the resulting checksums against the contents of the manifest file.

   Use the following PowerShell command to get the file hash and convert it to lower case for easy comparison:

   ```
   $(Get-FileHash .\imprivata6.2.ovf -Algorithm SHA1 | Select -ExpandProperty
   Hash).ToLower()
   ```

4. Compare the output of the PowerShell command with the checksum in the manifest file.
   - If the checksums match, it confirms that the download is good and that the extracted files are good.
   - If the checksums do not match, it indicates that the files may be corrupted and may indicate a problem with either the extraction or download process.

Recommended Steps

1. Do not delete the existing RAR archive; it may still be usable.
2. Download the archive again, using an alternate browser from the original download method. While the download is in process, you can recheck the original file:

a. Use a different extraction utility to extract the original RAR archive. The choice of extraction utility may affect the outcome when extracting large archives.
b. Run the checksum process on the newly extracted files to determine whether the files are good.
   - If the checksums match, cancel the new download.
   - If the checksums do not match, continue the new download and repeat the verification process.

Issues Deploying OVF File to VMware

If you experience problems deploying the OVF file, consider the following:

- When deploying, select only the OVF and VMDK files, not the MN (manifest) file.

  The hypervisor may attempt to run a checksum on the manifest file, which does not contain a checksum for itself.

- Use the vSphere Web Client on Google Chrome, not Internet Explorer, to run the deployment.

  Internet Explorer has a maximum file size limit of 4GB, which may truncate the VMDK during the upload, causing the error:

  ```
  The checksum(s) from the provided manifest file do not match
  the content of the file(s).
  ```

- If you still experience problems, deploy the files using the vSphere command line tool instead of the Web Client.

  Example

  ```
  ovftool.exe -ds=VMFS005_3PAR109 --net:"Network 1”=”Network A VLAN 432"
  -n=WSLXIMP1901 "D:\Temp\S3x64\Imprivata5.5hf1demo_OVF10.ovf"
  vi://adminrb@100.64.0.25/
  ```

  Syntax

  ```
  ovftool --net: "source_network_name"="destination_network_name"
  -ds="destination_datastore" -n="destination_virtual_machine_name"
  "vi://domain\username@source_vcenter_fqdn/source_datacenter_name/
  virtual_machine_name/virtual_machine_folder/virtual_machine"
  "vi://domain\username@destination_vcenter_fqdn/host/cluster_name"
  ```

Deploy a Microsoft Hyper–V Appliance

The following sections detail how to install a virtual appliance to Microsoft Hyper–V and add it to the network.

Deploying the Imprivata VHD Image

To deploy the appliance:

1. From your fulfillment letter, download and extract the Imprivata Virtual Appliance RAR file.
2. In the Hyper-V Manager, click **Action** > **Import Virtual Machine**.
3. Browse to **imprivata*version***. *Version* specifies the version of the appliance.
4. Click **Next**.
5. Choose the type of import to perform:
   - **Register** – You have an environment where you have already put all of the virtual machine files exactly where you want them, and you only need Hyper-V to begin using the virtual machine as is.
   - **Restore** – Your virtual machine files are stored on a file share, or removable drive. For example — you want Hyper-V to move the files to the appropriate location for you, and then register the virtual machine.
   - **Copy** – You have a set of virtual machine files that you want to import multiple times. For example — using them as a template for new virtual machines. This selection copies the files to an appropriate location, gives the virtual machine a new unique ID, and then registers the virtual machine.
6. Click **Next**, and follow the wizard to complete the deployment.
7. In the Hyper–V Manager, right–click the appliance, and click **Settings**.
8. Select **Network Adapter**, connect to a virtual switch, and click **OK**.

Adding the Appliance to the Network

To add the appliance to the network:

1. Power on the appliance, and open the console to start the appliance initialization scripts.
   - The initialization scripts run in the background and do not display progress. The time to complete is approximately 15 minutes.
   - The Imprivata Appliance Console displays the IP address, subnet mask, and gateway that is initially assigned to the appliance. For more information, see Appliance System Requirements and Guidance.

2. (Optional, or if DHCP is unavailable on your network) If required, you can add or change the network configuration manually:
   a. At the **login** prompt type **menu**, and then press **Enter**.
   b. Type **1**, and then press **Enter** to assign or reassign the values.

> **NOTE**: If you receive a database error message when trying to log in, the appliance has not finished initializing.

3. Exit the Imprivata Appliance Console.
4. In a web browser, enter https://<*appliance_IP_address*>:81 to complete the setup using the appliance configuration (setup) wizard.

Accessing the Virtual Appliance Functions

You access the virtual appliance function menu from the Imprivata virtual appliance menu. Not all menu options are available until you complete the Imprivata Configuration Wizard.

To access the Imprivata virtual appliance menu:

1. Open the virtual machine console.
2. Select **Login** and press **Enter**.
3. At the login prompt, enter **menu** and press **Enter**. If prompted, enter the menu password and press **Enter**. The Imprivata virtual appliance functions menu opens.

The menu options are:

- **Configure Network** — Lets you change the default gateway for the appliance. It is for installation only. Change this setting from the Network tab under the Network page of the Imprivata Appliance Console.
- **Reset SSL** — Clears all SSL information, including the optional SSL 2.0 setting.
- **Reset Administrator password for Imprivata Appliance Console**— Resets the Administrator password to *admin*. You cannot reset the Super Administrator password.
- **Modify Password for this menu** — Lets you set or clear the password for this menu.
- **Restage** — Resets the appliance to factory settings. Contact Imprivata Customer Support for assistance with restaging an appliance.
- **Restart** — Restarts the appliance. It is best to restart the appliance by using the Imprivata Appliance Console **System** page > **Operations** tab > **Reboot/shutdown options** > **Reboot this appliance**, unless the Imprivata Appliance Console is unreachable.
- **Shutdown** — Shuts down the appliance. The Virtual Machine is still deployed in the VMware host.
- **Quit**

Deploy a Nutanix Appliance

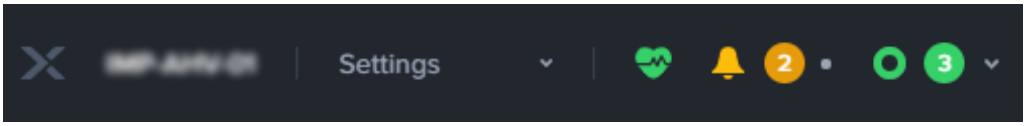
The following sections detail how to install a virtual appliance to Nutanix and add it to the network.

Creating the Appliance Image

You upload the Imprivata VMDK file (system-disk1) to create the appliance image.

To create the image:

1. From your fulfillment letter, download and extract the Imprivata Virtual Appliance RAR file.
2. In the Prism UI, select **Settings** from the main menu.

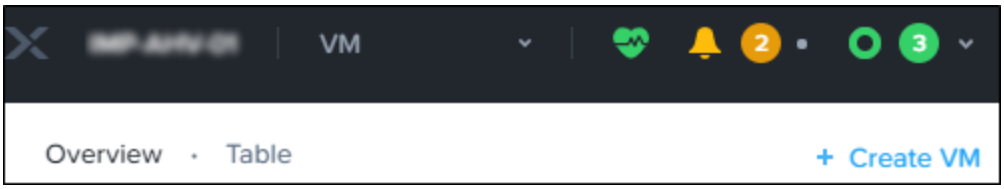


3. On the **Settings** page, click **Image Configuration**, and then click **Upload Image**.
4. Enter a name for the image.
5. From the **Image Type** list, select **Disk**.
6. Select a storage container, specify the image source location, and then click **Save**.

Creating the Virtual Machine

To deploy the appliance:

1. In Prism UI, select **VM** from the main menu, and then click **Create VM**.



2. On the **Create VM** dialog:
   a. Enter a name and select a timezone.
   b. Under **Compute Details**, allocate the minimum required RAM and CPU, and then click **Add New Disk.**

      See "*Imprivata OneSign Supported Components*" in the Imprivata Environment Reference for the minimum requirements.
3. On the **Add Disk** dialog:

a. From the **Operation** list, select **Clone from Image Service** .
b. From the **Image** list, select the appliance image that was created using the Imprivata VMDK file, and click **Add**.

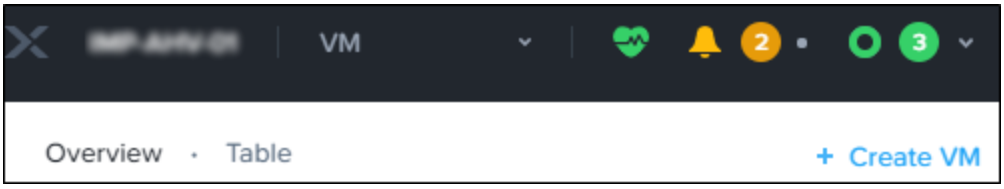
4. On the **Create VM** dialog:
   a. Under **Disks**, select **Disk** as the boot device.
   b. Under **Network Adapters (NIC)**, click **Add New NIC**.
5. On the **Create NIC** dialog:
   a. From the **VLAN** list, select the target virtual LAN.
   b. Deploy the NIC in a **Connected** state, and then click **Add**.
6. On the Create VM dialog, click **Save**.

Adding the Appliance to the Network

The following procedures detail how to add the appliance to the network.

Power on the Virtual Machine

1. In the Prism UI, select **VM** from the main menu, and then click **Table**.



2. Locate the virtual machine, click the name, and then click **Power on**.
3. Click **Launch Console**.

> **NOTE**: The initialization scripts run and display progress. The time to complete is approximately 15 minutes. If you receive a database error messaging when trying to log in, the appliance has not finished initializing.

Configure the Network Settings

To add the appliance to the network:

1. Power on the appliance, and open the console to start the appliance initialization scripts.
   - The initialization scripts run in the background and do not display progress. The time to complete is approximately 15 minutes.
   - The Imprivata Appliance Console displays the IP address, subnet mask, and gateway that is initially assigned to the appliance. For more information, see Appliance System Requirements and Guidance.

2. (Optional, or if DHCP is unavailable on your network) If required, you can add or change the network configuration manually:
   a. At the **login** prompt type **menu**, and then press **Enter**.
   b. Type **1**, and then press **Enter** to assign or reassign the values.

   > **NOTE**: If you receive a database error message when trying to log in, the appliance has not finished initializing.

3. Exit the Imprivata Appliance Console.
4. In a web browser, enter https://<*appliance_IP_address*>:81 to complete the setup using the appliance configuration (setup) wizard.

Accessing the Virtual Appliance Functions

You access the virtual appliance function menu from the Imprivata virtual appliance menu. Not all menu options are available until you complete the Imprivata Configuration Wizard.

To access the Imprivata virtual appliance menu:

1. Open the virtual machine console.
2. Select **Login** and press **Enter**.
3. At the login prompt, enter **menu** and press **Enter**. If prompted, enter the menu password and press **Enter**. The Imprivata virtual appliance functions menu opens.

The menu options are:

- **Configure Network** — Lets you change the default gateway for the appliance. It is for installation only. Change this setting from the Network tab under the Network page of the Imprivata Appliance Console.
- **Reset SSL** — Clears all SSL information, including the optional SSL 2.0 setting.
- **Reset Administrator password for Imprivata Appliance Console**— Resets the Administrator password to *admin*. You cannot reset the Super Administrator password.
- **Modify Password for this menu** — Lets you set or clear the password for this menu.
- **Restage** — Resets the appliance to factory settings. Contact Imprivata Customer Support for assistance with restaging an appliance.
- **Restart** — Restarts the appliance. It is best to restart the appliance by using the Imprivata Appliance Console **System** page > **Operations** tab > **Reboot/shutdown options** > **Reboot this appliance**, unless the Imprivata Appliance Console is unreachable.
- **Shutdown** — Shuts down the appliance. The Virtual Machine is still deployed in the VMware host.
- **Quit**

Troubleshooting

Verify the RAR File Download

Verify that the files were not corrupted during download.

1. In the Imprivata Virtual Appliance RAR file, there should be three files:
   - .mf - a manifest files, containing checksums for the OVF and VMDK files.
   - .ovf - the virtual machine template file, containing a description of the virtual machine.
   - .vmdk - the virtual machine hard disk file.
2. Open the .mf file in a text editor. It is formatted similar to the following example:

   ```
   SHA1(imprivata6.2.ovf)= a956be53480a2d6f4ca43a9c6ef46fba2e326150
   SHA1(system-disk1.vmdk)= a2bedcb3bfb14e7bbbf5ad481d58104aa1ec79ba
   ```

3. Run a hash of each of these two files to verify the resulting checksums against the contents of the manifest file.

   Use the following PowerShell command to get the file hash and convert it to lower case for easy comparison:

   ```
   $(Get-FileHash .\imprivata6.2.ovf -Algorithm SHA1 | Select -ExpandProperty
   Hash).ToLower()
   ```

4. Compare the output of the PowerShell command with the checksum in the manifest file.
   - If the checksums match, it confirms that the download is good and that the extracted files are good.
   - If the checksums do not match, it indicates that the files may be corrupted and may indicate a problem with either the extraction or download process.

Recommended Steps

1. Do not delete the existing RAR archive; it may still be usable.
2. Download the archive again, using an alternate browser from the original download method. While the download is in process, you can recheck the original file:
   a. Use a different extraction utility to extract the original RAR archive. The choice of extraction utility may affect the outcome when extracting large archives.
   b. Run the checksum process on the newly extracted files to determine whether the files are good.
      - If the checksums match, cancel the new download.
      - If the checksums do not match, continue the new download and repeat the verification process.

Issues Deploying OVF File to Nutanix

If you experience problems deploying the OVF file, consider the following:

- When deploying, select only the OVF and VMDK files, not the MN (manifest) file.

  The hypervisor may attempt to run a checksum on the manifest file, which does not contain a checksum for itself.

Deploy to a VMware ESX Thin-Provisioned Environment

Imprivata virtual appliances can be deployed using VMware ESX thin-provisioning. These appliances have the same performance as standard virtual appliances, as determined by the ESX infrastructure. Disk provisioning selection does not affect memory, CPU, and other Imprivata virtual appliance allocations.

NOTE:
Thin-provisioned virtual appliances never shrink in size when space is allocated by the hypervisor. This is a limitation of ESX Thin Provisioning, and is not limited to the Imprivata virtual appliance. You may see significant increases in Imprivata virtual appliance disk sizes if an appliance is unreachable for replication traffic in a problem situation. The only way to recover disk space is to replace appliances (see Replacing Existing Imprivata Virtual Appliances with Thin-Provisioned Imprivata Virtual Appliances).

Managing Thin-Provisioned Virtual Appliances

Carefully monitor the virtual appliance deployment space, for both the hypervisor (datastore) and the storage device (local disk, SAN, NFS). The initial thin-provisioned size of the virtual appliance is about 20 GB. The maximum thin-provisioned virtual appliance disk usage is 250 GB plus 8 GB of memory. The virtual appliance guest assumes it has a 250 GB disk available. If the storage device or datastore runs out of space, then the virtual appliance fails at the first event that requires more disk space. You can monitor virtual appliance disk usage in ESX, in the Imprivata Appliance Console **System** page **Operations** tab, or in the appliance logs.

CAUTION:
There is **no warning** if the hypervisor cannot allocate more disk space for the Imprivata virtual appliance. The host and Imprivata continue to operate normally until disk space runs out, and then unpredictable problems occur. Assume that, in this case, Imprivata OneSign (formerly Imprivata OneSign) shuts down and does not provide service to users.

Replacing Existing Imprivata Virtual Appliances with Thin-Provisioned Imprivata Virtual Appliances

To replace existing virtual appliances with thin-provisioned virtual appliances:

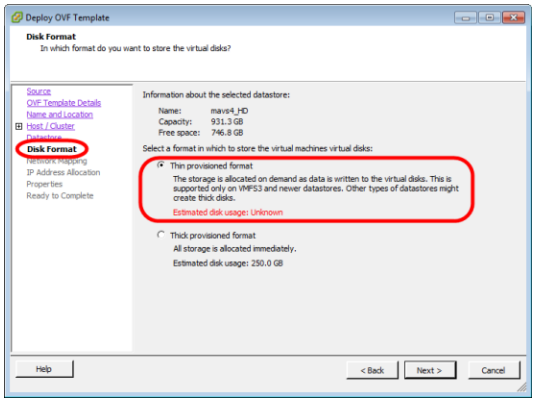
1. Remove the existing Imprivata virtual appliance from the enterprise. Confirm that the virtual appliance is powered off.
2. Deploy the new thin-provisioned Imprivata virtual appliance.

3. Synchronize the enterprise database from the Imprivata Appliance Console **System** page > **Operations** tab.
4. Add the thin-provisioned virtual appliance to the enterprise.
5. Delete the original virtual appliance.

Deploying a Thin-Provisioned Imprivata Virtual Appliance

To deploy a virtual appliance to a thin-provisioned ESX disk:

1. Log into VMware vSphere Client and **Create a new virtual machine** as you would for a standard VM, but for **Disk Format**, select **Thin provisioned format** instead as shown in the following image:



2. Complete the process and deploy as you would for a thick-provisioned VM.

> **NOTE:** As with all thin-provisioned VMs, the Used Storage grows over time and never diminishes of its own accord.

As the SAN fills up, you may want to recover some of that space. See Replacing Existing Imprivata Virtual Appliances with Thin-Provisioned Imprivata Virtual Appliances

Deploy G4 Appliances on Azure

The sections below describe how to deploy Imprivata G4 (fourth generation) virtual appliances on Microsoft Azure infrastructure services through the Azure Marketplace.

The release introduction history and supported migration path history of G4 and G3 (third generation) virtual appliances and enterprises ***on Azure*** is:

- Imprivata OneSign 23.2 supported larger scale and higher performance deployments of G4 on Azure by adding service appliances and the new migrations described in the next bullet
- Imprivata OneSign 23.2 added support for the following enterprise migrations involving Azure:
  - G3 on premises to G4 on Azure
  - G3 on Azure to G4 on Azure
  - G4 on premises to G4 on Azure
  - Hybrid G3 to hybrid G4. A hybrid G3 enterprise has some G3 appliances on premises and some on Azure, and usually supports a Disaster Recovery configuration. A hybrid G3 enterprise can be migrated to a hybrid G4 enterprise with G4 appliances on premises and on Azure.

> **NOTE:**
> For the procedure for *all* migrations to a G4 enterprise, see "Migrating to a G4 Enterprise" in the Imprivata Upgrade Portal. **This topic you are reading becomes part of that G4 migration procedure** when you are migrating to G4 *on Azure* or doing a hybrid G3 to G4 migration, in which case this topic occurs at section “Stage a G4 Appliance on Microsoft Azure” in the G4 migration topic.

- **Beginning with 23.2**, Imprivata adopted a new numbering scheme for Imprivata OneSignImprivata Confirm ID intended to reflect the yearly release cadence. The final release in the 7.x numbering scheme was Imprivata OneSignImprivata Confirm ID 7.12.
- **OneSign 7.10 through 7.12 supported G4 enterprises on Azure only for new enterprises of two database appliances**, although new enterprises of one database appliance can be used only for testing including Proof of Concept testing. **Scaling G4 appliances on Azure beyond two appliances by adding service appliances is only supported starting with OneSign 23.2 and later.**
- OneSign 7.10 supported either G3 or G4 appliances on Azure, but not both G3 and G4 appliances in the same enterprise.
- OneSign 7.4 through 7.10 supported G3 appliances on Azure.

NOTE:
You establish a G4 or G3 enterprise on Azure using different **private products** in the Azure Marketplace, so be sure to select the private product for the enterprise that you want.

Both G4 and G3 products were moved in the Azure Marketplace from their previous location in "Private offers" to a new location in a "Private product" category.

Assumptions

This documentation was written applying the following assumptions:

- You are familiar with Microsoft Azure Portal and Marketplace use and terminology.
- You are familiar with Microsoft Azure IaaS (Infrastructure as a Service) services.
- You have an active Azure tenant and subscription.

  NOTE:
  The Imprivata appliance on Azure is available as a private product in the Azure Marketplace. Microsoft blocks access to private products for Azure subscriptions owned by Azure Cloud Solutions Providers (CSPs). Therefore, customers using a CSP subscription must get their own Azure pay as you go tenant and subscription to access and use the Imprivata appliance on Azure.

- You adopt Microsoft's networking best practices.
- You are actively engaging with Imprivata service engineers (or other appropriate Imprivata personnel or partners) to ensure deployed resources are successfully connected to existing infrastructure.

Before You Begin

Before deploying an appliance on Azure, familiarize yourself with information associated with Microsoft Azure and the Imprivata G4 appliance. Review the following documentation:

- **Microsoft Azure documentation.** Many deployment tasks in this topic are performed in the Azure Portal and Marketplace. For more information, see the Azure documentation.
- "G4 Appliance Types" in the Imprivata online help.
- "The Imprivata Appliance Console" in the Imprivata online help.

Multiple Azure Hub-and-Spoke Topologies Supported

You can deploy Imprivata appliances into a variety of Azure hub-and-spoke network topologies. Your Azure network topology may depend on how much of your organization's infrastructure has been

migrated from being solely on-premises to being a hybrid mix of on-premises and in-cloud. Four common Azure network topologies into which you can deploy appliances are:

- Deploy appliances into one spoke virtual network in a single region. The Microsoft Active Directory (AD) is on premises.
- Deploy appliances into one spoke virtual network in a single region. The AD is in the hub virtual network in Azure.
- Deploy appliances into more than one spoke virtual network in different regions for enhanced local service, geographic redundancy, or due to latency or volume. The AD is in the hub virtual network.
- Deploy appliances into the hub virtual network to provide shared services to multiple spoke networks. The AD is in the hub virtual network.

For more information on the hub-and-spoke architecture, see Azure documentation on Hub-and-Spoke.

An Active Directory Domain Controller can be located on-premises or on Azure IaaS. If a Domain Controller is located on-premises, then before deploying an appliance on Azure, consider the following information:

- An Active Directory Domain Controller should be deployed into the Shared Services subnet in the hub virtual network. This reduces network traffic from the Azure data center to your on-premises network and associated network latency and data egress costs.
- The appliances are deployed as a spoke off of this central hub network and will depend on the gateway solution for any communication to on-premises resources.
- The appliance deployment should be targeted to the same geographic region as the hub virtual network to reduce inter-regional latency and data egress costs.

G4 Appliance Basic Specifications on Azure

Imprivata G4 appliances deployed on Azure are based on the same software stack as Imprivata G4 appliances on premises. The appliance is deployed on your choice of the following two options available:

- Azure F4s_v2 virtual machine (VM) having four vCPUs, 8 GB RAM, and 300 GB of storage.
- Azure F8s_v2 virtual machine having eight vCPUs, 16 GB RAM, and 300 GB of storage.

For both options, the Azure VM manages swap space in an external resource disk.

Number of G4 Appliances to Deploy on Azure

Imprivata supports automated deployment of G4 appliances on Azure, including both database appliances and service appliances. The database appliances and service appliances can be various mixes of Azure F4s_v2 VMs and/or F8s_v2 VMs, with one important recommendation: database appliances should have the same or greater processing power and capacity than service appliances in an enterprise. You must specify appliances with enough RAM and disk resources to handle the load expected for them as database or service appliances.

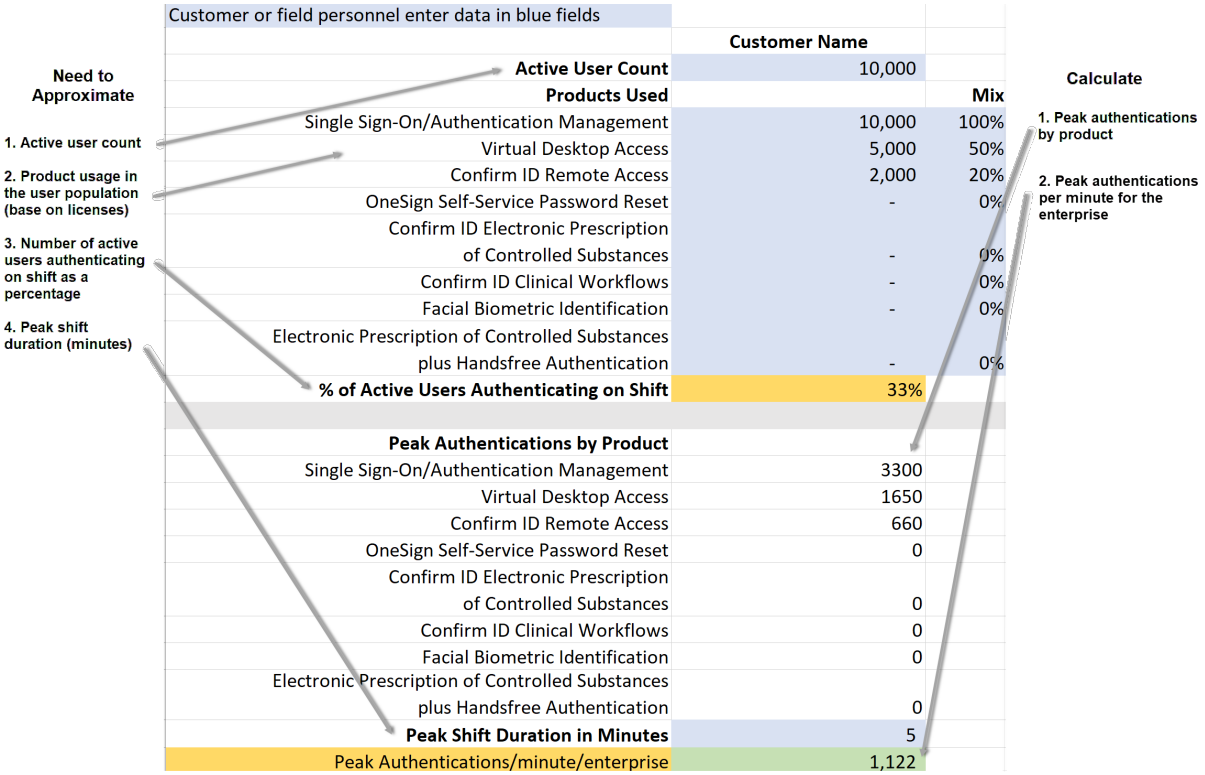
For an enterprise of only two database appliances, the Azure F4s_v2s may be sufficient. For higher performance needs, you can optionally scale up to using two F8s_v2s. For a larger enterprise of four or more appliances, the database appliances must be F8s_v2s to provide sufficient performance.

The number and type of appliances appropriate for an enterprise depends on numerous factors, including user counts, authentication methods, network topology, site configuration, and failover requirements. The table below shows baseline combinations of database appliances and service appliances in an Azure G4 enterprise for best performance and cost, assuming all appliances in the enterprise are active servicing endpoint requests. Alternatively, you can deploy enterprises with an odd number of appliances, but performance will vary. Larger enterprises on Azure are supported, but may yield only marginal performance improvements.

Recommended Options	2 Appliance Enterprise	2 Appliance Enterprise	4 Appliance Enterprise	6 Appliance Enterprise	6 Appliance Enterprise
Database Appliance Azure VM Type	F4s_v2 (4 VCPUs, 8 GB)	F8s_v2 (8 VCPUs, 16 GB)	F8s_v2 (8 VCPUs, 16 GB)	F8s_v2 (8 VCPUs, 16 GB)	F8s_v2 (8 VCPUs, 16 GB)
Number	2	2	2	2	2
Service Appliance Azure VM Type	None	None	F4s_v2 (4 VCPUs, 8 GB	F4s_v2 (4 VCPUs, 8 GB	F8s_v2 (8 VCPUs, 16 GB)
Number	0	0	2	4	4
Max Performance in Authentications per Minute	7,250	11,200	13,000	14,700	16,000

Estimate the maximum number of user authentications per minute needed for your enterprise at peak usage. You can then use the last row in the table above to determine the baseline enterprise that best matches your organization's needs.

To estimate the maximum number of user authentications per minute needed for your enterprise at peak usage, use the sample information in the graphic below as a general guide. Peak usage typically occurs at or near the start of a major work shift. Your Imprivata sales engineer or support person can help you with this estimation.



IMPORTANT:

Imprivata's G4 private product in the Azure Marketplace allows you to deploy up to 10 G4 appliances on 10 virtual machines (one appliance per VM) in one Azure resource group. This allows you to deploy some G4 appliances for a production enterprise, some for a staging enterprise, and some for a testing enterprise, all in the same Azure resource group. If you add more G4 appliances at a later time, you must add them to a different Azure resource group, and you cannot move them into the first Azure resource group. Therefore, if possible, deploy extra appliances, and if you don't need them, remove them later.

So, you should plan how many enterprises you will create, how many database and service appliances you will create in each enterprise, and which appliances will be Azure F4s_v2s or F8s_v2s. You can deploy up to 10 G4 appliances in one deployment process, including specifying F4s_v2 or F8s_v2 per appliance, and then during the wizarded configuration process for each appliance, you assign that appliance to an enterprise. The first two appliances assigned to an enterprise are always database appliances, and any more appliances assigned to that enterprise are always service appliances. Therefore, the order in which you assign appliances to an enterprise determines their type.

Also consider Imprivata G4 site recommendations, including “active/active” setups and using no more than two sites per G4 enterprise, as described in “Imprivata Sites for G4 Enterprises” in the Imprivata online help.

NOTE:
For specific questions about enterprise configuration or additional guidance, contact Imprivata Services or Support.

Network Services Configuration

When you deploy an appliance to Microsoft Azure, the Azure DHCP service assigns a networking configuration to the appliance.

CAUTION:
Do **not** change the networking configuration for the appliance (except as specified in the Note below if it applies). If you change network configuration values for the appliance, it may affect your ability to contact and control the virtual machine upon which the appliance runs.

Azure DHCP sets the following networking configuration values for the appliance that you should **not** change:

- Host name
- Domain name
- IP address
- Subnet mask
- Default gateway
- DNS servers
- NTP servers

NOTE:
If your Azure subscription uses a “Custom DNS,” meaning it uses your existing DNS infrastructure instead of the Azure DNS, then you must replace the domain name for the appliance after deployment and initialization and during configuration with a setup wizard, as mentioned in Appliance Initialization and Setup.

Deploying the Appliances

Gather the required data, consider the additional issues, and perform the tasks described in sections below to locate the Imprivata G4 appliance solution in the Azure Marketplace and perform the deployments.

Gathering the Azure and G4 Appliance Data Needed for Deployment

Collect and record the following Azure and G4 appliance resource data to use in the steps in Deploying the G4 Appliances from the Azure Marketplace:

- Your Azure **subscription ID**.
- An Azure **resource group** where the Imprivata appliance resources will live. You can use an existing resource group only if it is empty, such that no Azure resources are defined in it. Otherwise, you must create a resource group during the deployment.
- The Azure **region** (effectively the Azure Data Center) to which the appliance(s) will be deployed, such as East US, Central US, North Central US, or West Coast US. Appliance region placement is important because it impacts the performance of access to the Imprivata Appliance Console. Please follow Microsoft's recommendations regarding region selection in regard to proximity to your end users and latencies.
- The **virtual network** for the appliance(s), including whether you want to use an existing virtual network or create a new one.
- The **subnet** for the appliance(s) on that virtual network, including whether you want to use an existing subnet or manage your existing subnet configuration.
- The **diagnostic storage account** for the appliance(s). You can choose an existing account (if one exists) or create a new one. If you will create a new diagnostic storage account, decide on a name for it. The name must be between 3 and 24 characters long, inclusive, and include only lower-case letters and numbers with no spaces.
- Decide **how many G4 database and service appliances** you will create for production, test, and staging enterprises, and in total. Also decide which appliances will be F4s_v2s and which F8s_v2s. For guidance, see Number of G4 Appliances to Deploy on Azure above. For an individual enterprise, most customers deploy two database appliances for redundancy, plus optional service appliances if needed for performance. For a Proof of Concept (POC) deployment, deploy one database appliance. (You can also add an appliance later to a virtual network and subnet in which an existing appliance resides, but the new appliance must be placed in a different Azure resource group.)
- One or more **virtual machine (VM) names**, one for each VM that will host an appliance. Each name can be at most 28 characters long. The default values are imp-vm-01, imp-vm-02, and so on, which you can change. Consider creating a naming convention for your VM names. The VM name is applied as a prefix to the other resources deployed, for example, the NIC, private IP address, Network Services Group (NSG), and so on.

NOTE:
If you are deploying G4 appliances on Azure as part of migrating an enterprise to G4 on Azure, or as part of migrating a hybrid G3 enterprise to G4, then host names for appliances change during the migration. However, the host names of your original appliances must match the VM names you specify when creating the new G4 appliances on Azure, because an appliance's host name must always match its VM name. Therefore, note the original appliances' host names, or copy those host names from your enterprise export file, so you can specify them as the VM names for the new G4 appliances on Azure. In the export file, a host name appears as the first part of the FQDN (Fully Qualified Domain Name) for an appliance.

Considering Additional Issues

Consider these additional issues before you begin deploying the appliance(s):

- Establish required predefined **resources for backups and archiving,** such as file shares and file transfer systems (FTS).
- Assess **Disaster Recovery** (DR) region requirements and related network connectivity.
- An Azure **availability set** is automatically created for an appliance during the deployment. The availability set effectively splits a hosting virtual machine across server racks for increased reliability. If you plan to deploy multiple appliances, a different availability set is created for each appliance.
- Consider deploying your appliance(s) in an Azure **availability zone** in the Azure region where you will deploy the appliances.
- You can apply a **network security group** for an appliance on the hosting virtual machine NIC or subgroup.

Deploying the G4 Appliances from the Azure Marketplace

To locate and deploy the Imprivata G4 appliances from the Azure Marketplace:

1. In the Azure Portal, search for and select **Marketplace.**
2. Select **View Private Products.**
3. Select the Imprivata G4 product.

NOTE:
If you do not see this product, either contact your Imprivata representative or enter your contact information in the **Contact Me for Product** window and submit that request so that Imprivata can contact you. Imprivata must make the private product visible to you before you can proceed.

Do not select the **Imprivata OneSign/Confirm ID Solution (Preview)** product. That is the G3 appliance on Azure product.

A page displays describing the product.

4. Select **Create**. The **Create** page for the Imprivata G4 product opens to the **Basics** tab.

> **NOTE:**
> Moving quickly through the screens of the Azure deployment wizard may result in a verification error. To resolve the error, return to the previous screen and wait a short time before proceeding.

5. Under **Project details,** specify or select values for these fields:
   a. **Subscription:** Select your Azure subscription type, such as Pay-As-You-Go.
   b. **Resource group:** Either specify an existing, empty resource group that has no Azure resources defined in it, or select **Create new** and in the pop-up, specify a new resource group.
6. Under **Instance details**:

   Region: Select the Azure region for your appliances, which is often the region in which you are located.
7. Under **Configure virtual networks**:
   a. **Virtual network**: Select an existing virtual network or click **Create new** to create a new one.
   b. **Subnet**: Select an existing subnet or click **Manage subnet configuration** to manage your existing subnet configuration.

      For instructions on creating a new virtual network on Azure or managing your existing subnet configuration on Azure, see Microsoft's Azure documentation.

> **NOTE:**
> If you are deploying G4 appliances on Azure as part of *any* enterprise migration to G4 on Azure (or to a hybrid G4 enterprise on Azure and on premises), then you must specify virtual network and subnet values here, because any network values that you later import from your original enterprise export file will not be used.

8. Under **Storage account configuration**:

   Diagnostic storage account: Either select a value offered, if any, or click **Create New** and a frame appears on the right side of the interface. In that frame, specify a storage account name between 3 and 24 characters long, inclusive, and use only lower-case letters and numbers with no spaces. For the other three fields in the **Create storage** frame: **Account kind**, **Performance**, and **Replication**, use the default values.
9. Select **Next: Virtual Machine Settings**.
10. On the **Virtual Machine Settings** tab, specify or select values for the fields listed below. For guidance, see Number of G4 Appliances to Deploy on Azure above.

> **NOTE:**
> If you are deploying G4 appliances as part of migrating an enterprise to a new G4 enterprise on Azure, or as part of migrating a hybrid G3 enterprise to G4, then you must specify the host names of your original appliances in these fields as the virtual machine (VM) names for the new G4 appliances on Azure. This requirement is explained above in Gathering the Azure and G4 Appliance Data Needed for Deployment.

a. **First Virtual Machine name:** Either leave the default value imp-vm-01 unchanged or optionally change it. Each VM name can have at most 28 characters.

b. **First Virtual Machine size:** Specify whether to use a Standard_F4s_v2 Azure VM or a Standard_F8S_v2 Azure VM.

c. **Second Virtual Machine name:** Either leave the default value imp-vm-02 unchanged or optionally change it.

d. **Second Virtual Machine size:** Select an option to:
   - create an appliance using a Standard_F4s_v2 Azure VM
   - create an appliance using a Standard_F8S_v2
   - leave the default value selected to not deploy this appliance

e. For each of the third through tenth VMs, either leave the default VM name unchanged or optionally change it.
   For each VM, select from among the same three options as was offered for the **Second Virtual Machine size** field.

11. Click **Next: Review + create**. Azure reviews the configuration.

    If the validation passes, review your displayed selections and your displayed name, email address, and phone number. If any of your contact information is missing, enter it. Then click **Create** to deploy the solution.

    If the validation fails, view any error messages, resolve any issues, and click **Create** again.

The deployment starts and may take 5 to 10 minutes to complete.

As deployment progresses, the system displays status information. You can also confirm that deployment is in progress by clicking on the notification (bell) icon in the upper right corner of the Azure window. You can also select **Resource groups** in the Azure left frame and see your new Resource Group listed.

When the deployment is done, you can view the results in any of these ways:

- Click on the notification icon in the Azure window to view the Deployment Succeeded notification.
- From the **Notifications** drop-down, you can select **Go to resource group** and see your deployment with virtual machines, network interfaces (NICs), and disks, plus a network security group, a virtual network, a storage account, and an availability set.
- From that **Resource Group** display, you can select the virtual network to see your network settings and IP addresses.

- In the Resource Group left frame, you can select **Diagram** to see a diagram view of the network with a subnet, NICs, virtual machines, and a shared network security group.
- In that network diagram, you can select the network security group to see inbound and outbound ports with allow/deny settings and so on.

Appliance Initialization and Setup

After deployment, the appliance(s) power up automatically and initialization scripts run in the background and do not display progress. The time to complete is approximately 15 minutes for an appliance.

After that time, in a web browser, enter https://<*appliance_IP_address*>:81 to complete the setup of the first appliance using the appliance configuration wizard. During this configuration you specify the production, staging, or test enterprise to which to assign the appliance. Remember that the first two G4 appliances assigned to any G4 enterprise must be database appliances, and thereafter, all G4 appliances added to that same enterprise must be service appliances. Therefore, the order in which you assign appliances to an enterprise determines their type.

If your Azure subscription uses a "Custom DNS," meaning it uses your existing DNS infrastructure instead of the Azure DNS, then you must replace the domain name for the appliance during configuration with the wizard. In this case Azure DHCP supplies fake domain name reddog.microsoft.com during deployment and you must replace it with your existing domain name. You do this using the Imprivata Appliance Console during the networking step of the configuration setup.

If you deployed two or more G4 appliances, repeat the processes in this section for each additional G4 appliance.

If your G4 appliance deployments are part of an enterprise migration to G4 on Azure, or are part of a hybrid G3 enterprise migration to G4, then after you have completed setup of all the new G4 appliances on Azure, return to topic "Migrating to a G4 Enterprise", section "Export the Current Enterprise" on the Imprivata Upgrade Portal to continue your migration procedures.

Accessing the Appliance Functions

To access the Imprivata appliance functions menu:

1. In the Azure Portal, on the **Virtual Machines** window, in the **Support + Troubleshooting** section, access the Serial Console.
2. Open the console for the virtual machine hosting the Imprivata appliance.
3. At the system prompt, enter **menu** and press **Enter**. The Imprivata appliance functions menu opens.

The menu options are:

- **Configure Network** — Lets you change the default gateway for the appliance. Do *not* change this value for an appliance on Azure (see the Caution and Note in Network Services Configuration .)
- **Reset SSL** — Clears all SSL information.
- **Reset Administrator password for Imprivata Appliance Console** — Resets the Administrator password to *admin*. You cannot reset the Super Administrator password.
- **Modify Password for this menu** — Lets you set or clear the password for this menu.
- **Restage** — Resets the appliance to factory settings. Contact Imprivata Customer Support for assistance with restaging an appliance.
- **Restart** — Restarts the appliance. It is best to restart the appliance by using the Imprivata Appliance Console **System** page > **Operations** tab > **Reboot/shutdown options** > **Reboot this appliance**, unless the Imprivata Appliance Console is unreachable.
- **Shutdown** — Shuts down the appliance. The virtual machine is still deployed on the Azure host.
- **Quit**

Deploy a G3 Appliance on Azure

The sections below describe how to deploy an Imprivata G3 (third generation) virtual appliance on Microsoft Azure infrastructure services through the Azure Marketplace.

NOTE:
Imprivata recommends that you deploy G4 (fourth generation) appliances on Azure rather than G3 appliances, if possible. For instructions see Deploy G4 Appliances on Azure. You cannot have G4 and G3 appliances on the same enterprise, so if needed, consider migrating your enterprise to G4.

The release introduction history and supported migration path history of G3 appliances and enterprises *on Azure* is:

- Imprivata Enterprise Access Management (formerly Imprivata OneSign) 23.2 and later releases support enterprise migrations from G3 on Azure or on premises to G4 on Azure. For the procedure for *all* migrations to a G4 enterprise, see "Migrating to a G4 Enterprise" in the Imprivata Upgrade Portal.
- Imprivata OneSign 23.2 and later also support the migration of a hybrid G3 enterprise to a hybrid G4 enterprise. A hybrid G3 enterprise has some appliances on premises and some appliances on Azure, and usually supports a Disaster Recovery configuration. A hybrid G3 enterprise can be migrated to a hybrid G4 enterprise with G4 appliances on premises and on Azure.
- Imprivata OneSign 7.10 supported either G3 or G4 appliances on Azure, but not both G3 and G4 appliances in the same enterprise.
- Imprivata OneSign 7.4 through 7.10 supported G3 appliances on Azure.

NOTE:
You establish a G3 or G4 enterprise on Azure using different **private products** in the Azure Marketplace, so be sure to select the private product for the enterprise that you want. Both G3 and G4 products were moved in the Azure Marketplace from their previous location in "Private offers" to a new location in a "Private product" category.

Assumptions

This documentation was written applying the following assumptions:

- You are familiar with Microsoft Azure Portal and Marketplace use and terminology.
- You are familiar with Microsoft Azure IaaS (Infrastructure as a Service) services.
- You have an active Azure tenant and subscription.

> **NOTE:**
> The Imprivata appliance on Azure is available as a private product in the Azure Marketplace. Microsoft blocks access to private products for Azure subscriptions owned by Azure Cloud Solutions Providers (CSPs). Therefore, customers using a CSP subscription must get their own Azure pay as you go tenant and subscription to access and use the Imprivata appliance on Azure.

- You adopt Microsoft's networking best practices.
- You are actively engaging with Imprivata service engineers (or other appropriate Imprivata personnel or partners) to ensure deployed resources are successfully connected to existing infrastructure.

Before You Begin

Before deploying an appliance on Azure, familiarize yourself with information associated with Microsoft Azure and the Imprivata G3 appliance. Review the following documentation:

- **Microsoft Azure documentation.** Many deployment tasks in this topic are performed in the Azure Portal and Marketplace. For more information, see the Azure documentation.
- "G3 Appliance Types" in the Imprivata online help.
- "The Imprivata Appliance Console" in the Imprivata online help.

Multiple Azure Hub-and-Spoke Topologies Supported

You can deploy Imprivata appliances into a variety of Azure hub-and-spoke network topologies. Your Azure network topology may depend on how much of your organization's infrastructure has been migrated from being solely on-premises to being a hybrid mix of on-premises and in-cloud. Four common Azure network topologies into which you can deploy appliances are:

- Deploy appliances into one spoke virtual network in a single region. The Microsoft Active Directory (AD) is on premises.
- Deploy appliances into one spoke virtual network in a single region. The AD is in the hub virtual network in Azure.
- Deploy appliances into more than one spoke virtual network in different regions for enhanced local service, geographic redundancy, or due to latency or volume. The AD is in the hub virtual network.
- Deploy appliances into the hub virtual network to provide shared services to multiple spoke networks. The AD is in the hub virtual network.

For more information on the hub-and-spoke architecture, see Azure documentation on Hub-and-Spoke.

An Active Directory Domain Controller can be located on-premises or on Azure IaaS. If a Domain Controller is located on-premises, then before deploying an appliance on Azure, consider the following information:

- An Active Directory Domain Controller should be deployed into the Shared Services subnet in the hub virtual network. This reduces network traffic from the Azure data center to your on-premises network and associated network latency and data egress costs.
- The appliances are deployed as a spoke off of this central hub network and will depend on the gateway solution for any communication to on-premises resources.
- The appliance deployment should be targeted to the same geographic region as the hub virtual network to reduce inter-regional latency and data egress costs.

G3 Appliance Basic Specifications on Azure

Imprivata G3 appliances deployed on Azure are based on the same software stack as Imprivata on-premises G3 appliances. The appliance is deployed on an Azure F4 virtual machine (VM) having four vCPUs, 8 GB RAM, and 250 GB of storage. The Azure VM manages swap space in an external resource disk.

Number of G3 Appliances to Deploy on Azure

Imprivata supports automated deployment of only one or two G3 appliances per site on Azure. For redundancy, deploy two appliances. For a Proof of Concept deployment, deploy only one appliance, and if needed you can deploy one additional appliance for testing by using the G3 appliance private product again.

To add a second set of one or two G3 appliances on Azure, you must do the deployment process again and must deploy that second set into a different Azure resource group. Note that you ***cannot*** move the second set into the resource group of the first set.

NOTE:
For specific questions about enterprise configuration or additional guidance, contact Imprivata Services or Support.

The number of appliances appropriate for an enterprise depends on numerous factors, including user counts, authentication methods, network topology, site configuration, and failover requirements.

- In general, using the fewest appliances necessary to meet these requirements is optimal.
- Only add appliances for redundancy or disaster recovery.
- Include audit appliances in the active mix of appliances servicing authentication requests.
- Approximately 11,000 to 14,000 user sessions can be supported per appliance, based on workflows.

Network Services Configuration

When you deploy an appliance to Microsoft Azure, the Azure DHCP service assigns a networking configuration to the appliance.

CAUTION:
Do **not** change the networking configuration for the appliance (except as specified in the Note below if it applies). If you change network configuration values for the appliance, it may affect your ability to contact and control the virtual machine upon which the appliance runs.

Azure DHCP sets the following networking configuration values for the appliance that you should **not** change:

- Host name
- Domain name
- IP address
- Subnet mask
- Default gateway
- DNS servers
- NTP servers

NOTE:
If your Azure subscription uses a "Custom DNS," meaning it uses your existing DNS infrastructure instead of the Azure DNS, then you must replace the domain name for the appliance after deployment and initialization and during configuration with a setup wizard, as mentioned in Appliance Initialization and Setup.

Deploying the Appliance

Gather the required data, consider the additional issues, and perform the tasks described in sections below to locate the Imprivata G3 appliance solution in the Azure Marketplace and perform a deployment.

Gathering the Azure and G3 Appliance Data Needed for Deployment

Collect and record the following Azure and G3 appliance resource data to use in the steps in Deploying the G3 Appliance Solution from the Azure Marketplace:

- Your Azure **subscription ID**.
- An Azure **resource group** where the Imprivata appliance resources will live. You can use an existing resource group only if it is empty, such that no Azure resources are defined in it. Otherwise, you must create a resource group during the deployment.

- The Azure **region** (effectively the Azure Data Center) to which the appliance(s) will be deployed, such as East US, Central US, North Central US, or West Coast US. Appliance region placement is important because it impacts the performance of access to the Imprivata Appliance Console. Please follow Microsoft's recommendations regarding region selection in regard to proximity to your end users and latencies.
- Decide whether you will create **one or two** appliances. Most customers deploy two appliances for redundancy. For a Proof of Concept (POC) deployment, deploy one appliance. (You can also add an appliance later to a virtual network and subnet in which an existing appliance resides, but the new appliance must be in a different Azure resource group.)
- A **virtual machine (VM) name** for the VM that will host the appliance. The name can be a maximum of 28 characters long. The default value is imp-vm, which you can change. The deployment process appends a zero (0) to the VM name or a one (1) to a second VM name. Consider creating a naming convention for your VM names. The VM name is applied as a prefix to the other resources deployed, for example, the NIC, private IP address, Network Services Group (NSG), and so on.
- An **admin username and password** with which one or two VMs will be configured. The same admin username and password is used for two VMs if you deploy two appliances.
- The **virtual network** for the appliance(s), if you want to use an existing virtual network instead of accepting the supplied default value.
- The **subnet** for the appliance(s) on that virtual network, if you want to use an existing subnet instead of accepting the supplied default value.

Considering Additional Issues

Consider these additional issues before you begin deploying the appliance:

- Establish required predefined **resources for backups and archiving,** such as file shares and file transfer systems (FTS).
- Assess **Disaster Recovery** (DR) region requirements and related network connectivity.
- An Azure **availability set** is automatically created for the appliance during the deployment. The availability set effectively splits a hosting virtual machine across server racks for increased reliability. If you plan to deploy two appliances, a different availability set is created for each appliance.
- Consider deploying your appliance(s) in an Azure **availability zone** in the Azure region where you will deploy the appliances.
- You can apply a **network security group** for an appliance on the hosting virtual machine NIC or subgroup.

Deploying the G3 Appliance Solution from the Azure Marketplace

To locate and deploy the Imprivata G3 appliance solution from the Azure Marketplace:

1. In the Azure Portal, search for and select **Marketplace.**
2. Select **View Private Products.**

3. Select the **Imprivata OneSign/Confirm ID Solution (Preview).**

> **NOTE:**
> If you do not see this product, either contact your Imprivata representative or enter your contact information in the **Contact Me for Product** window and submit that request so that Imprivata can contact you. Imprivata must make the private product visible to you before you can proceed.
>
> Do not select the Imprivata G4 product.

When you can view the product and you select it, a page displays describing the solution.

4. Select **Create**. The **Create Imprivata OneSign/Confirm ID Solution** page opens.
5. On the **Basics** tab, under **Project details,** specify or select values for these fields:
   a. **Subscription:** Select your Azure subscription type, such as Pay-As-You-Go.
   b. **Resource group:** Either specify an existing, empty resource group that has no Azure resources defined in it, or select **Create new** and in the pop-up, specify a new resource group.
6. On the **Basics** tab, under **Instance details,** specify or select values for these fields:
   a. **Region:** Select the Azure region for your appliances, which is often the region in which you are located.
   b. **Virtual Machine name:** Either leave the default value imp-vm unchanged or optionally change it. The name can have at most 28 characters.
   c. **Choose the amount of appliances you want to create:** Select to deploy one or two appliances.
   d. **Username:** Specify an admin username for the VM. This username and its password are required by Azure, but you will not use them after specifying them here.
   e. **Password:** Specify a password. Password requirements are displayed in a pop-up as you enter or complete the password.
   f. **Confirm password:** Specify the password again.
   g. Select **Next: Virtual Machine Settings**.
7. On the **Virtual Machine Settings** tab, specify or select values for these fields:
   a. **Virtual machine size:** Leave the default value unchanged. Only the default size is supported.
   b. **Diagnostic storage account:** Leave the default value unchanged.
   c. **Public IP address for the VM:** Select value None.

> **CAUTION:**
> You should **not** use a public IP address for an appliance for security reasons. Anyone, including malicious users, who can discover that IP address can use it to access the appliance.

   d. **DNS prefix for the public IP address:** This field becomes disabled when you specify None for the Public IP address.

8. On the **Virtual Machine Settings** tab, under **Configure virtual networks,** specify or select values for these fields:
    a. **Virtual network**: Specify an existing virtual network or accept the supplied default value.
    b. **Subnet**: Specify an existing subnet or accept the supplied default value.
9. Click **Next: Review + create**. Azure reviews the configuration.
10. If the validation passes, review your selections and then click **Create** to deploy the solution.

    If the validation fails, view any error messages, resolve any issues, and click **Create** again.

    The deployment starts and may take 5 to 10 minutes to complete.

As deployment progresses, the system displays status information. You can also confirm that deployment is in progress by clicking on the notification (bell) icon in the upper right corner of the Azure window. You can also select **Resource groups** in the Azure left frame and see your new Resource Group listed.

When the deployment is done, you can view the results in any of these ways:

- Click on the notification icon in the Azure window to view the Deployment Succeeded notification.
- From the **Notifications** drop-down, you can select **Go to resource group** and see your deployment with one or two virtual machines, network interfaces (NICs), and disks, plus a network security group, a virtual network, a storage account, and an availability set.
- From that **Resource Group** display, you can select the virtual network to see your network settings and IP addresses.
- In the Resource Group left frame, you can select **Diagram** to see a diagram view of the network with a subnet, one or two NICs and virtual machines, and a shared network security group.
- In that network diagram, you can select the network security group to see inbound and outbound ports with allow/deny settings and so on.

Appliance Initialization and Setup

After deployment, the appliance powers up automatically and initialization scripts run in the background and do not display progress. The time to complete is approximately 15 minutes.

After that time, in a web browser, enter https://<*appliance_IP_address*>:81 to complete the setup using the appliance configuration wizard.

If your Azure subscription uses a “Custom DNS,” meaning it uses your existing DNS infrastructure instead of the Azure DNS, then you must replace the domain name for the appliance during configuration with the wizard. In this case Azure DHCP supplies fake domain name reddog.microsoft.com during deployment and you must replace it with your existing domain name. You do this using the Imprivata Appliance Console during the networking step of the configuration setup.

If you deployed two appliances, repeat the processes in this section for the second appliance.

Accessing the Appliance Functions

To access the Imprivata appliance functions menu:

1. In the Azure Portal, on the **Virtual Machines** window, in the **Support + Troubleshooting** section, access the Serial Console.
2. Open the console for the virtual machine hosting the Imprivata appliance.
3. At the system prompt, enter **menu** and press **Enter**. The Imprivata appliance functions menu opens.

The menu options are:

- **Configure Network** — Lets you change the default gateway for the appliance. Do ***not*** change this value for an appliance on Azure (see the Caution and Note in Network Services Configuration .)
- **Reset SSL** — Clears all SSL information.
- **Reset Administrator password for Imprivata Appliance Console** — Resets the Administrator password to *admin*. You cannot reset the Super Administrator password.
- **Modify Password for this menu** — Lets you set or clear the password for this menu.
- **Restage** — Resets the appliance to factory settings. Contact Imprivata Customer Support for assistance with restaging an appliance.
- **Restart** — Restarts the appliance. It is best to restart the appliance by using the Imprivata Appliance Console **System** page > **Operations** tab > **Reboot/shutdown options** > **Reboot this appliance**, unless the Imprivata Appliance Console is unreachable.
- **Shutdown** — Shuts down the appliance. The virtual machine is still deployed on the Azure host.
- **Quit**

Replacing G3 Appliances on Premises with G3 Appliances on Azure, or Creating a Hybrid G3 Enterprise

NOTE:
Imprivata OneSign 23.2 and later releases support enterprise migrations from G3 on premises or on Azure to G4 on Azure, and from a hybrid G3 enterprise to a hybrid G4 enterprise. For the procedure for *all* migrations to a G4 enterprise, see "Migrating to a G4 Enterprise" in the Imprivata Upgrade Portal.

For an existing Imprivata enterprise that has one or two Imprivata G3 appliances on premises, you can replace one or both of those appliances with Imprivata G3 appliances on Microsoft Azure. To do this, follow the procedure below, which is written using the assumption that you are replacing two existing G3 appliances.

Alternatively, you can add one or two G3 appliances on Azure to your existing on-premises G3 appliances, to create a hybrid on-premises and Azure G3 enterprise. If your on-premises G3 enterprise has more than two appliances and you want to extend it with one or two Azure appliances, you must ensure that your Azure appliances have sufficient CPU counts to support the service levels needed if appliances fail over.

Replacing Your License if You Replace Your On-Premises G3 Appliances

If you want to replace your G3 appliances on premises with G3 appliances on Azure, ask your Imprivata account team to issue a zero dollar replacement order. Imprivata Operations then provides you a temporary license with four serial numbers: two from your current on-premises production appliances, and two replacement serial numbers for your new G3 appliances on Azure. You, or Imprivata Professional Services if you have contracted for them to do this, then perform the procedure below to:

1. Create your new G3 appliances on Azure.
2. Add those appliances to your existing G3 enterprise.
3. Redirect your endpoints to your new Azure appliances.
4. Remove and then permanently delete your on-premises appliances from your enterprise.

Imprivata Operations then makes permanent the replacement appliance serial numbers by issuing to you a new license that includes only the new serial numbers. Your previous on-premises appliance serial numbers are omitted from that license.

Procedure to Replace G3 Appliances on Premises with G3 Appliances on Azure, or to Create a Hybrid G3 Enterprise

To replace your G3 appliances on premises with G3 appliances on Azure, complete all of the steps in the procedure below. Alternatively, to create a hybrid on-premises and Azure G3 enterprise, stop following the procedure at the end of step 7. The complete procedure through step 11 is written using the assumption that you are replacing two existing on-premises G3 appliances. One step in the procedure includes a 24-hour waiting period, so include that period in your work plan. If you follow the procedure from a PDF document, you also must have access to Imprivata OneSign online help to view the details of some steps in the procedure.

Before starting the procedure, read the full section Deploy a G3 Appliance on Azure to prepare for the appliance deployments on Azure.

Here is the procedure:

1. Deploy two G3 appliances on Azure at the same time by following the procedure in Deploying the G3 Appliance Solution from the Azure Marketplace.

   Note these tips:

   - You will likely need to specify a different subnet for the Azure appliances than are used for the on-premises appliances.
   - Do **not** complete the setup yet of each Azure appliance using the appliance configuration setup wizard.

2. Authorize the first Azure appliance by following the procedure in Step 1: Authorize the New Appliance, which appears in online help topic "Adding an Appliance to the Enterprise". (You only do Step 1 in that topic.)

   Note these tips:

   - Use an on-premises appliance that is also an audit server to authorize the Azure appliances.
   - Specify the existing site that includes the two physical appliances.
   - **Make note of the Azure appliance's serial number and connection password as you specify them.**
   - Specify that each of the new appliances will be audit servers.
   - Do **not** change the optional field values (networking configuration). They were set by the Azure DHCP service during appliance deployment, and the authorization process may overwrite some of those values with values populated from the authorizing appliance.
3. Authorize the second Azure appliance by repeating step 2.
4. Run the appliance configuration setup wizard for the first Azure appliance, by following the instructions in Appliance Initialization and Setup.

   Note these tips:

   - You may need to replace the domain name for the appliance, as explained in the linked section.
   - An appliance's serial number and connection password that you use in the setup wizard **must match** the values you used earlier when authorizing the appliance. Otherwise, the new appliance will get an authorization failed message when trying to join the enterprise in the wizard process.
5. Monitor the database replication process for the first appliance to ensure it has synced up with the enterprise.

   In the Imprivata Admin Console, select the **gear icon > Sites**. The status for the site containing the new appliance should be displayed as Up. After adding a new appliance, site status can be in a warning state until the new appliance has time to automatically sync up its database.
6. Run the appliance configuration setup wizard for the second Azure appliance by repeating step 4 for the second Azure appliance.

   When you are done with this step, you have a hybrid, four-appliance G3 enterprise, with two on-premises G3 appliances and two G3 appliances on Azure.
7. Wait for at least 24 hours for all Imprivata endpoint agents to recognize the new appliance topology. The time needed depends on the size of your environment.

   To keep your hybrid enterprise, stop following this procedure here.

   To replace your on-premises G3 appliances with your new Azure G3 appliances, complete these additional steps:
8. Update all endpoints to point all Imprivata endpoint agents to the Azure appliances.

   Methods to redirect your endpoints to the Azure appliances vary by endpoint type. A representative example is provided here for Windows endpoints:

Update the **IPTXPrimServer** registry key in the Windows endpoints to be redirected. Typical methods to do this include using a Microsoft Windows Group Policy Object (GPO) or a software distribution tool such as Microsoft Endpoint Manager (formerly called Microsoft System Center Configuration Manager, SCCM) or Ivanti Unified Endpoint Manager (formerly called LANDESK).

The registry key is located at:

HKEY_LOCAL_MACHINE\SOFTWARE\SSOProvider\ISXAgent

Change only the DNS hostname part of the URL for the Azure appliance to be used. For example, if the existing registry key value is:

https://**ova1.myhealth.edu**/sso/servlet/messagerouter

then change that value to something like this:

https://**new-ova1.myhealth.edu**/sso/servlet/messagerouter

9. Remove the on-premises appliances from the enterprise using the instructions in "Removing or Deleting an Appliance from the Enterprise" in the Imprivata online help.

   When you are done with this step, you have a two appliance G3 enterprise on Azure.
10. Confirm that users can log in using the Imprivata endpoint agents pointed to the new appliances.
11. Permanently delete the on-premises appliances from the enterprise using the instructions in "Removing or Deleting an Appliance from the Enterprise in the Imprivata online help.