Dialogic®

Dialogic® BorderNet™ Virtualized Session Border Controller (SBC)

Installation and Set-Up Guide

December 2013

www.dialogic.com

Copyright and Legal Notice

All contents of this document are furnished for informational use only and are subject to change without notice and do not represent a commitment on the part of Dialogic Inc. and its affiliates or subsidiaries ("Dialogic"). Reasonable effort is made to ensure the accuracy of the information contained in the document. However, Dialogic does not warrant the accuracy of this information and cannot accept responsibility for errors, inaccuracies or omissions that may be contained in this document.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH DIALOGIC® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in certain safety-affecting situations. Please see http://www.dialogic.com/company/terms-of-use.aspx for more details.

Due to differing national regulations and approval requirements, certain Dialogic products may be suitable for use only in specific countries, and thus may not function properly in other countries. You are responsible for ensuring that your use of such products occurs only in the countries where such use is suitable. For information on specific products, contact Dialogic Inc. at the address indicated below or on the web at *www.dialogic.com*.

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic does not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic and no such licenses are provided except pursuant to a signed agreement with Dialogic. More detailed information about such intellectual property is available from Dialogic's legal department at 6700 de la Cote-de-Liesse Road, Suite 100, Borough of Saint-Laurent, Montreal, Quebec, Canada H4T 2B5. **Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements.**

Dialogic, Dialogic Pro, Dialogic Blue, Veraz, Brooktrout, Diva, BorderNet, PowerMedia, ControlSwitch, I-Gate, Mobile Experience Matters, Network Fuel, Video is the New Voice, Making Innovation Thrive, Diastar, Cantata, TruFax, SwitchKit, Eiconcard, NMS Communications, SIPcontrol, Exnet, EXS, Vision, inCloud9, NaturalAccess and Shiva, among others as well as related logos, are either registered trademarks or trademarks of Dialogic Inc. and its affiliates or subsidiaries. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at 6700 de la Cote-de-Liesse Road, Suite 100, Borough of Saint-Laurent, Montreal, Quebec, Canada H4T 2B5. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic's trademarks requires proper acknowledgement.

The names of actual companies and products mentioned herein are the trademarks of their respective owners.

This document discusses one or more open source products, systems and/or releases. Dialogic is not responsible for your decision to use open source in connection with Dialogic products (including without limitation those referred to herein), nor is Dialogic responsible for any present or future effects such usage might have, including without limitation effects on your products, your business, or your intellectual property rights.

Table of Contents

Revision History

Revision	Release date	Notes
2.0	December 2013	Release 3.2
1.0	August 2013	Release 3.1

Refer to www.dialogic.com for product updates and for information about support policies, warranty information, and service offerings.

1. Overview

The Dialogic® BorderNet™ Virtualized Session Border Controller (SBC) is a software-only solution created for a virtualized environment. The BorderNet Virtualized SBC supports features such as:

- Session Routing (Static, Dynamic Policy, SIP Message-Based Routing, and so forth)
- Security Features (ALG, Rate Control, Bandwidth Reservation, Policing, and so forth)
- Networking (IPv4, IPv6, VLAN tagging, IP Routing, VLAN Default Gateway)
- Session Control (SIP Signaling, B2BUA, Offer/Answer, Peer Connectivity, IPv4-to-IPv6 Interworking, Media Relay, and so forth)
- Transport (UDP, TCP, TLS)
- Session Transparency
- Stand-Alone and High Availability (HA) Deployment

The BorderNet Virtualized SBC is designed to operate in a hypervisor (virtual machine) environment on compatible commercial off-the-shelf server hardware. The BorderNet Virtualized SBC can be deployed in service provider and enterprise networks.

Intended Audience

This document is intended for system administrators who are familiar with IP networks and virtual machine technology.

How to Use This Guide

The *Dialogic® BorderNet™ Virtualized Session Border Controller Installation and Set-Up Guide* provides information you need to download, install, and set-up the BorderNet Virtualized SBC.

The following chapters should be completed in the order presented:

- Chapter 2: Before You Begin provides prerequisite information and a checklist to ensure you have the information you need prior to beginning the procedures in this document.
- Chapter 3: Planning and Turn-Up provides guidance on replacing an existing SBC with the BorderNet Virtualized SBC.
- Chapter 4: Installing the BorderNet Virtualized SBC Software provides procedures for deploying the BorderNet Virtualized SBC Virtual Machine (VM) instance, setting up the web-based management system, obtaining a license file, and initial configuration.
- Chapter 5: Accessing the BorderNet Virtualized SBC WebUI provides procedures for first-time browser access.
- Chapter 6: Configuration and Provisioning provides basic configuration and provisioning examples to configure user access and provision traffic.

2. Before You Begin

This chapter provides the prerequisites that must be in place before installing the BorderNet Virtualized SBC. Use the Pre-Installation Checklist to verify you have the necessary components prior to beginning the BorderNet Virtualized SBC installation procedures.

Note: Dialogic does not provide product or support services for VMware vSphere ESXi or the underlying x86 hardware. The customer is responsible for:

- Providing and maintaining an x86 server(s) compatible with the VMware vSphere.
- Ensuring that the server(s) meet or exceed Dialogic's Minimum Hardware Requirements.
- Installing, configuring, and maintaining VMware vSphere ESXi (version 5.0 or later) and the vSphere Client.

Prerequisites

The prerequisites in the following sections must be met before installing the BorderNet Virtualized SBC:

- Minimum Hardware Requirements
- Qualified Servers
- Hypervisor Installation Requirements
- Hypervisor Logical Network Example
- License Information

Minimum Hardware Requirements

The BorderNet Virtualized SBC can be installed on an x86 server platform that is compatible or certified with the VMware VSphere Hypervisor ESXi (version 5.0 or higher) and meets the minimum hardware requirements below. Refer to the VMware website for a list of compatible servers.

Category	Minimum Requirement
Hypervisor	VMWare vSphere ESXi version 5.0 or higher
CPU	• Two (2) 64-bit CPU or One (1) 64-bit dual core processor • 2.4GHz or faster Intel 64 or AMD 64 processor **Note**: The Itanium (IA64) processor is not supported
Memory	4GB RAM
Disk Space	Minimum 40GB, with up to 2GB free disk space to decompress the installation (OVF) archive 80GB or higher preferred

Network Interfaces	Four (4) 1GbE connections preferred Recommended allocation includes: • Two (2) 1GbE interfaces for signaling and media • One (1) 1GbE interface for High Availability • One (1) for Administration

Qualified Servers

The underlying physical servers can be any x86 hardware that is compatible with the VMware vSphere Hypervisor**.**

Dialogic has tested and qualified the BorderNet Virtualized SBC on the following servers:

- Dell PowerEdge R710 and R720 Servers
- HP Proliant BL and ML series servers

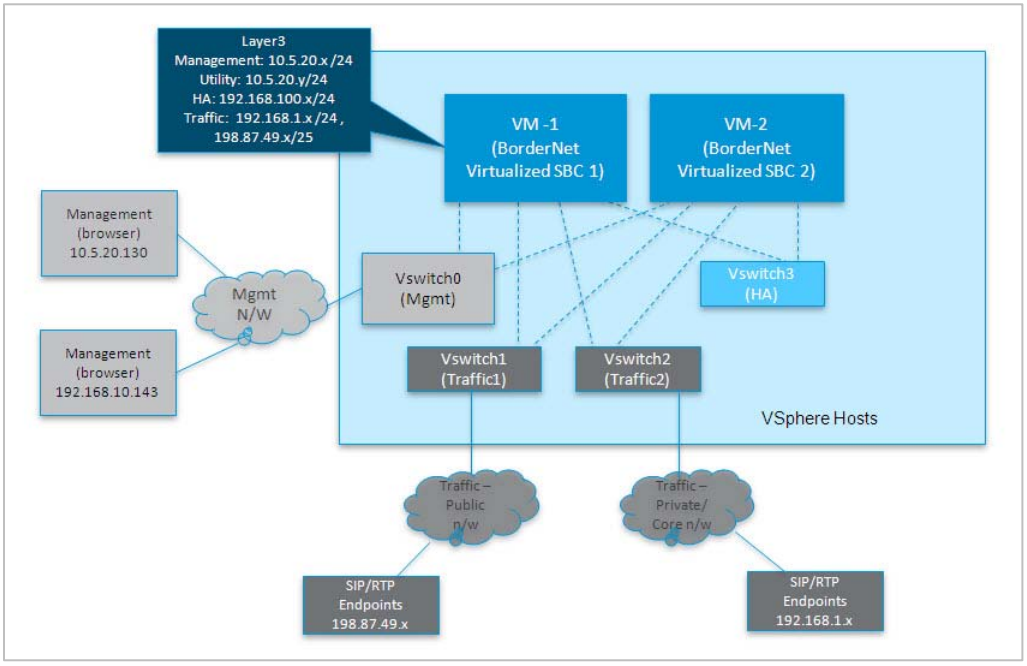
Note: Dialogic does not favor or recommend any particular brand of server.

Hypervisor Installation Requirements

- The VMware ESXi hypervisor must be installed directly on top of the server.
- The server must have VMware vSphere ESXi 5 installed and fully configured prior to installing the BorderNet Virtualized SBC.
- The VMware vSphere Client must be installed to manage the hypervisor environment.

Sample Network Diagram

The following diagram shows an example of logical networks and subnets.

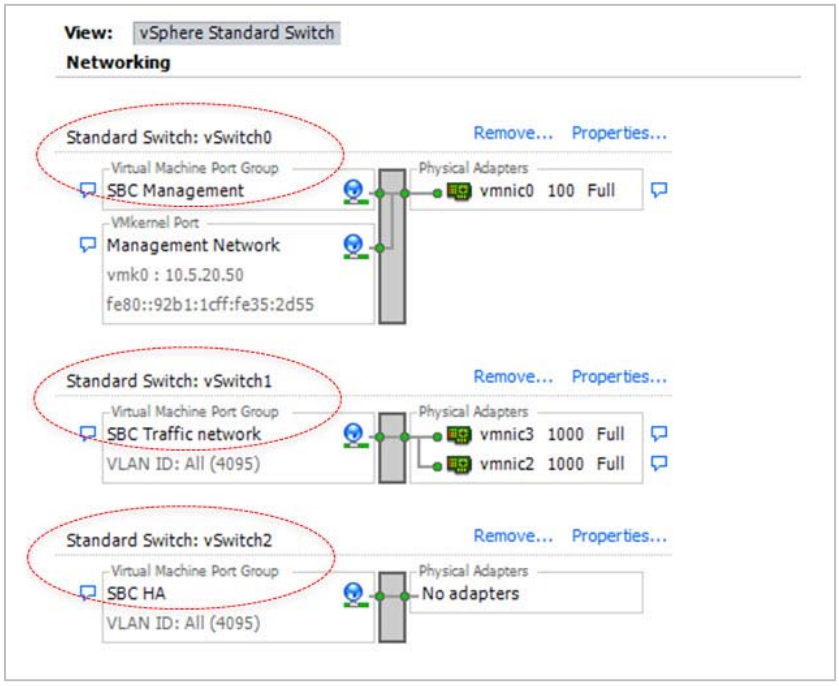


A typical network design contains three separate logical networks:

1. Management
2. Standard traffic
3. HA

Note: Subnets cannot overlap.

The following figure shows an example of logical networks and subnets in Vsphere, using virtual networking.



License Information

Trial and Production use of the BorderNet Virtualized SBC requires a specific License file. In order to obtain your license file, you will need:

- The email address of the Dialogic Order Desk from which this product was procured.
- The BorderNet Virtualized SBC Order Number.

Make a note of the above information. If you do not know the Order Desk email address or Order Number, contact your Dialogic Sales Representative.

Initial Set-Up Information

Prior to beginning the installation process, determine the initial set-up of your system. There are two ways set-up the BorderNet Virtualized SBC:

- A **Standalone** system has one virtual machine instance designated as the primary system.
- A **High Availability (HA)** system has two virtual machine instances where one instance is designated as “primary” and the other instance is designated as “secondary”.

Note: Once the designations have been made, they cannot be changed unless you reconfigure the initial system set-up.

Utility IP Address

Each virtual machine instance must have its own **Utility IP Address** that is used for access (for example, FTP or Telnet to the platform). The Utility IP address is fixed to the instance and is not shared.

Note: You cannot use utility IP address to access the BorderNet Virtualized SBC WebUI.

System Management IP Address

The **System Management IP Address** is used to access of the BorderNet Virtualized SBC, including WebUI access. For HA configurations, this IP Address is shared (floating) between the primary and secondary instances.

Intertask - HA IP Address

The **Intertask - HA IP Address** is used for HA communication and all communication within the BorderNet Virtualized SBC.

Note: This must be configured regardless of whether you are setting up an HA or a Standalone System. This IP address must be from a different subnet than the System Management IP address.

Pre-Installation Checklist

Complete the following pre-installation checklist before beginning the BorderNet Virtualized SBC installation procedures.

Physical Server	
☐	Compatible with VMWare vSphere ESXi 5.0 or later.
☐	Meets Dialogic's Minimum Hardware Requirements.
☐	Power and Network cabling completed.
☐	IP Connectivity is established and all interfaces are activated.
☐	Adequate disk space is available for temporary storage of the BorderNet Virtualized SBC OVF (approximately 1.6GB).
Hypervisor	
☐	VMware vSphere 5.0 ESXi 5.0 or later is fully installed and configured.
☐	VMware management tool(s) installed.
☐	Logical networks must be created in the hypervisor environment for Management, Session Traffic towards Public and Core networks, and HA networks (if applicable). See the Sample Network Diagram for an example.
Initial Set-Up Information for the BorderNet Virtualized SBC	
☐	Determine the type of initial set-up: Standalone or HA.
☐	Note the Utility IP Address.
☐	Note the System Management IP Address.
☐	Note the Intertask - HA IP Address
☐	Note the Netmask.
☐	Note the Gateway IP Address.
License Information	
☐	Note the Sales Order Number or Purchase Order Number of your BorderNet Virtualized SBC.
☐	Note the Platform Serial Number and License Request ID for each instance of the system.

3. Installing the BorderNet Virtualized SBC Software

This chapter provides the installation instructions for the BorderNet Virtualized SBC. There are four parts to the installation procedure:

- Downloading the .ova File
- Deploying the BorderNet Virtualized SBC VM
- Setting Up the Web-Based Management System
- Obtaining a License File
- Initial System Set-Up

Note: It will take one business day to obtain your license file. Once you have completed the Obtaining a License File portion the instructions, stop this procedure. Do not begin the Initial System Set-Up until you have received the license file.

Downloading the .ova File

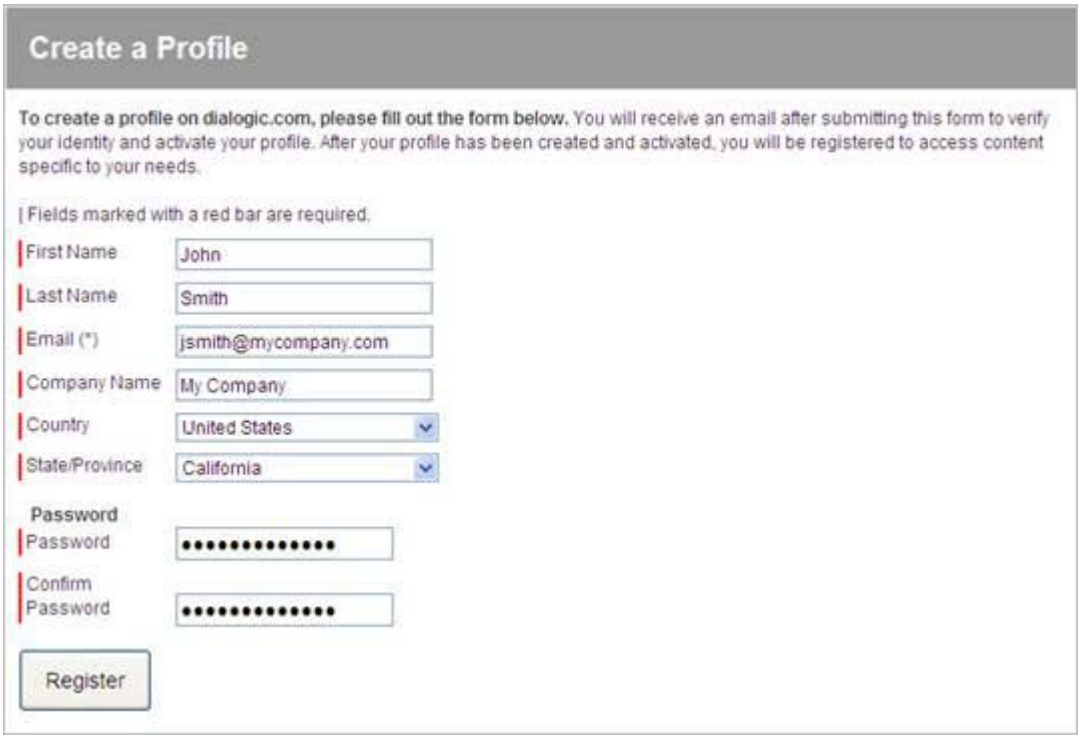
The BorderNet Virtualized SBC is delivered in an Open Virtualization Format (OVF), packaged as an **.ova** archive. Use the following procedure to download the .ova file.

- Go to http://www.dialogic.com/en/products/session-border-controllers/bordernet-virtualized-sbc.aspx.

- Under the **Related Links** menu, select **Download BorderNet Virtualized SBC**.
- You will be prompted to login with your email address and password.

- If you have already registered with Dialogic, enter your **Email** and **Password** and click **Login** to download the .ova file.

- If you have not registered with Dialogic, select **Register** to create a profile.
  - In the **Create a Profile** screen, enter the required information.
  - Click **Register**.
  - Check your email; you will receive a link to activate your profile.
  - Once your profile is activated, use your email address and password to login to download the .ova file.

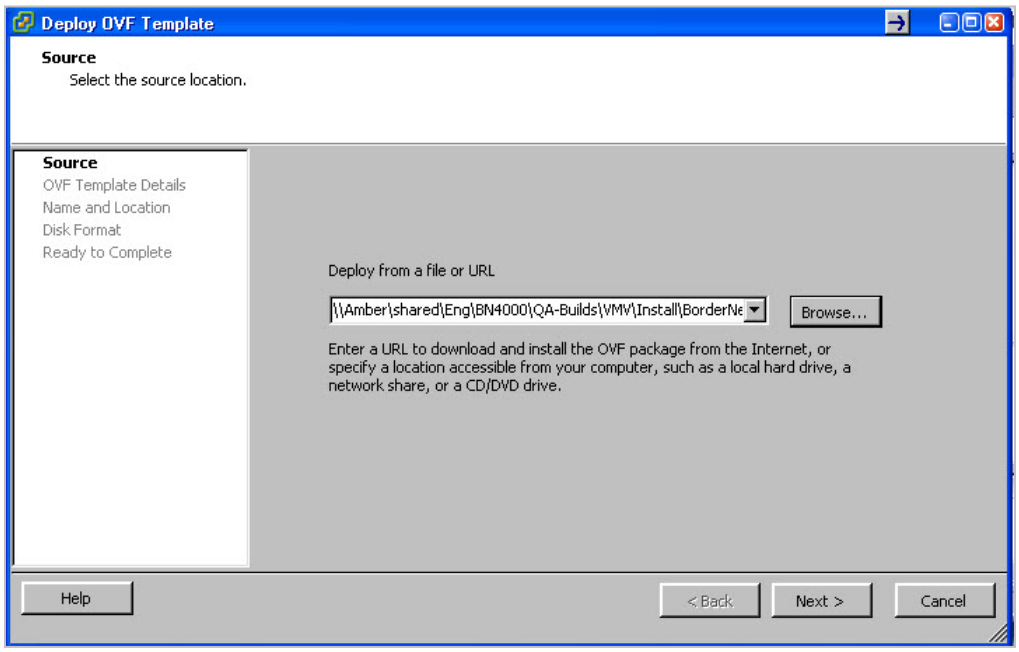


- Once you have downloaded the .ova file, save the file and make a note of its location.

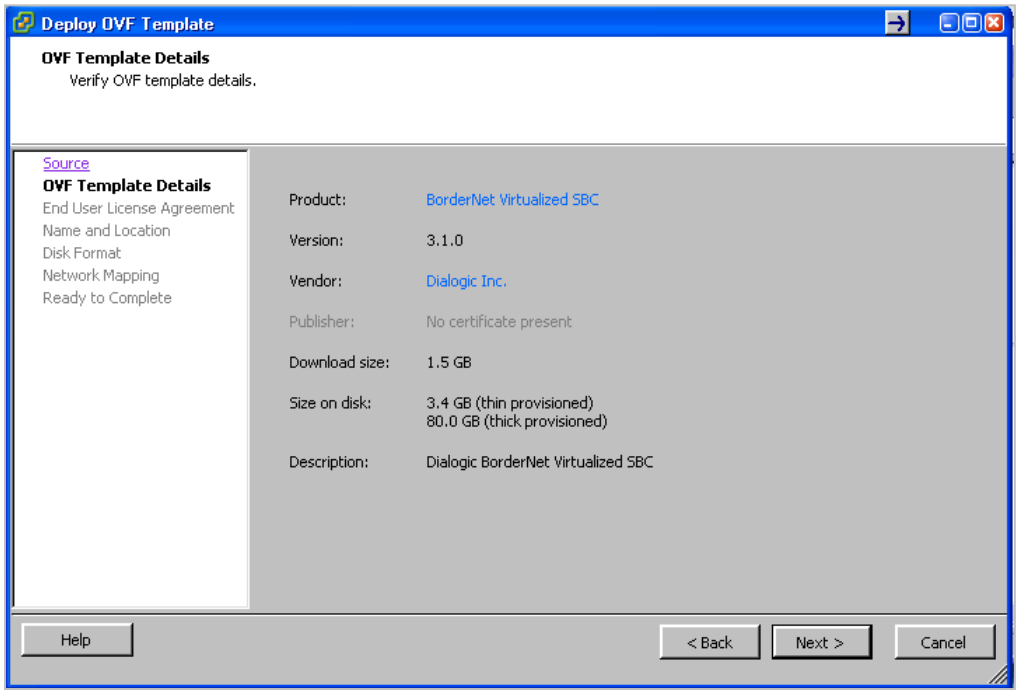
Deploying the BorderNet Virtualized SBC Virtual Machine

Use the following procedure to deploy the BorderNet Virtualized SBC Virtual Machine (VM) that is contained in the .ova file.

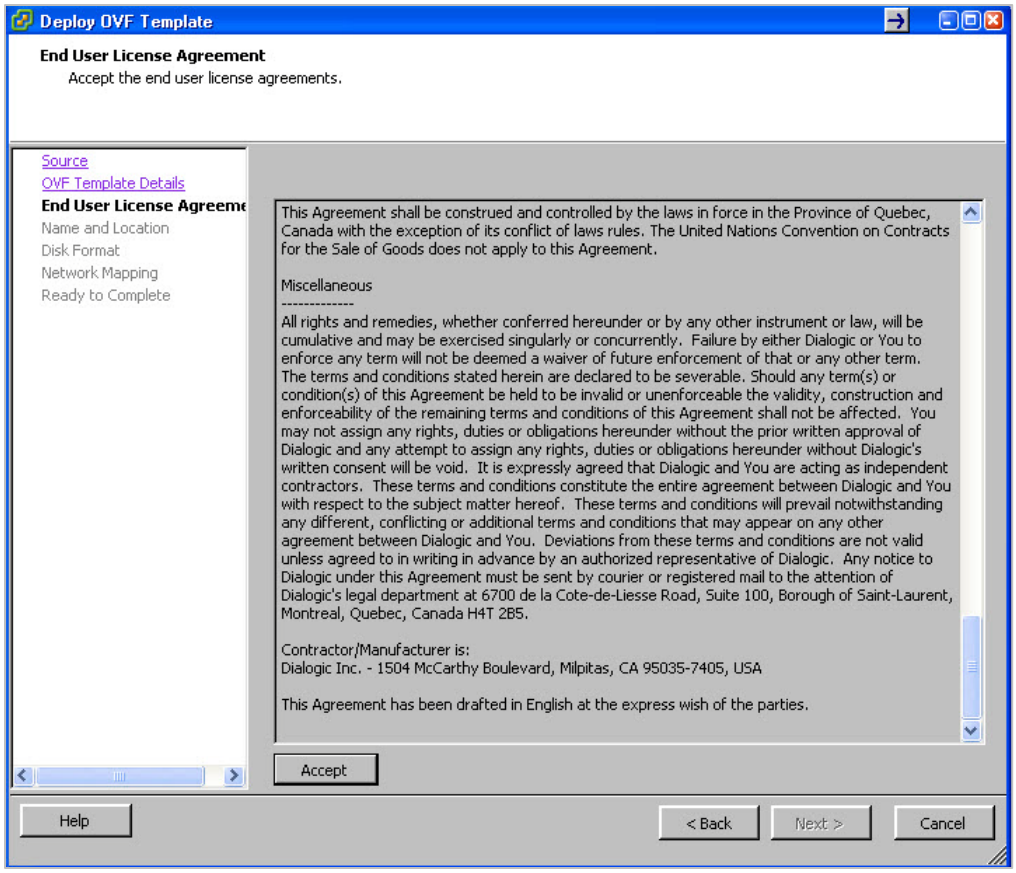
1. Open the VMWare Vsphere Client and select **File > Deploy OVF Template**.
2. Click the **Browse** button and locate the BorderNet Virtualized SBC **.ova** file.



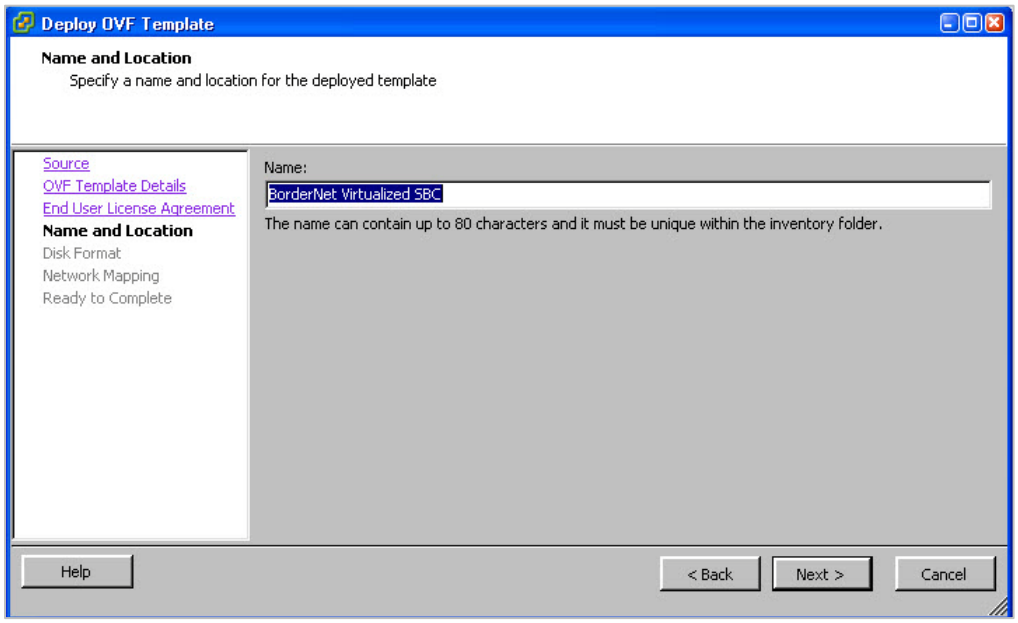
3. Click **Next** to review the OVF Template Details.



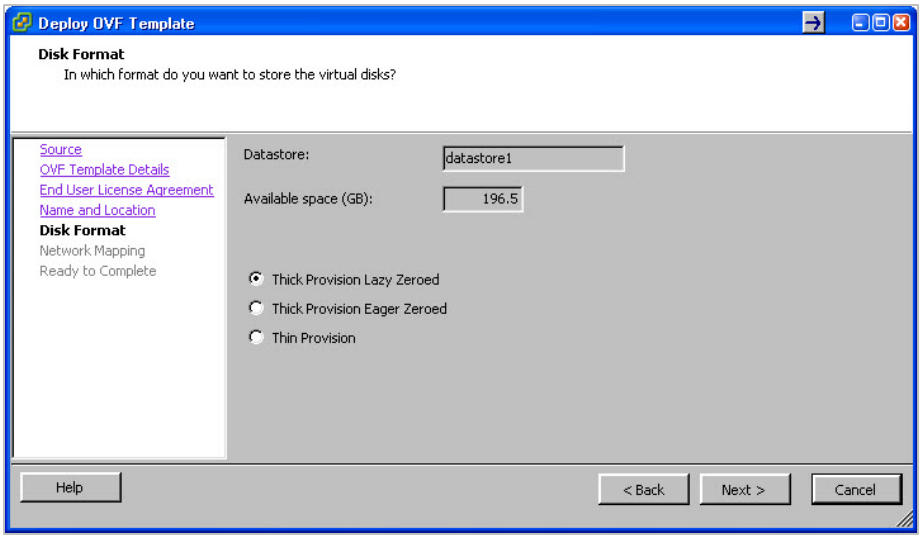
4. Click **Next** to review the End User License Agreement.



5. Read through the End User License Agreement and, if you agree, click **Accept**.
6. Click **Next**.
7. Enter a **Name** for your VM instance, or use the default **BorderNet Virtualized SBC** name.



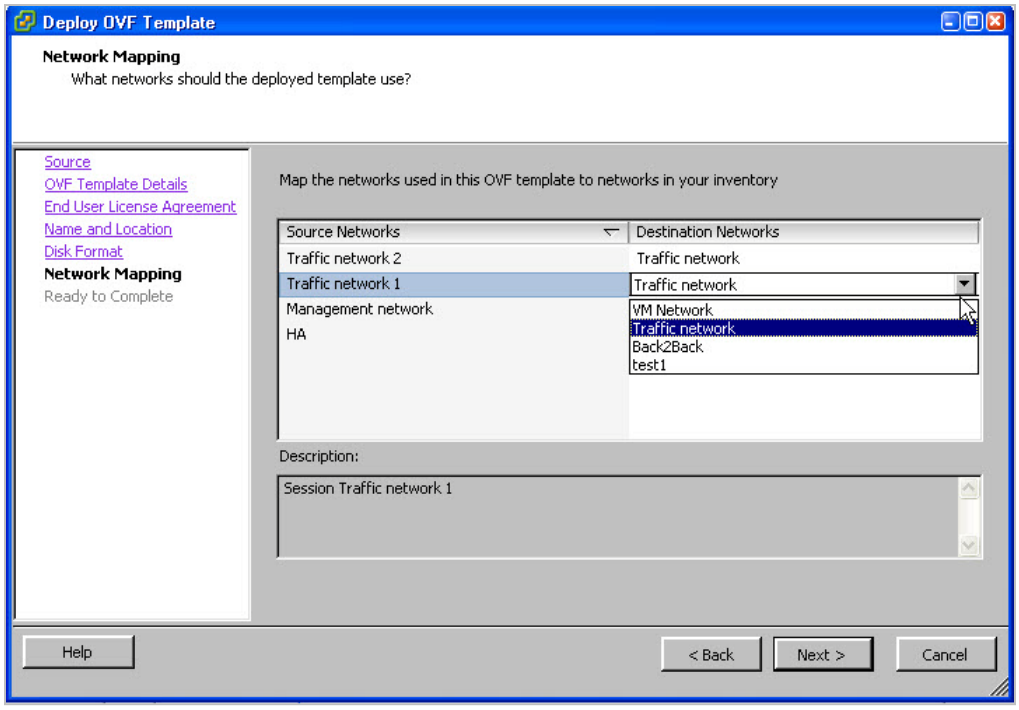
8. If prompted, select the **Host/Cluster** to run BorderNet Virtualized SBC VM instance and click **Next**.
9. Format the virtual disks:
    a. Select the **Datastore** (storage) location for the virtual disk space required by this VM instance.



    b. Select the Provisioning: **Thick Provision Lazy Zeroed**, **Thick Provision Eager Zeroed**, or **Thin Provision**.

    Refer to the *VMware vSphere ESXi and vCenter Server 5 Documentation* (www.vmware.com) for additional information.
10. Click **Next** to view the Network Mapping screen. The destination networks are the ones you created during the Hypervisor installation (see the Hypervisor Logical Network Example).
11. Use the drop-down list to connect the **Source Networks** to the **Destination Networks**. This connects the Virtual network adapters on the BorderNet Virtualized SBC VM (Source Networks) to the Logical Networks (Destination Networks) in your virtualized environment.

    Note: Source Networks are defined in the .ova file and automatically populated in the Network Mapping screen.



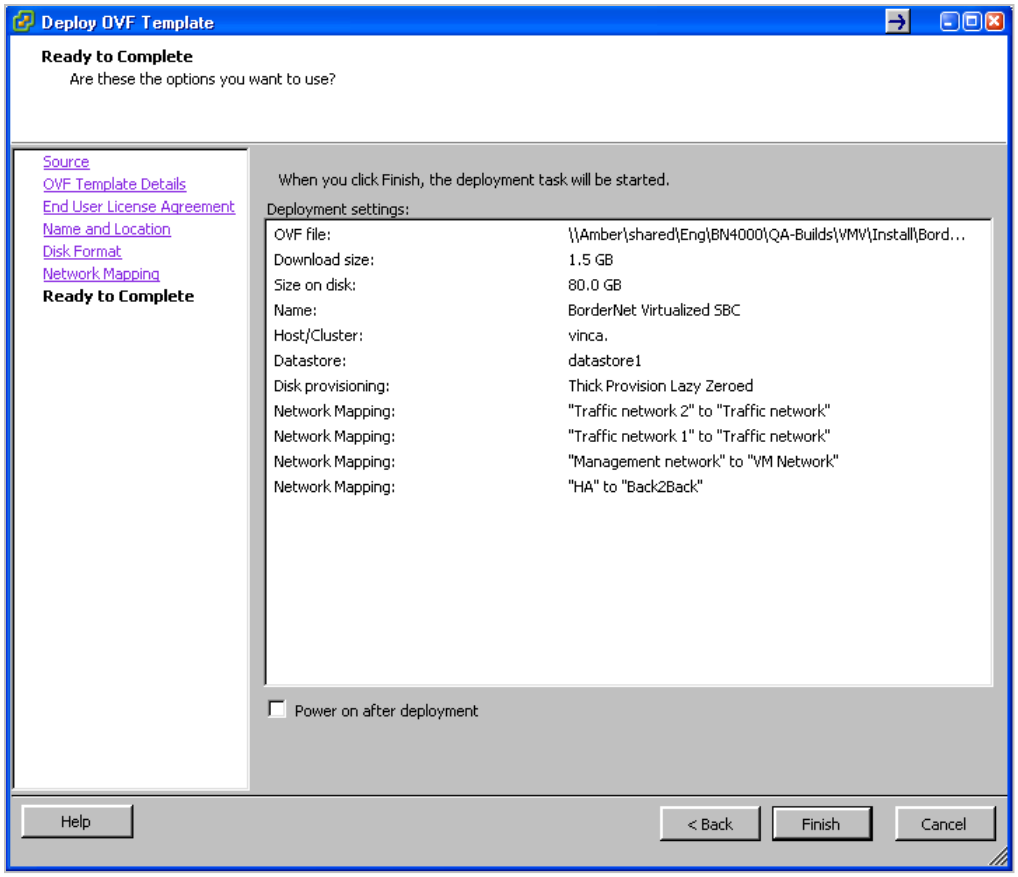
a. Connect the Source Network labeled **Management network** to your destination's Logical Management network.

b. Connect the Source Network labeled **Traffic network1** to your Destination's Session traffic network (for example, Core/Trusted network).

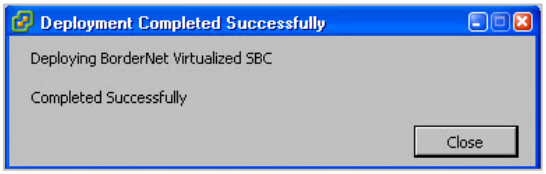
c. Connect the Source Network labeled **Traffic network2** to your Destination's Session traffic network (for example, Interconnect/Public network).

d. For HA configurations only: connect the Source Network labeled **HA network** to your Destination's logical network dedicated for network traffic between VM instances that form the HA pair.

12. Click **Next** to review your deployment settings.



13. Click **Finish** to complete the BorderNet Virtualized SBC Virtual Machine deployment. The deployment may take a few minutes.

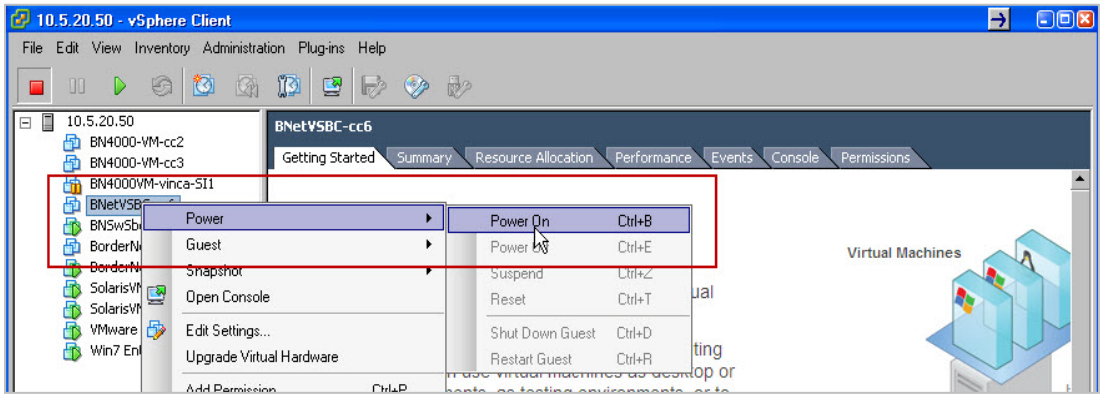


14. When the deployment is complete, click **Close**.

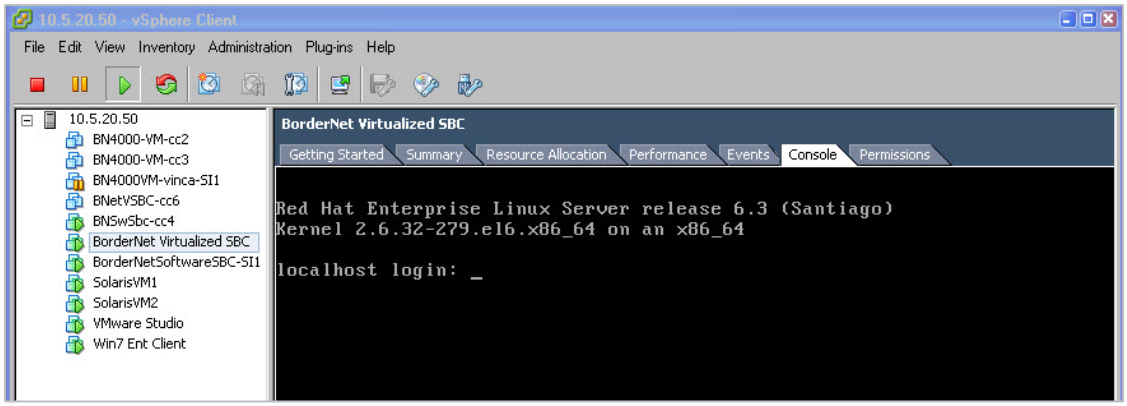
Setting Up the Web-Based Management System

After the BorderNet Virtualized SBC VM instance is deployed, use the following procedure to access the Console and set-up your web-based management system.

1. From the vSphere Client, right-click the VM instance and select **Power > Power ON**.

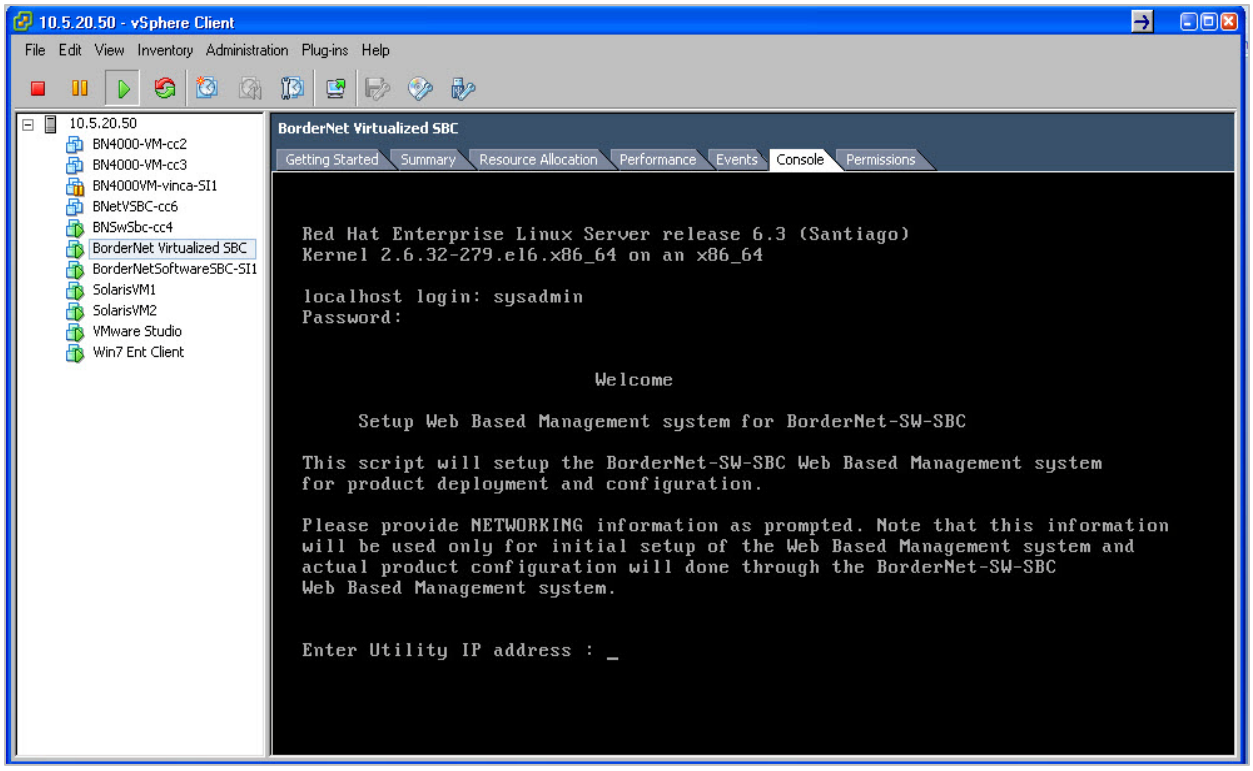


2. From the VMware vSphere Client interface, select your virtual machine's **Console** tab. The login prompt on the Console appears.



3. Enter the default user name and password:
   a. At the **localhost login** prompt, enter **sysadmin** and press **Enter**.
   b. At the **password** prompt, enter **dia10gic** (note that the number "10" is embedded in the default password), and press **Enter**.

Note: Change the default password (**dia10gic**) after the initial setup is complete.



4. Enter the **Utility IP address**, **Netmask**, and **Gateway IP address** information at the command prompts. It is recommended to use the IP address from the subnet that is accessible from your logical Management Network.

   Note: This may take a few minutes. When the process is complete, you will see the following information.

```
Assigning IP address 10.2.2.107 and netmask 255.255.255.0
to the eth0 interface  ..... Done.

Adding default gateway 10.2.2.1 ..... Done.

Setting up Web Based Management system,
This may take few minutes,
please wait ...

Web Based Management system is now ready for product deployment.

Access the Web MS at http://10.2.2.107/
and continue with the product deployment and configuration.
```

5. Using a different PC or virtual machine instance, open a browser and use the IP address configured above to access the BorderNet Virtualized SBC WebUI (for example, https://10.2.2.107).This will connect to the BorderNet Virtualized SBC Deployment GUI.

   The web-based management system set-up is complete.

Obtaining a License File

Use the following procedure to obtain a License file.

Prerequisites

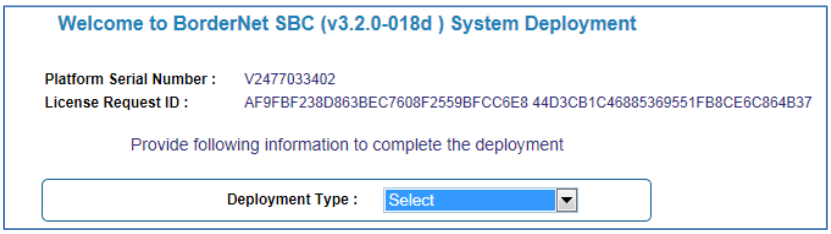
Before beginning the procedure, have the following information available:

- Your sales order number or purchase order number.
- A work email address at your company's work domain.
- You must have loaded the BorderNet Virtualized SBC on your server and have the following information from the installation:
    - Platform Serial Number
    - License Request ID
    - Platform Serial Number 2 (for HA systems only)
    - License Request ID Number 2 (for HA systems only)

Use the following procedure to obtain the Platform Serial Number and License Request ID.

1. From the vSphere Client, right-click your BorderNet Virtualized SBC VM instance and select **Power > Power ON**.
2. From a PC or VM, open a browser and enter the **Utility IP Address** to access the web-based management interface (this can be accessed from any laptop that can access the management network).
3. If a message appears indicating that the certificate is untrusted, choose **Continue**. The certificate for the BorderNet Virtualized SBC will be made trusted in a subsequent procedure.

   The initial deployment screen appears:

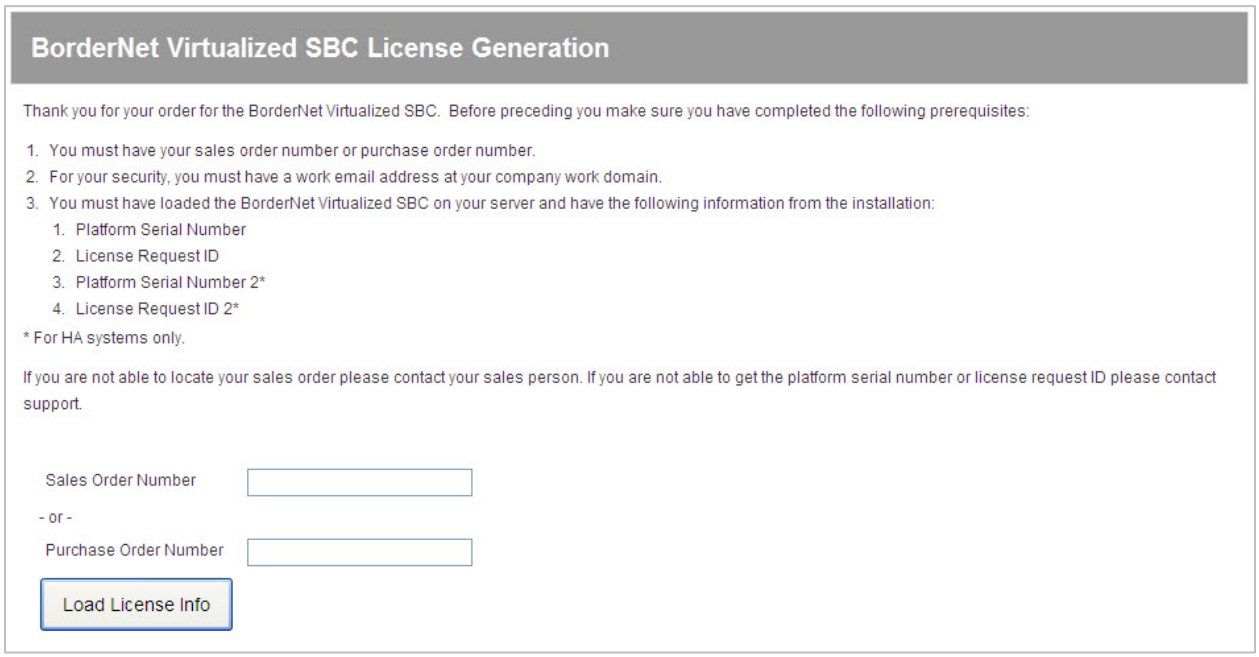


4. Copy the **Platform Serial Number** and **License Request ID** and paste that information into a text or other file.

Procedure

Use the following procedure to obtain a License file.

1. Open a browser window and go to http://www.dialogic.com/en/license/virtualized-sbc.aspx to open the **BorderNet Virtualized SBC License Generation** screen.



2. Enter the **Sales Order Number** or **Purchase Order Number**.
3. Click **Load License Info**.
4. Follow the screen instructions to obtain your license file(s).

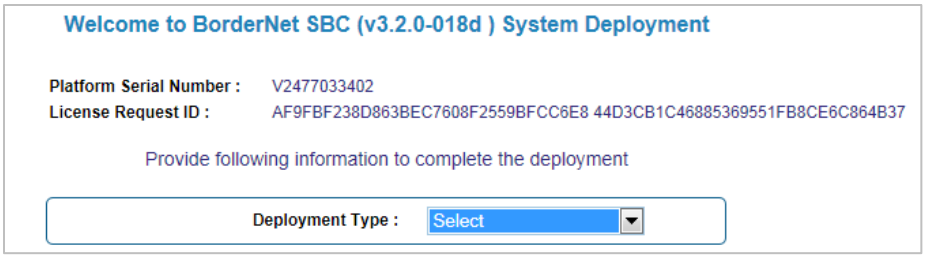
Initial System Set-Up

Select the appropriate procedure to set-up your BorderNet Virtualized SBC:

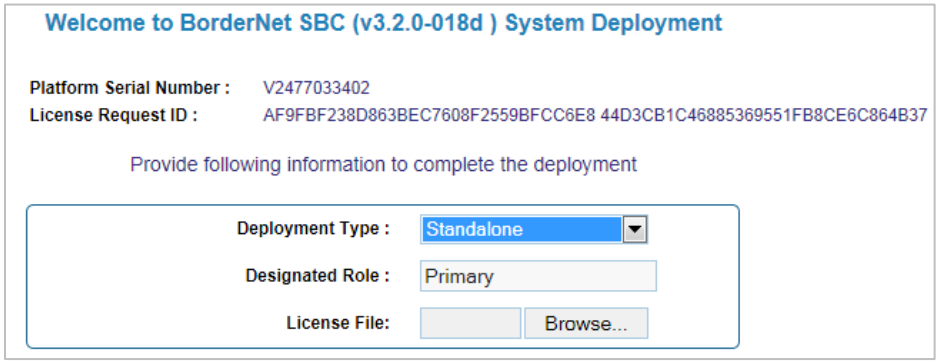
- Configuring a Standalone System
- Configuring a High Availability System

Configuring a Standalone System

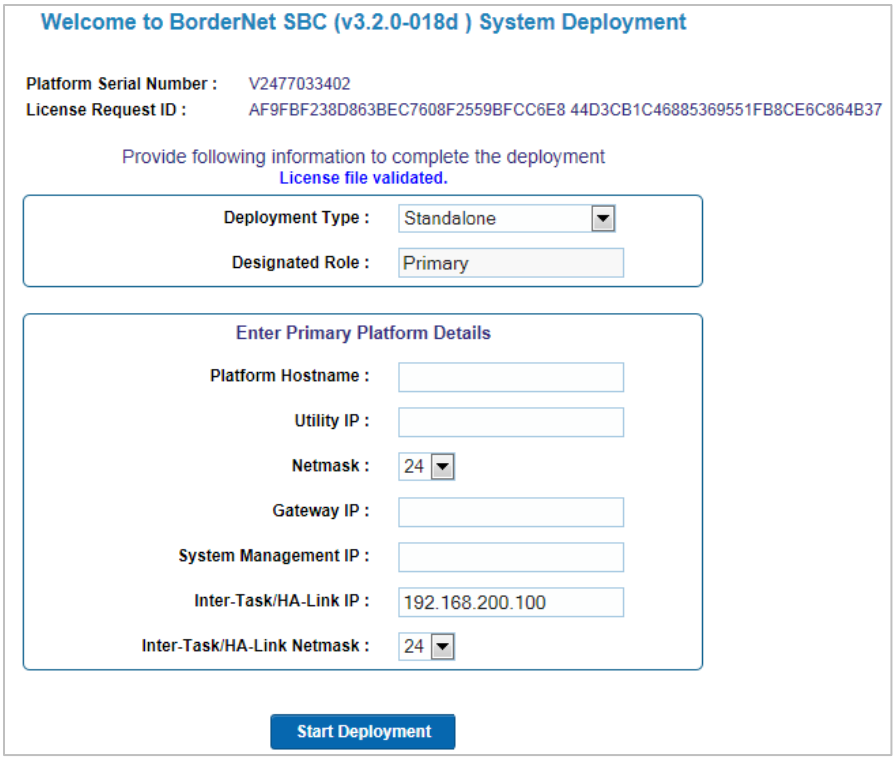
1. From the vSphere Client, right-click your BorderNet Virtualized SBC VM instance and select **Power > Power ON**.
2. Open a browser window and use the **Utility IP Address** to access the web-based management interface.
3. If a message appears indicating that the certificate is untrusted, choose **Continue**. The certificate for the BorderNet Virtualized SBC will be made trusted in a subsequent procedure.
4. Use a PC/virtual machine or laptop with a web browser that can reach the utility IP address to start the deployment process.
5. Select **Standalone** for the **Deployment Type**.



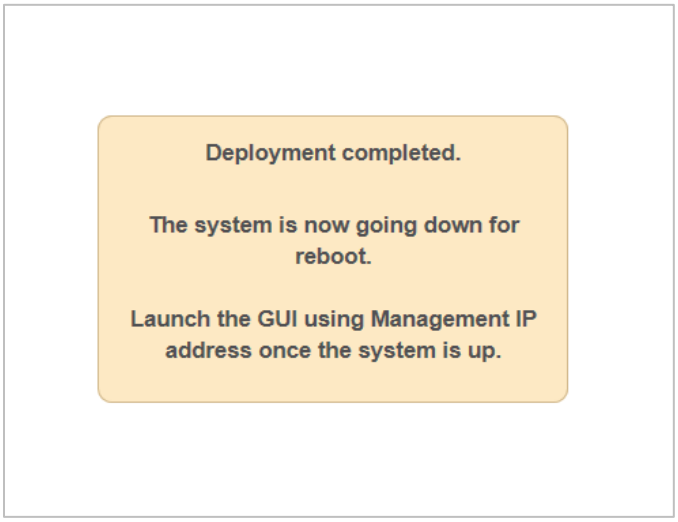
6. Select **Primary** as the **Designated Role**.



7. Click the **Browse** button and select the license file.
8. Click **OK**.
9. Enter the Primary Platform Details:
    a. **Platform Host Name**, which can be any alpha-numeric entry (such as VSBC01).
    b. **Utility IP**
    c. **Netmask**
    d. **Gateway IP**
    e. **System Management IP**
    f. **Inter-Task/HA-Link IP**. This must be configured regardless of whether you are setting up an HA or a Standalone System. This IP address must be from a different subnet than the System Management IP address.



10. Click **Start Deployment**.
11. Once the deployment is complete, the following screen appears:



You can now use the **System Management IP Address** to access the BorderNet Virtualized SBC WebUI.

Note: You must be on the same subnet as the System Management IP Address to access the Management Interface.

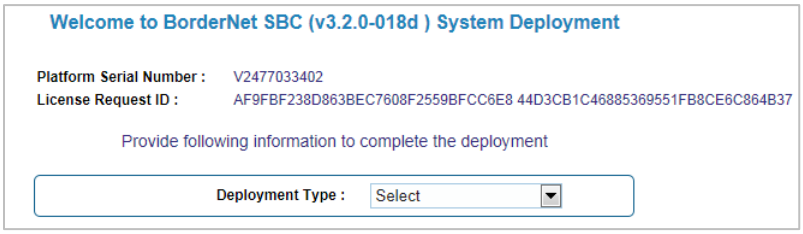
Configuring a High Availability System

For High Availability (HA) configurations, you will:

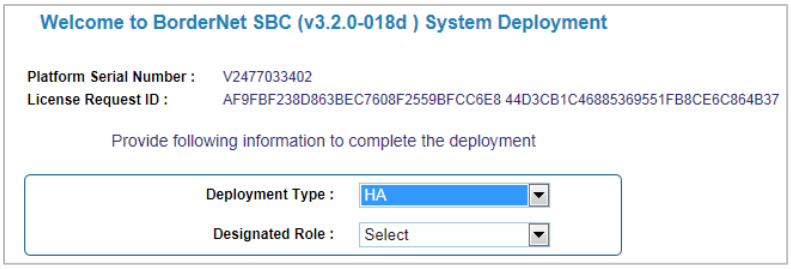
- Deploy the primary virtual instance (see Deploying the BorderNet Virtualized SBC Virtual Machine).
- Connect the secondary instance to the primary instance on the HA network (refer to the Hypervisor Logical Network Example).
- Ensure the primary instance is up and running.
- Deploy the secondary instance.

Use the following procedure to configure an HA system.

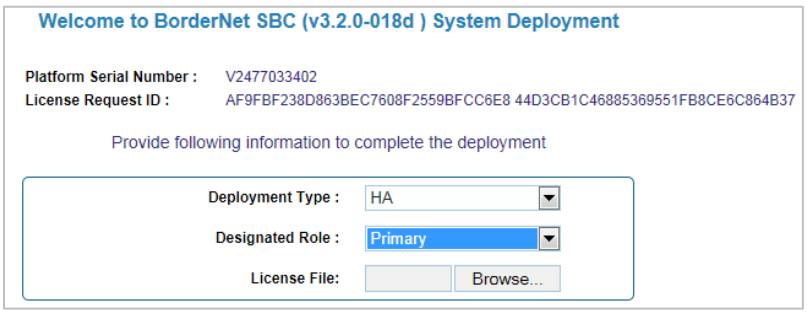
1. From the vSphere Client, right-click your BorderNet Virtualized SBC VM instance and select **Power > Power ON**.
2. Open a browser window and use the **Utility IP Address** to access the web-based management interface.
3. If a message appears indicating that the certificate is untrusted, choose **Continue**. The certificate for the BorderNet Virtualized SBC will be made trusted in a subsequent procedure.
4. From the **System Deployment** screen, select **HA** for the **Deployment Type.**



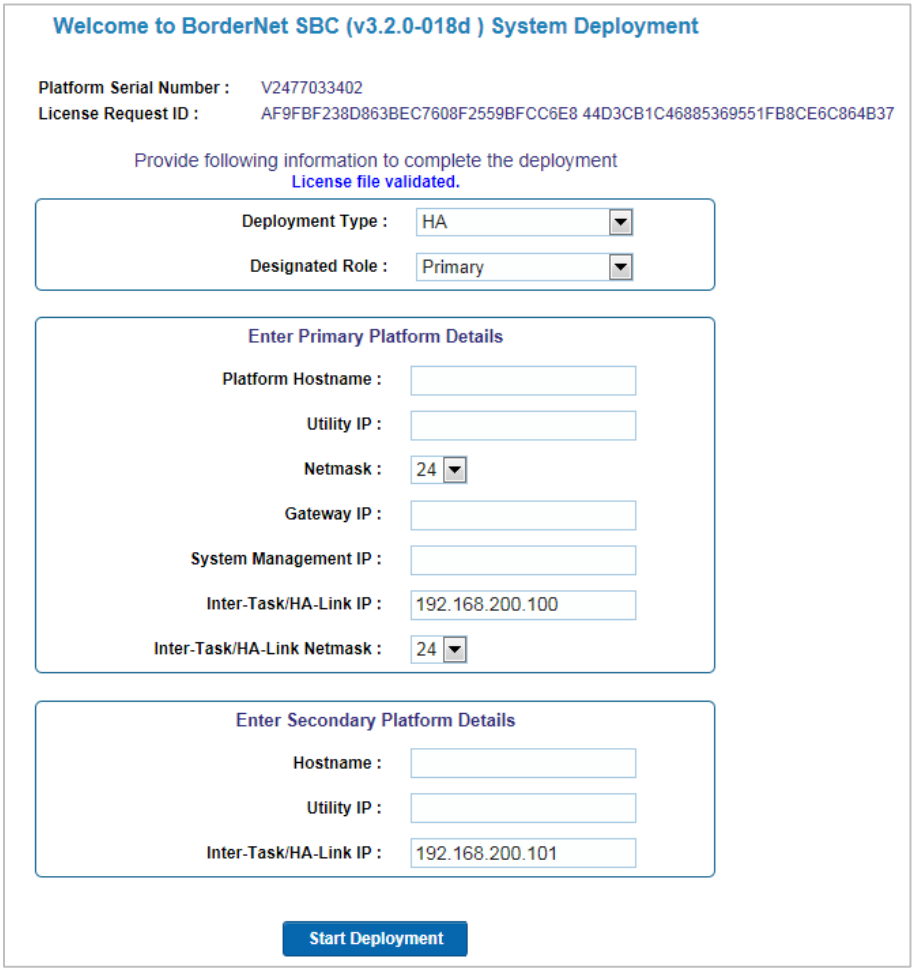
5. Select **Primary** for the **Designated Role**.



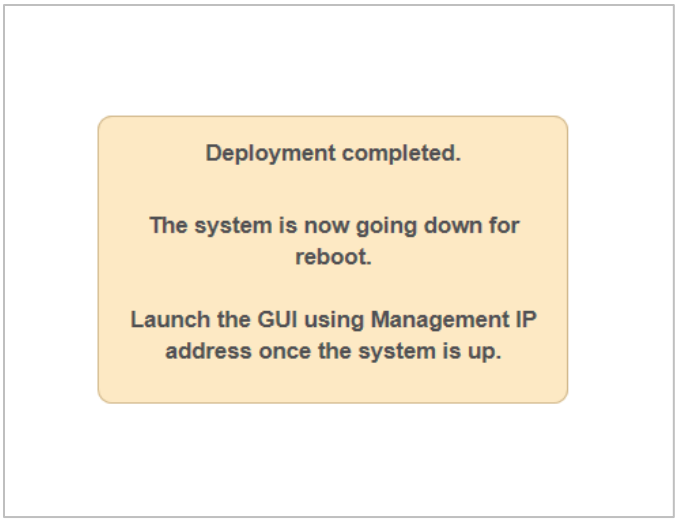
6. Click the **Browse** button and select the license file.



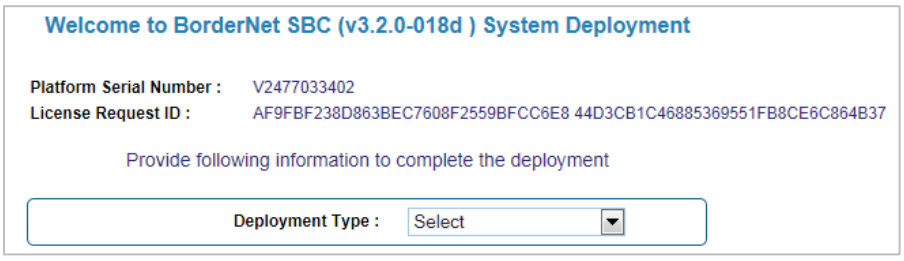
7. Click **OK**.
8. Enter the Primary Platform Details:
    a. **Platform Host Name**, which can be any alpha-numeric entry
    b. **Utility IP**
    c. **Netmask**
    d. **Gateway IP**
    e. **System Management IP**
    f. **Inter-Task/HA-Link IP** for each virtual instance on the same HA network. This IP address must be from a different subnet than the System Management IP address.
    g. Select the **Inter-Task/HA-Link Netmask** from the drop-down list.



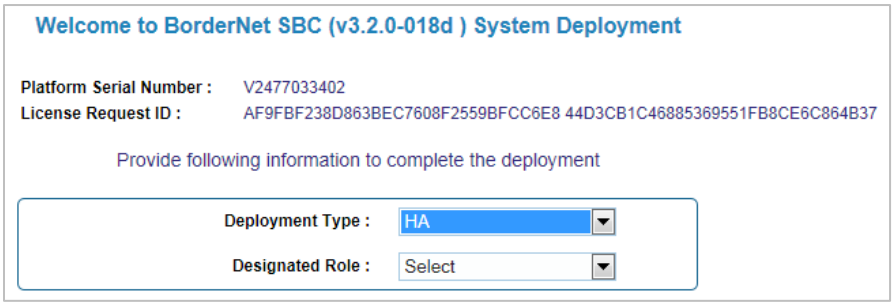
9. Click **Start Deployment**.
10. Once the deployment is complete, the following screen appears:



11. From a browser window, use the **Utility IP Address** to access the web-based management interface for the secondary BorderNet Virtualized SBC.
12. Select **HA** for the **Deployment Type.**

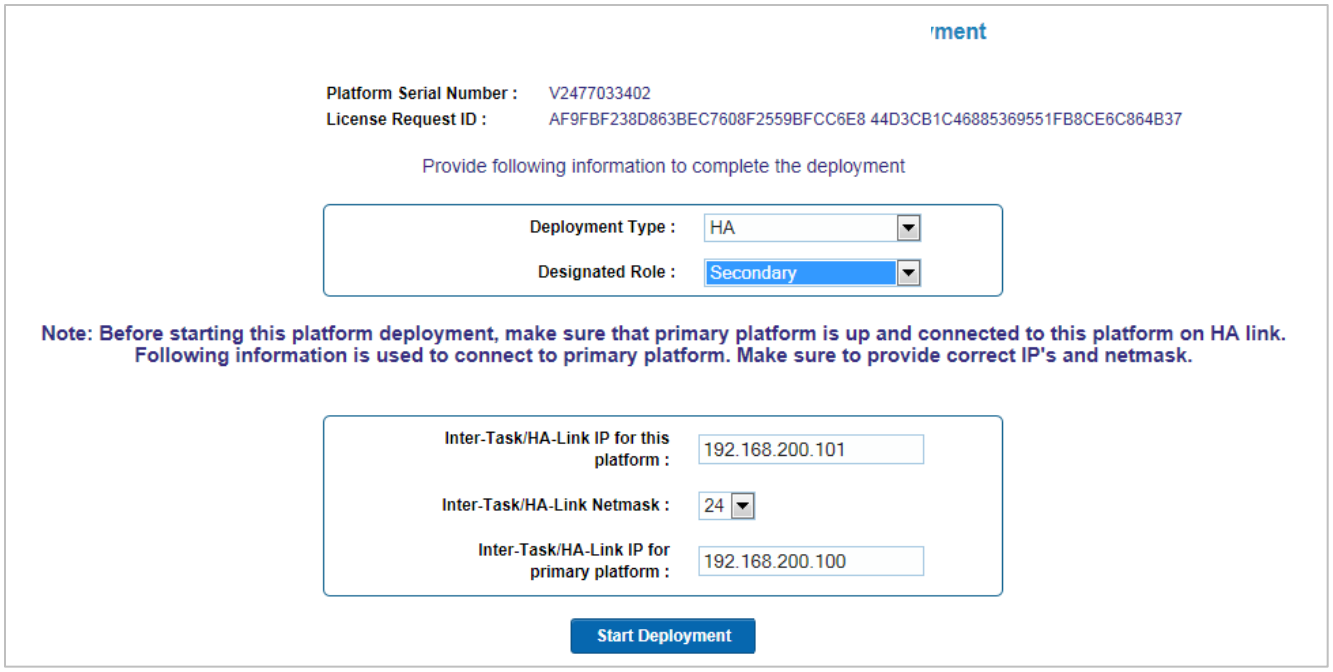


13. Select **Secondary** for the Designated Role.



14. Enter the **Inter-Task/HA-Link IP** for the current (secondary) platform.
15. Select the **Inter-Task/HA-Link Netmask** from the drop-down list.
16. Enter the **Inter-Task/HA-Link IP** for the primary platform.

Note: You must provide a unique **Inter-Task/HA-Link IP** for each virtual instance on the same HA network.



17. Click **Start Deployment**.

You can now use the **System Management IP Address** to access the BorderNet Virtualized SBC WebUI.

Note: You must be on the same subnet as the System Management IP Address to access the Management Interface.

Changing the BorderNet Virtualized SBC System Configuration

Redeploy the BorderNet Virtualized SBC to change the basic system configuration, such as:

- System management IP address
- HA link IP address
- Utility IP address
- Converting a standalone to an HA system (and vice versa)

Caution: Redeployment requires a system restart, which could be traffic-affecting. For a live system, only perform redeployment during a maintenance window.

Guidelines

You must have System Manager privileges to redeploy a system, and the redeployment screen can only be accessed from the System Management WebUI (using the System Management IP address). Redeployment does not affect the system configuration and provisioning data.

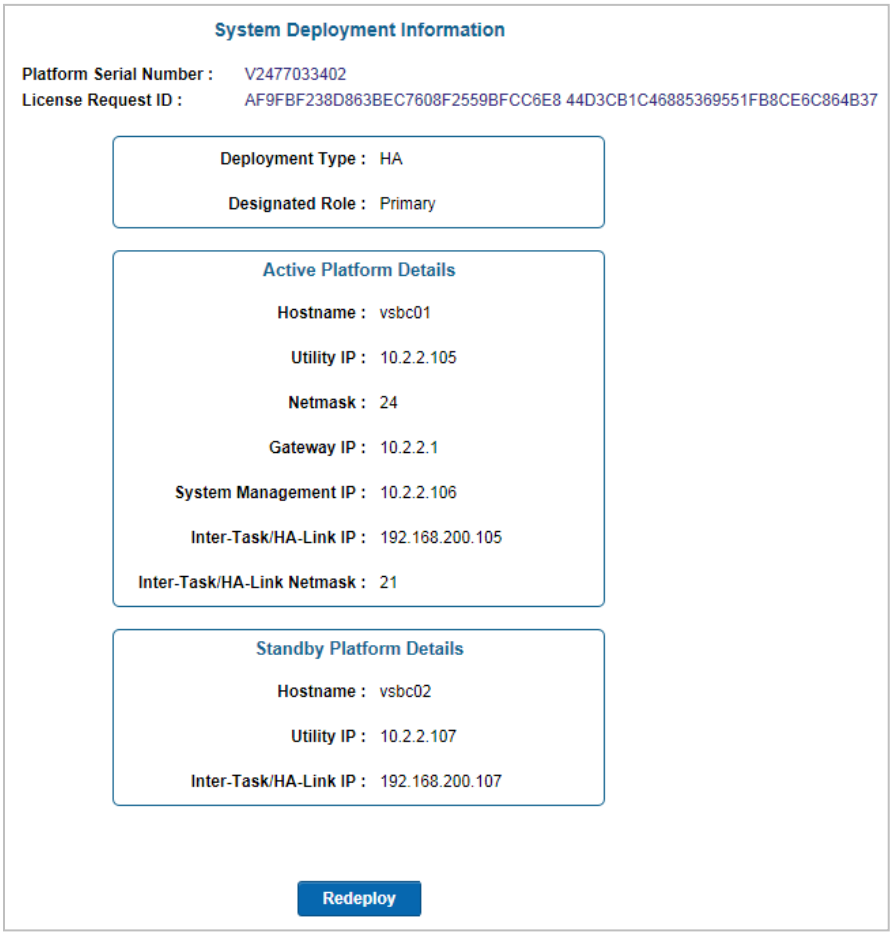
For HA configurations only:

- Existing data on the chosen primary platform is retained.
- Both the primary and secondary platform must be redeployed.
- Redeploy the primary platform before the secondary platform.
- The primary platform must be running and connected to secondary platform when you redeploy the secondary platform.

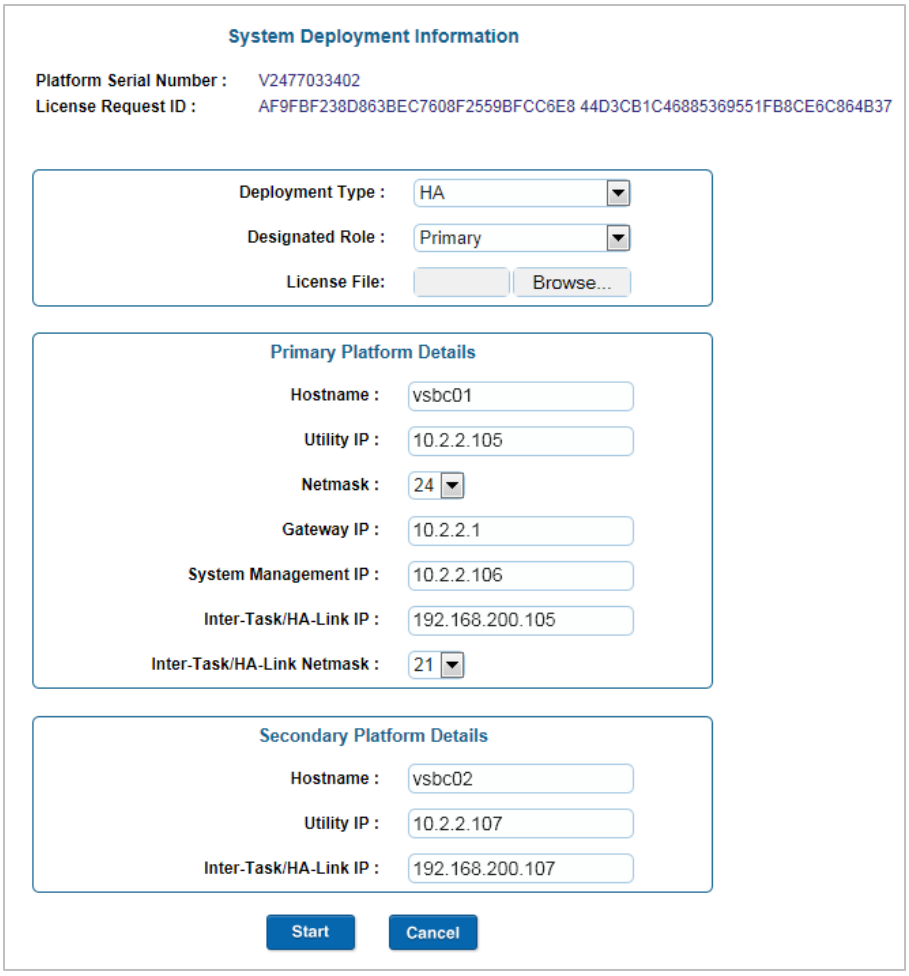
Procedure

The following procedure provides an example of a redeployment.

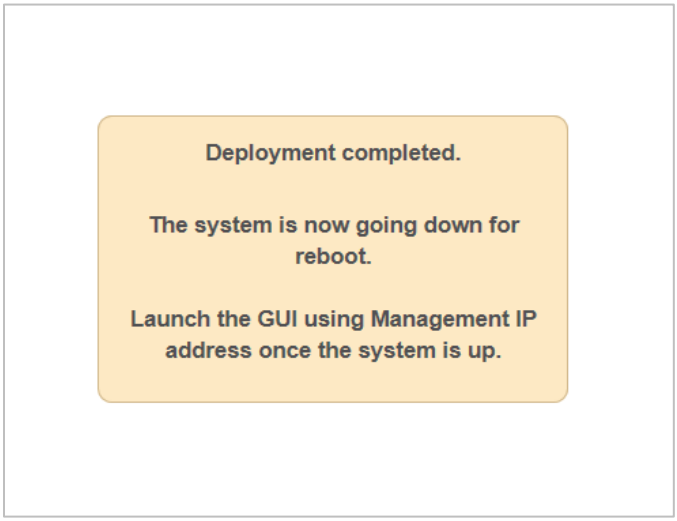
1. From **System** menu, select **Administration > Deployment** to access the System Deployment Information screen.



2. Click **Redeploy** to edit the values. The following screen appears:



3. Make the desired changes and click **Start**.
4. Once the redeployment is complete, the following screen appears:



4. Accessing the BorderNet Virtualized SBC WebUI

After the installation and deployment are complete, the BorderNet Virtualized SBC can be accessed via a web browser. The following web browsers are supported:

- Internet Explorer 8 and above
- Mozilla Firefox 5 and above

Note: **For first-time access, the host running the browser must be in the same subnet as the BorderNet Virtualized SBC System Management IP address.**

First-Time Access

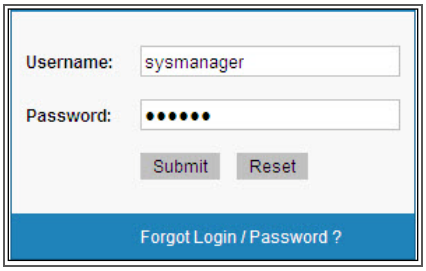
Use the following procedure to access to the BorderNet Virtualized SBC.

1. Enter the **System Management IP Address** into a browser.

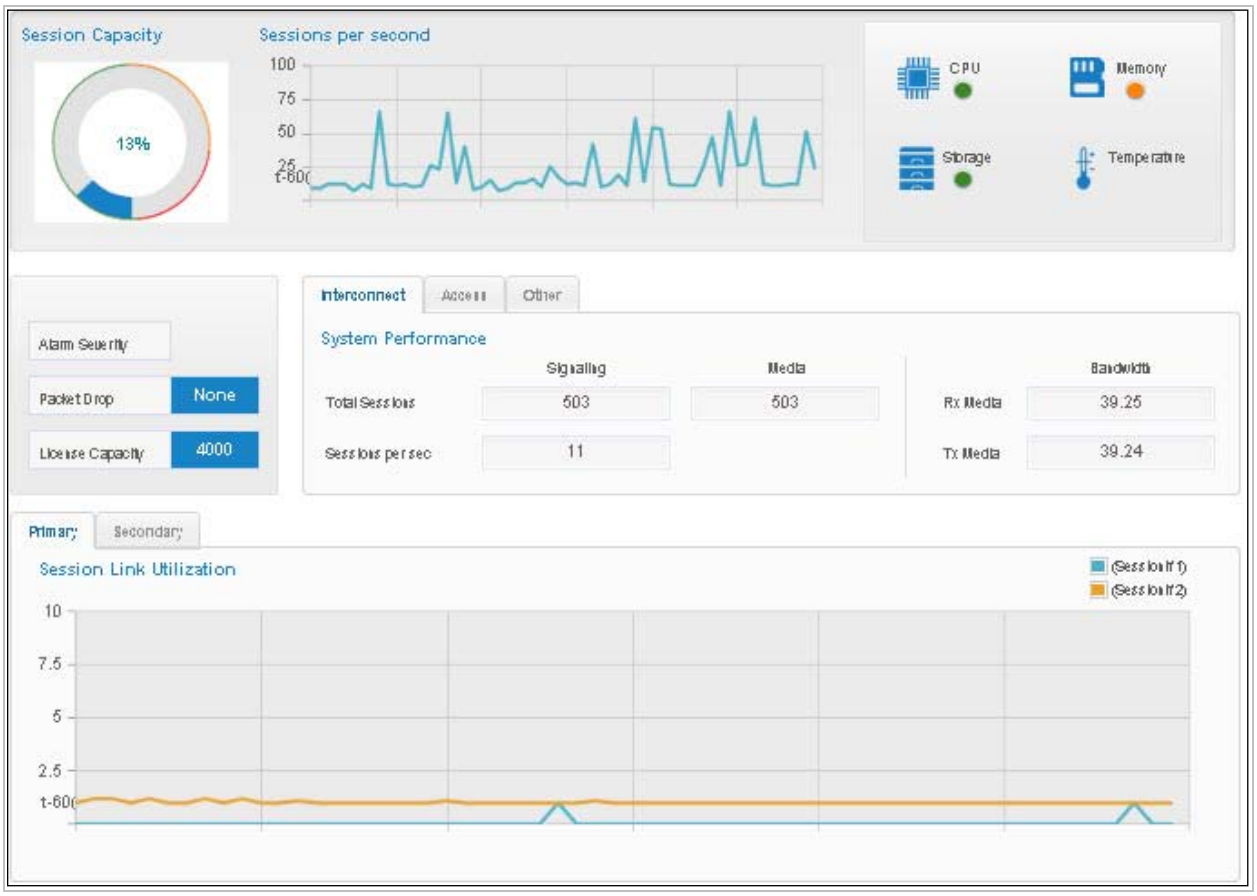
   Note: All http:// requests are automatically redirected to https:// requests.

2. If a message appears indicating that the certificate is untrusted (below), choose **Continue to this website**. The certificate for the BorderNet Virtualized SBC will be made trusted in a subsequent procedure.

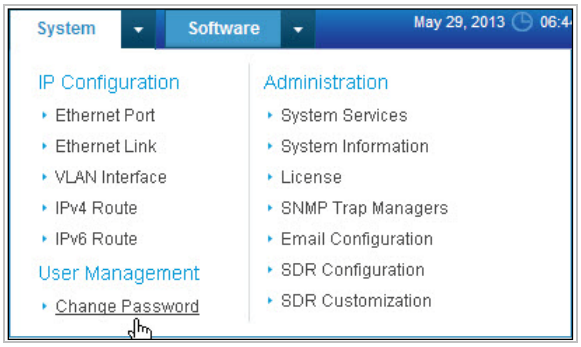
3. Login as the system administrator. For the initial login, the username is **sysmanager**, and the password is **SYSMGR**.



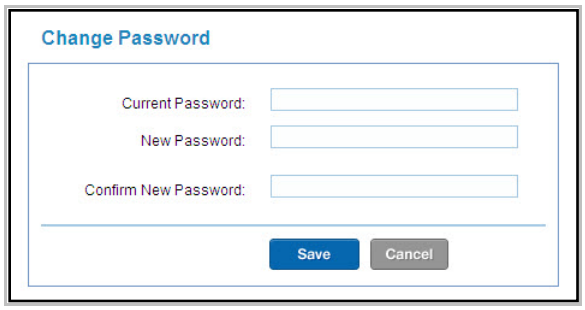
4. The **BorderNet Virtualized SBC Dashboard** screen appears.



5. From the **System** drop-down menu, select **User Management > Change Password**.



The **Change Password** screen appears.



6. Enter **SYSMGR** in the **Current Password** field.
7. Enter a new password in the **New Password** and **Confirm New Password** fields.
8. Click **Save**.

The initial login is complete.

Note: To enable a browser from a different subnet to access the BorderNet Virtualized SBC, that subnet must be added to the Access Control List (ACL). See "User-Defined ACLs" in the *Dialogic® BorderNet Virtualized SBC Configuration and Provisioning Guide* for instructions on creating ACLs.

Making Certificates Trusted

When the BorderNet Virtualized SBC URL is initially entered into a browser, a security warning appears about the certificate. This warning occurs because the BorderNet Virtualized SBC contains a self-signed digital certificate.

The BorderNet Virtualized SBC URL must be added to the browser as a trusted, secure site to resolve the certificate error. The procedure you follow depends on which browser you are using:

- Internet Explorer
- Mozilla Firefox

Internet Explorer

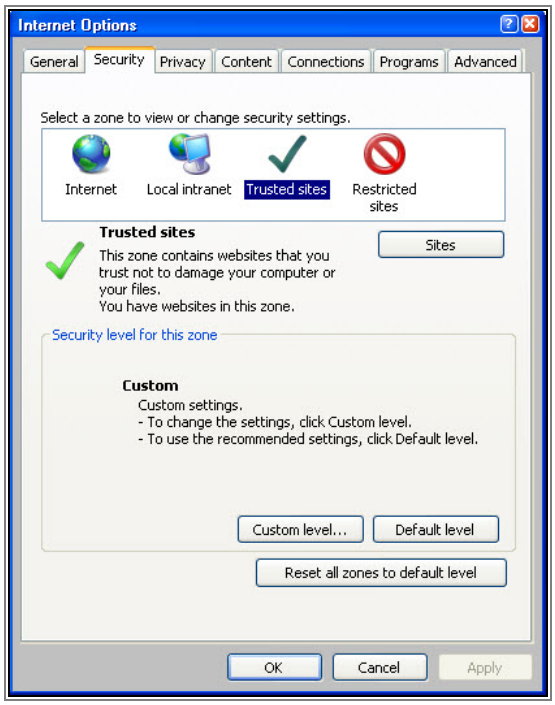
For Internet Explorer 9, first add the URL to Trusted Sites and then install the certificate.

For Internet Explorer 8, proceed directly to installing the certificate.

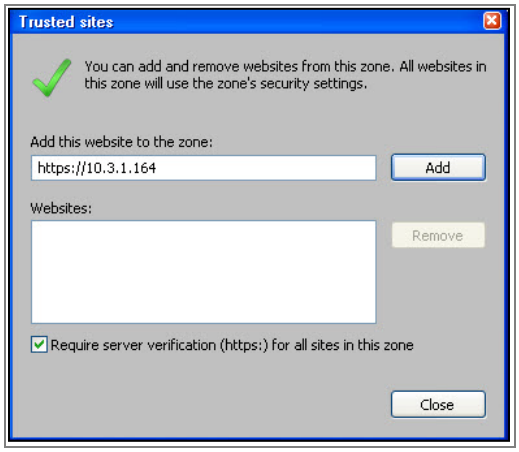
Adding the URL to Trusted Sites

Use the following procedure to add the BorderNet Virtualized SBC URL to Trusted Sites.

1. Open a browser window.
2. From the main menu, select **Tools > Internet Options > Security**.
3. Select **Trusted Sites**.



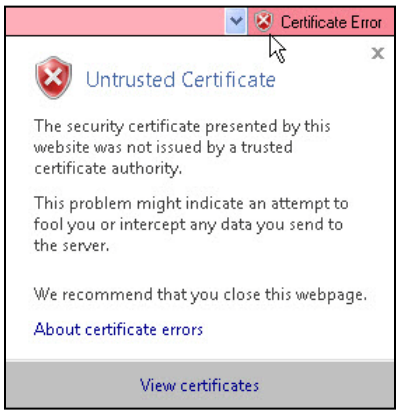
4. Click the **Sites** button. The **Trusted Sites** dialog box appears.



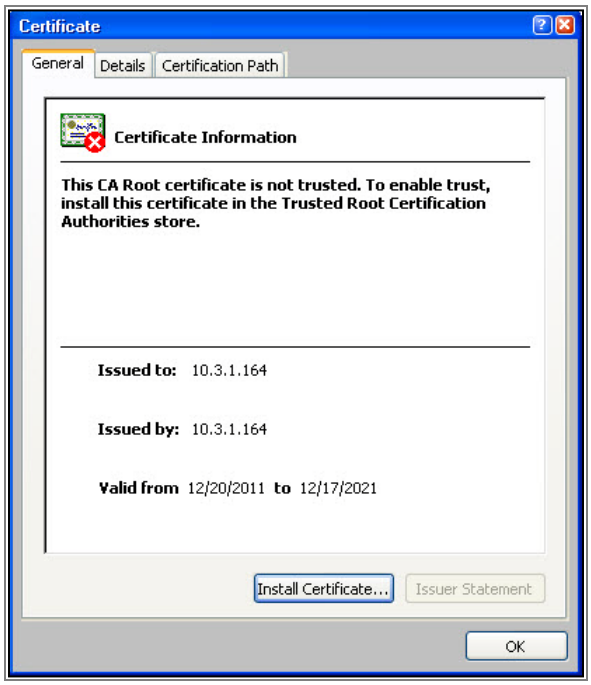
5. Enter the BorderNet Virtualized SBC web URL into the **Add this website to the zone:** field.
6. Click **Add**.
7. Click **Close**. Proceed to the Installing the Certificate procedure.

Installing the Certificate

1. Enter the BorderNet Virtualized SBC URL into the Internet Explorer browser.
2. Select **Continue to this website**.
3. Click the security icon next to the **Certificate Error**, and then select **View Certificates** at the bottom of the screen.

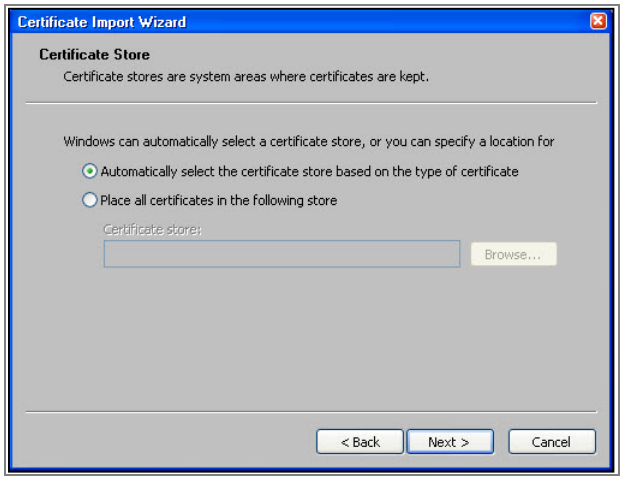


The **Certificate** information screen appears.

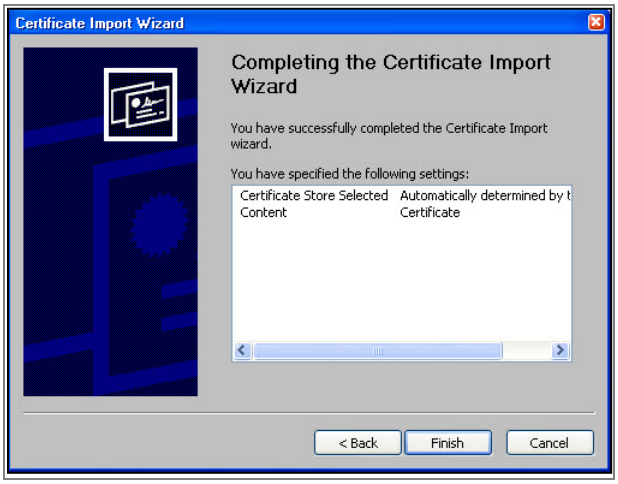


4. Verify that the Certificate Information is issued to the BorderNet Virtualized SBC IP address.
5. Click **Install Certificate**.
6. Click **OK**. The **Certificate Import Wizard** screen appears.

7. Click **Next**. The **Certificate Store** screen appears.



8. From the Certificate Store, select **Automatically select the certificate based on the type of certificate**.
9. Click **Next**. The **Completing the Certificate Import Wizard** screen appears.



10. Click **Finish**. A **Security Warning** appears.

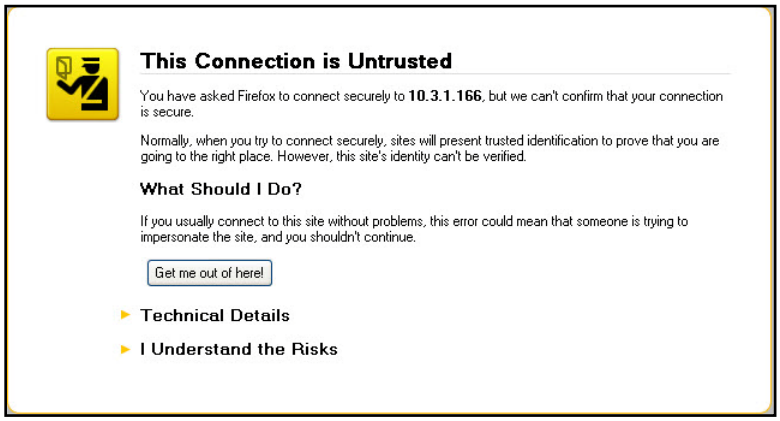
11. Click **Yes** to save the certificate.

The BorderNet Virtualized SBC security certificate will now work with Internet Explorer as a trusted site.

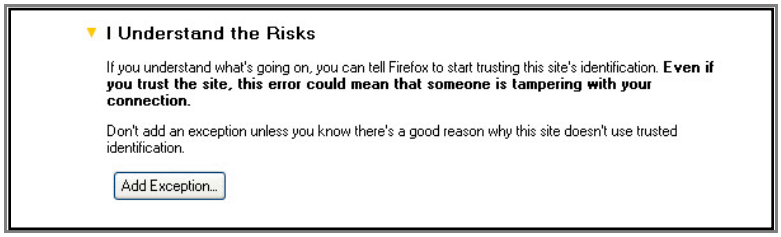
Mozilla Firefox

Use the following procedure to add the BorderNet Virtualized SBC URL to the Mozilla Firefox Exception List.

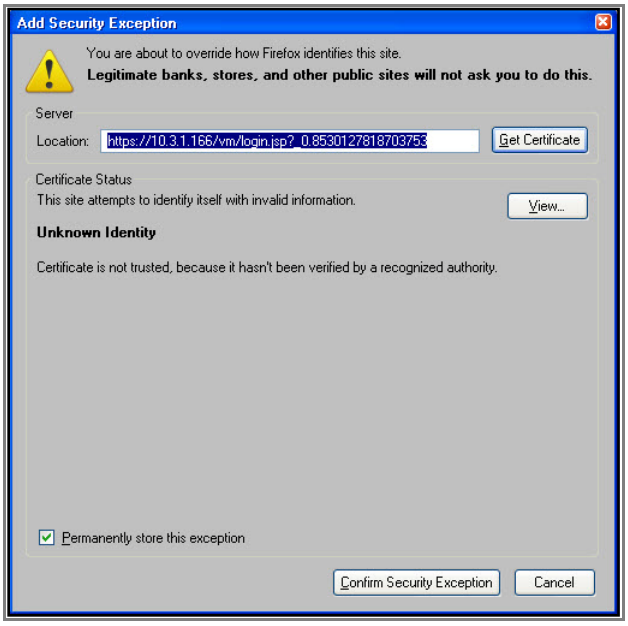
1. Open a browser window and enter the BorderNet Virtualized SBC URL. The following warning appears:



2. Select **I Understand the Risks**.



3. Click **Add Exception**. The **Add Security Exception** window appears.



4. Verify that the **Permanently store this exception** box is checked.
5. Click **Confirm Security Exception**.

The BorderNet Virtualized SBC security certificate is permanently stored with Mozilla FireFox as a trusted certificate, and the BorderNet Virtualized SBC login screen appears.

5. Configuration and Provisioning

Once the initial login is complete, the BorderNet Virtualized SBC can be configured for user access and provisioned for carrying traffic. In order enable traffic turn-up, the following steps need to be followed:

1. Create VLANs.
2. Create SIP interfaces.
3. Create SIP peers.
4. Associate interfaces to peers.
5. Create static routes.

Refer to the *Dialogic® BorderNet Virtualized SBC Configuration and Provisioning Guide* for additional information and procedures for each of these steps.